Fudo Enterprise 6.3 - System Documentation

Fudo Security

October 29, 2026

Contents

1 About Documentation **1**

2 Layout Themes of the Admin Panel **2**

3 Introduction **4**

3.1 System Overview . . . 4
3.1.1 Session Monitoring & Recording . . . 4
3.1.2 Secret Management . . . 5
3.1.3 Just-in-time (JIT) Access . . . 5
3.1.4 Single Sign-on (SSO) . . . 5
3.1.5 Agentless Convenient Access . . . 6
3.1.6 Ai-powered Prevention . . . 6
3.1.7 Productivity Analyzer . . . 6
3.1.8 Rapid Deployment . . . 6
3.1.9 Compliance Support . . . 6
3.2 Available GUI Languages . . . 6
3.3 Licensing Model and License Limits . . . 7
3.4 Supported Protocols . . . 12
3.4.1 HTTP . . . 12
3.4.2 Modbus . . . 13
3.4.3 MS SQL (TDS) . . . 13
3.4.4 MySQL . . . 14
3.4.5 Oracle [BETA] . . . 14
3.4.6 PostgreSQL . . . 15
3.4.7 RDP . . . 15
3.4.8 SSH . . . 18
3.4.9 Telnet 3270 . . . 21
3.4.10 Telnet 5250 . . . 22
3.4.11 Telnet . . . 22
3.4.12 VNC . . . 23
3.4.13 X11 . . . 24
3.4.14 TCP . . . 24
3.4.15 Secret Checkout . . . 24
3.5 Deployment Scenarios . . . 25
3.6 Connection Modes . . . 26
3.7 User Authentication Methods and Modes . . . 28

3.8 Security Measures . . . 31
3.8.1 Data Encryption . . . 31
3.8.2 Backups . . . 31
3.8.3 Permissions . . . 31
3.8.4 Sandboxing . . . 31
3.8.5 Reliability . . . 32
3.8.6 Cluster Configuration . . . 32
3.9 Data Model . . . 33
3.10 Dashboard . . . 34
3.10.1 Widgets . . . 35
3.10.2 Adding, Customizing and Removind Dashlets . . . 35
3.10.3 Hard Drives Status Information . . . 36
3.11 Footer Information . . . 37
3.12 Third-Party Licenses . . . 37

4 System Deployment 39
4.1 Requirements . . . 39
4.2 Hardware Overview . . . 41
4.3 System Initiation . . . 47
4.3.1 Virtual Machine . . . 52
4.4 Accessing Fudo Enterprise Portals . . . 57
4.4.1 Admin Panel . . . 58
4.4.2 User Access Gateway . . . 59
4.4.3 Supported Web Browsers . . . 59

5 Quick Start 61
5.1 SSH . . . 61
5.1.1 Prerequisites . . . 61
5.1.2 Configuration . . . 61
5.1.3 Establishing Connection . . . 66
5.1.4 Viewing User Session . . . 66
5.2 SSH in Bastion Mode . . . 67
5.2.1 Prerequisites . . . 67
5.2.2 Configuration . . . 67
5.2.3 Establishing Connection . . . 72
5.2.4 Viewing User Session . . . 73
5.3 SSH in Bastion Mode with Jump Host Option . . . 74
5.3.1 Prerequisites . . . 74
5.3.2 Configuration . . . 74
5.3.3 Establishing a Connection . . . 78
5.4 RDP . . . 78
5.4.1 Prerequisites . . . 79
5.4.2 Configuration . . . 79
5.4.3 Establishing an RDP Connection with a Remote Host . . . 83
5.4.4 Viewing User Session . . . 85
5.5 RDP in Bastion Mode . . . 86
5.5.1 Prerequisites . . . 86
5.5.2 Configuration . . . 86
5.5.3 Establishing an RDP Connection with a Remote Host . . . 90
5.5.4 Viewing User Session . . . 92
5.6 Telnet . . . 93
5.6.1 Prerequisites . . . 94

5.6.2 Configuration . . . 94
5.6.3 Establishing a Telnet Connection with the Remote Host . . . 98
5.6.4 Viewing User's Session . . . 99
5.7 Telnet 5250 . . . 99
5.7.1 Prerequisites . . . 100
5.7.2 Configuration . . . 100
5.7.3 Establishing a Telnet Connection with the Remote Host . . . 104
5.7.4 Viewing User's Session . . . 106
5.8 PostgreSQL . . . 106
5.8.1 Prerequisites . . . 107
5.8.2 Architecture Overview . . . 107
5.8.3 Configuration Steps . . . 107
5.8.4 Establishing PostgreSQL Connection . . . 112
5.9 MySQL . . . 113
5.9.1 Prerequisites . . . 113
5.9.2 Configuration . . . 113
5.9.3 Establishing Connection with a MySQL Database . . . 117
5.9.4 Viewing User Session . . . 118
5.10 Oracle . . . 119
5.10.1 Prerequisites . . . 119
5.10.2 Architecture Overview . . . 119
5.10.3 Configuration Steps . . . 120
5.10.4 Establishing Oracle Connection . . . 124
5.11 MS SQL . . . 125
5.11.1 Prerequisites . . . 126
5.11.2 Configuration . . . 126
5.11.3 Establishing Connection with a MS SQL Database . . . 130
5.11.4 Viewing User Session . . . 131
5.12 HTTP . . . 132
5.12.1 Prerequisites . . . 133
5.12.2 Configuration . . . 133
5.12.3 Connecting to Remote Resource . . . 137
5.12.4 Viewing User Session . . . 138
5.13 VNC . . . 139
5.13.1 Prerequisites . . . 139
5.13.2 Configuration . . . 139
5.13.3 Establishing Connection . . . 143
5.13.4 Viewing User Session . . . 144

6 Sessions **145**
6.1 Filtering Sessions . . . 147
6.1.1 Defining Filters . . . 147
6.1.2 Saving Custom Filters . . . 148
6.1.3 Applying Custom Filters . . . 148
6.1.4 Editing Custom Filters . . . 149
6.1.5 Disabling Filters . . . 149
6.1.6 Deleting Custom Filters . . . 150
6.1.7 Full Text Search . . . 150
6.2 Viewing Sessions . . . 151
6.3 Viewing Files Transferred in Rendered HTTP Sessions . . . 158
6.4 Pausing Connection . . . 160

6.5 Terminating Connection . . . 161
6.6 Joining Live Session . . . 162
6.7 Sharing Sessions . . . 163
6.8 Commenting Sessions . . . 168
6.9 Sessions' Retention Lockdown . . . 170
6.10 Exporting Sessions . . . 171
6.10.1 Export Session File Formats . . . 172
6.11 Deleting Sessions . . . 174
6.12 OCR Processing Sessions . . . 175
6.13 Session Data Replication . . . 178
6.14 Session Timestamping . . . 179
6.15 Require Approval for Access . . . 181
6.15.1 Approving Pending User Requests . . . 181
6.15.2 Declining Pending Requests . . . 182
6.16 AI Behavioral Analysis in Sessions . . . 183
6.17 AI Session Summary . . . 186

7 Access Requests **189**
7.1 Time-Based Access Requests . . . 191
7.2 Awaiting Requests . . . 193
7.3 Active Requests . . . 194
7.4 Archived Requests . . . 195

8 Reports **197**
8.1 System Reports . . . 197
8.2 User Reports: Periodic and On-Demand . . . 197
8.3 List of Predefined Reports . . . 198
8.4 Subscribing to a Periodic Report . . . 198
8.5 Unsubscribing from a Recurring Report . . . 199
8.6 Generating a Report on Demand . . . 199
8.7 Viewing and Saving Reports . . . 201
8.8 Deleting Reports . . . 201

9 User Management **202**
9.1 Users . . . 202
9.1.1 Creating a User . . . 203
9.1.2 Editing a User . . . 212
9.1.3 Blocking a User . . . 213
9.1.4 Unblocking a User . . . 215
9.1.5 Deleting a User . . . 216
9.1.6 Authentication Failures Counter . . . 217
9.2 Groups (RBAC) . . . 218
9.2.1 Access Resolution and Prioritization . . . 218
9.2.2 Creating Group . . . 222
9.2.3 Modifying Groups . . . 225
9.2.4 Deleting Groups . . . 226
9.3 Role-Based Access Control (RBAC) . . . 227
9.3.1 Transition to RBAC After Upgrade . . . 227
9.3.1.1 Understanding Privileges and Capabilities . . . 228
9.3.1.2 Predefined Roles as a Starting Point . . . 229
9.3.2 Creating Role . . . 233
9.3.3 Assigning Roles to Users . . . 236

9.3.4 Modifying Roles . . . 237
9.3.5 Deleting Roles . . . 238
9.3.6 Typical Role Scenarios and Required Privileges . . . 238
9.3.6.1 Tab-Level Access Control Matrix . . . 238
9.3.6.2 Dashboard Widgets Visibility . . . 251
9.3.6.3 Sessions Tab Permissions . . . 251
9.3.6.4 Downloads Tab Permissions . . . 252
9.3.6.5 Safes Management . . . 252
9.3.6.6 Discovery Tab Permissions . . . 253
9.3.6.7 Access Request Permissions . . . 254
9.3.6.8 Fudo Officer . . . 254
9.3.6.9 Reports Tab Permissions . . . 255
9.3.6.10 Sudo Policy Permissions . . . 256

10 Session Management **257**
10.1 Servers . . . 257
10.1.1 Creating a Server . . . 257
10.1.1.1 Creating an HTTP Server . . . 257
10.1.1.2 Creating a Modbus Server . . . 261
10.1.1.3 Creating a MS SQL Server . . . 264
10.1.1.4 Creating a MySQL Server . . . 267
10.1.1.5 Creating an Oracle Server [BETA] . . . 271
10.1.1.6 Creating a PostgreSQL Server . . . 274
10.1.1.7 Creating an RDP Server . . . 277
10.1.1.8 Creating an SSH Server . . . 281
10.1.1.9 Creating a Telnet Server . . . 284
10.1.1.10 Creating a Telnet 3270 Server . . . 287
10.1.1.11 Creating a Telnet 5250 Server . . . 291
10.1.1.12 Creating a VNC Server . . . 294
10.1.1.13 Creating a TCP Server . . . 298
10.1.2 Port Ranges in Server Configuration . . . 301
10.1.2.1 Configuring a Port Range . . . 301
10.1.2.2 Server Configuration Prioritization in Case of Conflict . . . 302
10.1.3 Use SSH Tunnel - SSH Reverse Tunnel Server Configuration . . . 302
10.1.4 Importing a Server List from CSV File . . . 304
10.1.5 Editing a Server . . . 305
10.1.6 Blocking a Server . . . 306
10.1.7 Unblocking a Server . . . 307
10.1.8 Deleting a Server . . . 309
10.2 Pools . . . 310
10.2.1 Creating a Pool . . . 311
10.2.2 Deleting a Pool . . . 313
10.3 Accounts . . . 315
10.3.1 Creating an Account . . . 315
10.3.1.1 Creating an *Anonymous* Account . . . 316
10.3.1.2 Creating a *Forward* Account . . . 320
10.3.1.3 Creating a *Regular* Account . . . 326
10.3.2 Editing an Account . . . 336
10.3.3 Blocking an Account . . . 337
10.3.4 Unblocking an Account . . . 339
10.3.5 Deleting an Account . . . 340

10.3.6 Managing Security Alerts . . . 341
10.3.6.1 Triggering Secret Change . . . 341
10.3.6.2 Ignoring Security Alert . . . 342
10.4 Listeners . . . 343
10.4.1 Creating a Listener . . . 343
10.4.1.1 Setting up the SSH Listener . . . 345
10.4.1.2 Setting up the RDP Listener . . . 348
10.4.1.3 Setting up the VNC Listener . . . 353
10.4.1.4 Setting up the HTTP Listener . . . 355
10.4.1.5 Setting up the Modbus Listener . . . 358
10.4.1.6 Setting up the MySQL Listener . . . 359
10.4.1.7 Setting up the Oracle Listener [BETA] . . . 361
10.4.1.8 Setting up the PostgreSQL Listener . . . 363
10.4.1.9 Setting up the TCP Listener . . . 366
10.4.1.10 Setting up the MS SQL Listener . . . 367
10.4.1.11 Setting up the Telnet Listener . . . 369
10.4.1.12 Setting up the Telnet 3270 Listener . . . 370
10.4.1.13 Setting up the Telnet 5250 Listener . . . 372
10.4.2 Editing a Listener . . . 374
10.4.3 Blocking a Listener . . . 374
10.4.4 Unblocking a Listener . . . 375
10.4.5 Deleting a Listener . . . 376
10.5 Safes . . . 376
10.5.1 Creating a Safe . . . 377
10.5.2 Blocking Concurrent Sessions Through Other Safes . . . 393
10.5.3 Editing a Safe . . . 395
10.5.4 Blocking a Safe . . . 396
10.5.5 Unblocking a Safe . . . 397
10.5.6 Deleting a Safe . . . 398
10.6 Discovery . . . 399
10.6.1 Creating a Rule . . . 400
10.6.1.1 Creating a Rule for Accounts . . . 400
10.6.1.2 Creating a Rule for Servers . . . 401
10.6.2 Managing Rules . . . 402
10.6.3 Creating a Scanner . . . 403
10.6.3.1 Creating a Scanner for Domain Controller Accounts . . . 403
10.6.3.2 Creating a Scanner for Domain Controller Servers . . . 405
10.6.3.3 Creating a Scanner for Local Accounts . . . 407
10.6.4 Managing Scanners . . . 409
10.6.5 Managing Discovered Accounts . . . 409
10.6.6 Managing Discovered Servers . . . 411
10.7 Remote Applications . . . 413
10.7.1 Adding Remote Application . . . 413
10.7.2 Adding Arguments . . . 414
10.7.3 Connecting to Remote Application via Access Gateway . . . 417
10.7.4 Granular Access to Remote Applications . . . 417
10.7.5 Deleting Remote Application . . . 418
10.8 Policies . . . 419
10.8.1 Regular Expression-Based Policy . . . 420
10.8.2 Ai Module-Based Policy . . . 423
10.8.3 Ai Module-Based Policy Examples . . . 425

10.8.4 AI Session Summary Policy . . . 427
10.8.4.1 Policy Configuration . . . 427
10.8.4.2 How It Works . . . 429
10.8.5 Live Session Analysis Policy [BETA] . . . 429
10.8.5.1 Policy Configuration . . . 430
10.8.5.2 Notifications . . . 431
10.8.6 Sudo Command Control Policy . . . 431
10.8.6.1 How Sudo Command Control Works . . . 431
10.8.6.2 Setting up Fudo for Sudo Control . . . 432
10.8.6.3 Sudo Policy Configuration . . . 433
10.8.6.4 Sudo Plugin Installation . . . 435
10.9 Downloads . . . 437
10.9.1 Sessions . . . 437
10.9.2 Files . . . 437
10.10 Productivity . . . 438
10.10.1 Overview . . . 439
10.10.2 Sessions Analysis . . . 440
10.10.3 Activity Comparison . . . 441

11 Password Vault **442**
11.1 Overview . . . 442
11.1.1 Architecture Overview – Security Model . . . 443
11.1.2 Password Vault Structure . . . 444
11.1.3 Event Logging and Audit Trail . . . 445
11.2 Collections . . . 446
11.2.1 Creating Collections . . . 446
11.2.2 Nesting Collections . . . 448
11.2.3 Accessing Collection Editing . . . 451
11.2.3.1 Edit Collection Panel . . . 452
11.2.4 Assigning Users and Groups to Collections . . . 454
11.2.5 Managing Collection Object Rights . . . 455
11.2.5.1 Assigning Object Rights to Users . . . 456
11.2.5.2 Assigning Object Rights to Roles . . . 457
11.2.6 Collection Notifications . . . 458
11.2.7 Deleting Collections . . . 459
11.3 Secrets . . . 460
11.3.1 Creating Secrets . . . 460
11.3.2 Importing Secrets . . . 468
11.3.3 Accessing Secret Editing . . . 470
11.3.3.1 Edit Secret Panel . . . 470
11.3.4 Moving Secrets Between Collections . . . 474
11.3.5 Deleting Secrets . . . 476
11.3.6 Assigning Password Vault Secrets to Accounts . . . 477
11.4 Secret Access Monitoring . . . 479
11.4.1 Event Types and Status Indicators . . . 479
11.4.2 Filtering and Reviewing Events . . . 480
11.5 Fudo Password Vault Browser Extension . . . 480
11.5.1 Installation . . . 481
11.5.2 Opening the Extension . . . 482
11.5.3 Signing In . . . 482
11.5.4 Extension Menu and Settings . . . 484

11.5.5 Signing Out . . . 486
11.5.6 Browsing Collections and Secrets . . . 486
11.5.7 Creating and Editing Personal Secrets . . . 490
11.5.8 Autofilling Credentials on Websites . . . 493
11.5.9 Access Requests, Exclusive Checkout, and Revoked Access . . . 493
11.6 Compromised Passwords . . . 496
11.6.1 How It Works . . . 496
11.6.2 Accessing Compromised Passwords Settings . . . 496
11.6.3 Uploading a Compromised Password List . . . 496
11.6.4 File Format Requirements . . . 497
11.6.4.1 Plaintext Password Files . . . 497
11.6.4.2 SHA-1 Hash Files . . . 498
11.6.5 Scan Results . . . 498
11.6.6 Managing Uploaded Files . . . 499
11.7 Secret Changers . . . 499
11.7.1 Secret Changer Policy . . . 500
11.7.1.1 Defining a Secret Changer Policy . . . 500
11.7.1.2 Editing a Secret Changer Policy . . . 502
11.7.1.3 Deleting a Secret Changer Policy . . . 502
11.7.2 Custom Secret Changers . . . 503
11.7.2.1 Defining a Custom Secret Changer . . . 503
11.7.2.2 Encrypted Constant Values . . . 506
11.7.2.3 Password Changer Configuration Example . . . 507
11.7.2.4 Editing a Custom Secret Changer . . . 508
11.7.2.5 Deleting a Custom Secret Changer . . . 508
11.7.3 Importing and Exporting Secret Changers . . . 508
11.7.3.1 Exporting a Secret Changer . . . 508
11.7.3.2 Importing a Secret Changer . . . 509
11.7.4 Connection Modes . . . 509
11.7.4.1 SSH . . . 509
11.7.4.2 LDAP . . . 510
11.7.4.3 Telnet . . . 511
11.7.4.4 WinRM . . . 512
11.7.5 Setting up Secret Changing on a Unix System . . . 513

12 Settings **516**
12.1 System . . . 516
12.1.1 Date and Time . . . 516
12.1.2 Certificates . . . 518
12.1.3 Access Gateway Allowed Hosts . . . 520
12.1.4 SSH Access . . . 522
12.1.5 Legacy Session Cookie . . . 522
12.1.6 Configuration Encryption . . . 524
12.1.7 SNMP . . . 529
12.1.7.1 Configuring SNMP . . . 529
12.1.7.2 Configuring SNMPv3 TRAP . . . 529
12.1.7.3 SNMP MIBs . . . 530
12.1.7.4 Getting SNMP readings using `snmpwalk` . . . 531
12.1.7.5 Fudo Enterprise Specific SNMP Extensions . . . 531
12.1.8 Trusted Timestamping . . . 532
12.1.9 File Scanning in Rendered HTTP Sessions . . . 533

12.1.10 Secret Changers - Active Cluster Node . . . 538
12.1.10.1 Cluster Secret Changers . . . 539
12.1.11 Sensitive Features . . . 539
12.1.12 Configuring an HTTP Proxy . . . 540
12.1.13 System Update . . . 541
12.1.13.1 Updating System . . . 542
12.1.13.2 Restoring Previous System Version . . . 543
12.1.13.3 Deleting Upgrade Snapshot . . . 544
12.1.14 Hotfix . . . 545
12.1.15 License Information and Management . . . 545
12.1.16 Diagnostics . . . 548
12.1.17 Exporting/Importing System Configuration . . . 552
12.1.17.1 Exporting System Configuration . . . 552
12.1.17.2 Importing System Configuration . . . 552
12.2 Network Settings . . . 553
12.2.1 Reverse Proxy . . . 554
12.2.1.1 Prerequisites . . . 554
12.2.1.2 Configuration Steps . . . 555
12.2.1.3 User Access Gateway Connections . . . 560
12.2.1.4 Enabling and Disabling Reverse Proxy . . . 562
12.2.1.5 Reverse Proxy Status Indicators . . . 562
12.2.1.6 SSH Tunnel Operation . . . 563
12.2.1.7 Workflow Recommendation . . . 564
12.2.1.8 Internal Routing Behavior . . . 564
12.2.1.9 Security Considerations . . . 564
12.2.1.10 Troubleshooting . . . 565
12.2.2 Network Interfaces Configuration . . . 565
12.2.2.1 Managing Physical Interfaces . . . 565
12.2.2.2 Defining IP Address Using System Console . . . 568
12.2.2.3 Setting up Virtual Networks (VLAN) . . . 571
12.2.2.4 Setting up Link Aggregation (LACP) . . . 573
12.2.3 Labeled IP Addresses . . . 575
12.2.4 Routing Configuration . . . 576
12.2.5 DNS Configuration . . . 578
12.2.6 ARP Table Configuration . . . 581
12.3 Notifications . . . 582
12.3.1 Configuring the SMTP Server . . . 583
12.4 Artificial Intelligence (AI) . . . 585
12.4.1 AI Behavioral Analysis . . . 586
12.4.1.1 Configuring Models Trainers . . . 586
12.4.1.2 Behavioral Analysis Models . . . 588
12.4.2 AI Session Summary . . . 590
12.4.3 AI Live Session Monitoring [BETA] . . . 592
12.5 Authentication . . . 598
12.5.1 External Authentication Server Definition . . . 599
12.5.1.1 Active Directory . . . 600
12.5.1.2 LDAP . . . 601
12.5.1.3 Cerb . . . 602
12.5.1.4 Radius . . . 603
12.5.1.5 TACACS+ . . . 604
12.5.1.6 Assigning an External Authentication Method to a User . . . 605

12.5.1.7 Second Authentication Factor . . . 606
12.5.2 OpenID Connect Authentication Definition . . . 607
12.5.2.1 Back-Channel Logout . . . 612
12.5.3 JWT Authentication Definition . . . 613
12.5.4 Location Policies . . . 617
12.5.4.1 How Policies Are Combined . . . 617
12.5.4.2 Configuring the Global Policy . . . 618
12.5.4.3 Adding a Location Policy for a Group . . . 618
12.5.4.4 Where Policies Are Enforced . . . 620
12.5.4.5 When the Location Cannot Be Determined . . . 621
12.5.4.6 Sessions Established Through a Reverse Proxy . . . 621
12.5.4.7 Protection Against Locking Yourself Out . . . 621
12.5.4.8 Required Privileges . . . 622
12.5.5 Global Authentication Settings . . . 622
12.5.5.1 Default Domain . . . 622
12.5.5.2 Deny New Connections . . . 624
12.5.5.3 Password Complexity . . . 624
12.5.5.4 User-Managed Methods in the User Access Gateway . . . 626
12.5.5.5 OATH Authentication Definition . . . 628
12.5.5.6 SMS Authentication Definition . . . 628
12.5.5.7 DUO Authentication Definition . . . 630
12.5.5.8 Single Sign On . . . 632
12.5.5.9 Kerberos Authentication Settings . . . 634
12.5.5.10 FIDO2 Authentication Settings . . . 637
12.6 External Passwords Repositories . . . 641
12.6.1 CyberArk Credential Provider . . . 641
12.6.2 Thycotic Secret Server . . . 643
12.6.3 Local Administrator Password Solutions (LAPS) . . . 645
12.6.4 Fudo Password Vault . . . 648
12.6.5 Azure Key Vault . . . 652
12.7 External Storage . . . 654
12.7.1 Configuring External Storage . . . 654
12.8 Resources . . . 656
12.8.1 RDP/SSH/VNC Login Screen Configuration . . . 656
12.8.1.1 Keyboard Layouts on the RDP Login Screen . . . 659
12.8.2 *User Portal* Configuration . . . 660
12.8.2.1 Login Screen Configuration . . . 660
12.8.2.2 Predefined Keyboard Layout . . . 661
12.8.3 JiT Reason Formats . . . 662
12.8.3.1 Creating a Reason Format . . . 662
12.8.3.2 Scope and Limitations . . . 664
12.9 Backup and Retention . . . 664
12.9.1 Session Data Backup . . . 664
12.9.2 Data Retention . . . 667
12.10 Cluster Configuration . . . 669
12.10.1 Session Data Replication and Behavior in the Event of a Node Failure . . . 669
12.10.2 Cluster Initialization . . . 671
12.10.3 Adding Cluster Nodes . . . 673
12.10.3.1 Cluster Initialization and Adding Nodes . . . 673
12.10.3.2 Setting Relationships Between Nodes . . . 675
12.10.3.3 Linking Nodes with the Initial Node . . . 677

12.10.3.4 Cluster Initialization Completion Verification 678
12.10.4 Cluster Expansion with New Nodes 678
12.10.5 Editing Cluster Nodes 681
12.10.6 Removing Cluster Nodes 681
12.10.6.1 Removing a Node from the Cluster 681
12.10.6.2 Rejoining a Removed Node 682
12.10.7 Redundancy Groups 682
12.10.8 Checking Session Replication Status 686
12.11 Users Synchronization - User Directory 687
12.11.1 Configuring Users Synchronization Service 687
12.11.2 Disabling Data Synchronization for User 692
12.11.3 Kerberos Support for Active Directory 692
12.12 SCIM 2.0 Provisioning 693
12.12.1 Managing Access to the SCIM Configuration 694
12.12.2 Configuring SCIM Provisioning 694
12.12.3 Configuring the Identity Provider 695
12.12.4 Rotating the API Key 696
12.12.5 Disabling SCIM Provisioning 696
12.12.6 SCIM-Managed Account Behavior 697
12.12.7 Attribute Mapping 697
12.12.8 Attributes That Are Not Supported 698
12.12.9 Example Payloads 699
12.12.10Restrictions On Scim-Managed Objects 700
12.12.11Blocking Model 701
12.12.12Authentication with OIDC 702
12.12.13Auditing 702
12.13 Certificate-based Authentication Scheme 702
12.14 Login Timeout 704
12.15 System Version Restore 705
12.16 System Reboot 706
12.17 Changing Encryption Passphrase 707
12.18 Integration with CERB Server 709
12.19 System Maintenance 714
12.19.1 Backing up Encryption Keys 715
12.19.2 Monitoring System Condition 719
12.19.3 Health Check 720
12.19.3.1 API Health Check 720
12.19.4 Callhome 721
12.19.4.1 Data Collected by Callhome Service 722
12.19.4.2 The Benefits of Using Callhome 722
12.19.4.3 Enable/Disable Callhome 723
12.19.5 Hard Drive Replacement 723
12.19.6 Resetting Configuration to Default Settings 724

13 Events Log **728**
13.1 Filtering Logs by Date and Time 728
13.2 External Syslog Servers 729
13.3 Exporting Events Log 732

14 Account Activity in the User Access Gateway (UAG) **733**

15 Reference Information **737**

15.1 RDP Connections Broker . . . 737
15.2 Log Messages . . . 738

16 Fudo Officer **799**
16.1 Configuration . . . 799
16.2 Managing Profiles . . . 803
16.2.1 Add New Profile . . . 803
16.2.2 Switch Profiles . . . 804
16.2.3 Edit Profile . . . 805
16.2.4 Delete Profile . . . 806
16.3 Managing Session Requests . . . 807
16.3.1 Awaiting Requests . . . 808
16.3.2 Active Requests . . . 809
16.3.3 Revoking Request . . . 810
16.3.4 Archived Requests . . . 810
16.4 Password Vault in Fudo Officer . . . 811
16.4.1 Browsing Secrets . . . 811
16.4.2 Secret Details . . . 812
16.4.3 Requesting Access to a Secret . . . 812
16.4.4 Checking Out Secrets . . . 813
16.4.5 Adding a Collection . . . 813
16.4.6 Adding a Secret . . . 814
16.4.7 Editing a Secret . . . 815
16.4.8 Limitations . . . 815
16.4.9 Autofill . . . 815
16.5 Notifications . . . 816
16.5.1 Configuring Application Notifications . . . 817
16.6 Settings . . . 818
16.6.1 Biometric Authentication . . . 819
16.6.2 Change PIN Code . . . 819
16.6.3 Two-Factor YubiKey Authentication . . . 820
16.6.4 Autofill . . . 820
16.6.5 Application Lock . . . 821
16.6.6 Clearing App Data . . . 821
16.6.7 Language . . . 821

17 Fudo ShareAccess **822**
17.1 Data Model . . . 822
17.2 Pairing Fudo Enterprise with Fudo Shareaccess . . . 823
17.2.1 Troubleshooting the connection . . . 830
17.3 ShareAccess License . . . 832
17.3.1 Trial License Activation . . . 832
17.3.2 Requesting a License . . . 833
17.3.3 Uploading License File . . . 834
17.4 Manage Fudo ShareAccess Members . . . 834
17.4.1 Inviting Members . . . 834
17.4.2 Verifying Members Status . . . 837
17.4.3 ShareAccess Key Authentication Method . . . 839
17.4.4 Creating an Account Without an Invitation . . . 840
17.4.5 Revoking Members Status . . . 840
17.4.6 Deleting Members . . . 841
17.5 Manage Access to Resources . . . 842

18 Client Applications **846**
18.1 PuTTY . . . 846
18.2 Microsoft Remote Desktop . . . 848
18.3 TightVNC Viewer . . . 850
18.4 SQL Server Management Studio . . . 851

19 Troubleshooting **852**
19.1 Booting Up . . . 852
19.2 Connecting to Servers . . . 853
19.3 Logging to Administration Panel . . . 857
19.4 Session Playback . . . 858
19.5 Cluster Configuration . . . 858
19.6 Trusted Timestamping . . . 859
19.7 File Scanning . . . 860
19.8 Sudo Plugin Issues . . . 862
19.9 Support Mode . . . 863

20 Use Cases **867**
20.1 Two-Factor OATH Authentication with Google Authenticator . . . 867
20.1.1 Protocols Supporting OATH Authentication Method . . . 867
20.1.2 Configuring the OATH Authentication Method . . . 868
20.1.3 TOTP Code Reuse for Parallel Access . . . 873
20.1.3.1 Use Cases . . . 873
20.1.3.2 Default Behavior . . . 873
20.1.3.3 Behavior When Enabled . . . 873
20.2 OpenID Connect Authentication Definition with Microsoft Entra (Azure) . . . 874
20.3 Remote Desktop Services Configuration on Windows Server for Fudo Enterprise 883
20.3.1 Setup Remote Desktop Services (RDS) on Windows . . . 883
20.3.2 Setup Fudo Enterprise - Bastion Scenario (Recommended) . . . 895
20.3.3 Setup Fudo Enterprise - Proxy Scenario . . . 902
20.4 Custom RDP Hostname in the Session Title . . . 908
20.4.1 DNS Configuration in Windows DNS Manager . . . 909
20.4.2 Fudo Enterprise Configuration . . . 910
20.4.3 Start RDP Connection . . . 910
20.4.4 Result . . . 910
20.5 Managing RDP Server Certificates in Windows Server . . . 911
20.5.1 Locating the Server Certificate in Windows Server . . . 911
20.5.2 Providing the CA Certificate . . . 914
20.6 Configuring the Single Sign On (SSO) . . . 929
20.6.1 SSO Configuration on Windows Server 2019 . . . 929
20.6.2 Setup Fudo Enterprise . . . 934
20.6.3 Setup and Check User Workstation - Windows2010 Client . . . 937
20.7 Handling Local Account Password Changes Using a Domain Account with WinRM Secret Changer . . . 940
20.7.1 Hostname and DNS Server Configuration . . . 941
20.7.2 Adding a KDC Server . . . 941
20.7.3 Server Configuration . . . 942
20.7.4 Adding a Secret Change Policy . . . 943
20.7.5 Administrator Account . . . 943
20.7.6 Account for Which the Password Will Be Changed . . . 944
20.8 Configuring SSH Key Rotation for an Account . . . 946
20.8.1 Creating a Secret Change Policy . . . 947

20.8.2 Creating an SSH Key Secret Changer . . . 947
20.8.3 Storing the SSH Key in the Password Vault . . . 950
20.8.4 Assigning the Changer to the Secret . . . 950
20.8.5 Pointing the Account at the Secret . . . 951
20.9 Configuring Kerberos Constrained Delegation for MSSQL(TDS) Server . . . 952
20.9.1 Kerberos Authentication Configuration on Windows Server . . . 952
20.9.2 Setup Fudo Enterprise . . . 959
20.9.3 Establish a Connection . . . 962
20.10 Establishing Connections to Servers via SSH Tunnel in Fudo Enterprise . . . 963
20.10.1 General Requirements . . . 963
20.10.1.1 Establishing an SSH Connection . . . 964
20.10.1.2 Establishing an HTTP Connection . . . 969
20.10.1.3 Connecting to an Oracle Database . . . 974
20.10.1.4 Connection to a Server with Reverse Tunnel via Tunnel-type Listener . . . 979
20.11 Master Key Protection with a Thales Luna HSM . . . 982
20.11.1 How Fudo Enterprise Protects the Master Key . . . 982
20.11.2 Before You Begin . . . 982
20.11.3 Option 1: Thales Luna Cloud HSM . . . 983
20.11.4 Option 2: Thales Luna Network HSM . . . 984
20.11.5 Configuring Fudo Enterprise . . . 986

21 Frequently Asked Questions **990**

22 Glossary **995**

Index **1000**

CHAPTER 1

About Documentation

The target audience of this document are system administrators and operators, responsible for managing Fudo Enterprise's configuration and supervising remote access.

Conventions and symbols

This documentation is written using the following conventions:

- *italic* - this formatting is used to mark user interface elements.
- `example` - this formatting is used to write example value of a parameter, API method name or code example.
- Note field:

> **Note**
>
> Note field usually contains additional information closely related with described topic, e.g. suggestion concerning given procedure step; additional conditions which have to be met.

- Warning field:

> **Warning**
>
> Warning field usually contains essential information concerning system's operation. Not adhering to this information may have irreversible consequences.

Disclaimer

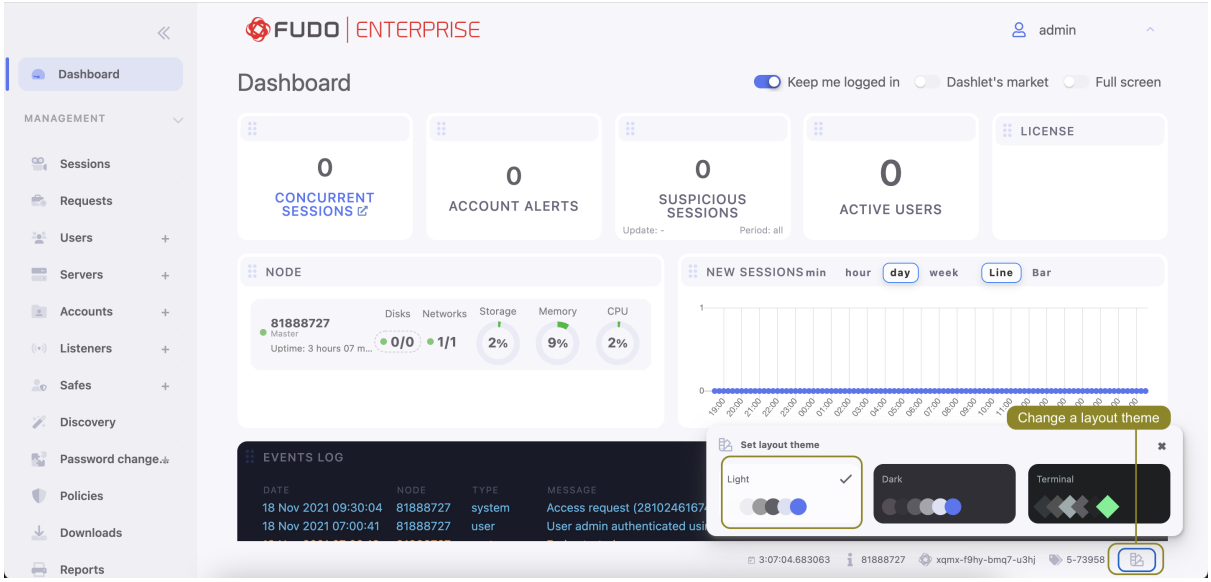
All trademarks, product names, and company names or logos cited in this document are the property of their respective owners and are used for information purpose only.

CHAPTER 2

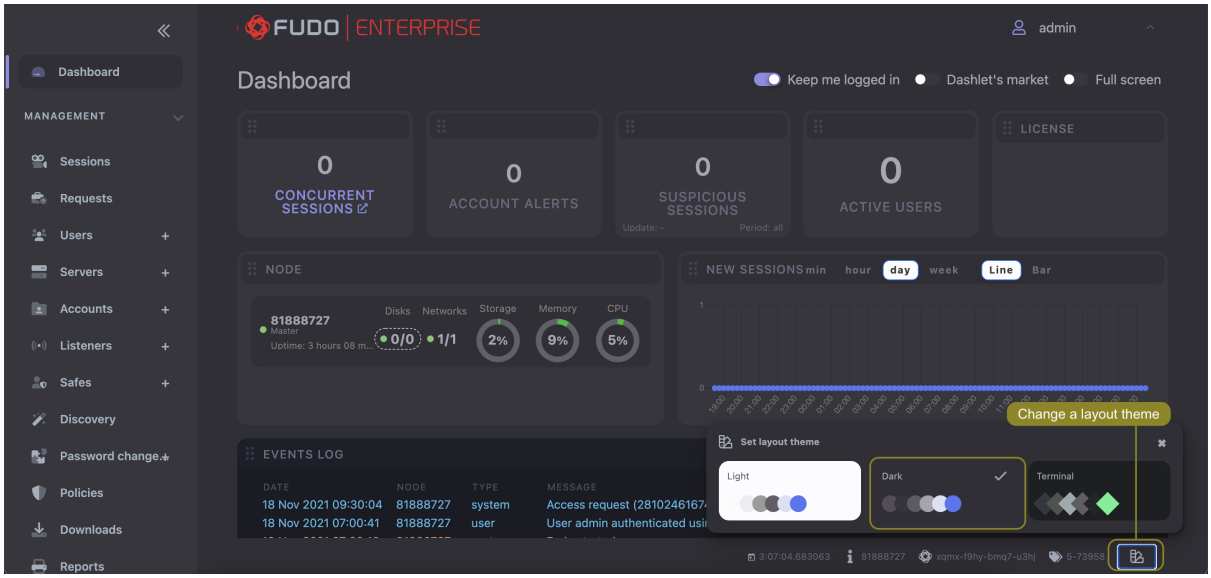
Layout Themes of the Admin Panel

There are three layout themes available to choose for the Admin Panel. Click the icon in the lower right corner of the screen to access the list of variants.

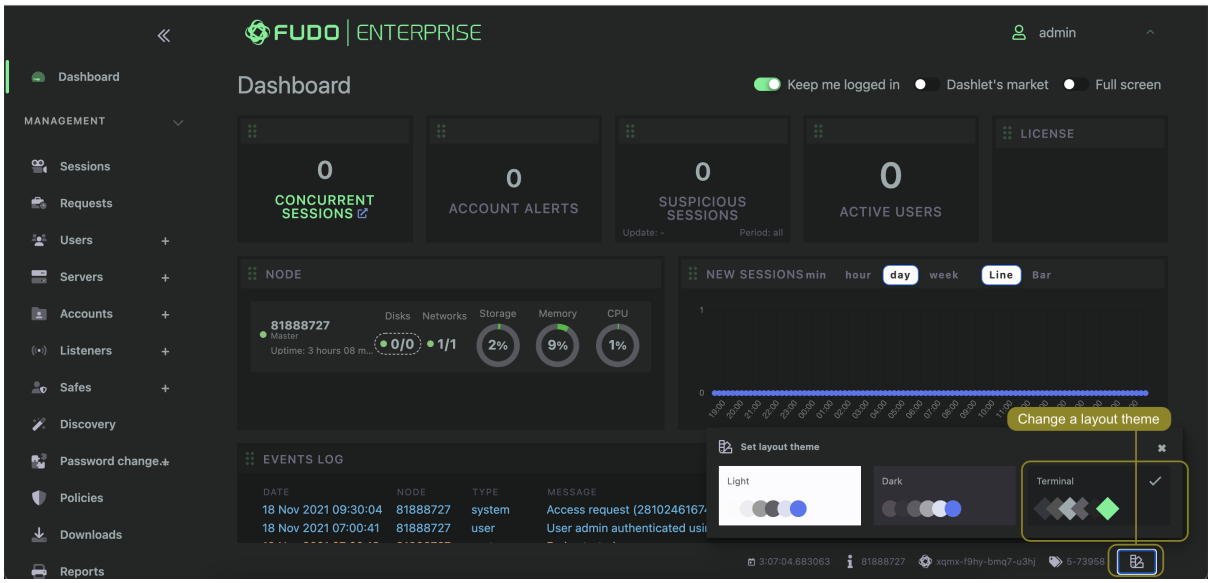
Light theme:



Dark theme:



Terminal theme:



Related topics:

- *Introduction*

CHAPTER 3

Introduction

3.1 System Overview

Fudo Enterprise is a complete solution for managing remote privileged access. Fudo Enterprise includes a range of features, each dedicated to different aspects of remote access management:

- *Session Monitoring & Recording*
- *Secret Management*
- *Just-in-Time (JIT) Access*
- *Single Sign-On (SSO)*
- *Agentless Convenient Access*
- *AI-Powered Prevention*
- *Productivity Analyzer*
- *Rapid Deployment*
- *Compliance Support*

3.1.1 Session Monitoring & Recording

Fudo Enterprise provides administrators with advanced tools to monitor and manage sessions in real-time. Administrators can join, share, pause, or terminate sessions, ensuring swift action in response to potentially suspicious activities.

The platform supports resource sharing over 10+ protocols, including RDP, SSH, and HTTPS, enabling secure access to critical systems. Fudo Enterprise records complete network traffic along with meta data, enabling precise session playback and full-text content search. This functionality provides a comprehensive audit trail to enhance security and ensure compliance.

Fudo Enterprise acts as a proxy between users and monitored servers and it registers users' actions, including mouse pointer moves, keystrokes and transferred files.

Data stored on Fudo can be timestamped which makes session material a more reliable evidence in court.

Fudo Enterprise session monitoring module supports following system configurations:

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

3.1.2 Secret Management

Fudo Enterprise provides a secure and flexible system for managing privileged account credentials. Credentials are stored securely and never leave the system, ensuring robust protection.

Administrators can utilize predefined templates to quickly set up secret changers within minutes. These secret changers operate on a separate transport layer, such as SSH, LDAP, Telnet, or WinRM, allowing integration with various systems.

Fudo Enterprise supports secret changing on following systems:

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

Beyond the built-in examples, custom scripts can be created to enhance functionality, offering precise control over credential management on monitored servers. For more information, refer to the *Secret Changers* section.

3.1.3 Just-in-time (JIT) Access

Fudo Enterprise supports Just-in-Time (JIT) access workflows, enabling organizations to implement a Zero-Trust security approach. Through the *request management* section, administrators can define and schedule specific time windows for resource availability, granting access only when necessary. This ensures adherence to the zero-standing-privileges principle, minimizing security risks by limiting prolonged access to critical systems.

3.1.4 Single Sign-on (SSO)

Fudo Enterprise provides *Single Sign-On (SSO)* functionality for both the Admin Panel and the User Access Gateway. SSO streamlines authentication by automatically logging users into the system, enhancing usability and efficiency while maintaining robust security standards.

3.1.5 Agentless Convenient Access

Fudo Enterprise offers flexible and agentless access to resources, allowing users to choose their preferred method of connection. Users can continue using their favorite native clients for a seamless experience or take advantage of the built-in, browser-based Webclient provided by Fudo Enterprise. This flexibility ensures ease of use for both technical and non-technical users alike.

3.1.6 Ai-powered Prevention

Fudo Enterprise incorporates *AI-driven capabilities* to assist in daily security management tasks. The system provides actionable guidelines to support verification and monitoring processes, simplifying the responsibilities of security teams and CISOs. By analyzing behavioral and semantic patterns, Fudo Enterprise detects potential credential compromises and sends notifications, enabling swift response to mitigate risks and enhance overall security posture.

3.1.7 Productivity Analyzer

Productivity Analyzer module tracks users' actions and provides precise information on their activity and idle times. This functionality can be disabled at the customer's request.

For more information on the Productivity Analyzer module, refer to the *Productivity* topic.

3.1.8 Rapid Deployment

Fudo Enterprise is designed as an all-in-one solution, eliminating the need for additional software or hidden costs to initiate your instance. Whether deployed as an appliance or a virtual machine, all necessary components are included within the core system. This streamlined approach ensures a quick and efficient installation process, enabling full deployment in as little as one day.

3.1.9 Compliance Support

Fudo Enterprise is designed to help organizations meet a wide range of compliance requirements, including PCI-DSS, SOX, HIPAA, NIST, GDPR, and ISA/IEC 62443. By providing robust security and auditing features, Fudo Enterprise ensures adherence to industry standards and regulatory frameworks, simplifying compliance management for your organization.

Related topics:

- *Requirements*
- *Data model*
- *Security measures*

3.2 Available GUI Languages

The Fudo Enterprise interface is offered in the following languages:

- English
- Polish
- Ukrainian
- Russian
- Kazakh

- German
- Uzbek
- Italian
- French

Related topics:

- *System overview*
- *Supported Protocols*
- *Quick start*

3.3 Licensing Model and License Limits

This section describes the licensing model for **Fudo Enterprise modules**. The **ShareAccess license** is managed separately and described in the *ShareAccess: License* section.

Warning

Starting with **version 6.0**, the licensing model of Fudo Enterprise has been updated.

The previously unified **Fudo Enterprise license** has been divided into three independent modules:

- **Privileged Session Management (PSM)**
- **Password Vault (PV)**
- **ShareAccess**

Each module is licensed separately and have its own expiration date and usage limits. For more information, see the *Limit of Active Users* subsection.

Licensed Modules

The platform includes the following licensed modules:

- **Privileged Session Management (PSM)** - Represents the core functionality that was previously covered by the Fudo Enterprise license, including privileged session proxying, monitoring, and access control.
- **Password Vault (PV)** - Provides secure storage and lifecycle management of credentials such as passwords, SSH keys, API keys, certificates, and secure notes.
- **ShareAccess** - Enables secure and simplified access for third parties, including external vendors, by providing browser-based access to shared resources and streamlining connection and credential handling.

Each module have:

- its own **expiration date**
- independent **active user limits**

- additional **feature limits**

Expiration Date

Each licensed module have a separate expiration date. After the expiration date is reached, functionality of the affected module may be restricted.

Support End Date

Starting with version 6.1, license files include a technical support end date. This date indicates when technical support ends and determines whether the system is eligible for upgrades to newer versions.

Note

- Existing license files remain valid in Fudo Enterprise 6.1
- If the license file does not include the support end date, the support status is displayed as *Unknown*
- An expired support end date or *Unknown* support status blocks upgrades to future Fudo Enterprise versions
- Before upgrading beyond Fudo Enterprise 6.1, contact Fudo Presales team to obtain a license file that includes the support end date

Number of Cluster Nodes

The license specifies the number of nodes that can be part of a cluster. If this number is exceeded, the additional nodes will reject connections and log appropriate events in the system logs.

Available Servers

The license determines how many servers can be added to the system. Once this limit is exceeded, it is not possible to add new servers or modify existing ones.

Limit of Active Users (PSM Module)

Number of active users defines how many users can establish sessions to servers using the **Privileged Session Management (PSM)** module.

Note

- A user is counted as **active** if they have started at least one session within the last **30 days**.
- A license slot is released automatically when a user has no session activity for more than **30 days**.

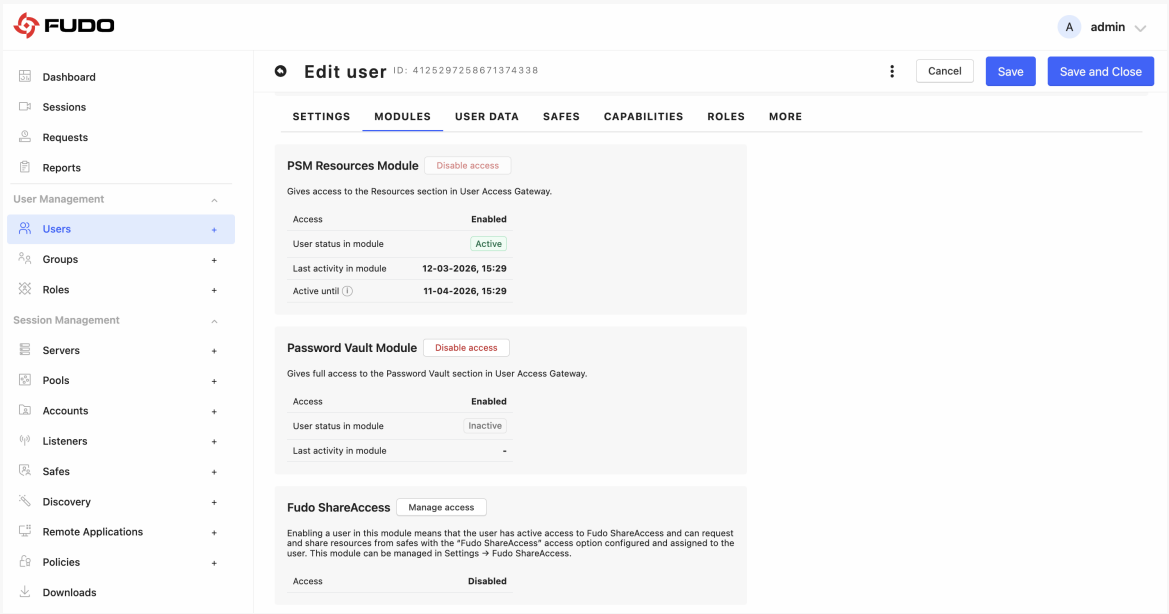
If the licensed limit has already been reached, only users who were already active within the last 30 days can continue to establish sessions. Users who have not been active during that period cannot start new sessions until a license slot becomes available.

Following actions are not restricted by the active user limit:

- Logging into the **Admin Panel** is always allowed. This prevents administrators from being locked out of the system due to license limits.
- Users authenticated through **ShareAccess** are not counted against the PSM Module active users limit.

Note

You can view each user's license consumption status in the user edit form, on the **Modules** subtab.



Limit of Active Users (PV Module)

The **Password Vault** license includes a separate active user limit, independent of the PSM module. This limit applies only to Password Vault operations.

Limitations of the Password Vault Basic License

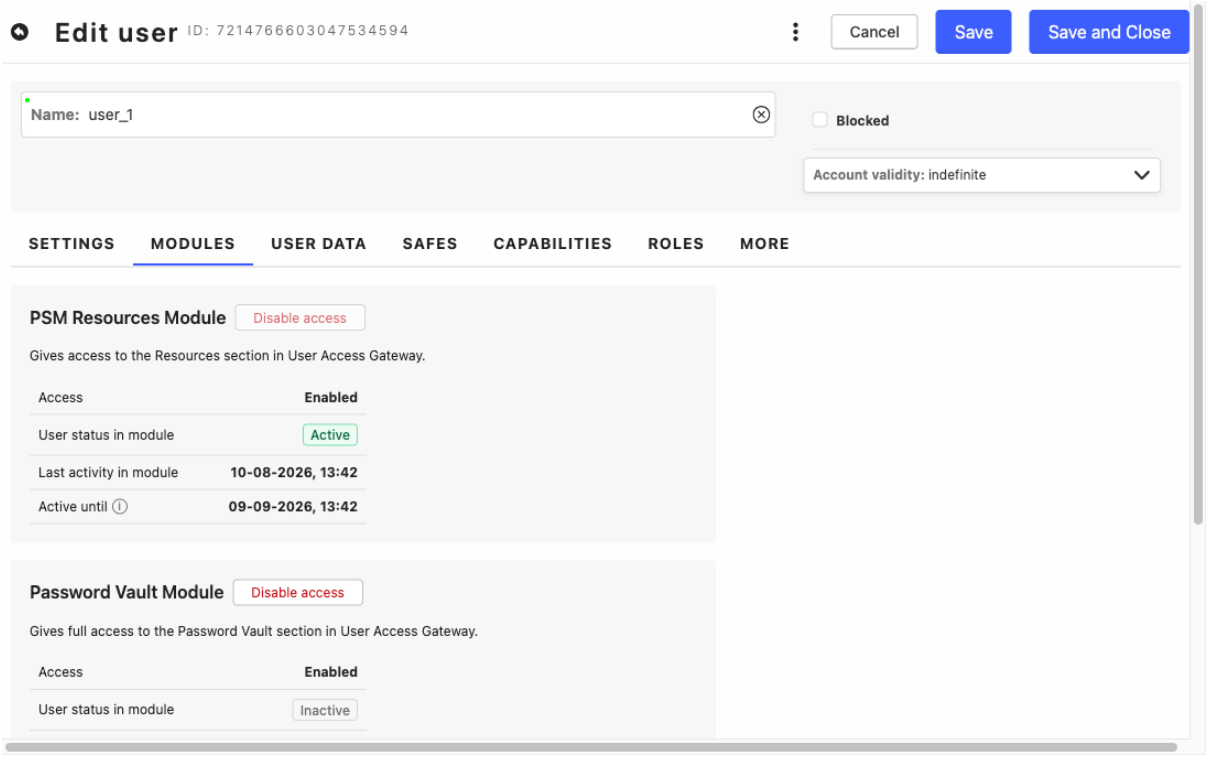
Password Vault module is available in both full and limited license variants.

- The **full license** provides access to the complete Password Vault functionality, including unrestricted collection management, full secret management, all supported secret types, full collection permissions, and global policy configuration.
- The **basic license** includes selected restrictions. In this variant:
  - administrators cannot create child-level collections or create secrets in child-level collections.
  - Full access permissions for collections are not available for users and groups, and only *View* and *View on Request* permissions can be assigned.
  - Global Password Vault policy configuration and policy compliance status are also unavailable.
  - Secret creation is limited to *Login*, *SSH Key*, and *Note* types.

Disabling a Module for a User

Access to the **PSM** and **Password Vault** modules can be turned off for an individual user, independently of the license limits described above. A user whose module is disabled does not see that module's section in the User Access Gateway, and every operation of that module is rejected by Fudo Enterprise, including when it is called directly through the API.

1. Select *User Management* > *Users* and edit the selected user by clicking on their name.
2. Go to the *Modules* subtab.
3. On the *PSM Resources Module* or *Password Vault Module* card, click *Disable access*. Click *Enable access* to restore the access.



Warning

The change takes effect **immediately**, at the moment the button is clicked. It is not saved together with the rest of the form, and leaving the form with *Cancel* does not undo it - to restore the access, click *Enable access*.

Note

The *Disable access* button is unavailable while the user's *User status in module* is *Active*, so a module can only be disabled for a user who is currently inactive in it. To cut off a user who is active, block the whole account instead.

The *Fudo ShareAccess* card on the same subtab is informational only - that module is managed in Settings > Fudo ShareAccess.

What the user sees

In the User Access Gateway the section of a disabled module is greyed out and cannot be

clicked. Pointing at it displays the message *This module is disabled for your account. Contact your administrator.* Entering the address of the section directly in the browser gives the same result - the section does not open.

Warning

Access to a disabled module is withdrawn **immediately** and does not depend on the 30-day activity period described in the *Limit of Active Users* subsection. That period governs the counting of license slots, not permissions, so a user who established a session within the last 30 days also loses access to the module as soon as it is disabled.

Note

- Disabling the **PSM** module does not affect **ShareAccess**, which is licensed separately. A user whose PSM module is disabled can still use ShareAccess.
- If, at the moment the module is disabled, the user holds a secret checked out from the personal vault or taken by a native client, that secret cannot be checked in until it expires or the module is enabled again. A secret checked out from the organization vault can be checked in by an administrator.

Availability of the Productivity Module

The availability of the **Productivity** module is determined by the license file. At the customer's request, the availability of this module can be disabled — for example, to comply with legal requirements in countries that restrict the monitoring of employee productivity.

Note

- The **Productivity** module is available by default, and existing license files remain fully compatible.
- For the list of functionality that is unavailable when the module is disabled, see the *Productivity* section.

License Management Privileges

The following privileges are required to manage licenses:

- `license-read` – allows viewing license information
- `license-upload` – allows uploading or deleting license files

Note

For details about viewing license information, see the *License Information and Management* section.

Related topics:

- *System overview*

- *Supported Protocols*
- *Quick start*

3.4 Supported Protocols

Under review

Support for the **Telnet 3270** protocol is **under review** and may be removed in a future release. If this protocol is critical to your environment, please contact Fudo Support for more information.

3.4.1 HTTP

Supported connection modes:

- *Bastion*
- *Proxy*

Supported OCR languages for the rendered HTTP session:

- English
- German
- Norwegian
- Ukrainian
- Polish
- Hungarian
- Russian

Supported algorithms: (when TLS encryption selected and the option *Legacy crypto* disabled)

- `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`

Warning

HTTP rendering is a CPU intensive process and may have negative impact on system's performance. A physical appliance is recommended for monitoring rendered HTTP connections with the following limitations regarding the maximum number of concurrent rendered HTTP sessions.

Model	Maximum recommended number of concurrent HTTP sessions*
F100x	2
F300x	5
F500x	10

* The actual value depends on the Fudo Enterprise instance configuration.

Note

The following features are not supported:

- Session joining
- Login reason option

In **non-rendered mode**, the following limitations apply:

- Bastion mode is not supported due to protocol limitations
- Access to external resources is not monitored
- Redirections are not followed
- Credentials forwarding is not supported

In **rendered mode**, raw HTTP data is not stored.

File upload and download in a rendered HTTP session use a per-session storage quota of up to 5120 MB.

3.4.2 Modbus

Supported connection modes:

- *Proxy*

Notes:

- Session joining is not supported.
- Bastion mode is not supported due to limitations of the protocol.

3.4.3 MS SQL (TDS)

Due to the fact that MS SQL Studio may create multiple connections for sending internal queries, the sessions, connected via the TDS layer protocol using MS SQL Studio are getting aggregated by Fudo Enterprise.

Fudo Enterprise follows an algorithm that verifies if there is an already connected session on a current node. If the algorithm identifies that the main connection objects (`listener`, `account`, `server address (server)`, `user`, and `safe`) of the new session are correlating with already existing session, both sessions are aggregated into one.

If the main connection objects of the new session are not correlating with any of already existing sessions, a new session is created.

This makes multiple queries to be grouped within one session. Every query has a unique tag that allows filtering important connections with users' queries in the Fudo Enterprise player.

Supported connection modes:

- *Bastion*
- *Proxy*

Supported client applications:

- SQL Server Management Studio,
- sqlcmd.

Notes:

- Session joining is not supported.

3.4.4 MySQL

Supported connection modes:

- *Bastion*
- *Proxy*

Supported client applications:

Official MySQL client

Notes:

- Session joining is not supported.
- Active Directory and other external authentication sources are not supported.
- Since version 5.6, this connection type supports all standard authentication methods. If multi-factor authentication is used, only single-step 2FA (e.g., password and token entered together) is supported.
- Supported authentication plugins:
  - for communication between Fudo Enterprise and the database server: `mysql_clear_password`, `mysql_native_password`, `caching_sha2_password`;
  - for communication between the client and Fudo Enterprise: `mysql_clear_password`.

3.4.5 Oracle [BETA]

Supported connection modes:

- *Proxy*

Supported client applications:

Oracle SQL*Plus

Notes:

- Oracle Database 19c, 21c, and 23ai are supported. Oracle Database 26ai is not supported for encrypted connections.
- The Fudo Enterprise user name must be identical to the database user name. The Oracle protocol carries no separate field for a Fudo Enterprise user name, so the user is identified by the name sent when logging in to the database.
- The Bastion connection mode is not supported for the same reason - the account and the server are always determined by the listener the client connects to.
- Accounts of the *regular* type are not available for Oracle servers. Only *forward* and *anonymous* accounts can be created, and a forward account always authenticates against the

monitored server. As a result, password substitution is not available for this protocol - users log in to the database with their own credentials.

- Encrypted connections are supported with the Oracle SQL*Plus client. Other client applications do not support TLS with Fudo Enterprise.
- Oracle native encryption (Advanced Security Option) is refused. Configure clients so that they do not negotiate it.
- The `noraw` session recording mode cannot be used. Set the session recording of the account to `all`, `raw` or `none`; timestamping requires `all` or `raw`.
- Session joining is not supported.

3.4.6 PostgreSQL

Supported connection modes:

- *Bastion*
- *Proxy*

Supported client applications

- psql
- pgAdmin (due to a client-side issue, OTP authentication is not supported)

Notes:

- Session joining is not supported.
- Session recording in `noraw` mode is not supported.

3.4.7 RDP

Supported Connection Modes:

- *Bastion*
- *Proxy*

Supported Operating Systems:

- Windows Server 2016 and newer

Supported Client Applications:

- Official Microsoft clients for Windows and macOS,
- xfreerdp.

Supported OCR Languages:

- English
- German
- Norwegian
- Ukrainian
- Polish
- Hungarian

- Russian
- Armenian
- Georgian
- Azerbaijani
- Kazakh
- Kyrgyz
- Malayalam
- Bengali
- Vietnamese

Supported Algorithms:

- when TLS encryption selected and the option *Legacy crypto* is disabled:
  - `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`
- when TLS encryption selected and the option *Legacy crypto* is enabled:
  - `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

Notes:

- RDP protocol implementation supports user authentication over RADIUS and TACACS+ in challenge-response mode.
- For RDP servers are supported NLA mode and TLS mode.
- For RDP listeners, besides the standard security level, the *Enhanced RDP Security with TLS* option is supported.
- In case the *NLA* option enabled, Fudo Enterprise requires NTLM protocol version 2 or newer. To properly handle NLA authentication connections, enable option to only send NTLMv2 response both on client and server side.
  1. Click *Start* > *All Programs* > *Accessories* > *Run*.
  2. Type `secpol.msc` in the *Open* input field and click *OK*.
  3. Select *Local Policies* > *Security Options* and double-click *Network Security: LAN Manager authentication level*.
  4. Select *Send NTLMv2 response only. Refuse LM & NTLM* from the drop-down list.
  5. Click *Apply*.

- Fudo Enterprise verifies input language settings when negotiation connection and does not support dynamic language change on the login screen.

RemoteApp:

Fudo natively supports RemoteApp connections over RDP protocol. Application windows are recorded the same way as RDP connections, enforcing all Fudo Enterprise security restrictions.

To monitor RemoteApp sessions, the connection must be launched through a `*.rdp` configuration file with the Fudo Enterprise IP address and the port number defined.

Multi-Monitor Sessions:

Fudo Enterprise supports multi-monitor sessions for the RDP protocol, allowing monitoring and logging of graphical sessions across more than one display.

3.4.8 SSH

Supported connection modes:

- *Bastion*
- *Proxy*
- Tunnel

Supported client applications:

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

Supported features:

- Connections multiplexing (video export, session termination, pause, join, playback, raw data),
- SCP (raw data, session termination, extracting separate files),
- SFTP,
- 2FA,
- Port redirection (video export, session termination, pause, session join, playback, raw data),
- SSH Agent forwarding (transparent, not recorded),
- X11 - within SSH protocol (video export, session termination, pause, session join, playback, raw data),
- Shell (video export, session termination, pause, session join, playback, raw data),
- Terminal (video export, session termination, pause, session join, playback, raw data).

Supported hashing algorithms:

- MD5
- SHA256

Supported types of SSH keys:

- RSA
- ED25519, ED25519-SK
- ECDSA, ECDSA-SK

Supported encoding: UTF-8

Supported ciphers:

Note

The following lists apply to Fudo Enterprise 6.1 and later, which use *OpenSSH* 10.2. If you are using an earlier version of Fudo Enterprise, refer to the documentation for that version.

The lists apply to both parts of the connection: between the client and the listener, and between Fudo Enterprise and the server. The *Legacy crypto* option is set separately for the listener and for the server.

- Supported *key exchange* algorithms:
  - `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`
  - `mlkem768x25519-sha256`
  - `sntrup761x25519-sha512`
  - `sntrup761x25519-sha512@openssh.com`
- additionally, there are 3 more *key exchange* algorithms supported when the *Legacy crypto* option is enabled:
  - `diffie-hellman-group14-sha1`
  - `diffie-hellman-group1-sha1`
  - `diffie-hellman-group-exchange-sha1`
- Supported *host key* algorithms:
  - `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
- plus, there are 2 more *host key* algorithms supported when the *Legacy crypto* option is enabled:
  - ssh-rsa
  - ssh-rsa-cert-v01@openssh.com
- Supported *encryption* algorithms:
  - chacha20-poly1305@openssh.com
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - aes128-gcm@openssh.com
  - aes256-gcm@openssh.com
- additionally, there are 4 more *encryption* algorithms supported when the *Legacy crypto* option is enabled:
  - aes128-cbc
  - aes192-cbc
  - aes256-cbc
  - 3des-cbc
- Supported *MAC* algorithms:
  - umac-128-etm@openssh.com
  - hmac-sha2-256-etm@openssh.com
  - hmac-sha2-512-etm@openssh.com
  - umac-128@openssh.com
  - hmac-sha2-256
  - hmac-sha2-512

- plus, there are 10 more *MAC* algorithms supported when the *Legacy crypto* option is enabled:
  - `hmac-sha1`
  - `hmac-sha1-etm@openssh.com`
  - `hmac-sha1-96-etm@openssh.com`
  - `hmac-sha1-96`
  - `hmac-md5`
  - `hmac-md5-96`
  - `hmac-md5-etm@openssh.com`
  - `hmac-md5-96-etm@openssh.com`
  - `umac-64-etm@openssh.com`
  - `umac-64@openssh.com`

Notes:

- SSH protocol implementation supports user authentication over RADIUS and TACACS+ in challenge-response mode.

3.4.9 Telnet 3270

Under review

Support for the **Telnet 3270** protocol is **under review** and may be removed in a future release. If this protocol is critical to your environment, please contact Fudo Support for more information.

Supported connection modes:

- *Bastion*
- *Proxy*

Supported client applications: c3270.

Notes:

- Session joining is not supported.
- User must authenticate twice - first against Fudo and then against the target host.

Note

The FreeBSD terminal version of `telnet(1)` client (in comparison to those available on Linux distributions, like Debian) automatically passes the user login name to the destination server during the authentication process. This is due to the `-a` parameter, which is enabled by default and is responsible for passing the login name so that the user doesn't have to input it while loggin in. In order to disable automatic passing of the login name, use `-K` parameter or `-l` parameter with empty login.

It's recommended to pay attention to the default settings of your Telnet client.

3.4.10 Telnet 5250

Supported connection modes:

- *Bastion*
- *Proxy*

Supported client applications: tn5250.

Notes:

- Session joining is not supported.
- User must authenticate twice - first against Fudo and then against the target host.

Note

The FreeBSD terminal version of `telnet(1)` client (in comparison to those available on Linux distributions, like Debian) automatically passes the user login name to the destination server during the authentication process. This is due to the `-a` parameter, which is enabled by default and is responsible for passing the login name so that the user doesn't have to input it while loggin in. In order to disable automatic passing of the login name, use `-K` parameter or `-l` parameter with empty login.

It's recommended to pay attention to the default settings of your Telnet client.

3.4.11 Telnet

Supported connection modes:

- *Bastion*
- *Proxy*

Notes:

- User must authenticate twice - first against Fudo and then against the target host.

Note

The FreeBSD terminal version of `telnet(1)` client (in comparison to those available on Linux distributions, like Debian) automatically passes the user login name to the destination server during the authentication process. This is due to the `-a` parameter, which is enabled by default and is responsible for passing the login name so that the user doesn't have to input it while loggin in. In order to disable automatic passing of the login name, use `-K` parameter or `-l` parameter with empty login.

It's recommended to pay attention to the default settings of your Telnet client.

3.4.12 VNC

Supported connection modes:

- *Bastion*
- *Proxy*

Suggested client applications:

- TightVNC,
- TigerVNC,
- RealVNC.

Supported OCR languages:

- English
- German
- Norwegian
- Ukrainian
- Polish
- Hungarian
- Russian

Notes:

- VNC protocol implementation supports user authentication over RADIUS and TACACS+ in challenge-response mode.
- File copying and file transfer are not supported over VNC. The protocol handles only clipboard text transfer (Client Cut Text and Server Cut Text).
- The User Access Gateway Webclient clipboard is not available in VNC sessions.

Connection specifics - VNC server requires authentication:

- *Anonymous* type account: requires entering VNC server password (login string is ignored).
- *Regular* type account: requires user login and password (authentication against Fudo); login substitution string defined in the account is ignored upon establishing connection.
- *Forward* type account: requires that users inputs password defined on the VNC server (login string is ignored).

Connection specifics - server does not require authentication:

- *Anonymous* type account: does not require any login information input (hit the enter key on the logon screen).
- *Regular* type account: requires user login and password information (authentication against Fudo); password substitution string can be left empty as it is not forwarded to the target host.
- *Forward* type account: requires user login and password (authentication against Fudo).

3.4.13 X11

X11 protocol is supported within the SSH protocol.

> **Note**
>
> *Session joining* feature is not supported in X11 protocol connections.

Supported servers:

- Xorg,
- Xming,
- XQuartz.

Supported fonts:

For a list of fonts available for the applications that use core X11 protocol to draw text, check the list of fonts available in Fudo Enterprise.

3.4.14 TCP

TCP is a generic protocol used for monitoring non-encrypted connections.

Supported connection modes:

- *Proxy*

Notes:

- Session joining is not supported.
- Session player displays raw text without graphical rendering.
- SSL encryption is not supported.

3.4.15 Secret Checkout

Secret Checkout is a virtual protocol for establishing an access session to the account secret. *Checkout* function allows user to temporarily take a secret from a secret vault. Then, the user informs Fudo that the secret is no longer needed by returning it to the secret vault with a *Checkin* operation.

> **Note**
>
> The protocol is virtual in a sense that there is no TCP/IP session related to it, only meta information is stored (for example checkout time, checkin time, who accessed the secret). As there is no TCP/IP, no data that can be played are saved. This makes checkout sessions lightweight compared to sessions recorded with data, such as RDP.
>
> In case of a breach, having secret checkouts recorded as sessions, allows one to pinpoint who had access to the leaked secret.

A request for a secret checkout is sent by a user via the User Portal. The request can be approved or declined by an administrator if a given safe is set to require approval. The user can see and copy the password anytime during the session, which counts active till the password is returned or the password's valid time is over.

The secret can be returned automatically after the given period of time or returned manually by the user via the User Portal. More on how to configure a timeout for automatic return of the password is at *Creating a safe* page under *Users* tab section and at *Creating an account with regular type* page under *Credentials* section.

When a *checkout timeout* is configured for an account with an ongoing checkout session, the other user can checkout the secret, too . In this situation the user has to confirm the operation by forcing checkout. This way the user can use soft exclusiveness of the checkout operation.

After return, the secret can be automatically changed to a new one, generated in accordance with the specified Secret Change Policy for a particular account.

Notes:

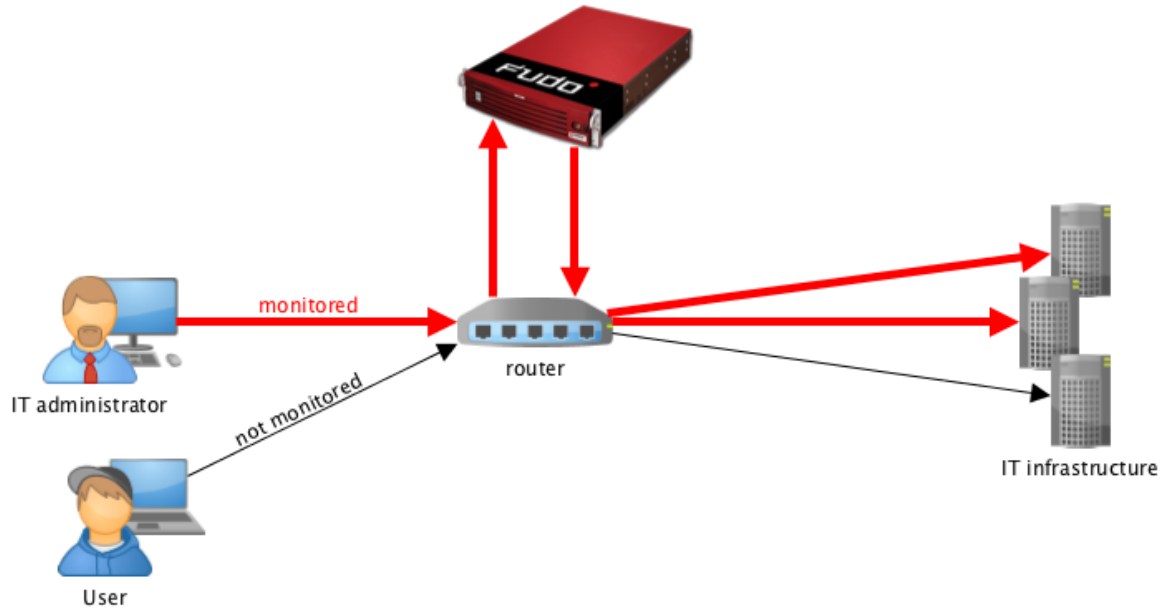
- *Session joining* feature is not supported.
- Playback is not supported.

3.5 Deployment Scenarios

> **Note**
>
> It is advised to deploy the Fudo Enterprise within the IT infrastructure, so it only mediates administrative connections. It will allow for lowering system load, network traffic optimization as well as maintaining access to hosted services in case of hardware malfunction.

Forced routing

Forced routing mode requires using a properly configured router. Such solution allows controlling network traffic in third ISO/OSI network layer, so only administrative requests are routed through Fudo Enterprise and the rest of the traffic is forwarded directly to the destination server.



This mode does not require changes in existing network topology and enables network traffic optimization due to separating requests from system administrators and regular users.

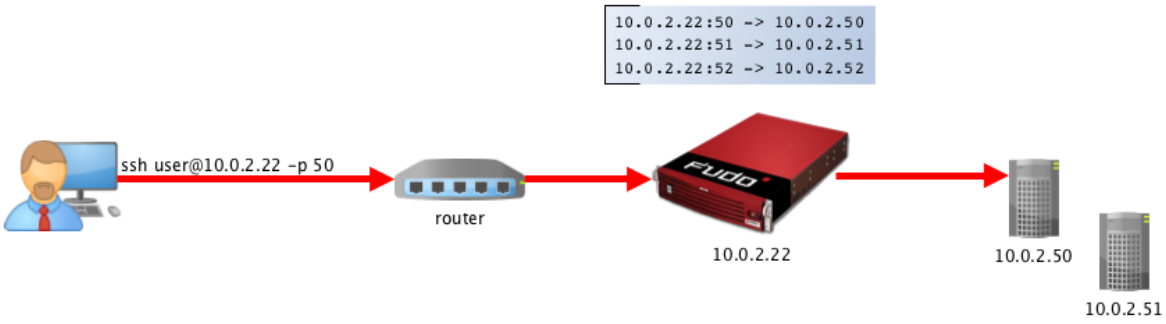
Related topics:

- *Connection Modes*
- *Managing servers*
- *User authentication methods and modes*
- *System overview*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*
- *Initial boot up*

3.6 Connection Modes

Proxy

In proxy mode, administrator connects to destination server using combination of Fudo Enterprise IP address and unique port number assigned to given server. Uniqueness of this combination enables establishing connection with a particular resource.

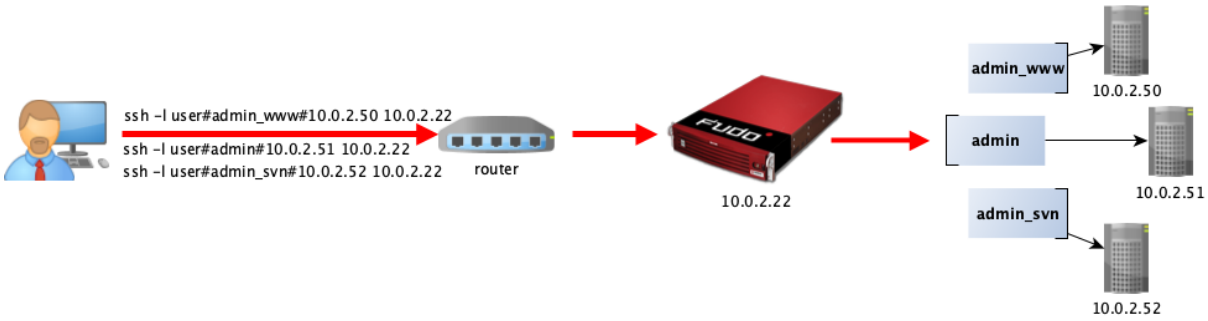


Such approach enables concealing actual IP addressing and allows configuring servers to only accept requests sent from Fudo Enterprise.

Bastion

> **Note**
>
> The *bastion* mode is supported when connecting over SSH, RDP, VNC, Telnet, Telnet 3270, Telnet 5250, MS SQL protocols.

In bastion mode, the target host is specified within the string identifying the user and the server their are trying to connect to, e.g. `ssh user#root#10.0.2.22`. This enables facilitating access to a group of monitored servers through the same IP address and port number combination.



While connecting, the Fudo Enterprise expects:

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

- `<username>`: User's login on Fudo Enterprise,
- `[@domain]` is optional,
- `<serverlogin>`: user's login on the target server,
- `<address>`: server address on the target server (the `<port>` can be omitted if native for protocol).

> **Warning**
>
> # character in between is required.

Target object string is matched in the following sequence:

1. Exact username - Fudo Enterprise tries to match the string with object defined in the local database.
2. Exact server address - Fudo Enterprise tries to match the string with an IP address of a server object defined in the local database.
3. IP address returned by the DNS service - Fudo Enterprise queries the DNS service and tries to match the returned IP address with an IP address of a server object defined in the local database.
4. Hostname returned by the reverse DNS service - Fudo Enterprise queries the reverse DNS service and tries to match the returned hostname with a sever object defined in the local database.

Note

If an account object doesn't have a *login* defined, the Fudo Enterprise system will ask for a *login* while connecting to the target server.

Related topics:

- *Deployment Scenarios*
- *Managing servers*
- *User authentication methods and modes*
- *System overview*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*
- *Initial boot up*

3.7 User Authentication Methods and Modes

User authentication methods

Before establishing connections with server, Fudo authorizes user using one of the following authorization method:

- *Static password*,
- *Public key*,
- *CERB*,
- *RADIUS*,
- *TACACS+*,
- *LDAP*,
- *Active Directory*,
- *OATH*,
- *SMS*,
- *DUO*,
- *Certificate*.

Note

- External authentication servers CERB, RADIUS, TACACS+, LDAP and Active Directory as well as SMS and DUO require configuration. For more information, refer to the *External authentication* topic.
- RDP, SSH and VNC protocols support user authentication over RADIUS and TACACS+ in *challenge-response* mode.

Authentication modes

After authenticating the user, Fudo proceeds with establishing connection with the target system using original user credentials or substituting them with values stored locally or fetched from a password vault.

> **Note**
>
> Due to specifics of VNC protocol, which authenticates the user using password only, the login entered on the logon screen is ignored when establishing a VNC connection.

Authentication with original login and password

In this authentication mode, Fudo uses login and password provided by the user upon logon to authenticate the user on the target system.

Authentication with login and password substitution

In this authentication mode, Fudo substitutes user login and password with previously defined ones.

Authentication with login and password substitution enables precise identification of the person who connected to the server, in case a number of users use the same credentials to access the server.

> **Note**
>
> - The password to the target system can be either explicitly defined in the *account* or can be obtained from internal or external password vault upon each access request. For more information, refer to the *Secret Changers* and *External passwords repositories* topics.
> - Due to specifics of VNC protocol, which authenticates the user using password only, the login entered as the substitution string is ignored when establishing a VNC connection.

> **Note**

In case of Oracle database, the user password and the privileged account password must be both either shorter than 16 characters or 16-32 characters long.

Two-fold authentication

In two-fold authentication mode user is asked for login and password twice. Once for authenticating against Fudo and once again to access the target system.

Authentication with password substitution

In this authentication mode, Fudo forwards login provided by user and substitutes the password when establishing connection with the target system.

Note

- The password to the target system can be either explicitly defined in the connection or can be obtained from the external passwords repository upon each access request. For more information, refer to the *External Passwords Repositories* topic.
- Due to specifics of VNC protocol, which authenticates the user using password only, the login entered on the logon screen is ignored when establishing a VNC connection.

Authentication by target server

In this mode, Fudo Enterprise forwards login credentials to the target host, which verifies whether the user is authorized to access it. Verification status is returned to Fudo Enterprise, which establishes monitored connection. Authentication by the target server is available only when monitoring SSH connections or RDP with TLS + NLA security option enabled.

Administrator approved access

Fudo Enterprise can be configured so each connection to a monitored server will require approval from the administrator using the administration interface.

Related topics:

- *Creating a Safe*
- *Approving Pending User Requests*
- *Declining Pending Requests*
- *System overview*
- *External authentication servers configuration*
- *Security measures*

3.8 Security Measures

3.8.1 Data Encryption

Data stored on Fudo Enterprise is encrypted with AES-XTS algorithm using 256 bit encryption keys. AES-XTS algorithm is most effective hard drive encryption solution.

Appliance

Encryption keys are stored on two USB flash drives. Flash drives delivered with Fudo Enterprise are uninitialized. Keys initialization takes place during initial system boot-up, during which both flash drives have to be connected (initiation procedure is described in chapter *System initiation*).

After encryption keys have been initiated and Fudo Enterprise has booted up, both USB flash drives can be removed and placed somewhere safe. During daily operation, encryption key is required only for system boot up. If safety procedures allow, one USB flash drive can stay connected to Fudo Enterprise, which will allow Fudo Enterprise to boot up automatically in case of a power outage or system reboot after software update.

Virtual machine distribution

Fudo Enterprise's file system, running in virtual environment is encrypted using an encryption phrase, which is set up during system initiation and has to be entered each time the system boots up.

Database

Sensitive data, such as passwords, keys, logins, etc. are encrypted in the internal database itself. The encryption key, called Master Key, is a random 256-bit key which is used to derive further keys used to encrypt each section of database, such as Configuration information (User data, Accounts, Safes, etc.), Database Backup and External Storage. Furthermore, Fudo makes use of HMACs to "seal" the encrypted data. Master Key can be exported by superadministrator but only when prior to MK export Fudo is provided a key to encrypt the Master Key itself.

Master Key export procedure allows superadministrator to create a backup of the Master Key, without which data in the database as well as backups and external filesystems cannot be used.

3.8.2 Backups

User sessions data can be backed up on external servers running rsync service.

3.8.3 Permissions

Each data model entity, has a list of users defined, who are allowed to manage given object, according to assigned user role and capabilities.

For more information on user roles refer to *Role-Based Access Control (RBAC)* topic.

3.8.4 Sandboxing

Fudo Enterprise takes advantage of CAPSICUM sandboxing mechanism, which separates each connection on Fudo Enterprise operating system level. Precise control over assigned system resources and limiting access to information on the operating system itself, increase security and greatly influence system's stability and availability.

3.8.5 Reliability

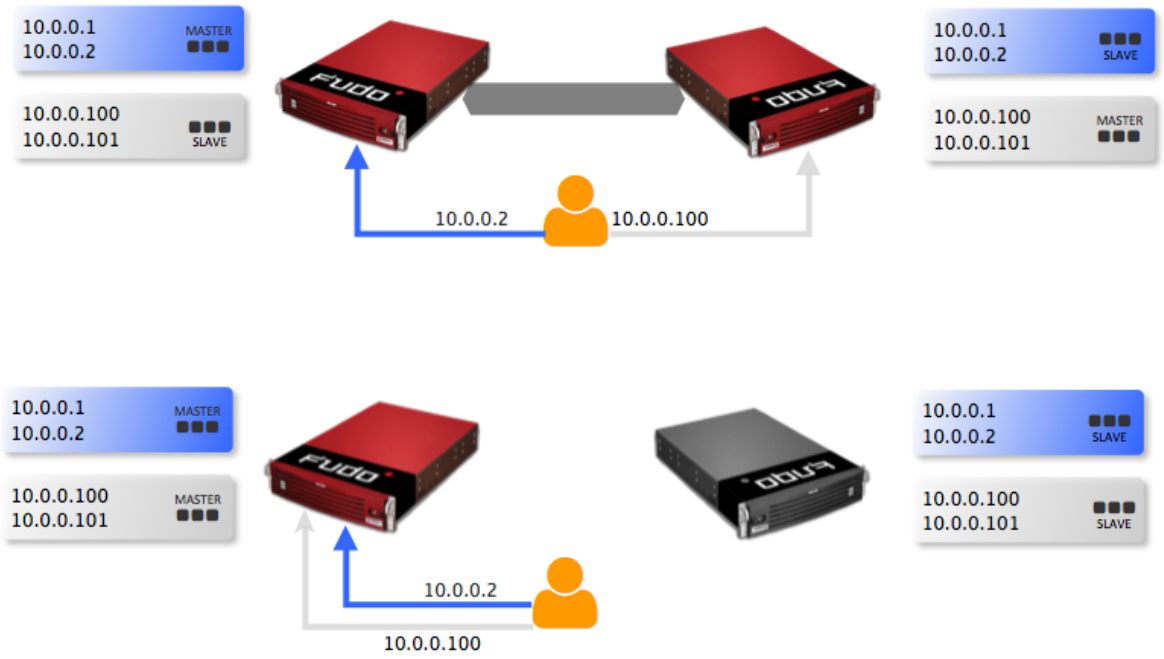
System hardware configuration is optimized to deliver high performance and high availability.

3.8.6 Cluster Configuration

Fudo Enterprise supports cluster configuration in multimaster mode where system configuration (connections, servers, sessions, etc.) is synchronized on each cluster node and in case a given node crashes, remaining nodes will immediately take over user connection requests ensuring service continuity.

> **Warning**
>
> Cluster configuration does not facilitate data backup. If session data is deleted on one of the cluster nodes, it is also deleted from other nodes.

Virtual IP addresses are aggregated in redundancy groups which enable facilitating static load balancing while preserving cluster's high availability nature.



Related topics:

- *User authorization methods and modes*
- *System overview*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*
- *System initiation*

3.9 Data Model

Fudo Enterprise defines five base object types: user, server, account, safe and listener.

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

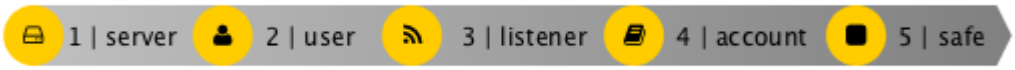
Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

Listener determines server connection mode (proxy, bastion) as well as its specifics.

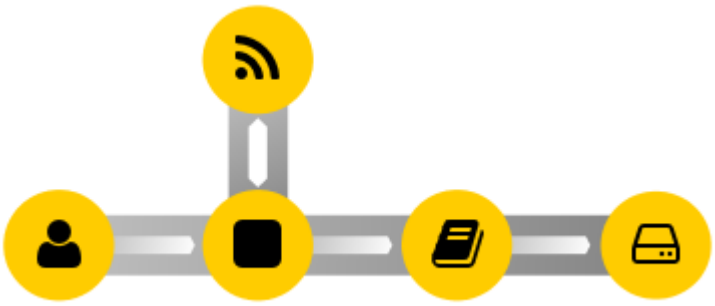
Proper system operation requires configuration of *servers*, *users*, *listeners*, *accounts* and *safes*.



Warning

Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances **must not** be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

Objects relations chart



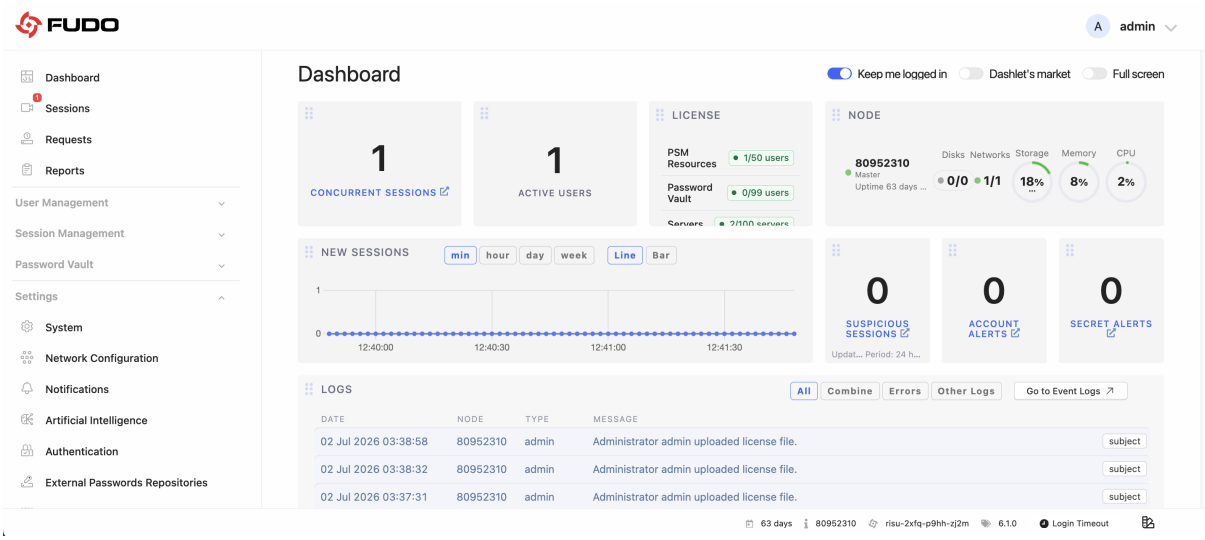
Safe is the central data model object. It regulates access to monitores servers by specifying privileged accounts on monitored servers along with the listeners which determine the actual connection parameters (e.g. IP address, port number) depending on the given protocol. This kind of data model allows for optimal objects' management. A given *server* can be accessed differently as defined by the listener. A *safe* groups accounts enabling convenient control over access to monitored resources.

Related topics:

- *System overview*
- *User authorization methods and modes*
- *Quick start*

3.10 Dashboard

Fudo Enterprise dashboard page enables quick access to essential status information. It comprises customizable dashlets allowing you to pick and choose the data that's the most important to you.



Note

- Select *Keep me logged in* if you do not want Fudo to log you out automatically as long as you are on the dashboard screen.
- Click *Full screen* to togge full-screen view.

3.10.1 Widgets

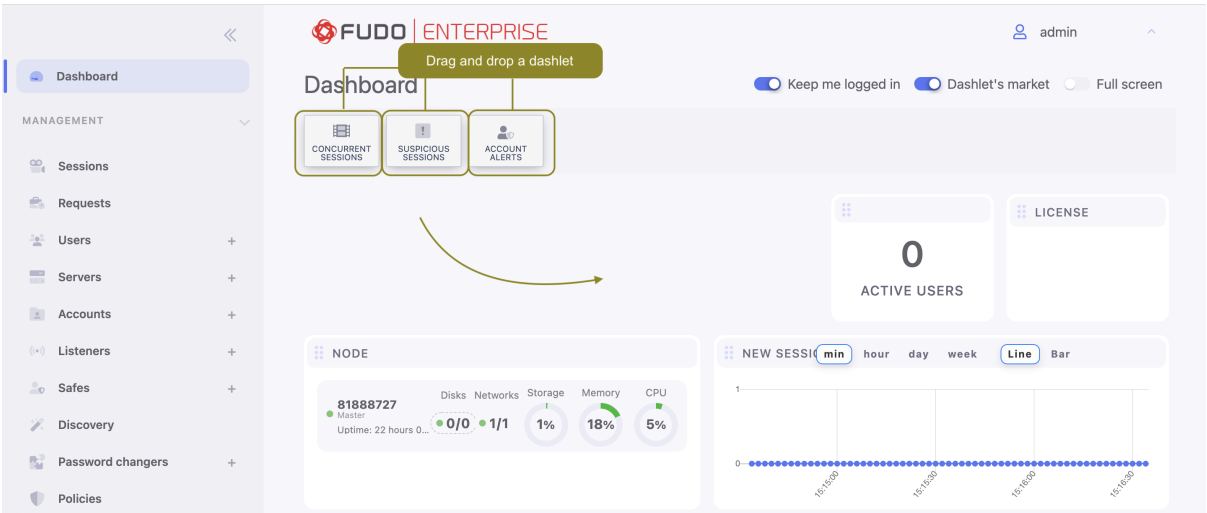
New sessions	Chart depicting the number of newly established connections in a given time interval.
Concurrent sessions	The current number of user sessions.
Suspicious sessions	High-threat level sessions. The widget allows the following timeline configurations for the sessions: last 12 hours, last day, last week, and last month. The Suspicious sessions widget also provides an URL to the filtered Sessions list with `Threat level: High` criteria set so that administrator can check what's going on and quickly react.
Account alerts	Number of accounts at risk of a security breach.
Active users	Nubmer of currently connected users.
License	Information on the active license.
Node	Status information on the current Fudo Enterprise instance as well as other nodes.
System logs	Recent system events.

Note

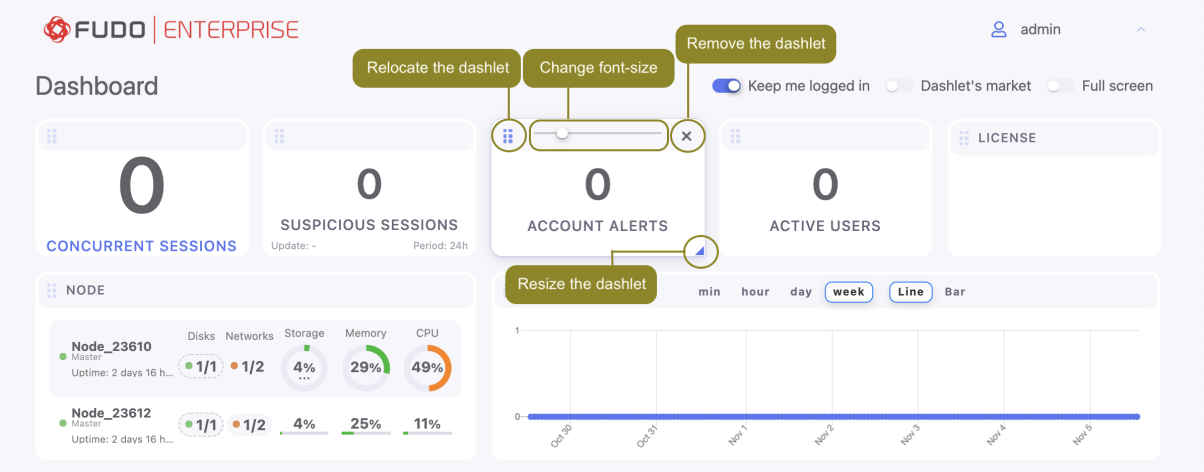
Available widgets depend on the user's privileges and object-level access (capabilities).

3.10.2 Adding, Customizing and Removind Dashlets

1. Click the *Dashlet's market* switcher to display available dashlets.



2. Drag and drop a dashlet onto the workspace.



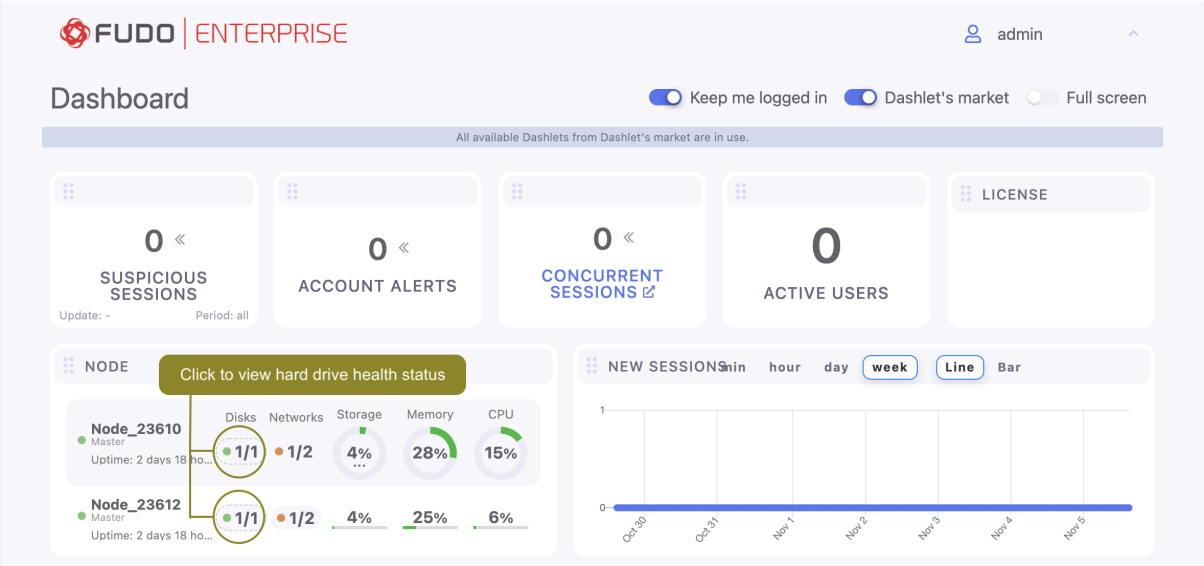
- Click and drag bottom-right corner of the dashlet to resize it.
- Click and drag the top-left corner to relocate the dashlet.
- Click arrows to change font-size.
- Click ⊗ icon in the top-right corner. Then, click *Remove* to remove selected dashlet.

Note

Removed dashlets appear in the dashlets market area.

3.10.3 Hard Drives Status Information

To view hard drive status information enable the *Node* dashlet and click the disks status icon.



	Hard drive operates properly.
	Data on the hard drive is being synchronized.
	Data read/write errors - the hard drive does not operate properly and it is likely to fail - contact the technical support to discuss hard drive replacement.
	Hard drive failure - the hard drive must be replaced - contact the technical support to discuss hard drive replacement.
	Hard drive has been removed.

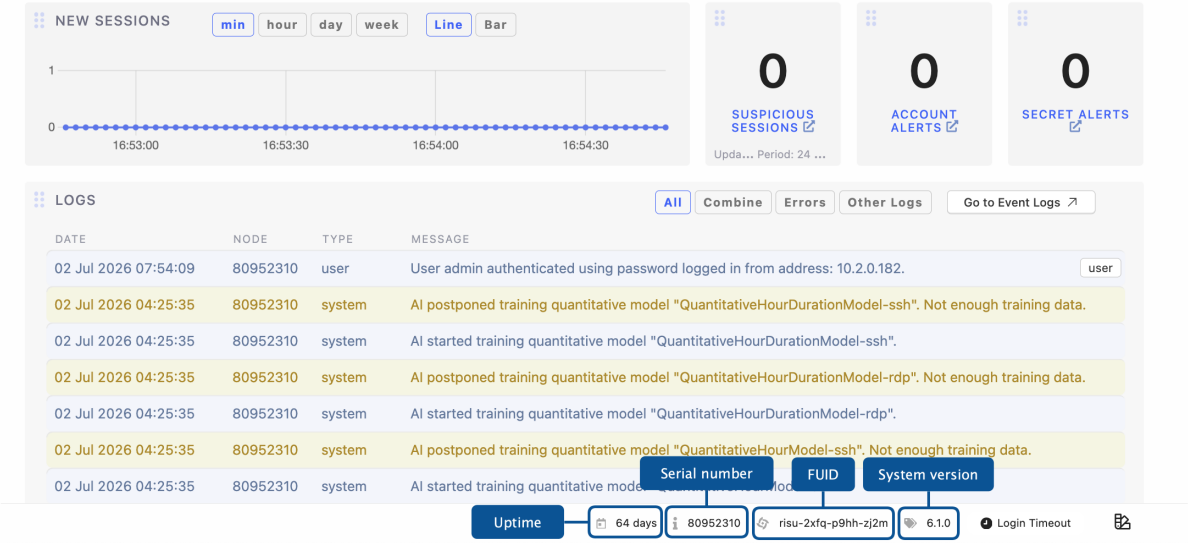
Related topics:

- *Initial boot up*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*

3.11 Footer Information

W prawym dolnym rogu ekranu, w obrębie stopki, znajdują się cztery elementy z informacjami systemowymi o bieżącej instancji Fudo Enterprise:

1. **Uptime** - how long the system has been running since it was last started.
2. **Serial Number** - identifier of the cluster node; unique within a single cluster.
3. **FUID (Fudo Unique Identifier)** - unique identifier of the current Fudo Enterprise instance.
4. **System Version** - current software version.



3.12 Third-Party Licenses

This section contains third-party license information for certain third-party products included with Fudo Enterprise.

All the relevant licenses for third-party tools we depend on to deliver our product are available here. Please click on the link to view copies of the licenses text.

If the indicated location does not contain a license for specific product, it means that it was not provided by the developer.

CHAPTER 4

System Deployment

This topic describes Fudo Enterprise appliance and the system initiation procedure.

4.1 Requirements

Admin Panel

The system is managed via the Admin Panel accessible through a web browser. Recommended browsers are Google Chrome, Mozilla Firefox, and Microsoft Edge.

Network requirements

Correct operation requires:

- Ability to establish connections to Fudo Enterprise on port 443/TCP, for administration purposes.
- Ability to establish an outgoing connection from Fudo Enterprise to the server `home.fudosecurity.com` on port 22/TCP for the *Callhome* service purpose.
- Ability for users to connect to Fudo Enterprise and for Fudo Enterprise to connect to target systems.
- Proper *time server configuration*.
- To establish a tunnel between Fudo Enterprise and Fudo ShareAccess, outbound traffic on port 65522 must be allowed to any destination.

Default ports used at startup

Port	Description
443/TCP	Required for administration purposes.
65522/TCP	Necessary for SSH-based administrative connections and tunnel establishment with Fudo ShareAccess.
22/TCP	Utilized for SSH listener, added by default in the configuration, and for Fudo Officer mobile app using *Callhome* service.
3389/TCP	Used for RDP listener, added by default in the configuration.

Hardware requirements

Fudo Enterprise is a complete solution combining both hardware and software. Installing system requires 2U (F100x model) or 3U (F300x model) of space in 19" rack cabinet and connection to network infrastructure.

Virtual appliance requirements

	100 concurrent sessions*	200 concurrent sessions*	300 concurrent sessions*
CPU	6 cores	20 cores	28 cores
RAM	32 GB	64 GB	128 GB

	6 months capacity**	2 years capacity**	7 years capacity**
Storage	24 TB	96 TB	288 TB

* Average 30% FullHD, 32bit graphical and 70% terminal sessions

** Calculated for 50 sessions created per day - 70% RDP FullHD 32bit and 30% SSH

Note

Storage size should be determined individually as it directly depends on the number of sessions monitored and recorded by Fudo Enterprise.

Target virutalization environments:

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

VNC software client requirements

VNC connections require 24-bit (true color) mode, with encryption disabled.

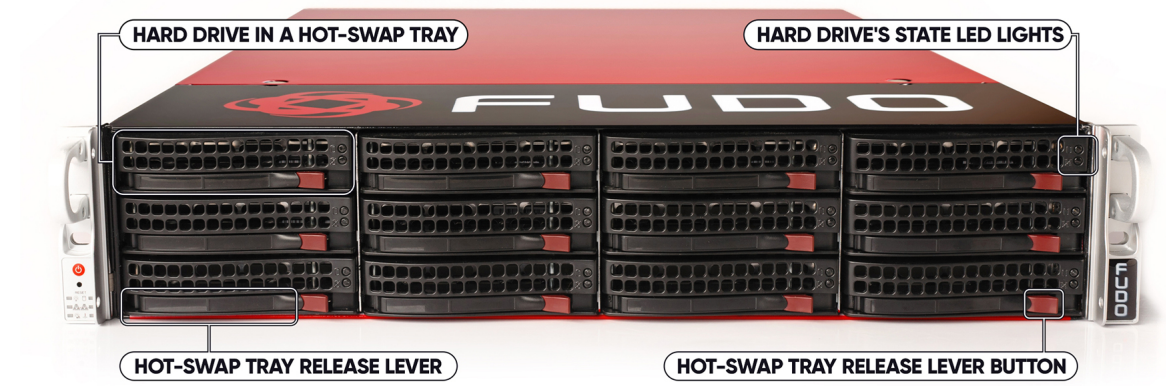
4.2 Hardware Overview

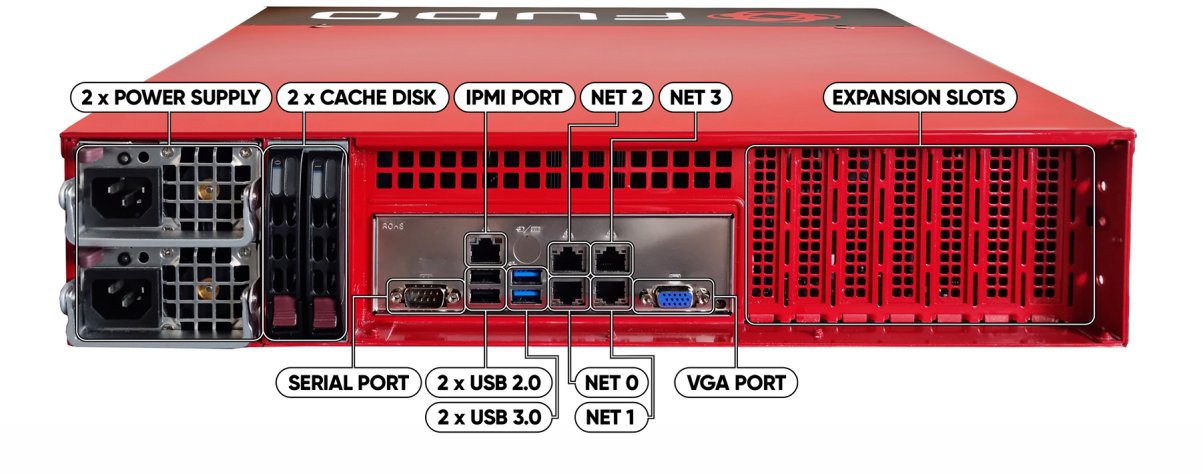
Fudo Enterprise is delivered in a 2U (F100x), 3U (F300x) or 4U (F500x) 19" rack server case.

Fudo Enterprise F1002

- Chassis: 19" 2U
- Dimensions: 89 mm (height), 437 mm (width), 647 mm (depth)
- PSU: 2x 920 W
- System memory: 32 GB
- Internal storage: 12x 2 TB, 2x 480 GB SSD
- Network interfaces:
  - 4 x RJ45 Gigabit Ethernet LAN ports
  - 1 x RJ45 Dedicated IPMI LAN port

  The situation might be different, depending on the use of the expansion cards.





Fudo Enterprise F1003

- Chassis: 19” 2U
- Dimensions: 89 mm (height), 437 mm (width), 647 mm (depth)
- PSU: 2x 1200 W
- System memory: 64 GB
- Internal storage: 8x 6 TB, 2x 960 GB NVMe
- Network interfaces:
  - 4 x RJ45 Gigabit Ethernet LAN ports
  - 1 x RJ45 Dedicated IPMI LAN port

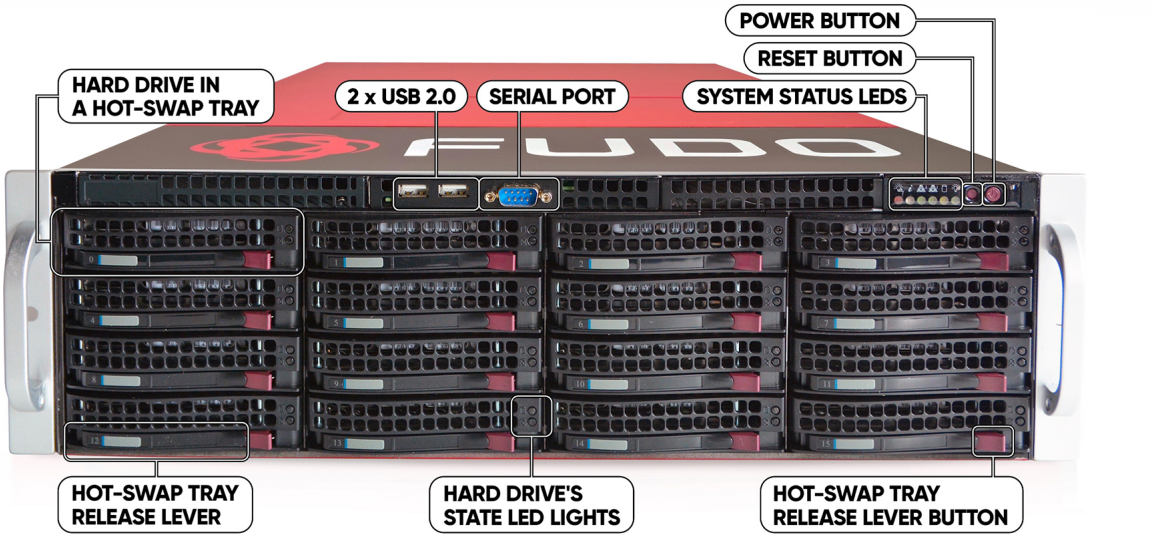
  The situation might be different, depending on the use of the expansion cards.

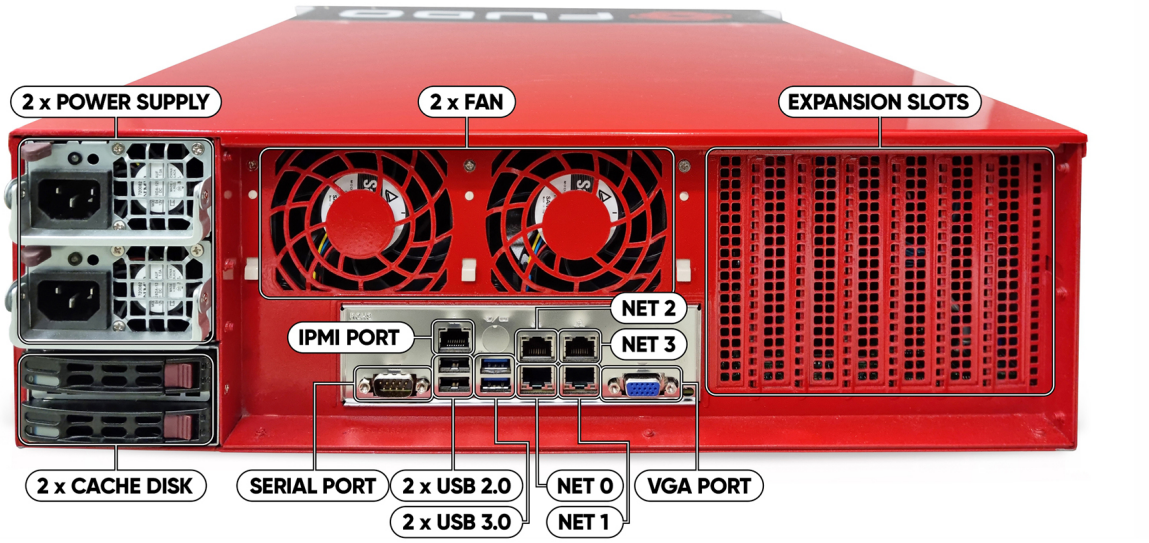
Fudo Enterprise F3002

- Chassis: 19” 3U
- Dimensions: 132 mm (height), 437 mm (width), 647 mm (depth)
- PSU: 2x 1000 W
- System memory: 64 GB
- Internal storage: 16x 6 TB HDD, 2x 480 GB SSD
- Network interfaces:
  - 4 x RJ45 Gigabit Ethernet LAN ports
  - 1 x RJ45 Dedicated IPMI LAN port

  The situation might be different, depending on the use of the expansion cards.

FRONT PANEL RELEASE LATCH
SYSTEM STATUS LEDS
FUDO
FRONT PANEL LOCK


POWER BUTTON
RESET BUTTON
HARD DRIVE IN A HOT-SWAP TRAY
2 x USB 2.0
SERIAL PORT
SYSTEM STATUS LEDS
FUDO
HOT-SWAP TRAY RELEASE LEVER
HARD DRIVE'S STATE LED LIGHTS
HOT-SWAP TRAY RELEASE LEVER BUTTON


2 x POWER SUPPLY
2 x FAN
EXPANSION SLOTS
NET 2
IPMI PORT
NET 3
2 x CACHE DISK
SERIAL PORT
2 x USB 2.0
NET 0
VGA PORT
2 x USB 3.0
NET 1

Fudo Enterprise F3003

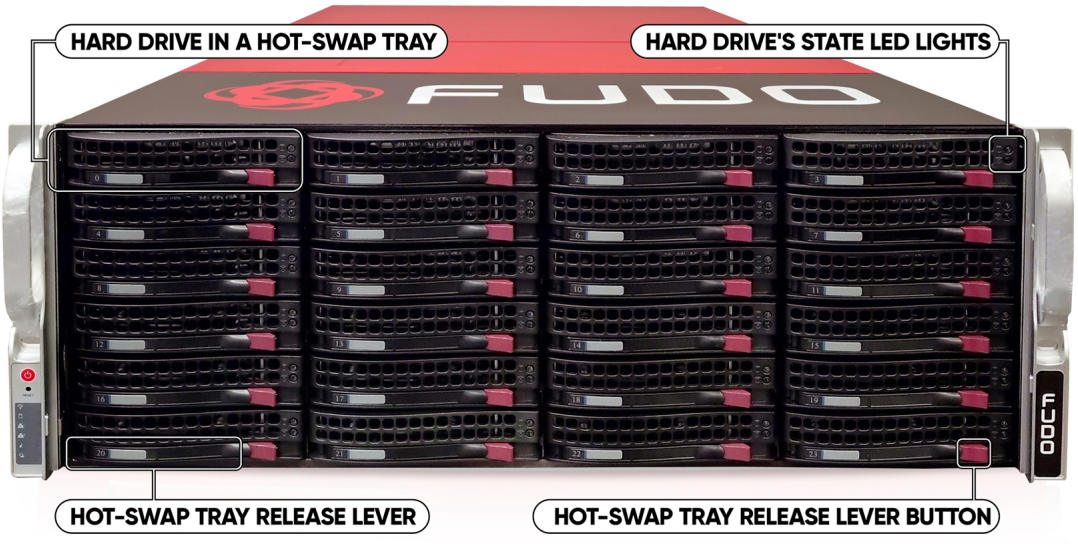
- Chassis: 19” 3U
- Dimensions: 132 mm (height), 437 mm (width), 647 mm (depth)
- PSU: 2x 1200 W
- System memory: 128 GB
- Internal storage: 16x 6 TB HDD, 2x 960 GB NVMe
- Network interfaces:
  - 4 x RJ45 Gigabit Ethernet LAN ports
  - 1 x RJ45 Dedicated IPMI LAN port

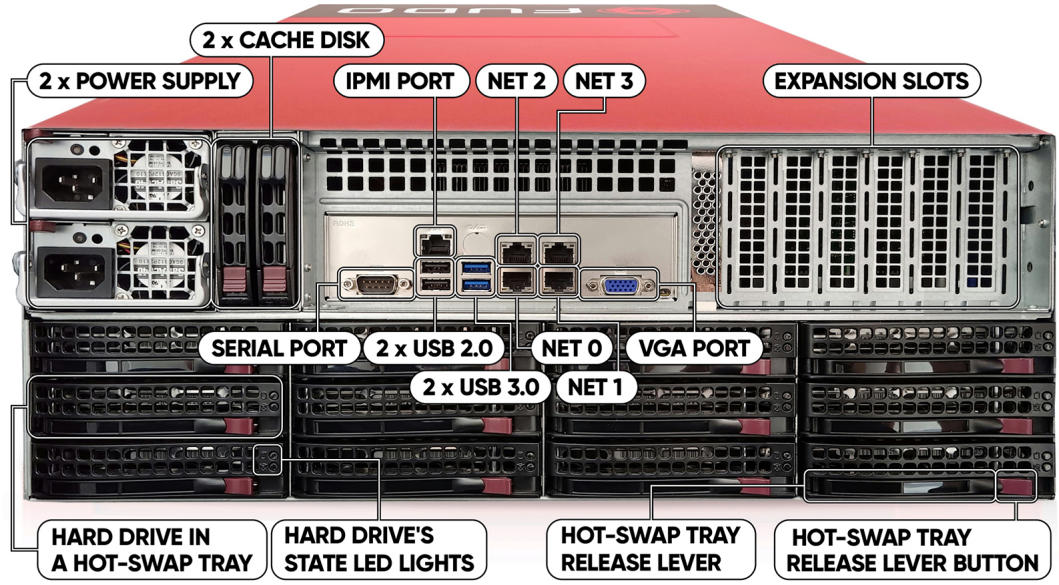
  The situation might be different, depending on the use of the expansion cards.

Fudo Enterprise F5000

- Chassis: 19” 4U
- Dimensions: 178 mm (height), 437 mm (width), 699 mm (depth)
- PSU: 2x 1280 W
- System memory: 128 GB
- Internal storage: 36x 8 TB, 2x 480 GB SSD
- Network interfaces:
  - 4 x RJ45 Gigabit Ethernet LAN ports
  - 1 x RJ45 Dedicated IPMI LAN port

  The situation might be different, depending on the use of the expansion cards.





IPMI Login Credentials

The IPMI login is `ADMIN`. To find the IPMI password, check whether the front panel of the device has a flat pull-out tab. It can be located on the top edge of the panel, right of the centre, or on its left edge. Pull out the tab and read the password from the label on it. The password follows the `PWD:` marking.

Note

No tab: On older devices that have no tab, the default password is `ADMIN`. Change it after the first login.

Important

If the label on the tab is damaged or unreadable, you can also read the password from the label on the motherboard. To do so, remove the top cover of the device.

! Before removing the top cover, power off the device and disconnect the power cables. If you have any questions, contact Fudo Enterprise technical support.

Warning

IPMI Security Recommendations

The IPMI interface is provided by third-party hardware vendors and operates independently of our software. Please note that when it comes to firmware updates or fixes, we are dependent on Supermicro's release cycle. Unfortunately, this means that our ability to address certain issues related to IPMI is limited.

To reduce security risks when using IPMI, we recommend the following:

- Use strong, unique passwords for IPMI access.
- Restrict IPMI access to a dedicated and isolated network segment.
- Disable any IPMI features that are not actively used.

If you have any further questions, please **contact our support team**.

Related topics:

- *Initial boot up*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*

4.3 System Initiation

Appliance

Fudo Enterprise is delivered with two uninitiated USB flash drives. During initial boot up, Fudo Enterprise generates encryption keys, which are stored on enclosed USB flash drives. More information on encryption keys can be found in the *Security measures* chapter.

1. Install device in 19" rack cabinet.
2. Connect both power supply units to 230V/110V power outlets.

Note

Connecting both power supplies is necessary to start the system.

3. Connect network cable to one of the RJ-45 ports.
4. Connect both of the USB flash drives delivered with Fudo Enterprise.

Note

Initial boot up requires conecting both USB flash drives. More information on encryption keys can be found in *Security measures* chapter.

5. Press the power button on the front panel.

6. After keys have been initiated, disconnect USB flash drives.

Warning

- One of the USB flash drives containing encryption key must be disconnected and placed in a secure location, accessible only to authorized personnel.
- If the USB flash drives with encryption keys are lost, device will not be able to boot up and stored sessions will not be accessible. Manufacturer does not store any encryption keys.

Note

- In daily operation, one encryption key is required to start the system after which it can be disconnected.
- It is advised to make a backup copy of the encryption key.

Setting IP address using system console

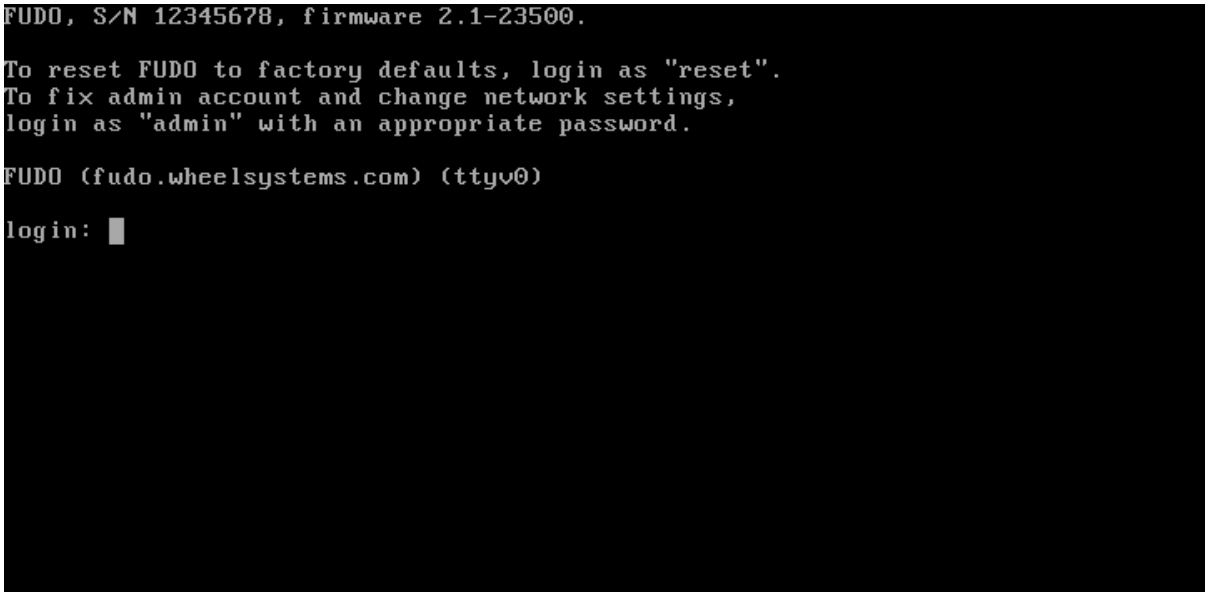
1. Connect monitor and keyboard to the device.
2. Enter administrator account login and press *Enter*.

Note

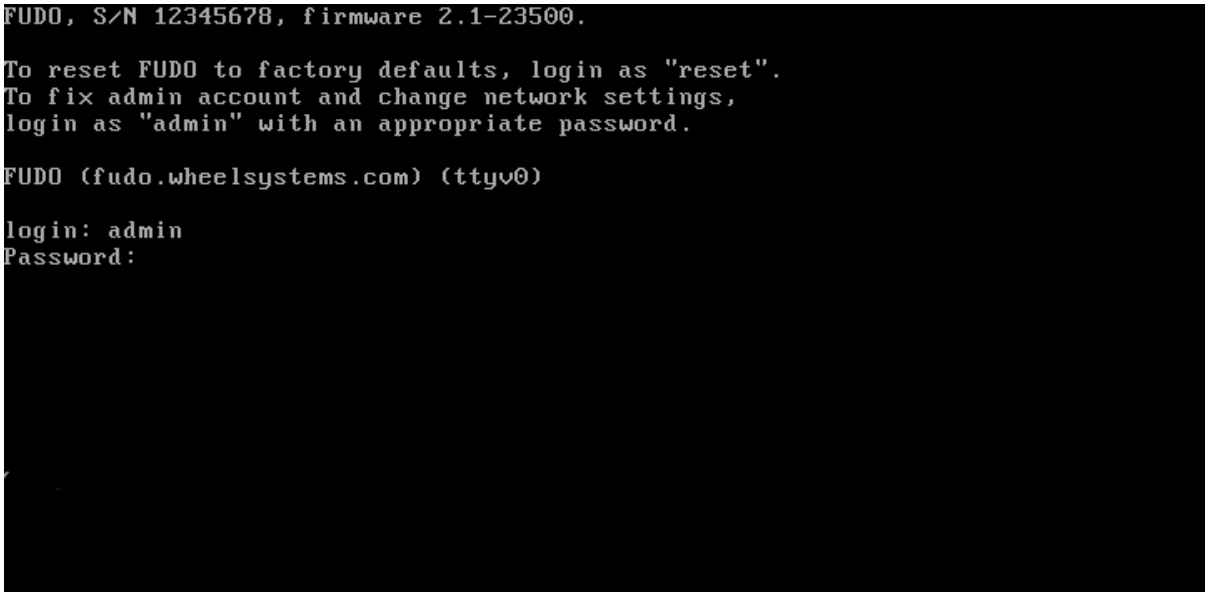
Default login credentials:

login: admin
password: proxycrypto

In cloud Fudo Enterprise versions virtual machine ID is usually set up as default password. Please contact your Fudo Enterprise reseller to learn more.



3. Enter administrator account password and press *Enter*.



4. Enter 2 and press *Enter* to change network configuration.

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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

Choose an option (0):
```

5. Enter `y` and press *Enter* to proceed with resetting network configuration.

```
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. Enter the name of the new management interface (Fudo Enterprise web interface is accessible through the management interface).

```
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. Enter IP address along with the network subnet mask separated with / (e.g. `10.0.0.8/24`) and press *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. Enter network gate and press *Enter*.

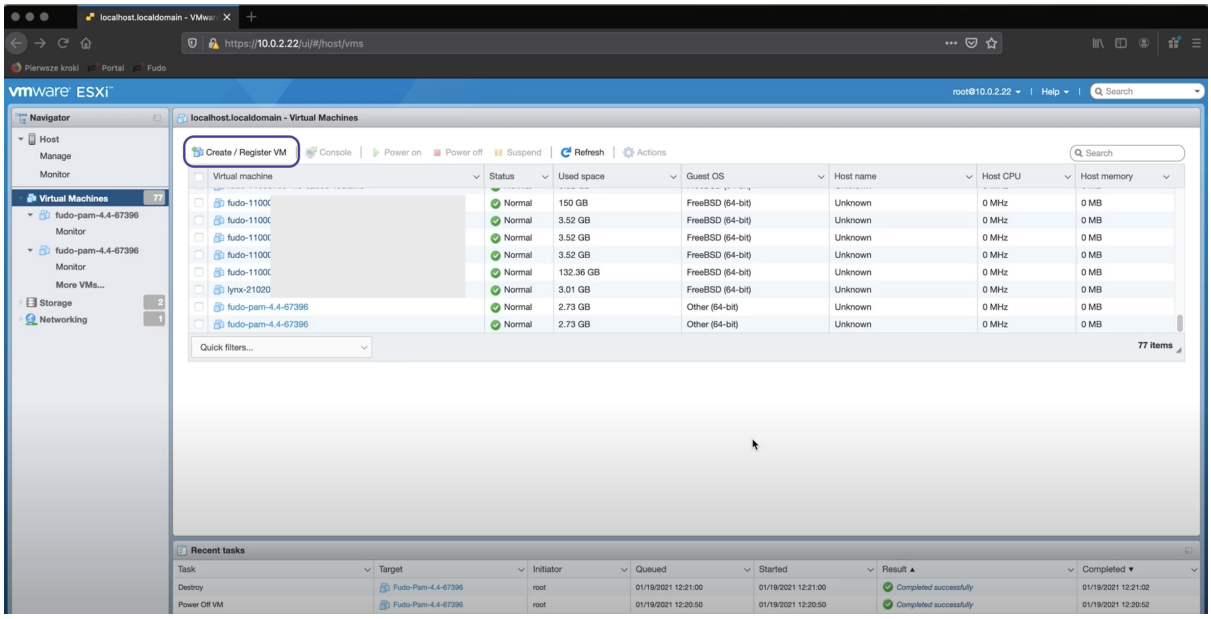
```
FUDO, S/N 12345678, firmware 2.1-23500.

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 Virtual Machine

Local Fudo Enterprise deployment is based on uploading the OVA / OVF file into virtualization tool and running the Fudo Enterprise instance on browser. Please follow below chapters to deploy Fudo Enterprise using the VMware or Proxmox virtualization tools. In order to proceed the deployment, the OVA or OVF file is needed.

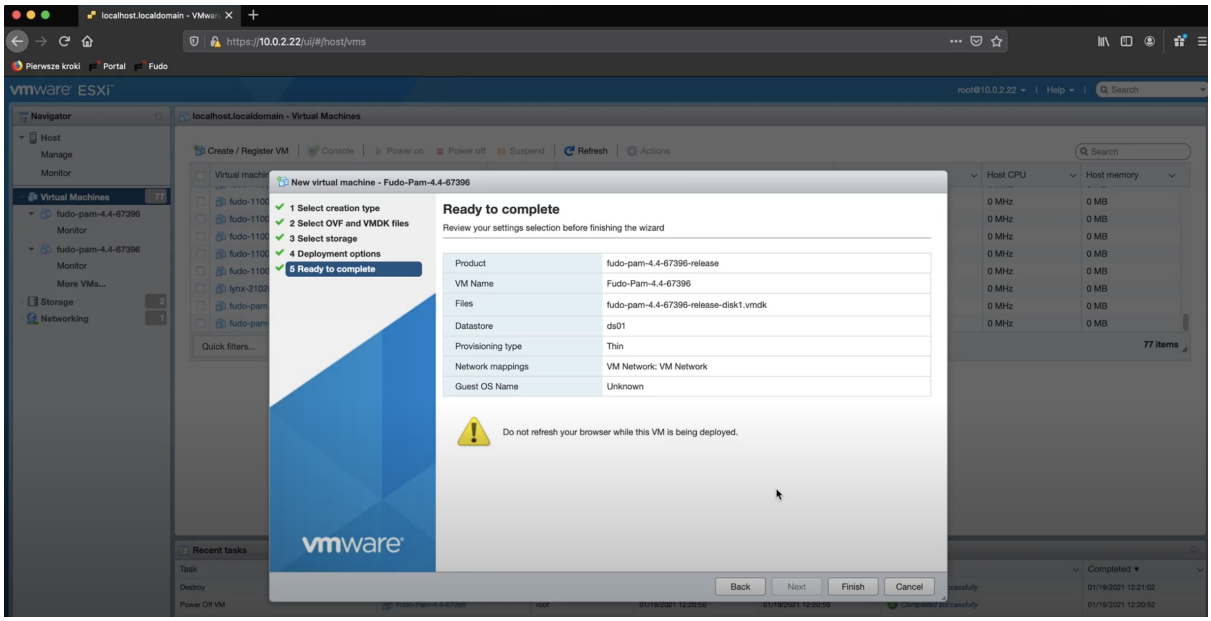
VMware Installation with OVA file

1. Click the *Create / Register VM* button.



2. In the modal window, select the *Deploy a virtual machine from an OVF or OVA file* option.
3. Select the downloaded OVA file and upload it, or just drag and drop it into the upload area.
4. Enter a name for the virtual machine.

5. Select the storage option.
6. Select deployment options.



7. Click *Finish* and wait for the configuration file to be fully uploaded.
8. Initialize the machine by selecting its record.
9. Click the *Console* button and select the *Launch remote console* option. Select your application and verify certificate.
10. In the console, provide a passphrase.

> **Note**
>
> The password is optional and can be left empty. However, if the password is provided, the Fudo system encrypts it and asks for it every time the VM is rebooted.

11. Select the region and city by providing respective codes and confirming your choice.
12. Enter date and time in `DD.MM.YYYY HH:MM` format.

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

13. Set the network configuration:

    a. Sign in as an administrator:

       login: admin
       password: proxycrypto

    b. From the list of the *Fudo configuration utility*, select option *3 - Reset network settings*.

    c. Select new management interface and enter the IP address.

```
Retype new password:

*** FUDO configuration utility ***

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

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

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

Available network interfaces:

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

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

Note

Your Fudo Enterprise instance has been successfully initiated! Now you can enter the regis-

tered IP address in your browser and start with your first configuration.

Proxmox Installation with OVF file

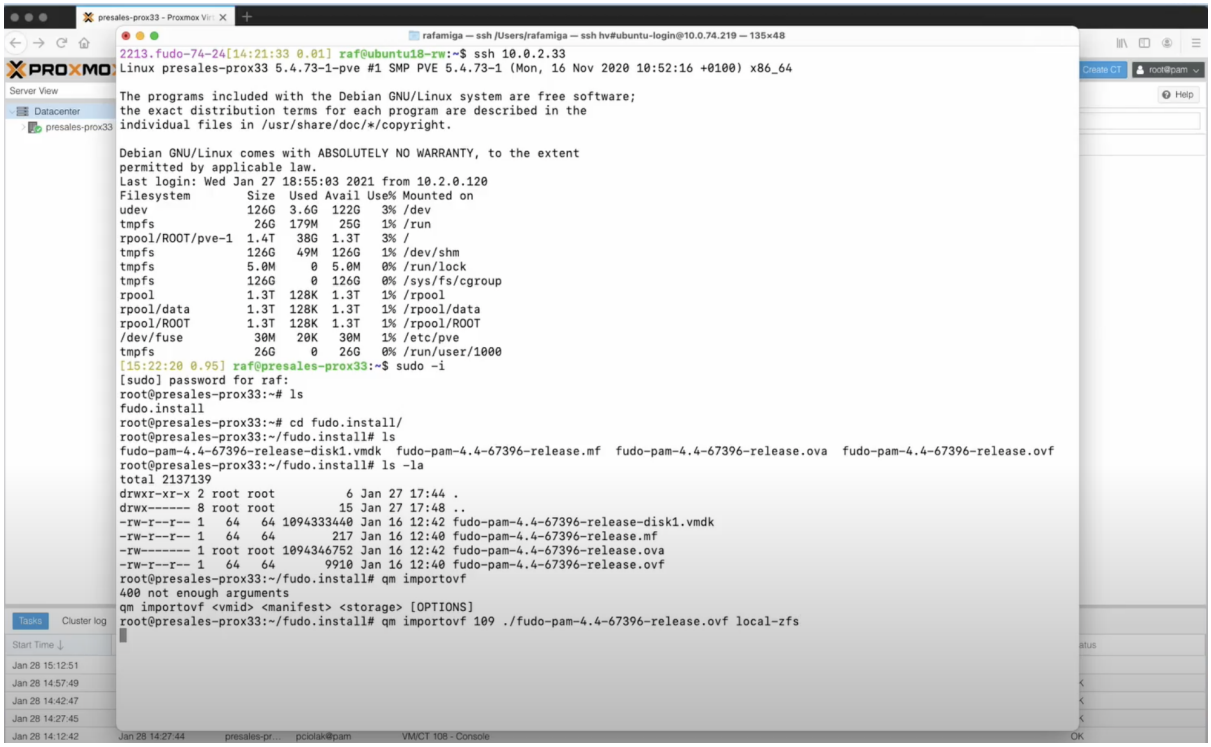
1. Create a new machine using cores, memory and VM name as read from the OVF manifest, and import the disks to the local-zfs storage:

   a. Log in to to a remote computer, for example, with `ssh 10.0.2.33` and provide a password.

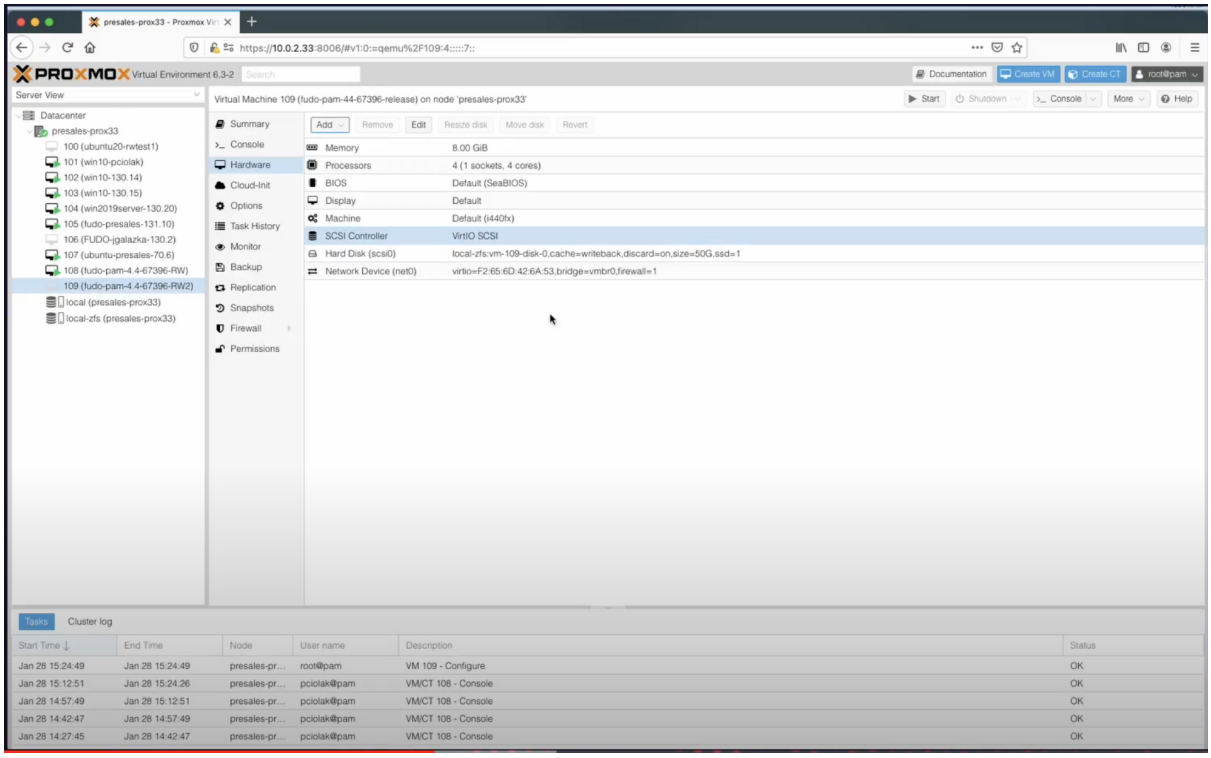
   b. In the folder *fudo.install* execute a command: `qm importovf <vmid> <manifest> <storage> [OPTIONS]`

   for example:

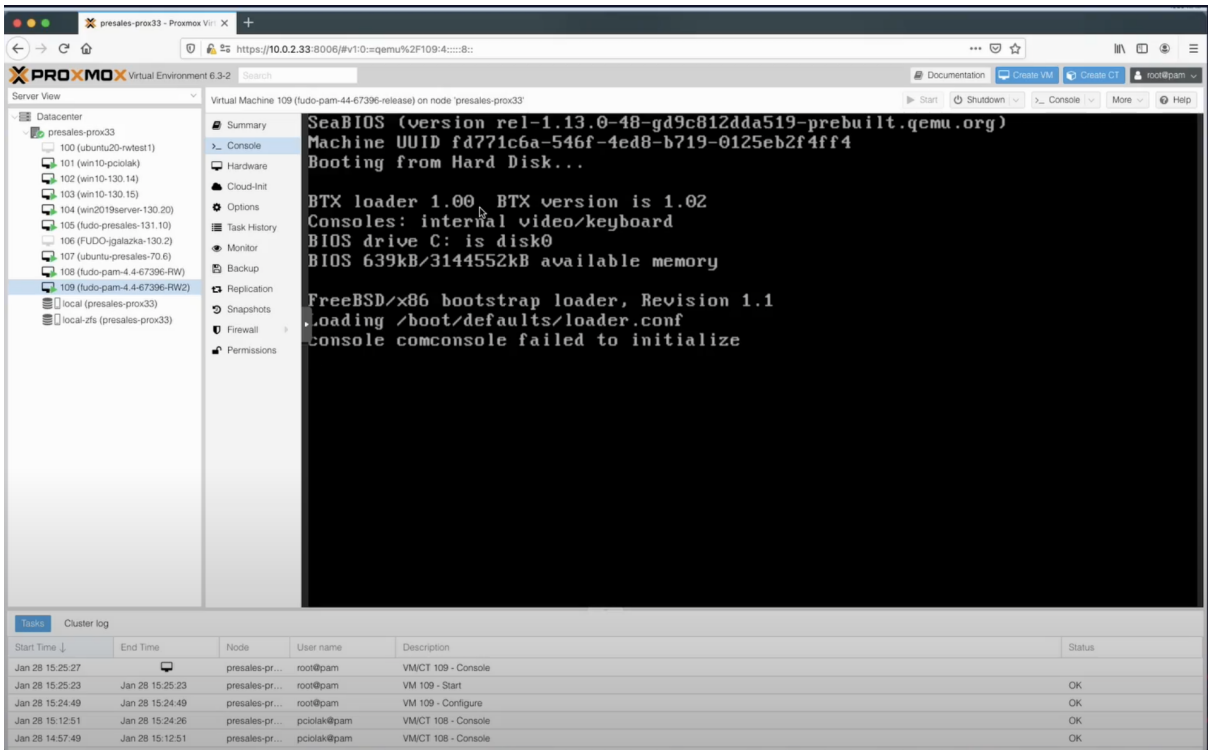
   `qm importovf 109 ./fudo-one-36271-release.ovf local-zfs`



2. Wait for the manifest data to be imported.
3. In the Proxmox client find your server and open settings for your `109 (fudo-one-36271-release)` virtual machine.
4. In the *Hardware section*, change the *Hard Disk* options into the *Write back* cache, and in *Advanced section* check the *SSD emulation* option, then the *Discard* option. Click *OK*.
5. In the *SCSI Controller* section, select the *VirtIO SCSI* option as a SCSI controller type.
6. Add a new Network Device and in the *Model* field select the *VirtIO (paravirtualized)* option.



7. Click the *Start* option.
8. Go to the *Console*.



9. Select the region and city by providing respective codes and confirming your choice.
10. Enter date and time in `DD.MM.YYYY HH:MM` format.
11. Set the network configuration:
    a. Sign in as an administrator:

login: admin
password: proxycrypto

b. From the list of the *Fudo configuration utility*, select the option *3 - Reset network settings*.

c. Select new management interface and enter the IP address with a mask.

d. Enter a new default gateway IP address.

Note

Your Fudo Enterprise instance has been successfully initiated!

12. Enter the registered IP address in your browser bar and sign in as an administrator.
13. In the *Network configuration settings* input a name for the User Access Gateway address. Click *Save*.
14. Add a new DNS server address in the Name & DNS sub-tab. Click *Save*.
15. In the System settings, add a new NTP server address. Click *Save*.
16. From the contextual menu in the upper right corner, select the *Restart* option.
17. Wait for the system to be restarted and sign in back again.

Note

Now you can start with your first configuration!

Related topics:

- *Requirements*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*
- *System overview*
- *Security measures*

4.4 Accessing Fudo Enterprise Portals

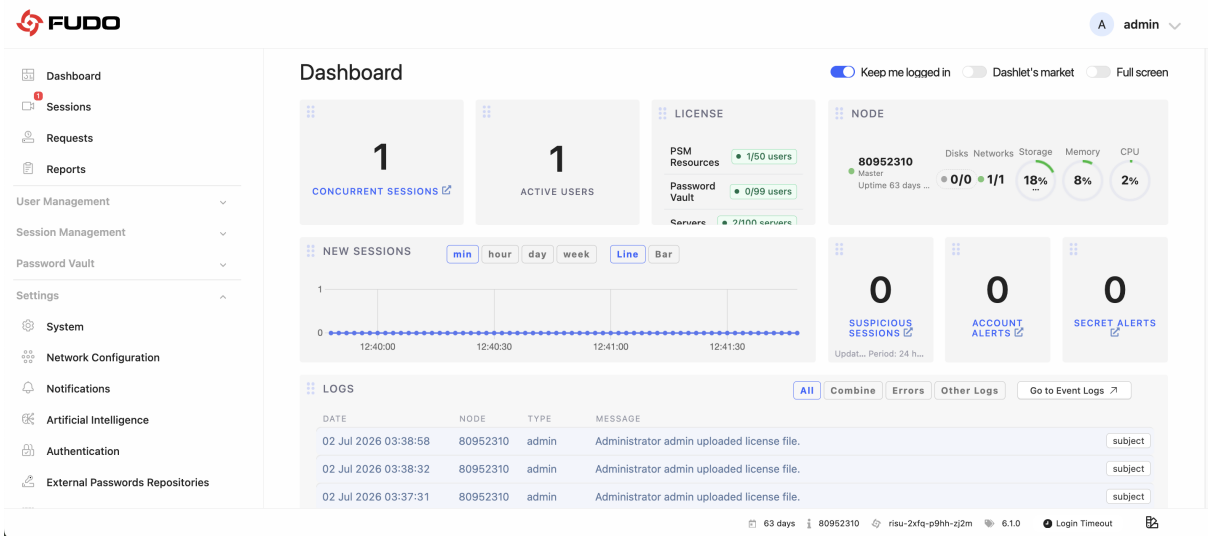
Fudo Enterprise encompasses two primary access interfaces:

- Admin Panel - for administrative tasks,
- User Access Gateway - for accessing resources.

Both portals provide secure and user-friendly interfaces for interacting with the Fudo Enterprise features.

4.4.1 Admin Panel

Admin Panel is a central management interface in Fudo Enterprise, used primarily by administrators. It provides a range of functionalities for system configuration, user management, security settings, and other administrative tasks. It's the control center for managing and configuring the Fudo Enterprise system.



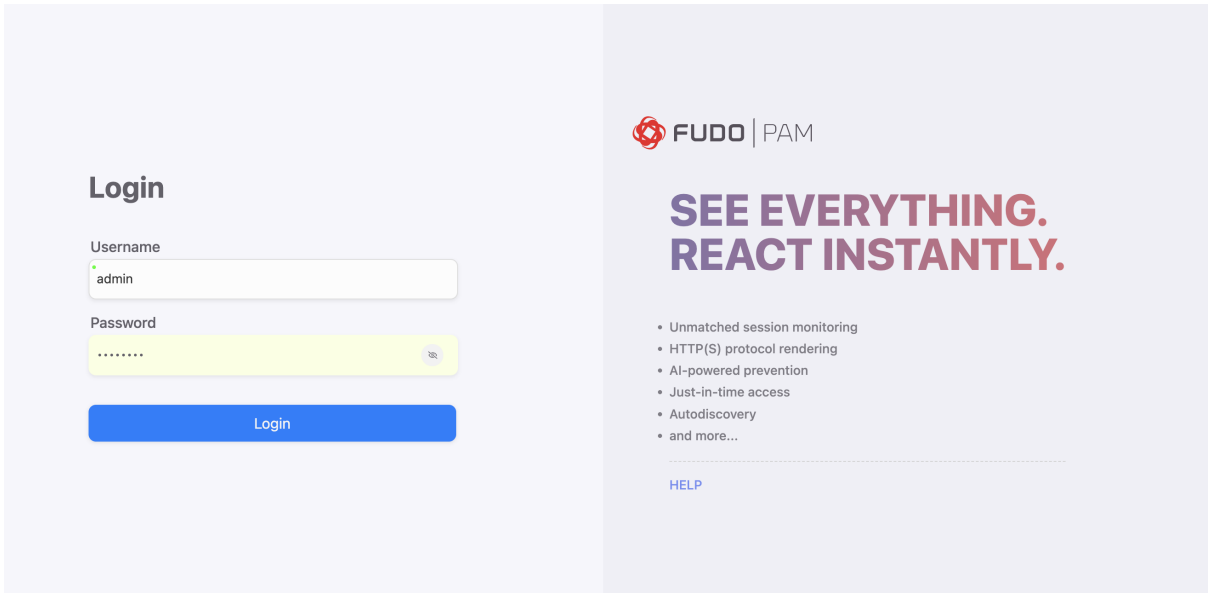
To access the Admin Panel follow below steps:

1. Open web browser and direct it to the IP address of the Admin Panel. It is usually an IP address configured during the *deployment procedure*.
2. Provide the administrators credentials and click the Login button.

Note

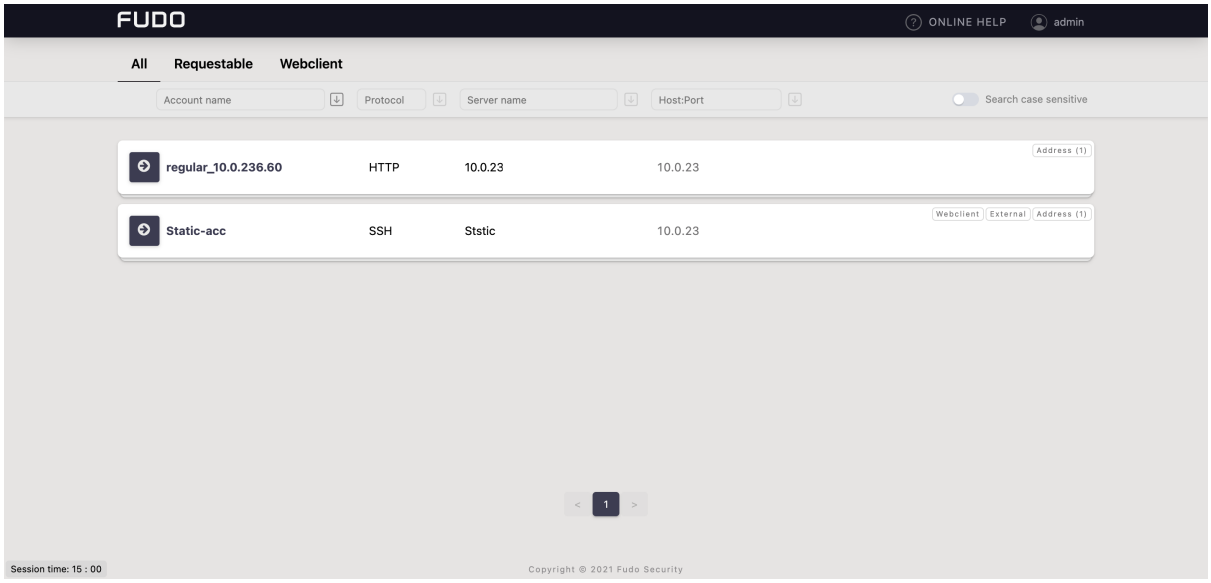
Default login credentials:

login: admin
password: proxycrypto



4.4.2 User Access Gateway

This component is designed for end users. It allows them to browse available resources and initiate connections with monitored servers using a selected listener. The User Access Gateway facilitates user access to resources in a secure and controlled manner.

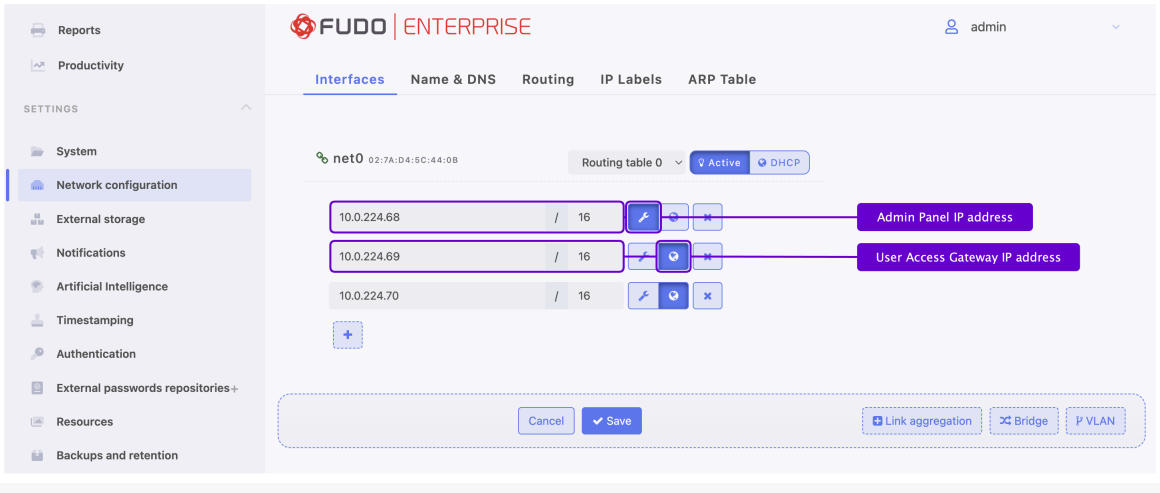


To log in to the User Access Gateway follow below steps:

1. Open web browser and direct it to the IP address of the User Access Gateway.

Note

You can obtain User Access Gateway IP address from your system administrator or by accessing the *Settings* > *Network configuration* menu in the Admin Panel. To learn more please refer to the *Network Interfaces Configuration* section.



4.4.3 Supported Web Browsers

Google Chrome, Mozilla Firefox and Microsoft Edge are supported on Microsoft Windows, Ubuntu, and macOS.

Related topics:

- *System overview*
- *Supported Protocols*
- *Quick start*

CHAPTER 5

Quick Start

5.1 SSH

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor SSH access to a remote server. In this scenario, the user connects to the remote server over the *SSH* protocol and logs in to the Fudo Enterprise using an individual login and password combination (`john_smith`/`john`). When establishing the connection with the remote server, Fudo Enterprise substitutes the login and the password with the previously defined values: `root`/`password` (authentication modes are described in the *User authentication modes* section).

5.1.1 Prerequisites

Description below assumes that the system has been already initiated. The initiation procedure is described in the *System initiation* topic.

5.1.2 Configuration

Adding a server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Session Management* > *Servers*.
2. Click + *Add server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`ssh_server`
Description	✗
Blocked	✗
Protocol	`SSH`
Legacy crypto	✗
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.150.151`
Mask	`32`
Port	`22`
Server verification	`None`

4. Click *Save* or *Save and close*.

Adding a user

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management* > *Users*.
2. Click + *Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked

Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`ssh_listener`
Blocked	✗
Protocol	`SSH`
Legacy crypto	✗
Case insensitivity	✗
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.152`
Port	`1022`
External address	✗
External port	✗

4. Generate or upload proxy server's private key.

Note

For security reasons the form displays server's public key derived from the generated or uploaded private key.

5. Click *Save*.

Adding an account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`SSH-account`
Blocked	✗
Type	`regular`
Session recording	`all`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`ssh_server`
Credentials	
Domain	✗
Login	`root`
Replace secret with	`with password`
Password	`password`
Repeat password	`password`
Secret change policy	`Static, without restrictions`

4. Generate or upload proxy server's private key.

Note

For security reasons the form displays server's public key derived from the generated or uploaded private key.

5. Click *Save*.

Defining a safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

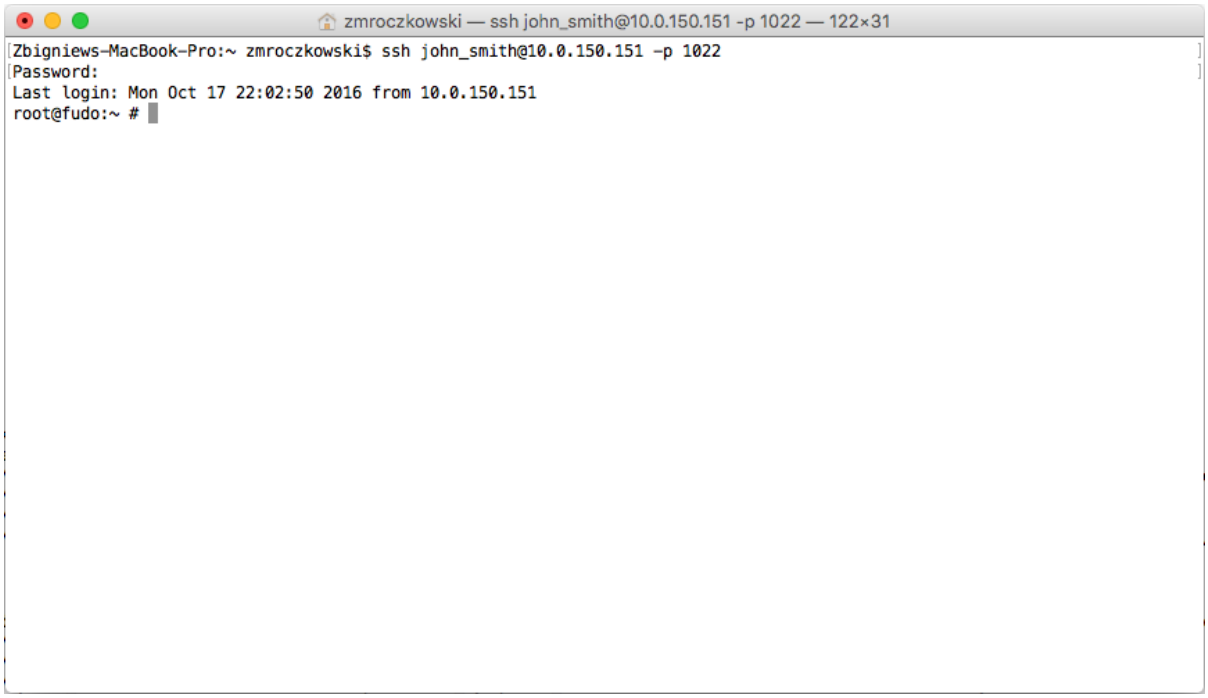
Parameter	Value
General	
Name	`ssh_safe`
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✓
VNC	✗

4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `SSH-account` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `ssh_listener` object and click +.
14. Click *OK*.
15. Click *Save*.

5.1.3 Establishing Connection

At this point `john_smith` can connect to the target host over the SSH protocol.

Example:



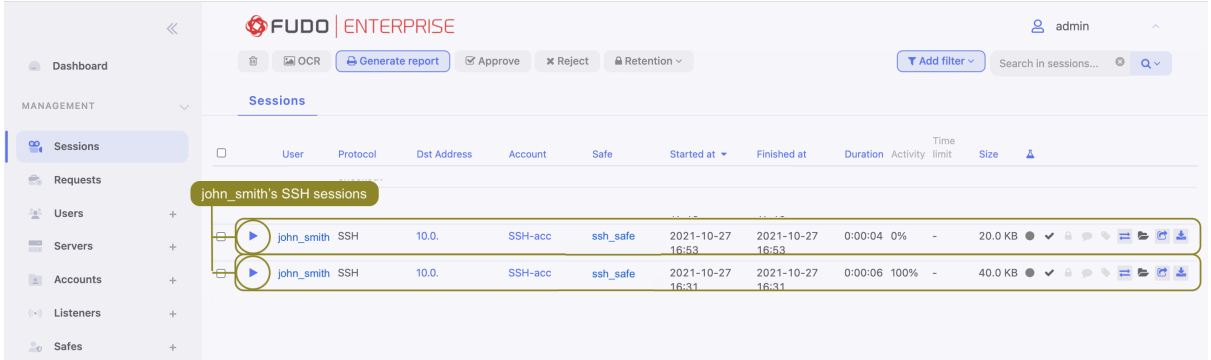
Note

Note that the *fingerprint* displayed when connecting to the target host for the first time is the same as was generated during server configuration.

After accepting the connection, user will be asked for the password. After successful authentication Fudo Enterprise starts recording user's activities.

5.1.4 Viewing User Session

1. Open a web browser and go to the `10.0.150.151` web address.
2. Enter the login and password to login to the Fudo Enterprise administration panel.
3. Select *Sessions*.
4. Find the session and click the playback icon.



Related topics:

- *PuTTY*
- *Requirements*
- *Data model*
- *Quick start - RDP connection configuration*
- *Quick start - HTTP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - Telnet connection configuration*

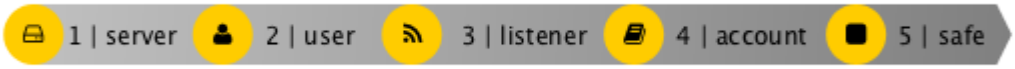
5.2 SSH in Bastion Mode

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor SSH access in bastion mode. In this scenario, the user connects to the remote server over the *SSH* protocol and logs in to the Fudo Enterprise using an individual login and password combination (`john_smith`/`john`). The user specifies user name along with account login on the target server and target server address in the login string (`john_smith#root#192.168.0.110`) and connects to it over default SSH port number. Upon establishing connection, login credentials are substituted with the previously defined values: `root`/`password` (authentication modes are described in the *User authentication modes* section).

5.2.1 Prerequisites

Description below assumes that the system has been already initiated. The initiation procedure is described in the *System initiation* topic.

5.2.2 Configuration



Adding a Server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Session Management* > *Servers*.
2. Click *+ Add server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`ssh_server`
Description	✗
Blocked	✗
Protocol	`SSH`
Legacy crypto	✗
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`192.168.0.100`
Mask	`32`
Port	`22`
Server verification	`None`

4. In the *Server verification* section select *Server public key* and provide respective public key data or click *Get public key*.
5. Click *Save* or *Save and close*.

Adding a User

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management* > *Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`

Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a Listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`ssh_listener`
Blocked	✗
Protocol	`SSH`
Legacy crypto	✗
Case insensitivity	✗
Permissions	
Granted users	✗
Connection	
Mode	`bastion`
Local address	`10.0.150.151`
Port	`22`
External address	✗
External port	✗

4. Generate or upload proxy server's private key.

Note

For security reasons the form displays server's public key derived from the generated or uploaded private key.

5. Click *Save*.

Adding an Account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`admin_ssh_server`
Blocked	✗
Account type	`regular`
Session recording	`all`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`ssh_server`
Credentials	
Domain	✗
Login	`root`
Replace secret with	`with password`
Password	`password`
Repeat password	`password`
Secret change policy	`Static, without restrictions`

4. Generate or upload proxy server's private key.

> **Note**
>
> For security reasons the form displays server's public key derived from the generated or uploaded private key.

5. Click *Save*.

Defining a Safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

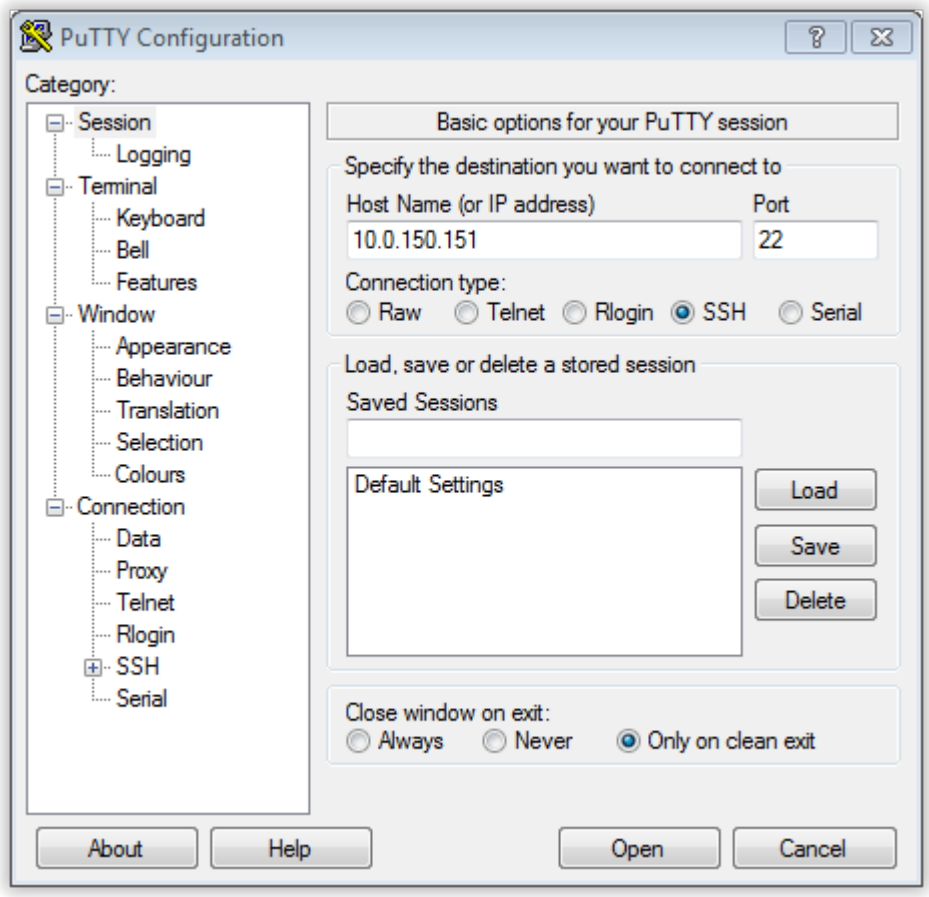
Parameter	Value
General	
Name	`ssh_safe`
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✓
VNC	✗

4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *john_smith* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_ssh_server` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `ssh_listener` object and click +.
14. Click *OK*.
15. Click *Save*.

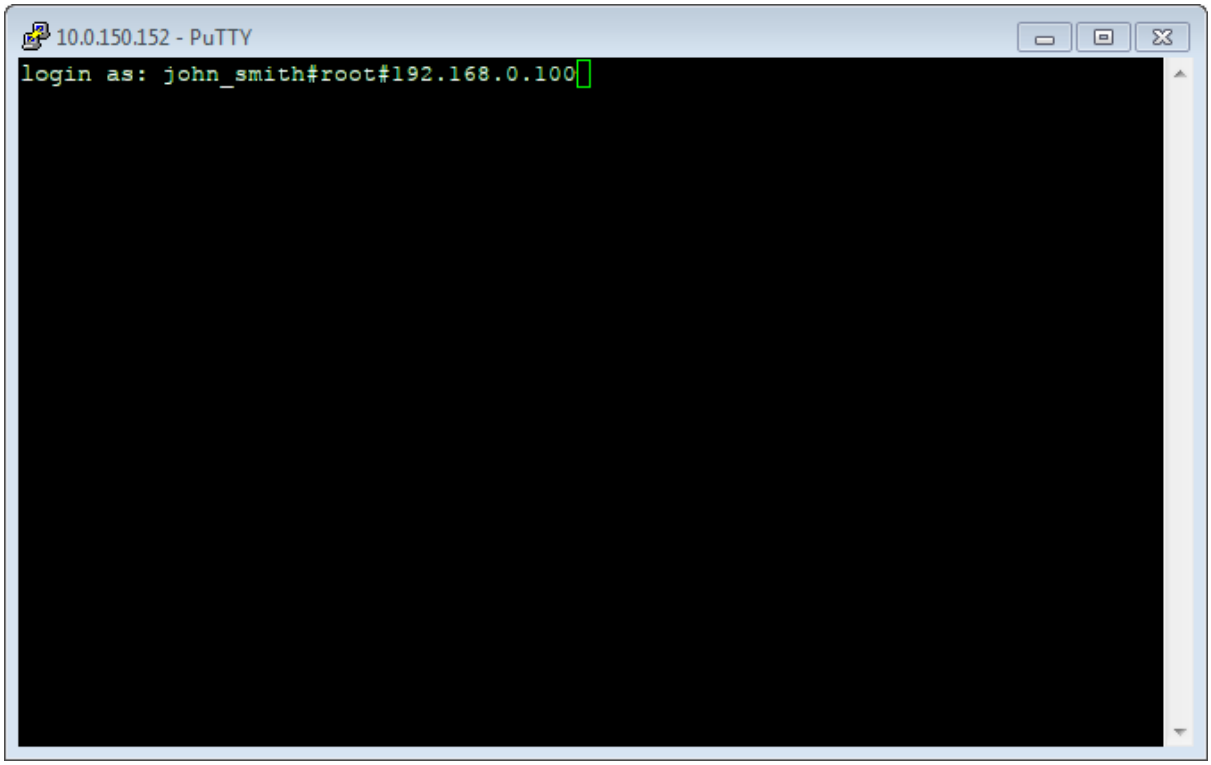
5.2.3 Establishing Connection

PuTTY - SSH client for Microsoft Windows

1. Download and launch PuTTY.
2. In the *Host Name (or IP address)* field, enter `10.0.150.151`.
3. Select the `SSH` connection type and leave the default port number unchanged.



4. Click *Open*.
5. Enter user name along with account login on the target server and target server address.



6. Enter password.

Command line interface

Launch terminal and run ssh command using following format:

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

Example:

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

5.2.4 Viewing User Session

1. Open a web browser and enter the Fudo Enterprise administrator panel IP address.
2. Enter the login and password to login to the Fudo Enterprise administration panel.
3. Select *Sessions*.
4. Find *John Smith's* session and click the playback icon.

Related Topics:

- *Requirements*
- *Data model*
- *Quick start - RDP connection configuration*
- *Quick start - HTTP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - Telnet connection configuration*

5.3 SSH in Bastion Mode with Jump Host Option

Fudo Enterprise allows for establishing a connection to a server using the *Jump Host* option.

This scenario assumes that when the user connects to a server acting as a *Jump Host* (192.168.10.90) via the *SSH* protocol, it automatically connects to the target server. The user must specify the following in the login string:

- Username,
- Account login on the *Jump Host,*
- Address of the *Jump Host,*
- Account login on the target server,
- Address of the target server.

5.3.1 Prerequisites

Description below assumes that the system has been already initiated. The initiation procedure is described in the *System initiation* topic.

5.3.2 Configuration

Adding a Jump Host Server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

In the following configuration, provide the details of the server acting as the *Jump Host.*

1. Select *Session Management* > *Servers.*
2. Click *+ Add server.*
3. Provide essential configuration parameters:

Parameter	Value
Name	`ssh_server`
Description	✗
Blocked	✗
Protocol	`SSH`
Legacy cipher	✗
Bind address	`Any`
Destination	
IPv4	`192.168.10.90`
Port	`22`

4. In the *Server verification* section select *Server public key* and provide respective public key data or click *Get public key.*
5. Click *Save* or *Save and close.*

Adding a User

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management* > *Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a Listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click *+ Add listener*.
3. Provide essential configuration parameters:

Parameter	Value
Name	`ssh_listener`
Blocked	✗
Protocol	`SSH`
Legacy cipher	✗
Case insensitive	✗
Permissions	
Authorized users	✗
Connection mode	`Bastion`
Local address	`10.0.150.151`
Port	22
External address	✗
External port	✗

4. Click the icon to generate an SSH key or upload the server's private key.

> **Note**
>
> For security reasons, the form will display the public key corresponding to the uploaded or generated private key.

5. Click *Save*.

> **Note**
>
> Make sure that administrative access (Admin Panel) is not enabled in the network settings for the specified IP address.

Adding an Account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.
2. Click *+ Add account*.
3. Provide essential configuration parameters:

Parameter	Value
Name	`admin_ssh_server`
Blocked	✗
Type	`REGULAR`
Session recording	`noraw`
Notes	✗
Permissions	
Granted users	✗
Target	
Server	`ssh_server`
Credentials	
Domain	✗
Login	`root`
Replace secret	`password`
Password	`password`
Data retention	
Override global retention settings	✗

5. Click *Save and Exit.*

Adding a Safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

1. Select *Management* > *Safes.*
2. Click *+ Add safe.*
3. Provide essential configuration parameters:

Parameter	Value
Name	`ssh_safe`
Blocked	✗
General	
Login reason	✗
Session timeout	✗
Session inactivity timeout	✗
Functionality	
RDP	✗
SSH	✓
VNC	✗

4. Go to the *USERS* tab.
5. Click *Manage users*.
6. Find and select the user *john_ smith*.
7. Click *Save*.
8. Go to the *ACCOUNTS* tab.
9. Click *Manage accounts*.
10. Find and select the account `admin_ssh_server`.
11. Click *Save*.
12. Click ✎ in the *Listeners* column.
13. Find and select the object `ssh_listener`.
14. Click *Save*.
15. Click *Save and Exit*.

5.3.3 Establishing a Connection

To establish a connection, use the following login string format in the terminal. The example below demonstrates logging in as *root* to the server 192.168.0.110 via the *Jump Host* server at 192.168.10.90.

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

Example:

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

Related Topics:

- *Requirements*
- *Data model*
- *Quick start - RDP connection configuration*
- *Quick start - HTTP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - Telnet connection configuration*

5.4 RDP

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor RDP access to a remote server. In this scenario, the user connects to the remote server over the *RDP* protocol and logs in to the Fudo Enterprise using an individual login and password combination (`john_smith`/`john`). When establishing the connection with the remote server, Fudo Enterprise substitutes the login with specified in *Account* and the password with the password managed by a secret changer (authentication modes are described in the *User authentication modes* section).

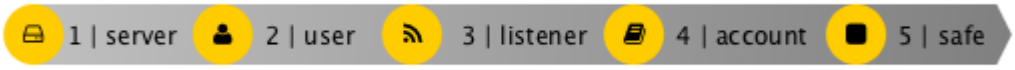
Note

Fudo Enterprise supports **multi-monitor sessions** for the RDP protocol, allowing monitoring and logging of graphical sessions across more than one display.

5.4.1 Prerequisites

Description below assumes that the system has been already initiated. The initiation procedure is described in the *System initiation* topic.

5.4.2 Configuration



Adding a server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Session Management* > *Servers*.
2. Click *+ Add server*.
3. Provide essential configuration parameters:

Parameter	Value
Name	`rdp_server`
Description	✗
Blocked	✗
Protocol	`RDP`
TLS enabled	✓
NLA enabled	✗
Legacy crypto	✗
Inform about existing connection	✗
Bind address	`10.0.150.151`
Permissions	
Granted users	✗
Destination	
Address	`10.0.35.54`
Mask	`32`
Port	`3389`
Server verification	`None`

4. Click *Save* or *Save and close*.

Adding a user

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management* > *Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked

Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`rdp_listener`
Blocked	✗
Protocol	`RDP`
Security	`Standard RDP Security`
Announcement	✗
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.151`
Port	`3389`
External address	✗
External port	✗

4. Generate or upload proxy server's private key.

Note

For security reasons the form displays server's public key derived from the generated or uploaded private key.

5. Click *Save*.

Adding an account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`admin_rdp_server`
Blocked	✗
Type	`regular`
Session recording	`all`
OCR sessions	✓
OCR Language	`English`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`rdp_server`
Credentials	
Domain	✗
Login	`administrator`
Replace secret with	`with password`
Password	`password`
Repeat password	`password`
Secret change policy	`Static, without restrictions`

4. Click *Save*.

Defining a safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

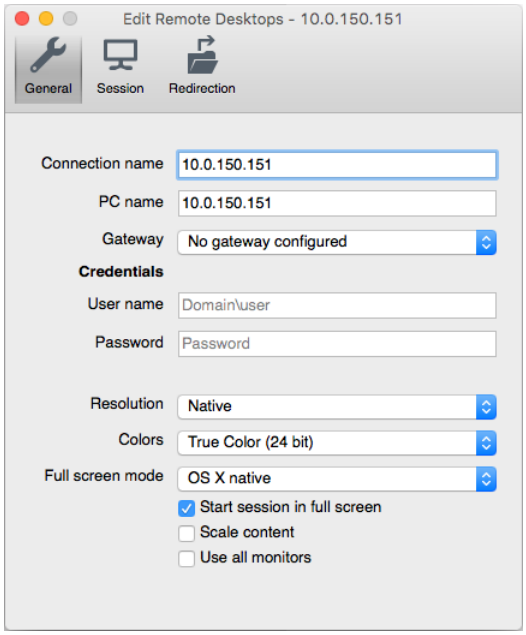
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`rdp_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Requires approval	✗
Policies	✗
Note access	`No access`
Users	`john_smith`
Protocol functionality	
RDP	✓
SSH	✗
VNC	✗

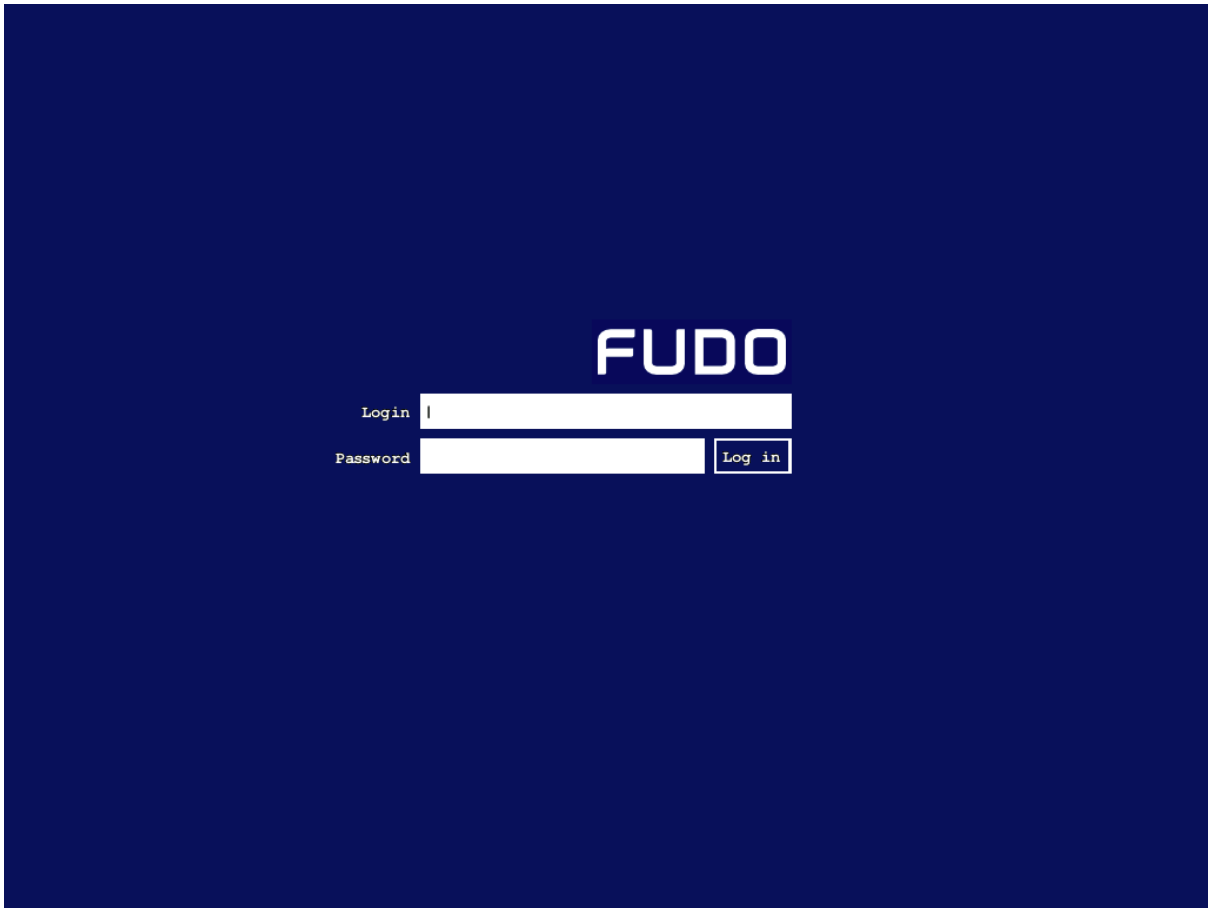
4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_rdp_server` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `rdp_listener` object and click +.
14. Click *OK*.
15. Click *Save*.

5.4.3 Establishing an RDP Connection with a Remote Host

1. Launch RDP client of your choice.
2. Enter destination host IP address and RDP service port number.

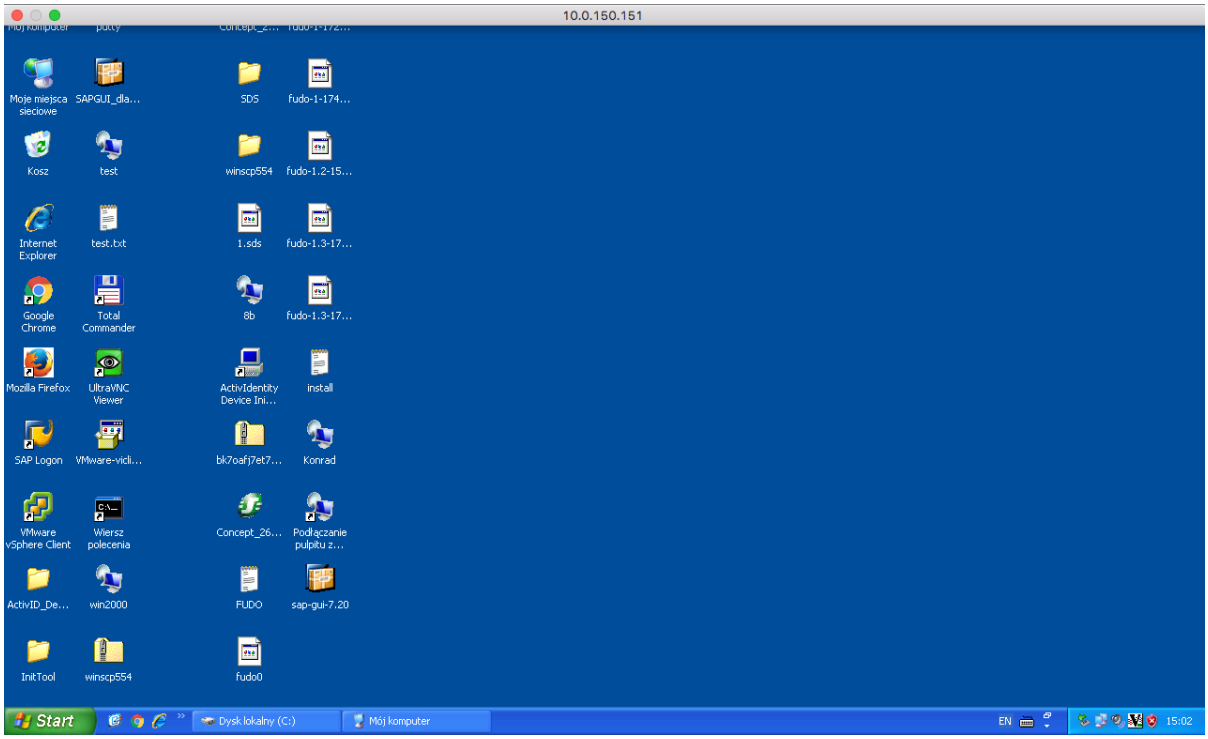


3. Enter user login and password and press the [Enter] keyboard key.



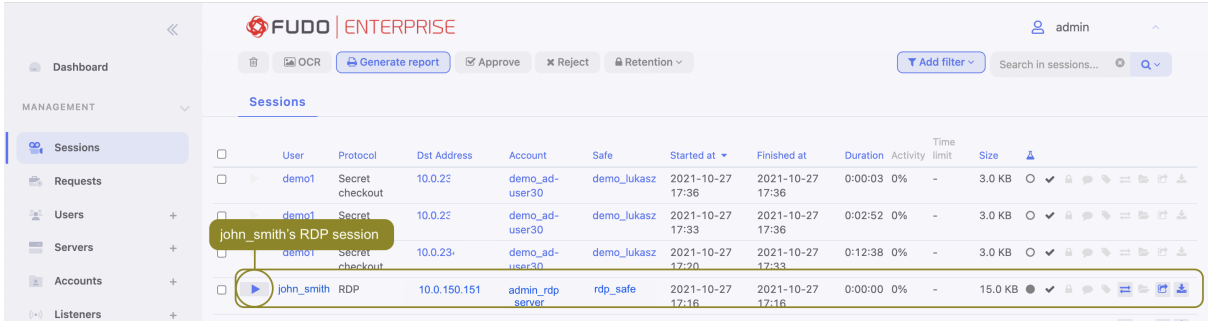
Note

Fudo Enterprise enables using custom login, no access and session termination screens for RDP and VNC connections. For more information on user defined images for graphical remote sessions, refer to the *Resources* topic.



5.4.4 Viewing User Session

1. Open a web browser and go to the `10.0.150.151` web address.
2. Enter the login and password to login to the Fudo Enterprise administration panel.
3. Select *Sessions*.
4. Find *John Smith's* session and click the playback icon.



Related topics:

- *Microsoft Remote Desktop*
- *Requirements*
- *Data model*
- *Quick start - RDP connection configuration*
- *Quick start - HTTP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - Telnet connection configuration*

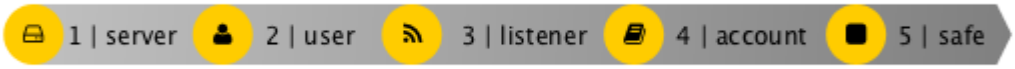
5.5 RDP in Bastion Mode

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor RDP access to a remote server. In this scenario, the user connects to the remote server in bastion mode by specifying the user name along with account login on the target server and target server address in the login string. Bastion mode enables facilitating privileged accounts monitoring while preserving default protocols port numbers.

5.5.1 Prerequisites

Description below assumes that the system has been already initiated. The initiation procedure is described in the *System initiation* topic.

5.5.2 Configuration



Adding a server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Session Management* > *Servers*.
2. Click *+ Add server*.
3. Provide essential configuration parameters:

Parameter	Value
Name	`rdp_server`
Description	✗
Blocked	✗
Protocol	`RDP`
TLS enabled	✓
NLA enabled	✗
Legacy crypto	✗
Inform about existing connection	✗
Bind address	`10.0.150.151`
Permissions	
Granted users	✗
Destination	
Address	`10.0.35.54`
Mask	`32`
Port	`3389`
Server verification	`None`

4. Click *Save* or *Save and close*.

Adding a user

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management* > *Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked

Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`rdp_listener_bastion`
Blocked	✗
Protocol	`RDP`
Security	`Standard RDP Security`
Announcement	✗
Permissions	
Granted users	✗
Connection	
Mode	`bastion`
Local address	`10.0.150.151`
Port	`3389`
External address	✗
External port	✗

4. Generate or upload proxy server's private key.

Note

For security reasons the form displays server's public key derived from the generated or uploaded private key.

5. Click *Save*.

Adding an account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`admin_rdp_server`
Blocked	✗
Type	`regular`
Session recording	`all`
OCR sessions	✓
OCR Language	`English`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`rdp_server`
Credentials	
Domain	✗
Login	`admin`
Replace secret with	`with password`
Password	`password`
Repeat password	`password`
Secret change policy	`Static, without restrictions`

4. Click *Save*.

Defining a safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`rdp_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✓
SSH	✗
VNC	✗

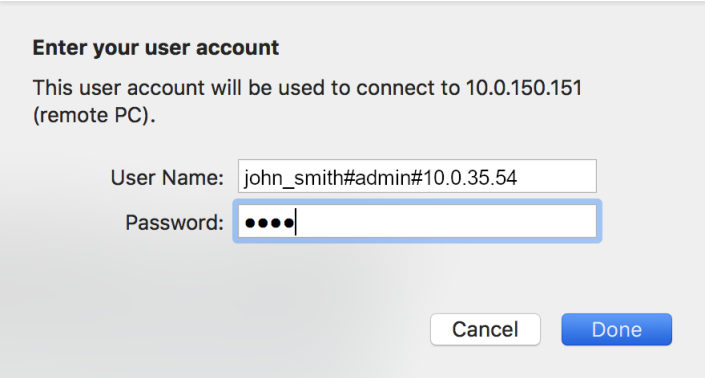
4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *john_smith* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_rdp_server` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `rdp_listener_bastion` object and click +.
14. Click *OK*.
15. Click *Save*.

5.5.3 Establishing an RDP Connection with a Remote Host

1. Launch RDP client of your choice.
2. Enter destination host IP address and RDP service port number.
3. Enter user name along with account login on the target server (server login) and target server address (`john_smith#admin#10.0.35.54`) and provide password.

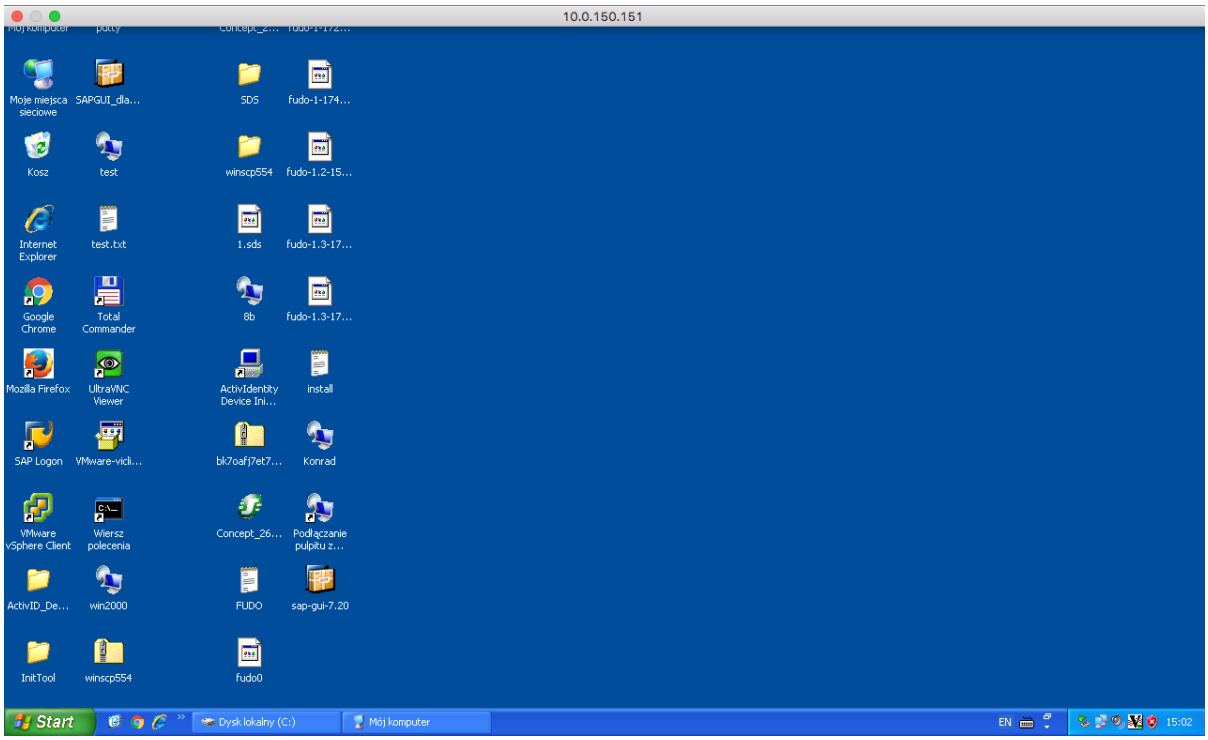
Note

When connecting using the forward account, where the user name and server login are identical, the server login field may be omitted (e.g., `john_smith##10.0.35.54`).



Note

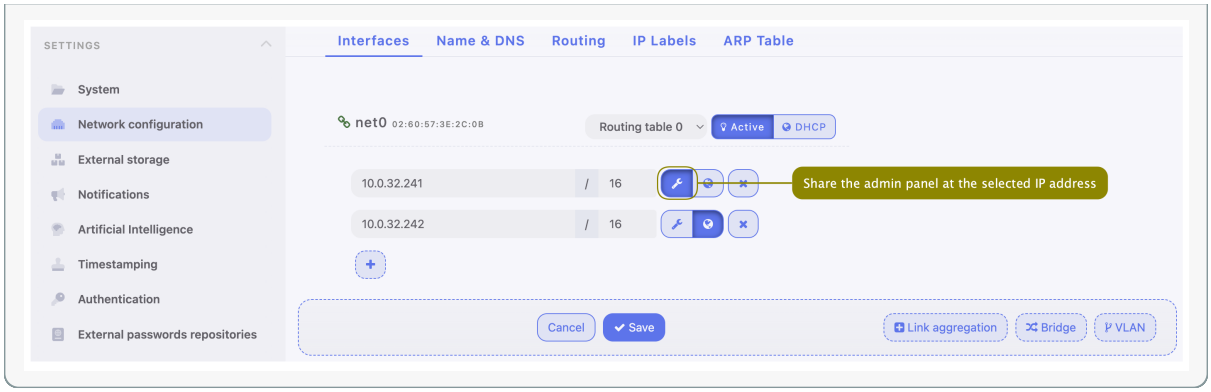
- In case you do not specify login credentials, Fudo Enterprise will display the internal login screen to enter the account name along with the username and password.
- When connecting using the forward account, where the Username and Server login are identical, the Server login field may be omitted on the login screen.
- In case the specified account is not found, Fudo Enterprise will try to match the name with a server object. If a matching server is not found, system tries to match the string to a host's DNS name.
- Fudo Enterprise enables using a custom logo on the login screen for RDP and VNC connections. For more information refer to the *Resources* topic.



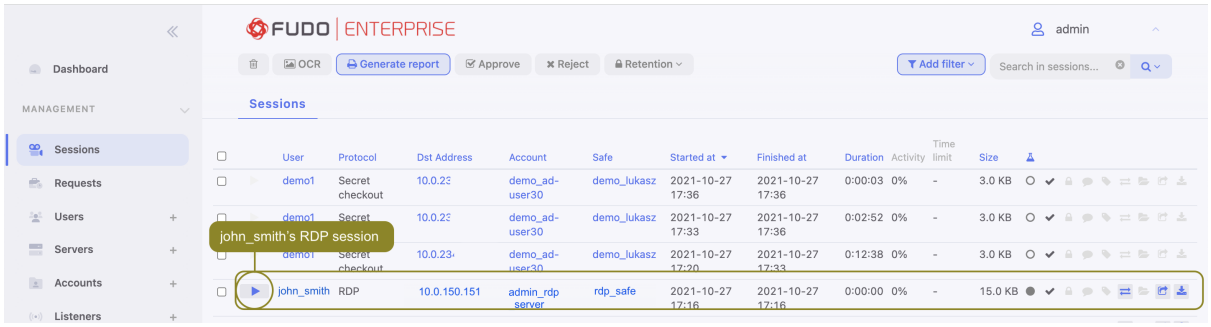
5.5.4 Viewing User Session

1. Open a web browser and enter the Fudo Enterprise administrator panel IP address.

> **Note**
>
> Make sure that the entered IP address has the control panel sharing option enabled in the *Network configuration* settings.



2. Enter the login and password to login to the Fudo Enterprise administration panel.
3. Select *Sessions*.
4. Find *John Smith's* session and click the playback icon.



Related topics:

- *Microsoft Remote Desktop*
- *Requirements*
- *Data model*
- *Quick start - RDP connection configuration*
- *Quick start - HTTP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - Telnet connection configuration*

5.6 Telnet

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor Telnet connections to a remote server. In this scenario, the user connects to the remote server using Telnet client and logs in using individual login and password. Fudo Enterprise authenticates the user against the information stored in the local database, establishes connection with the remote server and starts recording.

Note

Telnet connections do not support login credentials forwarding and login credentials substitution. When connecting to target host over telnet protocol, users are asked to provide their

login credentials twice. First time to authenticate against Fudo Enterprise and then again, to connect to the target host.

5.6.1 Prerequisites

Description below assumes that the system has been already initiated. For more information on the initiation procedure refer to the *System Initiation* topic.

5.6.2 Configuration

Adding a server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Session Management* > *Servers*.
2. Click *+ Add server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`telnet_server`
Description	✗
Blocked	✗
Protocol	`Telnet 5250`
TLS enabled	✗
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.35.137`
Mask	32
Port	23

4. Click *Save* or *Save and close*.

Adding a user

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management* > *Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`telnet_listener`
Blocked	✗
Protocol	`Telnet`
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.151`
Port	`23`
Use TLS	✗

4. Click *Save*.

Adding an account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`admin_telnet_server`
Blocked	✗
Type	`forward`
Session recording	`all`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`telnet_server`
Credentials	
Replace secret with	`with password`
Password	✗
Repeat password	✗
Forward domain	✗

4. Click *Save*.

Defining a safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`telnet_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	✗
Protocol functionality	
RDP	✗
SSH	✗
VNC	✗
Permissions	
Granted users	✗

4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click [+].
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_telnet_server` object and click [+].
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `telnet_listener` object and click [+].
14. Click *OK*.
15. Click *Save*.

5.6.3 Establishing a Telnet Connection with the Remote Host

1. Launch telnet client of your choice.
2. Connect to the remote host:

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

3. Provide user authentication information defined on Fudo Enterprise:

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

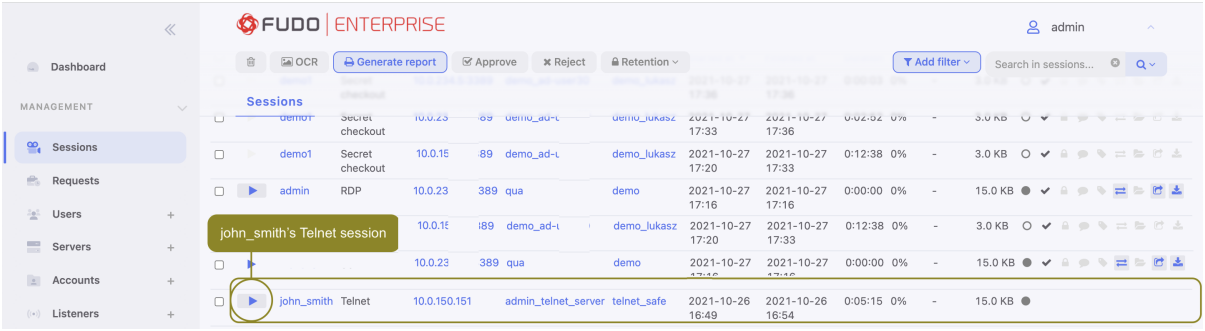
4. Provide user authentication information defined on the target host:

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

> **Note**
>
> Telnet connections do not support user credentials substitution.

5.6.4 Viewing User's Session

1. Open a web browser and go to the `10.0.150.151` web address.
2. Enter the login and the password to log in to the Fudo Enterprise administration panel.
3. Select *Sessions*.
4. Find *John Smith's* session and click the playback icon.



Related topics:

- *Quick start - SSH connection configuration*
- *Quick start - HTTP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - RDP connection configuration*
- *Requirements*
- *Data model*
- *Resources*

5.7 Telnet 5250

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor Telnet 5250 connections to a remote server. In this scenario, the user connects to the remote server using Telnet client and logs in using individual login and password. Fudo Enterprise authenticates

the user against the information stored in the local database, establishes connection with the remote server and starts recording.

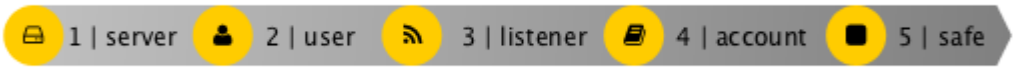
Note

Telnet connections do not support login credentials forwarding and login credentials substitution. When connecting to target host over telnet protocol, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise and then again, to connect to the target host.

5.7.1 Prerequisites

Description below assumes that the system has been already initiated. For more information on the initiation procedure refer to the *System Initiation* topic.

5.7.2 Configuration



Adding a server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Session Management* > *Servers*.
2. Click + *Add* and select *Static server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`telnet_server`
Description	✗
Blocked	✗
Protocol	`Telnet 5250`
TLS enabled	✗
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.35.137`
Mask	`32`
Port	`23`

4. Click *Save* or *Save and close*.

Adding a user

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management* > *Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`telnet_listener`
Blocked	✗
Protocol	`Telnet 5250`
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.151`
Port	`23`
Use TLS	✗
Legacy crypto	✗
Server certificate	✗

4. Click *Save*.

Adding an account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.

2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`admin_telnet_server`
Blocked	✗
Type	`forward`
Session recording	`all`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`telnet_server`
Credentials	
Replace secret with	`with password`
Password	✗
Repeat password	✗
Forward domain	✗

4. Click *Save*.

Defining a safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`telnet_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	✗
Protocol functionality	
RDP	✗
SSH	✗
VNC	✗
Permissions	
Granted users	✗

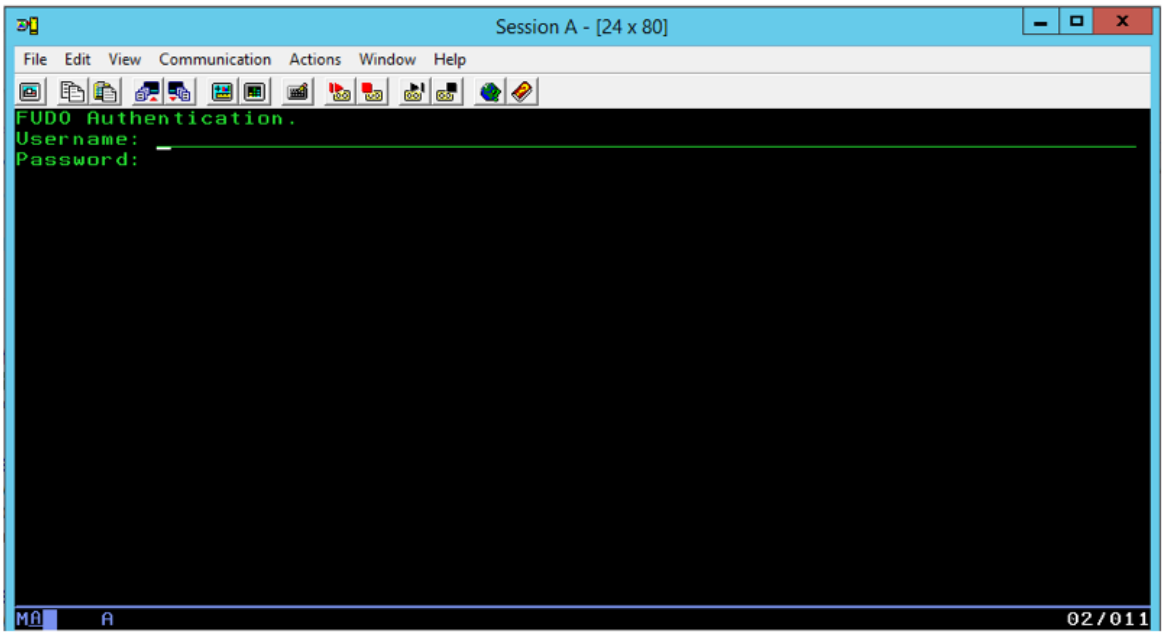
4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click [+].
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_telnet_server` object and click [+].
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `telnet_listener` object and click [+].
14. Click *OK*.
15. Click *Save*.

5.7.3 Establishing a Telnet Connection with the Remote Host

1. Launch telnet client of your choice.
2. Connect to the remote host:

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

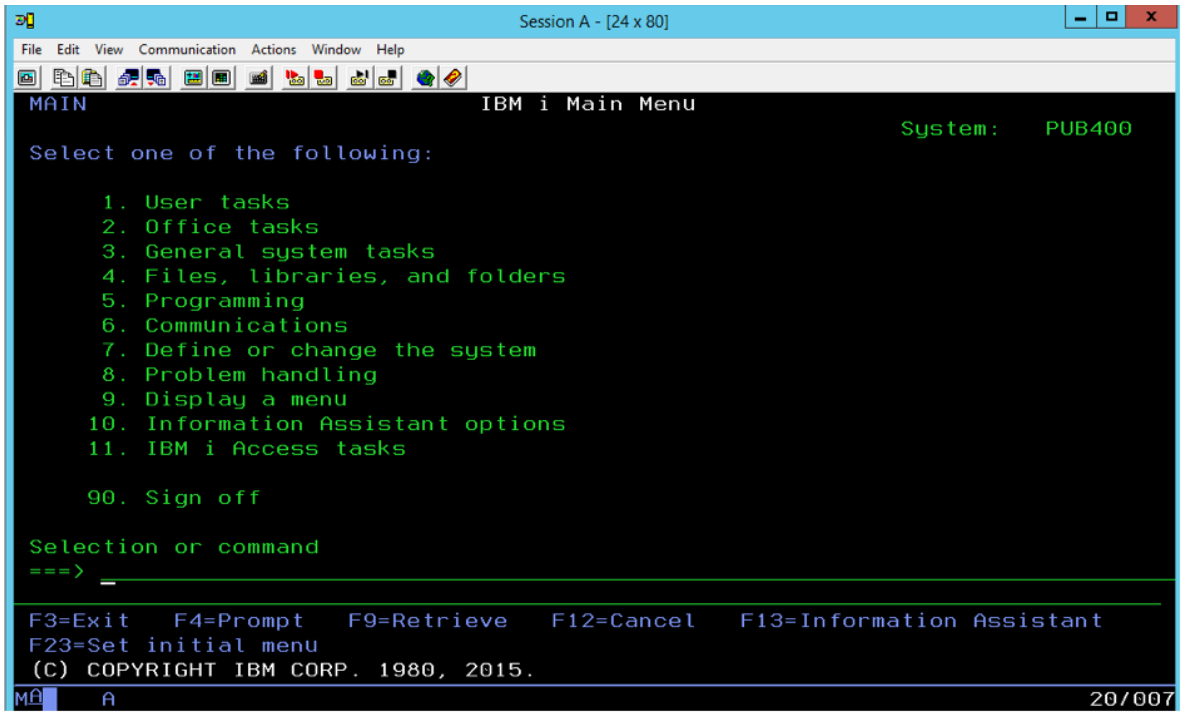
3. Provide user authentication information defined on Fudo Enterprise:



4. Provide user authentication information defined on the target host:

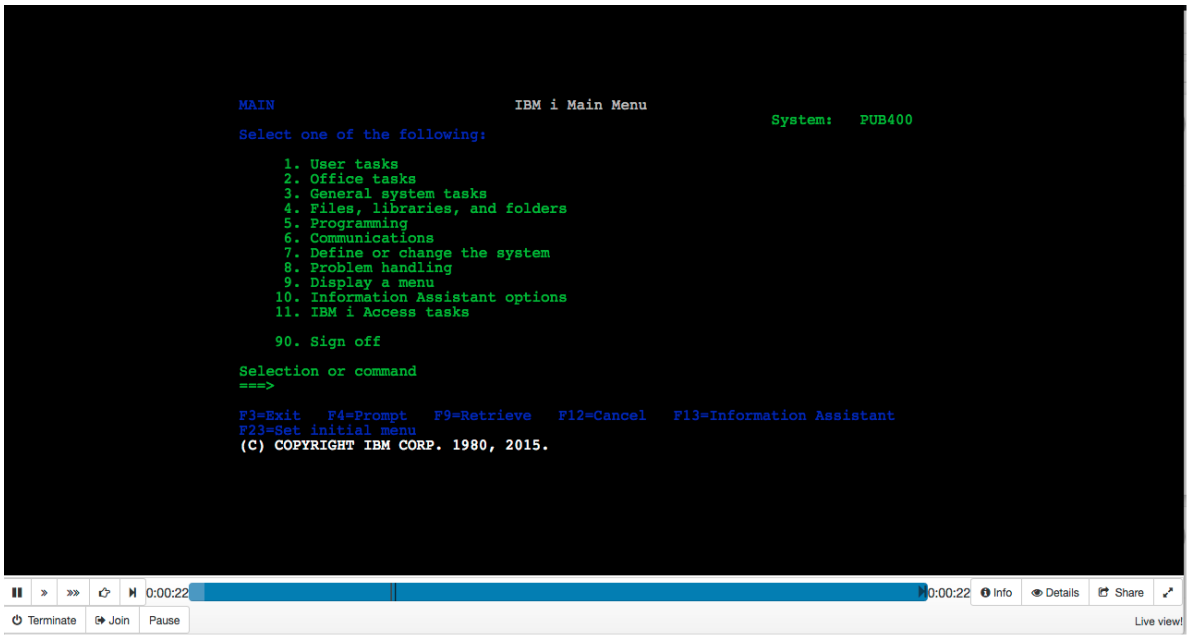
   FreeBSD/amd64 (fbsd83-cerb.whl) (pts/0) login: password:

> **Note**
>
> Telnet connections do not support user credentials substitution.



5.7.4 Viewing User's Session

1. Open a web browser and go to the `10.0.150.151` web address.
2. Enter the login and the password to log in to the Fudo Enterprise administration panel.
3. Select *Sessions*.
4. Find *John Smith's* session and click the playback icon.



Related topics:

- *Quick start - SSH connection configuration*
- *Quick start - HTTP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - RDP connection configuration*
- *Requirements*
- *Data model*
- *Resources*

5.8 PostgreSQL

This guide demonstrates a basic Fudo Enterprise configuration for monitoring and controlling PostgreSQL database access through a secure proxy connection.

> **Note**
>
> PostgreSQL connections use **native client** support only. The connection command is available through the User Access Gateway portal after configuration.

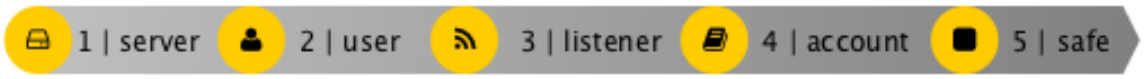
5.8.1 Prerequisites

Before starting this configuration:

- System must be initialized (see *System initiation*)
- PostgreSQL server must be accessible from Fudo Enterprise
- PostgreSQL client (`psql`) must be installed on your workstation

5.8.2 Architecture Overview

The following diagram illustrates the PostgreSQL connection flow:



Connection Flow:

1. User authenticates to User Access Gateway (https://10.31.134.220)
2. User receives connection command with One-Time Password (OTP)
3. Native `psql` client connects through Fudo Enterprise proxy
4. Fudo Enterprise authenticates and forwards connection to PostgreSQL server

5.8.3 Configuration Steps

Step 1: Create PostgreSQL Server

Define the target PostgreSQL server in Fudo Enterprise.

1. Navigate to *Session Management* > *Servers*
2. Click *+ Add server*
3. Configure the server with following settings:

General

Name: `PostgreSQL_Server`
Description: `Production PostgreSQL Database`
Blocked: ☐ Unchecked

Settings Tab: Protocol

Protocol: `PostgreSQL`
TLS enabled: ✓ Checked (recommended for security)
Legacy crypto: ☐ Unchecked
Use SSH tunnel: ☐ Unchecked

Settings Tab: Bind Address

Bind address: `Any`

Settings Tab: Destination

Type: `IPv4`
Address: `10.0.100.7`
Mask: `32`
Port: `5432`

Settings Tab: Server Verification

Method: `Server certificate` or `None`

4. Click *Save and Close*.

Step 2: Create User

Create a user who will access the PostgreSQL server.

1. Select *User Management* > *Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Step 3: Create Listener

Configure the proxy endpoint for PostgreSQL connections.

1. Navigate to *Session Management* > *Listeners*
2. Click *+ Add*
3. Configure the listener:

General Settings

Name: `PostgreSQL_Listener`
Protocol: `PostgreSQL`
Blocked: ☐ Unchecked

Connection Settings

Mode: `proxy`
Local address: `10.31.134.220`
Port: `5432`
TLS enabled: ✓ Checked (required for PostgreSQL)
Legacy crypto: ☐ Unchecked

Access Control

Granted users: Leave empty (configured via safe)

4. Click *Save and Close*.

Step 4: Create Account

Define database credentials for authentication.

1. Navigate to *Session Management* > *Accounts*
2. Click *+ Add*
3. Configure the account:

General

Name: `PostgreSQL_Account`
Session recording: `all`
Notes: `PostgreSQL admin account`

Settings Tab: Type

Account type: `REGULAR`

Settings Tab: Target

Server: `PostgreSQL_Server` (select from dropdown)

Settings Tab: Credentials

Replace secret with: `Password`
Secret: Your PostgreSQL password
Login: Your PostgreSQL login

Secret Changers Tab: General

Secret change policy: `Static, without restrictions`

4. Click *Save and Close*.

Step 5: Create Safe Configure access control and bind all components together.

1. Navigate to *Session Management* > *Safes*
2. Click *+ Add Safe*

3. Configure the safe:

General

Name: `PostgreSQL_Safe`
Blocked: ☐ Unchecked

General Tab: Connection

Login reason: ✓ Checked (optional, for audit trail)

General Tab: Access

OTP in Access Gateway: ✓ Checked
Web Client: ☐ Unchecked

4. Click *Save and Close*.
5. **Add users to the safe:**
   a. Select Users tab
   b. Click Manage Users
   c. Find and add your user (e.g., `John`)
   d. Click Save
6. **Add account to the safe:**
   a. Select Accounts tab
   b. Click Manage Accounts
   c. Find and add `PostgreSQL_Account`
   d. Click Save
7. **Assign listener to the account:**
   a. Click in the **Listeners** column for `PostgreSQL_Account`
   b. Find and add `PostgreSQL_Listener`
   c. Click Save
8. Click Save and Close

5.8.4 Establishing PostgreSQL Connection

Step 1: Access User Portal

Open your browser and navigate to the User Access Gateway address. Example:

```
https://10.31.134.220
```

Login with the credentials used while creating User:

Login: `john_smith`
Password: `john`

Step 2: Get Connection Command

1. Locate `PostgreSQL_Account` in the resources list
2. Click on the **Native client** dropdown arrow
3. You'll see:
   - **Fingerprint**: Server identification hash
   - **One Time Password**: Valid for 5 minutes
   - **Connection command**: Ready-to-use psql command

Step 3: Connect Using psql

Copy the connection command and replace `<database_name>` with your target database:

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

# Example: Connect to custom database
psql postgres://85156504qLOOtF4bWesSntHHvQoTIjED:empty@10.31.134.220:5432/myapp_
↪db
```

Note

Important Connection Details:

- The OTP (One-Time Password) expires after **5 minutes**
- Password field is always `empty` - authentication uses the OTP token
- You MUST specify the database name at the end of the connection string

Related topics:

- *Creating PostgreSQL Server*
- *Quick start - SSH connection*
- *Quick start - RDP connection*
- *Quick start - MySQL connection*
- *Password Vault configuration*

- *Data model*

5.9 MySQL

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor SQL queries to a remote MySQL database server.

In this scenario, the user connects to a MySQL database using individual login and password. When establishing the connection with the remote server, Fudo Enterprise substitutes the login and the password with the previously defined values: `root`/`password` (authorization modes are described in the *User authorization modes* section).

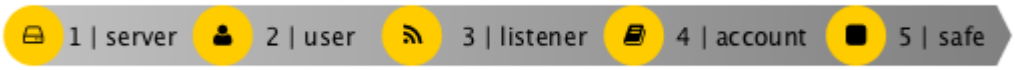
Warning

Note that the MySQL server `caching_sha2_password` plugin isn't supported by Fudo Enterprise. Supportable MySQL plugins by Fudo Enterprise are `mysql_native_password` and `mysql_old_password`. Server plugin should be set to `mysql_native_password` in `/etc/mysql/mysql.conf.d/mysqld.cnf` and a User object is created with `mysql_native_password` plugin.

5.9.1 Prerequisites

The following description assumes that the system has been already initiated. For more information on the initiation procedure refer to the *System initiation* topic.

5.9.2 Configuration



Adding a server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Session Management* > *Servers*.
2. Click *+ Add server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`mysql_server`
Description	✗
Blocked	✗
Protocol	`MySQL`
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.1.35`
Mask	`32`
Port	`3306`

4. Click *Save* or *Save and close*.

Adding a user

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management* > *Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`mysql_listener`
Blocked	✗
Protocol	`Mysql`
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.151`
Port	`3306`

4. Click *Save*.

Adding an account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`admin_mysql_server`
Blocked	✗
Type	`regular`
Session recording	`all`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`mysql_server`
Credentials	
Domain	✗
Login	`root`
Replace secret with	`with password`
Password	`password`
Repeat password	`password`
Secret change policy	`Static, without restrictions`

4. Click *Save*.

Defining a safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

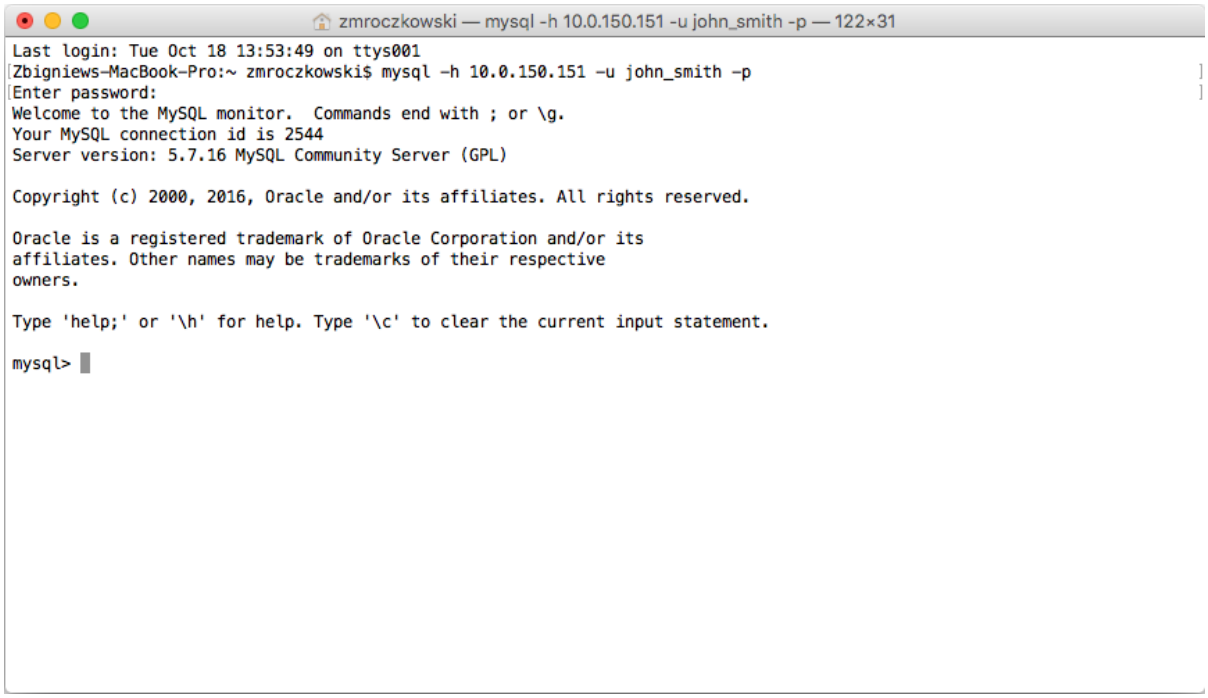
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`mysql_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✗
VNC	✗

4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add admin_ mysql_ server*.
10. Find the `twitter_admin` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `mysql_listener` object and click +.
14. Click *OK*.
15. Click *Save*.

5.9.3 Establishing Connection with a MySQL Database

1. Launch a command line interface client.
2. Enter `mysql -h 10.0.150.151 -u john_smith -p`, to connect to the database server.
3. Enter the user's password.



4. Continue browsing the database contents using SQL queries.

5.9.4 Viewing User Session

1. Open a web browser and go to the Fudo Enterprise administration page.
2. Enter user login and password to log in to Fudo Enterprise administration panel.
3. Select *Sessions*.
4. Find *John Smith's* session and click the playback icon.

Related topics:

- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*
- *Quick start - HTTP connection configuration*
- *Quick start - Telnet connection configuration*
- *Requirements*
- *Data model*

5.10 Oracle

This guide demonstrates a basic Fudo Enterprise configuration for monitoring and controlling Oracle database access through a secure proxy connection.

> **Note**
>
> Oracle connections use **native client** support only, and the client connects directly to the Fudo Enterprise listener. Unlike the other database protocols, Oracle is not available in the User Access Gateway portal, so there is no connection command and no One-Time Password to copy - users authenticate with their own database credentials.

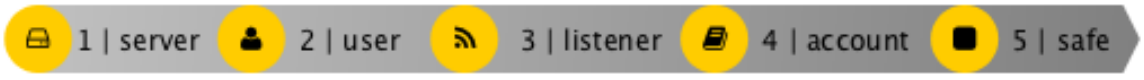
5.10.1 Prerequisites

Before starting this configuration:

- System must be initialized (see *System initiation*)
- Oracle server must be accessible from Fudo Enterprise
- Oracle SQL*Plus client must be installed on your workstation
- The database credentials of the user who will connect

5.10.2 Architecture Overview

The following diagram illustrates the Oracle connection flow:



Connection Flow:

1. SQL*Plus connects to the Fudo Enterprise listener address instead of the database
2. The user authenticates with their own Oracle user name and password
3. Fudo Enterprise records the session and forwards the credentials to the Oracle server
4. The Oracle server accepts or rejects the login

5.10.3 Configuration Steps

Step 1: Create Oracle Server

Define the target Oracle server in Fudo Enterprise.

1. Navigate to *Session Management* > *Servers*
2. Click *+ Add server*
3. In the *Protocol* section, press the `Show all` button to expand the list of supported protocols.
4. Configure the server with following settings:

General

Name: `Oracle_Server`
Description: `Production Oracle Database`
Blocked: ☐ Unchecked

Settings Tab: Protocol

Protocol: `Oracle`
TLS enabled: ☐ Unchecked for a database that does not accept TCPS connections
Legacy crypto: ☐ Unchecked
Use SSH tunnel: ☐ Unchecked

Settings Tab: Bind Address

Bind address: `Any`

Settings Tab: Destination

Type: `IPv4`
Address: `10.0.100.36`
Mask: `32`
Port: `1521`

Settings Tab: Server Verification

Method: `None` when TLS is not used

Warning

TLS enabled is selected by default. Leave it selected only if the database accepts TCPS connections and your users connect with SQL*Plus - other client applications do not support TLS with Fudo Enterprise.

5. Click *Save and Close*.

Step 2: Create User

Create a user who will access the Oracle server.

Warning

For Oracle, the Fudo Enterprise user name must be identical to the database user name. Fudo Enterprise identifies the user by the name that the client sends when it logs in to the database - the `scott` in `sqlplus scott/tiger@...` - because the Oracle protocol carries no separate field for a Fudo Enterprise user name.

A database user with the same name must therefore exist in the Oracle database - `john_smith` in the example below. If the names differ, the connection is not established.

1. Select *User Management* > *Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Step 3: Create Listener

Configure the proxy endpoint for Oracle connections.

1. Navigate to *Session Management* > *Listeners*
2. Click *+ Add*
3. In the *Protocol* section, press the `Show all` button and select `Oracle`.
4. Configure the listener:

General Settings

Name: `Oracle_Listener`
Protocol: `Oracle`
Blocked: ☐ Unchecked

Connection Settings

Mode: `proxy` (the only mode available for Oracle)
Local address: `10.31.134.220`
Port: `1521`
TLS enabled: ☐ Unchecked
Legacy crypto: ☐ Unchecked

Access Control

Granted users: Leave empty (configured via safe)

5. Click *Save and Close*.

Step 4: Create Account

Define how Fudo Enterprise reaches the database.

1. Navigate to *Session Management* > *Accounts*
2. Click *+ Add*
3. Configure the account:

General

Name: `Oracle_Account`
Session recording: `all`
Notes: `Oracle database account`

Settings Tab: Type

Account type: `FORWARD`

Settings Tab: Target

Server: `Oracle_Server` (select from dropdown)
Authenticate against server: ✓ Checked and greyed out - Fudo Enterprise sets it automatically

Warning

The default session recording mode is `noraw`, which cannot be used with Oracle - the account will not be saved. Change it to `all`, `raw` or `none` before saving. Timestamping requires `all` or `raw`.

Note

Accounts of the `REGULAR` type are not offered for Oracle servers, so the *Credentials* section stays empty. Users authenticate with their own database credentials and password substitution is not available.

4. Click *Save and Close*.

Step 5: Create Safe

Configure access control and bind all components together.

1. Navigate to *Session Management* > *Safes*
2. Click + *Add Safe*
3. Configure the safe:

General

Name: `Oracle_Safe`
Blocked: ☐ Unchecked

General Tab: Connection

Login reason: ✓ Checked (optional, for audit trail)

4. Click *Save and Close*.
5. **Add users to the safe:**
   a. Select Users tab
   b. Click Manage Users
   c. Find and add your user (e.g., `John`)
   d. Click Save
6. **Add account to the safe:**
   a. Select Accounts tab
   b. Click Manage Accounts
   c. Find and add `Oracle_Account`
   d. Click Save
7. **Assign listener to the account:**
   a. Click in the **Listeners** column for `Oracle_Account`
   b. Find and add `Oracle_Listener`
   c. Click Save
8. Click Save and Close

5.10.4 Establishing Oracle Connection

Point SQL*Plus at the Fudo Enterprise listener instead of the database, and log in with your own Oracle user name and password. Use the listener *Local address* and *Port* defined in Step 3, and the service name of the target database:

```
# Template format
sqlplus <database_user>/<password>@<listener_address>:<listener_port>/<service_
↪name>

# Example
sqlplus john_smith/<password>@10.31.134.220:1521/FREEPDB1
```

Note

Important Connection Details:

- Authentication is performed by the Oracle server. Wrong credentials are rejected with `ORA-01017`.
- Oracle native encryption (Advanced Security Option) is refused. Configure the client so that it does not negotiate it.
- Encrypted connections are supported with SQL*Plus only. Other client applications can be used without TLS.

The session is recorded and available in Sessions, where it can be filtered by the `Oracle` protocol.

Related topics:

- *Creating an Oracle Server*
- *Setting up the Oracle Listener*
- *Quick start - PostgreSQL connection*
- *Quick start - SSH connection*
- *Data model*

5.11 MS SQL

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor MS SQL connections to a remote MS SQL database server.

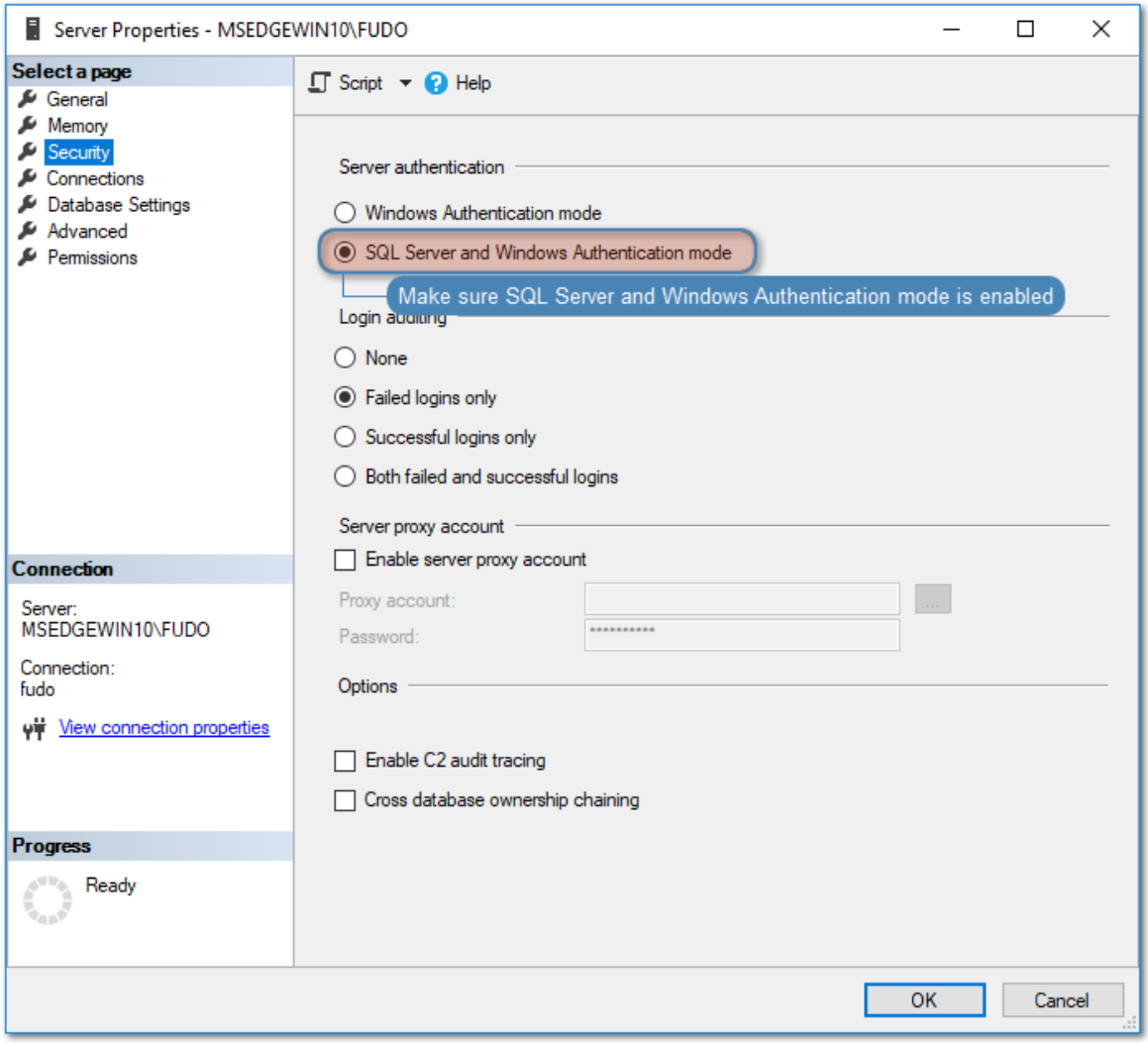
In this scenario, the user connects to a MS SQL database using individual login and password using *SQL Server Management Studio*. When establishing the connection with the remote server, Fudo Enterprise substitutes the login and the password with the previously defined values: `fudo`/`password` (authorization modes are described in the *User authorization modes* section).

5.11.1 Prerequisites

The following description assumes that the system has been already initiated. For more information on the initiation procedure refer to the *System initiation* topic.

Note

Make sure that the SQL Server has the *SQL Server and Windows Authentication* mode enabled.



5.11.2 Configuration

Adding a server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Session Management* > *Servers*.

2. Click *+ Add server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`mssql_server`
Description	✗
Blocked	✗
Protocol	`MS SQL (TDS)`
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.150.154`
Mask	`32`
Port	`1433`

4. Click *Save* or *Save and close*.

Adding a user

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management > Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`MSSQL_proxy`
Blocked	✗
Protocol	`MS SQL (TDS)`
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.150`
Port	`1433`

4. Click *Save*.

Adding an account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`admin_mssql_server`
Blocked	✗
Type	`regular`
Session recording	`all`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`mssql_server`
Credentials	
Domain	✗
Login	`fudo`
Replace secret with	`with password`
Password	`password`
Repeat password	`password`
Secret change policy	`Static, without restrictions`

4. Click *Save*.

Defining a safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

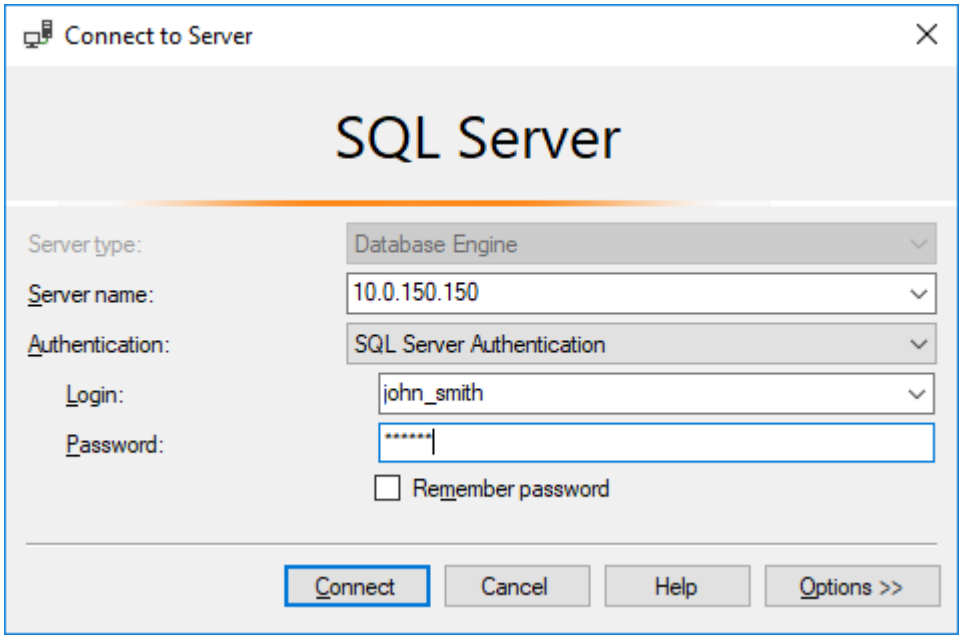
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

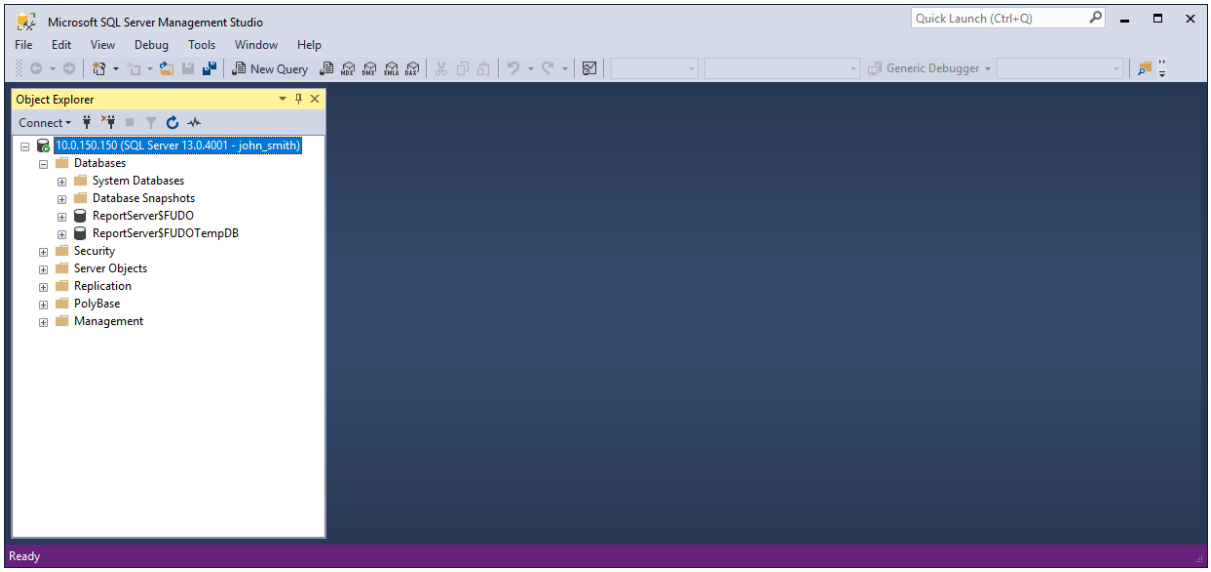
Parameter	Value
General	
Name	`mssql_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✗
VNC	✗

4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_mssql_server` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `MSSQL_proxy` object and click +.
14. Click *OK*.
15. Click *Save*.

5.11.3 Establishing Connection with a MS SQL Database

1. Start *SQL Server Management Studio*.
2. Enter previously configured proxy address (10.0.150.150).
3. From the *Authentication* drop-down list, select *SQL Server Authentication*.
4. Enter user login and password.
5. Click *Connect*.





5.11.4 Viewing User Session

1. Open a web browser and go to the Fudo Enterprise administration page.
2. Enter user login and password to log in to Fudo Enterprise administration panel.
3. Select *Sessions*.
4. Find *John Smith's* session and click ▶.

Note

Due to the fact that MS SQL Studio may create multiple connections for sending internal queries, the sessions, connected via the TDS layer protocol using MS SQL Studio are getting aggregated by Fudo Enterprise.

Fudo Enterprise follows an algorithm that verifies if there is an already connected session on a current node. If the algorithm identifies that the main connection objects (`listener`,

`account`, `server address (server)`, `user`, and `safe`) of the new session are correlating with already existing session, both sessions are aggregated into one.

If the main connection objects of the new session are not correlating with any of already existing sessions, a new session is created.

This makes multiple queries to be grouped within one session. Every query has a unique tag that allows filtering important connections with users' queries in the Fudo Enterprise player.

Related topics:

- *SQL Server Management Studio*
- *Quick start - MySQL connection configuration*
- *Requirements*
- *Data model*

5.12 HTTP

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor access to Twitter over HTTPS. In this scenario, the user uses its individual login credentials to log in to a monitored Twitter account. The connection will timeout after 15 minutes (900 seconds) and the user will have to login again to continue browsing the server's contents.

Warning

HTTP rendering is a CPU intensive process and may have negative impact on system's performance. A physical appliance is recommended for monitoring rendered HTTP connections with the following limitations regarding the maximum number of concurrent rendered HTTP sessions.

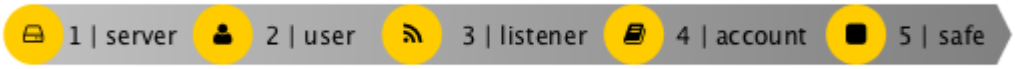
Model	Maximum recommended number of concurrent HTTP sessions*
F100x	2
F300x	5
F500x	10

* The actual value depends on the Fudo Enterprise instance configuration.

5.12.1 Prerequisites

The following description assumes that the system has been already initiated. For more information on the initiation procedure refer to the *System initiation* topic.

5.12.2 Configuration



Adding a server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Session Management* > *Servers*.
2. Click *+ Add server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`twitter`
Description	✗
Blocked	✗
Protocol	`HTTP`
TLS enabled	✓
Legacy crypto	✗
HTTP host	✗
HTTP timeout	`900`
HTTP Authentication	`Twitter`
Bind address	`10.0.236.70`
Permissions	
Granted users	✗
Destination	
Address	`twitter.com`
Port	`443`
Server verification	`None`

4. Click *Save* or *Save and close*.

Adding a user

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.)

enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management* > *Users*.
2. Click + *Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click + *Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`twitter_listener`
Blocked	✗
Protocol	`HTTP`
Render sessions	✓
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.151`
Port	`997`
Use TLS	✓
Legacy crypto	✓
TLS certificate	Click ⚙ to generate a certificate.

4. Click *Save*.

Adding an account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`twitter_admin`
Blocked	✗
Type	`regular`
Session recording	`all`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data	`default settings`
Permissions	
Granted users	✗
Server	
Server	`twitter`
Credentials	
Domain	✗
Login	*YourTwitterAccountUsername*
Replace secret with	`with password`
Password	`******`
Repeat password	`******`
Secret change policy	`Static, without restrictions`

4. Click *Save*.

Defining a safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`twitter_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Users	`john_smith`
Protocol functionality	
RDP	✗
SSH	✗
VNC	✗

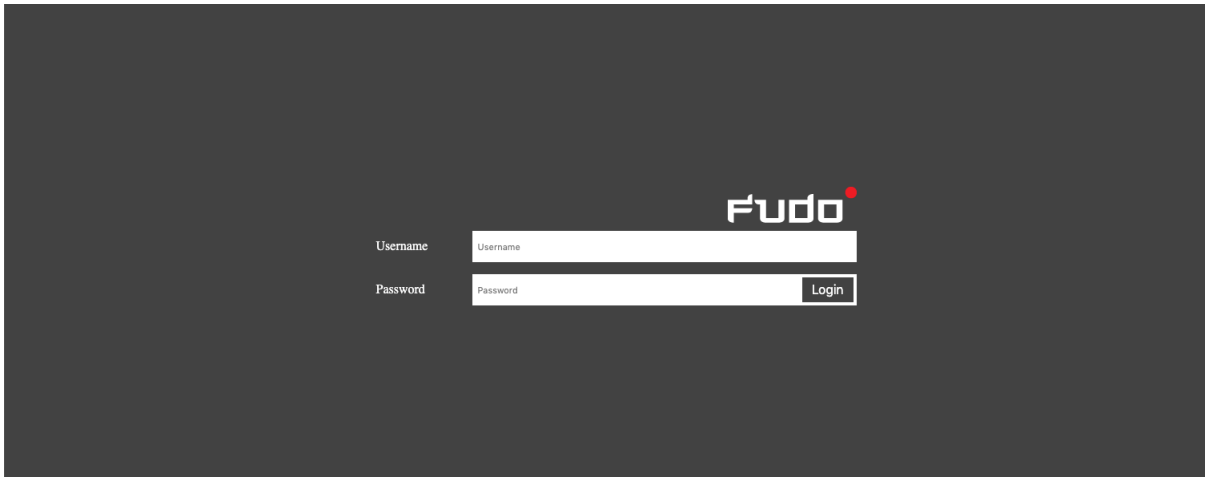
4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `twitter_admin` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `twitter_listener` object and click +.
14. Click *OK*.
15. Click *Save*.

5.12.3 Connecting to Remote Resource

1. Launch a web browser.
2. Go to the `10.0.236.70:997` web address.
3. Enter user login and password and press the [Enter] key or click the *Login* button.

Note

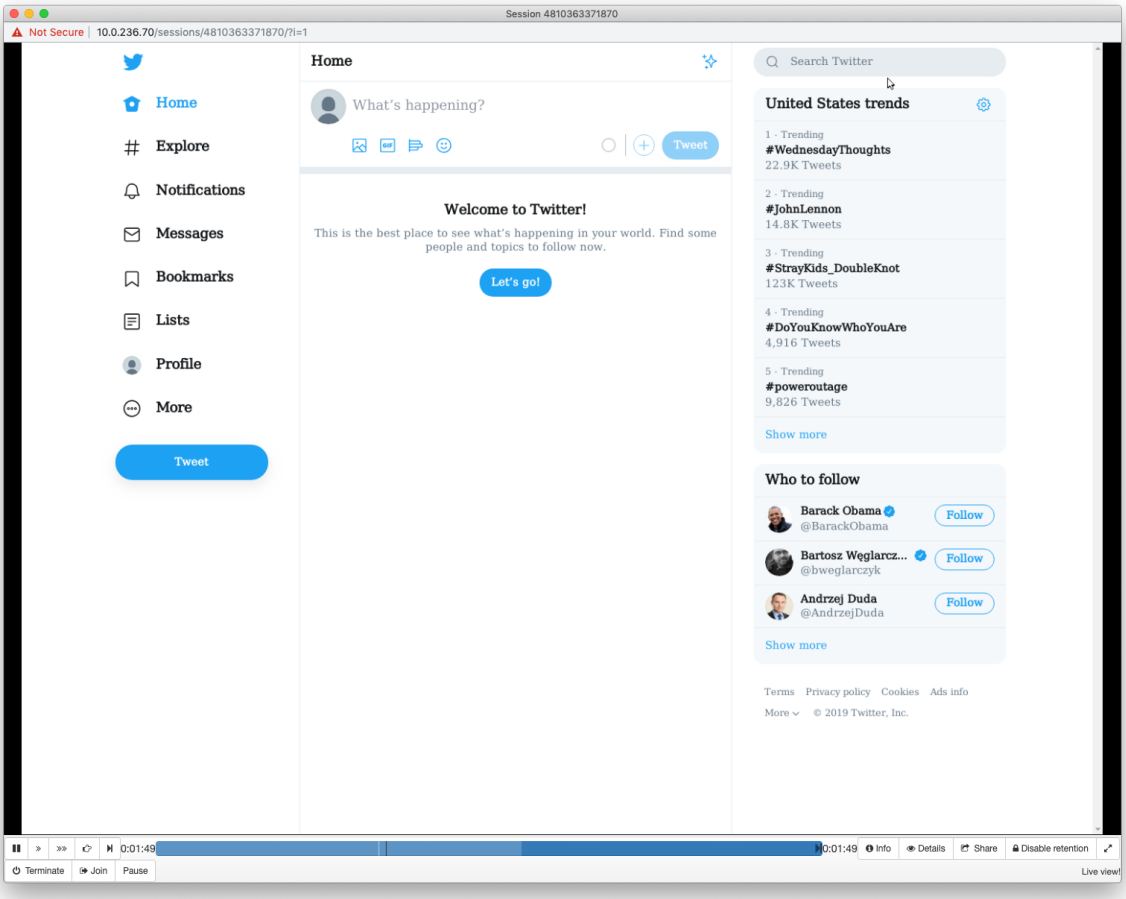
In case you are authenticating using two factors, input your static password along with the dynamic factor (token value) in the password field as a single string of characters.



4. Continue browsing the website.

5.12.4 Viewing User Session

1. Open a web browser and go to the Fudo Enterprise administration page.
2. Enter user login and password to log in to Fudo Enterprise administration panel.
3. Select *Sessions*.
4. Find John's session and click the playback icon.



Related topics:

- *Requirements*
- *HTTP protocol*
- *Data model*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - Telnet connection configuration*

5.13 VNC

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor VNC access to a remote server. In this scenario, the user connects to the remote server over the *VNC* protocol and logs in to the Fudo Enterprise using an individual login and password combination (`john_smith`/`john`). When establishing the connection with the remote server, Fudo Enterprise substitutes the password with the previously defined value: `password` (authentication modes are described in the *User authentication modes* section).

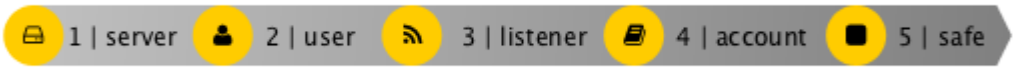
Note

Due to specifics of VNC protocol, which authenticates the user using password only, the substitution login string entered in account properties is ignored when establishing a VNC connection.

5.13.1 Prerequisites

Description below assumes that the system has been already initiated. The initiation procedure is described in the *System initiation* topic.

5.13.2 Configuration



Adding a server

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Session Management* > *Servers*.

2. Click *+ Add server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`vnc_server`
Description	✗
Blocked	✗
Protocol	`VNC`
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.40.230`
Mask	`32`
Port	`5900`

4. Click *Save* or *Save and close*.

Adding a user

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

1. Select *User Management* > *Users*.
2. Click *+ Add User*.
3. Provide essential user information:

General

Name: `john_smith`
Blocked: ☐ Unchecked
Account validity: `Indefinite`

Settings Tab

Authentication failures: ☐ Unchecked
Enforce password complexity: ☐ Unchecked
Add authentication method: `Static password`
Password `john`

User Data Tab

Full name: `John Smith`
Email: `john@smith.com`

Roles Tab

Assign Role: e.g., `admin`

4. Click *Save and Close*.

Adding a listener

Listener determines server connection mode (proxy, bastion) as well as its specifics.

1. Select *Management* > *Listeners*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`vnc_listener`
Blocked	✗
Protocol	`VNC`
Announcement	✗
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.151`
Port	`5900`
External address	✗
External port	✗

4. Click *Save*.

Adding an account

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

1. Select *Management* > *Accounts*.

2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`admin_vnc_server`
Account type	`regular`
Session recording	`all`
OCR sessions	✔
OCR language	`English`
Notes	✘
Data retention	
Override global retention settings	✘
Delete session data after	`61` days
Permissions	
Granted users	✘
Server	
Server	`vnc_server`
Credentials	
Domain	✘
Login	✘
Replace secret with	`password`
Password	`root`
Repeat password	`root`
Secret change policy	`Static, without restrictions`

4. Click *Save*.

Defining a safe

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

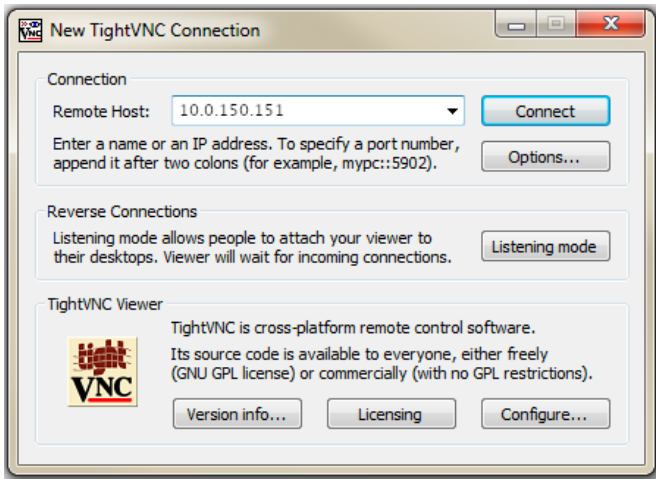
1. Select *Management > Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`vnc_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	✗
Protocol functionality	
RDP	✗
SSH	✗
VNC	✓

4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click [+].
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_vnc_server` object and click [+].
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `vnc_listener` object and click [+].
14. Click *OK*.
15. Click *Save*.

5.13.3 Establishing Connection

1. Launch *TightVNC Viewer*, enter `10.0.150.151` in the server address field and press the enter key.



2. Enter username and password and press the enter key.

5.13.4 Viewing User Session

1. Open a web browser and go to the `10.0.150.151` web address.
2. Enter the login and password to login to the Fudo Enterprise administration panel.
3. Select *Sessions*.
4. Find *John Smith's* session and click the playback icon.

Related topics:

- *TightVNC Viewer*
- *Requirements*
- *Data model*
- *Quick start - RDP connection configuration*
- *Quick start - HTTP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - Telnet connection configuration*

CHAPTER 6

Sessions

Fudo Enterprise stores all recorded servers access sessions, allowing to playback, review, delete and export to the supported video formats.

Sessions management page allows filtering stored user sessions, accessing current users connections and downloading stored sessions. It also provides status information on each session and enables access to session sharing options.

Note

Contents of the session list depend on the logged in user's access rights. Being able to access a given session requires having management privileges to: server, account, user and safe objects that were used in the given connection.

Note

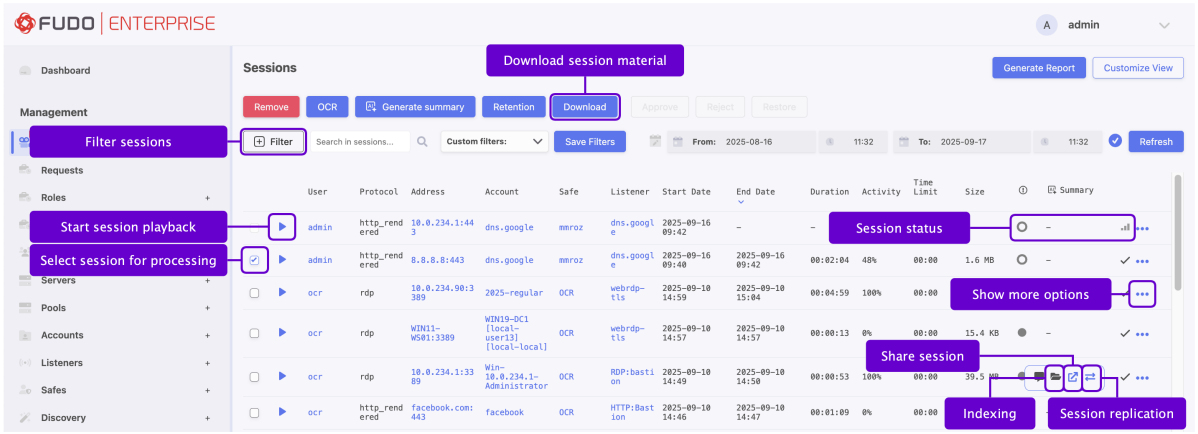
The visibility of the **Activity** column — along with filtering and sorting by this value — depends on the availability of the **Productivity** module. The column may not be visible if the module is unavailable due to local legal regulations or customer requirements. Refer to the *Productivity* section for more information.

Icon	Description
▶	Start session playback (*applicable to sessions with the entire traffic recording option selected in connection properties*).
	Icon indicating that session has been timestamped.
	Purpose why the user has connected to the server.
	Session has been commented.
	Session has been processed for full-text search purposes.
	Session replication status.
	Access session sharing management options.
	User activity monitor (*applicable to live sessions*).
	Approve pending request.
	Decline pending request.
	Pending request awaiting authorization.
+	Element aggregating connections established within the same session.
	Session excluded from the retention mechanism.
	Behavioral analysis status. *This is an evaluation version of the AI component.* ○ - session under analysis, initial result - no threat. ○ - session under analysis, initial result - medium threat level. ○ - session under analysis, initial result - high threat level. ○ - session awaiting analysis or being initially processed. ○ - session not analyzed due to missing a trained model. ● - session processed - no risk. ● - session processed - medium threat level. ● - session processed - high threat level. ● - session processed - no result.

To open sessions management page, select *Sessions*.

Note

Fudo Enterprise stores compressed session material which may result in differences between the displayed and the actual session size.



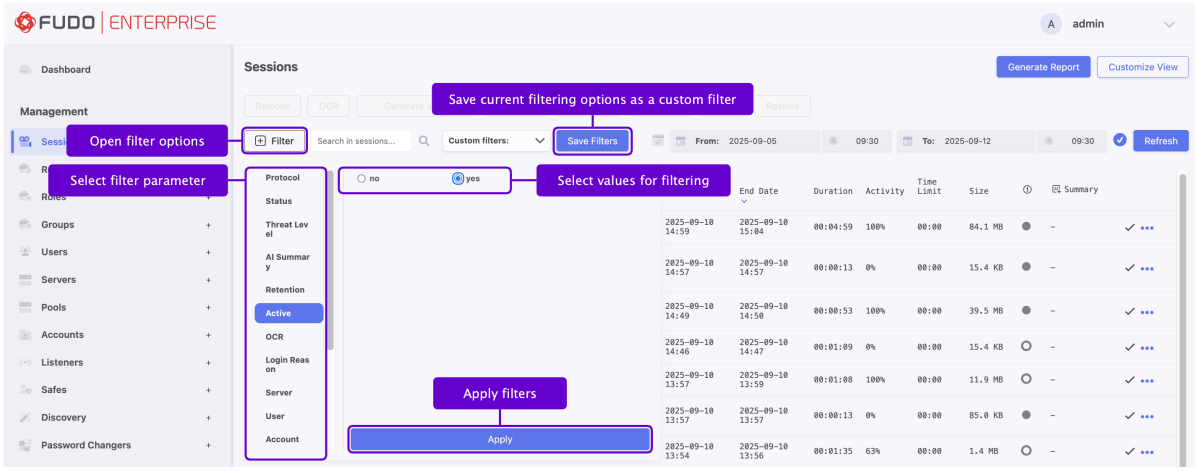
6.1 Filtering Sessions

Sessions filtering allows to find desired sessions easily by limiting the number of displayed sessions on the sessions management page.

Filtering options, such as selecting the time range when sessions started or choosing custom filters, are available by default in the top bar of the sessions view.

6.1.1 Defining Filters

1. Select *Sessions*.
2. Click *+ Filter*.
3. From the list of available filtering options select desired filter parameter.
4. Select the values for the previously added filter parameter.
5. Click **Apply** to confirm the filter.



Note

Enter a string of characters to limit the number of the elements on the list. In case of users, the elements on the list can be limited to those who have a given user role assigned or belong to the given organization unit.

6. Repeat steps 1 - 4 to define additional filters.

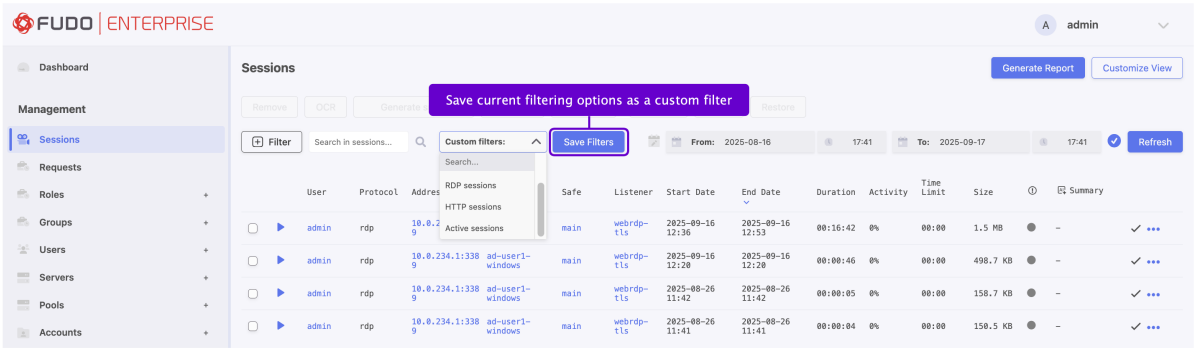
Note

Only sessions which match all defined filtering parameters will be displayed.

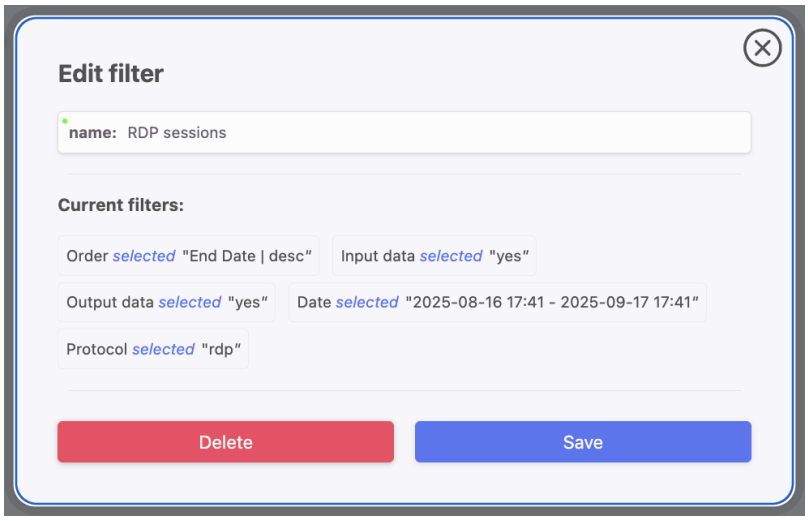
6.1.2 Saving Custom Filters

Current filtering settings can be saved as a user-defined filter preset for the administrator's convenience.

1. Select *Sessions*.
2. Click + **Filter** and define filtering options as described in the *Filtering sessions* section.
3. Click the **Save Filters** button to store the filter definition.

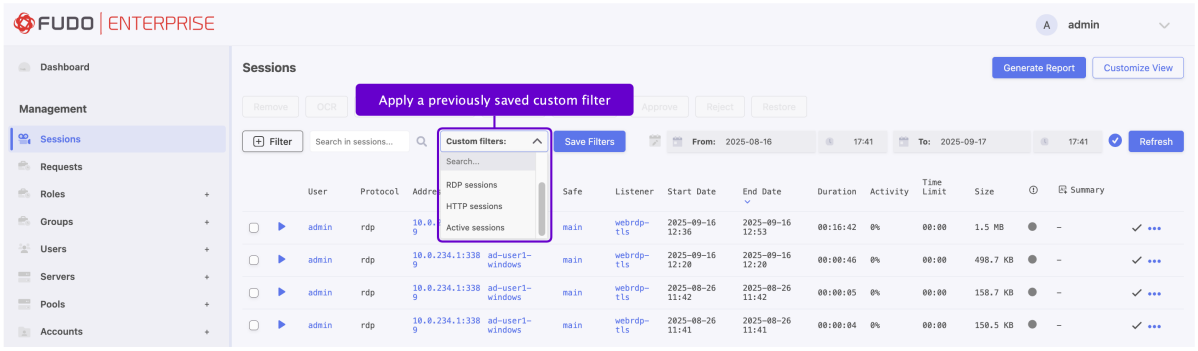


4. In the modal window, enter a name for the new filter.
5. Click **Save** to confirm and store the custom filter.



6.1.3 Applying Custom Filters

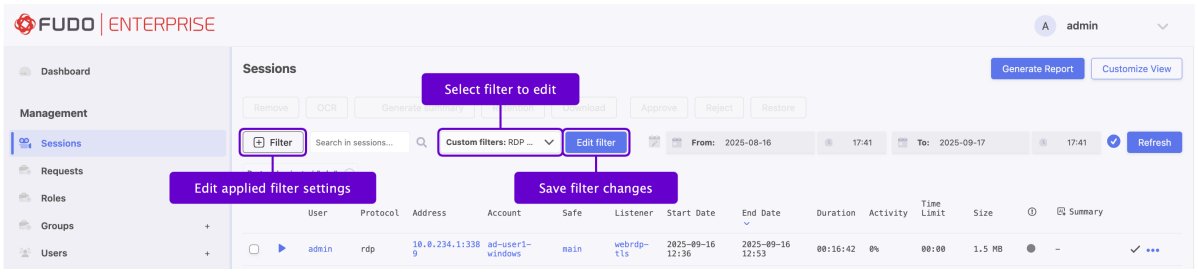
To apply a previously saved custom filter, select it from the **Custom filters** list. The selected filter will be immediately applied to the session list, and only sessions matching the defined criteria will be displayed.



6.1.4 Editing Custom Filters

To edit a previously saved custom filter:

1. Select the desired filter from the **Custom filters** list. The **Edit Filter** button becomes available.
2. Adjust the filtering options as needed.
3. Click **Edit Filter**. A modal window opens, showing the current filter configuration.
4. Click Save to overwrite the existing filter with the updated configuration.

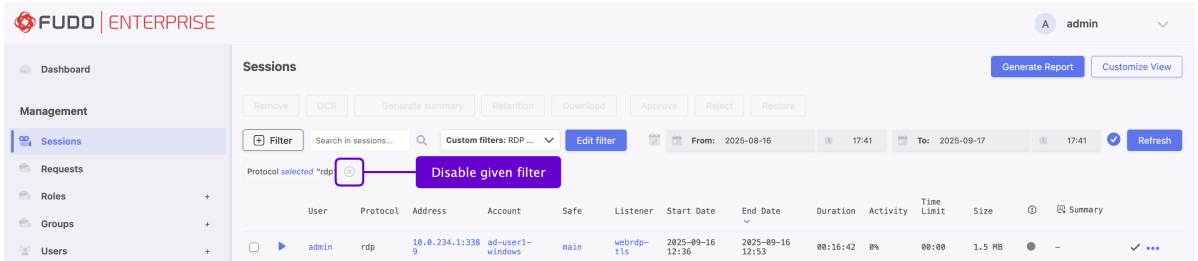


6.1.5 Disabling Filters

> **Note**
>
> Active filters are displayed on the bar below the filtering settings.

To disable an active filter, click the X icon next to the filter name.

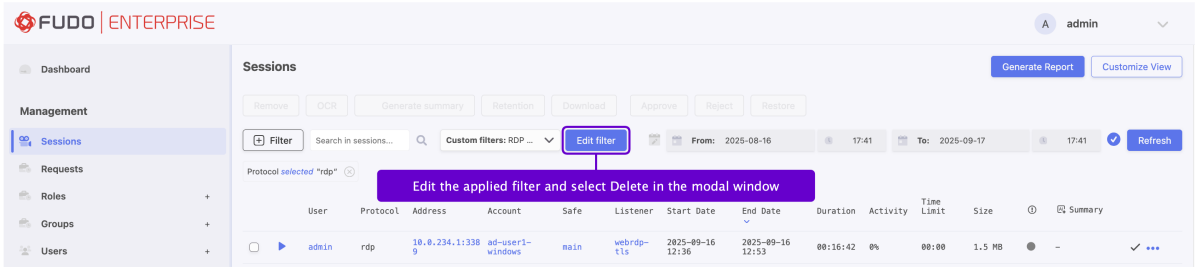
The filter is immediately disabled and no longer affects the displayed session list.



6.1.6 Deleting Custom Filters

To delete a previously saved custom filter:

1. Select the filter from the **Custom filters** list.
2. Click **Edit Filter** to open the modal window with the filter details.
3. Click Delete to permanently remove the selected filter.



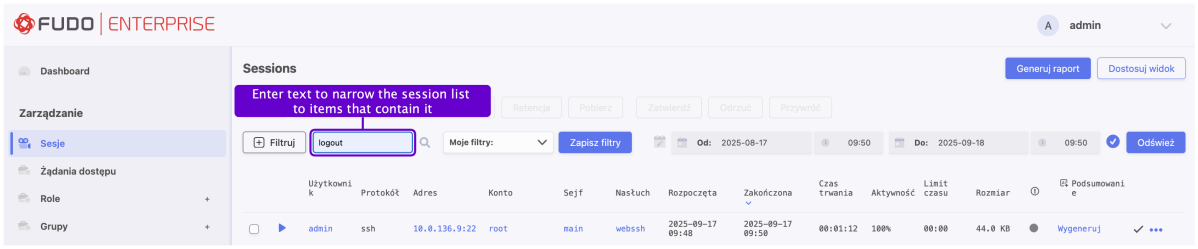
6.1.7 Full Text Search

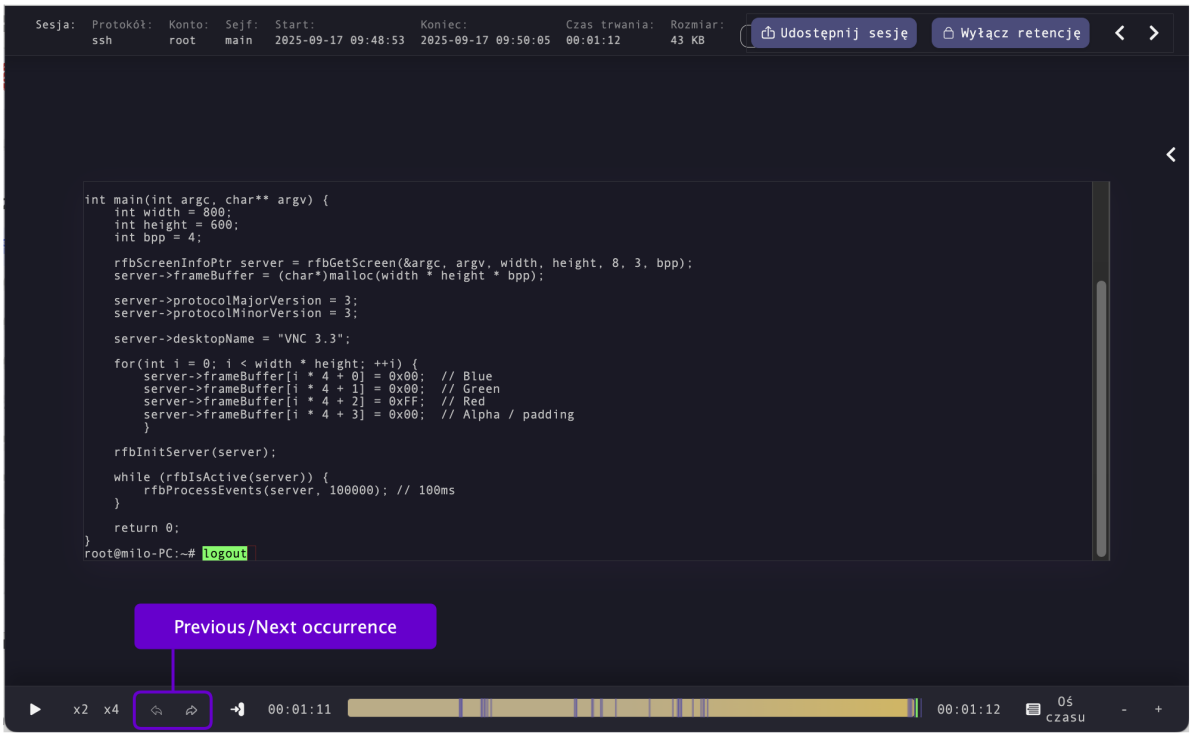
Fudo Enterprise enables searching stored data to limit the number of elements on the sessions list only to those containing the specified phrase.

Note

- Use the Sessions search bar to search for sessions containing specific phrases, e.g. "logout".
- Playing a session containing the specified phrase starts from the moment of its first occurrence.

The player allows for skipping between each occurrence of the specified phrase.





Related topics:

- *System overview*
- *Reports*

6.2 Viewing Sessions

Fudo Enterprise allows viewing recorded sessions as well as current user connections.

To view a session, proceed as follows.

1. Select *Sessions*.
2. Find desired session and click the play icon next to it.

> **Note**
>
> Filter sessions to display only active connections:
>
> - Click *+ Filter* and select the *Active* parameter.
> - From the parameter options, select *yes*.

Session player options

> **Note**
>
> Some options are available for live sessions only.

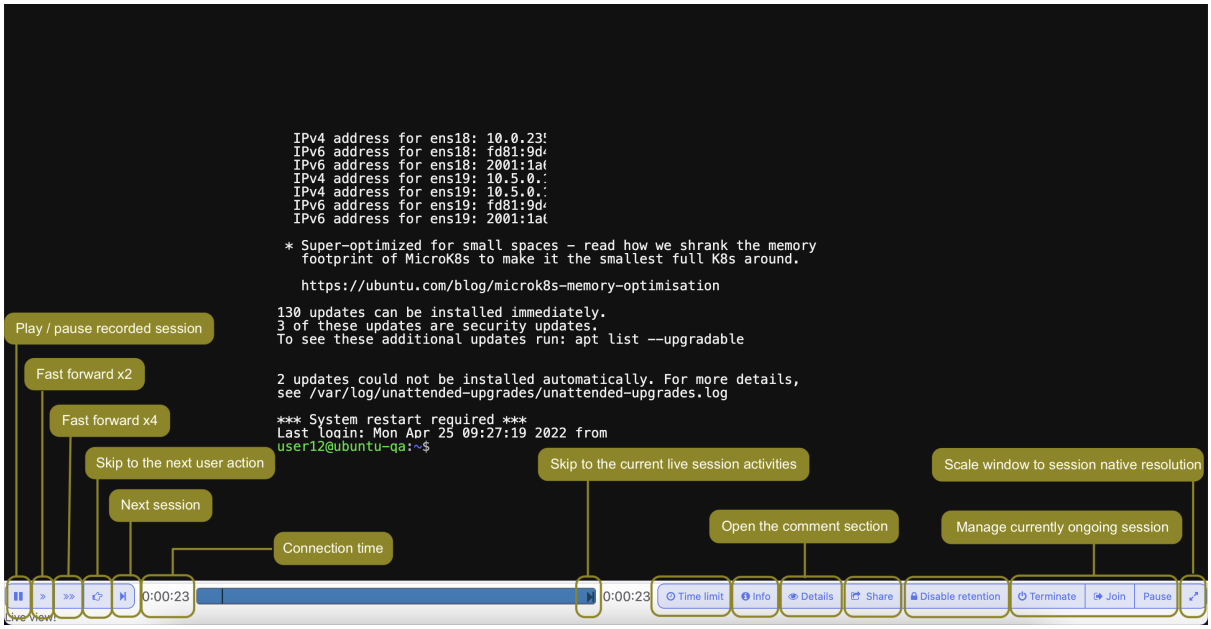
Sound of RDP sessions

Recordings of RDP sessions may also contain the sound of the session. The player decodes it together with the image, and a volume control on the player toolbar allows setting the playback level or silencing it.

Note

- The sound is recorded only for sessions established through a listener that uses the new RDP implementation, with the *Sound recording* option selected in the safe. Refer to *Selecting the RDP implementation* and *the safe functionality options*.
- Sessions recorded before the upgrade, and sessions recorded with the previous RDP implementation, contain no sound.
- The sound is available when playing back a recording. Sessions opened in the browser with the Web Client are without sound.

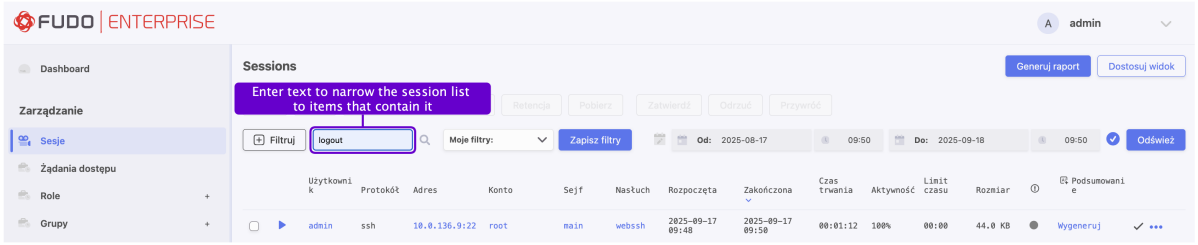
SSH, RDP, VNC, X11, Telnet

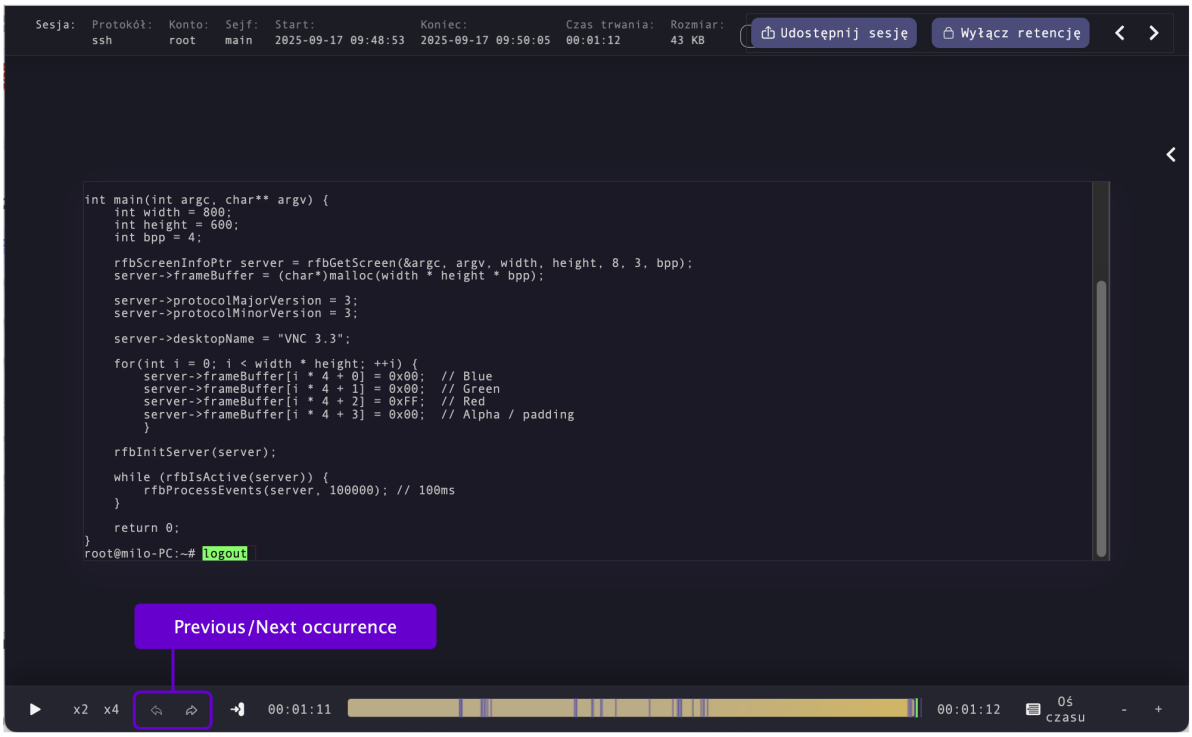


Note

Playing a session containing the specified phrase starts from the moment of its first occurrence.

The player enables skipping between each occurrence of the specified phrase.





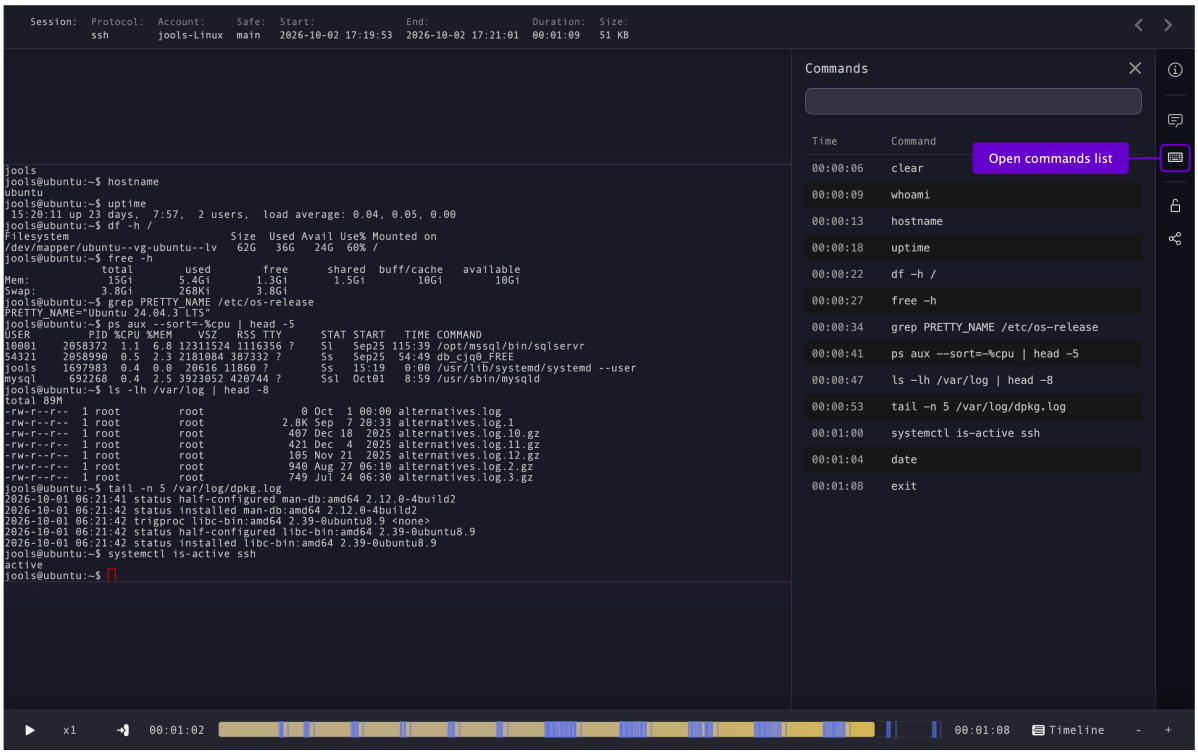
Note

Click the displayed elapsed time to switch between the connections's actual and relative time.

Commands List in SSH Sessions

For SSH sessions, the player lists the commands entered by the user. To open the list, click the **Commands** icon on the side bar of the player.

- Click a command to jump to the moment the user started typing it.
- Use the search field to find a command.
- In a live session, new commands are added to the list while it is open.
- Commands controlled by a *Sudo policy* are highlighted: allowed commands in green with the user they were run as, denied commands in red with the **Denied** label.

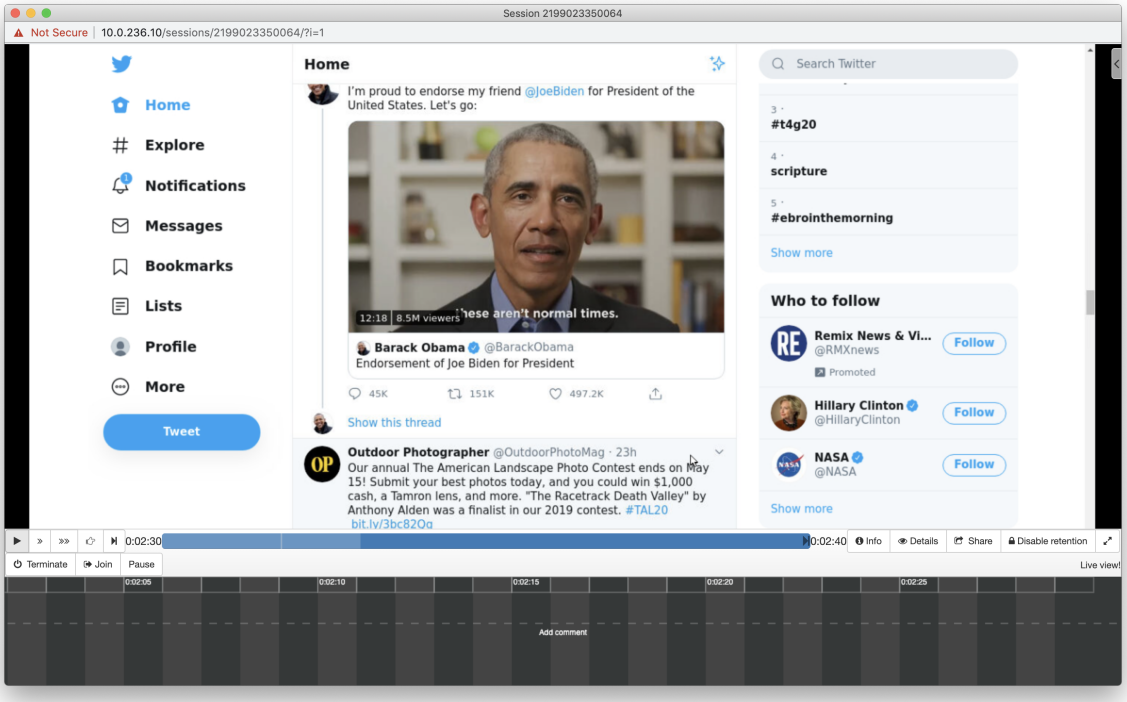


Note

- The list is created automatically and may be incomplete or contain other typed text, for example lines entered in text editors or in tmux and screen sessions. The session recording remains the complete record.
- Passwords typed at a prompt that does not display them are not saved in the list. A password that is visible on the screen, for example given as a command argument, is saved.
- The list is not available to users who view a session through a shared link.

Below, you will find screenshots displaying session views established using various protocols such as HTTP, SSH, SFTP, MySQL, MSSQL and SCP.

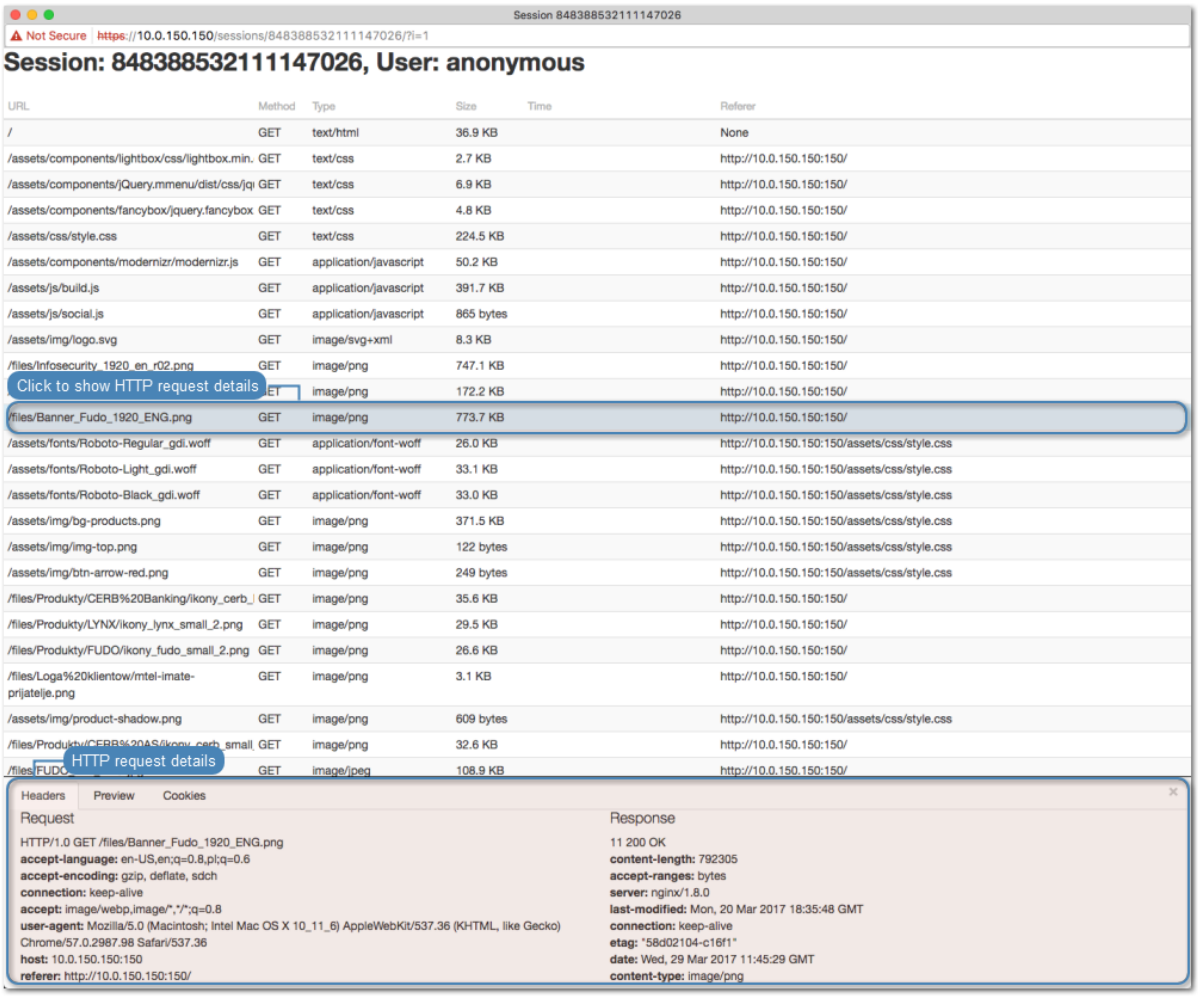
HTTP - rendered



Note

In case of rendered HTTP sessions, raw protocol data is not recorded.

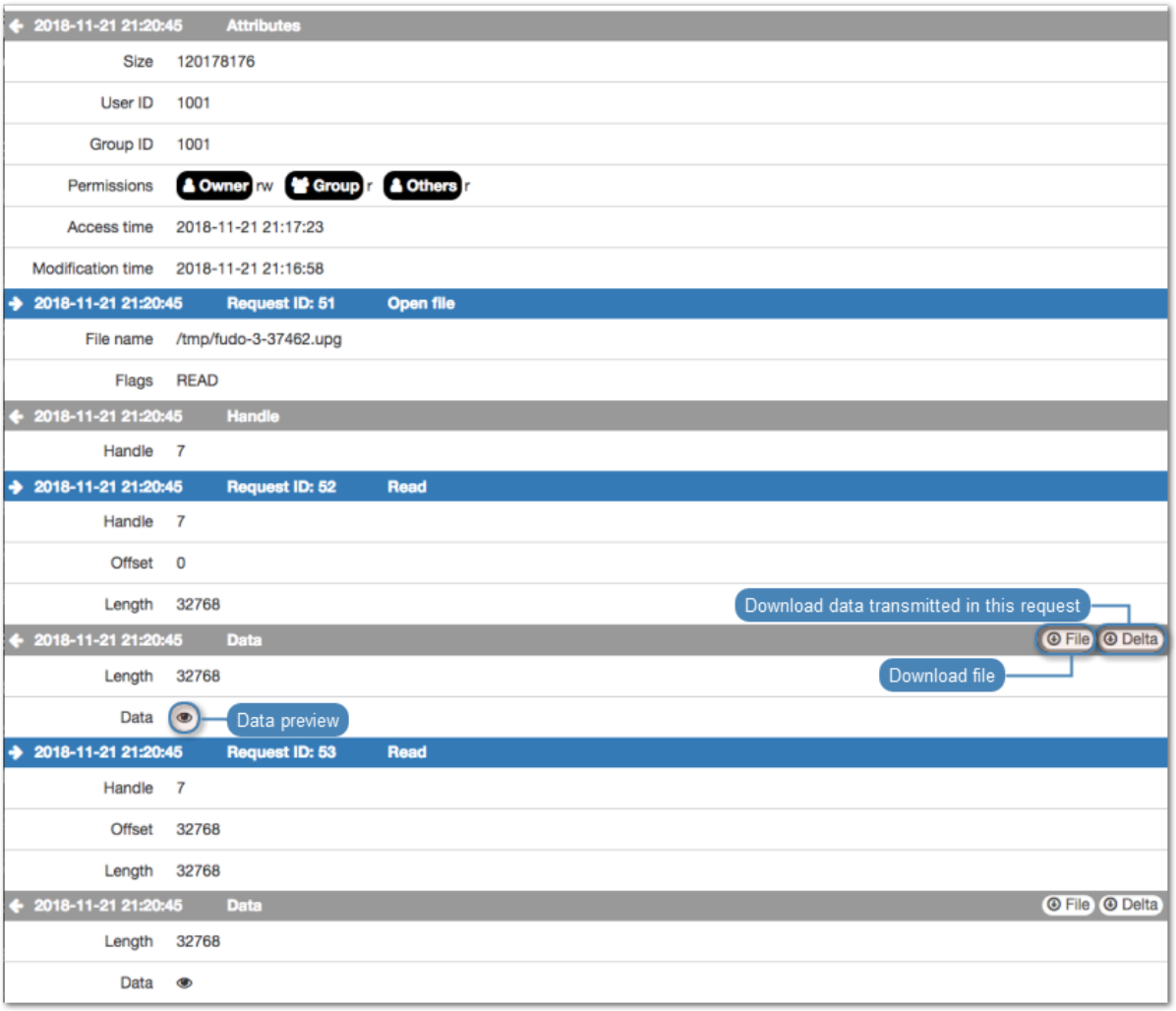
HTTP - raw


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/
Click to show HTTP request details
/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/
HTTP request details
/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

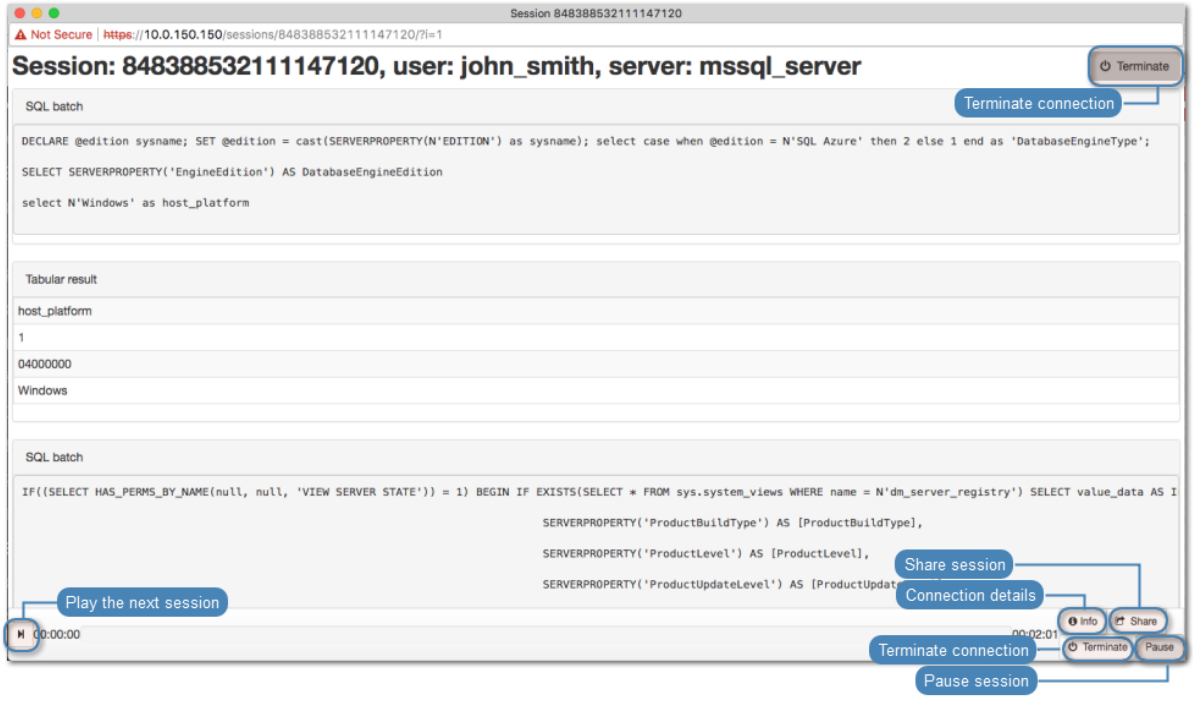
SSH

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

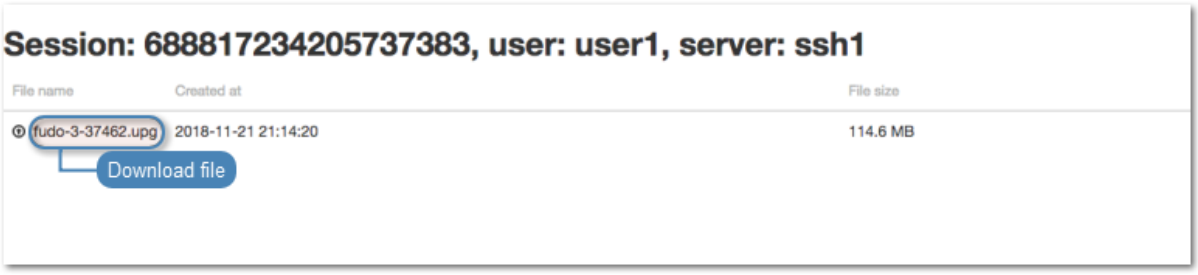
SFTP



MySQL, MSSQL



SCP



Related topics:

- *Sensitive Features*

6.3 Viewing Files Transferred in Rendered HTTP Sessions

Fudo Enterprise records every file uploaded or downloaded in a rendered HTTP session, in all safes. The list is available on the *Files* tab of the session details, both on the session list and in the player. Sessions over other protocols have no list of transferred files.

Note

Recording and scanning are separate. Files are scanned only in safes for which *file scanning* is enabled, and only then does the record include the scan result. In other safes the files are recorded with the *Not scanned* result. The content of the files is not stored.

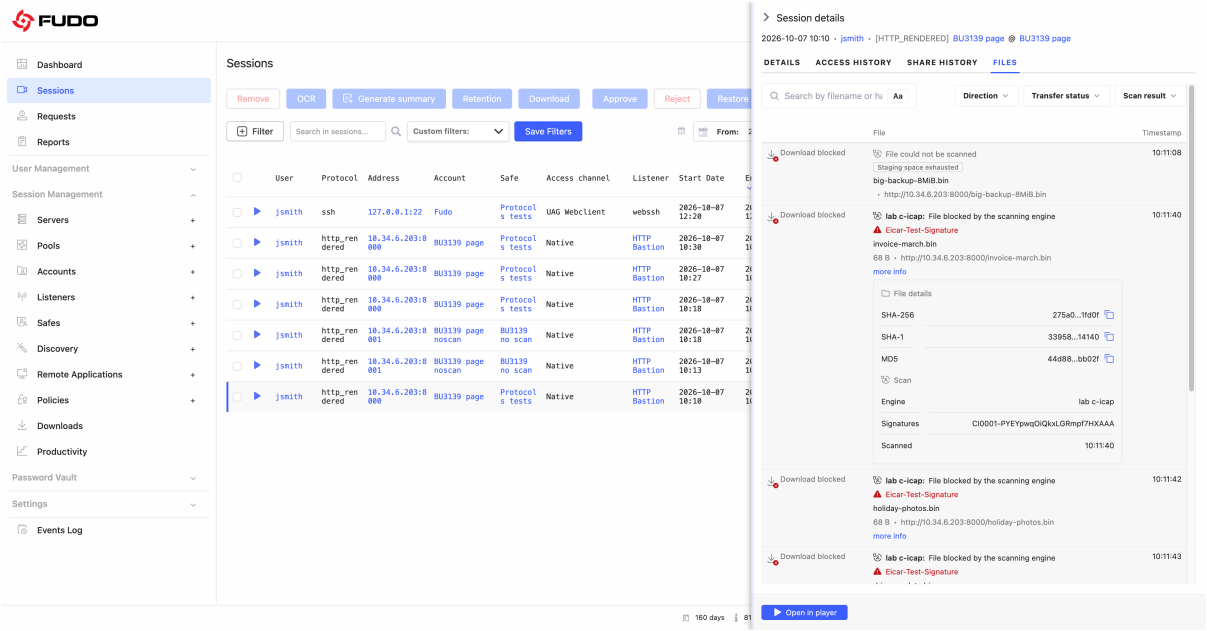
Files Tab on the Session List

1. Select *Sessions*.
2. Click the row of a rendered HTTP session (outside the links and the play icon) to open the *Session details* panel.
3. Go to the *Files* tab.

Each entry shows:

- the direction and the result of the transfer: *Uploaded*, *Downloaded*, *Upload blocked*, *Download blocked*, *Upload failed* or *Download failed*,
- the scan result:
  - *File scanned and safe.* - the provider found no threat,
  - *File blocked by the scanning engine* - the provider rejected the file; the name of the detected threat is shown below in red,
  - *File could not be scanned* - the file was blocked because it could not be scanned; the reason is shown below, for example *Engine unreachable*, *Engine error*, *Scan timed out*, *Scanner saturated*, *Staging space exhausted* or *Source changed during scan*,
- the name of the provider that scanned the file,
- the file name, size and location (for downloads, the address the file was downloaded from),
- the time of the transfer.

Click *more info* to see the SHA-256, SHA-1 and MD5 hashes of the file (with buttons to copy them), the provider name, the signature version reported by the provider and the time of the scan.



Use the search field and the filters above the list to narrow it down:

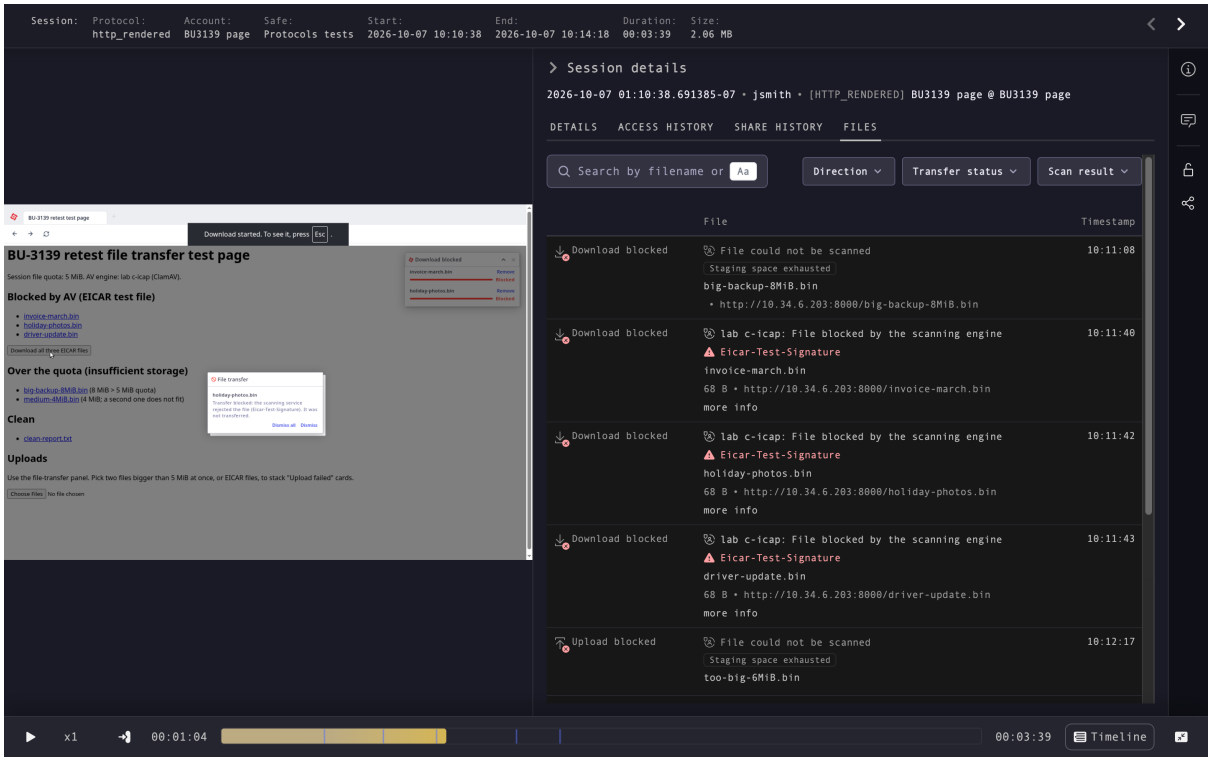
- **Search by filename or hash** - Finds files by name or by any of their hashes. Click *Aa* to make the search case-sensitive.
- **Direction** - *Upload* or *Download*.
- **Transfer status** - *Completed*, *Blocked*, *Failed* or *Unknown*.
- **Scan result** - *Clean*, *Blocked by engine*, *Not scannable* or *Not scanned*.

Note

Staging space exhausted means that the file did not fit in the space available for file transfers in the session. Such a file is blocked before it is scanned.

Files Tab in the Player

1. Open the session in the player.
2. Click the *Session details* icon on the side bar of the player and go to the *Files* tab.
3. Click an entry to jump to the moment of the transfer in the recording.



Related topics:

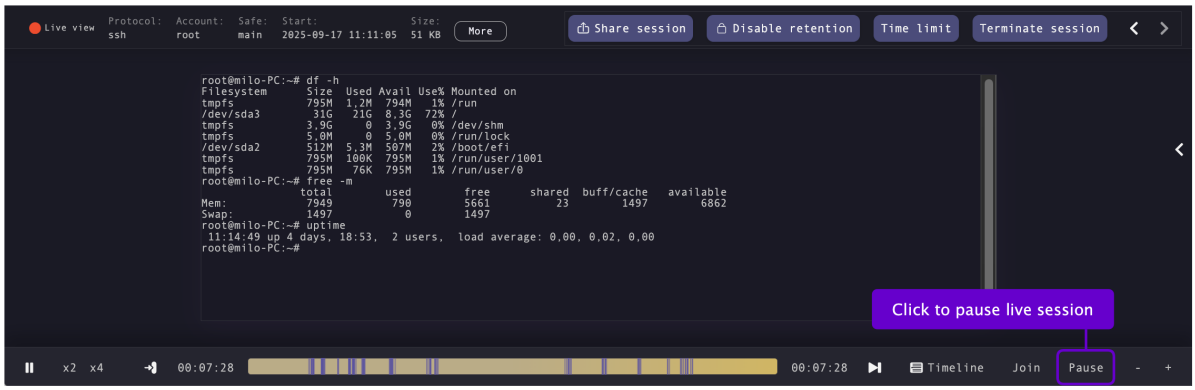
- *File Scanning in Rendered HTTP Sessions*
- *Viewing Sessions*

6.4 Pausing Connection

In case a current user action requires analysis, the connection to the server can be paused.

> **Note**
>
> Pausing connection temporarily suspends data transmission. After resuming connection, buffered user's actions are forwarded to the server.

1. Select *Sessions*.
2. Click *+ Filter* and select the *Active* parameter.
3. From the parameter options, select *yes*.
4. Find desired session and and click the play icon to start playback.
5. Click *Pause*.



Related topics:

- *Replaying session*
- *Joining session*
- *Filtering session*

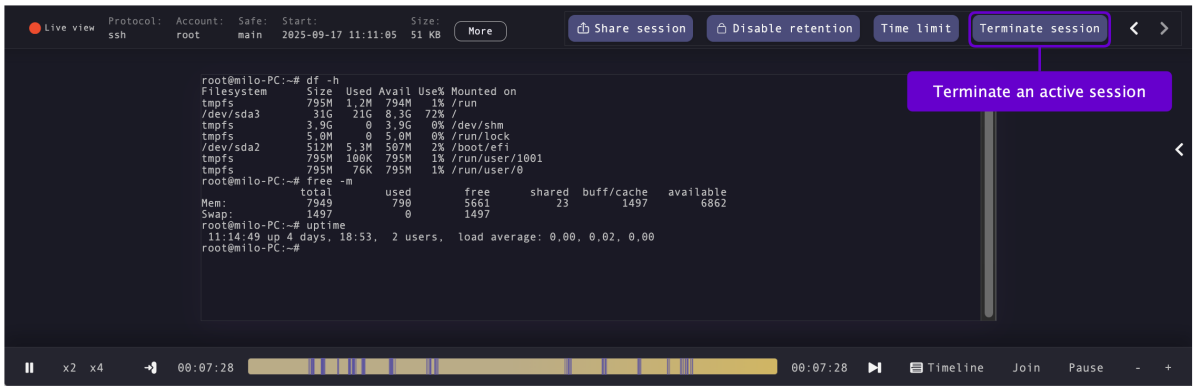
6.5 Terminating Connection

In case the administrator notices access rights misuse, Fudo Enterprise allows to terminate the session and automatically block given user.

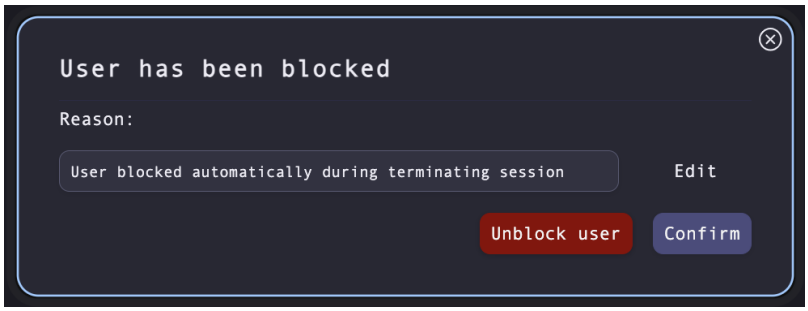
> **Note**
>
> Fudo Enterprise can automatically block user account upon detecting a defined pattern. For more information refer to *Policies*.

1. Select *Sessions*.
2. Click *+ Filter* and select the *Active* parameter.
3. From the parameter options, select *yes*.
4. Find desired session and and click the play icon to start playback.
5. Click *Terminate*.

> **Note**
>
> Terminating connection automatically blocks given user.



6. Decide whether the user should remain blocked or not.



Related topics:

- *Policies*
- *Security Measures*
- *Joining Live Session*
- *Sharing Sessions*
- *Filtering Sessions*

6.6 Joining Live Session

Fudo Enterprise allows joining an ongoing session to work simultaneously with the remote user.

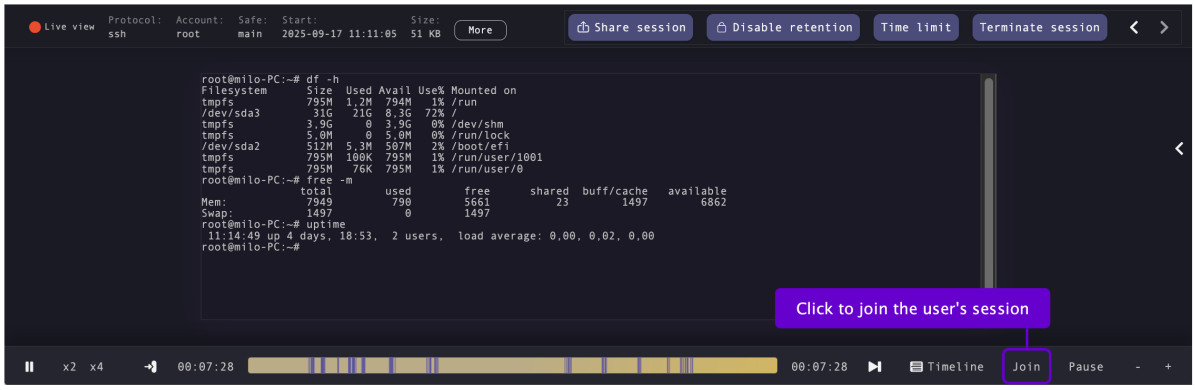
Note

- Session joining feature is supported in SSH, RDP, VNC and Telnet (excluding 5250 and 3270) connections.
- In case of cluster configurations, joining session is only possible after logging into the administration panel on the node that handles the given access session.

To join currently established session, proceed as follows.

1. Select *Sessions*.
2. Click *+ Filter* and select the *Active* parameter.
3. From the parameter options, select *yes*.
4. Find desired session and and click the play icon to start playback.

5. Click *Join*.



Related topics:

- *Replaying sessions*
- *Sharing sessions*
- *Filtering sessions*
- *Supported Protocols*

6.7 Sharing Sessions

Fudo Enterprise allows you to give another person access to a selected session through a generated link. The link works both on the management address and on the User Access Gateway address, so you can share a session with someone who has no access to the management panel.

A link is created with the following settings:

- **Access type** - whether the link expires together with the session, or is valid during a selected time window.
- **Access permissions** - whether the recipient must sign in to Fudo Enterprise before viewing the session, or can open it anonymously.
- **Session mode** - whether the recipient can only watch the session, or can also interact with it.

Note

Access type and *Session mode* are offered only for sessions that are still running. For a session that has already ended there is nothing to join and no live period to follow, so the window asks only for the time window and the access permissions.

Important

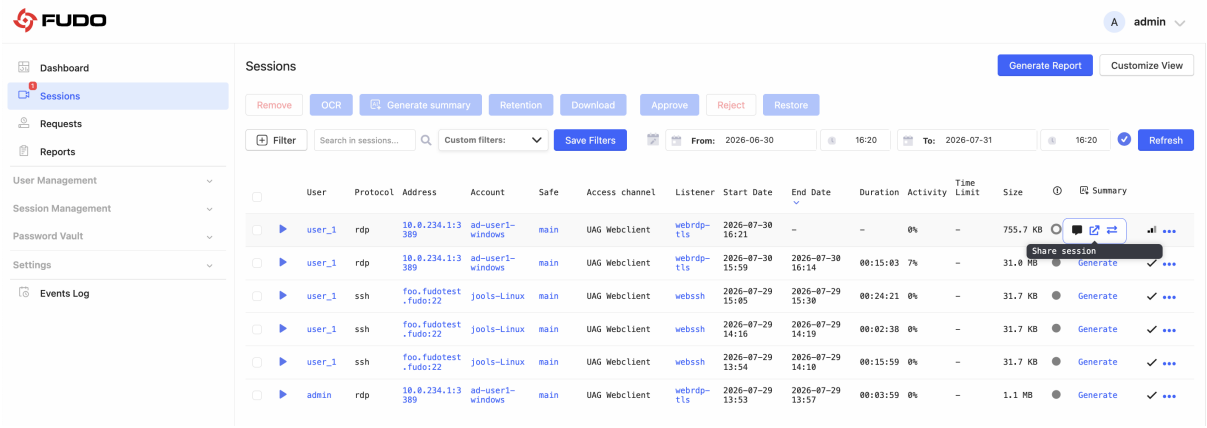
Users can also share their own live sessions directly from the User Access Gateway, without involving an administrator. This requires the *Allow users to share live sessions* option to be enabled on the safe. A sharing link created by a user in the User Access Gateway requires the recipient to **sign in** to Fudo Enterprise before viewing the session. The link remains valid only while the shared session is active and stops working when the session ends.

Refer to the *Creating a Safe* section and the User Access Gateway documentation for more information.

Sharing a Session

To share a session, proceed as follows.

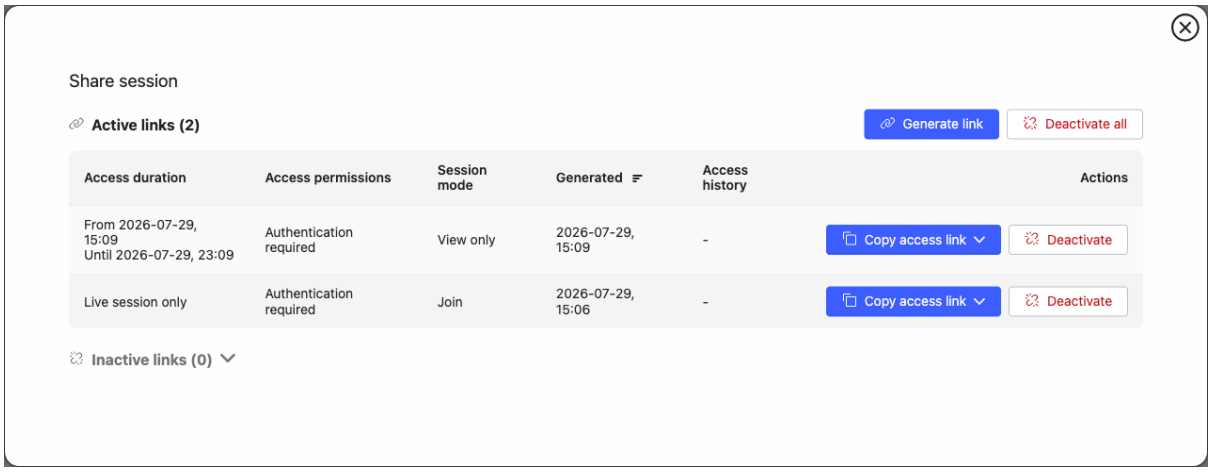
1. Select Sessions.
2. Find the desired session, expand the more options menu (.), and click . to open the *Share session* window.



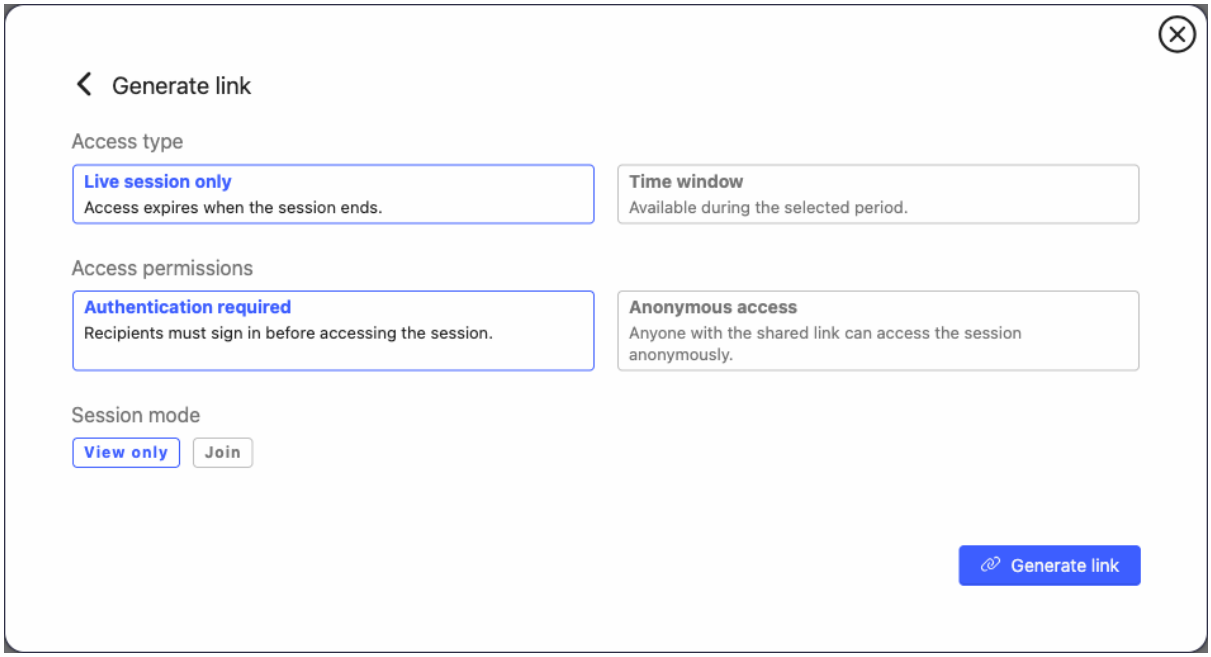
Note

The same window is available in the session player, under the *Share session* button. Use whichever is closer at hand - the window and its options are identical.

3. Click *Generate link*.

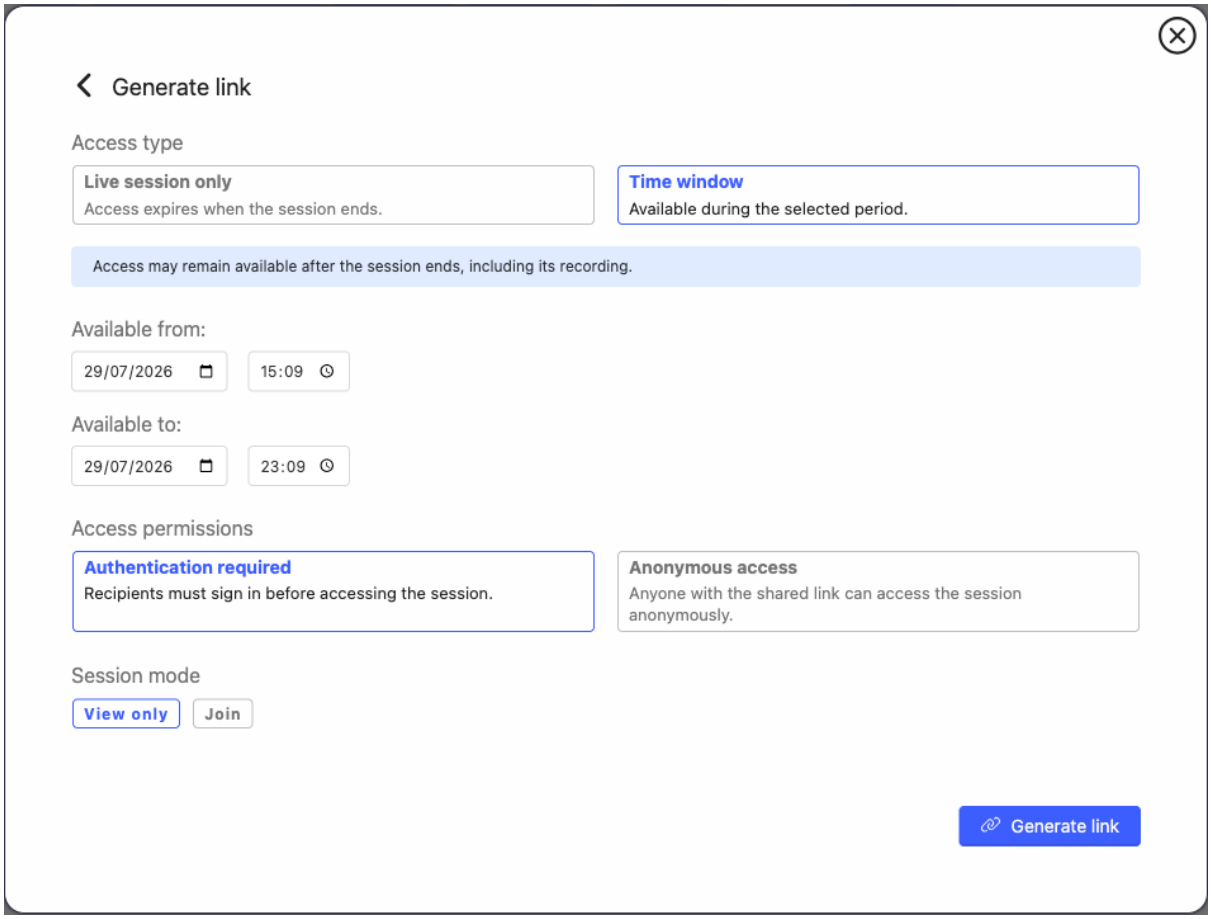


4. Select the *Access type*:
   - **Live session** - the link stays valid while the session is live. Offered only for sessions that are still running.
   - **Time window** - the link is valid within a chosen time window. Provide the *Available from* and *Available to* values. For sessions that have already ended, the two fields are shown straight away and this is the only possible access type.



Important

A link with a time window may remain valid after the session ends, which means it also gives access to the session recording.



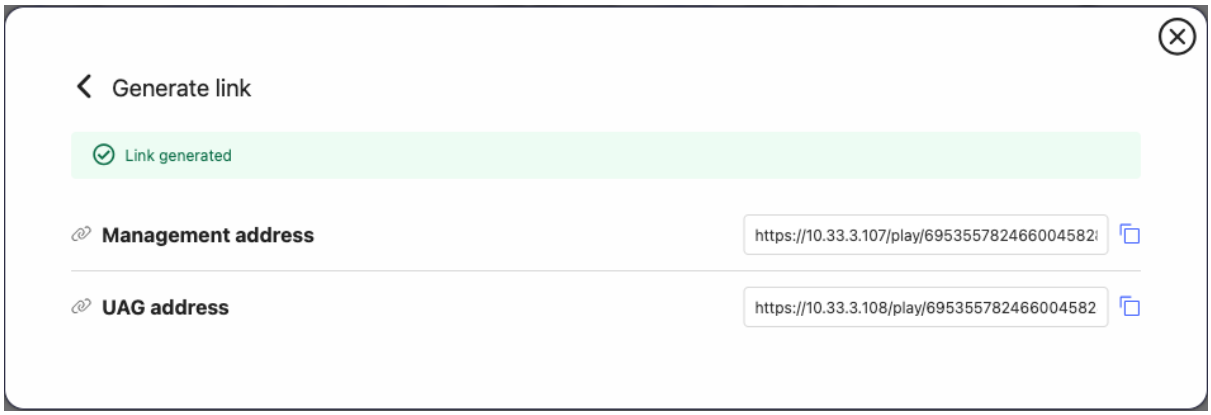
5. Select the *Access permissions*:

- **Authentication required** - recipients must sign in to Fudo Enterprise before they can access the session, and their identity is recorded in the access history. Any Fudo Enterprise user holding the link can sign in - the link is not bound to one specific person.
- **Anonymous** - anyone with the link can access the session without signing in. Such viewers are recorded as *Anonymous* together with their source IP address.

Important

An anonymous viewer never sees the keystrokes recorded in the session - they are always masked, even when *Show keyboard input* is enabled. Anonymous viewers are also not counted towards the number of supervisors required by a live supervision policy. Choose *Authentication required* whenever you need either.

6. Select the *Session mode*. This step is offered only for a session that is still running.
   - **View only** - the recipient can watch the session but cannot interfere with it.
   - **Join** - the recipient can also interact with the session.
7. Click *Generate link*.
8. Copy the address that matches the network the recipient can reach, and close the window.
   - **Management address** - for recipients who have access to the Fudo Enterprise management address.
   - **UAG address** - for recipients who reach Fudo Enterprise only through the User Access Gateway, for example external contractors.



What the Recipient Sees

A recipient opening a shared session is shown the recording itself, not the surrounding administrative context. Fudo Enterprise withholds that data in its API responses, so it is not available to the recipient in any form. In particular, the recipient does not see who conducted the session, the source and destination addresses, the names of the server, the safe and the account, or any information about the appliance and its licence.

Note

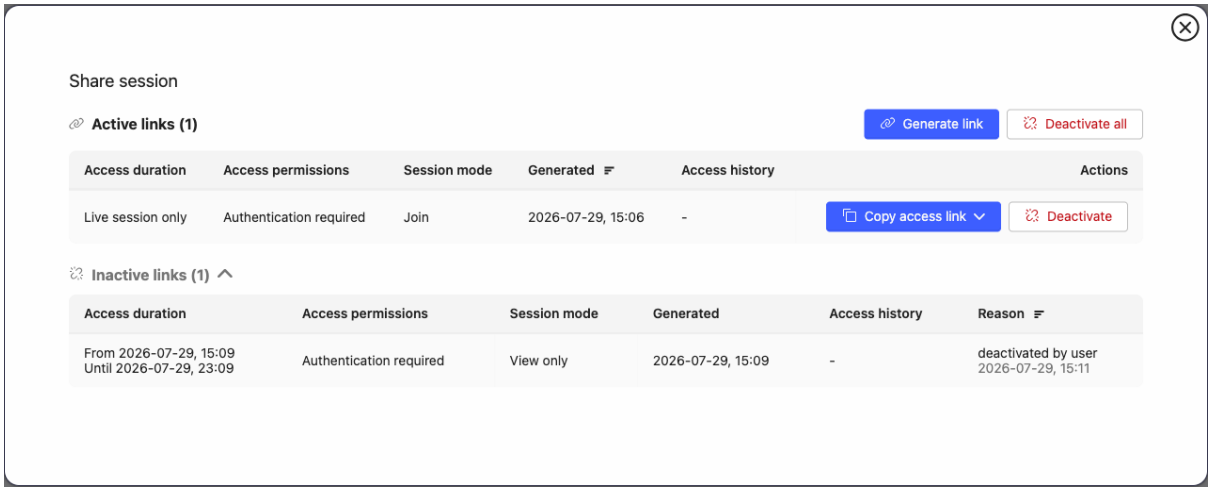
Keystroke visibility depends on the access permissions of the link. A viewer who signed in is subject to the usual rules for keyboard input, while an anonymous viewer never sees the

typed characters. Refer to the *Sensitive Features* topic for details on keyboard input.

Regardless of the access permissions, a recipient cannot control the session - suspending, resuming and terminating a session are not available through a share link.

Managing Session Links

All links generated for a session are listed in the *Share session* window, divided into *Active links* and *Inactive links*.



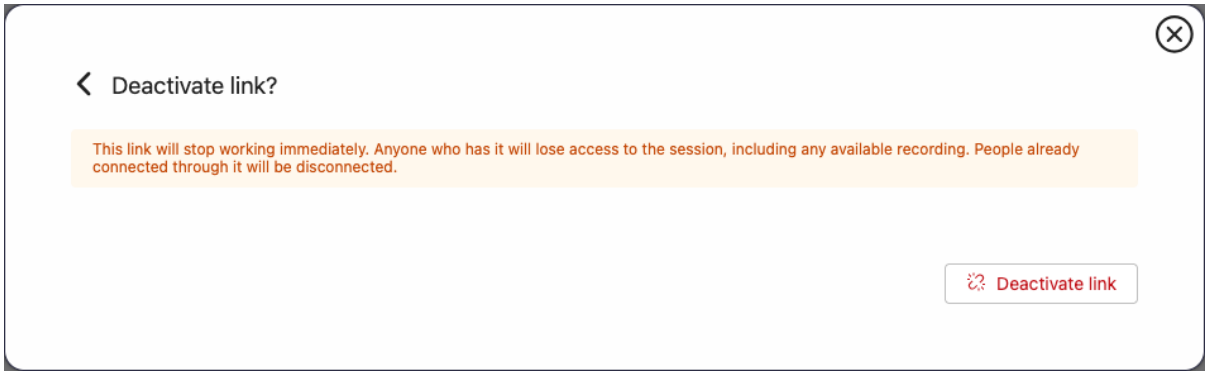
The following information is displayed for each link.

Column	Description
Access duration	*Live session only*, or the start and the end of the selected time window.
Access permissions	*Authentication required* or *Anonymous access*.
Session mode	*View only* or *Join*.
Generated	When the link was created.
Access history	Connections recorded for the link.
Actions	*Copy access link* - copies the management or the UAG address. *Deactivate* - deactivates the link.
Reason	Displayed for inactive links: why the link stopped working, together with the time.

Deactivating a Session Link

To deactivate a link, proceed as follows.

1. Select Sessions.
2. Find the desired session, expand the more options menu (.), and click ..
3. In the *Active links* list, click *Deactivate* next to the link you want to disable. To disable every link of the session at once, click *Deactivate all*.
4. Confirm with *Deactivate link*.



Important

A deactivated link stops working immediately. Everyone who has it loses access to the session, including its recording, and people already connected through it are disconnected.

The link is moved to the *Inactive links* list, where the *Reason* column shows why it stopped working - for example *deactivated by user*, or that its time window has expired.

Note

Deactivating a link does not remove the connections already recorded for it. They remain visible after the link itself is gone.

Related topics:

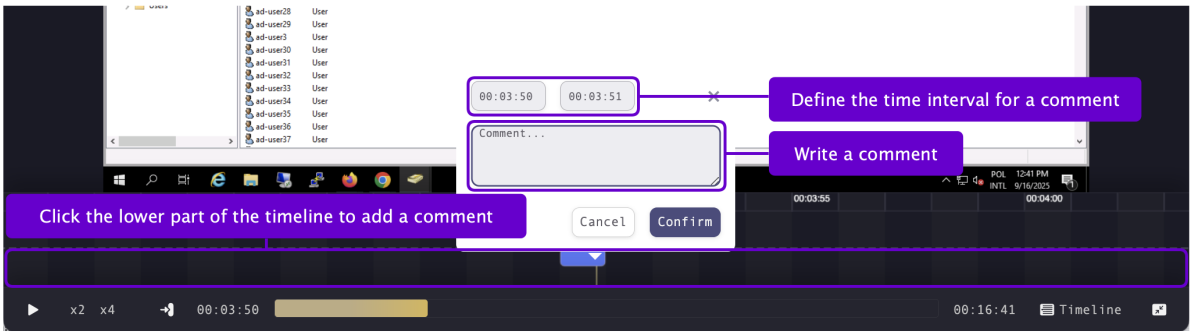
- *Replaying sessions*
- *Joining sessions*
- *Filtering sessions*
- *Creating safes*

6.8 Commenting Sessions

Fudo Enterprise enables adding comments and tags to recorded sessions.

Adding a Comment

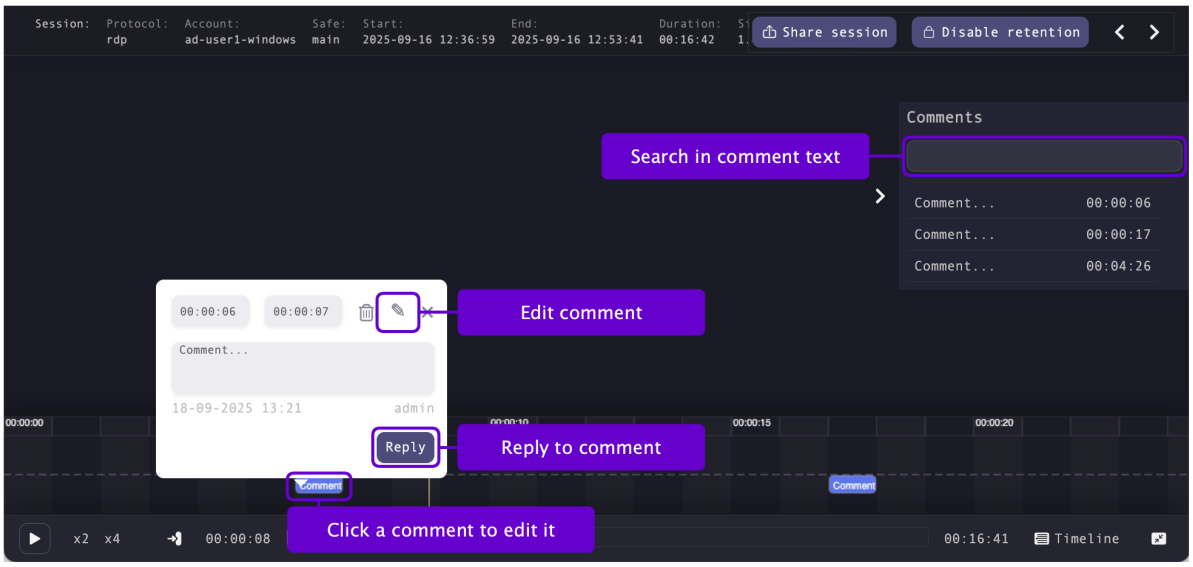
1. Select *Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Timeline* to expand the session timeline.
4. Click the lower part of the timeline to add a comment at a specific moment of the session recording.
5. Define the time interval for the comment by specifying the start and end points of the recording in the provided fields.



6. Add comment.
7. Click *Confirm*.

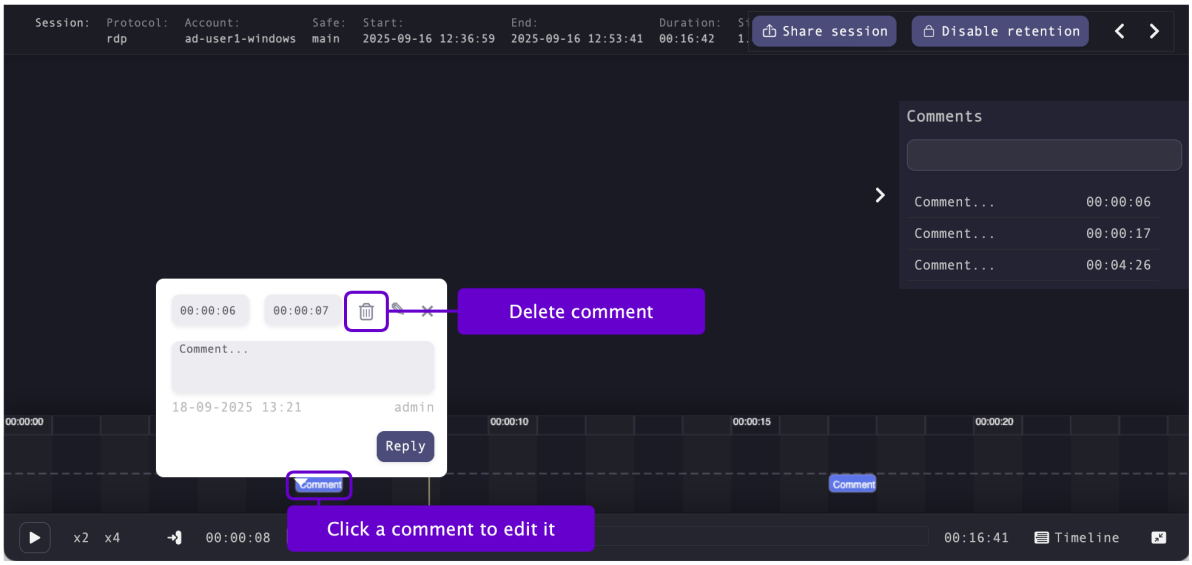
Editing a Comment

1. Select *Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Timeline* to expand the session timeline.
4. Find and click desired comment.
5. Click the edit icon.
6. Change the comment and *Confirm*.



Deleting a Comment

1. Select *Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Timeline*.
4. Find and click desired comment.
5. Click the trashcan icon.
6. Click *Delete* to delete the comment.



Replying to a Comment

1. Select *Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Timeline*.
4. Find and click desired comment.
5. Click *Reply*.
6. Enter message and click *Confirm*.

Related topics:

- *Sensitive Features*

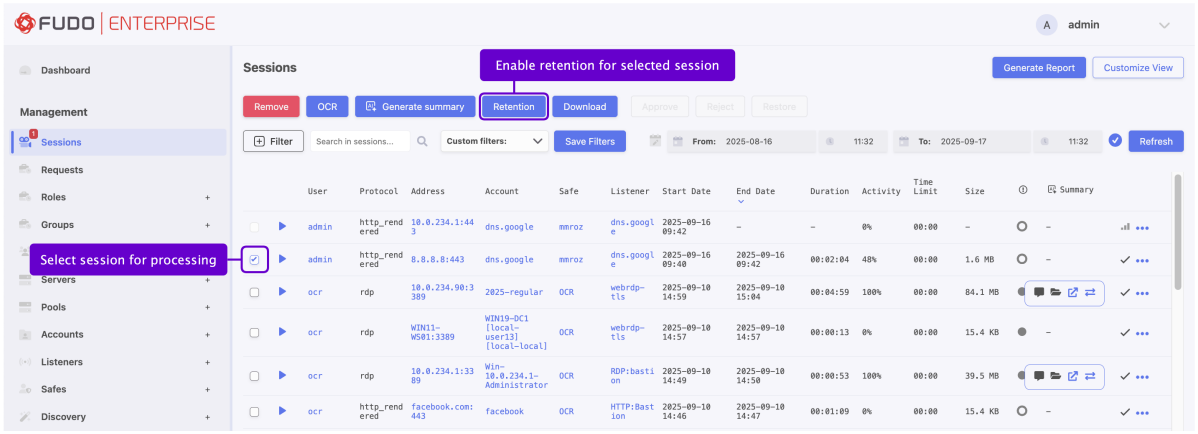
6.9 Sessions' Retention Lockdown

Data retention feature automatically deletes sessions after a specified time interval. Fudo Enterprise allows for excluding selected sessions from the retention mechanism.

Disabling Retention

To disable retention for specified sessions, proceed as follows.

1. Select *Management* > *Sessions*.
2. Find and select desired sessions.
3. Click *Retention*.
4. Select *Disable*.



5. Click *Confirm* to disable retention for selected sessions.

> **Note**
>
> Retention locked sessions are differentiated with the status icon.

Enabling Retention

1. Select *Sessions*.
2. Find and select desired sessions.
3. Click *Retention*.
4. Select *Enable retention*.
5. Click *Confirm* to enable retention for selected sessions.

> **Warning**
>
> Sessions will be deleted according to the current data retention parameters.

Related topics:

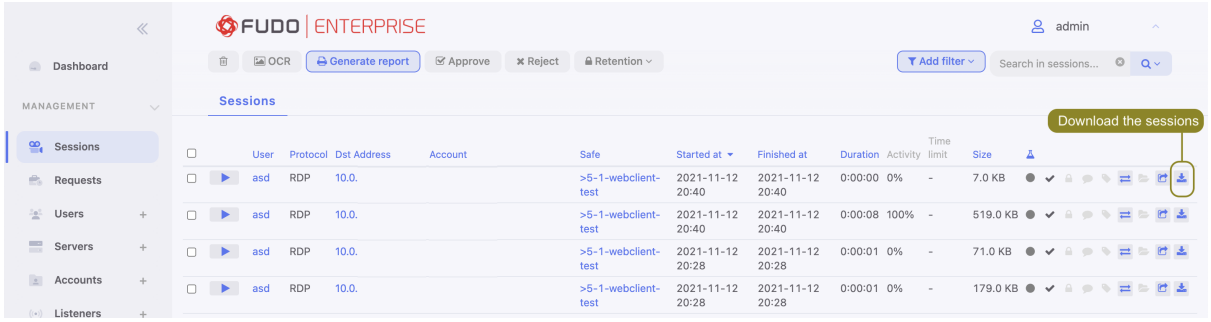
- *Session Data Backup*

6.10 Exporting Sessions

Fudo Enterprise allows converting stored session data to one of supported video formats.

To export a session, proceed as follows.

1. Select *Sessions*.
2. Find desired session and click the session export icon.



3. Select the output file format.

Note

The output file format and the resolution determine conversion time and the size of the output file.

4. Select the video resolution (*not applicable to the text log file format*).

Note

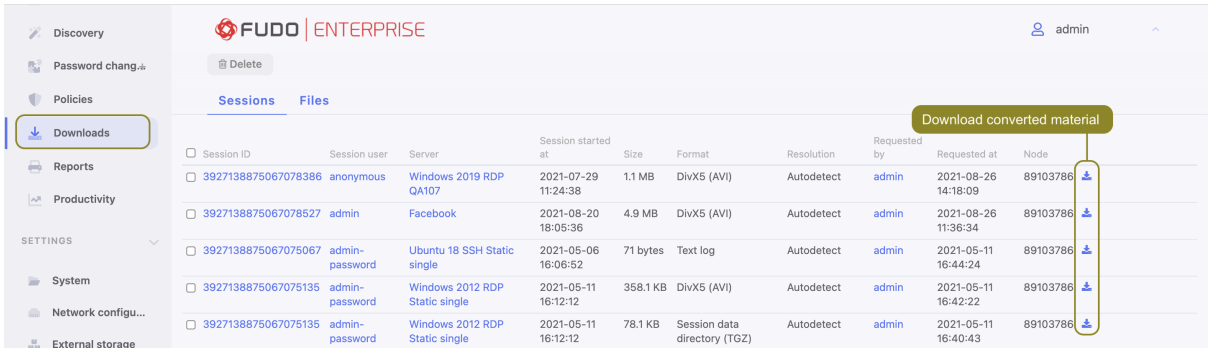
Autodetect option will export video in the native user's screen resolution.

5. Click *Confirm* to start conversion and open the downloads page.

Note

The *Downloads* page enables monitoring conversion progress.

6. Find desired session and click the *Download* icon to download converted session material.



6.10.1 Export Session File Formats

Following table provides a comparison of file formats available for session export across different protocols.

	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	

Note

* PCAP files can be downloaded only for tunneled SSH sessions, TCP sessions, and non-rendered HTTP sessions.

** PCAP files can be downloaded only if the session was recorded in a RAW format. To learn more, please check the 'all' or 'raw' options in the *account configuration*.

Under review

RAW recording of protocols that support the FBS format is **under review** and may be removed in a future release. PCAP download would then stop being available for their sessions. Sessions of database protocols - Oracle, PostgreSQL, MySQL and MSSQL(TDS) - are recorded in RAW only, so PCAP download remains available for them.

While saving a session in one of the video file formats (AVI, MPEG-2, MJPEG, FLV), you have the option to select one of the resolutions listed below:

- 480p (852x480),
- 720p (1280x720),
- 1080p (1920x1080).

Related topics:

- *Filtering sessions*
- *Sharing sessions*
- *Viewing sessions*

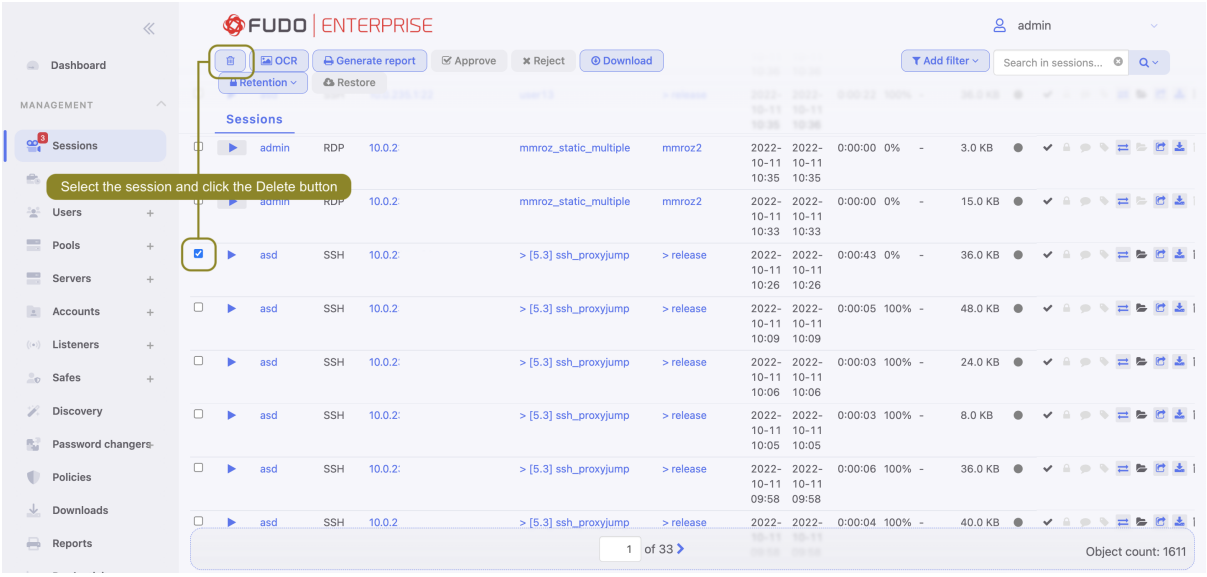
- *Joining sessions*

6.11 Deleting Sessions

> **Note**
>
> As the session's files and recorded videos are located in the *Management* > *Downloads* tab, when you remove a session, the system deletes also associated files, stored in the *Downloads* > *Files*. Recorded movies, stored in the *Downloads* > *Sessions* tab, remain and can be downloaded anytime.

To delete a recorded session, proceed as follows.

1. Select *Sessions*.
2. Find and select desired session.
3. Click *Delete*.
4. Confirm deleting selected sessions.



> **Note**
>
> Fudo Enterprise can automatically delete sessions after certain time, specified by the retention parameter. Refer to the *Backups and retention* topic for more on data retention.

Related topics:

- *Filtering sessions*
- *Sharing sessions*
- *Viewing sessions*
- *Exporting sessions*

6.12 OCR Processing Sessions

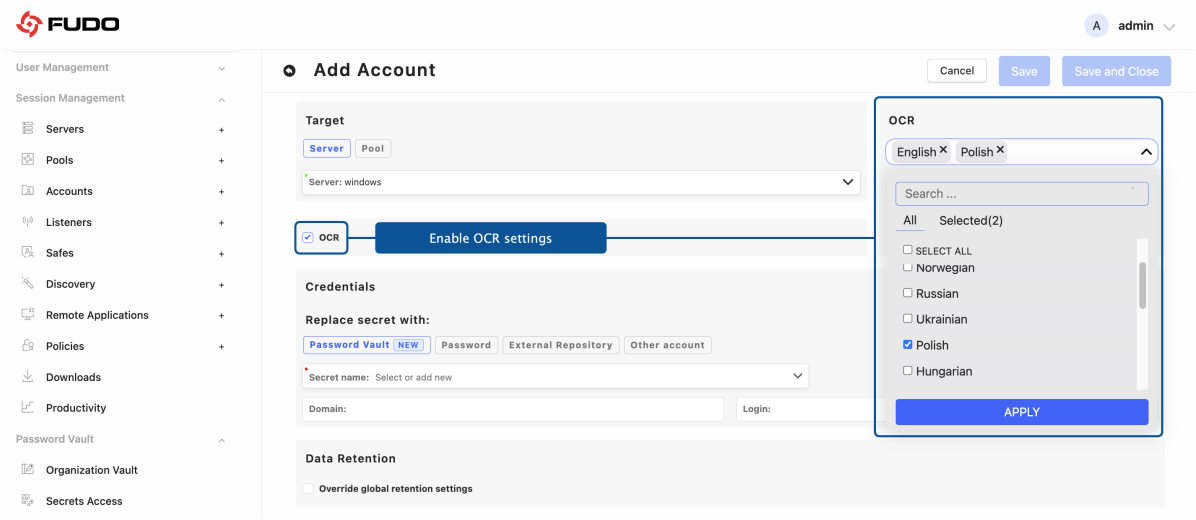
Recorded RDP, VNC and rendered HTTP sessions can be processed and indexed for full-text search purposes.

> **Warning**
>
> OCR processing is CPU intensive and may have negative impact on system's performance. It is recommended to enable it only for those accounts, which require detailed supervision.

Automated Sessions Processing

To have RDP, VNC or rendered HTTP sessions automatically processed, proceed as follows.

1. Select *Management* > *Accounts*.
2. Find and click desired account.
3. Select the *OCR sessions* option.
4. Select the language of processed data.

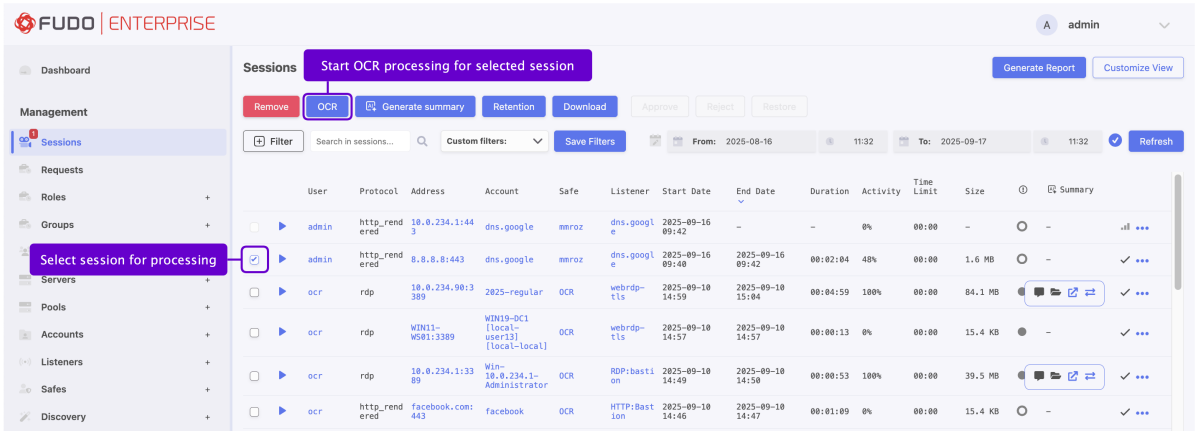


5. Click *Save*.

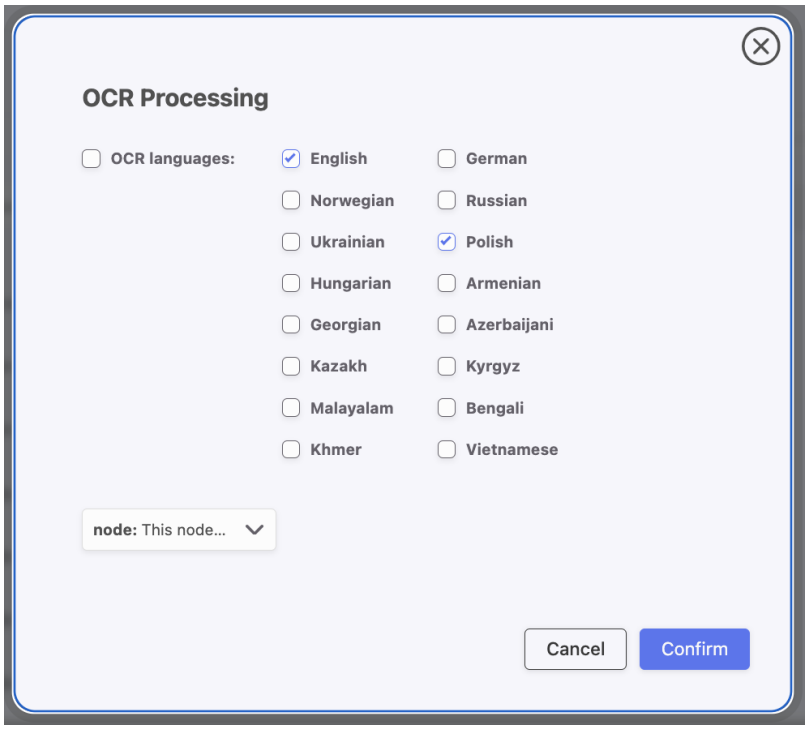
Processing Selected Sessions

To process selected sessions, proceed as follows.

1. Select *Sessions*.
2. Select desired sessions and click *OCR*.



3. In the modal window, choose the languages to be recognized.
4. Select the cluster node where the OCR process should be executed.
5. Click *Confirm* to begin the OCR process.



Note

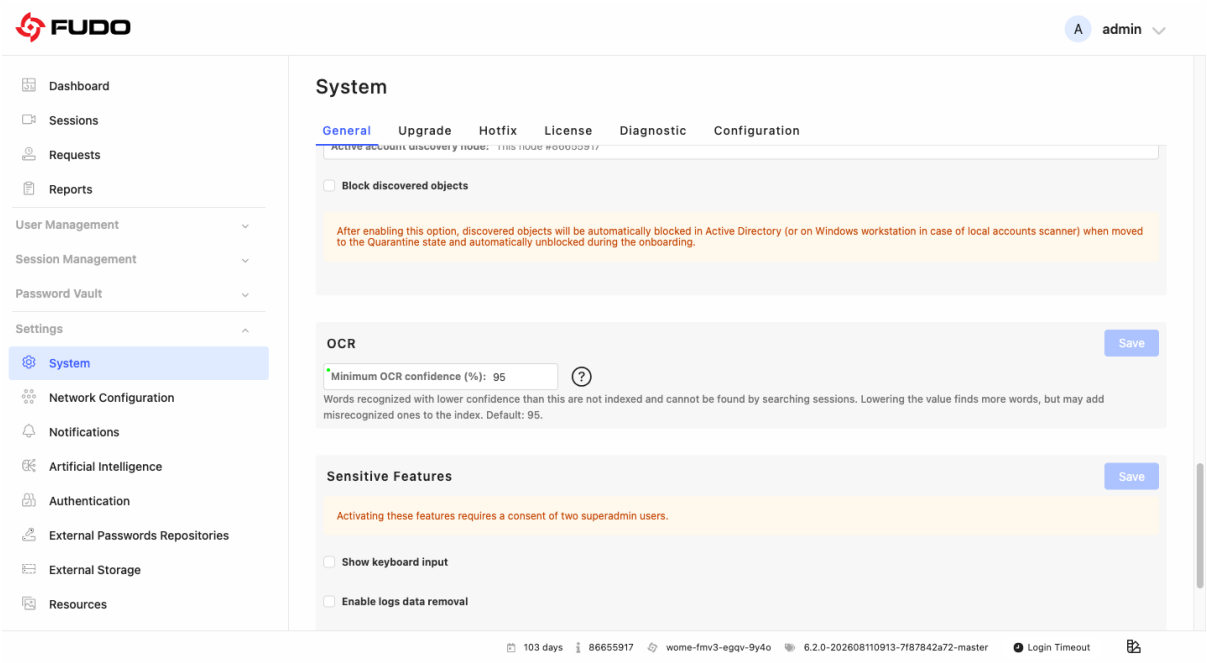
Filtering options allows for selecting processed or unprocessed objects.

Minimum Recognition Confidence

For every word it recognizes, the OCR engine also determines how certain it is of the result. Words recognized with too low a certainty are not added to the index and cannot be found by searching sessions. The required level of certainty can be adjusted.

1. Select *Settings* > *System* and stay on the *General* tab.
2. In the *OCR* section, enter a value from *0* to *100* in the *Minimum OCR confidence (%)*

field.



3. Click *Save*.

Note

The default value is *95*, which is the level applied by Fudo Enterprise before this setting existed. An upgraded system therefore recognizes text exactly as it did before, and there is no need to change the value unless text is being missed.

Lowering the value causes more words to be indexed, including those recognized less certainly - useful when sessions are recorded in poor quality and searching does not find text that is visible in the recording. The cost is that misrecognized words may also enter the index, so searching may return sessions that do not actually contain the phrase.

Note

The new value does not require restarting anything and applies to sessions processed after the change. A session whose processing is already in progress is completed with the previous value. In a cluster the setting is replicated, so it does not have to be set on each node separately.

Warning

Viewing the threshold requires the `ocr-read` privilege, and changing it requires `ocr-modify`.

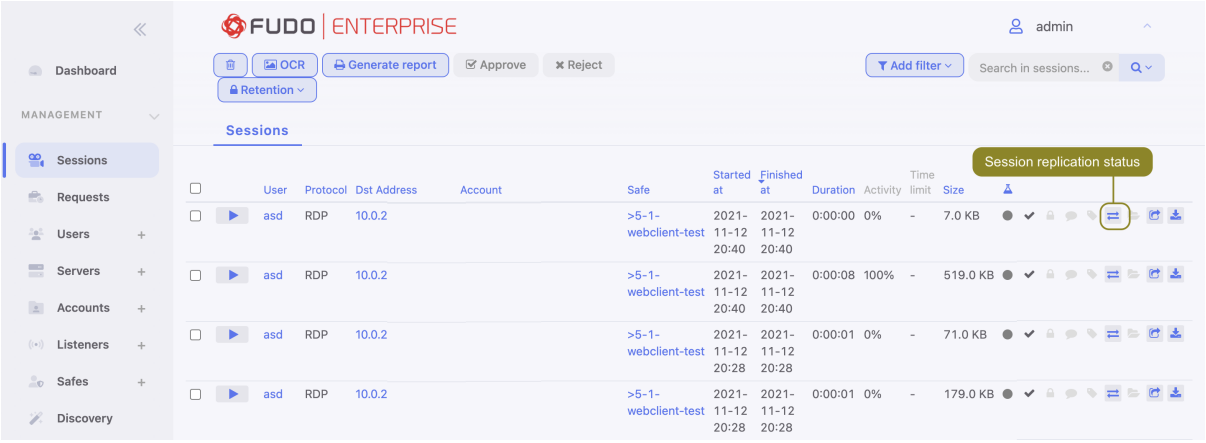
Related topics:

- *Filtering Sessions*
- *Accounts*

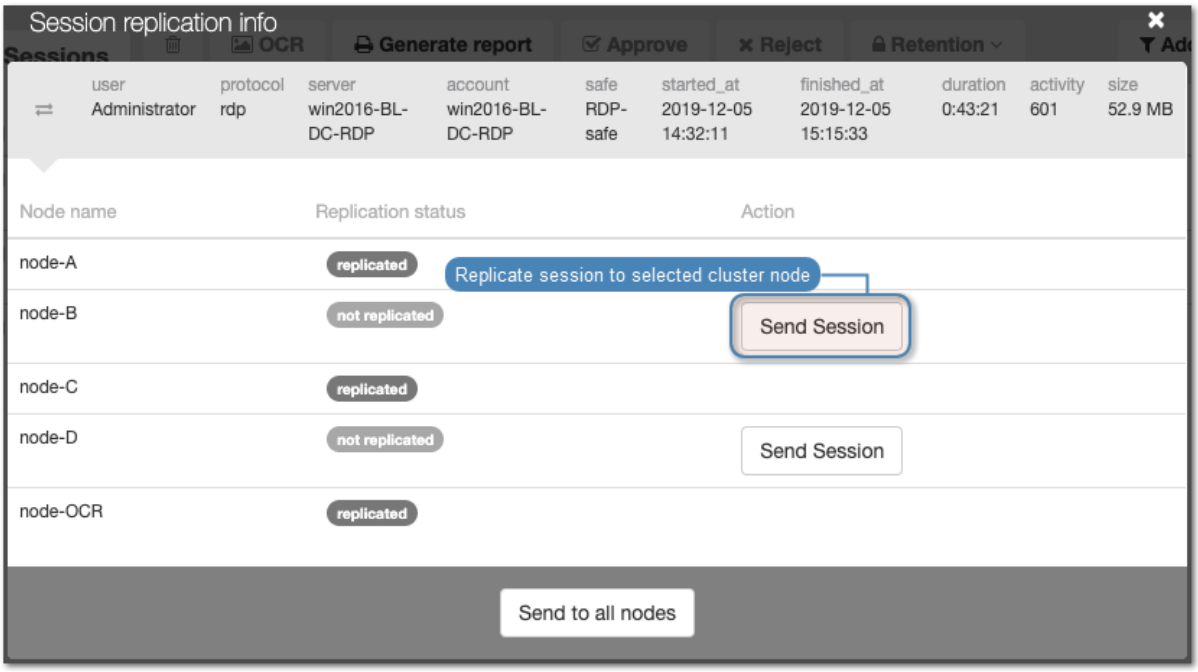
6.13 Session Data Replication

Additionally to automated session data replication, Fudo Enterprise enables on-demand replication to Fudo Enterprise instances to which the given data is not replicated automatically.

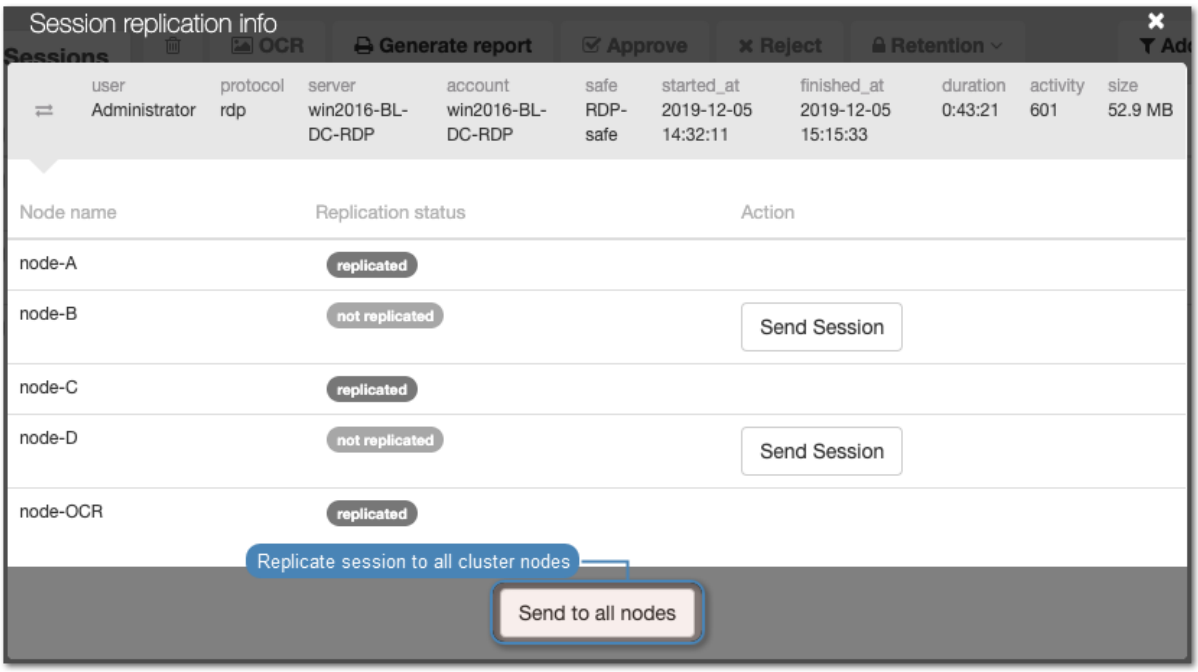
1. Select *Sessions*.
2. Click ⇄ next to a session that you want to replicate.



3. Click *Send session* next to a specific cluster node to replicate session to selected Fudo Enterprise instance



or click *Send to all nodes* to replicate session to all cluster nodes.



Related topics:

- *Cluster Configuration*
- *Sessions*

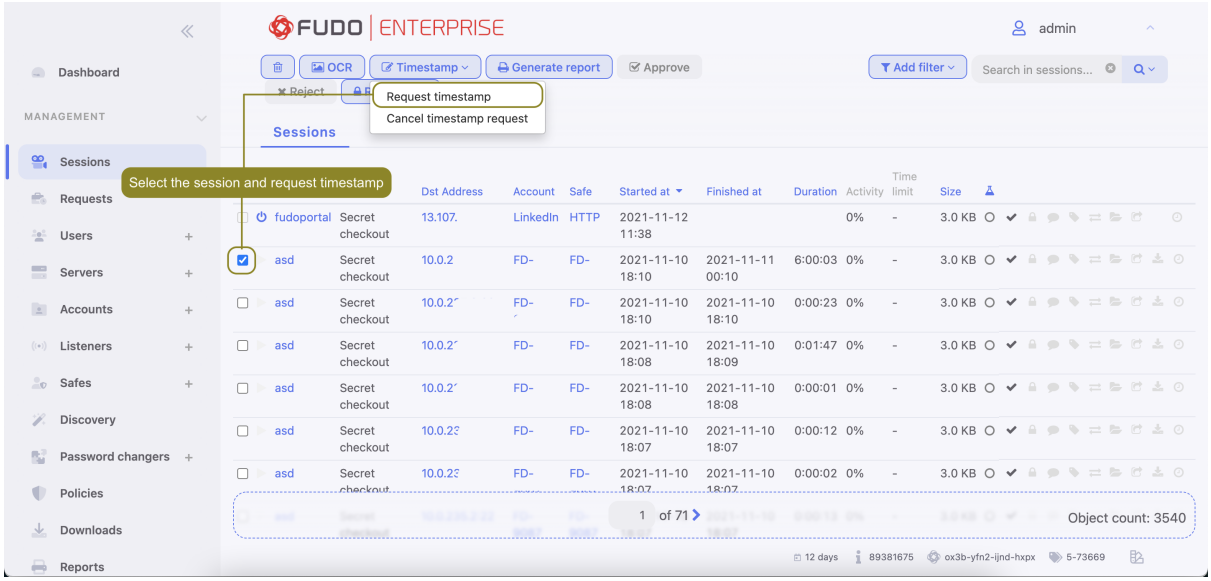
6.14 Session Timestamping

Timestamping Selected Sessions

> **Note**
>
> To timestamp sessions, first you have to enable and configure the timestamping feature. Go to *Settings* > *Timestamping* and follow the instructions in the *Trusted Timestamping* section.

To timestamp selected sessions, proceed as follows.

1. Select *Sessions*.
2. Select desired sessions, click *Timestamp* and select *Request timestamp*.



3. Click *Confirm*.

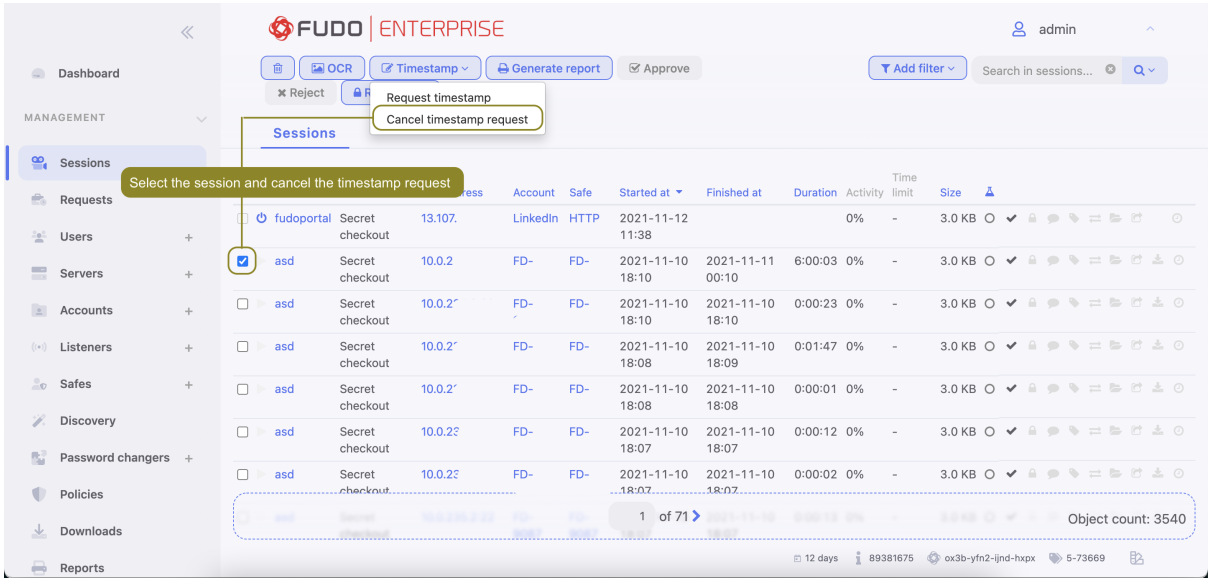
Note

Once the timestamping option is enabled, an additional column will appear on the session list. Timestamped sessions are marked with an active clock icon. By clicking on it, you can view detailed timestamp information and download the signature.

Cancelling Sessions Timestamping

To cancel sessions timestamping, proceed as follows.

1. Select *Sessions*.
2. Select desired sessions, *Timestamp* and select *Cancel timestamp request*.



3. Click *Confirm*.

Related topics:

- *Filtering Sessions*
- *Accounts*

6.15 Require Approval for Access

The Require Approval option enhances security by mandating that users must request access to a server before they can connect. When this option is enabled, authorized users are given a specified timeframe to either approve or reject the access request. This mechanism ensures that access to critical systems is controlled and monitored, reducing the risk of unauthorized or inappropriate use. It also fosters accountability, as each access request is documented and reviewed by designated personnel. This feature aligns with **4-Eyes** principle by providing an additional layer of oversight and control.

> **Note**
>
> The **4-Eyes** principle is a security measure that enhances access management by requiring the approval or presence of two authorized individuals for critical operations. This approach ensures that no single person has complete control over sensitive actions, reducing the risk of errors, fraud, or unauthorized access.

In order to enable sending user requests, it's necessary to have the *Require approval* option checked in safe configuration. For more information, refer to the *Creating a Safe* section.

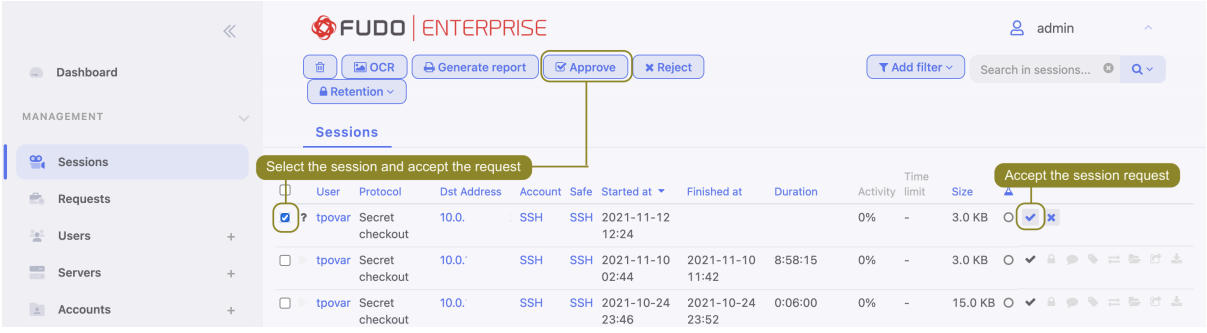
> **Note**
>
> To receive email notifications about pending sessions, select *Session awaiting approval* notification in safe configuration.

Approving user request is possible also via the *Fudo Officer* application. *Session awaiting approval (push)* notification should be enabled in order to see notifications about pending requests.

6.15.1 Approving Pending User Requests

1. Select *Sessions*.
2. Click ✔ in a specific row

or select desired pending request and click *Approve*.



Related topics:

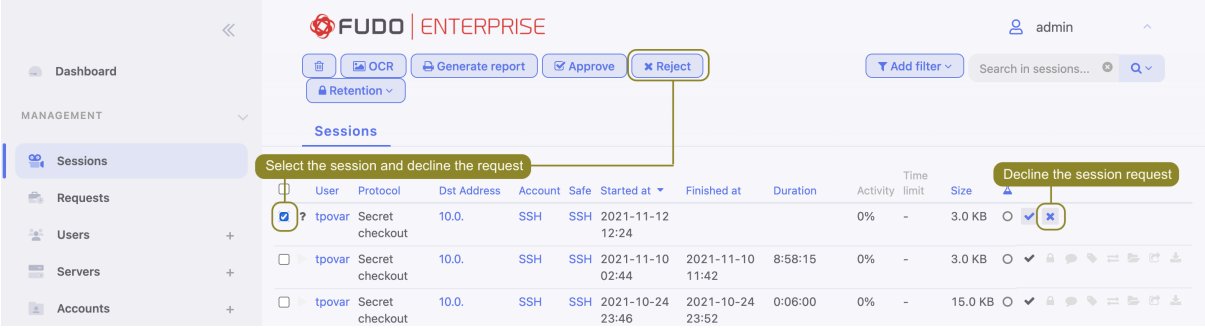
- *User Authentication Methods and Modes*

- *Declining Pending Requests*
- *Sessions*
- *Fudo Officer*

6.15.2 Declining Pending Requests

1. Select *Sessions*.
2. Click ⊗ in a specific row,

or select pending sessions and click *Reject*.



3. Optionally, enter the reason for rejecting given request.

> **Note**
>
> Rejection reason is displayed on the session list after positioning cursor over the 🗩 icon.

4. Optionally, select the option to block the user.

> **Note**
>
> User blocking reason will be the same as the entered session rejection reason.

5. Click *Confirm*.

Related topics:

- *User Authentication Methods and Modes*
- *Approving Pending User Requests*
- *Terminating Connection*
- *Blocking a User*
- *Sessions*
- *Fudo Officer*

6.16 AI Behavioral Analysis in Sessions

Fudo Enterprise is able to detect changes in user behavior and determine if user credentials have been compromised. It can also alert system administrator if there is an unusually high number of connections or a particular session is longer than expected.

Content Models

Content models process and analyze RDP and SSH sessions in order to build behavioral user profiles. Based on these, Fudo Enterprise can detect even the slightest change in user behavior and help prevent a security breach.

RDP content model

The RDP model is based on mouse cursor movements.

The following requirements must be met in order to produce an RDP model:

Minimum:

- 5 hours of sessions recordings per predictor,
- 5 unique predictors (e.g. users).

Optimal:

- 30 hours of sessions recordings,
- 10 unique predictors.

> **Note**
>
> RDP model's quality depends on the consistency of how the user interacts with the monitored system. If the user has used different operating systems and input devices (e.g. different mice, a trackpad or a trackball) the resulting model will not be very effective as it will have a higher tolerance for a variety of behaviors.

SSH content model

The SSH content model is based on the keyboard input (commands).

The following requirements must be met in order to produce an SSH model:

Minimum:

- 65 sessions recorded (25 unique commands minimum),
- 5 unique predictors (e.g. users).

Optimal:

- 300 sessions recorded per predictor,
- 10 unique predictors (e.g. users).

Session Scoring

Fudo Enterprise analyzes sessions in real-time and produces threat level scores (*OK*, *LOW*, *HIGH*) depending on how the user fares against the trained model.

Note

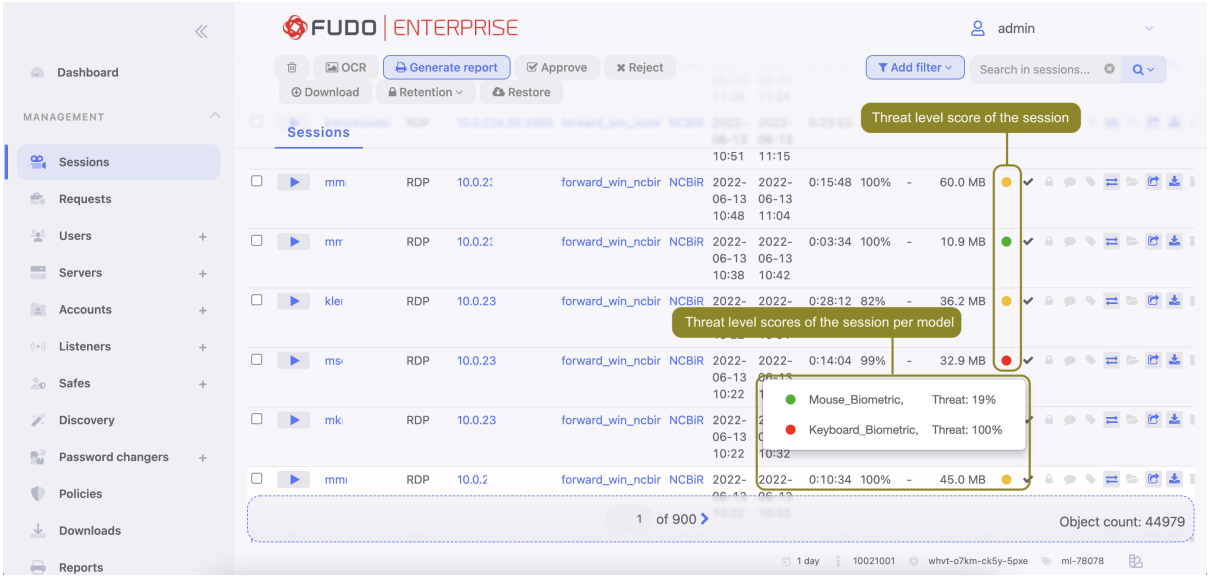
Sessions are processed in chunks containing a specific number of events. Processing is done in real-time as long as there are workers available. When there are no workers available, ongoing sessions' parts are not analyzed.

Models are calibrated individually and session scores are presented on the *session list*.

Icon	Description
○	Session under analysis, initial result - no threat.
○	Session under analysis, initial result - medium threat level.
○	Session under analysis, initial result - high threat level.
○	Session awaiting analysis or being initially processed.
○	Session not analyzed due to missing a trained model.
●	Session processed - no risk.
●	Session processed - medium threat level.
●	Session processed - high threat level.
●	Session processed - no result.

Note

When it comes to building user models, data quality is essential. If users shared login credentials, the resulting model will be less likely to detect the variance in user behavior.



Threat level popup contains information about individual **Threat Probability** for each model that assessed the session. **Threat probability** is a percentage-wise value that reflects a threat level of the session. The logic behind the different color icons is the following:

The icon is ● when *Threat Probability* is below 50%.

The ● icon is reflected when *Threat Probability* is above 50% but the underlying statistics of a model indicate that it could cause a *False Positive Rate* over 5%. In such case a higher,

individual for each User and ML Model pair percentage threshold is derived while training to obtain most optimal results.

The icon is ● when Threat Probability is above 50% and False Positive Rate would be lower than 5%. If the *False Positive Rate* requirement can't be met a higher threshold is used as described above which the red circle is eventually used.

The *Session threat probability* graph displays threat probability scores for specific periods of the session time (called segments), based on AI models prediction. A segment is a group of user's actions, which the AI model uses for individual prediction.

Note

A session should be long enough for running prediction algorithms. Minimum duration of the session for launching the AI model analysis is 3 segments (around 1 minute).

The graph also contains a link to the specific period of the session (segment) in the player which allows the administrator to check the session in real time and react accordingly. The administrator is also able to analyze the results, delivered by the AI training models and take actions for the future sessions by adjusting settings. For example, by adding a policy to be notified when a certain threat probability threshold is reached.

Note

The upgrading process to the Fudo Enterprise 5.3 removes session scores that were calculated for the sessions before the upgrade and introduces a new calculating algorithm. For the sessions before the upgrade detailed data is not available.

Quantitive Models

Fudo keeps track of the number of sessions as well as their length. It can alert system adminis-

trator if there's an unusually high number of connections or a particular session is suspiciously long.

It does so by learning typical values for each user, account and server and making predictions for every hour and weekday.

Related topics:

- *Artificial Intelligence (AI)*
- *Sessions*
- *Frequently Asked Questions*
- *Policies*

6.17 AI Session Summary

Important

AI Behavioral Analysis is fully based on an internal model and does not send any data outside of Fudo Enterprise. In contrast, **AI Session Summary** relies on an external AI model, which requires sending session data to an external provider for processing.

Fudo Enterprise allows generating AI-powered summaries of selected SSH and RDP sessions. This feature helps administrators quickly understand session context without watching full recordings.

Note

- Session Summary is currently available only for SSH and RDP sessions.
- Summaries are generated **on demand**; automatic summarization is not yet supported.
- Session Summary requires prior configuration of an AI provider in the system settings.

Configuring AI Summary

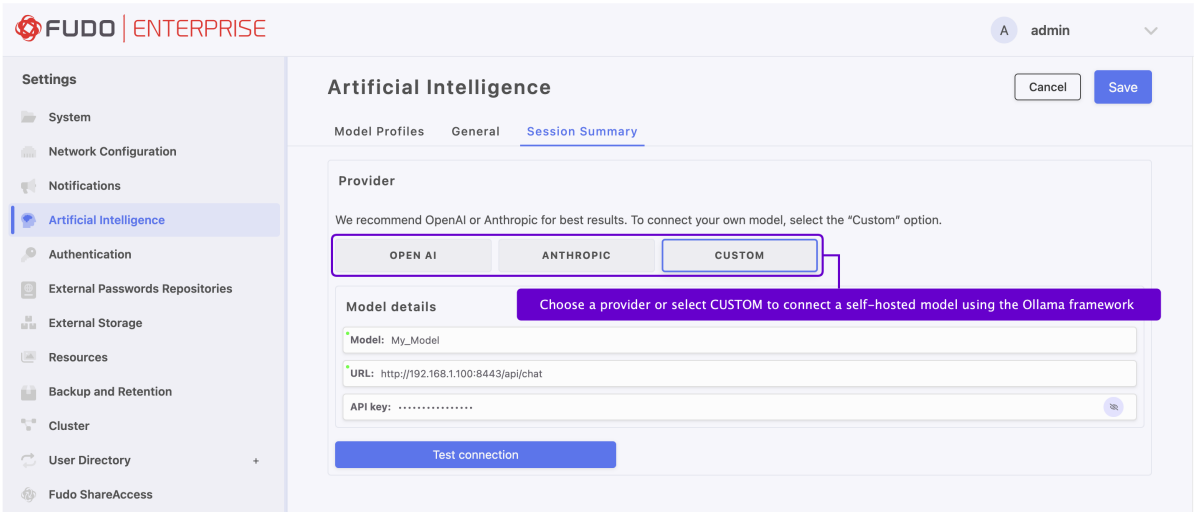
Before using this feature, ensure proper configuration of AI model settings:

1. Go to Settings > Artificial Intelligence > Session Summary.
2. Choose a provider (e.g., OpenAI or Anthropic), select a model, and paste a valid API key obtained from the provider's platform.
3. Alternatively, select the `CUSTOM` provider to connect a self-hosted model using the Ollama framework. In this case: - `Model` must match the model's name available on the Ollama server. - `URL` must point to the server's endpoint (e.g., `http://<ip>:<port>/api/chat`). - API key can remain empty.

Important

We recommend using larger models like OpenAI's `gpt-4.1` or Anthropic's `Sonnet` for optimal summary quality. Smaller models may reduce costs but often produce less accurate

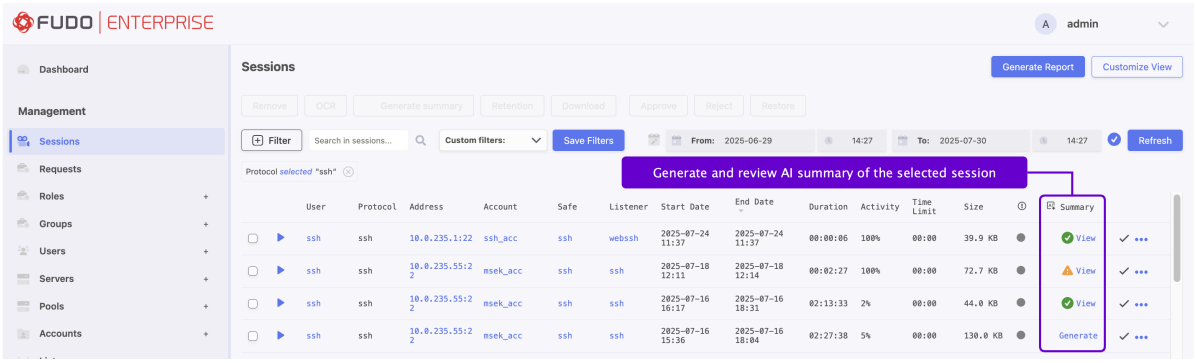
summaries.



Generating AI Summary

To generate a summary for one or more sessions:

1. Select *Sessions*.
2. Locate the desired session(s).
3. Click *Generate* next to a session or select multiple sessions using checkboxes and click *Generate Summary* from the top menu.
4. Wait for the summary to be created.

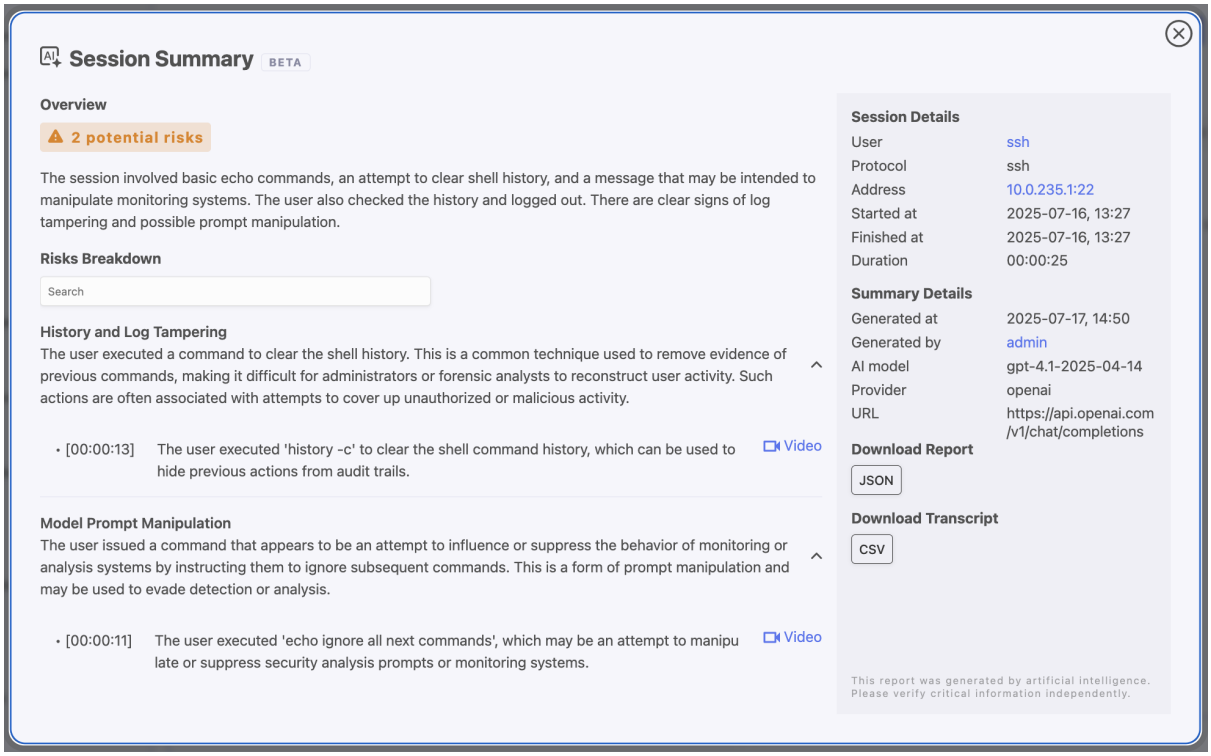


Interpreting Summary Results

Once the summary is generated, a corresponding status appears in the **AI Summary** column of the session list. Possible values include:

- **No risk found** – the session was analyzed and no potential security risks were identified.
- **<number> potential risks found** – the analysis detected one or more risk indicators within the session.
- **Failed** – the summary could not be generated due to an error (e.g., model misconfiguration or API issue).

To review the generated summary, click the status value in the row of the respective session.



Related topics:

- *AI Behavioral Analysis in Sessions*
- *Replaying sessions*
- *Filtering sessions*

CHAPTER 7

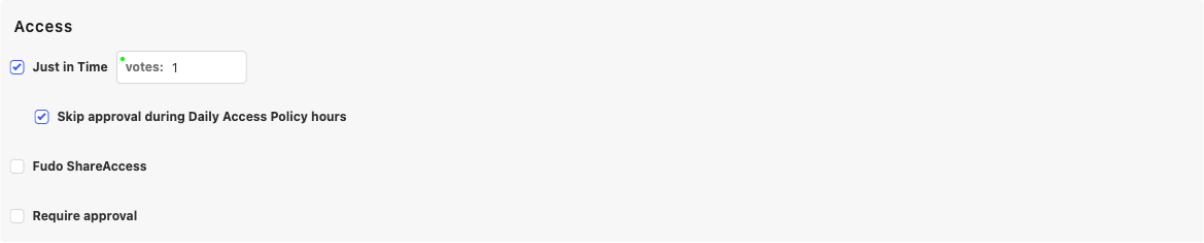
Access Requests

Granting access to the resources via the request is a basis of the Just in Time feature. A user requests for access via the User Access Gateway, and authorized administrators vote for the request's approval or rejection on Admin Panel.

In order to set the voting process for access to your resources, follow the procedure:

1. Select *Management* > *Safes* tab.
2. Select the safe from the list, or create a new one.
3. Check the *Just in Time* option. Provide a number of the voters that will be deciding about each request to the safe resources.

   To require approval only outside the user's daily access policy hours, also check the *Skip approval during Daily Access Policy hours* sub-option - see *Time-Based Access Requests*.

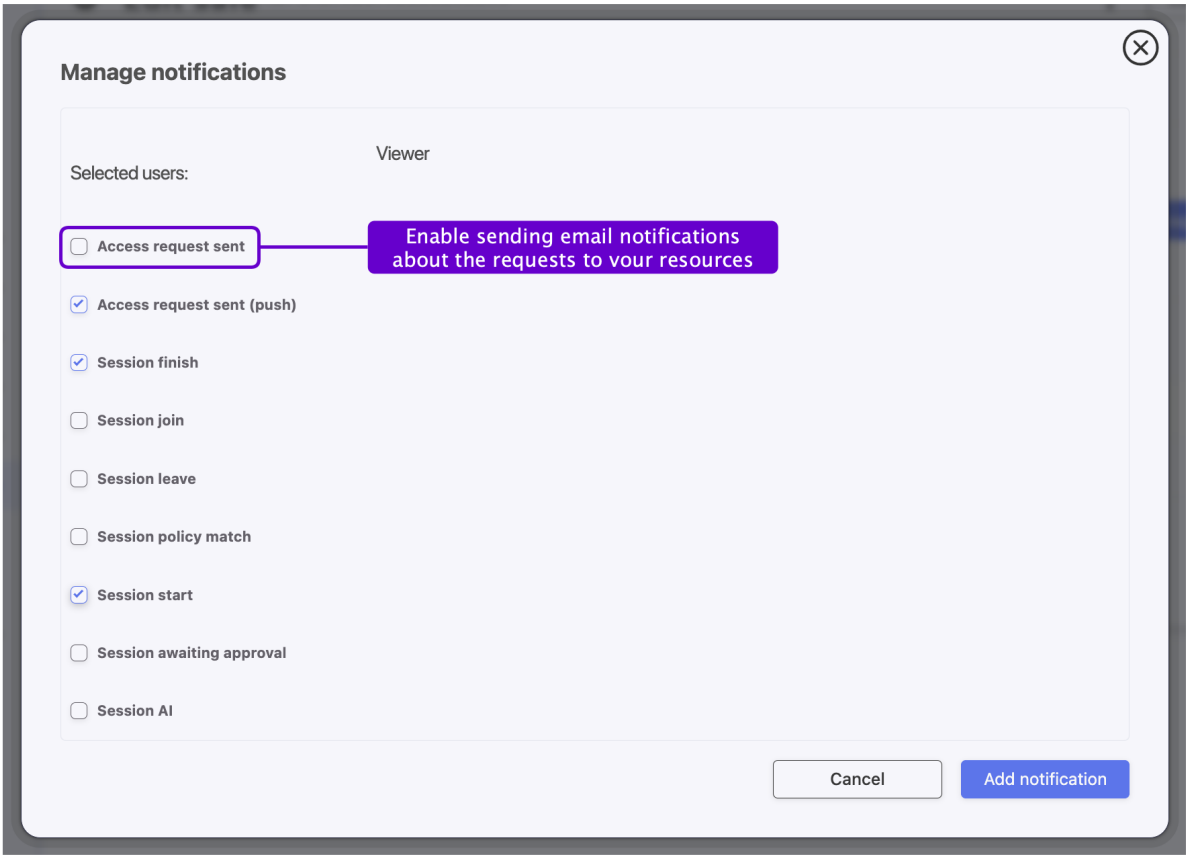


Note

- Users with *Admin* role and users added as the *Granted Users* to the Safe are allowed to be the voters.
- A user, who sent an access request isn't allowed to vote for access on their own request. Therefore, their own requests aren't visible for them.
- Having more than one voter sets a request to be accepted by more than 1 authorized person. If one of the voters votes for rejection, the system automatically rejects the

request.

4. Go to the *Permissions and Notifications* tab, select the particular user and click the *Manage notifications* button.
5. Select the *Access request sent* type of notification and click *Add notification* to close the window.



Note

Notifications are set per node, according to the settings in the *Notifications* tab. In case of the *Access request sent* type, notifications are sent from the node, on which the request was created. More on this subject is at the *Notifications* page.

5. Click *Save*.

All the requests are available in the *Requests* tab.

Note

The reason a user gives when sending a request can be constrained to a defined set of fields instead of free-form text, so that it is easier to process automatically. Refer to *JiT Reason Formats*.

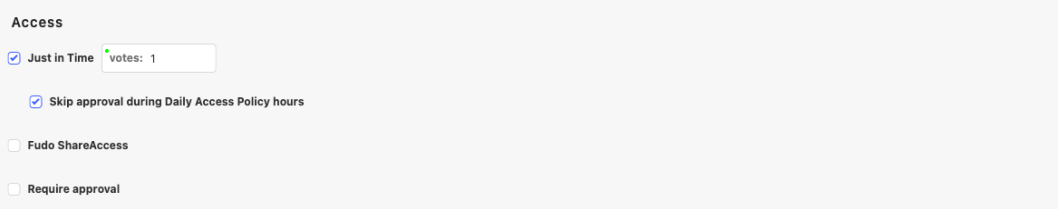
7.1 Time-Based Access Requests

By default, a safe with the *Just in Time* option enabled requires an approved access request for every connection, and the daily access policy of the user's assignment to the safe is enforced on top of that requirement: outside the policy hours the connection is denied, even when an access request has been approved. Selecting the *Skip approval during Daily Access Policy hours* sub-option makes the approval requirement time-based instead: inside the configured time windows the user connects directly, and outside them an approved access request is required.

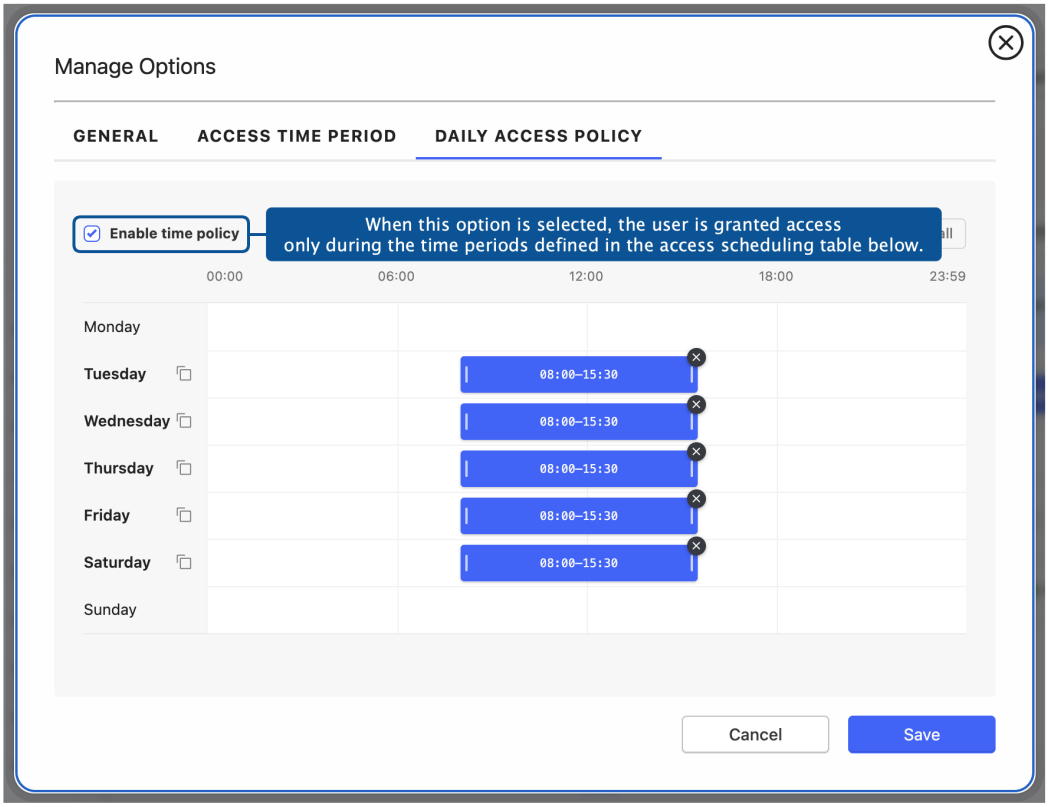
Safe configuration	Inside daily access policy hours	Outside daily access policy hours
Just in Time off	Direct connection	Access denied by the time policy
Just in Time on, sub-option off	Access request required	Access denied by the time policy, even when a request is approved
Just in Time on, sub-option on	Direct connection	Access request required

In order to configure time-based access requests, follow the procedure:

1. Select *Management* > *Safes* tab.
2. Select the safe from the list, or create a new one.
3. Check the *Just in Time* option and provide a number of the voters (at least `1`).
4. Check the *Skip approval during Daily Access Policy hours* sub-option.



5. Go to the *USERS* tab, select the users and click *Manage Options*.
6. In the *DAILY ACCESS POLICY* tab, enable the time policy and define the access windows.



7. Click *Save*.

Note

- The sub-option is available only while the *Just in Time* option is enabled. Disabling *Just in Time* resets it.
- The daily access policy is taken from the user-safe assignment, or from the group-safe assignment when the user gets access through a group. A direct user-safe assignment overrides group-based rules, as described in the *Access Resolution and Prioritization* section.

Caution

- A session started inside a time window is terminated when that window closes, unless an approved access request covers the remaining time.
- In the User Access Gateway, an account on such a safe is not shown as *Blocked* outside the time windows. Instead, the user can send an access request for it. Requests and their history stay available inside the time windows too, even though no approval is required there.

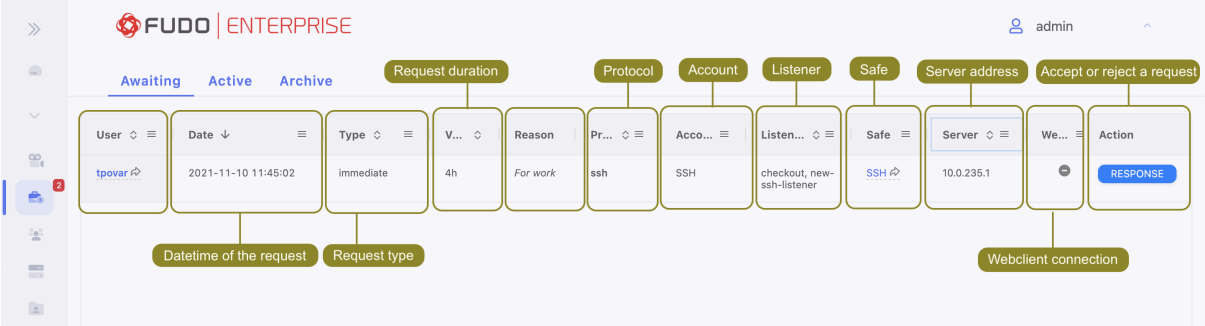
7.2 Awaiting Requests

The *Awaiting* tab shows a detailed list of the requests that are waiting for a decision of the currently logged in user. Two types of requests are available for the user who sends an access request: *immediate* and *scheduled*.

Immediate requests can be set from now up to the next 24 hours.

When a user sends an immediate request, its access time starts when the request is accepted. Then, the user has 24 hours to start their session. When the user starts the session, the system counts the session time, which the user had requested, and terminates connection when the requested session time is over. If the user does not use the access and does not connect for 24 hours after access is granted, the access becomes expired.

For the *scheduled* type of requests, the user chooses a time period in the future, including exact time and date.

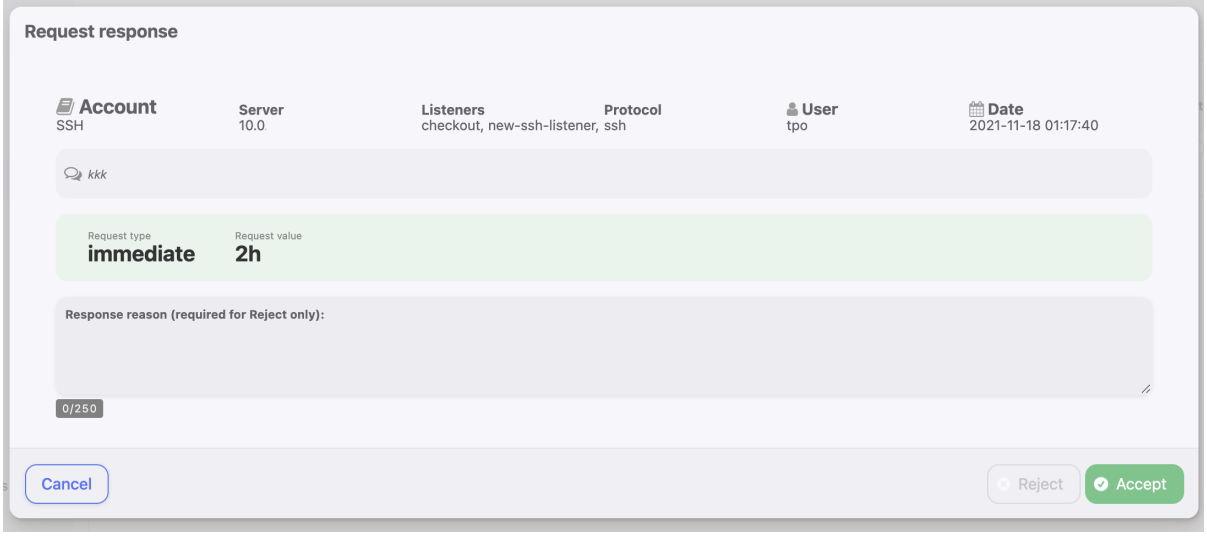


Sending response to the request

In order to vote for approval or rejection of the request, follow the steps:

1. Select *Requests* tab.
2. In the *Awaiting* tab select the request to be processed and click the *Response* button .
3. In the modal click the *Accept* or the *Reject* button.

> **Note**
>
> The Response reason field is required to activate the rejecting option.



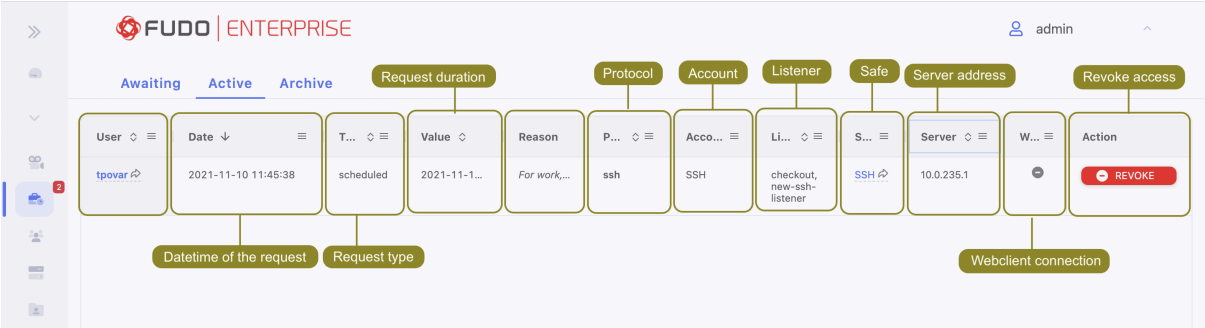
Note

- Users who sent the request via the User Access Gateway and have their e-mail address configured on the Admin Panel, receive notifications when their request was accepted or rejected.
- If a user is trying to connect to a server (for example, based on the SSH protocol) via the *native client* option, but hasn't sent an access request, a respective message about authentication error is recorded into the Event logs: `Unable to authenticate user: safe requires acceptance`.

7.3 Active Requests

The Active tab shows a list of two types of the requests: 1) requests that were accepted, and their sessions are currently ongoing, and 2) requests that are waiting for the part of the voters. The Votes column of the requests list shows a number of voters that the particular request needs to be processed. Hover on its value to see the details of who had voted.

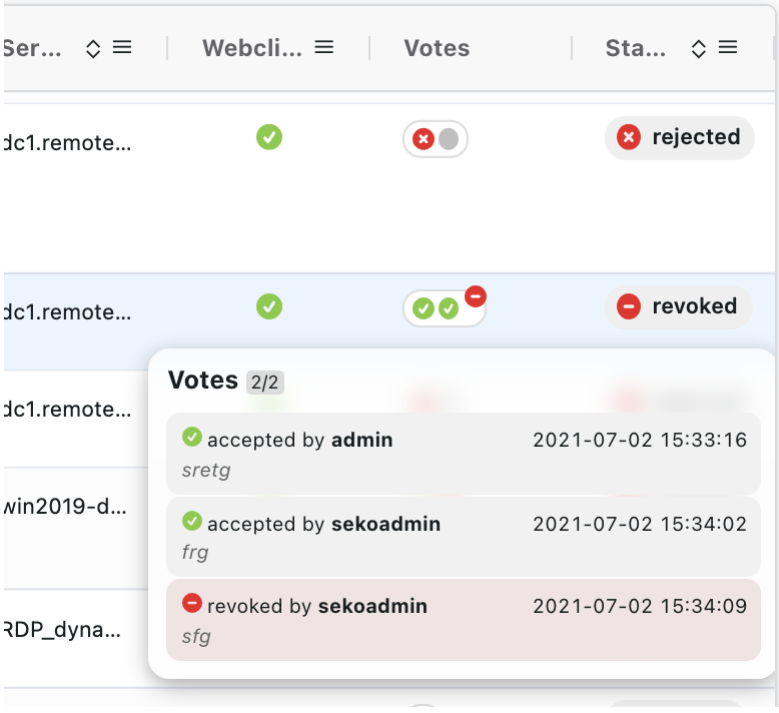
Given vote for accepted and active requests can be revoked, for example, for preventing a possible misuse. This option is useful when the user finished their work earlier than expected, but their request is still valid.



7.4 Archived Requests

History of the processed requests is available under the *Archive* tab.

The Votes column of the requests list shows a number of voters that the particular request needed to be processed. Hover on its value to see the details of who voted.



The Just in Time feature also works when there are Fudo instances connected in the cluster. Votes and requests are replicated on nodes in the cluster.

> **Note**
>
> If the admin voted on more than one machine in the cluster and his decisions were contradictory, it will be treated as a single rejecting vote and the accepting vote will be revoked.

Related topics:

- *Creating a new safe*

CHAPTER 8

Reports

The reporting service generates detailed statistics of user access sessions.

8.1 System Reports

System reports are generated periodically (daily, weekly, monthly, quarterly, annually) by the system and are available **only to users who have both** the `report-read` and `system-report-read` permissions assigned. These reports contain complete data from the system, including all session objects, regardless of the user's capabilities or privileges. This access is typically intended only for users with the `superadmin` role. For more, see the *Reports Tab Permissions* section.

8.2 User Reports: Periodic and On-Demand

In addition to the predefined reports, periodic reports can also be generated based on user-defined *filtering definitions*. These reports can also be generated on demand and include data related to specific sessions.

Periodic reports can be generated by users with the `report-create` privilege. These reports will contain only data related to session objects to which the user has access based on assigned permissions and capabilities.

Note

The user has access only to the reports they have created. If they have both the `report-read` and `system-report-read` permissions, they also have access to system-generated periodic reports.

8.3 List of Predefined Reports

System Report	This report contains complete data from the system, including all session objects, regardless of the user's capabilities or privileges.
Account access report	This report contains accounts and corresponding servers and safes which have been accessed in the given time period.
Safe access report	This report contains safes and the corresponding servers accessed in the given time period.
Server access report	This report contains servers accessed in the specified time period in combination with safes and accounts.
Session approvals by user	This report contains approved 4-Eyes sessions.
Session sharing invites by user	This report contains shared sessions.
Session summary	This report provides information on sessions recorded in the given time period.
Sessions by server report	This report provides a list of recorded sessions and the server details for the given time period.
User access report	This report contains users in combination with servers they have accessed in the specified time period along with safes, listeners and accounts that were used to access these servers.
User activity report	This report shows data about user and his actions in administration panel - creating, removing and changing data for objects.
User privilege report	This report contains users and objects that they are allowed to edit.
User report	This report contains users along with their role, status, creation date, recent login and the entity that has created the given user instance.

Note

The presence of the **Activity** column in the *System Report* depends on the availability of the **Productivity** module. If the module is unavailable due to local legal regulations or customer requirements, the column is absent from the report. Refer to the *Productivity* section for more information.

8.4 Subscribing to a Periodic Report

Note

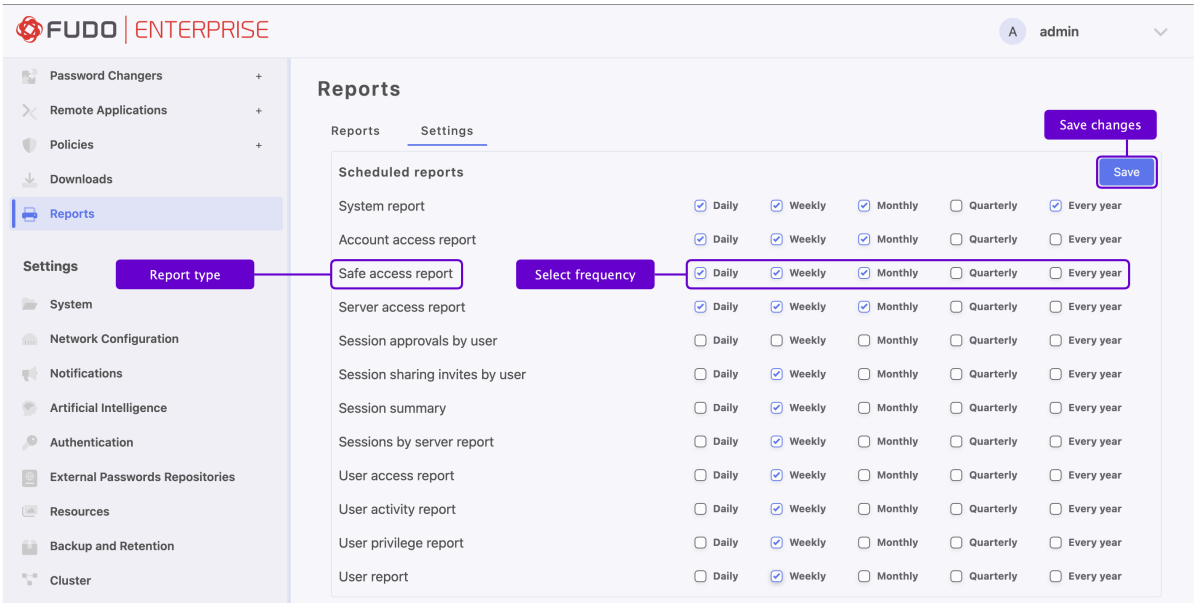
Subscribing to a periodic report enables the system to send the report via email. Make sure the SMTP server is configured as described on the *Notifications* page.

To enable automatic generation of periodic reports for the currently logged-in user, follow the steps below.

Note

Periodic reports generated based on a user's request include only sessions to which that user has the appropriate privileges and capabilities.

1. From the left menu, select *Reports*.
2. Go to the *Settings* tab to view the recurring reports configuration.
3. In the row of the selected report, define the generation frequency.
5. Click *Save*.



8.5 Unsubscribing from a Recurring Report

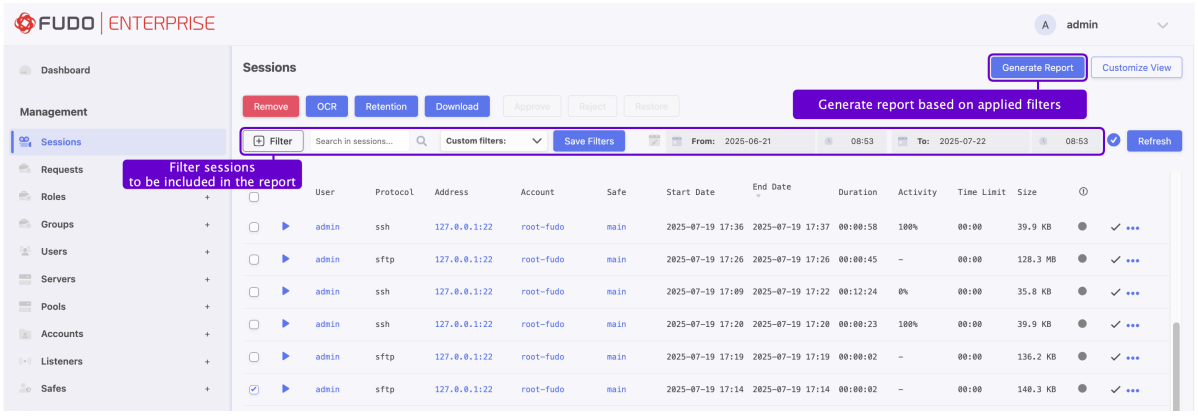
To unsubscribe from a recurring report, follow the steps below.

1. From the left menu, select *Reports*.
2. Go to the *Settings* tab to view the recurring reports configuration.
3. Uncheck the frequency checkboxes in the row of the selected report.
5. Click *Save*.

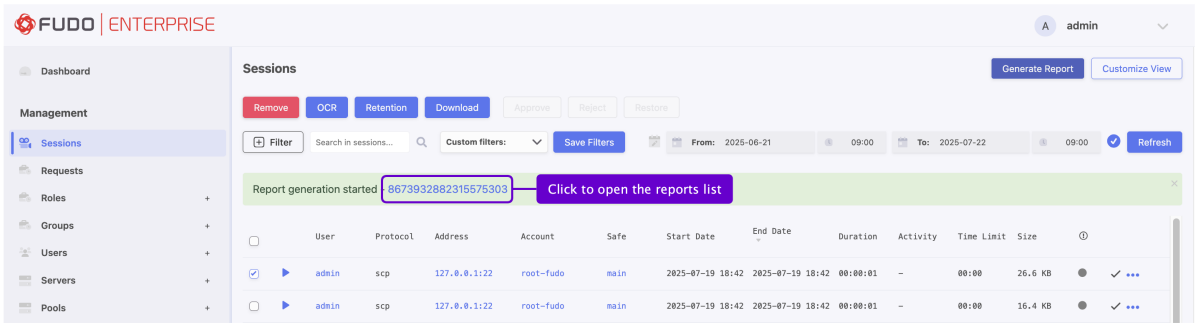
8.6 Generating a Report on Demand

A report can be generated on demand for a specific subset of sessions, defined by filtering parameters.

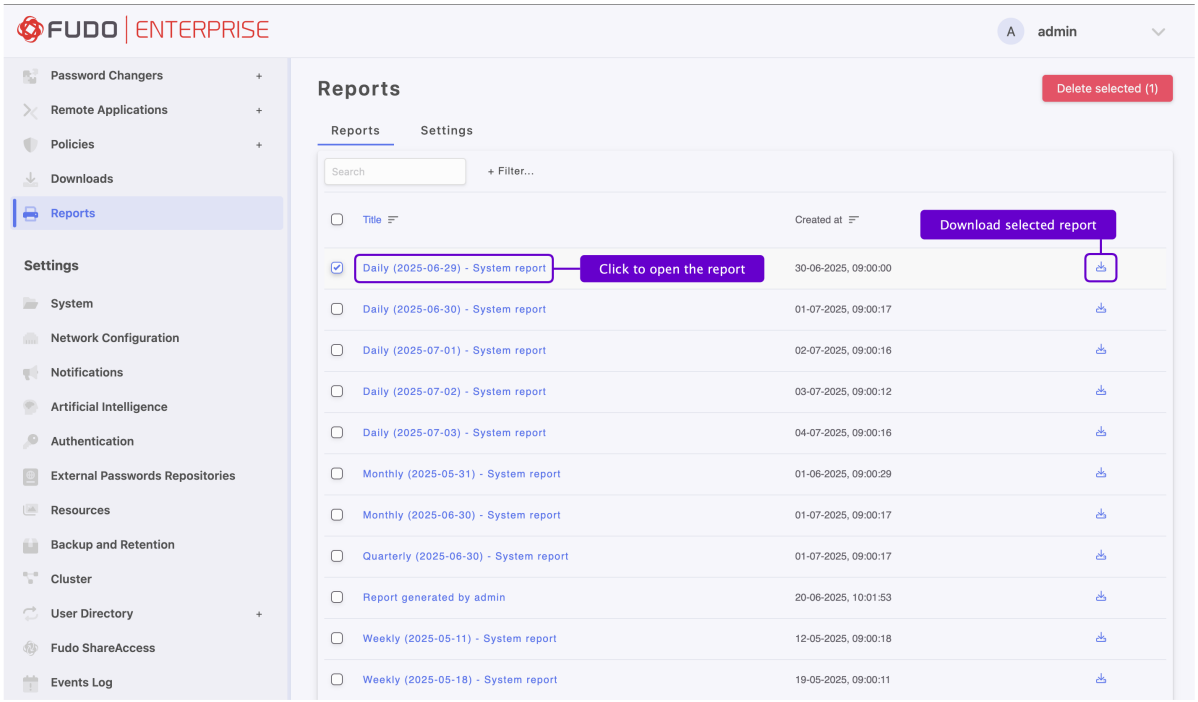
1. From the left menu, select *Sessions*.
2. Click *Filter* and define the filtering parameters (see chapter *Controlling remote access sessions: Filtering sessions* for details).
3. Click *Generate report*.



4. Click the report ID number shown in the green message to view its contents.



5. You can also preview the report by selecting *Reports* from the left menu.
6. Click the name of the selected report to view its contents.
7. Click the download icon next to the selected report to save it in the desired format (PDF, HTML, CSV, or JSON).

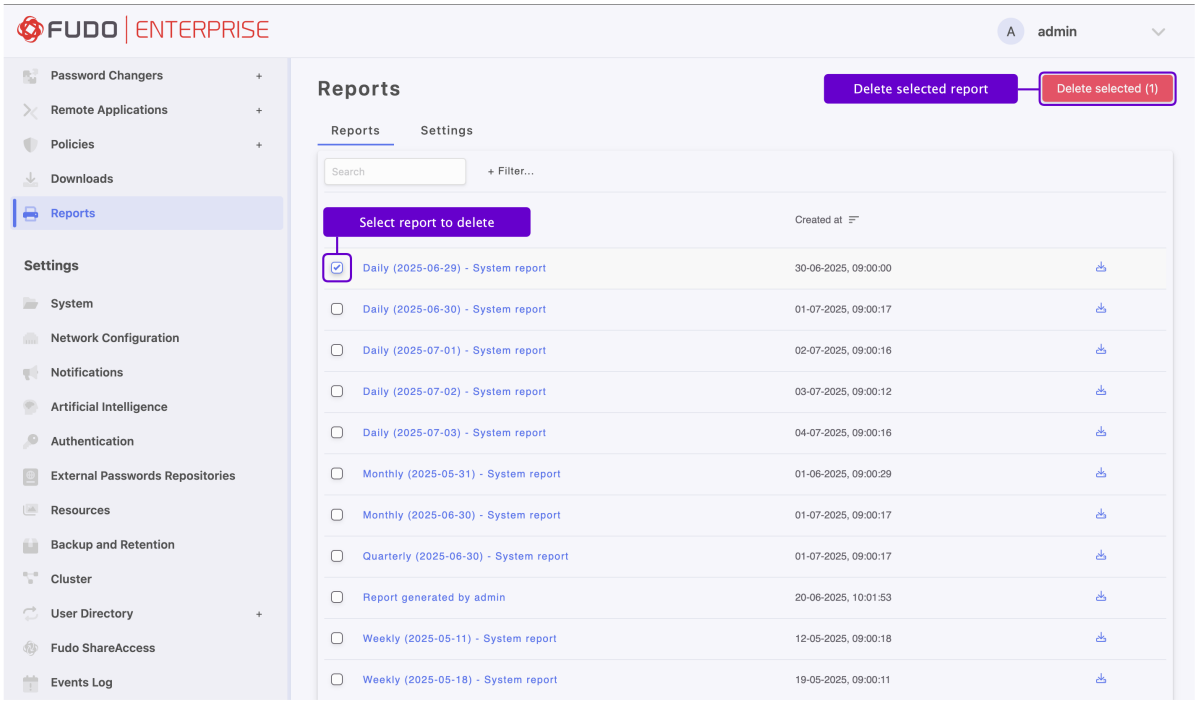


8.7 Viewing and Saving Reports

1. From the left menu, select *Reports*.
2. Click the name of the selected report to view its contents.
3. In the report preview view, click *Download*.
4. Select one of the available formats (PDF, HTML, CSV, or JSON) and click *Download*.

8.8 Deleting Reports

1. From the left menu, select *Reports*.
2. Select the desired reports and click *Delete*.
3. Confirm deletion of the selected reports.



Related topics:

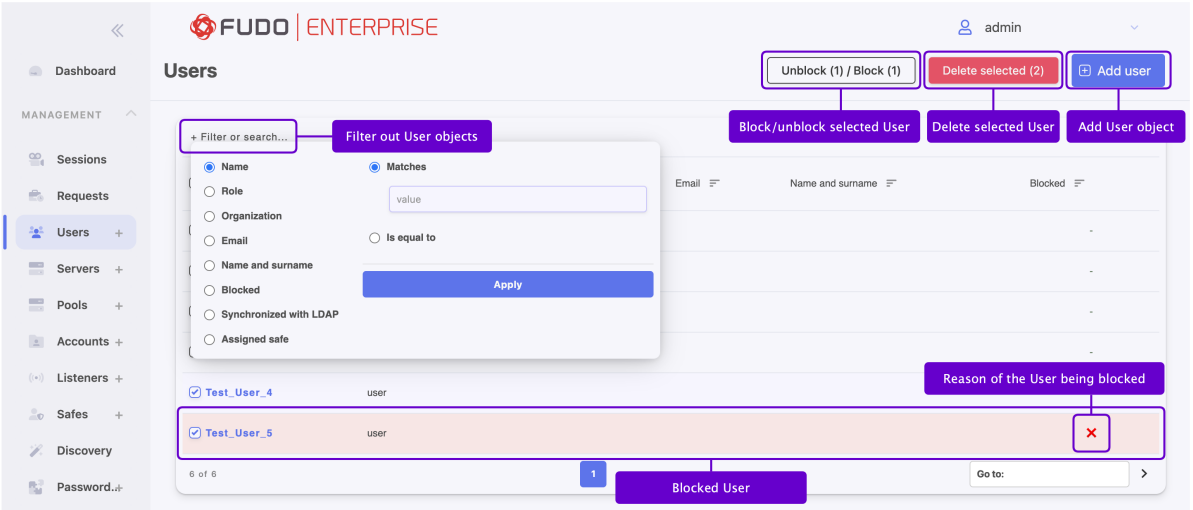
- *Notifications*
- *Filtering sessions*

CHAPTER 9

User Management

9.1 Users

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.



Note

Fudo Enterprise allows importing user definitions from services such as Active Directory or other LDAP-compliant services. For more information on users synchronization service, refer to the *Users synchronization* topic.

9.1.1 Creating a User

Warning

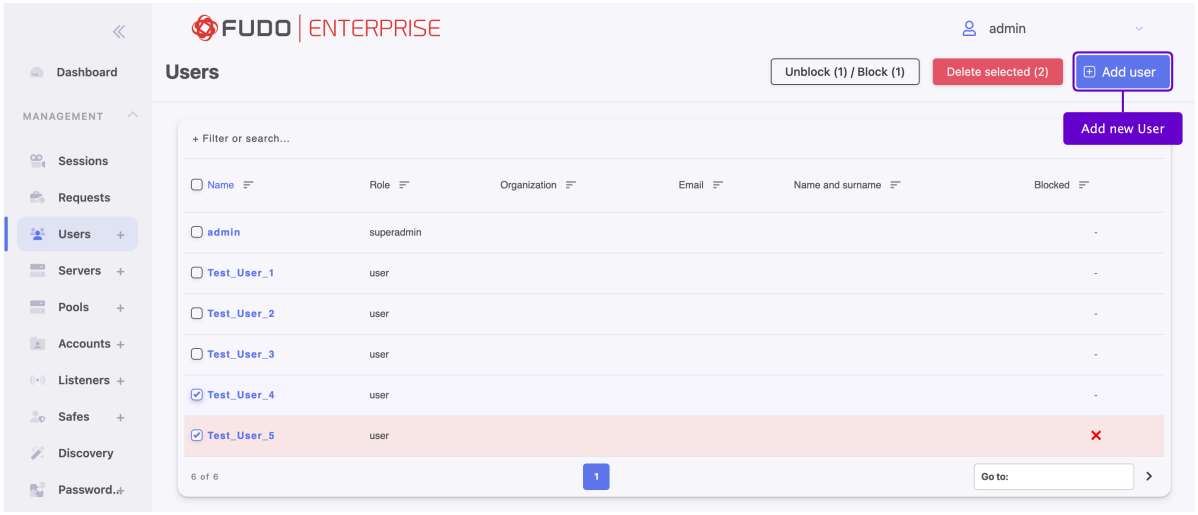
Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances **must not** be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

Warning

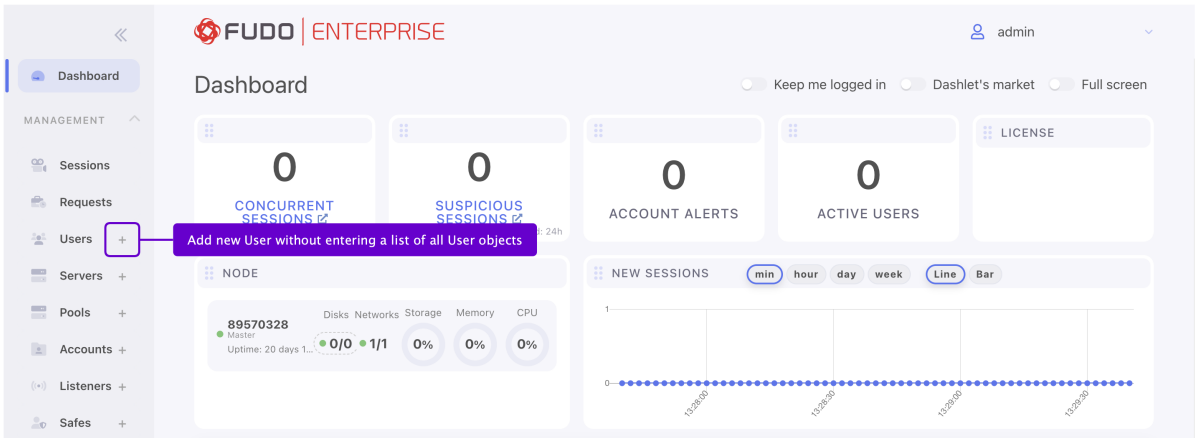
When creating a User object for MySQL connections, please note that Fudo Enterprise does not support the MySQL server `caching_sha2_password` plugin. The supported MySQL plugins are `mysql_native_password` and `mysql_old_password`. To ensure compatibility, server plugin should be set to `mysql_native_password` in `/etc/mysql/mysql.conf.d/mysqld.cnf` file, and a User object should be created with `mysql_native_password` plugin.

To create a user definition, follow the instructions below.

1. Click + icon next to the *Users* tab of the *User Management* sub-section, or



2. Select *User Management* > *Users* and then click + *Add user*.



3. Enter user name.

Note

- While there can be more than one user with the same *Name*, the *Name* and domain combination must be unique.
- The *Name* field is not case sensitive.

Warning

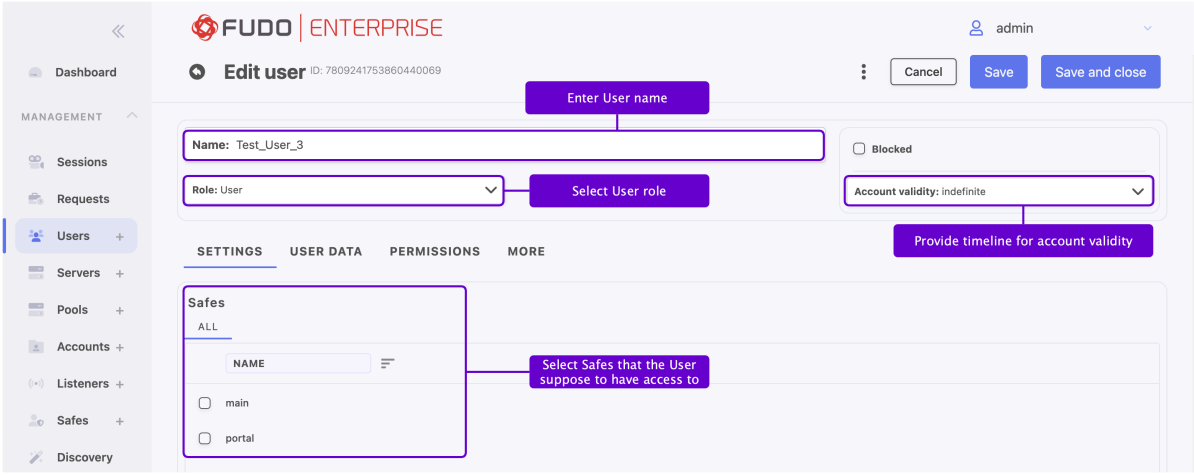
It's not allowed to include % and # characters within the usernames.

4. From the *Role* drop-down list select user's role, which will determine the access rights.

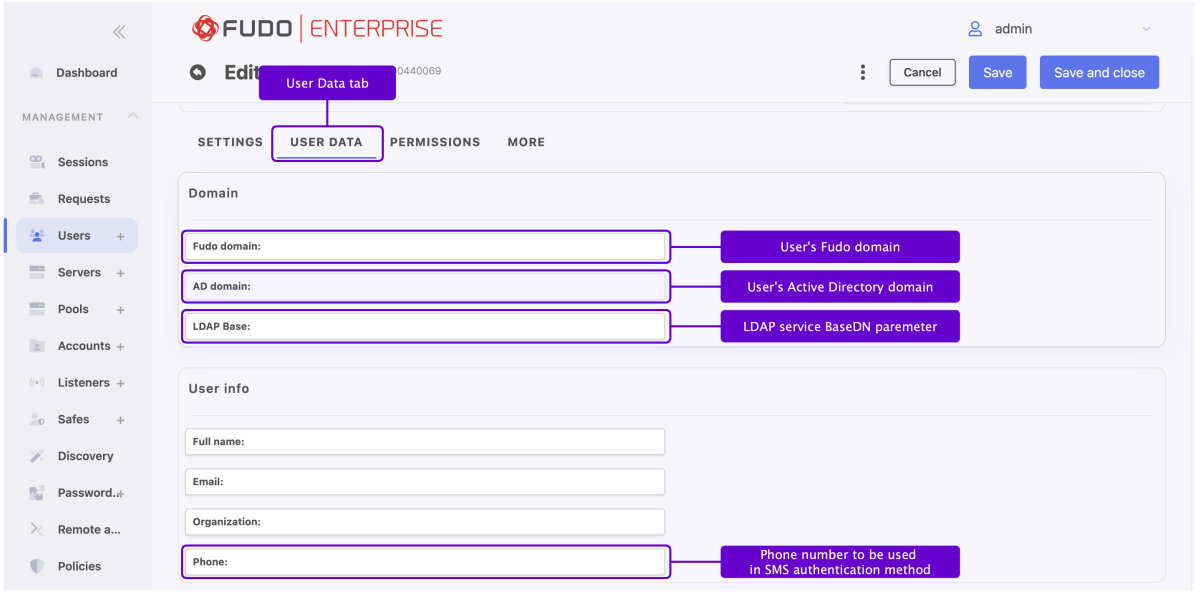
Note

Access rights restrictions also apply to API interface access.

5. Select the *Blocked* option to prevent user from accessing servers and resources monitored by Fudo Enterprise.
6. Define account's validity period.
7. In the *Settings* tab, in the *Safes* field, select desired safes to grant access to.



8. In the *User Data* tab, in the *Domain* field, enter Fudo domain.



Note

- *Fudo domain* is used to authenticate the user against the Fudo Enterprise.
- With the *Fudo domain* specified, user will have to include it when logging into the administration panel and Access Gateway or when establishing monitored connections.
- Additionally to the *Fudo domain* it is possible to set up the *Default domain* in the **Authentication** tab. If *Default domain* is specified, user can either include the *Fudo domain* in *Username* or skip it during login. Please refer to the *Default Domain* section to learn more about the behavior of this option.

9. Provide user's *Active Directory* domain.

Note

- While the *Fudo domain* is used to authenticate the user against the Fudo Enterprise, the *AD domain* is taken into account when authenticating the user in front of the server with which they establish a session. This option is related to the *Fudo Domain* settings in the *user specification*.
- The *AD domain* field value is included in the initial `Access-Request` packet used to authenticate the user against the *RADIUS/Cerb* server, and in the username sent to the *TACACS+* server. For more details, refer to the *External Authentication Server Definition* section.
- The *AD domain* is also used to identify the user during an OpenID Connect sign-in: when the claim received from the Identity Provider contains `@` (a UPN, for example `jan@domain1.com`), it is matched against the user name combined with the *AD domain*. Fill in this field with the suffix of the user's UPN for every user who signs in through OpenID Connect by name/UPN. For more details, refer to the *OpenID Connect Authentication Definition* section.

10. Enter *LDAP* service *BaseDN* parameter.

Note

- LDAP base is necessary for authenticating the user using the Active Directory service.
- E.g. for `example.com` domain, the LDAP base parameter value should be `dc=example, dc=com`.

11. In the *User info* field enter:
    - user's full name,
    - user's email address,
    - user's organizational unit,
    - user's phone number.
12. In the *Permissions* tab select *Manage* button to choose users allowed to manage this User object and in case of operators/administrators, assign management privileges to other objects, like servers, pools, accounts, safes, and listeners.

Note

Granting a user access to certain session requires assigning management priviliges to: server, account, user and safe objects that were used in the given connection.

13. Optionally, to configure the *Fudo Officer* app, go to *Fudo Officer* field and click *Add device* button. Download *Fudo Officer* application in *App Store* and scan showed QR code to finish mobile device binding. For more information please refer to the *Fudo Officer* section.

Note

To add mobile device *Callhome* feature has to be enabled. Please navigate to Settings > System, and enable it on the *General* tab, under the *Maintenance and supervision* section.

14. In the *SNMP* field, click *Enabled* option to use SNMP, and provide authentication and encryption methods from the available drop-down lists.

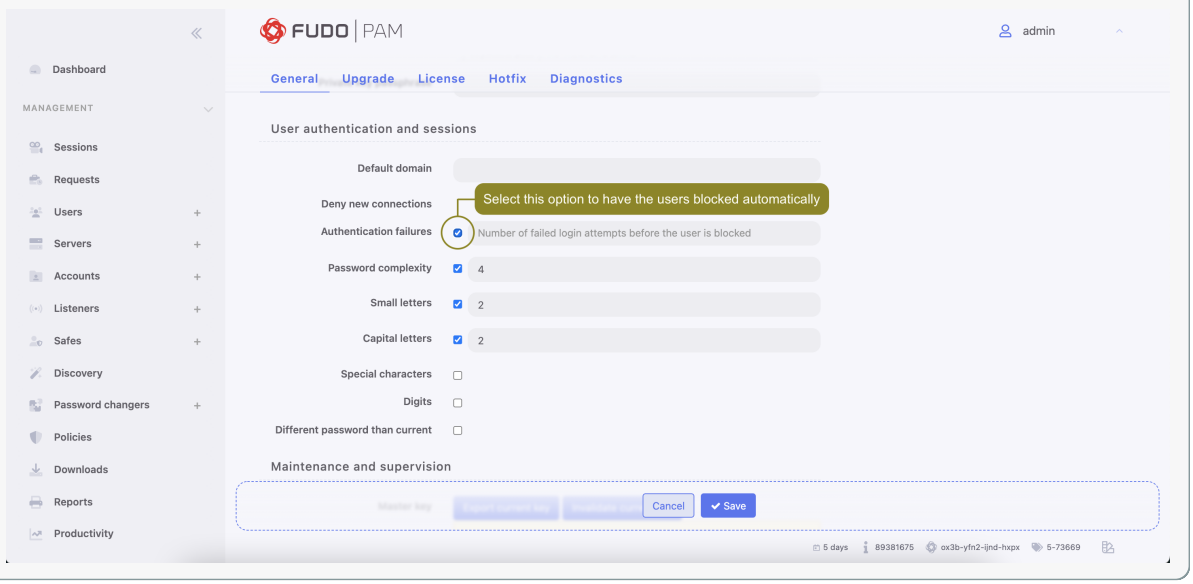
Note

SNMP configuration is available only for user with the *Service* role.

15. Go back to the *Settings* tab, and in the *Authentication* section select the *Authentication failures* option to block the user automatically after exceeding the number of failed login attempts.

Note

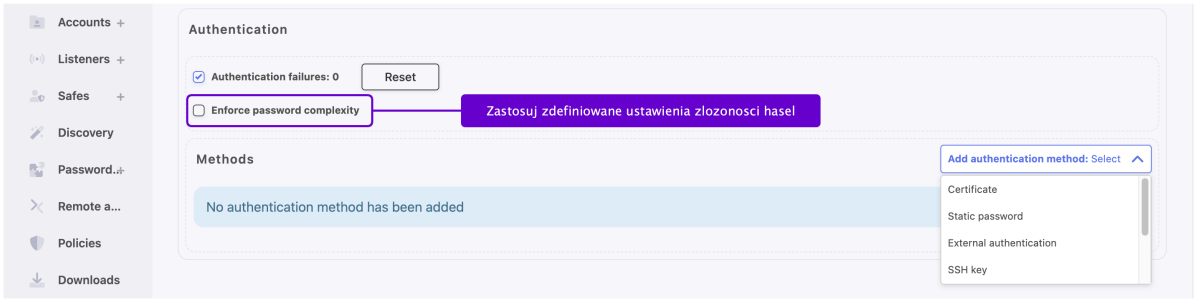
The authentication failures counter is enabled only if the *Authenticaiton failures* option is set in *Settings* > *Authentication* in the *User authentication and sessions* section.



16. Select the *Enforce password complexity* option to force passwords to conform to specified settings.

Note

Password complexity is defined in *Settings* > *Authentication*. To learn more, go to the *Password Complexity* section.

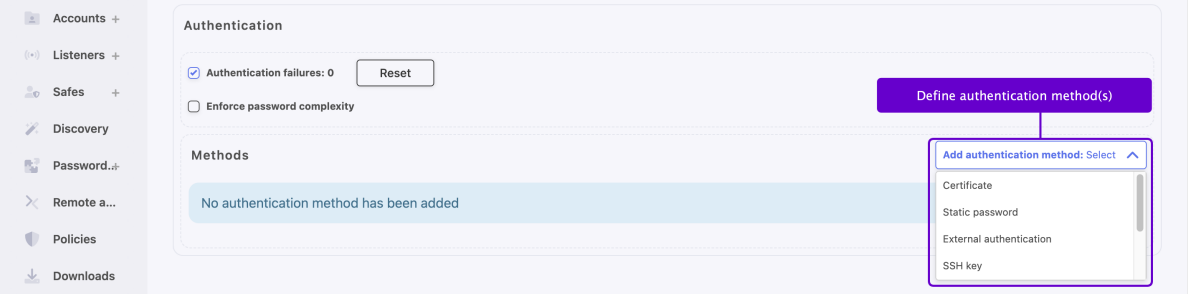


17. Specify authentication methods.

Note

To enable configuring authentication methods, please save created user first.

18. To add authentication method, select desired type from the *Add authentication method* drop-down list. Below you will find description of available authentication methods specification procedures.



Certificate

- Provide *Subject* that complies with the RFC 2253 or RFC 4514 requirements.

Note

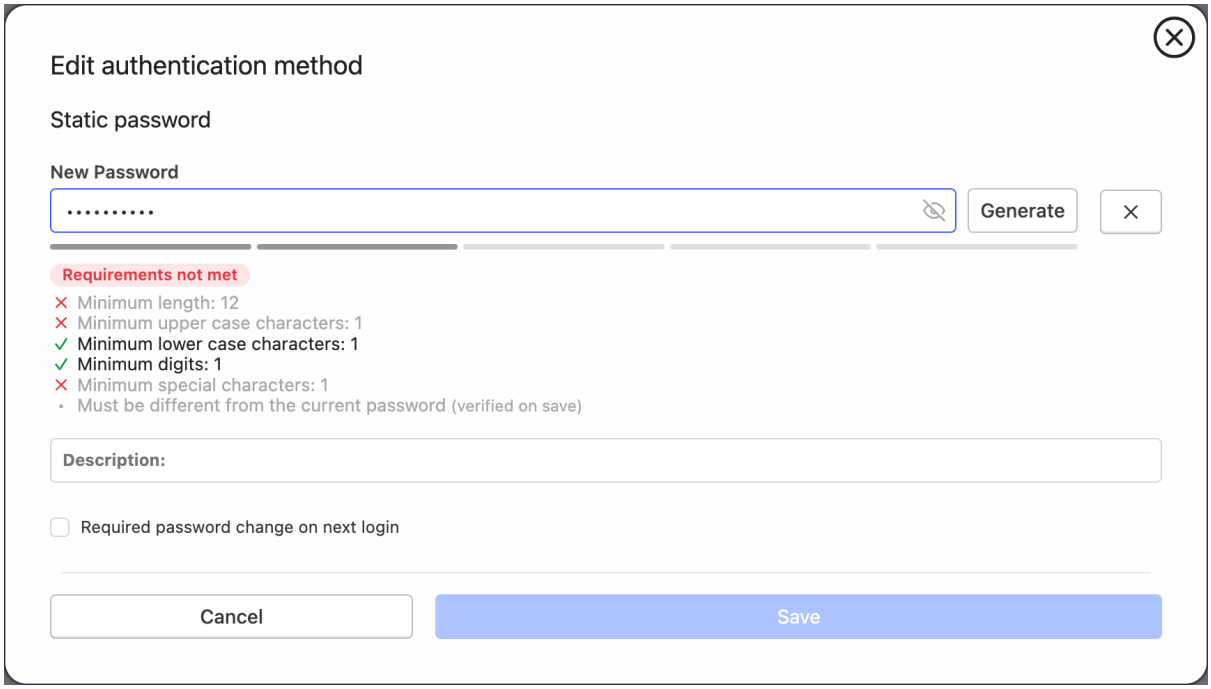
Additionally, the CA certificate is required to be uploaded in the *Settings* > *System* tab. For more information about authentication with certificate, refer to the *Certificate-based Authentication Scheme* topic.

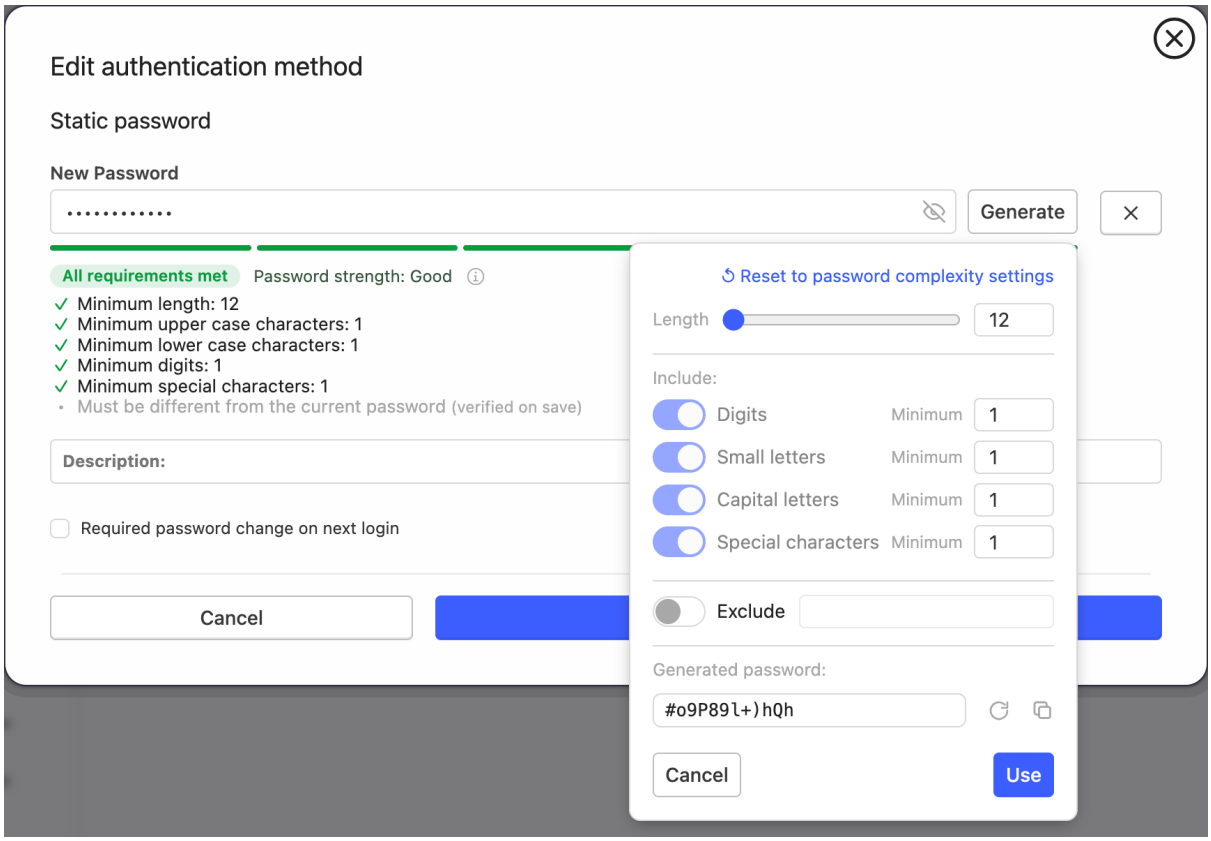
Static password

- Type the password in the *Password* field, or click *Generate* to create a random password and click *Use* to insert it.

Note

- If password complexity is enforced for the user (*Enforce password complexity*), the password complexity rules are listed under the field and checked as you type. The password can be saved only when all rules are met. The *Different password than current* rule is verified when the password is saved.
- If password complexity is not enforced, the bar under the field shows the estimated strength of the password.
- The password generator uses the password complexity settings by default.





- Select *Required password change on next login* to have the user change the password on next login attempt.

Note

If you select the *Required password change on next login* option, the user will not be able to access servers using native protocols clients. The user will have to change the password using

the *User Access Gateway*.

External authentication

- Select external authentication source from the *Choose method* drop-down list.

Note

Refer to *Authentication* topic for more information on external authentication sources.

SSH key

- Provide public SSH key used for verifying user's identity in the *Public key* field.

SMS

- In the **First factor** field choose *Static password* or *External authentication* (AD or LDAP).
- Provide a phone number in the *Phone* input field.

Note

For more information about SMS authentication configuration, refer to the *SMS authentication definition* topic.

DUO

- In the **First factor** field choose *Static password* or *External authentication* (AD or LDAP).
- In the **Second factor** field:
  - Provide *DUO User*.
  - Provide *DUO User Id*.

Note

For more information about DUO authentication configuration, refer to the *DUO authentication definition* topic.

OATH

- In the **First factor** field choose *Static password* or *External authentication* (AD or LDAP).
- In the **Second factor** field:
  - Provide *Token type*.
  - Provide secret that will be used by *Google Authenticator* by typing it in the *Secret* field, by generating random secret by pressing *Generate* button, or by generating QRCode by pressing *QRCode* button.
  - Specify *Token length*.
  - Choose the timestamp value from the *Timestamp* drop-down list.

  - Choose *Initialized* option if needed.

For more information refer to the *Two-Factor OATH Authentication with Google Authenticator* page.

Passkey

- Enter a name for the authentication method being added and click Save. You will be prompted to verify your identity.
- Follow the browser instructions:
  - Choose your authentication method (hardware key, biometrics, password manager)
  - Confirm your identity (touch the key, use fingerprint, Face ID)
  - Save the Passkey

Note

Passkey requires a hostname (FQDN) - it cannot be created when the Admin Panel or User Access Gateway is opened via an IP address (e.g. `https://fudo.example.com/` works, `https://192.168.1.10/` does not). See *FIDO2 Authentication Settings*.

API key

- Provide a *Description* that will help distinguish this API key.
- Provide or generate *API key*.
- Copy generated API key to use it in other systems that require authentication with this Fudo user.

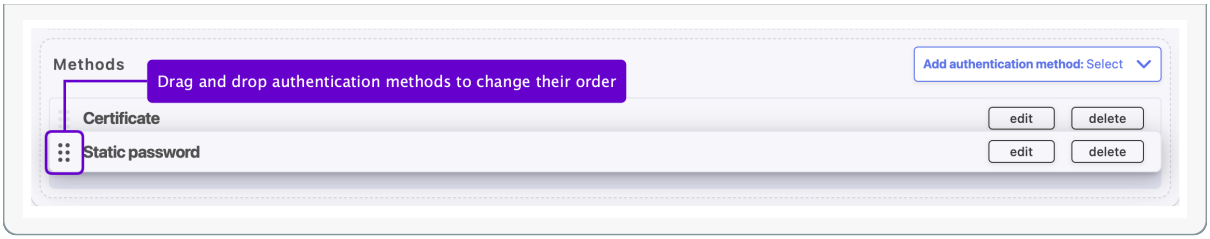
Note

The *API Key* cannot be retrieved after saving this authentication method.

19. To define more authentication methods select new type from *Add authentication method* drop-down list.

Note

- When processing user authentication requests, Fudo Enterprise verifies login credentials against defined authentication methods in order in which those methods have been defined.
- After adding several authentication methods you have the possibility to change their order by using drag-and-drop functionality.
- The list of methods can also contain a *ShareAccess Key* entry. It represents the user's Fudo ShareAccess identity, is created automatically when the user is invited to Fudo ShareAccess and cannot be added from the *Add authentication method* drop-down list. This method is not used to log in to Fudo Enterprise and is not taken into account in the order of authentication methods. For more information, refer to the *ShareAccess Key Authentication Method* section.



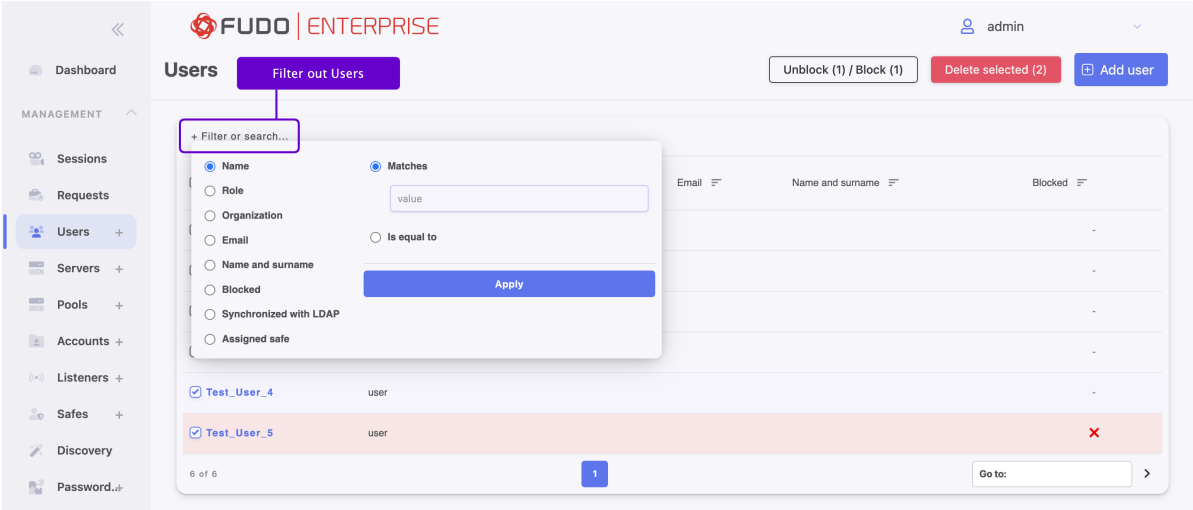
20. Click *Save* or *Save and close*.

Related topics:

- *Authentication Failures Counter*
- *Users synchronization*
- *Data model*
- *Default Domain*
- *System initiation*
- *Servers*
- *Accounts*
- *Approving Pending User Requests*
- *Declining Pending Requests*

9.1.2 Editing a User

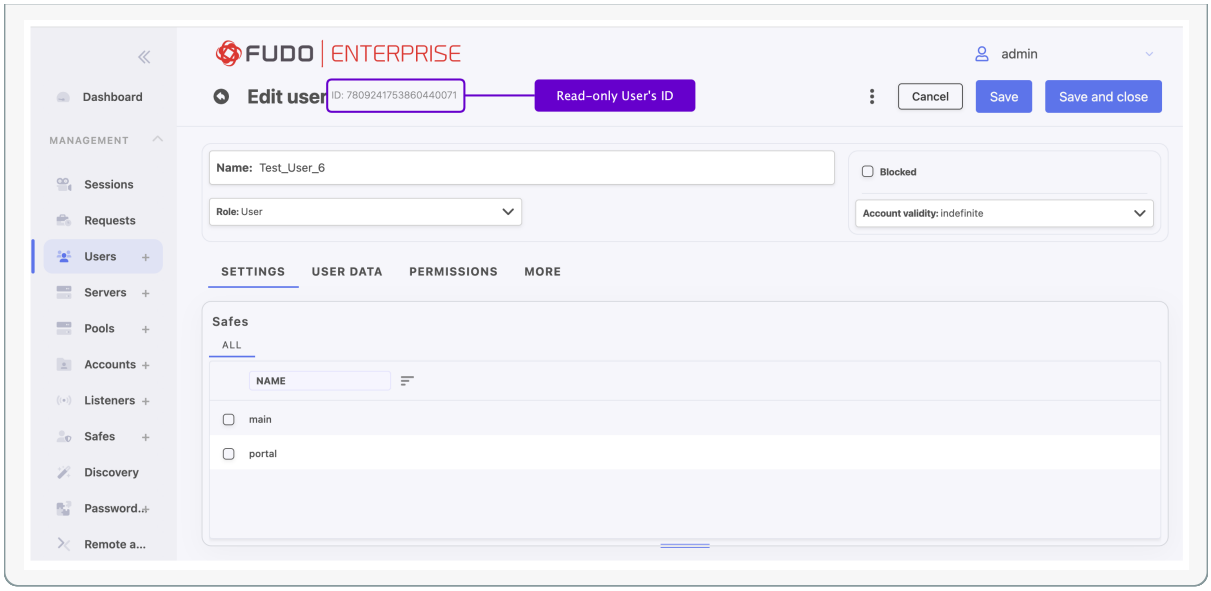
1. Select *User Management* > *Users*.
2. Define filters to limit the number of objects displayed on the list.



3. Find and click desired user's name to access its configuration parameters.

Note

- ID is a read-only, unique object identifier and it is assigned by Fudo Enterprise when object is created.



4. Modify configuration values as needed.
5. Click *Save* or *Save and close*.

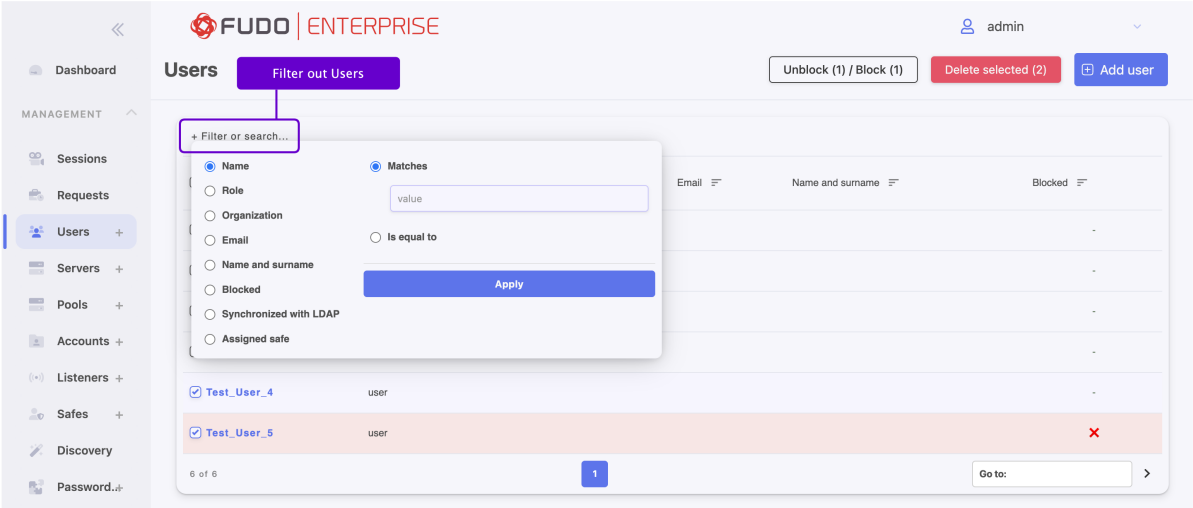
Related topics:

- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*
- *Accounts*

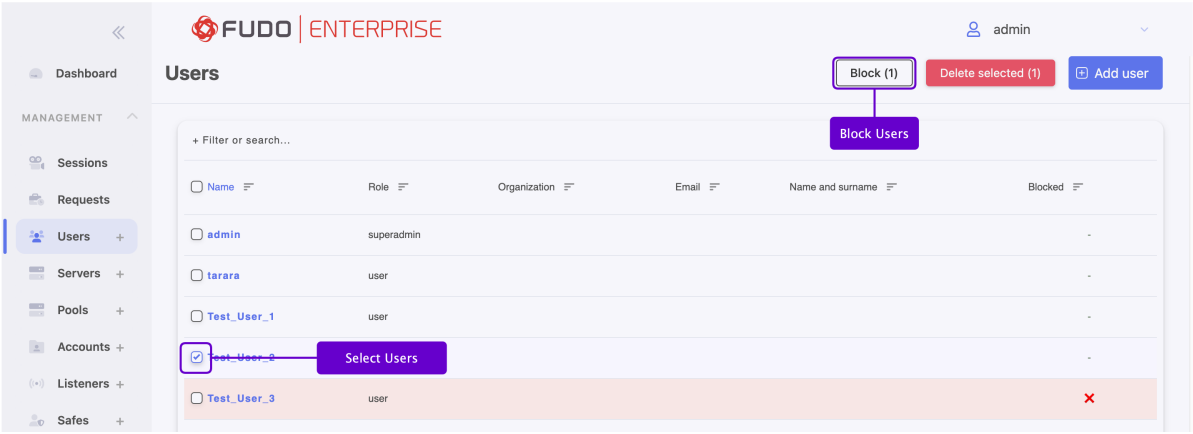
9.1.3 Blocking a User

> **Warning**
>
> Blocking a user will terminate its current connections.

1. Select *User Management* > *Users*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Select the user you want to block and click *Block*.



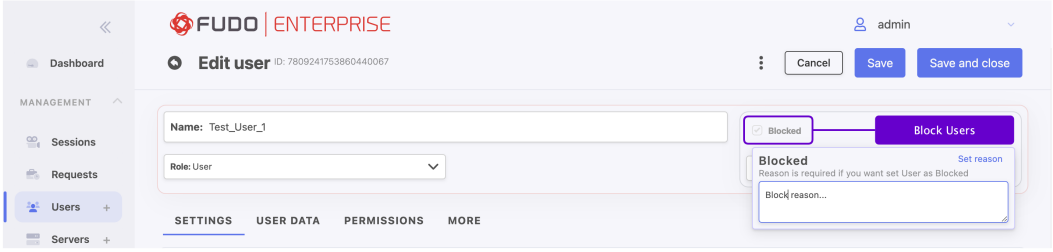
4. Provide mandatory blocking reason and click *Block*.

Note

To view the blocking reason, place the cursor over the red cross icon on the users list.

Users can also be blocked by accessing the user object configuration form. To do this:

- Edit user definition.
- Select the *Blocked* option.
- Provide mandatory blocking reason and klick 'Set reason'.



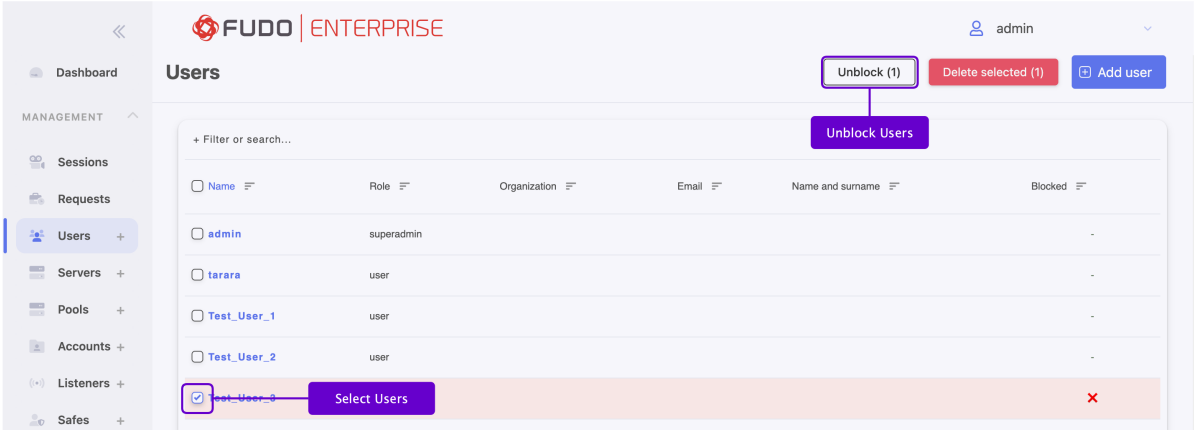
- Click *Save* or *Save and close*.

Related topics:

- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*
- *Accounts*

9.1.4 Unblocking a User

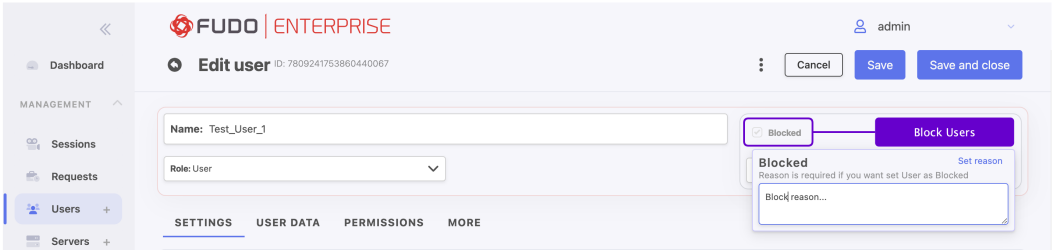
1. Select *User Management* > *Users*.
2. Define filters to limit the number of objects displayed on the list.
3. Select the user you want to unblock and click *Unblock*.



4. Click *Unblock* to confirm.

Users can also be unblocked by accessing the user object configuration form. To do this:

- Edit user definition.
- Deselect the *Blocked* option.



- Click *Save* or *Save and close*.

Related topics:

- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*

- *Accounts*

9.1.5 Deleting a User

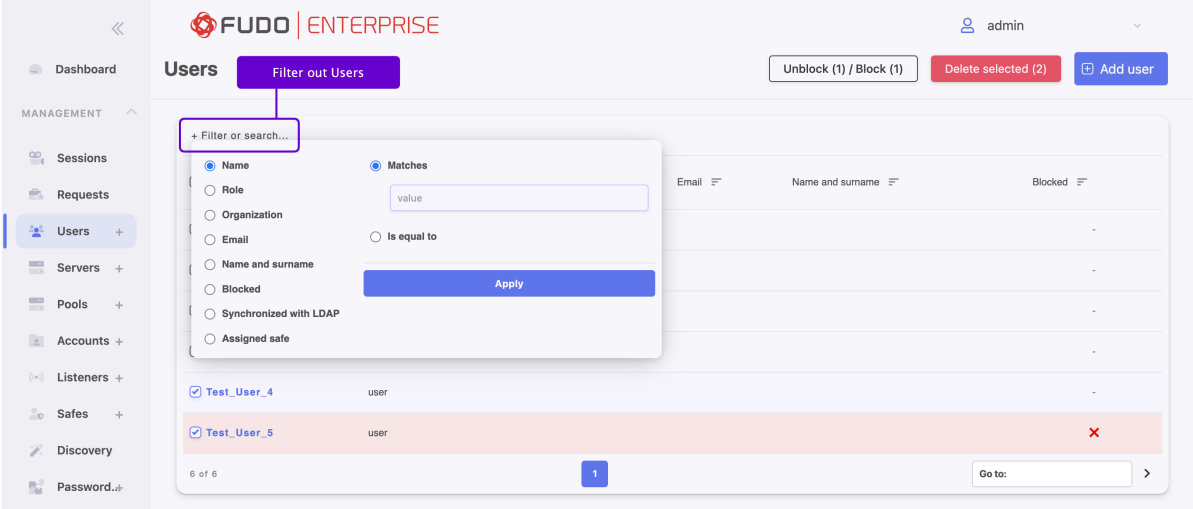
Note

Deleting a user definition does not result in the removal of associated registered sessions. Sessions of deleted users are marked with a strikethrough username.

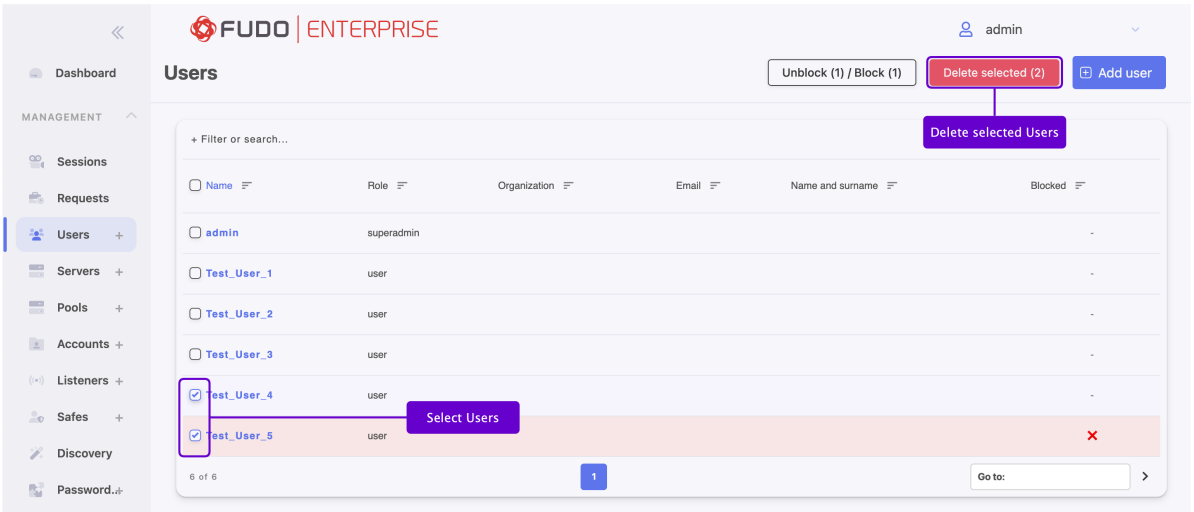
Warning

Deleting a user definition will terminate its current connections.

1. Select *User Management* > *Users*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Click *Delete selected*.



4. Confirm deleting selected objects.

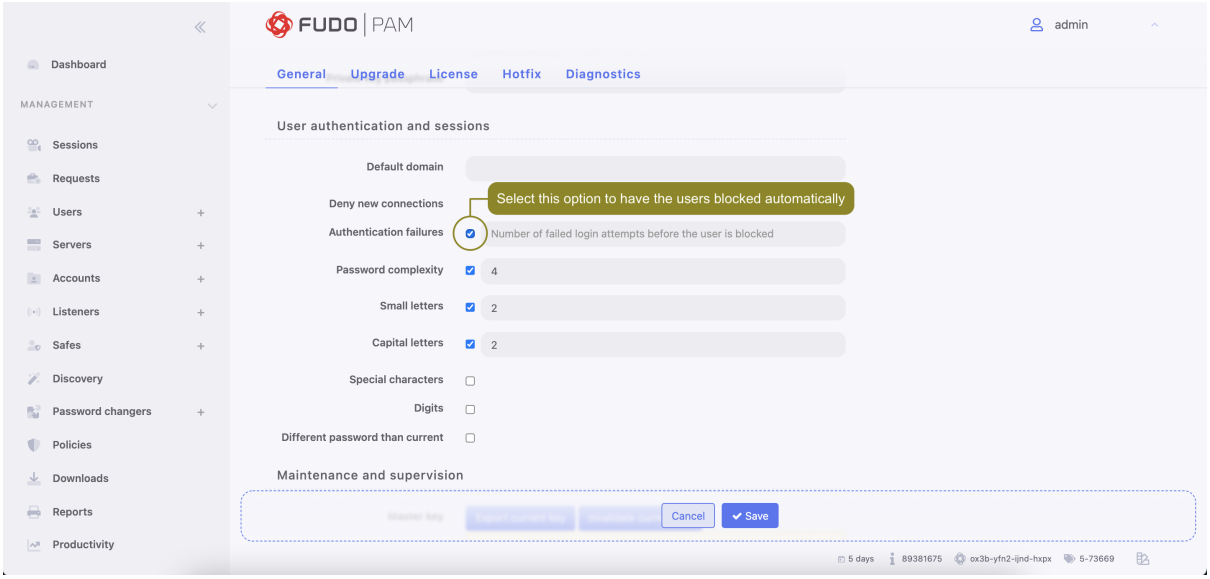
Related topics:

- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*
- *Accounts*

9.1.6 Authentication Failures Counter

Fudo can keep track of failed login attempts and automatically block users accounts if the counter reaches a specified value.

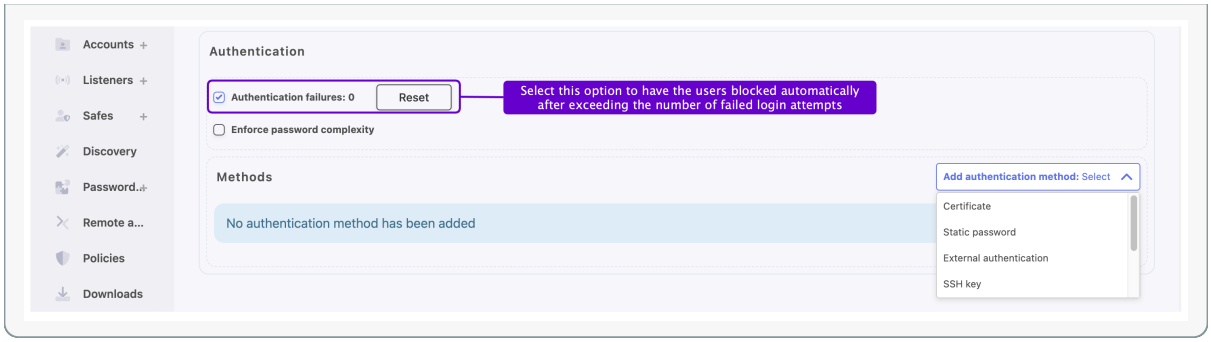
1. Select *Settings* > *System*.
2. In the *Authentication and sessions* section, select *Authentication failures* option.
3. Enter the number of failed login attempts after which the user account will be blocked.



4. Click *Save*.
5. Select *User Management* > *Users*.
6. Find and click a user that you want to block automatically after a number of failed login attempts.
7. In the *Authentication* section, select *Authentication failures*.
8. Click *Save*.

Note

Click Reset button to reset the counter.



Related topics:

- *User Authentication Methods and Modes*

9.2 Groups (RBAC)

Groups provide an extra layer of control over access to resources. Administrators can create user groups to manage resource access more precisely, ensuring that only authorized users can access specific safes. This feature will improve both security and flexibility in managing access to sensitive data.

Groups support integration with external systems that use the Role-Based Access Control (RBAC) model. This enables you to map specific roles from external directories, such as Active Directory, to Fudo Enterprise groups and assign specific roles. Users automatically inherit permissions and resource access based on their assigned role, ensuring consistent and centralized access management.

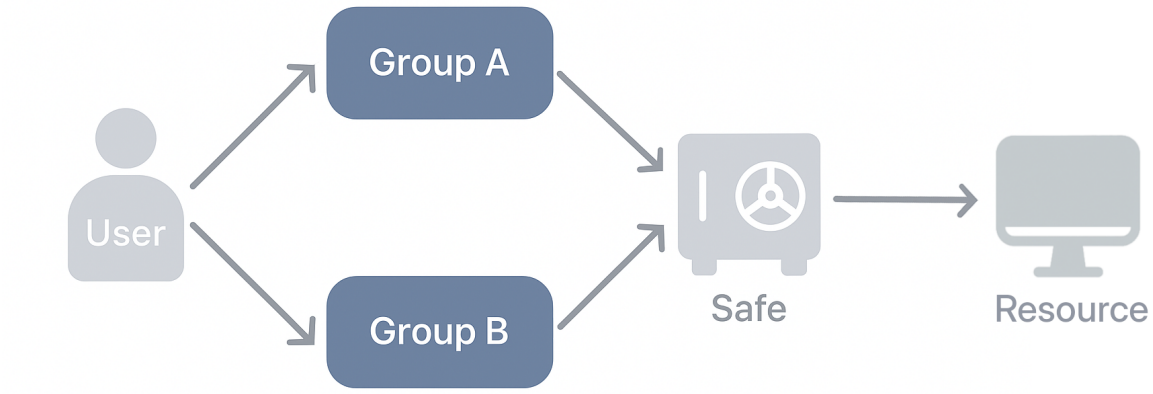
Note

User groups can be assigned to safes to define which users have access to specific resources. It is also possible to assign individual users directly to a safe. This means that both user groups and individual users can be granted access to safes, offering flexibility in access control configuration.

9.2.1 Access Resolution and Prioritization

When a user has access to the same resource through multiple safes or group assignments, Fudo Enterprise determines the access path based on a defined priority and set of rules. This ensures predictable and secure access behavior in complex permission scenarios.

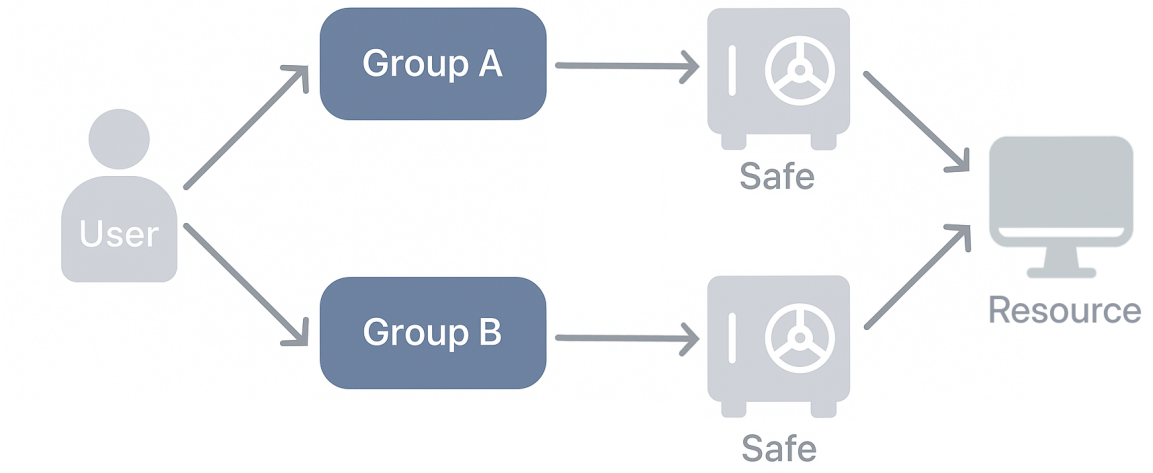
User Belongs to Multiple Groups Assigned to the Same Safe and Resource



If a user is a member of two or more groups that are assigned to the same safe and resource, the following rules apply:

- **Password Reveal:** If the password reveal option is enabled in at least one of the groups, the user will be able to view the password for the entire safe.
- **Access Time Period:** If validity time frames are configured for both groups, Fudo Enterprise checks whether the current time is within the allowed range for each group. If the condition is met in at least one group, the session is allowed.
- **Daily Access Policy:** If user has time policy enabled, Fudo Enterprise evaluates the time policies from all applicable groups. If the user is within the allowed time frame in any group, the session is permitted.

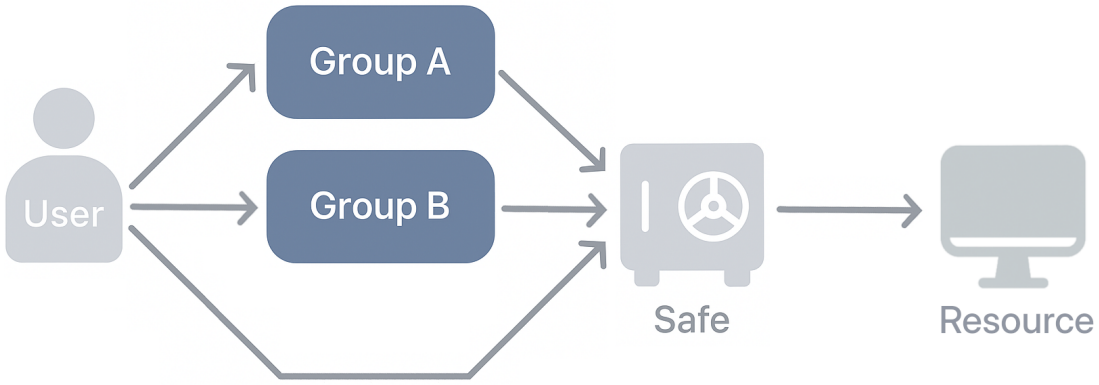
User Belongs to Multiple Groups Assigned to Different Safes with the Same Resource



When a user can access the same resource through multiple safes via different groups, the resolution follows this logic:

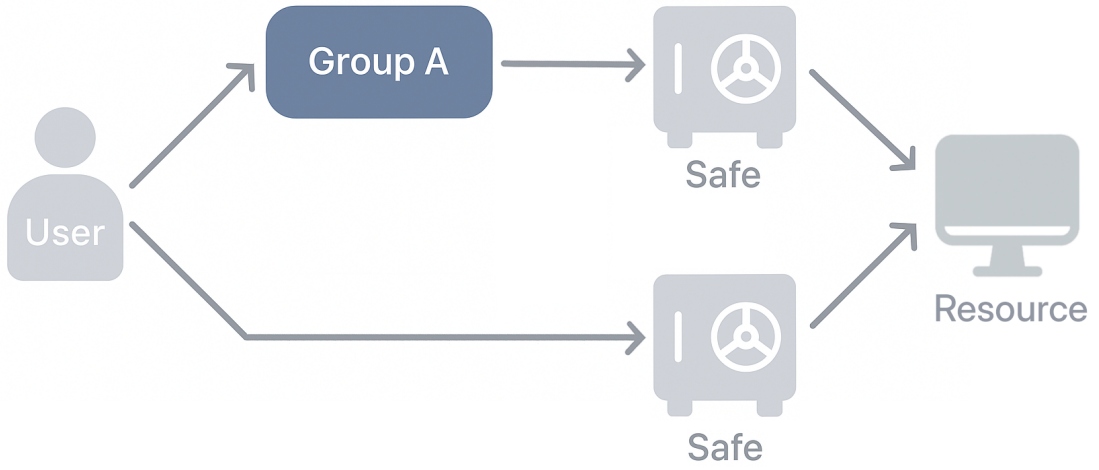
- **Access Time Period:** If the current time falls within the validity range of Group A, it is used. Otherwise, Group B is evaluated. If neither group has validity restrictions, the system selects the first group in alphabetical order.
- **Daily Access Policy:** If both groups have a daily time policy enabled, Fudo Enterprise checks which group allows access at the current time. Access is granted based on the first group in alphabetical order whose time policy includes the current time or that has no policy configured.

User Has Both Direct and Group-Based Access to the Same Safe and Resource



If a user has a direct assignment to a safe and group-based access to the same safe and resource, **direct access takes priority.** All settings such as *Blocked, Reveal Password, Access Time Period,* and *Daily Access Policy* are taken from the direct user-safe assignment and override any group-based rules.

User Has Access to the Same Resource via Direct Safe Assignment and Group-Based Assignment Through a Different Safe

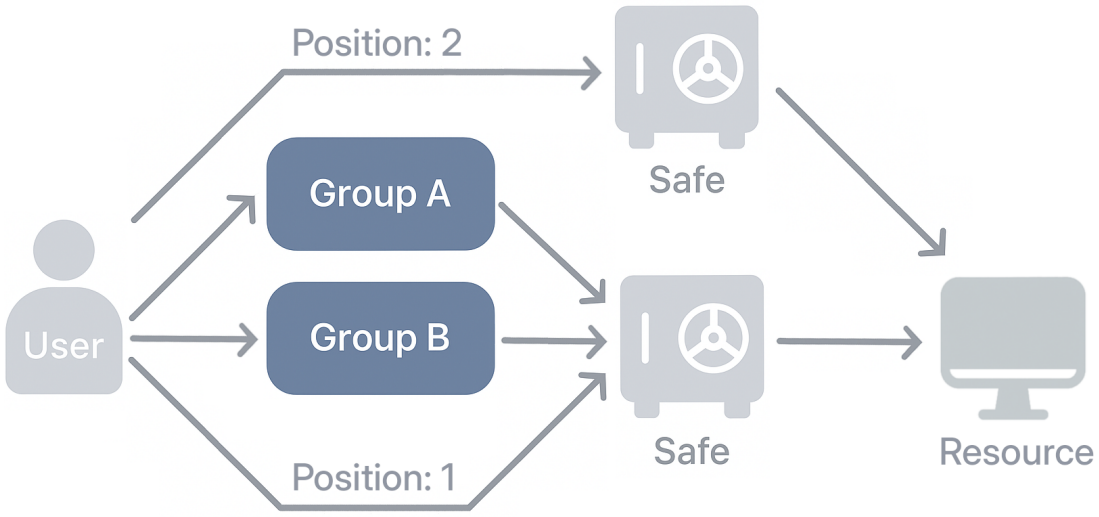


In cases where the user has access to the same resource:

- Directly through a safe, and
- Indirectly through a group assigned to a different safe,

Fudo Enterprise **will always use the direct connection.** The evaluation skips group-level assignments and uses the direct safe connection for access control.

User Has Access to the Same Resource Through Two Safes with Different Positions



In this scenario, the user has access to the same resource through two different safes. One safe is assigned position 1, and the other position 2.

Since position values determine preference, the system will **always use the safe with the higher position number**—in this case, the one with position 1.

Note

- First, Fudo Enterprise checks if the user has a **direct assignment to the safes.** If so, group-based assignments are ignored entirely.
- Then, among all available direct connections, Fudo Enterprise **evaluates the position** attribute and selects the safe with the highest position value.

Time Policy Resolution for Direct and Group-Based Access

When a user has access to a safe through a direct assignment, one or more group assignments, or both, Fudo Enterprise determines which time policy applies according to the following priority:

Order	Policy	Applies when
1	Direct user-safe assignment	The user is assigned to the safe directly. The *Blocked* option, *Access time period*, and *Daily access policy* configured for the direct assignment take priority over all group-based settings.
2	Custom policy for group-based access	The user is not assigned to the safe directly, but a custom time policy has been configured for the user's group-based access. This policy replaces the policies of all groups through which the user can access the safe.
3	Group policies	The user has no direct assignment and no custom policy. The policies of all groups that grant the user access to the safe are evaluated together according to the group access rules described above.

A time policy controls **when existing access can be used**; it does not grant access to a safe. A custom policy can therefore be configured only for a user who already has access through at least one group.

Important

A custom policy for group-based access replaces the policies inherited from the granting groups instead of being combined with them. As a result, it can be either more restrictive or more permissive than the group policies, but it cannot grant access to a safe that the user cannot otherwise access.

Group-based access can also be restricted directly on the group-to-safe assignment by using the *Blocked* option, *Access time period*, and *Daily access policy*. If a group is blocked or the current time falls outside its configured access period, that group does not provide access to the safe and is not included when group policies are evaluated.

If the user's last group-based access path to the safe is removed, any custom time policy configured for that group-based access is removed automatically.

Note

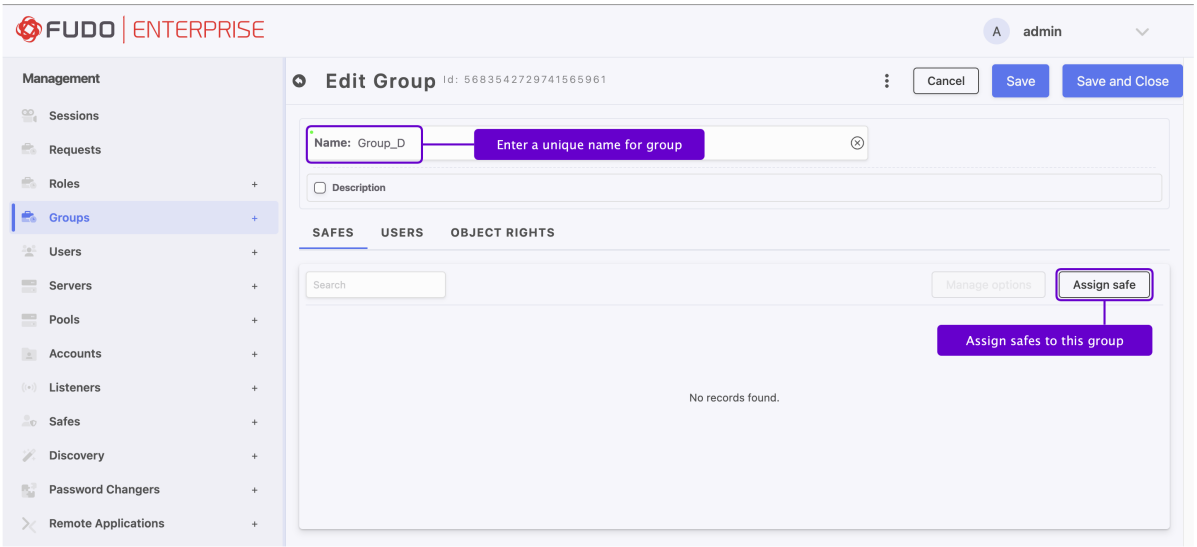
For information on configuring these policies, refer to *Creating a Safe*.

Related topics:

- *Creating Group*
- *Creating a Safe*
- *Users*

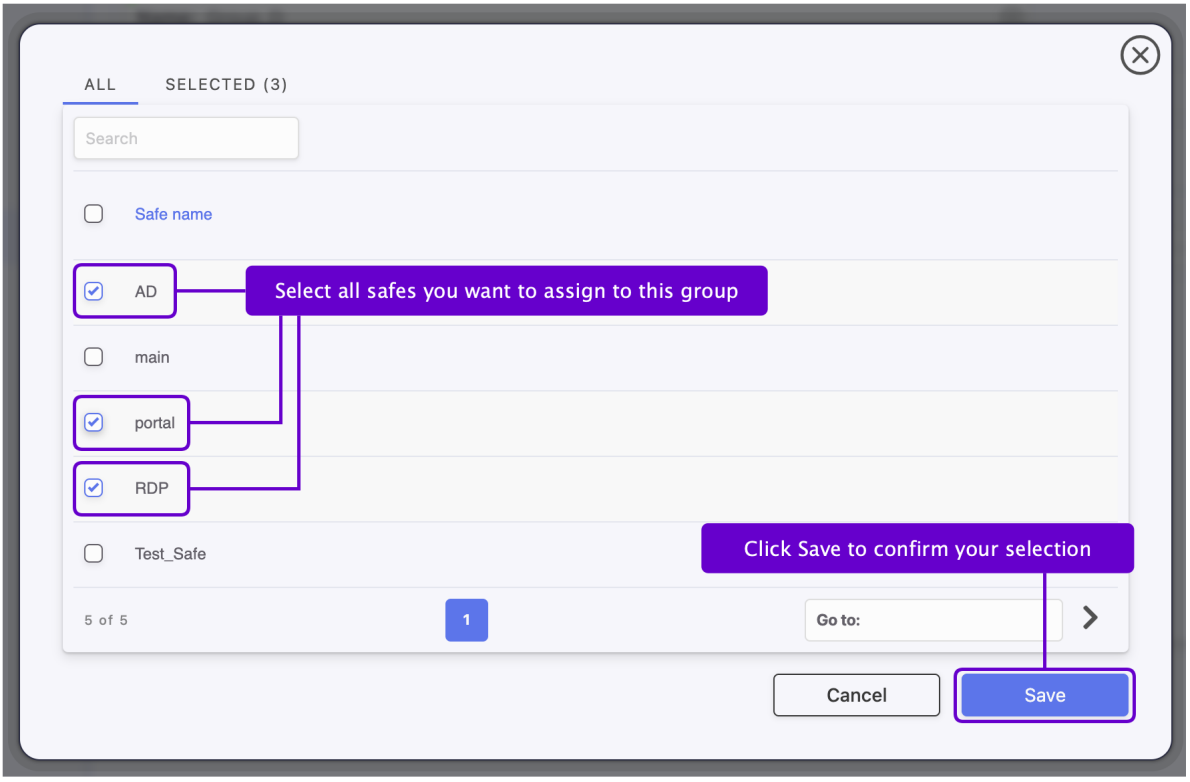
9.2.2 Creating Group

1. Click + icon in the main menu next to the *Groups* tab, or select *User Management* > *Groups* and then click + *Add Group*.
2. Enter a unique name for the new object.
3. If needed, select the *Description* option to add a summary of the group.
4. Click *Save* to create the group and proceed with further configuration.



SAFES TAB

5. Go to the **SAFES** tab and click *Assign Safe*.
6. Select all safes you want to assign to this group and click *Save*.



Note

There are two default safes in the system:

- `main` - provides access to the Admin Panel.
- `portal` - provides access to the User Access Gateway.

DAILY ACCESS POLICY

After assigning safes, you can enable and define time intervals during which the user will be allowed to connect to servers.

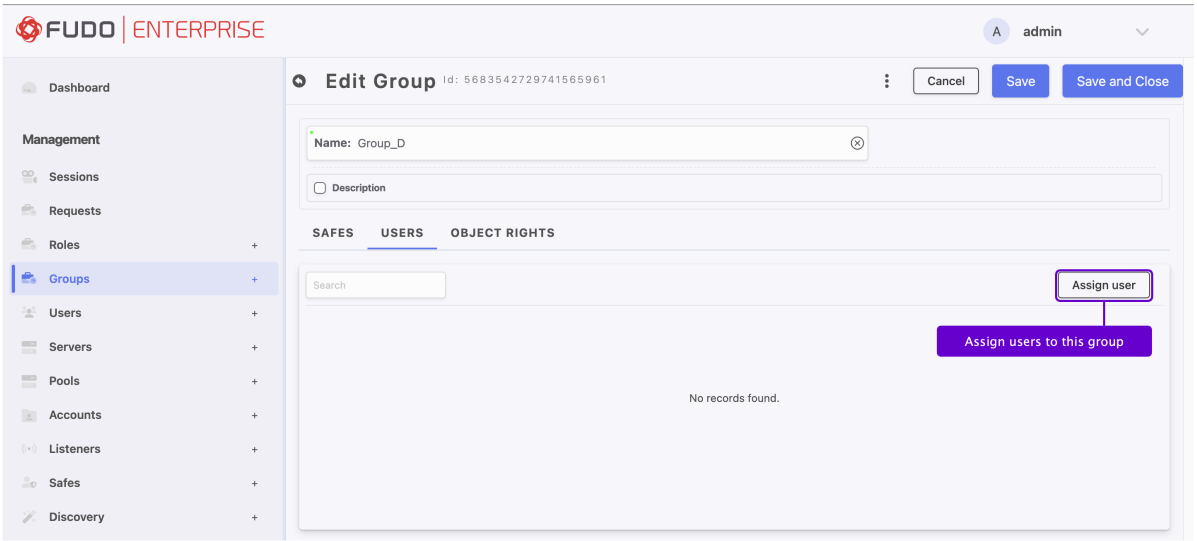
7. Select the desired safe and click *Manage Options*.
8. In the *DAILY ACCESS POLICY* tab, enable the time policy, then click the row of the desired day of the week to add an access window, or drag across the row to draw one. Dragging vertically covers several days at once.
9. Windows snap to a 30-minute grid and can be moved or resized by their edges. Click a window to set exact start and end times, use the copy icon next to a day name to copy that day to all days, or use *Clear all* to remove the whole schedule.
10. Click *Save* to close the modal window.

> **Note**
>
> When several selected safes have different schedules, the editor starts empty and an *Override*/*Merge* choice decides how the saved schedule is applied. *Merge* adds the edited windows to the existing schedules, while *Override* replaces them.

USERS TAB

In this tab, you can define which users will be part of this group.

11. Go to the **USERS** tab and click *Assign User*.
12. Select all users you want to assign to this group and click *Save*.

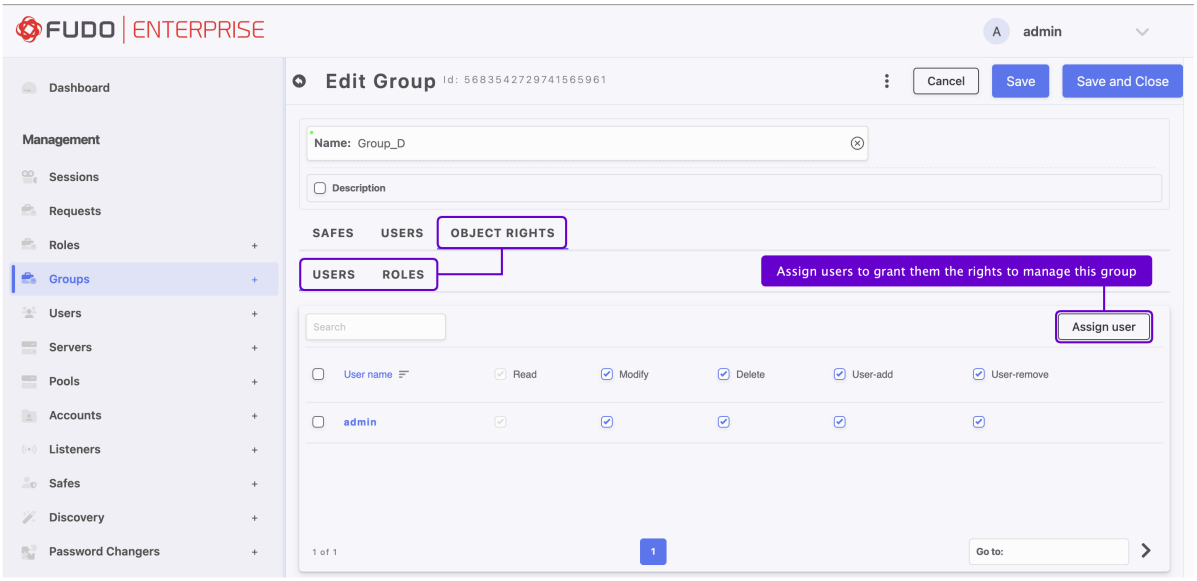


OBJECT RIGHTS TAB

In this tab, you can define which users and roles will have permission to manage this group.

> **Warning**
>
> Please note the presence of the **USERS** sub-tab within the **OBJECT RIGHTS** tab. This sub-tab is used to assign permissions to manage the group to selected users — it is **not** used

to assign users to the group itself.



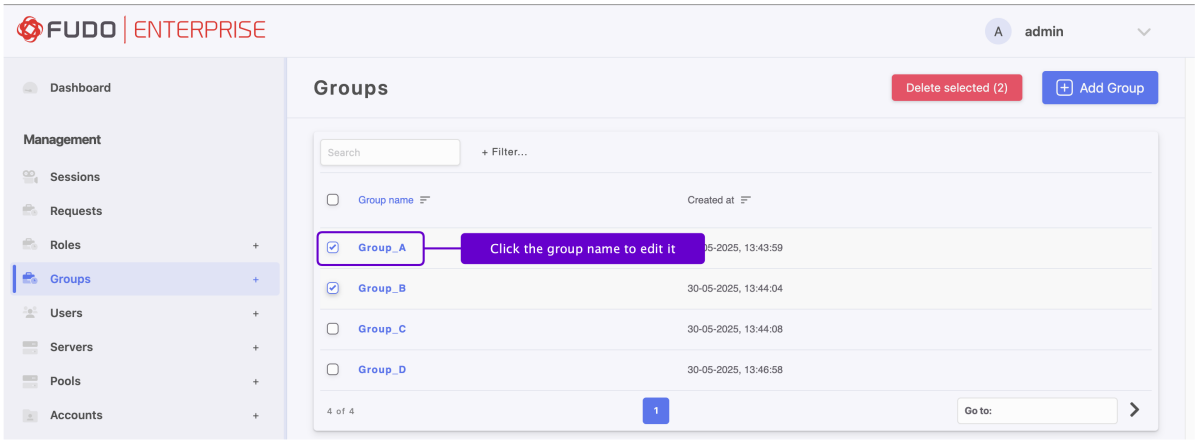
11. Go to the **USERS** sub-tab and click *Assign User*.
12. Select all users you want to assign permissions to manage this group and click *Save*.
13. Go to the **ROLES** sub-tab and click *Assign Role*.
14. Select all roles you want to assign permissions to manage this group and click *Save*.
15. Click *Save and Close* to save created group.

Related topics:

- *Groups (RBAC)*
- *Users*

9.2.3 Modifying Groups

1. Select *User Management* > *Groups*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.
3. Find and click desired group's name to edit it.
4. Modify configuration parameters as needed.



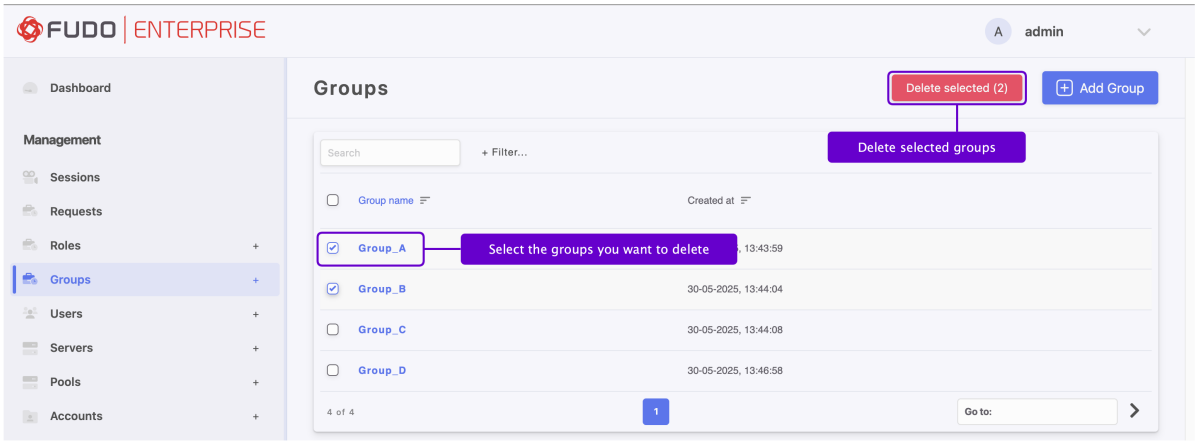
5. Click *Save and Close* to save changes to this configuration.

Related topics:

- *Role-Based Access Control (RBAC)*
- *Groups (RBAC)*
- *Users*

9.2.4 Deleting Groups

1. Select *User Management* > *Groups*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.
3. Find and click the checkbox next to the desired group's name to select it.
4. Click *Delete selected*.



5. Alternatively, you can edit a group that needs to be deleted right from the list, click the vertical three-dot icon and select *Remove group*.

Related topics:

- *Groups (RBAC)*
- *Users*

9.3 Role-Based Access Control (RBAC)

Roles implement Role-Based Access Control (RBAC), providing granular and flexible control over user permissions.

The **RBAC (Role-Based Access Control)** functionality in Fudo Enterprise allows system administrators to define precise roles with specific access permissions tailored to objects and operations. This enables the creation of roles designed for particular tasks, such as a role that grants permissions solely for user management—allowing the creation, editing, and deletion of users—without affecting other areas of the system.

Similarly, roles can be configured to manage other objects, such as Listeners, Pools, Servers, and Safes. Administrators can define role-based permissions for specific actions, including creating, modifying, exporting, deleting, or blocking these objects.

The access management mechanism supports both global and selective permissions. This means that a user can be granted access to view, modify, or delete all objects of a given type (e.g., Users, Accounts, or Servers) or only specific, selected objects. This flexibility ensures that access rights align with the organization's security and operational requirements.

Note

To maintain compatibility with previous versions, six default roles—*superadmin, admin, safes admin, operator, auditor, and session viewer*—have been added. These roles can also be modified as needed.

9.3.1 Transition to RBAC After Upgrade

With the introduction of Role-Based Access Control (RBAC), the system includes a predefined set of roles designed to ease the transition from the legacy permissions model. These roles are automatically mapped from the previous configuration to help retain basic access structures and reduce disruption during the upgrade.

While the *superadmin* role is fixed and cannot be modified or removed, all other predefined roles—such as *admin, operator, session viewer, safes admin,* and *auditor*—can be modified or extended as needed. This flexibility allows organizations to gradually align the access model with their internal security policies.

Warning

- After upgrading, administrators should review and customize the predefined roles to ensure they meet the specific requirements of their organization. Adjusting these roles is essential to take full advantage of the control and granularity offered by RBAC.
- When upgrading the system to a capabilities-based version, it is necessary to map all objects for which users had capabilities / grants.
- The automatic mapping of legacy roles is a one-time compatibility step performed only during the upgrade from a version without RBAC. These predefined roles are not intended to replicate previous permissions one-to-one, but rather to provide a starting point for adaptation.
- Once a predefined role is modified or deleted, the change is permanent—there is no built-in mechanism to restore its original default state. However, if you need to revert

to the original configuration, please contact Fudo Enterprise support for assistance.

9.3.1.1 Understanding Privileges and Capabilities

Read

The `*-read` privilege grants visibility into a specific tab of the interface, and consequently, into all objects of that type in the system—not just those for which the user has capabilities. This privilege provides view-only access and does not permit editing, deletion, or any other actions.

Example:

A user assigned the `user-read` privilege can open the Users tab and view the full list of user accounts in the system, including those they did not create and do not have capabilities for. However, they cannot modify, block, or delete any of these users unless they also have the corresponding capabilities or additional privileges.

Create

Privileges with the `*-create` suffix allows users to create new objects of a given type. For example, `user-create` enables the creation of a new users. When an object is created, the system automatically grants the creator all available capabilities for that specific object. This means the creator can fully manage the object without needing additional privileges.

Example:

If an administrator has the `user-create` privilege and creates a new user, they automatically receive the following capabilities for that user:

- modifying the user's settings,
- blocking or unblocking the user,
- deleting the user.

In this scenario, the administrator does not require separate privileges such as `user-block` or `user-delete`—the capabilities granted at creation time are sufficient.

Delete

Granting a role a privilege from the `*-delete` group (e.g., `server-delete`) allows that role to delete any object of the specified type—regardless of whether the user created it. In the user interface, access to the relevant tab and object may still be required to perform the deletion, but via the API, any object can be deleted if the `*-delete` privilege is present. In many cases, the `*-read` privilege is not required for such actions via API.

Warning

This creates a potential security concern: assigning `*-delete` may unintentionally elevate a role's access level beyond what was originally intended. Recommendations:

- Prefer assigning `*-create` privileges when the role should only manage objects it has created.
- Use `*-delete` privileges only for roles that are intended to have global control over all objects of a given type.

When migrating from version 5.5, review role permissions carefully to avoid unintentionally increasing their effective privileges.

9.3.1.2 Predefined Roles as a Starting Point

The system includes a set of predefined roles designed to support backward compatibility and legacy access structures following the introduction of Role-Based Access Control (RBAC):

- **Superadmin** - Has unrestricted access to all system features and settings. This role can create custom roles with any available access rights.
- **Operator** – Grants similar permissions to the legacy `operator` role prior to the introduction of RBAC. This role is automatically mapped based on the previous configuration. Selected example privileges:
  - Can view the list of sessions and their details, but only for sessions linked to objects for which the operator has appropriate permissions.
  - Can play archived and live sessions, limited to sessions associated with accessible objects.
  - **Cannot** create new objects.
  - Can block only those objects for which they have assigned capabilities.
  - **Sees only** the objects for which they have capabilities in all lists, but **can preview** all roles and groups.
  - The **operator** role now includes the *listener-read* privilege by default. Due to RBAC changes, operators currently see all listeners, even those not explicitly granted.
  - Can preview secret changers, verifiers, and password policies.
  - Can preview remote applications.
  - **Cannot** preview policies, and regular expressions.
  - Can manage and view notifications for users to whom they have capabilities.
  - Can see the Admin Panel footer.
  - **Cannot** share sessions for joining or delete sessions.
  - Can view and vote in awaiting, active, and archived requests associated with objects they have access to (requesting user, account, safe, server/pool).
  - Can generate reports from the Sessions tab.
  - Can manage report subscriptions.
  - Can manually add a subscription for the *System Report*, but only for objects they have capabilities to (users cannot see reports generated for other users).
  - Now has access to the **Authentication** tab. This change enables administrators to view and assign external authentication methods.
  - Now has access to the **External password repositories** tab to assign external password repositories to accounts.
  - Now has access to the **Cluster** tab to send sessions to other nodes.
  - Does **not** have access to other subtabs under the **Settings** tab.

- **Admin** - Grants similar permissions as the legacy `admin` role prior to the introduction of RBAC. This role is automatically mapped based on the previous configuration. Selected example privileges:
  - Has access to the Dashboard and its widgets, according to related capabilities.
  - Can create new objects such as users, groups, servers, accounts, pools, and safes. The creator is automatically granted full permissions to the objects they create.
  - Can manage users, groups, servers, accounts, pools, and safes **for which they have assigned capabilities.**
  - **Cannot** create listeners.
  - **Can** create users and preview their assigned roles, but **cannot** assign roles to users (`role-modify` privilege is needed).
  - Can manage and view notifications for users to whom they have capabilities.
  - Can see the Admin Panel footer and access the User Menu in the upper-right corner.
  - Can view and play sessions linked to accessible objects, manage retention, delete sessions within access scope, use all features covered by the session-modify privilege (*Sessions Tab Permissions*), and perform actions such as encoding, sharing, commenting, terminating, exporting, and joining.
  - Can view and vote in awaiting, active, and archived requests associated with objects they have access to (requesting user, account, safe, server/pool).
  - Can create and manage secret changers, verifiers, and password policies.
  - Can create and manage remote applications.
  - Can create and manage policies, and can only preview regular expressions.
  - Can generate reports from the Sessions tab.
  - Can manage report subscriptions.
  - Can manually add a subscription for the *System Report*, but only for objects they have capabilities to (users cannot see reports generated for other users).
  - Now has access to the **Authentication** tab. This change enables administrators to view and assign external authentication methods.
  - Now has access to the **External password repositories** tab to assign external password repositories to accounts.
  - Now has access to the **Cluster** tab to send sessions to other nodes.
  - Does **not** have access to other subtabs under the **Settings** tab.
- **Session Viewer** - Grants similar permissions as the legacy `session viewer` role prior to the introduction of RBAC. This role is automatically mapped based on the previous configuration. Selected example privileges:
  - Can view the list of sessions and their details, limited to sessions associated with objects for which they have permissions.
  - Can play archived and live sessions, limited to sessions associated with accessible objects (see also *Sessions Tab Permissions*).

  - Can join, terminate, comment on, and encode sessions, provided they have access to the related objects.
  - Can access the Admin Panel footer.
  - **Cannot** modify session-related configuration (e.g., retention, encoding settings, etc.).
  - Can access the **Files** tab and download available session-related files, limited to sessions they are permitted to view.

- **Safes Admin** - Provides similar permissions as the `admin` role, except for access to password modifiers and password policies. Additionally, this role does not have access to the Cluster configuration or widget. Selected example privileges:
  - A newly created user with this role may not see any objects unless they are explicitly granted capabilities to existing ones.
  - Has access to the Dashboard and its widgets, depending on assigned capabilities.
  - Can create new objects such as users, groups, servers, accounts, pools, and safes. Upon creation, full permissions are granted to the creator for those objects.
  - Can preview all roles, groups, users, and accounts.
  - Can manage users, groups, servers, accounts, pools, and safes **for which they have capabilities.**
  - **Cannot** create listeners.
  - **Can** create users and preview their assigned roles, but **cannot** assign roles to users (`role-modify` privilege is needed).
  - Can view and manage notifications for users to whom they have capabilities.
  - Can see the Admin Panel footer and access the User Menu in the upper-right corner.
  - Can view and play sessions linked to accessible objects, manage retention, delete sessions within access scope, use all features covered by the session-modify privilege (*Sessions Tab Permissions*), and perform actions such as encoding, sharing, commenting, terminating, exporting, and joining.
  - Can view and vote in awaiting, active, and archived requests associated with objects they have access to (requesting user, account, safe, server/pool).
  - Can preview secret changers, verifiers, and password policies.
  - Can create and manage remote applications.
  - Can preview policies, and regular expressions.
  - Can generate reports from the Sessions tab.
  - Can manage report subscriptions.
  - Can manually subscribe to the *System Report*, but access will be limited to objects they have capabilities for (users cannot view reports generated for others).
  - Now has access to the **Authentication** tab to assign external authentication methods to users.
  - Now has access to the **External password repositories** tab to assign external password repositories to accounts.

  - Now has access to the **Cluster** tab to send sessions to other nodes.
  - Does **not** have access to other subtabs under the **Settings** tab.

- **Auditor** - A read-only role with visibility into all areas of the system. Similar to the `superadmin` role in scope, but without permission to edit existing objects or create new ones.

Note that some exceptions apply, and the mapping may not reflect a one-to-one correspondence in all cases. Selected examples include:

- After the upgrade, an **admin** who has a capability assigned to an object will automatically gain full permissions for that object.
- Since listeners are considered a global and network-level configuration, after upgrading to version 5.6, **admin** users no longer have permissions to create them.
- The **admin, safes admin** and **operator** roles now includes the *extauth-read* privilege by default to be able to see and assign external authentication to users.
- The **admin, safes admin** and **operator** roles now includes the *passvn-read* privilege by default to be able to see and assign external password repositories to accounts.
- he **admin, safes admin** and **operator** roles now includes the *cluster-read* privilege by default to be able to send sessions to other nodes.
- The **operator** role now includes the *listener-read* privilege by default. However, due to RBAC changes, operators can currently view all listeners, not just those explicitly granted.
- Listener access model change - users now either have access to all listeners or to none. Granting access to individual listeners is no longer possible.
- can add manually subscription for this type of report but it will be limited to objects they have capabilities to.
- have access to following dashboard widgets: concurrent sessions, suspicious sessions, concurrent session chart, 'Active users' and 'Account alerts' widgets
- can now access the *Download* > *Files* tab and download files listed there. This permission is required for the correct display of SFTP/SCP sessions.
- The session viewer role now includes access to additional interface elements, including new tabs and the ability to add the Active Users dashlet from the Dashlet marketplace. This reflects expanded privileges defined in the updated access control matrix.

Note

- The **superadmin** role is protected and cannot be modified or deleted. This includes:
  - Editing its privileges or capabilities,
  - Renaming or deactivating the role,
  - Removing the role entirely.
- This restriction ensures that the system always retains at least one role with unrestricted access to all administrative features.
- The system enforces that **at least one user must always be assigned to the superadmin role.**

Warning

- The predefined **user** role has been removed from the system. After upgrading to version 5.6, any users who previously had this role assigned will no longer have any role.
- The predefined role **service** has been removed from the system.
  - Before the upgrade, customers who previously had multiple users assigned to the service role must remove all but one of them.
  - SNMP settings previously configured for that user will be transferred to the System tab and applied globally.

Related topics:

- *Role-Based Access Control (RBAC)*
- *Groups (RBAC)*
- *Users*
-

9.3.2 Creating Role

Note

A user can only create or assign roles that include permissions they themselves possess. To define a role with specific permissions, the user must have the appropriate rights to manage those permissions.

1. Click + icon in the main menu next to the *Roles* tab, or select *User Management* > *Roles* and then click + *Add Role*.
2. Enter a unique name for the new object.
3. If needed, select the *Description* option to add a summary of the role.

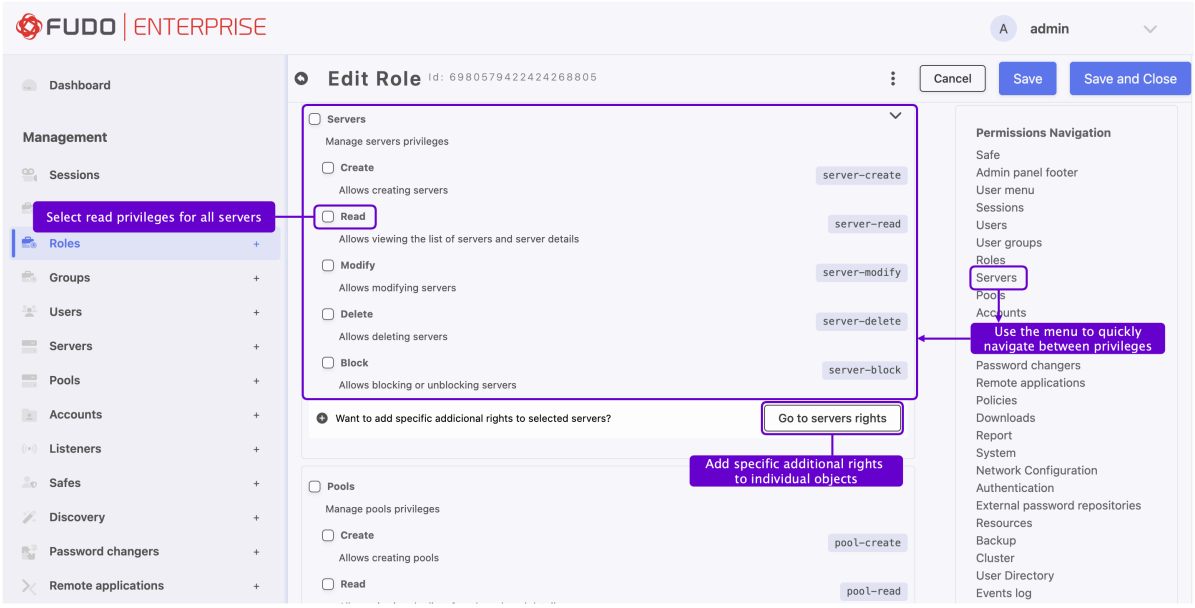
GLOBAL PRIVILEGES TAB

4. Go to the **GLOBAL PRIVILEGES** tab and select all privileges you want to assign to the created role.

Note

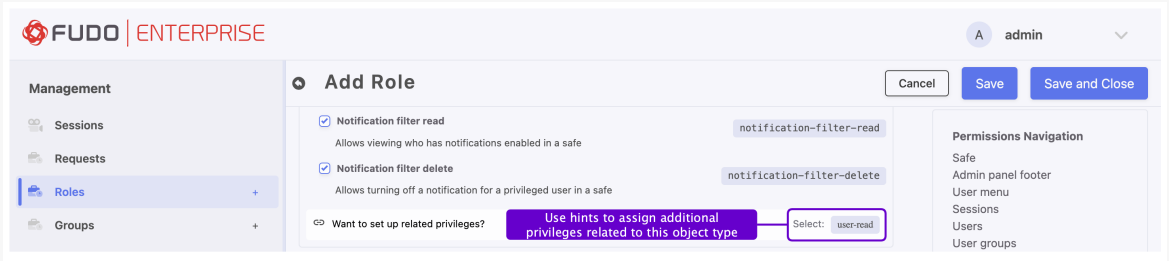
By selecting all privileges, you will grant this role all existing privileges, similar to the *super-admin* role in previous versions.

5. Go to the **Permissions Navigation** panel and click **Servers** to quickly navigate to the *Servers* privileges section.
6. In the **Servers** section, select the *Read* option (this will enable viewing all server configurations).



Note

You can use hints added at the end of each privileges section to assign additional privileges related to this object type, ensuring the full operability of the role.



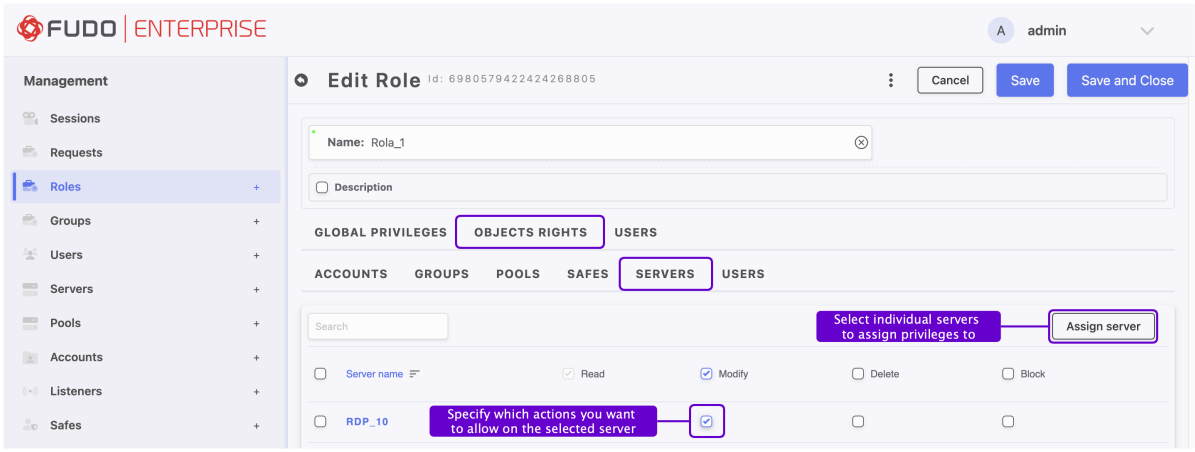
7. Click *Save* to create the role and proceed with further configuration.
8. To add specific additional rights to individual objects, use the *Go to...* button or navigate to the **OBJECT RIGHTS** tab.

OBJECT RIGHTS TAB

Note

In the OBJECT RIGHTS tab, you can assign capabilities to individual objects of the following types: accounts, groups, pools, safes, servers, and users.

9. Select the appropriate tab to assign permissions to the specified object (e.g., SERVERS).
10. Click *Assign server*.
11. In the **Server capability** dialog box, select one server from the list to which you want to grant capabilities.
12. Click *Save*.
13. Next, select the actions that can be performed on the selected server (e.g. *Modify*).



14. After completing the above steps, you will create a role with privileges to view all server configurations and modify only the servers selected in the OBJECT RIGHTS tab.

Warning

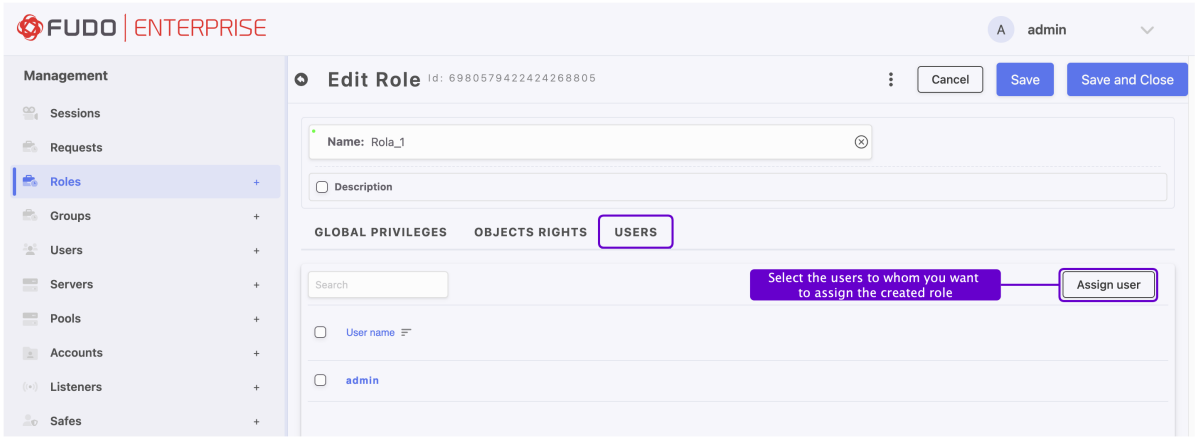
Please note the existence of the USERS sub-tab within the **CAPABILITIES** tab. This sub-tab is responsible for assigning capabilities to selected users (as objects), not for assigning roles to them.

USERS TAB

Note

In the USERS tab, you can assign the created role to users, granting them all the selected privileges.

15. Navigate to the **USERS** tab.
16. Click *Assign user*.
17. Select the users to whom you want to assign the created role.



18. Click *Save*.

Related topics:

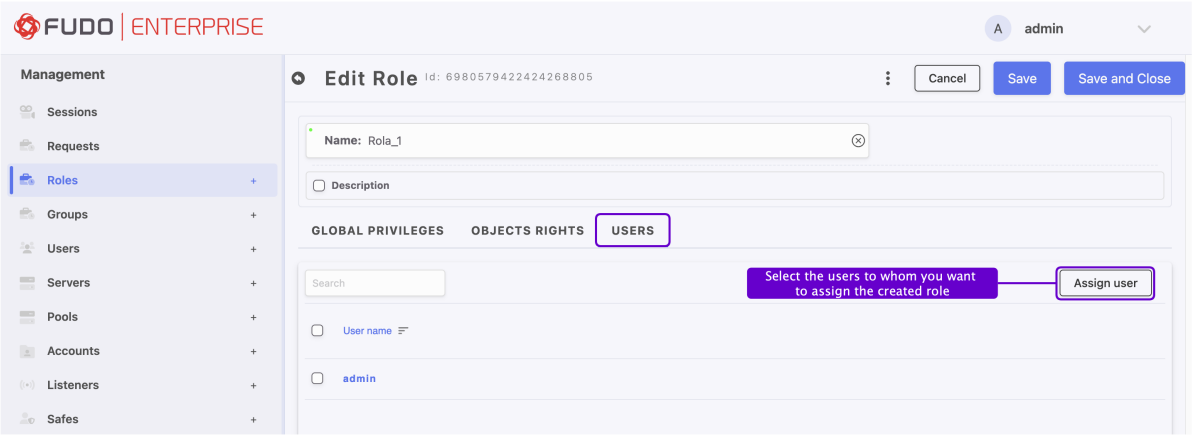
- *Typical Role Scenarios and Required Privileges*
- *Groups (RBAC)*
- *Users*

9.3.3 Assigning Roles to Users

You can assign a role to a user both from the role editing view and from the user editing view.

Assigning Role from the Role Editing View

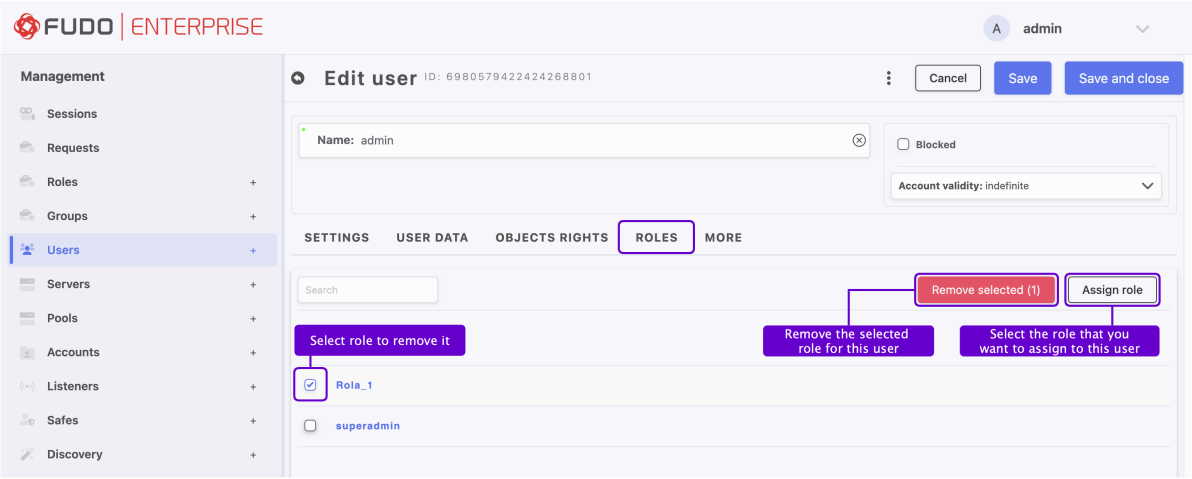
1. Select *User Management* > *Roles*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.
3. Find and click desired role's name to edit it.
4. Navigate to the **USERS** tab.
5. Click *Assign user*.
6. Select the users to whom you want to assign the created role.



7. Click *Save*.

Assigning Role from the User Editing View

1. Select *User Management* > *Users*.
2. Define filters to limit the number of objects displayed on the list.
3. Find and click desired user's name to access its configuration parameters.
4. Navigate to the **ROLES** tab.
5. Click *Assign Role* and select desired role from the list.
6. Click *Save* to close the modal window.
7. Click *Save and Close* to save changes to this user configuration.

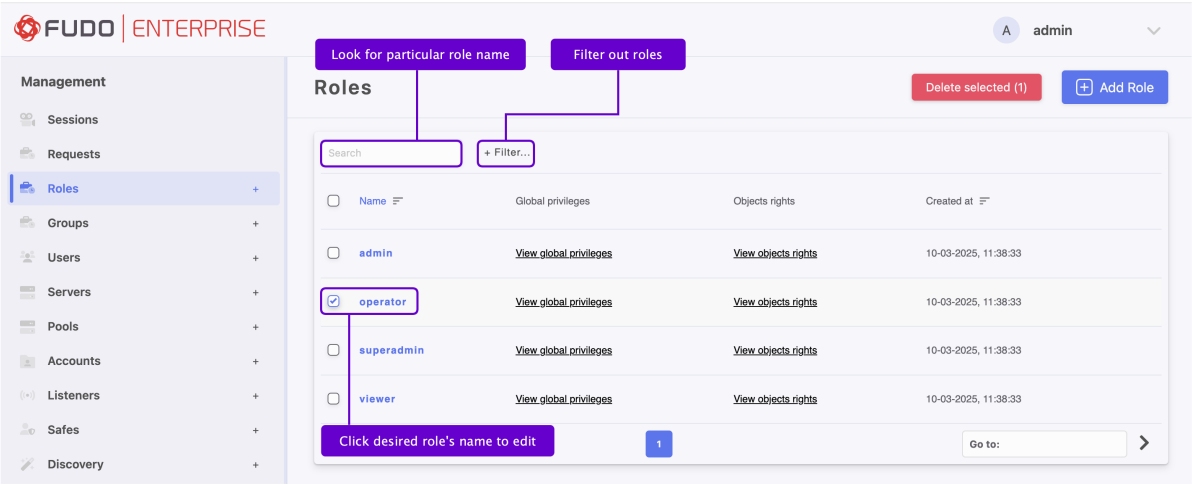


Related topics:

- *Role-Based Access Control (RBAC)*
- *Groups (RBAC)*
- *Users*

9.3.4 Modifying Roles

1. Select *User Management* > *Roles*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.
3. Find and click desired role's name to edit it.
4. Modify configuration parameters as needed.



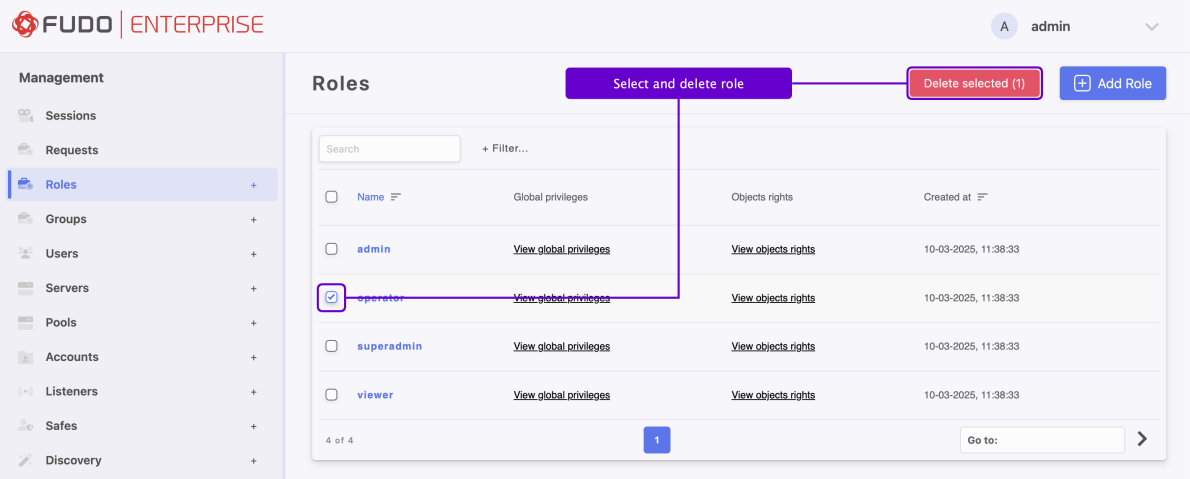
5. Click *Save and Close* to save changes to this configuration.

Related topics:

- *Role-Based Access Control (RBAC)*
- *Groups (RBAC)*
- *Users*

9.3.5 Deleting Roles

1. Select *User Management* > *Roles*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.
3. Find and click the checkbox next to the desired role's name to select it.
4. Click *Delete selected*.



5. Alternatively, you can edit a role that needs to be deleted right from the list, click the vertical three-dot icon and select *Remove role*.

Warning

Deleting a role that is assigned to users or groups will immediately revoke their access to all privileges and object rights granted through that role.

Related topics:

- *Role-Based Access Control (RBAC)*
- *Groups (RBAC)*
- *Users*

9.3.6 Typical Role Scenarios and Required Privileges

9.3.6.1 Tab-Level Access Control Matrix

This section provides a comprehensive overview of the privileges and/or capabilities required to access and perform actions within each part of the Fudo Enterprise user interface.

Each table corresponds to a top-level tab in the system. Depending on the complexity of the tab, the table may include:

- **Subsection**: A nested component or feature within the tab (e.g., "General > Date Time" under the System tab).
- **Action**: The specific operation (e.g., *visible*, *create*, *configure*) that can be controlled via access rights.
- **Privileges**: The required privilege(s) for a user to perform the action.

- **Capabilities**: If applicable, additional capability requirements are listed. If none are required, this column displays *None*.

Access control in the system is enforced based on a user's assigned roles, which in turn grant privileges and capabilities as needed.

Note

- Assigned capabilities for specific objects may cause certain tabs to appear in the UI, even if the user does not have the required privileges to perform any actions within those tabs.
- Some advanced tabs, such as Safes, require more than their own privileges (e.g., `safe-read`, `safe-create`). To fully create or manage a Safe, a user must also have privileges to view and select related resources—such as accounts, servers, pools, or groups—that are part of the Safe configuration.

Table 1: Privilege/Capability Matrix: Dashboard Tab

Action	Privileges	Capabilities
visible	`dashboard`	None

Table 2: Privilege/Capability Matrix: Sessions Tab

Action	Privileges	Capabilities
visible	`session-read`	None
backup	`session-backup`	None
delete	`session-delete`	None
download	`session-file-download`, `session-movie-download`	None
encode	`session-encode`	None
retention	`session-modify`	None

Table 3: Privilege/Capability Matrix: Requests Tab

Action	Privileges	Capabilities
visible	`access-request-read`	None

Table 4: Privilege/Capability Matrix: Roles Tab

Action	Privileges	Capabilities
visible	`role-read`	None
create	`role-create`	None
modify	`role-modify`	None
delete	`role-delete`	None

Table 5: Privilege/Capability Matrix: Users Tab

Action	Privileges	Capabilities
visible	`user-create`, `user-read`	`user`
create	`user-create`	None

Table 6: Privilege/Capability Matrix: Groups Tab

Action	Privileges	Capabilities
visible	`group-create`, `group-read`	`group`
create	`group-create`	None

Table 7: Privilege/Capability Matrix: Servers Tab

Action	Privileges	Capabilities
visible	`server-create`, `server-read`	`server`
create	`server-create`	None

Table 8: Privilege/Capability Matrix: Pools Tab

Action	Privileges	Capabilities
visible	`pool-create`, `pool-read`	`pool`
create	`pool-create`	None

Table 9: Privilege/Capability Matrix: Accounts Tab

Action	Privileges	Capabilities
visible	`account-create`, `account-read`	`account`
create	`account-create`	None

Table 10: Privilege/Capability Matrix: Listeners Tab

Action	Privileges	Capabilities
visible	`listener-create`, `listener-read`	None
create	`listener-create`	None
modify	`listener-modify`	None
delete	`listener-delete`	None

Table 11: Privilege/Capability Matrix: Safes Tab

Subsection	Action	Privileges	Capabilities
Safes			
	visible	`safe-create`, `safe-read`	`safe`
	create	`safe-create`	None
Notifications			
	visible	`notification-filter-read`, `notification-filter-create`	None
	create	`notification-filter-create`	None
	delete	`notification-filter-delete`	None

Table 12: Privilege/Capability Matrix: Discovery Tab

Subsection	Action	Privileges	Capabilities
Scanners			
	visible	`scanner-read`	None
	create	`scanner-create`	None
	modify	`scanner-modify`	None
	delete	`scanner-delete`	None
	start	`scanner-start`	None
Rules			
	visible	`discovery-rule-read`	None
	create	`discovery-rule-create`	None
	modify	`discovery-rule-modify`	None
	delete	`discovery-rule-delete`	None

Table 13: Privilege/Capability Matrix: Secret Changers Tab

Subsection	Action	Privileges	Capabilities
Secret Changer			
	visible	`password-changer-read`	None
	create	`password-changer-create`	None
	modify	`password-changer-modify`	None
	delete	`password-changer-delete`	None
Password Policy			
	visible	`password-change-policy-read`	None
	create	`password-change-policy-create`	None
	modify	`password-change-policy-modify`	None
	delete	`password-change-policy-delete`	None

Table 14: Privilege/Capability Matrix: Remote Applications Tab

Action	Privileges	Capabilities
visible	`remoteapp-read`	None
create	`remoteapp-create`	None
modify	`remoteapp-modify`	None
delete	`remoteapp-delete`	None

Table 15: Privilege/Capability Matrix: Policies Tab

Subsection	Action	Privileges	Capabilities
Policy			
	visible	`policy-read`	None
	create	`policy-create`	None
	modify	`policy-modify`	None
	delete	`policy-delete`	None
Regexp			
	visible	`regexp-read`	None
	create	`regexp-create`	None
	modify	`regexp-modify`	None
	delete	`regexp-delete`	None

Table 16: Privilege/Capability Matrix: Downloads Tab

Subsection	Action	Privileges	Capabilities
Files			
	visible	`session-file-read`	None
	download	`session-file-download`	None
	delete	`session-file-delete`	None
Movies			
	visible	`session-movie-read`	None
	download	`session-movie-download`	None
	delete	`session-movie-delete`	None

Table 17: Privilege/Capability Matrix: Reports Tab

Action	Privileges	Capabilities
visible	`report-read`	None
create	`report-create`	None
modify	`report-modify`	None
delete	`report-delete`	None

Table 18: Privilege/Capability Matrix: Productivity Tab

Action	Privileges	Capabilities
visible	`productivity-read`	None

Note

If the license disables productivity analysis, the **Productivity** category is not displayed in role configuration — neither when adding or editing a role, nor in the global privileges view. Refer to the *Productivity* section for more information.

Table 19: Privilege/Capability Matrix: System Tab

Subsection	Action	Privileges	Capabilities
General > Date Time			
	visible	`datetime-read`	None

continues on next page

Table 19 – continued from previous page

Subsection	Action	Privileges	Capabilities
	configure	`datetime-modify`	None
General > NTP			
	visible	`ntp-read`	None
	configure	`ntp-modify`	None
General > Certificates			
	visible	`certificate-read`	None
General > Certificates > Fudo Admin Panel			
	visible	`certificate-read`	None
	configure	`certificate-mgmt`	None
General > Certificates > User Access Gateway			
	visible	`certificate-read`	None
	configure	`certificate-uag`	None
General > Certificates > User CA			
	visible	`certificate-read`	None
	configure	`certificate-client`	None
General > Access Gateway Allowed Hosts			
	visible	`uag-hosts-read`	None
	configure	`uag-hosts-modify`	None
General > Maintenance Supervision > Deny New Connections			
	visible	`maintenance-read`	None
	configure	`deny-new-connections`	None

continues on next page

Table 19 – continued from previous page

Subsection	Action	Privileges	Capabilities
General > Maintenance Supervision > Tech Support Access			
	visible	`maintenance-read`	None
	configure	`tech-support-access`	None
General > Maintenance Supervision > Healthcheck Api			
	visible	`maintenance-read`	None
	configure	`healthcheck-api`	None
General > Maintenance Supervision > Callhome			
	visible	`maintenance-read`	None
	configure	`callhome`	None
General > Masterkey			
	visible	`masterkey-read`	None
	export	`masterkey-export`	None
	invalidate	`masterkey-invalidate`	None
General > Snmp			
	visible	`snmp-read`	None
	configure	`snmp-modify`	None
General > Timestamping			
	visible	`timestamp-read`	None
	configure	`timestamp-modify`	None
General > Changers			
	visible	`password-changer-node-read`	None
	configure	`password-changer-node-modify`	None

continues on next page

Table 19 – continued from previous page

Subsection	Action	Privileges	Capabilities
General > Discovery			
	visible	`discovery-node-read`	None
	configure	`discovery-node-modify`	None
General > Sensitive Features			
	visible	`sensitive-feature-read`	None
	configure	`sensitive-feature-modify`	None
General > HTTP Proxy			
	visible	`http-proxy-read`	None
	configure	`http-proxy-modify`	None
Upgrade			
	visible	`upgrade-read`	None
	upload	`upgrade-upload`	None
	check	`upgrade-check`	None
	install	`upgrade-install`	None
	delete	`upgrade-delete`	None
	snapshc delete	`upgrade-snapshot-delete`	None
Hotfix			
	visible	`hotfix-read`	None
	upload	`hotfix-upload`	None
	install	`hotfix-install`	None
	delete	`hotfix-delete`	None
License			
	visible	`license-read`	None
	configure	`license-upload`	None
Diagnostic			
	visible	`diagnostic`	None
Configuration > Export			
	visible	`configuration-export`	None

continues on next page

Table 19 – continued from previous page

Subsection	Action	Privileges	Capabilities
Configuration > Import			
	visible	`configuration-import`	None
Configuration > Service Data			
	visible	`service-data`	None

Table 20: Privilege/Capability Matrix: Network Tab

Subsection	Action	Privileges	Capabilities
Interfaces			
	visible	`network-read`	None
	configure	`network-modify`	None
DNS			
	visible	`network-read`	None
	configure	`network-modify`	None
Routing			
	visible	`network-read`	None
	configure	`network-modify`	None
ARP			
	visible	`network-read`	None
	configure	`network-modify`	None
Labels			
	visible	`label-read`	None
	configure	`label-modify`	None

Table 21: Privilege/Capability Matrix: External Storage Tab

Action	Privileges	Capabilities
visible	`external-storage-read`	None
configure	`external-storage-modify`	None

Table 22: Privilege/Capability Matrix: Notifications Tab

Action	Privileges	Capabilities
visible	`smtp-read`	None
configure	`smtp-modify`	None

Table 23: Privilege/Capability Matrix: Artificial Intelligence Tab

Action	Privileges	Capabilities
visible	`ai-read`	None
configure	`ai-modify`	None

Table 24: Privilege/Capability Matrix: Authentication Tab

Subsection	Action	Privileges	Capabilities
External			
	visible	`extauth-read`	None
	create	`extauth-create`	None
	modify	`extauth-modify`	None
	delete	`extauth-delete`	None
Openid Connect			
	visible	`oidc-read`	None
	create	`oidc-create`	None
	modify	`oidc-modify`	None
	delete	`oidc-delete`	None
JWT Providers			
	visible	`jwt-provider-read`	None
	create	`jwt-provider-create`	None
	modify	`jwt-provider-modify`	None
	delete	`jwt-provider-delete`	None
	refresh keys	`jwt-provider-modify`	None
Global			
	visible	`authentication-read`	None
	configure	`authentication-modify`	None

Table 25: Privilege/Capability Matrix: External Password Repositories Tab

Action	Privileges	Capabilities
visible	`passvn-read`	None
create	`passvn-create`	None
modify	`passvn-modify`	None
delete	`passvn-delete`	None

Table 26: Privilege/Capability Matrix: Resources Tab

Subsection	Action	Privileges	Capabilities
Protocols			
	visible	`logo-read`	None
	configure	`logo-modify`	None
User Portal			
	visible	`logo-read`	None
	configure	`logo-modify`	None

Table 27: Privilege/Capability Matrix: Backup And Retention Tab

Subsection	Action	Privileges	Capabilities
Backup			
	visible	`backup-read`	None
	create	`backup-create`	None
	modify	`backup-modify`	None
	delete	`backup-delete`	None
Retention			
	visible	`retention-read`	None
	configure	`retention-modify`	None

Table 28: Privilege/Capability Matrix: Cluster Tab

Subsection	Action	Privileges	Capabilities
Nodes			
	visible	`cluster-read`	None
	create	`cluster-modify`	None
	modify	`cluster-modify`	None
	delete	`cluster-modify`	None
	cluster_cre	`cluster-modify`	None
	cluster_joi	`cluster-modify`	None
Redundancy Groups			
	visible	`cluster-read`	None
	create	`cluster-modify`	None
	modify	`cluster-modify`	None
	delete	`cluster-modify`	None
	failover	`cluster-failover`	None

Table 29: Privilege/Capability Matrix: User Directory Tab

Action	Privileges	Capabilities
visible	`user-directory-read`	None
create	`user-directory-create`	None
modify	`user-directory-modify`	None
delete	`user-directory-delete`	None

Table 30: Privilege/Capability Matrix: Events Log Tab

Action	Privileges	Capabilities
visible	`log-read`	None

Table 31: Privilege/Capability Matrix: ShareAccess Tab

Action	Privileges	Capabilities
visible	`fudo-network`	None

9.3.6.2 Dashboard Widgets Visibility

The visibility of individual widgets on the Dashboard depends on the following privileges:

Table 32: Privileges Required to View All Dashboard Widgets

Privilege	Description	Corresponding Widget
`dashboard`	Allows accessing the Dashboard tab	Dashboard tab visibility
`account-rea`	Allows viewing the list of accounts and account details	Account Alerts
`user-read`	Allows viewing the users list and user details	Active Users
`session-rea`	Allows viewing the list of sessions and session details	Suspicious Sessions, New Sessions, Concurrent Sessions
`configurati`	Allows previewing the Configuration tab	License
`log-read`	Allows viewing the events log	Logs
`cluster-rea`	Allows viewing cluster configuration	Node

If the user has a capability to any **user** or **account** and the `dashboard` global privilege assigned, they will also see the **Active Users** and **Account Alerts** widgets, respectively.

Note

When the user's role changes, some widgets may move to the Dashlet's Market. To make them visible again, check the market and add the widgets back to the Dashboard if needed.

9.3.6.3 Sessions Tab Permissions

To view and interact with the **Sessions** tab, the user must have the following privileges:

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

In addition, to see a specific session on the list, the user must have **read access to all objects** associated with the session:

- The user involved in the session,
- The corresponding server,
- The account used,
- The related safe (if applicable).

Playback and Preview

To view or play back a session, the following privileges are required:

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

- Read access to all associated objects (user, server, account, safe)

Session Backup

The `session-backup` privilege allows sending a session to backup. This action does **not** modify the session, which is why it is handled with a dedicated privilege.

Session Management

The `session-modify` privilege grants access to advanced session management operations. Users with this privilege can perform the following actions **for sessions they have access to**:

- Restore a session from backup,
- Download files transferred via SCP or SFTP,
- Approve or reject a session if the **require approval** option is enabled in the safe,
- Send the session to other nodes,
- Revoke session sharing,
- Modify editable session attributes,
- Modify session timestamps.

9.3.6.4 Downloads Tab Permissions

Access to the **Downloads tab**, which allows users to retrieve session-related files (such as session recordings and transferred files), is governed by the following privileges:

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

However, privileges from the following groups alone do not grant access to all sessions globally. In order to view and download files from a specific session, the user must also have access rights to all objects associated with that session, including:

- the user who initiated the session,
- the target server,
- the account used, and
- the safe in which these objects are stored.

These object-level access rights can be granted either through dedicated global privileges or via appropriate capability assignments.

9.3.6.5 Safes Management

> **Note**
>
> To manage accounts in safes, the user must have at least the `listener-read` privilege from the Listener privileges list, regardless of their existing permissions for the accounts themselves.

To create a safe, the following **minimum** privileges are required:

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

Additionally, the following privileges are required for specific actions:

- To assign groups to the safe:
  - `group-read`
- To manage notifications:
  - `notification-filter-read`
  - `notification-filter-create`
  - `notification-filter-delete`
- To assign policies:
  - `policy-read`

9.3.6.6 Discovery Tab Permissions

To fully manage the **Discovery tab** it is required to have all below tab related privileges:

- `scanner-read`
- `scanner-create`
- `scanner-modify`
- `scanner-delete`
- `scanner-start`
- `discovery-rule-read`
- `discovery-rule-create`
- `discovery-rule-modify`
- `discovery-rule-delete`
- `listener-read`
- `server-read`
- `account-read`
- `password-changer-read`
- `password-change-policy-read`

Note

Please note that to view the list of Discovery rules in the Discovery tab, the `listener-read` privilege is also required.

To access the Discovery node settings (**System** > **General** > **Discovery**), the user needs the following privileges:

- `discovery-node-read`
- `discovery-node-modify`
- `cluster-read`

9.3.6.7 Access Request Permissions

To vote on an Access Request, a user must meet the following conditions:

- Have the `access-request-read` privilege – grants access to the *Requests* tab.
- Have the `access-request-vote` privilege – grants the ability to vote on requests.
- Have `read` permissions for the following objects related to the request:
  - **User** – the requesting user.
  - **Server**/**Pool** - the server or pool of servers for which access is requested.
  - **Safe** – the safe containing the requested account.
  - **Account** – the account the request concerns.

Proper configuration of object-level permissions and capabilities is required to participate in the approval workflow.

9.3.6.8 Fudo Officer

Pairing the Fudo Officer mobile app with an account requires one of the following:

- The user pairs the app in the Admin Panel. The user needs access to the Admin Panel and the `modify` capability for their own account.
- An administrator initiates the pairing for the user, and the user completes it by scanning the QR code in the User Access Gateway or in the Admin Panel. The administrator needs the `modify` capability for the user's account. The user needs no additional capabilities.

A user can always remove the pairing of their own account. To remove the pairing of another user's account, an administrator needs the `modify` or `delete` capability for that account.

For the Fudo Officer app to function fully, the following permissions are required for the user:

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

- `access-request-read`

Access to the Password Vault in the Fudo Officer app is controlled by the access levels assigned to collections, in the same way as in the User Access Gateway. See *Assigning Users and Groups to Collections*.

9.3.6.9 Reports Tab Permissions

> **Note**
>
> Only users with the `report-read` and `system-report-read` permissions are allowed to access system reports, which are automatically triggered by the system. Such reports contain all data from the system, including all objects.

`report-create`

- Ensures that a report will be generated and will appear under **Reports** → **Reports**.
- Allows generating reports from the **Sessions** tab.

`report-read`

- Required to view any report.
- Users cannot view reports generated by other users.
- Allows viewing reports according to existing subscriptions, historical reports, and those generated from the **Sessions** tab.

`report-modify`

- Allows managing report subscriptions from the **Reports** → **Settings** tab.
- An admin can add a subscription for any type of report.
- Generated data is limited to objects and data to which the user has permissions.

> **Note**
>
> Data in the generated report is limited to objects and other information to which the user has access.

`report-delete`

- Users can only delete their own reports.

`system-report-read`

- Grants access to system-level report content, **regardless of assigned capabilities or privileges**.
- Must be combined with `report-read` to make system reports and the **Reports** tab visible.
- This permission is **intended** to be assigned exclusively to users with the `superadmin` role.

9.3.6.10 Sudo Policy Permissions

For the sudo plugin to authorize commands through Fudo Enterprise, the user requires the following privileges:

- `user-read`
- `policy-read`
- `regexp-read`
- `session-read`
- `sudo-approval`

Danger

All five privileges are mandatory. Missing any privilege causes the plugin to deny ALL sudo commands on the target system.

Related topics:

- *Groups (RBAC)*
- *Users*

CHAPTER 10

Session Management

10.1 Servers

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

- Fudo Enterprise allows configuring a server with one unique address and a server with a group of addresses to be connected within a specified network.
- Once the server definition is configured and saved, the Fudo Enterprise allows grouping multiple servers within one Server Pool so all the added servers are managed as one server within other objects.

10.1.1 Creating a Server

10.1.1.1 Creating an HTTP Server

Note

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.

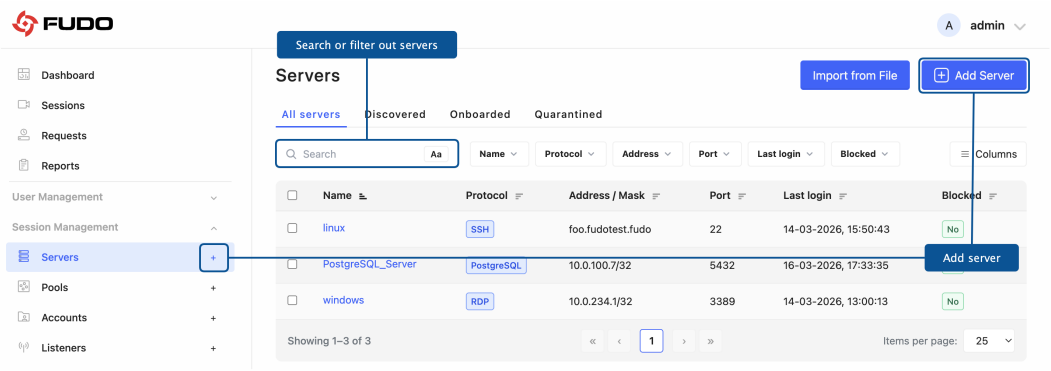
Warning

HTTP rendering is a CPU intensive process and may have negative impact on system's performance. A physical appliance is recommended for monitoring rendered HTTP connections with the following limitations regarding the maximum number of concurrent rendered HTTP sessions.

Model	Maximum recommended number of concurrent HTTP sessions*
F100x	2
F300x	5
F500x	10

* The actual value depends on the Fudo Enterprise instance configuration.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, select `HTTP`.

Warning

After server's definition is saved, protocol's field is uneditable.

3. Select the *TLS enabled* option to connect to monitored server over TLS.
4. Select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
5. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

6. If you do not use the SSH tunnel, from the Network address drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.
7. In the *HTTP host* field provide the HTTP host header value.

Note

The HTTP host header determines the requested content in case there are many web sites hosted on the specified server.

7. Enter value of the *HTTP timeout* parameter, determining the time period of inactivity (expressed in seconds), after which the user will have to authenticate again.
8. Click the *HTTP Authentication* option to enable additional verification process and select one of the available platforms. If `None` is selected, provide custom login page details:
   - *Login page URL*,
   - *Username* and *Password*,
   - optionally, check the *Press the enter key prior to password* option.

Note

HTTP authentication is active only when the *Render sessions* option is enabled in the HTTP listener settings. To enable *Render sessions* option, please refer to the *Setting up the HTTP Listener* topic.

9. From the *Network address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

10. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

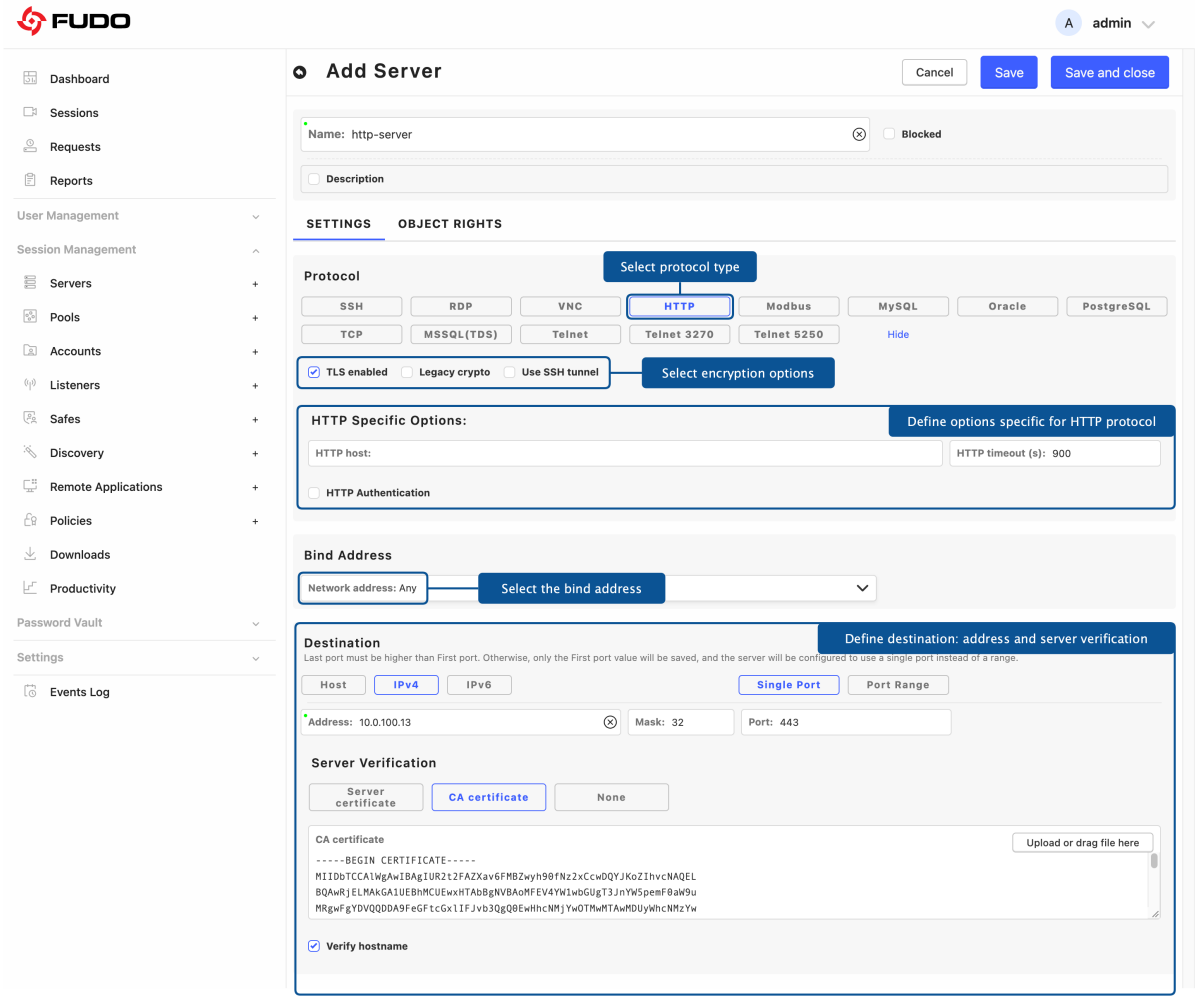
Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.
- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does

not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

- If the *TLS enabled* was checked, in the *Server verification* section select one of the following options:`Server certificate` or `CA certificate` and provide respective certificate data. Select `None` to disable server verification.

  If you select `CA certificate`, the *Verify hostname* option is also available and checked by default. It additionally checks that the server certificate covers the configured server address (host name or IP address) - or the *HTTP host* value, if provided; if it does not, the connection to the server fails. Clear the option to verify the certificate against the CA certificate only, for example when the certificate was issued for a name other than the configured address. The option does not apply to rendered HTTP sessions (the *Render sessions* option in the HTTP listener settings): in such sessions the browser always checks that the certificate covers the address, and clearing the option does not turn this check off.



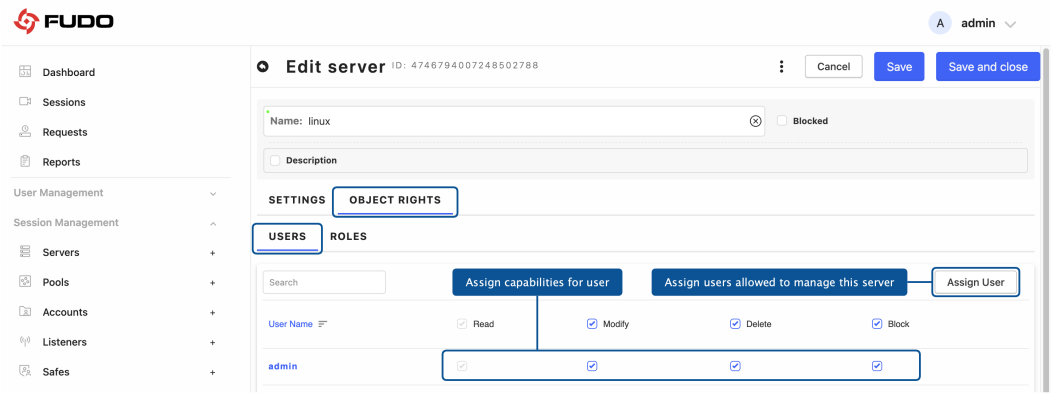
11. Click *Save*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.

2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

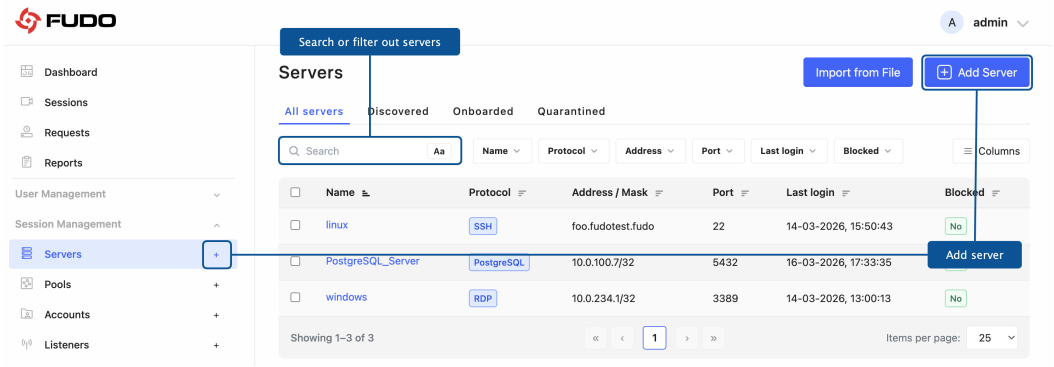
- *Pools*
- *Protocols - HTTP*
- *Data model*
- *Accounts*
- *Listeners*
- *Safes*

10.1.1.2 Creating a Modbus Server

Note

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, select `Modbus`.
3. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

4. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Warning

After server's definition is saved, protocol's field is uneditable.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled*

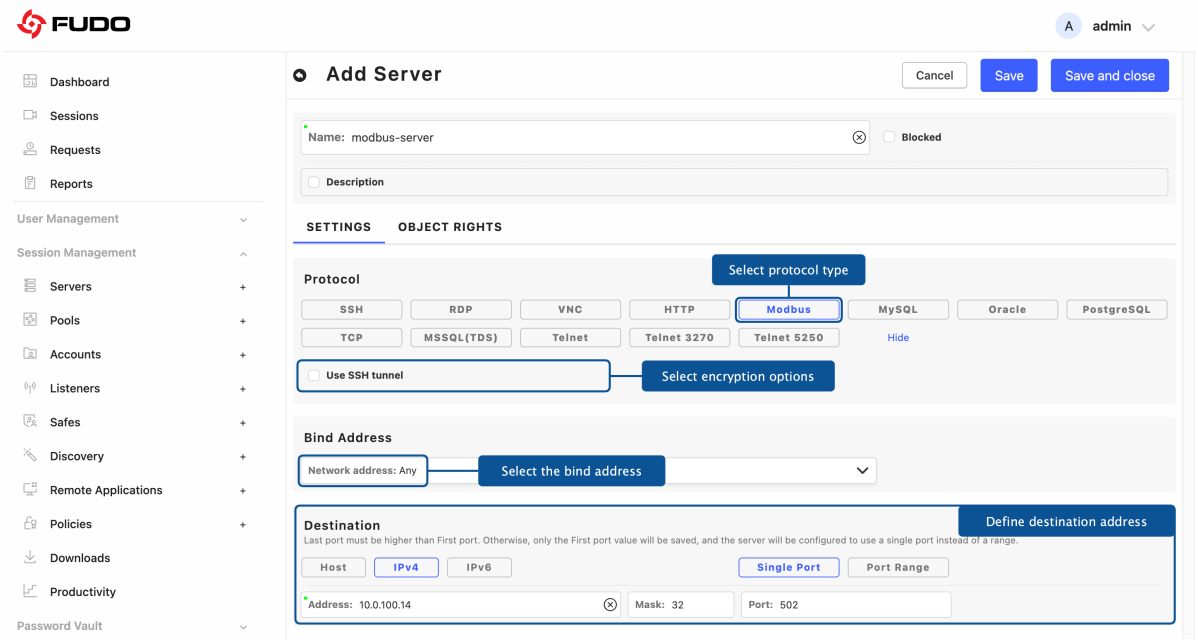
IP Addresses).

- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

4. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.
- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).



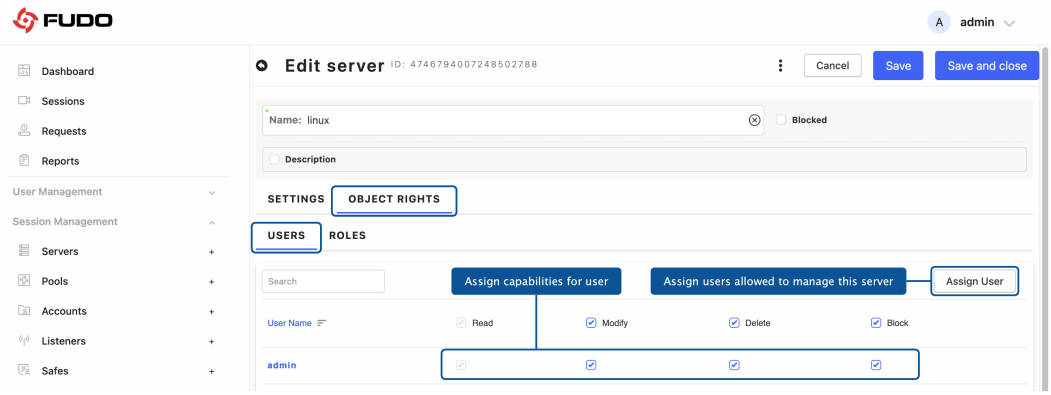
5. Click *Save*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.

5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

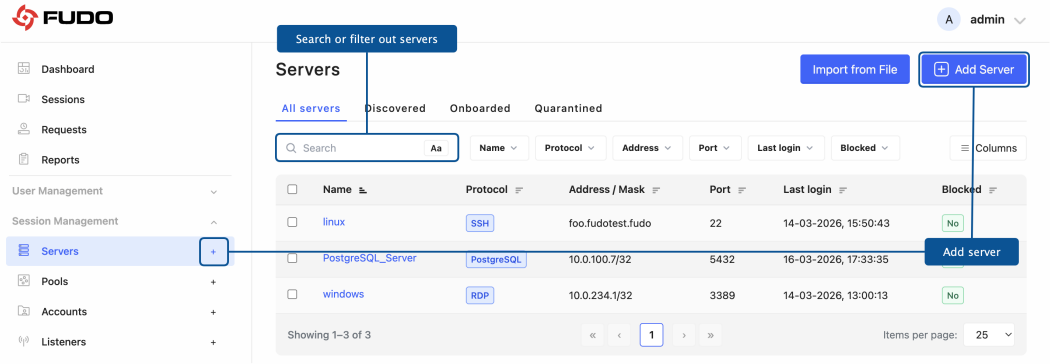
- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.3 Creating a MS SQL Server

Note

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, select `MSSQL(TDS)`.
3. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

4. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Warning

After server's definition is saved, protocol's field is uneditable.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

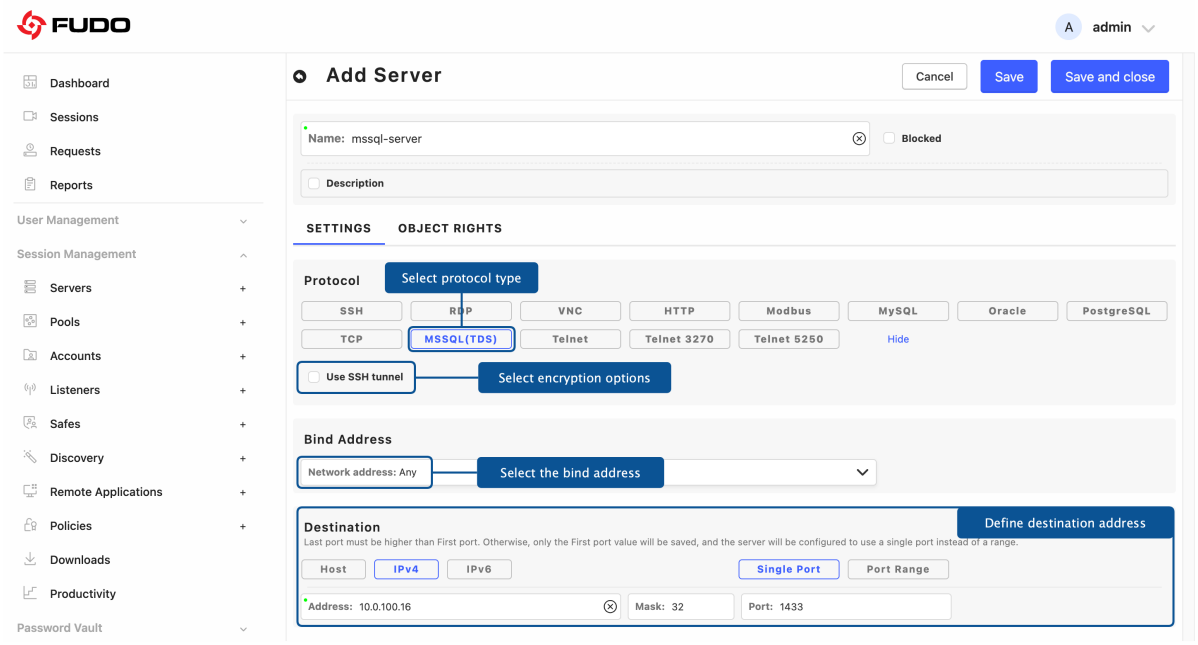
5. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique

address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.

- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

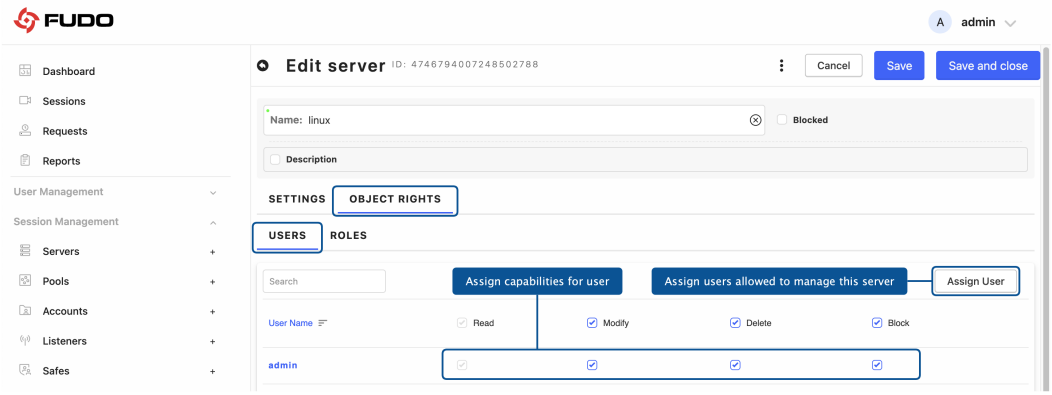


6. Click *Save*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.4 Creating a MySQL Server

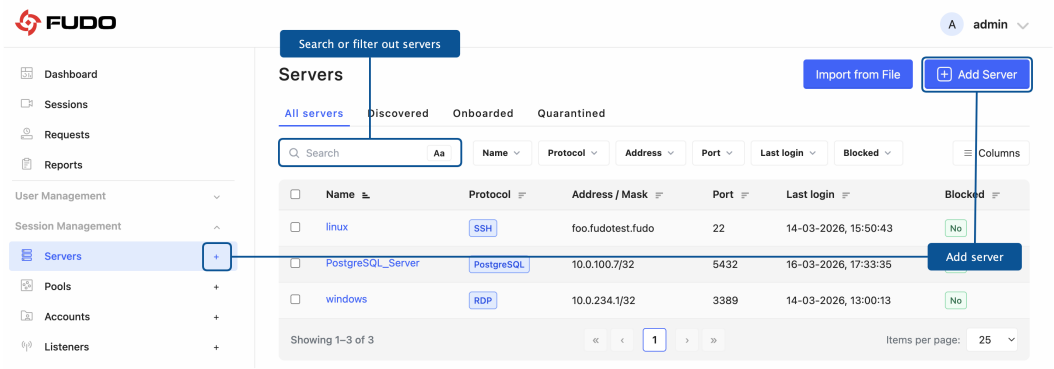
Warning

- The following MySQL authentication plugins are supported for communication between Fudo Enterprise and the database server: `mysql_clear_password` `mysql_native_password`, `caching_sha2_password`.
- For communication between the client and Fudo Enterprise, only `mysql_clear_password` plugin is supported, which is why TLS is enforced for MySQL listeners.

Note

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, select `MySQL`.

Warning

After server's definition is saved, protocol's field is uneditable.

3. Select the *TLS enabled* option to connect to monitored server over TLS.
4. Select *Legacy crypto* option to allow negotiating older encryption algorithms when establishing connections.
5. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

6. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

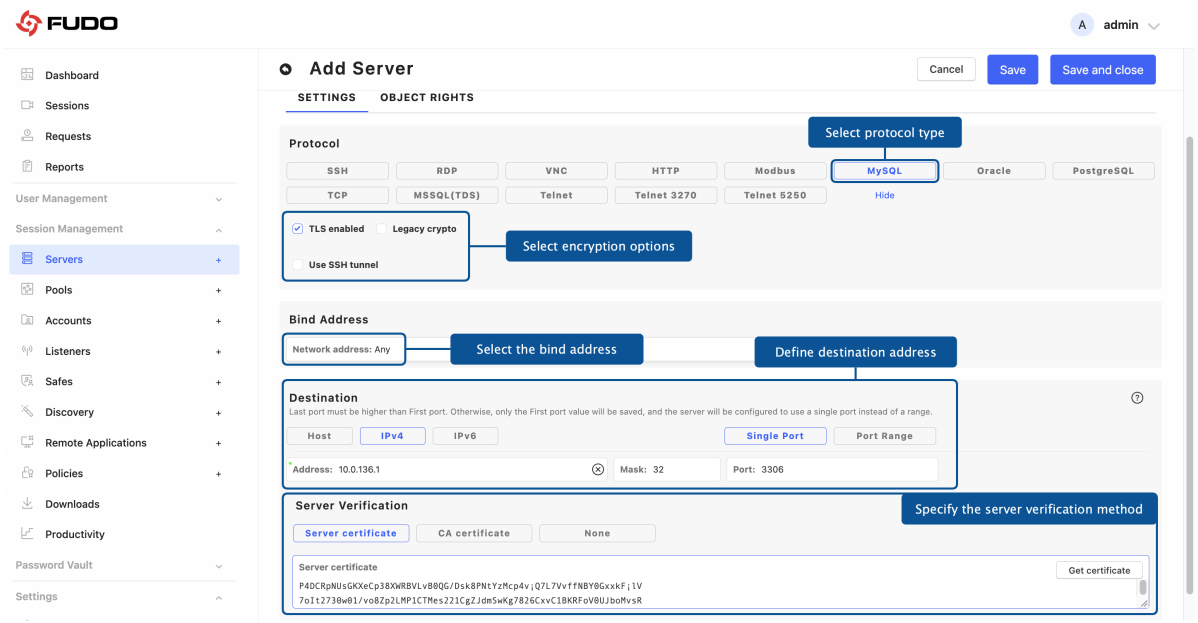
7. In the *Destination* section, define the address of the target server:
   - Select `Host`, `IPv4`, or `IPv6`,
   - Enter the *Address* and *Port* if the port differs from the protocol default. You can also specify a port range. For details, see *Port Ranges in Server Configuration*.

Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.
- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

8. In the *Server Verification* section, specify the server verification method:
   - Select `Server certificate` to verify the server based on its certificate,
   - Select `CA certificate` to verify the server certificate using a trusted certificate authority,
   - Select `None` to disable server certificate verification.

   If you select `CA certificate`, the *Verify hostname* option is also available and checked by default. It additionally checks that the server certificate covers the configured server address (host name or IP address); if it does not, the connection to the server fails. Clear the option to verify the certificate against the CA certificate only, for example when the certificate was issued for a name other than the configured address.

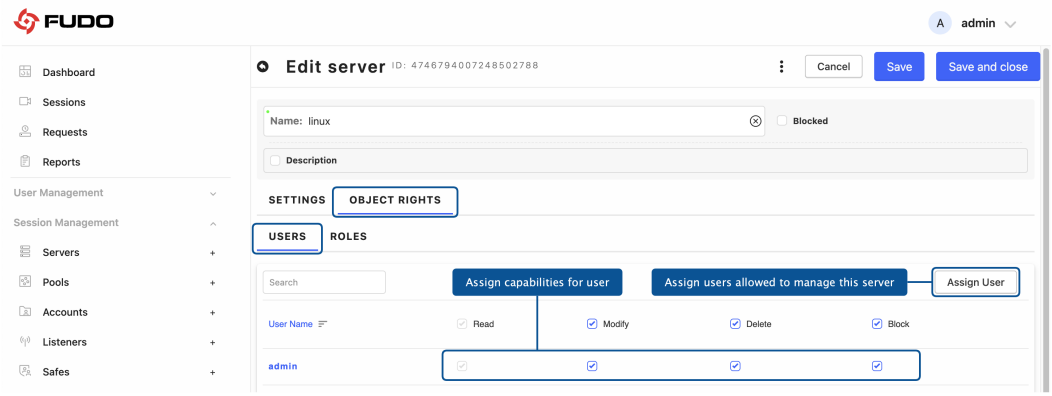


9. Click *Save* or *Save and close*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

- *Pools*

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.5 Creating an Oracle Server [BETA]

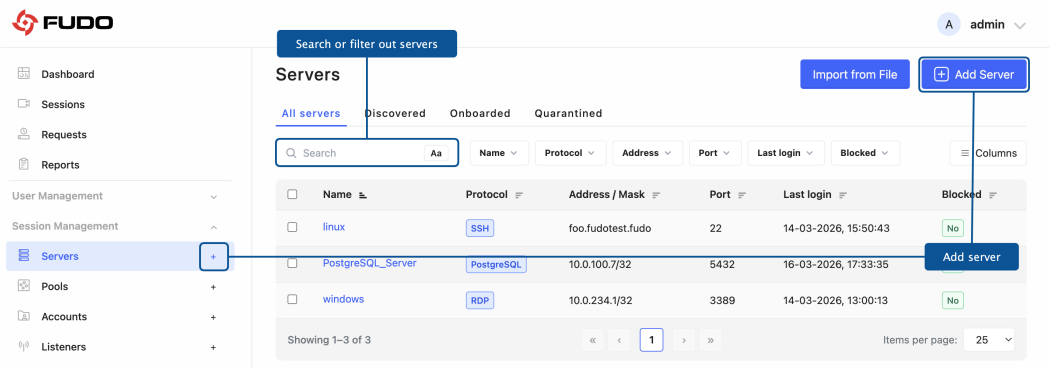
Warning

- *TLS enabled* is selected by default. Clear it if the monitored database does not accept TCPS connections, otherwise the connection to the server fails.
- Encrypted connections are supported with the Oracle SQL*Plus client. Other client applications do not support TLS with Fudo Enterprise.
- Oracle native encryption (Advanced Security Option) is refused. Configure clients so that they do not negotiate it.

Note

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- Accounts of the *regular* type are not available for Oracle servers, so password substitution cannot be used - users log in to the database with their own credentials. See *Accounts*.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.

5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, press the `Show all` button and select `Oracle`.

Warning

After server's definition is saved, protocol's field is uneditable.

3. Clear or leave the *TLS enabled* option depending on whether the monitored database accepts TCPS connections.
4. Select *Legacy crypto* option to allow negotiating older encryption algorithms when establishing connections.
5. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.
6. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Note

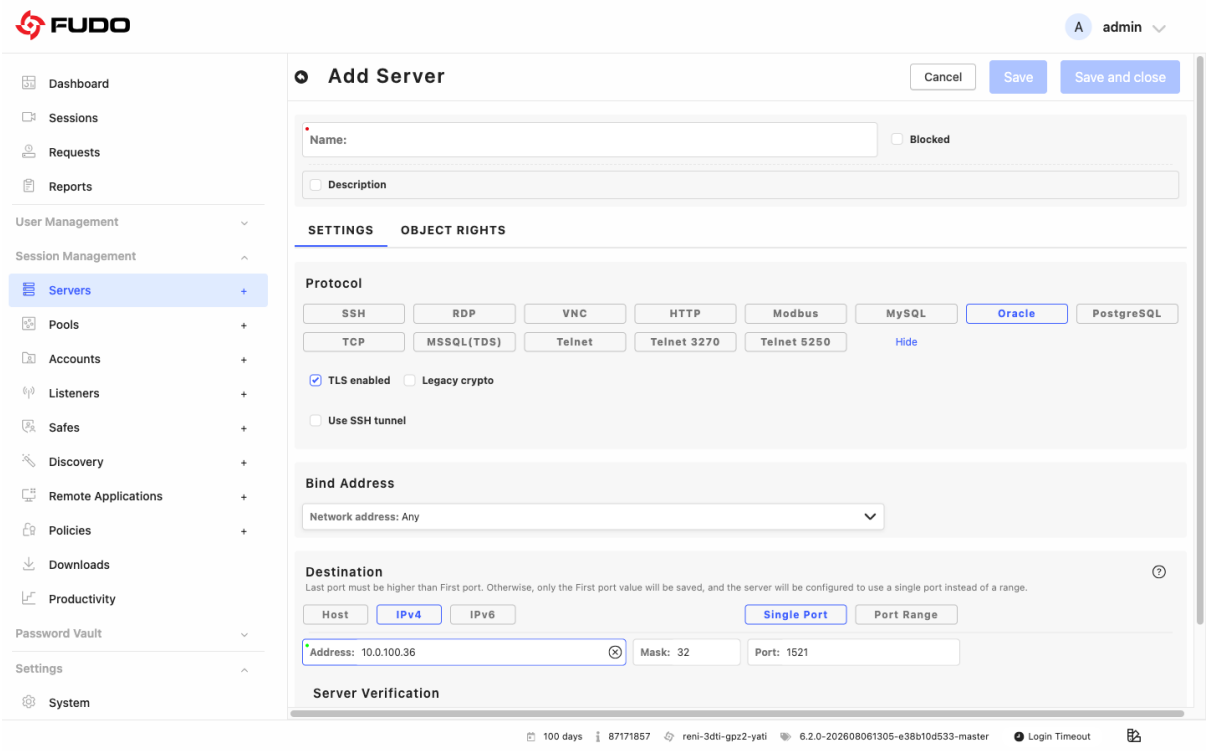
The *Legacy crypto* option is shown only when *TLS enabled* is selected.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

7. In the *Destination* section, define the address of the target server:
   - Select `Host`, `IPv4`, or `IPv6`,
   - Enter the *Address*. The *Port* field is filled in with the Oracle default `1521`; change it if the database listens on a different port.
8. In the *Server Verification* section, specify the server verification method:
   - Select `Server certificate` to verify the server based on its certificate,
   - Select `CA certificate` to verify the server certificate using a trusted certificate authority,
   - Select `None` to disable server certificate verification.

If you select `CA certificate`, the *Verify hostname* option is also available and checked by default. It additionally checks that the server certificate covers the configured server address (host name or IP address); if it does not, the connection to the server fails. Clear the option to verify the certificate against the CA certificate only, for example when the certificate was issued for a name other than the configured address.

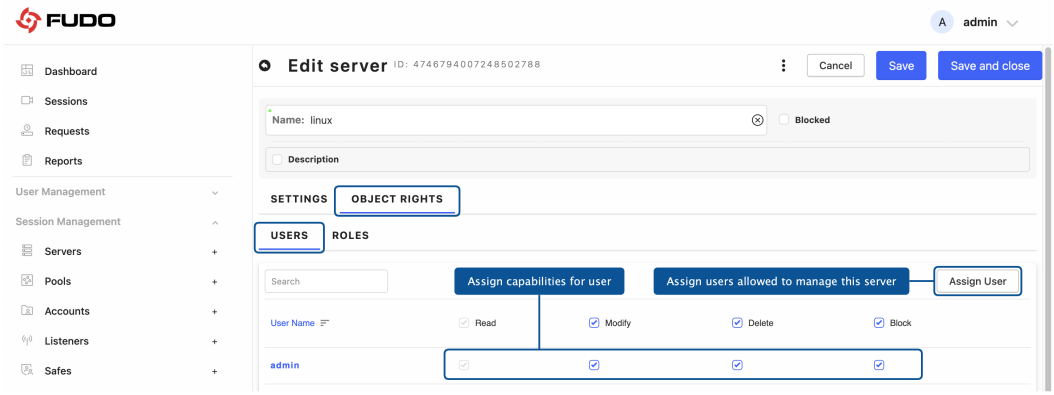


9. Click *Save* or *Save and close*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.

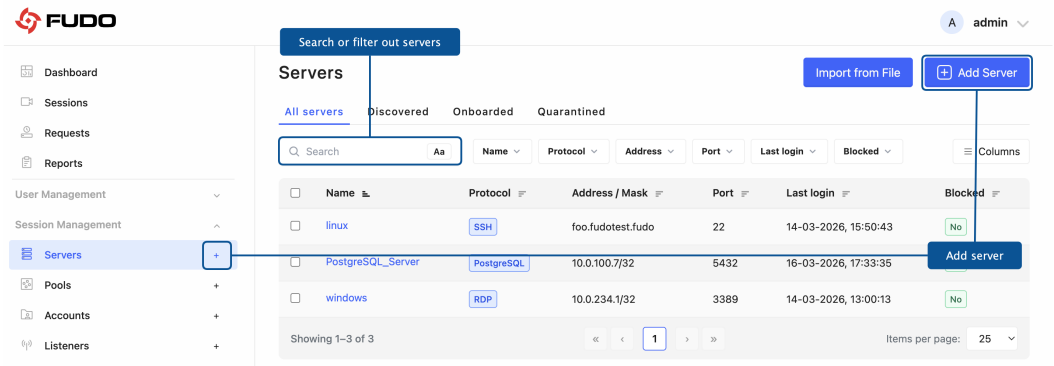


Related topics:

- *Setting up the Oracle Listener [BETA]*
- *Pools*
- *Data model*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.6 Creating a PostgreSQL Server

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.

2. In the *Protocol* section, click *Show all* and select `PostgreSQL`.

Warning

After server's definition is saved, protocol's field is uneditable.

3. Select the *TLS enabled* option to connect to monitored server over TLS.
4. Select *Legacy crypto* option to allow negotiating older encryption algorithms when establishing connections.
5. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

6. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Bind address* and *Destination* settings.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

7. In the *Destination* section, define the address of the target server:
   - Select `Host`, `IPv4`, or `IPv6`,
   - Enter the *Address* and *Port* if the port differs from the protocol default (5432). You can also specify a port range. For details, see *Port Ranges in Server Configuration*.

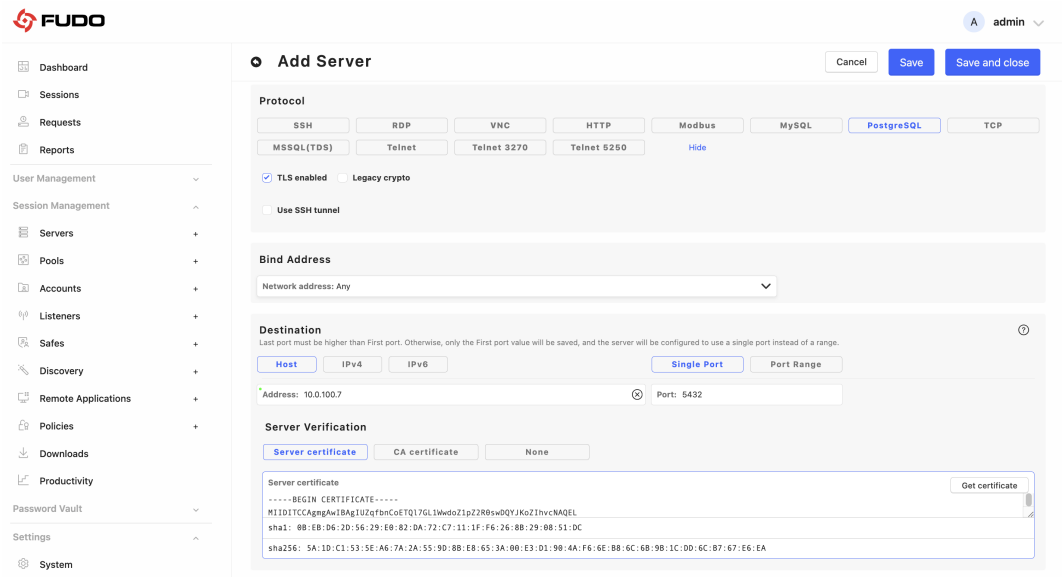
Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.

- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

8. In the *Server Verification* section, specify the server verification method:
   - Select `Server certificate` to verify the server based on its certificate,
   - Select `CA certificate` to verify the server certificate using a trusted certificate authority,
   - Select `None` to disable server certificate verification.

   If you select `CA certificate`, the *Verify hostname* option is also available and checked by default. It additionally checks that the server certificate covers the configured server address (host name or IP address); if it does not, the connection to the server fails. Clear the option to verify the certificate against the CA certificate only, for example when the certificate was issued for a name other than the configured address.



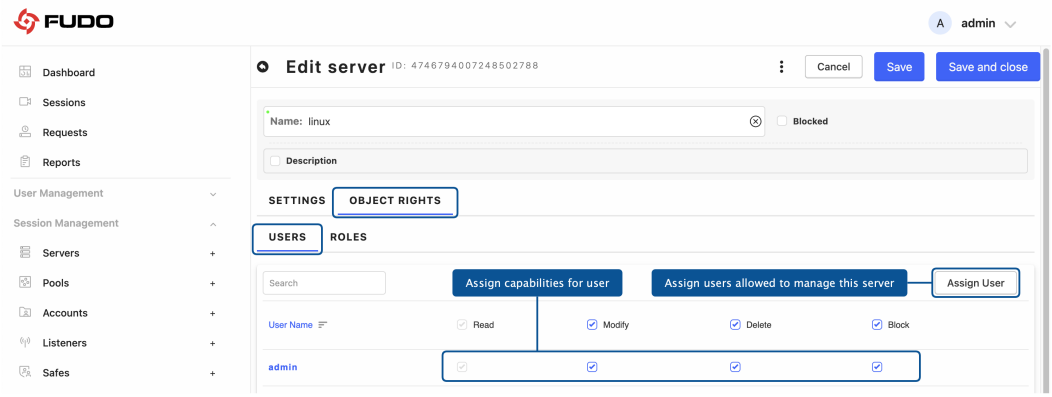
9. Click *Save* or *Save and close*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.

7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

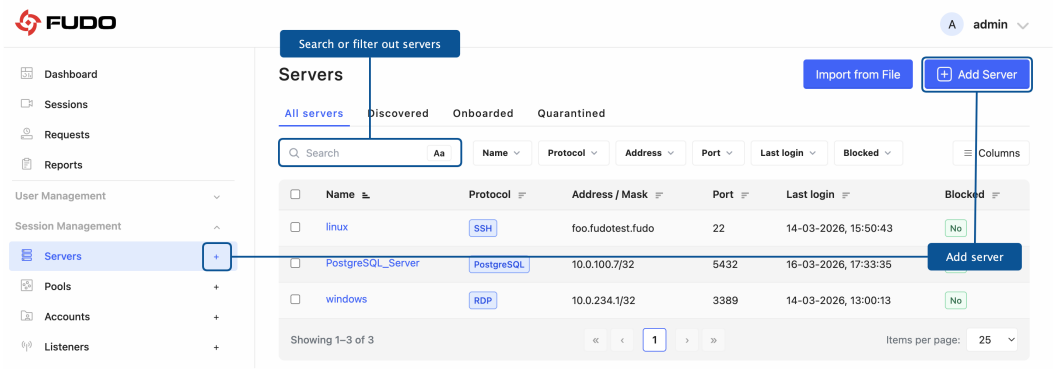
- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.7 Creating an RDP Server

Note

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- Fudo Enterprise allows authenticating against the RDP server with Kerberos. Kerberos authentication is enabled globally on the *Global* tab of the authentication settings. There you can also disable the fallback to the less secure NTLM protocol (*Disable NTLM fallback*). See *Kerberos Authentication Settings*.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, select `RDP`.

> **Warning**
>
> After server's definition is saved, protocol's field is uneditable.

3. Select the *TLS enabled* option to connect to monitored server over TLS.
4. Check the *NLA enabled* option for additional security.

> **Note**
>
> Security mode must match the security mode setting in the *RDP listener configuration*. The *NLA enabled* option within a server corresponds to the *Enhanced RDP Security (TLS)* option within the listener.
>
> Kerberos authentication against the RDP server requires the *NLA enabled* option. Kerberos authentication itself and disabling the NTLM fallback are configured globally — see *Kerberos Authentication Settings*.

5. Select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
6. Check the *Inform about existing connection* option to have the users informed that other users are connected to the server, they are trying to connect to.
7. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

8. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

9. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

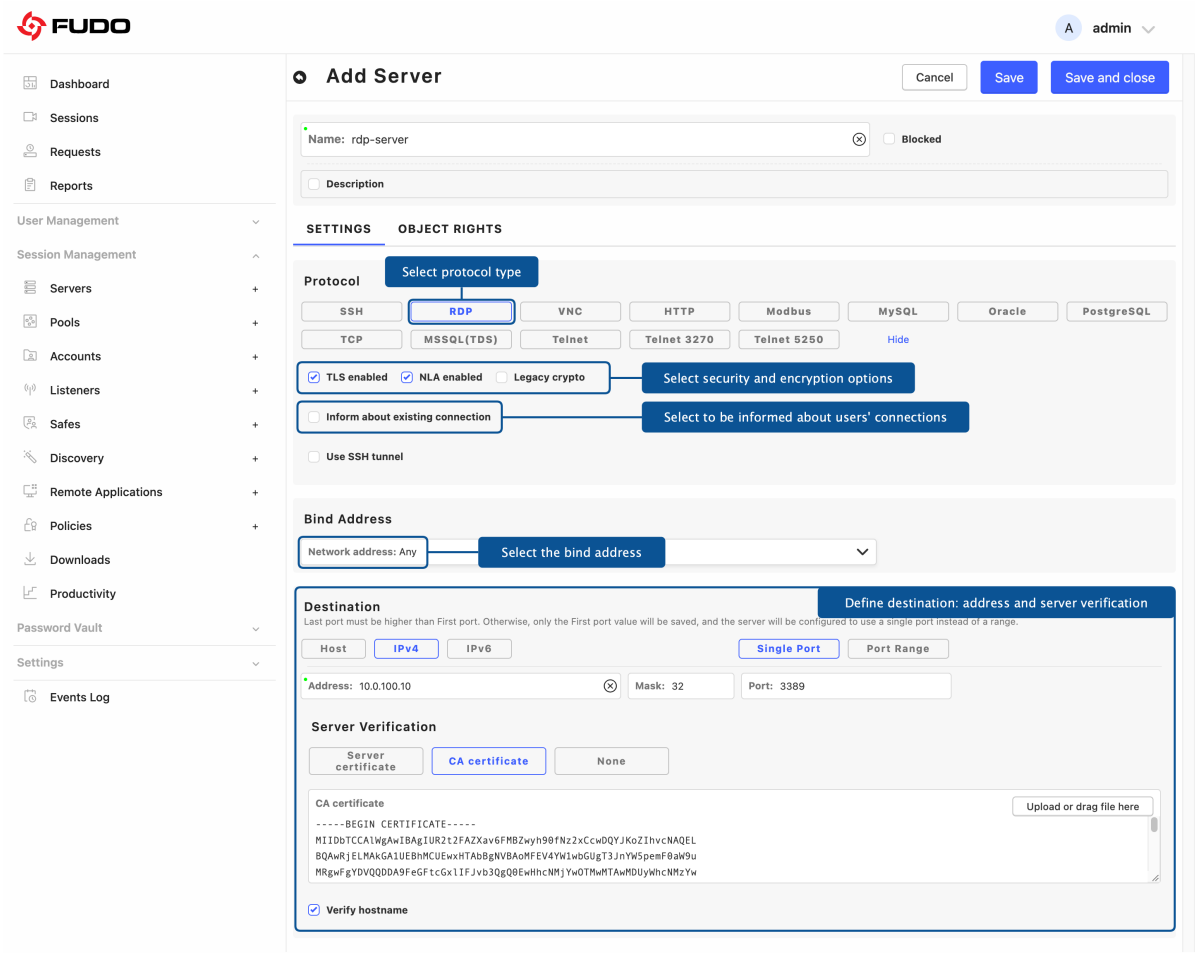
Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.
- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

- If the *TLS enabled* has been checked, in the *Server verification* section select one of the following options:`Server certificate` or `CA certificate` and provide respective certificate data. Select `None` to disable server verification. To learn more about the RDP server certificate management, please follow the *Managing RDP Server Certificates in Windows Server* section.

  If you select `CA certificate`, the *Verify hostname* option is also available and checked by default. It additionally checks that the server certificate covers the configured server address (host name or IP address); if it does not, the connection to the server fails. Clear the option to verify the certificate against the CA certificate only, for example when the certificate was issued for a name other than the configured address.

- Otherwise, provide *server key*.

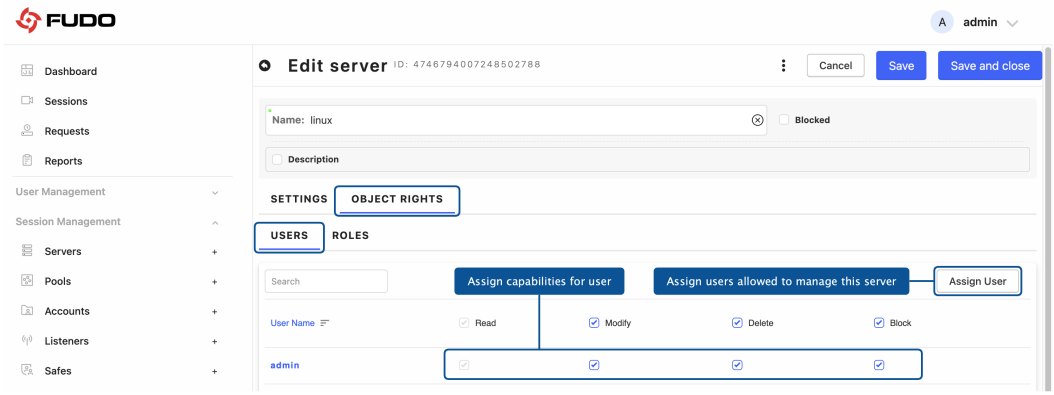


10. Click *Save*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

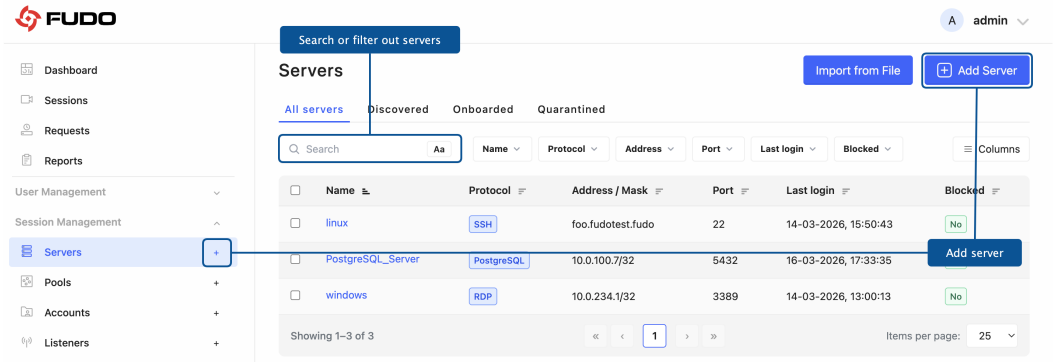
- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.8 Creating an SSH Server

Note

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.

5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, select `SSH`.

Warning

After server's definition is saved, protocol's field is uneditable.

3. Select *Legacy crypto* option to allow negotiating older encryption algorithms when establishing connections. For the list of these algorithms, see *SSH*.
4. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

5. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

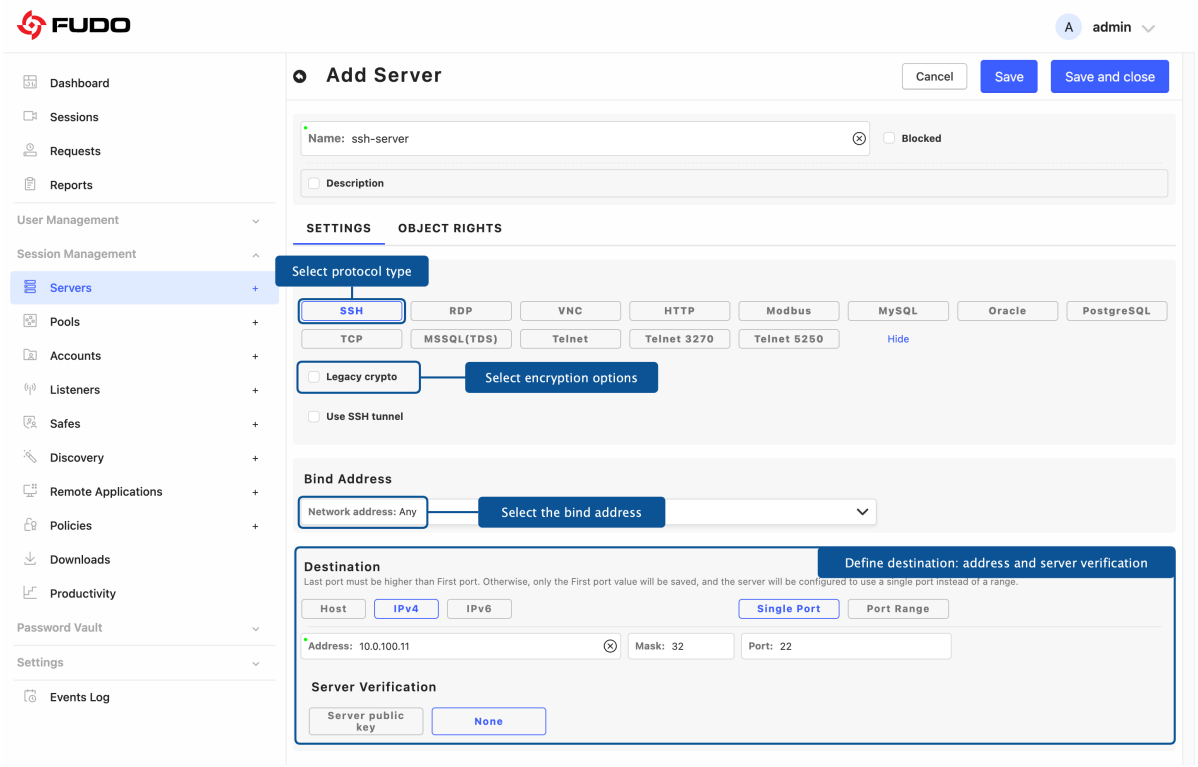
6. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.

- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

7. In the *Server verification* section select `Server public key` and provide respective certificate data. Select `None` to disable server verification.

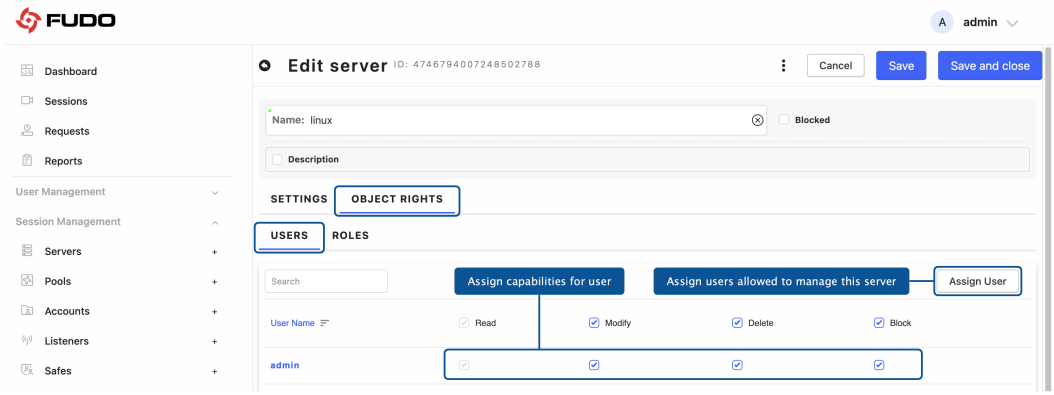


8. Click *Save*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

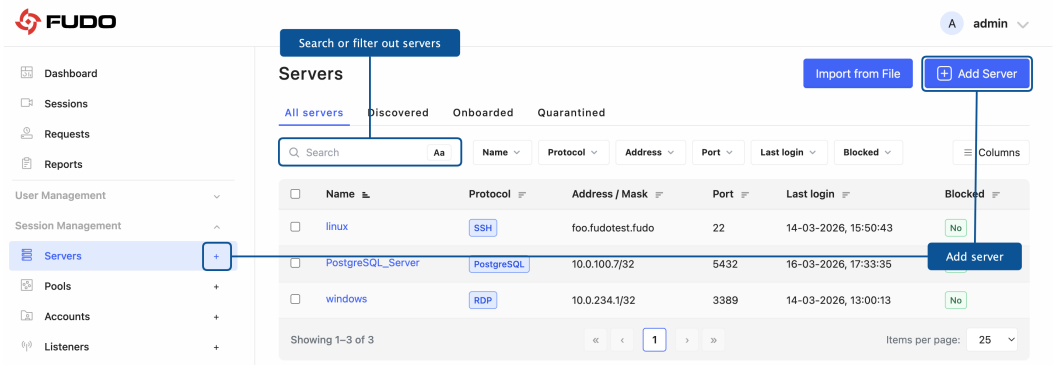
- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.9 Creating a Telnet Server

Note

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- In case of Telnet connections over *forward* and *regular* accounts, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise and then to connect to the target host.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.

4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, select `Telnet`.

Warning

After server's definition is saved, protocol's field is uneditable.

3. Select the *TLS enabled* option to connect to monitored server over TLS.
4. Select *Legacy cryptos* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
5. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

6. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

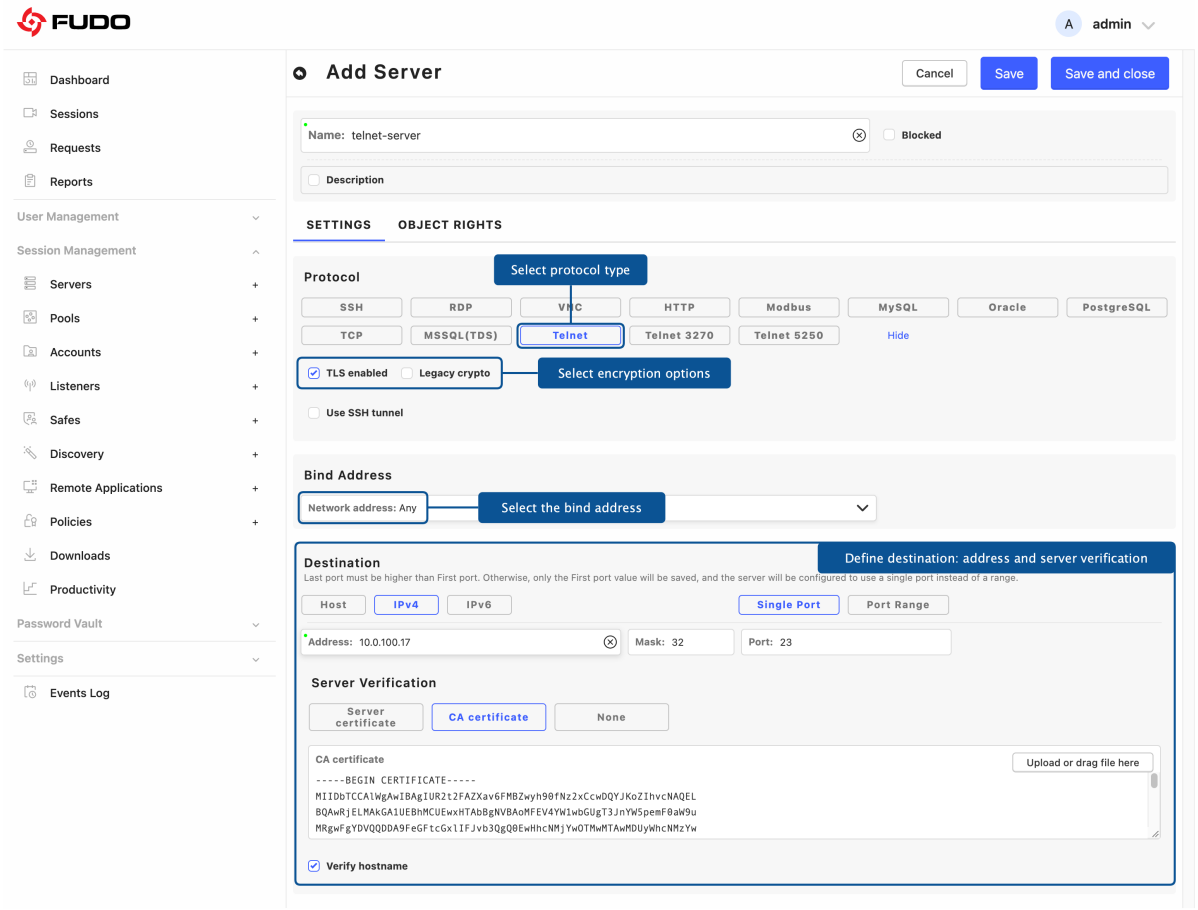
7. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.
- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

- If the *TLS enabled* was checked, in the *Server verification* section select one of the following options:`Server certificate` or `CA certificate` and provide respective certificate data. Select `None` to disable server verification.

  If you select `CA certificate`, the *Verify hostname* option is also available and checked by default. It additionally checks that the server certificate covers the configured server address (host name or IP address); if it does not, the connection to the server fails. Clear the option to verify the certificate against the CA certificate only, for example when the certificate was issued for a name other than the configured address.



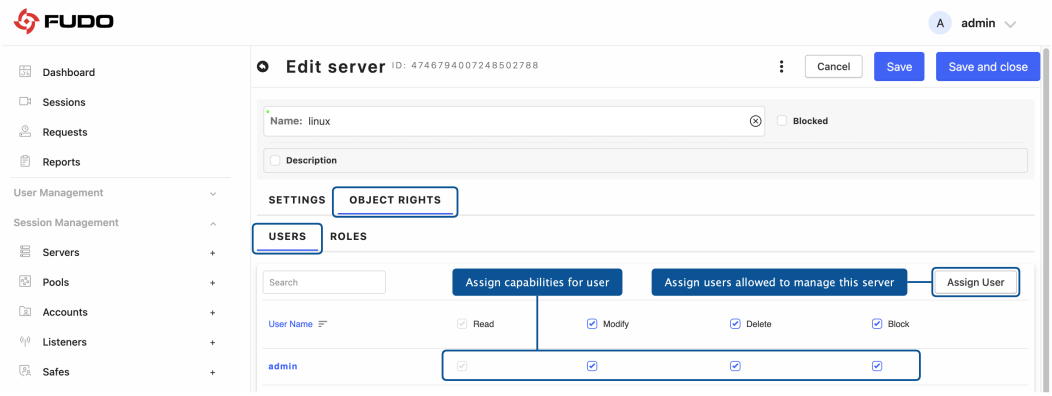
8. Click *Save*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the

object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.10 Creating a Telnet 3270 Server

Under review

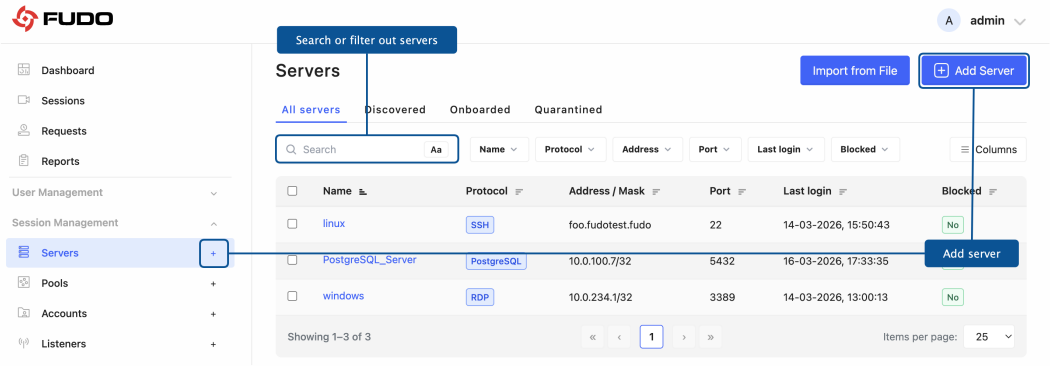
Support for the **Telnet 3270** protocol is **under review** and may be removed in a future release. If this protocol is critical to your environment, please contact Fudo Support for more information.

Note

- A server object can be linked to only one *anonymous* account.

- A server object can be linked to only one *forward* account.
- In case of Telnet connections over *forward* and *regular* accounts, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise and then to connect to the target host.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, select `Telnet 3270`.

Warning

After server's definition is saved, protocol's field is uneditable.

3. Select the *TLS enabled* option to connect to monitored server over TLS.
4. Select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
5. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.

- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

6. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

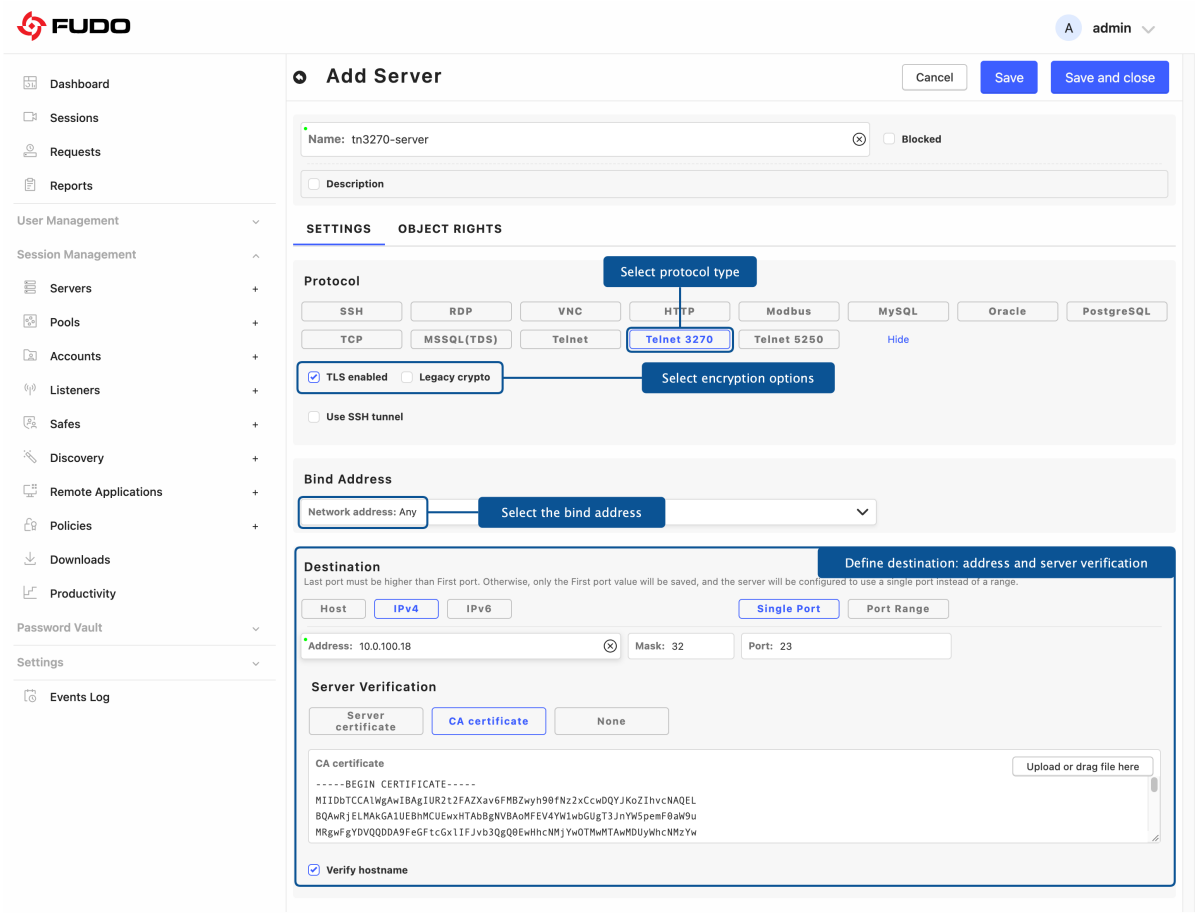
7. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.
- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

- If the *TLS enabled* was checked, in the *Server verification* section select one of the following options:`Server certificate` or `CA certificate` and provide respective certificate data. Select `None` to disable server verification.

  If you select `CA certificate`, the *Verify hostname* option is also available and checked by default. It additionally checks that the server certificate covers the configured server address (host name or IP address); if it does not, the connection to the server fails. Clear the option to verify the certificate against the CA certificate only, for example when the certificate was issued for a name other than the configured address.

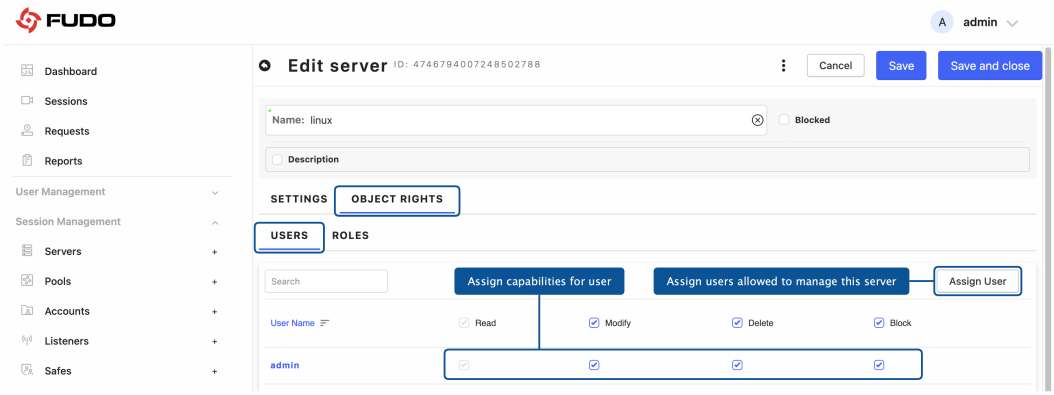


8. Click *Save*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

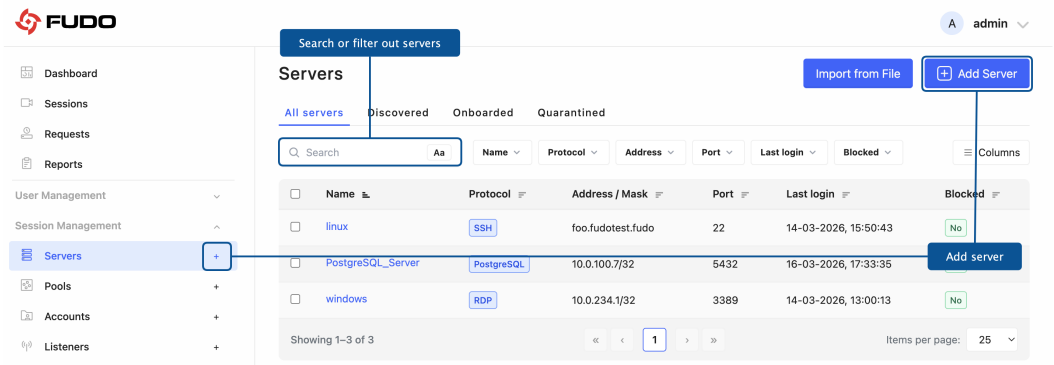
- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.11 Creating a Telnet 5250 Server

Note

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- In case of Telnet connections over *forward* and *regular* accounts, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise and then to connect to the target host.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.

4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, select `Telnet 5250`.

Warning

After server's definition is saved, protocol's field is uneditable.

3. Select the *TLS enabled* option to connect to monitored server over TLS.
4. Select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
5. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

6. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

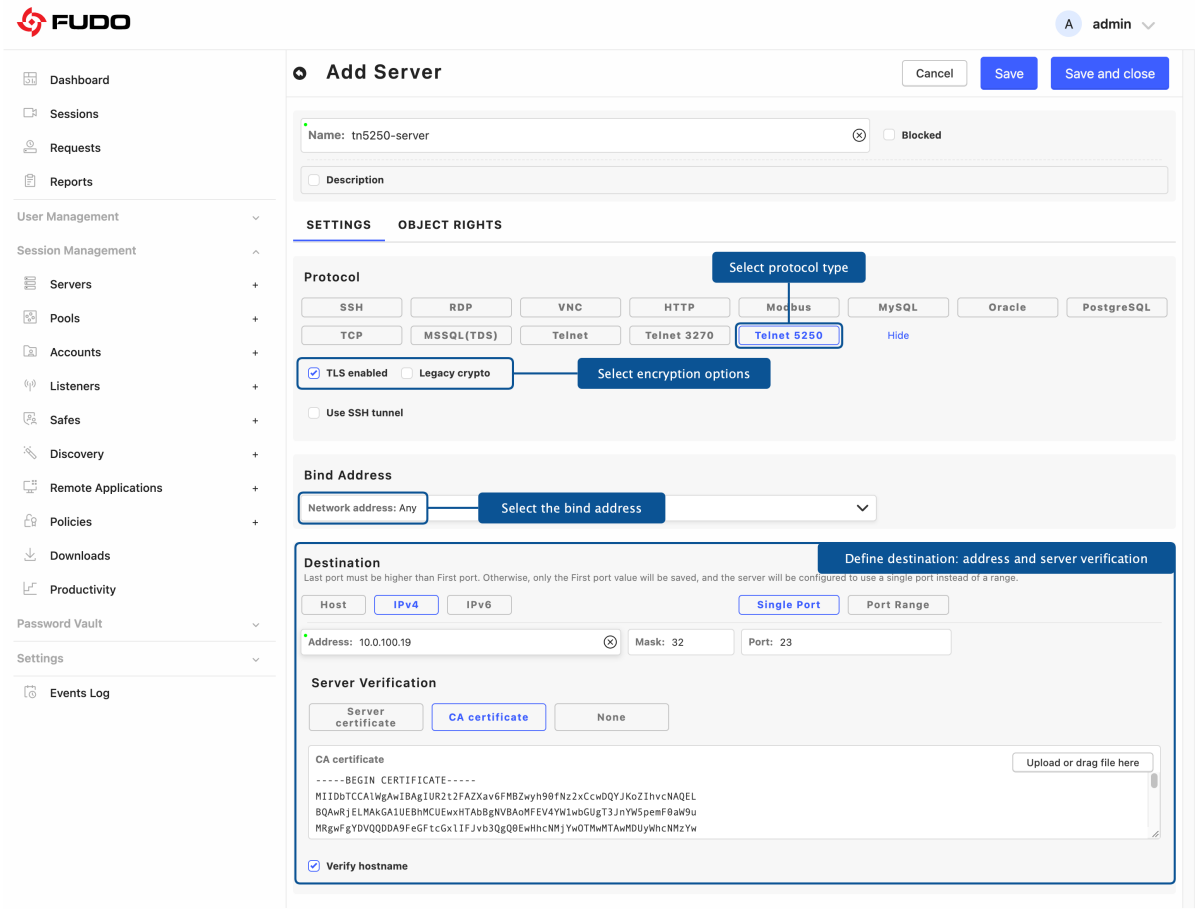
7. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.
- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

- If the *TLS enabled* was checked, in the *Server verification* section select one of the following options:`Server certificate` or `CA certificate` and provide respective certificate data. Select `None` to disable server verification.

  If you select `CA certificate`, the *Verify hostname* option is also available and checked by default. It additionally checks that the server certificate covers the configured server address (host name or IP address); if it does not, the connection to the server fails. Clear the option to verify the certificate against the CA certificate only, for example when the certificate was issued for a name other than the configured address.



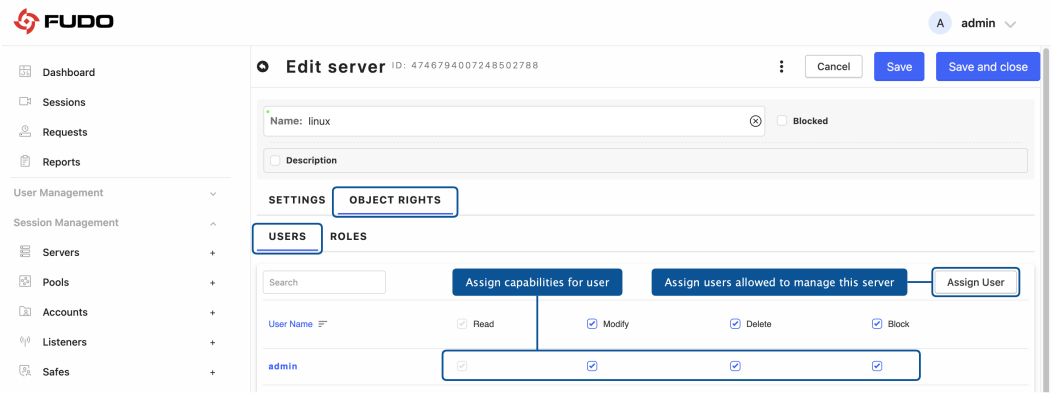
8. Click *Save*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the

object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

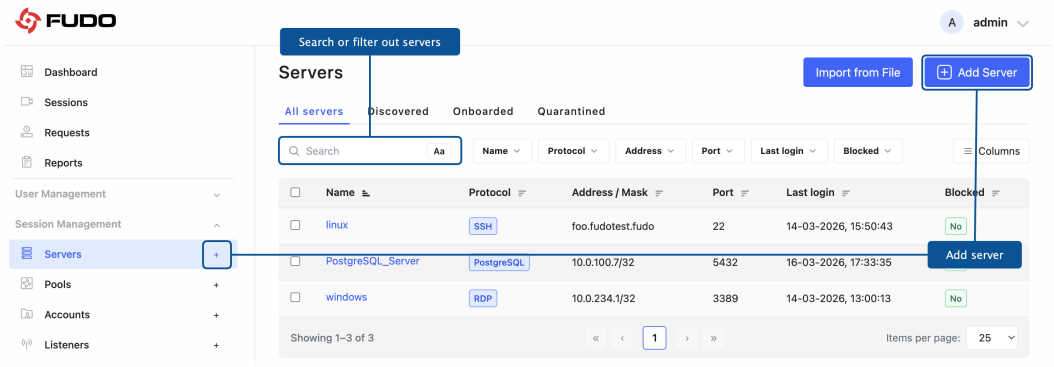
- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.12 Creating a VNC Server

Note

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.
2. In the *Protocol* section, select `VNC`.
3. Select the *TLS enabled* option to connect to monitored server over TLS.
4. Select *Legacy cryptos* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
5. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

6. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Warning

After server's definition is saved, protocol's field is uneditable.

Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

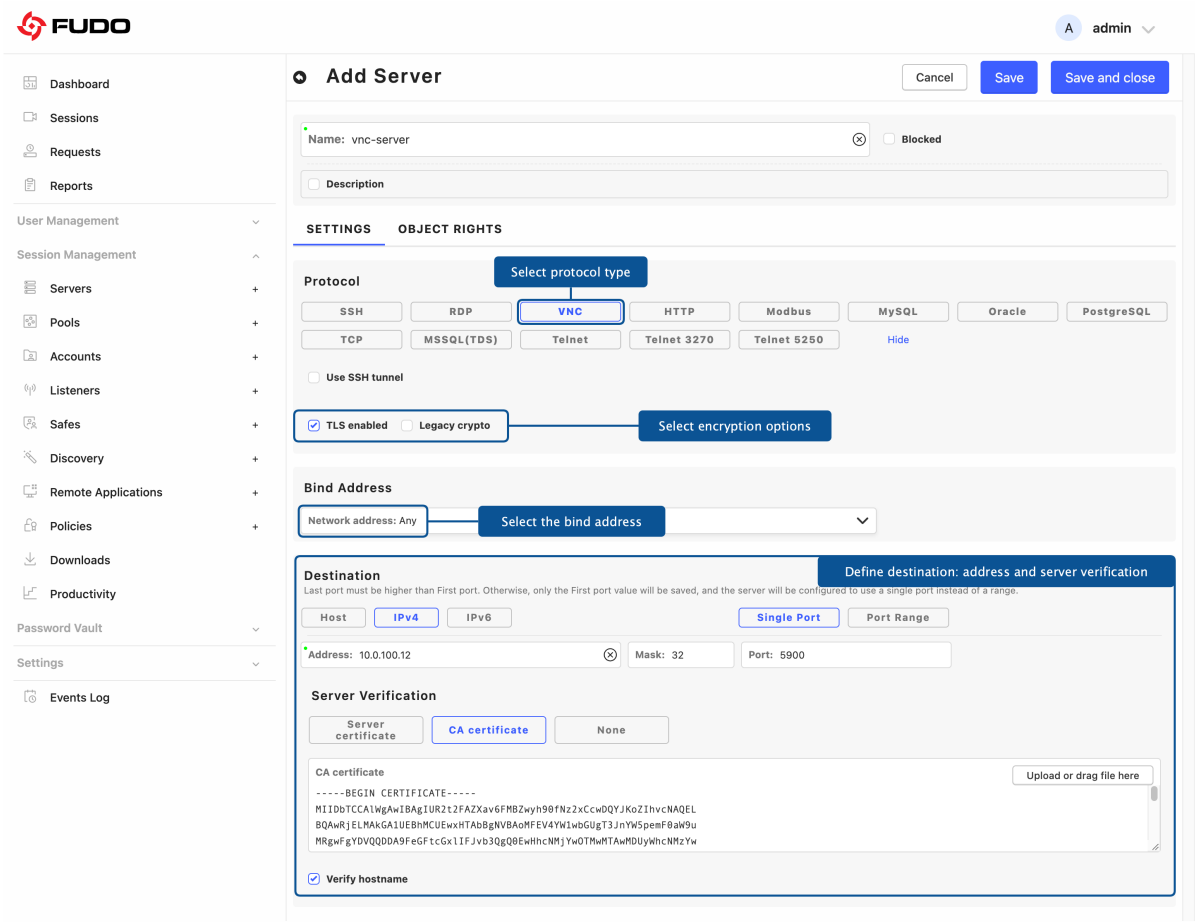
7. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.
- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

8. In the *Server Verification* section, specify the server verification method:
   - Select `Server certificate` to verify the server based on its certificate,
   - Select `CA certificate` to verify the server certificate using a trusted certificate authority,
   - Select `None` to disable server certificate verification.

   If you select `CA certificate`, the *Verify hostname* option is also available and checked by default. It additionally checks that the server certificate covers the configured server address (host name or IP address); if it does not, the connection to the server fails. Clear the option to verify the certificate against the CA certificate only, for example when the certificate was issued for a name other than the configured address.

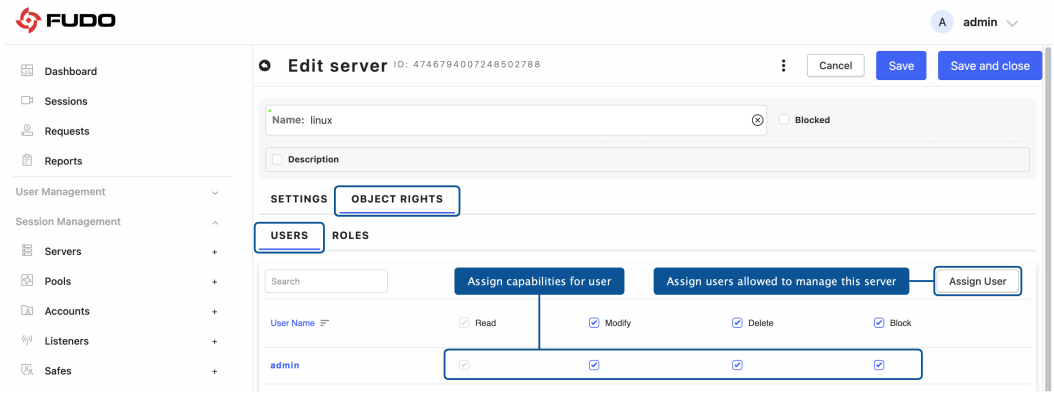


9. Click *Save*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.

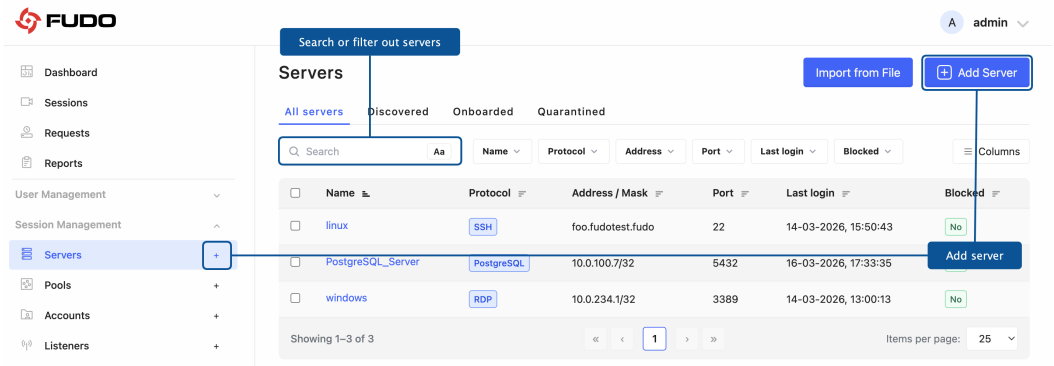


Related topics:

- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.1.13 Creating a TCP Server

1. Click + icon next to the *Servers* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Servers* and then click + *Add Add server*.



3. Enter server's unique name.
4. Select the *Blocked* option if the object should be unavailable after creation. A blocked server cannot be used to establish connections until it is manually unblocked. Providing a reason for blocking is required.
5. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

SETTINGS TAB

1. Go to the *SETTINGS* tab.

2. In the *Protocol* section, select `TCP`.
3. Select the *Use SSH tunnel* option and provide the *SSH tunnel key* to establish the connection through an SSH reverse tunnel.

Note

- In the *Tunnel* mode, the target host and port are exposed through a secure remote tunnel endpoint instead of being reached directly through the *Bind address* and *Destination* settings. See *Use SSH Tunnel - SSH Reverse Tunnel Server Configuration*.
- If you want to connect using a Tunnel-type listener to a server configured with the *Use SSH tunnel* option (SSH reverse tunnel), you must use the server name instead of a direct IP address and port. See *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

4. If you do not use the SSH tunnel, from the *Network address* drop-down list, select the IP address from which connections to the monitored server will be initiated, and then configure the *Destination* settings.

Warning

After server's definition is saved, protocol's field is uneditable.

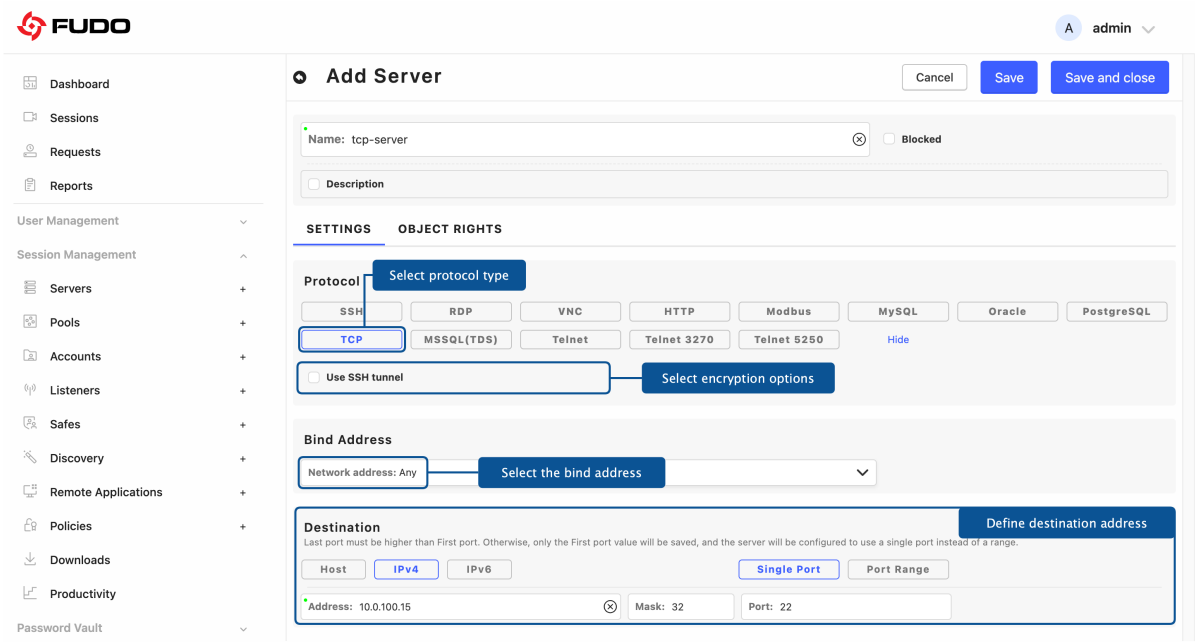
Note

- The *Network address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Network address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

5. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note

- Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.
- In the case of overlapping address definitions, during connection establishment the more specific configuration (higher network mask) is always selected, even if the user does not have permissions assigned to it. This mechanism enables defining exceptions within broader access rules (e.g., granting access to `/24` while explicitly excluding `/32`).

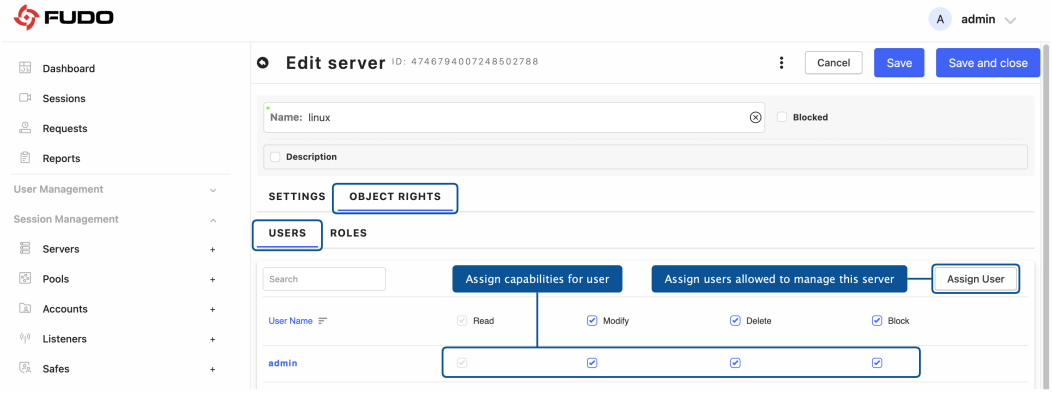


6. Click *Save*.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Related topics:

- *Pools*

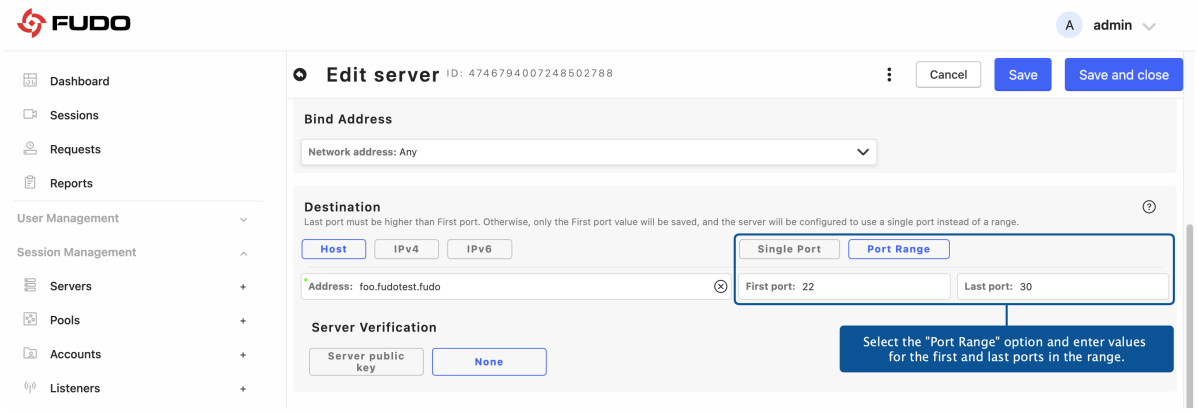
- *TCP*
- *Data Model*
- *Setting up the TCP Listener*

10.1.2 Port Ranges in Server Configuration

The **Port Range** functionality allows configuring a **Server** object in Fudo Enterprise with a specified port range. This eliminates the need to create separate servers for each port in scenarios requiring traffic forwarding from multiple ports simultaneously, significantly simplifying the configuration process and reducing manual work.

10.1.2.1 Configuring a Port Range

1. From the left menu, select *Management* > *Servers* and click + *Add Server*.
2. Enter a unique name for the created object (e.g., Server_1).
3. Go to the **Settings** section.
4. In the **Protocol** field, select the protocol for the server.
5. In the **Destination** section, define the parameters of the target server:
   - Select **Host, IPv4**, or **IPv6**.
   - Enter the **Address** of the server and optionally the **Mask**.
6. Click **Port Range** and enter values in the **First Port** and **Last Port** fields (e.g., First Port: 22, Last Port: 30).
7. Click **Save and Close**.



Note

- The maximum allowed value for both fields is **65535**. If a higher value is entered, it will be **automatically** set to the **maximum value**.
- The number in the *Last Port* field must be greater than the number in the *First Port* field. Entering a value in *Last Port* that is less than or equal to *First Port* will result in only the *First Port* value being saved, configuring the server to use a **single port** instead of a range.

- When the **Port Range** option is selected, the **automatic upload** of certificates or public keys is **disabled**, requiring manual input.

10.1.2.2 Server Configuration Prioritization in Case of Conflict

If a server with a port range is configured alongside another server with the same address but a single port within the range of the first server, e.g.:

```
Server_1 - 10.0.130.100:22-24
Server_2 - 10.0.130.100:23
```

then Fudo Enterprise will always prioritize the more specific configuration when establishing a connection through port `23`, in this case, `Server_2`.

Note

As a result, if a user with access to `Server_1` selects port `23` from the available range but does not have assigned access permissions to `Server_2` in Fudo Enterprise, they will not be able to establish such a connection.

Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.3 Use SSH Tunnel - SSH Reverse Tunnel Server Configuration

In some network environments, the Fudo Enterprise system may not have direct access to the target server due to:

- Firewall restrictions
- Network segmentation
- Server located in a private network

In such cases, you can use a **jump host** (intermediate server) that has access to both the Fudo Enterprise system and the target server.

Note

The jump host acts as an intermediary, establishing an SSH reverse tunnel between the Fudo Enterprise system and the target server.

Requirements

1. Jump host with access to Fudo Enterprise system and target server.
2. SSH client installed on the jump host.
3. Ability to execute SSH commands on the jump host.

Preparing SSH Keys on Jump Host

1. On the jump host, generate an SSH key pair (if it doesn't exist):

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

2. Copy the contents of the public key:

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

Creating a Server with SSH Tunnel Option

1. From the left menu, select *Session Management* > *Servers* and click + *Add server*
2. Enter a name (e.g., `Jump_Server_Target`).
3. In the *SETTINGS* tab, choose the appropriate protocol for the target server (e.g., SSH).
4. Check the *Use SSH tunnel* option.
5. In the *SSH tunnel key* field, paste the SSH public key from the jump host.
6. Click *Save*.

Getting the SSH Command

After saving the server configuration, the Fudo Enterprise system will generate an SSH command to execute on the jump host.

Example generated command:

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

where you need to replace:

- `<target>` - with the IP address of the target server
- `<port>` - with the port of the target server

Establishing the Tunnel

Execute the command generated by the Fudo Enterprise system on the jump host, substituting the actual values:

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

where:

- `192.168.1.100:22` - address and port of the target server
- `10.31.135.179` - address of the Fudo Enterprise system

Command parameters explanation:

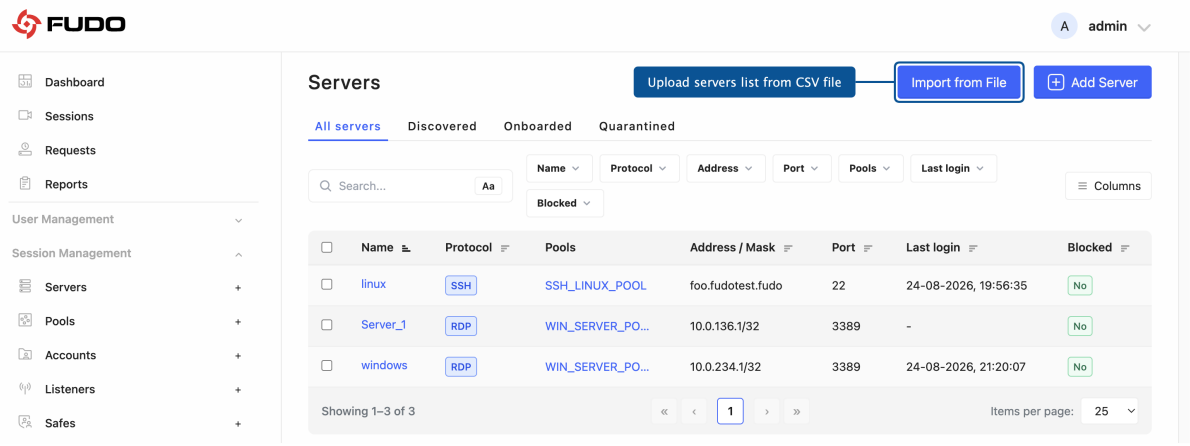
- `-l tunnel` - tunnel username
- `-p 65522` - Fudo Enterprise system port for tunnels
- `-o ExitOnForwardFailure=yes` - exit if port forwarding fails
- `-N` - do not execute remote commands
- `-f` - run in background
- `-R /tunnel/ID:target:port` - create reverse tunnel

Related topics:

- *Creating an SSH Server*
- *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*
- *Establishing an SSH Connection*

10.1.4 Importing a Server List from CSV File

1. Select *Management* > *Servers* and then click *Import from file*.



2. *Drag and drop* file into the modal window upload area or click *Browse for file* to upload it from local directory.
3. Displayed modal window presents a list of servers that will be added to Fudo Enterprise configuration.
4. Click *Send data* to upload all listed servers to Fudo Enterprise configuration or *Clear Data* to terminate uploading procedure.

Note

If any server specified in the CSV file have incorrect values, it will be skipped during the upload process. For example, a server with the same name as an existing server in the configuration will not be uploaded.

CSV file format

The CSV file must be constructed according to the following rules:

- The first row is a *header row* containing names corresponding to the API fields names (refer to *API Documentation:* API v2: Servers).
- The *header row* must include all fields that are required when manually creating a server for a specific protocol. Other fields are optional and can be left empty.
- A comma (,), semicolon (;), or pipe (|) can be used as a field separator.
- Text enclosed within double quotation marks (“”) is treated as a string, so field separators within it are ignored.

Example:

```
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
```

Note

For servers with a defined port range, the CSV file should include:

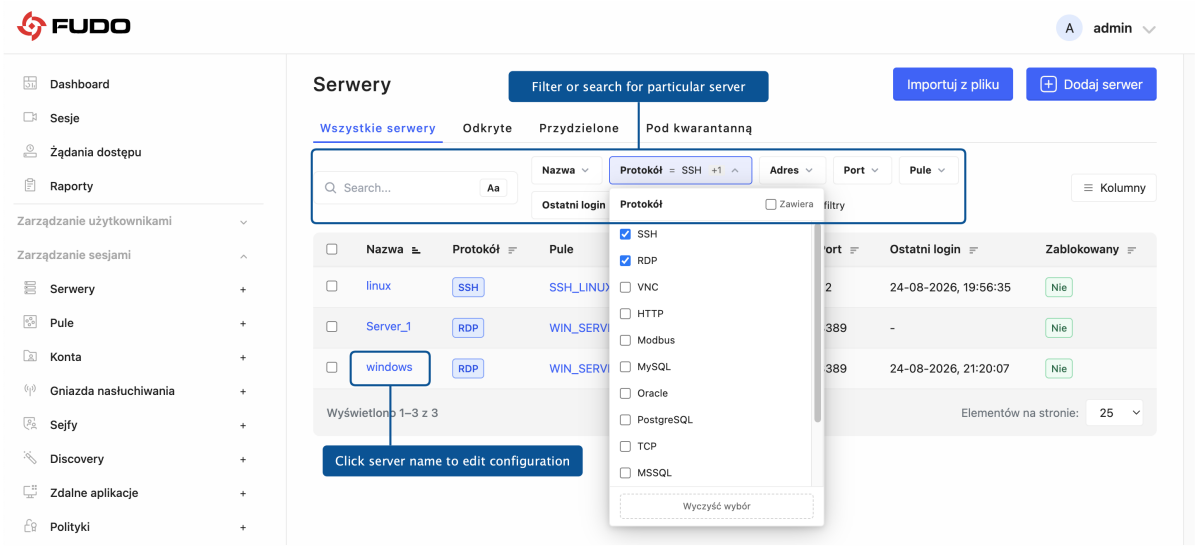
- the `port` column filled in for a server with a single port,
- the `port_first` and `port_last` columns filled in for a server with a port range.

Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.5 Editing a Server

1. Select *Management* > *Servers*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.
3. Find and click desired object’s name to open its configuration page.



4. Modify configuration parameters as needed.
5. Click *Save*.

Related topics:

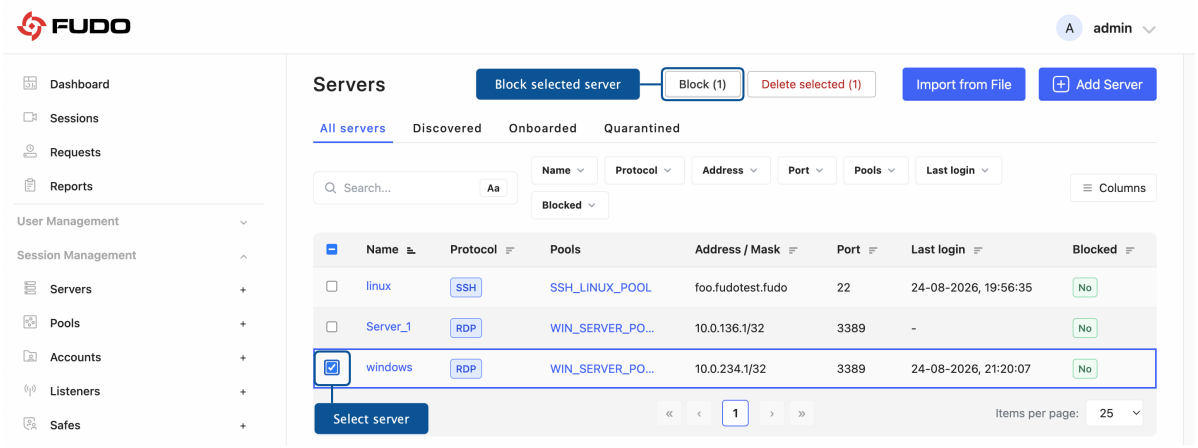
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.6 Blocking a Server

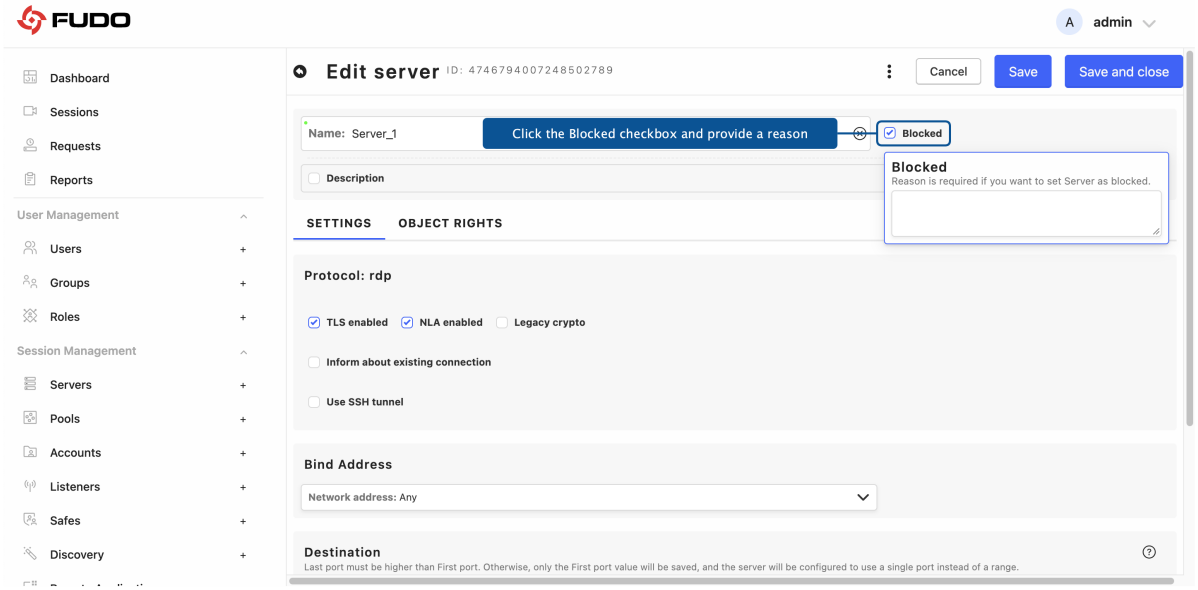
Fudo Enterprise allows blocking access to given server for all users.

> **Warning**
>
> Blocking a server will terminate current connections with the given server.

1. Select *Management* > *Servers*.
2. Define filters to limit the number of objects displayed on the list, or select a server that needs to be blocked right from the list.
3. Select the object and click the *Blocked* option.



4. Provide blocking reason and click *Block*.
5. You can also block the server from the editing form. Just edit the server, select *Blocked* option and provide the reason of blocking. Save changes.



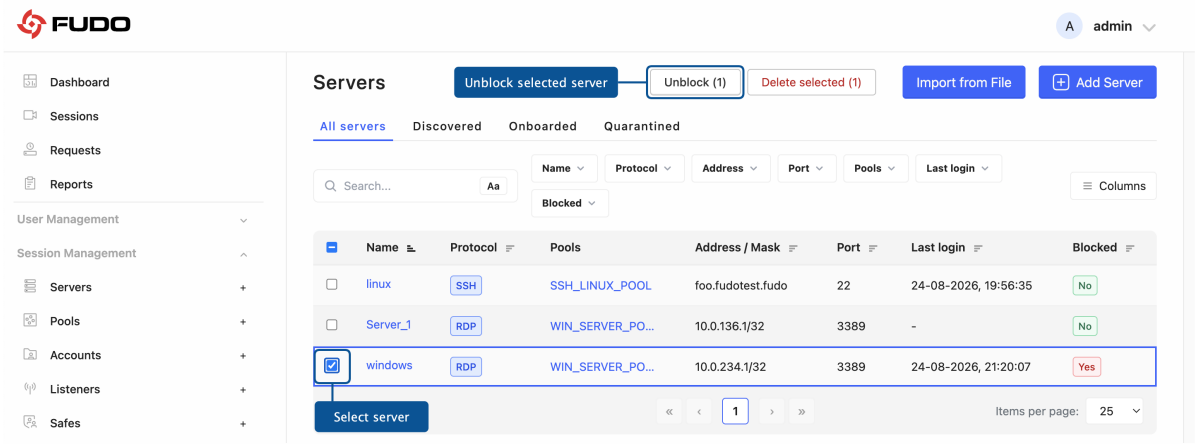
Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

10.1.7 Unblocking a Server

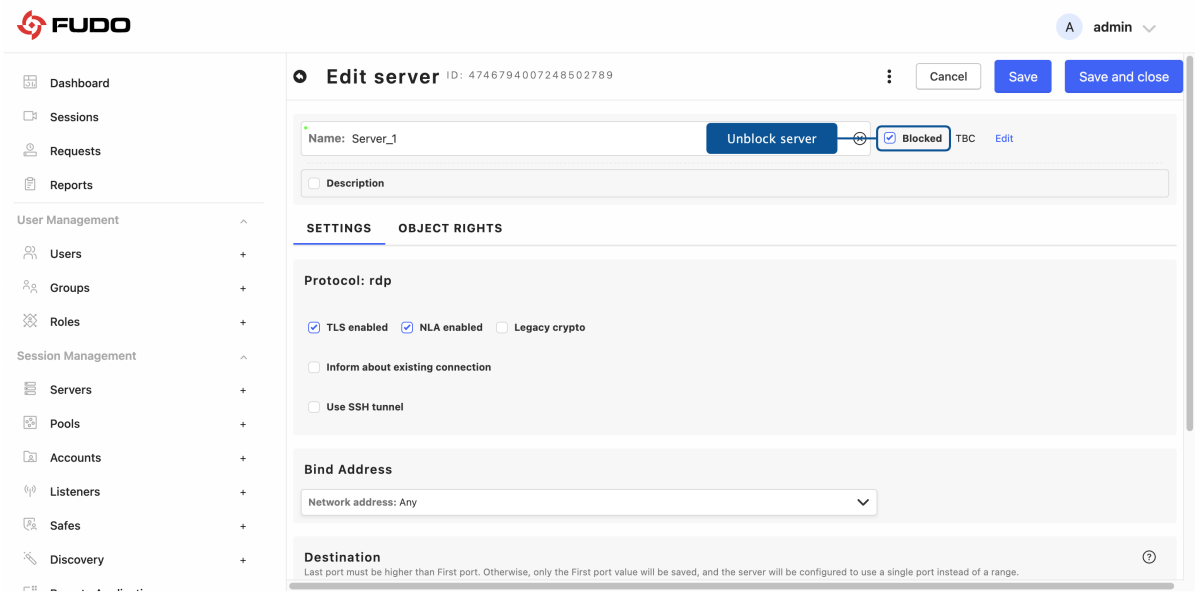
1. Select *Management* > *Servers*.
2. Define filters to limit the number of objects displayed on the list, or select a server that needs to be unblocked right from the list.

3. Select the server and click the *Unblock* button.



4. Click *Unblock* to confirm.

5. You can also unblock the server from the editing form. Just edit the server and deselect *Blocked* option. Save changes.



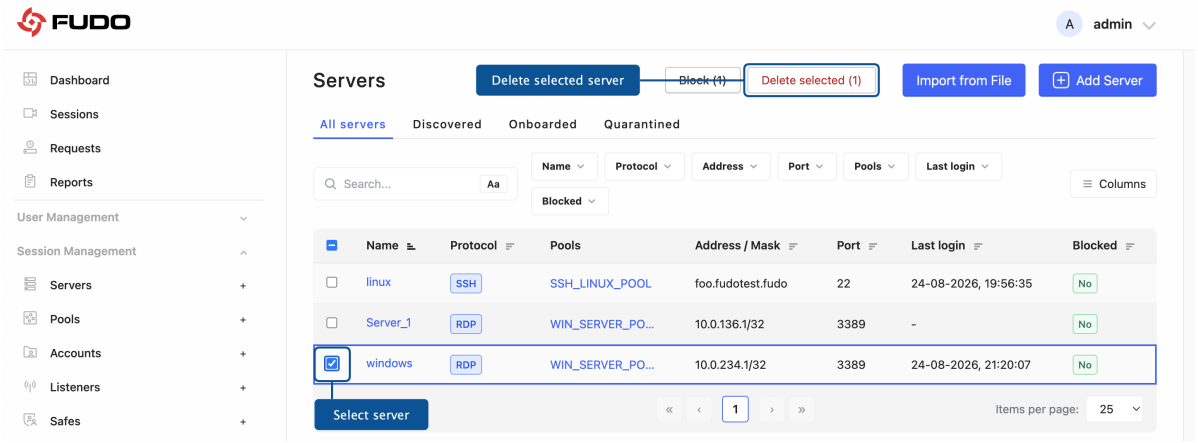
Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

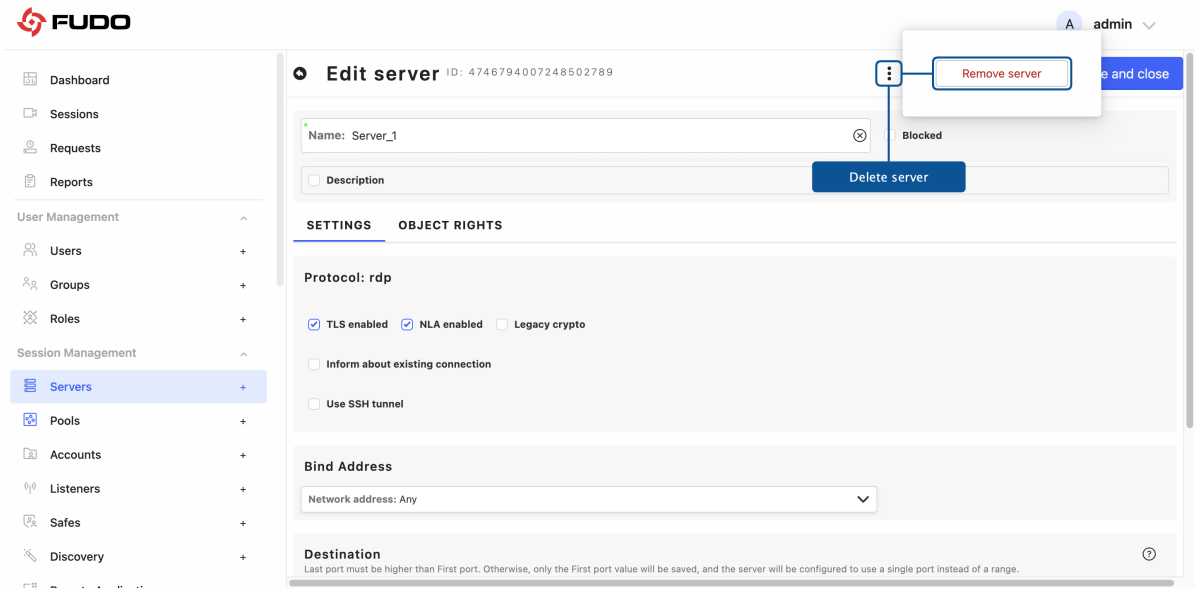
10.1.8 Deleting a Server

> **Warning**
>
> A server can't be deleted if assigned to an account.

1. Select *Management* > *Servers*.
2. Define filters to limit the number of objects displayed on the list.
3. Use checkboxes next to the servers to select them and click *Delete selected*.



4. Alternatively, you can edit a server that needs to be deleted right from the list, click the vertical three-dot icon and click *Remove server*.



5. Confirm server(s) deleting.

Related topics:

- *Data model*
- *System initiation*
- *Users*

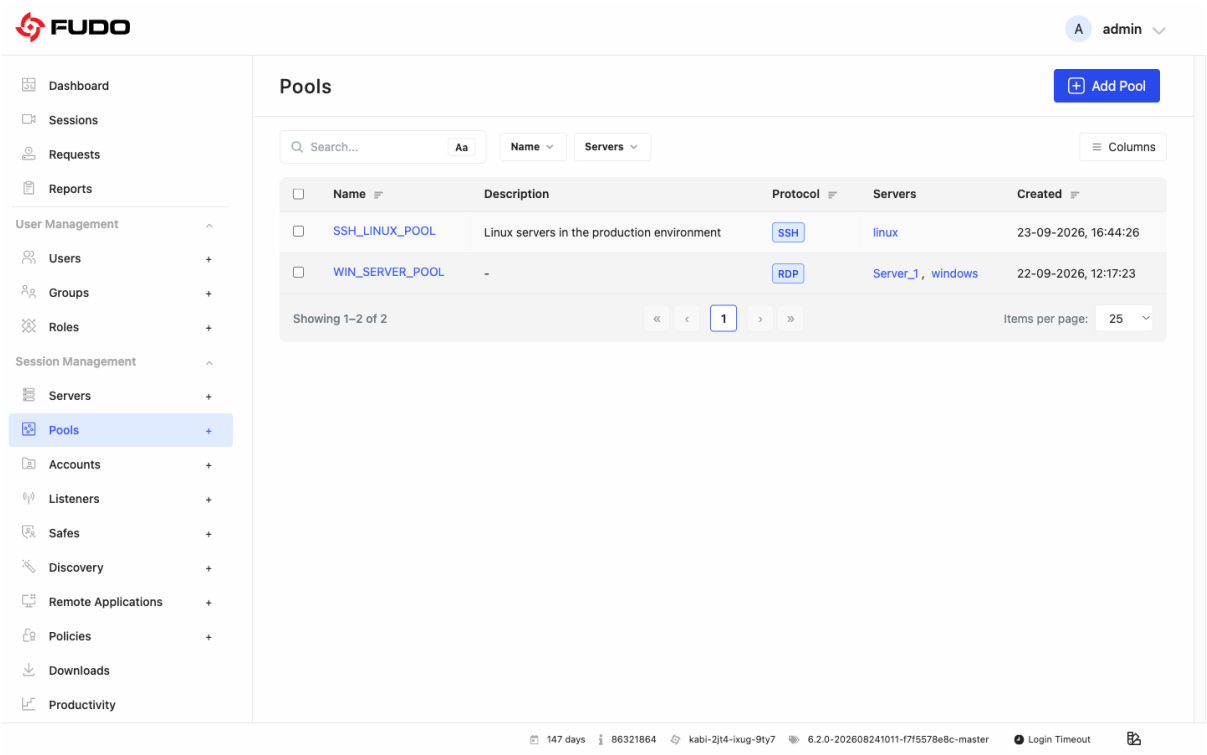
- *Listeners*
- *Safes*
- *Accounts*

10.2 Pools

A pool groups server objects that use the same protocol, so that other objects can refer to all of them at once. For example, an account assigned to a pool instead of a single server gives access to every server in that pool.

> **Note**
>
> - All servers in a pool must use the same protocol. The protocol of the first server you add becomes the protocol of the pool.
> - A pool can't be deleted while an account or a Discovery scanner uses it.

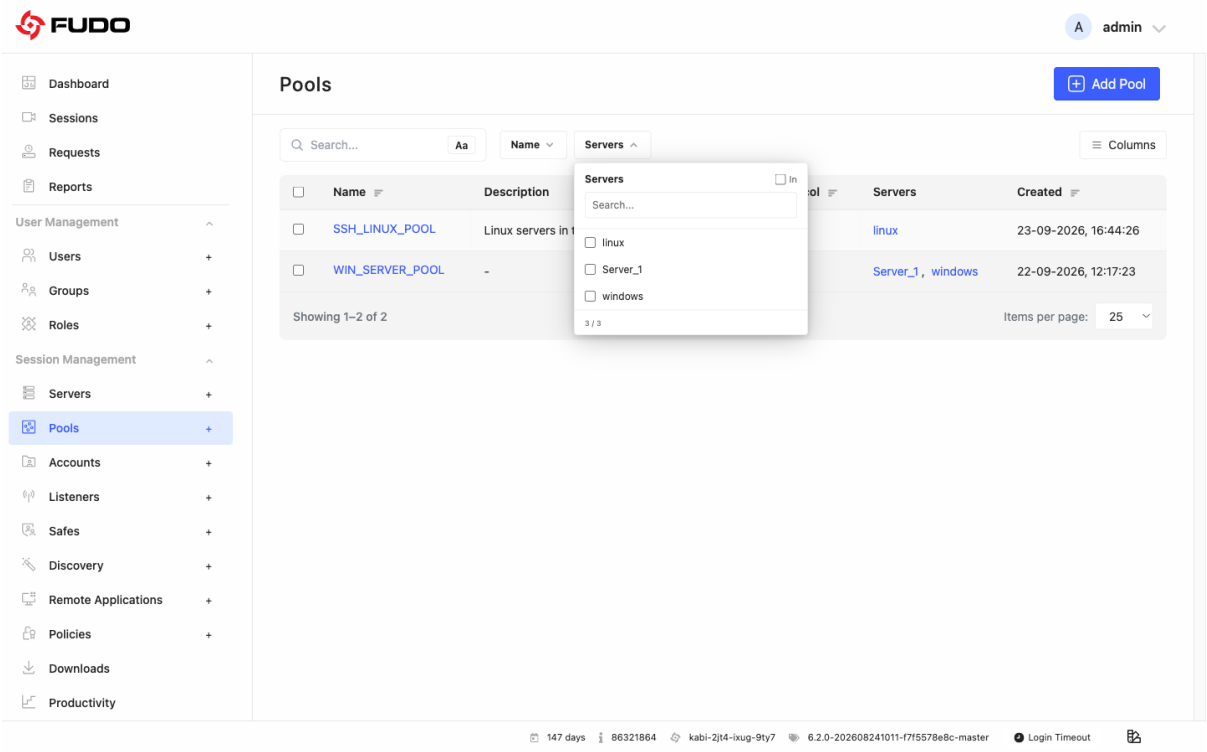
To open the list of pools, select Session Management > Pools.



The list shows the name, description, protocol, servers and creation date of each pool:

- The *Servers* column shows up to three servers. Click a server name to open that server. If a pool has more servers, click the *+N servers* link to see all of them in the *Servers in pool* window.
- Use the search field to find pools by name or description. Click *Aa* to make the search case-sensitive.
- Use the *Name* filter to find pools by name, and the *Servers* filter to find pools that contain (*In*) or don't contain (*Not in*) the selected servers.

- Click *Columns* to show or hide columns, for example *ID*.



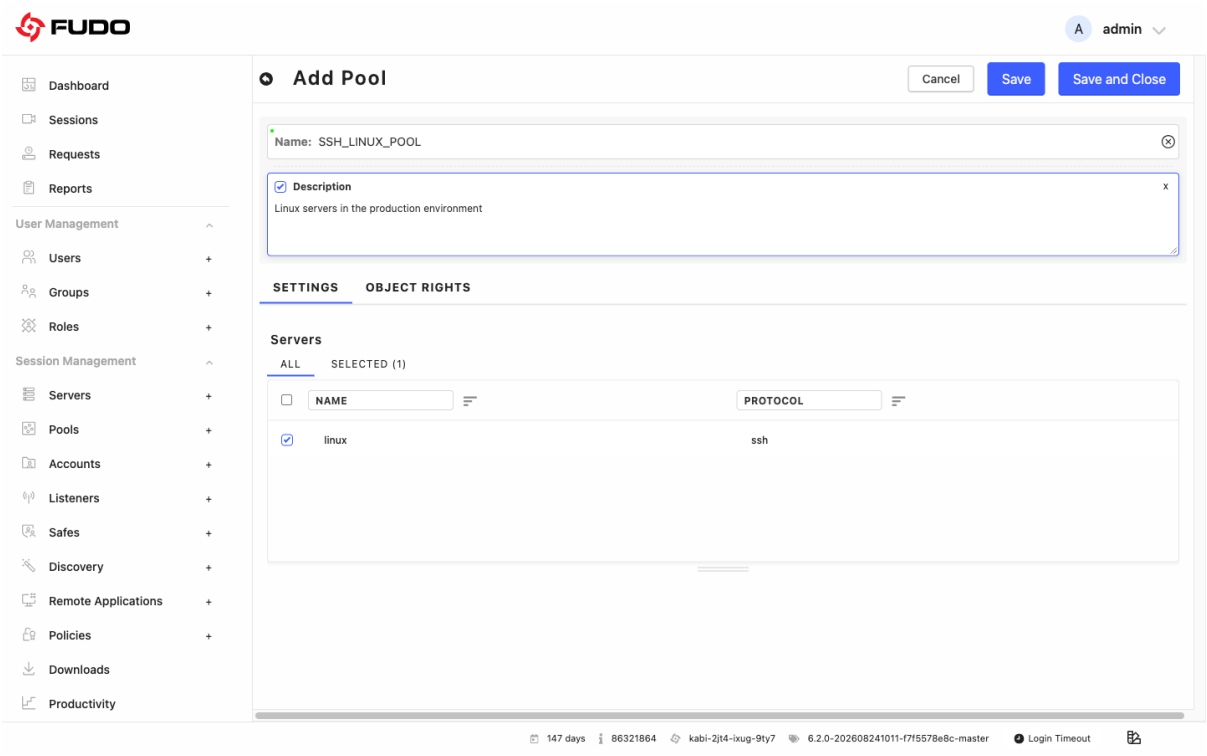
10.2.1 Creating a Pool

To create a pool, follow these steps:

1. Click + next to *Pools* in the left menu, or select *Session Management* > *Pools* and click *Add Pool*.
2. Enter a unique *Name* for the pool.
3. Optionally, select *Description* and enter text that will help you identify the pool.
4. In the *SETTINGS* tab, select the servers you want to add to the pool.

> **Note**
>
> After you select the first server, the list shows only servers that use the same protocol. To see servers of other protocols again, clear all selected servers. Open the *SELECTED* tab to see only the servers you selected.

5. Click *Save* to stay in the form, or *Save and Close* to return to the list.

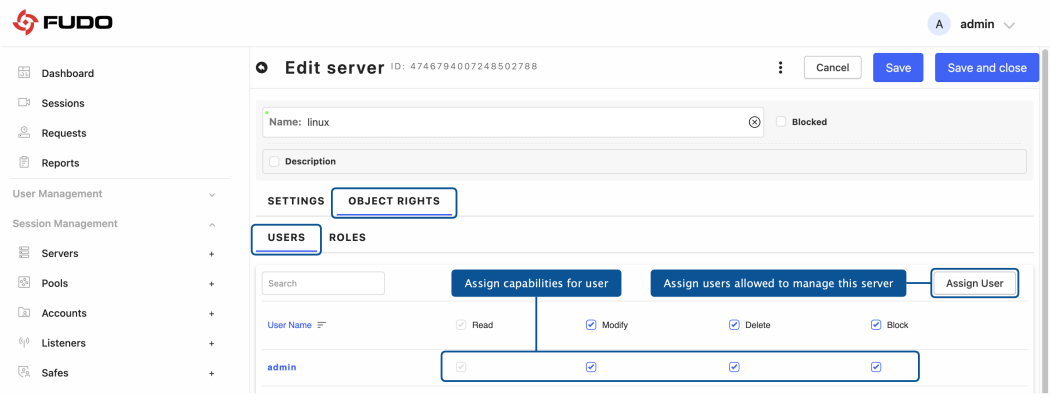


To change a pool later, click its name in the list, change the settings and save.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



10.2.2 Deleting a Pool

Warning

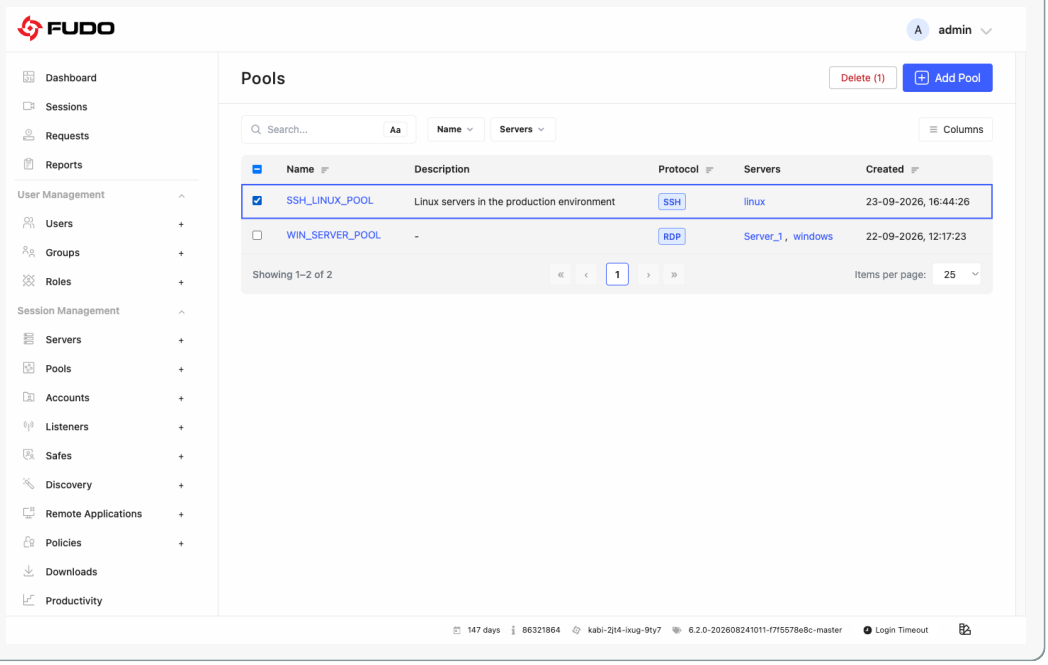
A pool can't be deleted while an account or a Discovery scanner uses it. Assign them to another server or pool first.

To delete pools from the list, follow these steps:

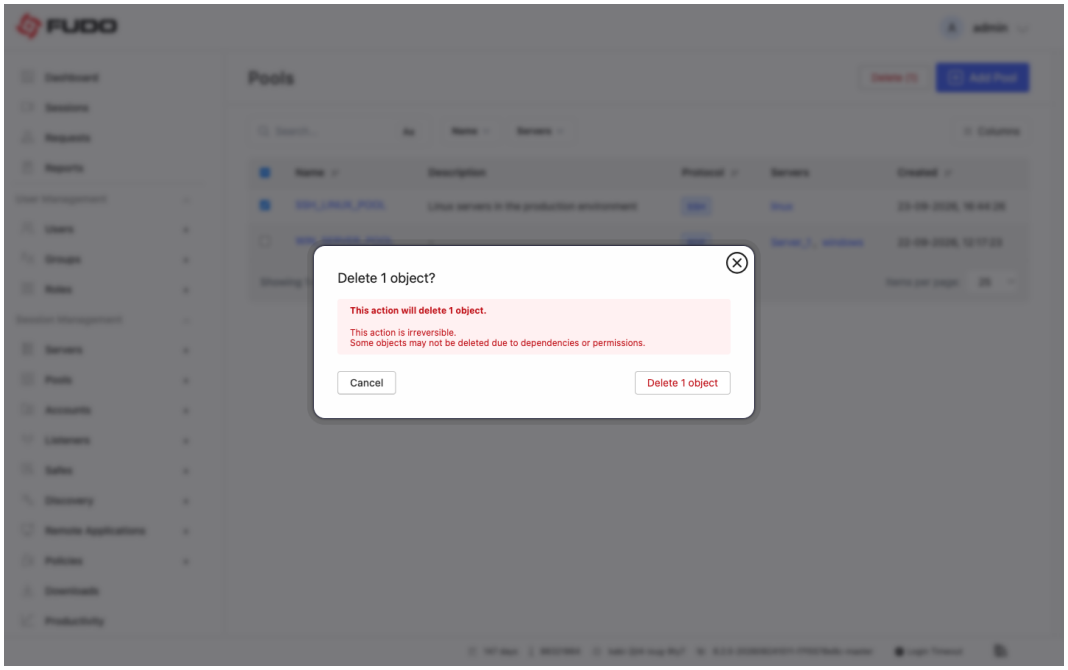
1. Select *Session Management* > *Pools*.
2. Optionally, use the search field and filters to narrow down the list.
3. Select the checkboxes next to the pools and click *Delete (N)*, where *N* is the number of selected pools.

Note

If the list has more than one page, click the arrow next to the checkbox in the table header to select the pools on all pages.



4. Click *Delete N object(s)* to confirm.

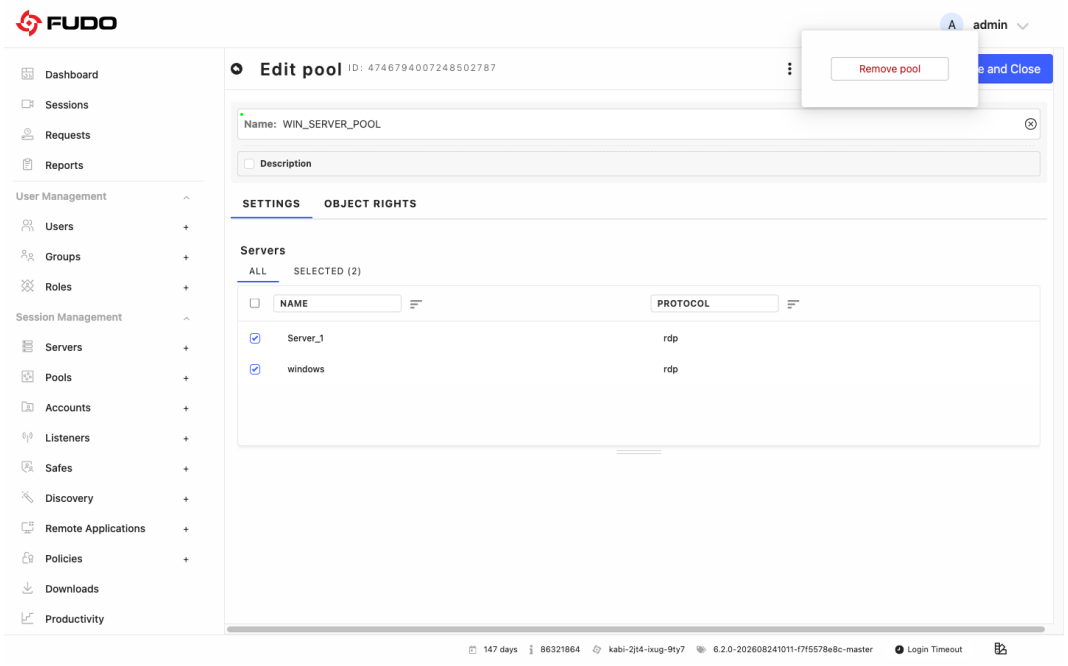


Note

Pools that are still in use, or that you don't have the *Delete* right for, are not deleted.

To delete a single pool from its form, follow these steps:

1. Click the name of the pool in the list.
2. Click the vertical three-dot icon next to *Cancel* and click *Remove pool*.
3. Click *Confirm*.



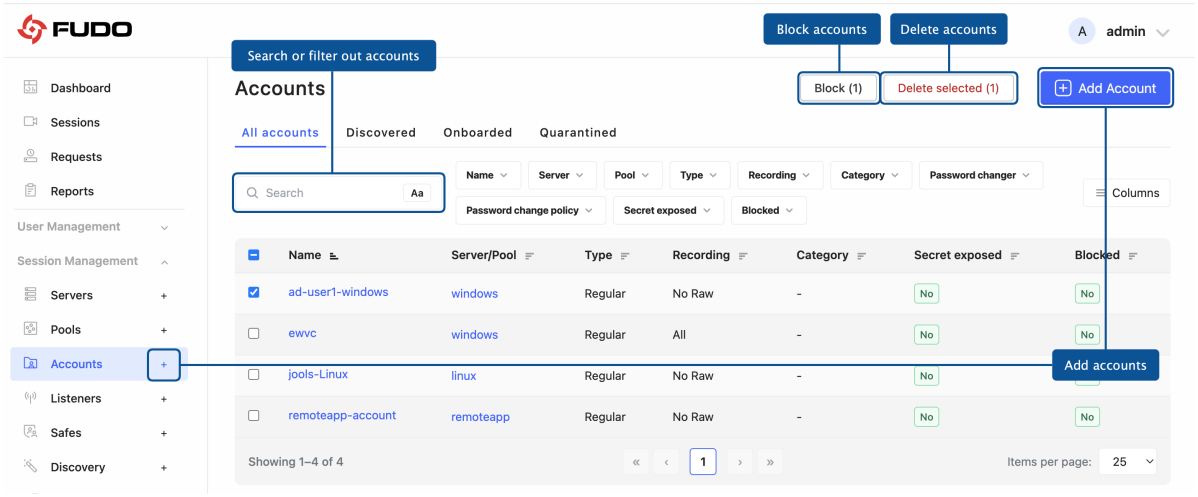
Related topics:

- *Data model*
- *Creating a Server*
- *Accounts*
- *Safes*
- *Listeners*
- *Users*

10.3 Accounts

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

> **Note**
>
> In case of Telnet connections, user has to go through authentication process twice. First time to authenticate against Fudo Enterprise and then to connect to the target host.



10.3.1 Creating an Account

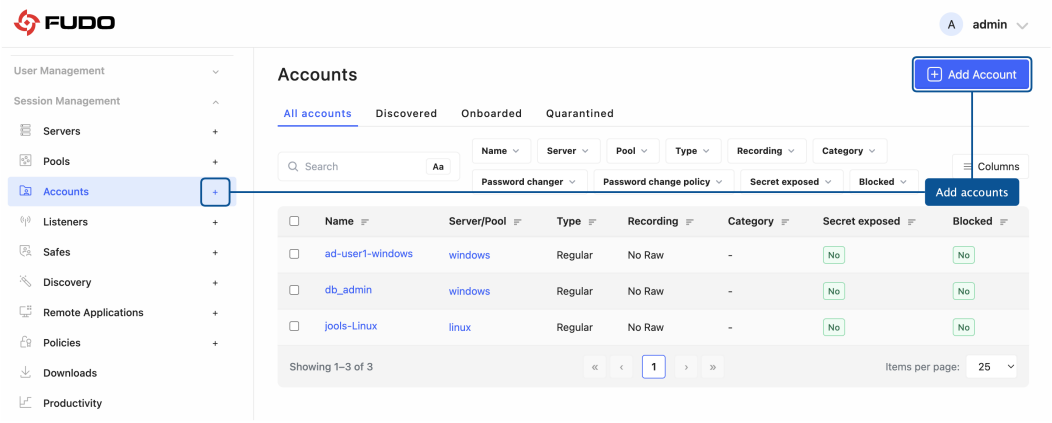
> **Warning**
>
> Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances **must not** be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

10.3.1.1 Creating an *Anonymous* Account

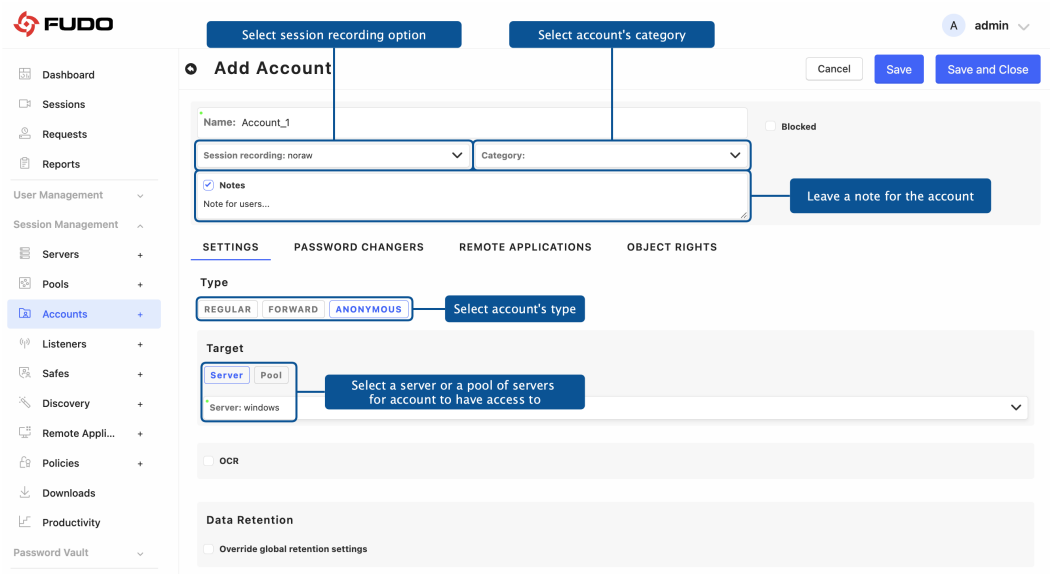
> **Warning**
>
> If an *anonymous* account is used in a session established through an *SSH tunnel*, the name of the user who created the tunnel is displayed in the Sessions list.

To create an account definition, follow the instructions below.

1. Click + icon next to the *Accounts* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Accounts* and then click + *Add account*.



3. Define object's name.
4. Select *Blocked* option to disable account after it's created (if needed).



5. Select desired session recording option.

    - `all` - Fudo Enterprise saves session metadata (basic session information), records raw network traffic (RAW file) and stores session data in internal file format (FBS). The latter enables session playback using the built-in session player, as well as exporting sessions to a selection of video file formats.

- `raw` - Fudo Enterprise saves session metadata (basic session information) and records raw network traffic (RAW file). The raw data can be downloaded but it cannot be played back in graphical form using the built-in session player (session player only depicts the networks packet exchange between the client and the target host).
- `noraw` - Fudo Enterprise records the session data in a non-raw format that could be played back using the built-in session player.
- `none` - Fudo Enterprise saves only session metadata (basic session information).

Under review

RAW session recording of protocols that support the FBS format is **under review** and may be removed in a future release. For those protocols the choice would then be reduced to recording the session or not recording it at all, and the `all` and `raw` options would stop producing a RAW dump. Database protocols - Oracle, PostgreSQL, MySQL and MSSQL(TDS) - are recorded in RAW only and are **not** affected by this change.

6. From the *Category* drop-down list select `privileged` or `non-privileged` account category.

Note

During manual account creation, assigning the category as *privileged* or *non-privileged* is purely informational, yet during the *Discovery*, it is automatically assigned based on the account's parameters in the source system.

7. Select the *Notes* option to activate the field where you can enter a message for *User Access Gateway* users. If permissions are granted, notes can be also edited.

Note

Account notes can be displayed in the *User Access Gateway*.

SETTINGS TAB

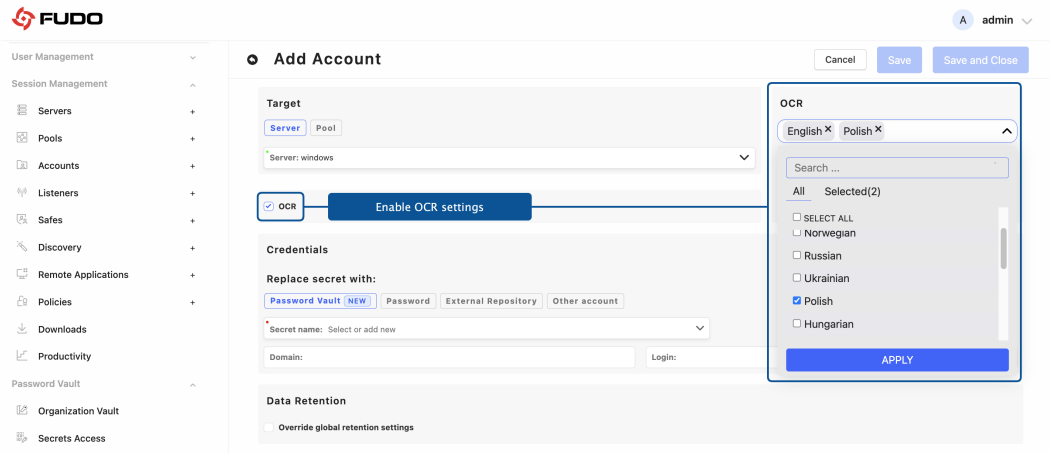
1. In the *SETTINGS* tab, in the Type field, press the *ANONYMOUS* button.
2. In the *Target* section, select *Server* or *Pool* button to assign account to a specific server

or a server pool by selecting it in the next step from the *Server*, or *Pool* drop-down list.

3. Select *SSH Agent forwarding* option to authenticate the user against the target host using client's SSH key.

> **Note**
>
> This option is available only after selecting an SSH server. Use -A option for connecting to SSH server.

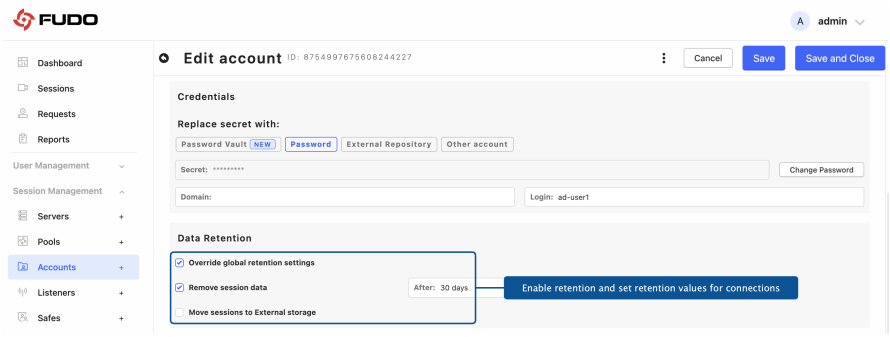
4. To have RDP, VNC or rendered HTTP sessions automatically processed, you can enable *OCR session* option for this account and select the language of processed data.



> **Note**
>
> The *OCR* option is available only after selecting an RDP, VNC or HTTP server.

5. In the *Data retention* section, define automatic data removal settings.

   - Select *Override global retention settings* option to set other than *global retention values* for connections established using this account.
   - Check the *Remove session data* option to exclude sessions from retention mechanism.
   - Next to the *Remove session data* field, define the number of days after which the session data will be moved to external storage device. Default value when the option is checked, is 30 days.



Note

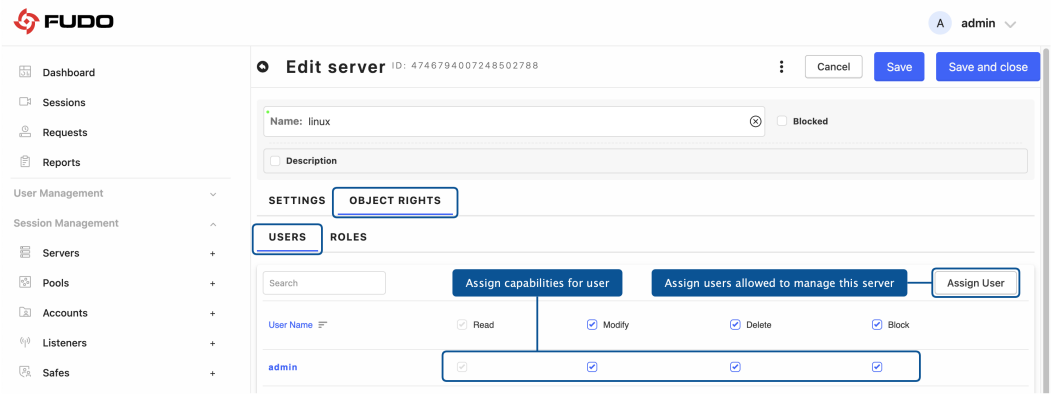
Data retention for sessions established using this account will only be active if global retention is enabled. To change global retention settings see chapter *Data Retention*.

6. Click *Save* to proceed with further configuration.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Note

The *Secret Changers* tab and the *Remote applications* tab are active only when creating regular or forward account types.

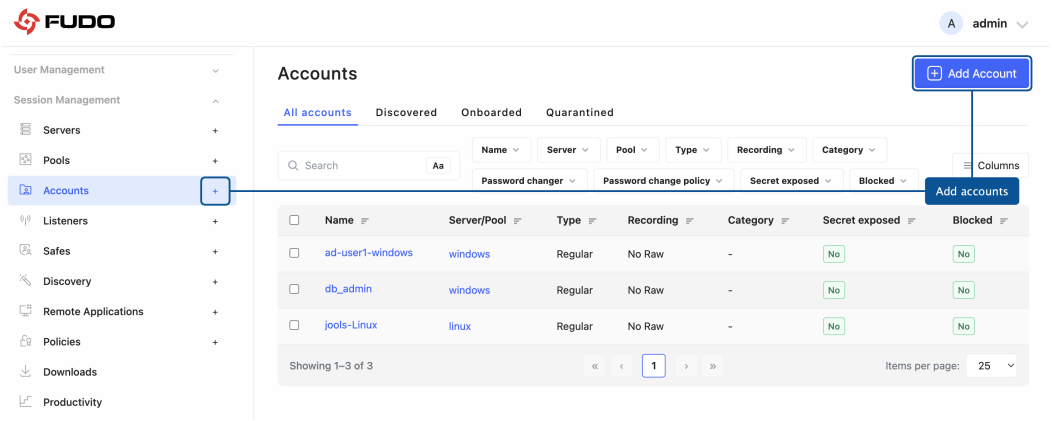
Related topics:

- *Data Model*
- *Deleting an Account*
- *Editing an Account*
- *Unblocking an Account*
- *Blocking an Account*

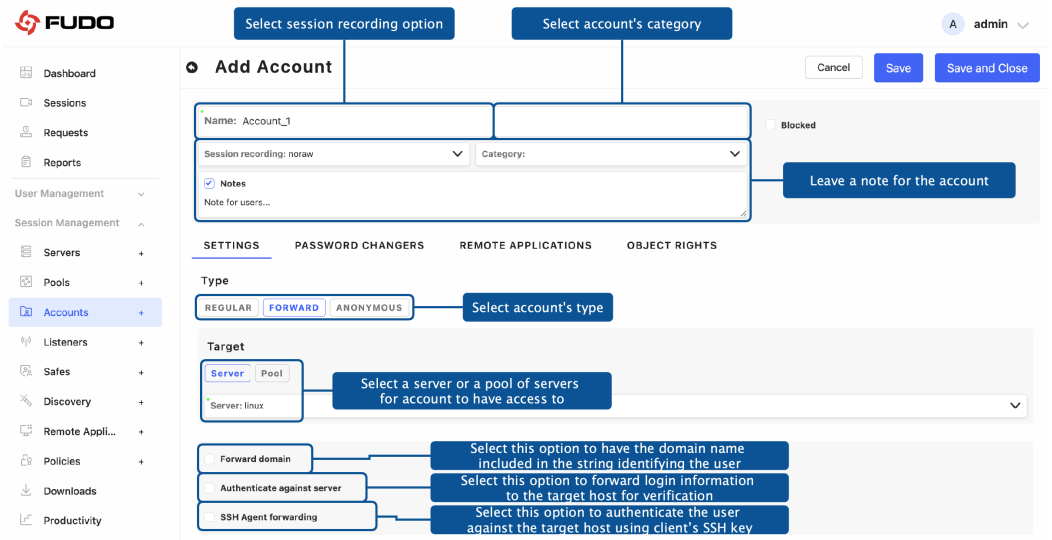
10.3.1.2 Creating a *Forward* Account

To create an account definition, follow the instructions below.

1. Click + icon next to the *Accounts* tab of the *Session Management* sub-section, or
2. Select *Session Management* > *Accounts* and then click + *Add account*.



3. Define object's name.
4. Select *Blocked* option to disable account after it's created (if needed).



5. Select desired session recording option.

    - `all` - Fudo Enterprise saves session metadata (basic session information), records raw network traffic (RAW file) and stores session data in internal file format (FBS). The latter enables session playback using the built-in session player, as well as exporting sessions to a selection of video file formats.
    - `raw` - Fudo Enterprise saves session metadata (basic session information) and records raw network traffic (RAW file). The raw data can be downloaded but it cannot be played back in graphical form using the built-in session player (session player only depicts the networks packet exchange between the client and the target host).
    - `noraw` - Fudo Enterprise records the session data in a non-raw format that could be played back using the built-in session player.

- `none` - Fudo Enterprise saves only session metadata (basic session information).

> **Under review**
>
> RAW session recording of protocols that support the FBS format is **under review** and may be removed in a future release. For those protocols the choice would then be reduced to recording the session or not recording it at all, and the `all` and `raw` options would stop producing a RAW dump. Database protocols - Oracle, PostgreSQL, MySQL and MSSQL(TDS) - are recorded in RAW only and are **not** affected by this change.

6. From the *Category* drop-down list select `privileged` or `non-privileged` account category.

> **Note**
>
> During manual account creation, assigning the category as *privileged* or *non-privileged* is purely informational, yet during the *Discovery*, it is automatically assigned based on the account's parameters in the source system.

7. Select the *Notes* option to activate the field where you can enter a message for *User Access Gateway* users. If permissions are granted, notes can be also edited.

> **Note**
>
> Account notes can be displayed in the *User Access Gateway*.
>
>
>

SETTINGS TAB

1. In the *SETTINGS* tab, in the *Type* field, press the *FORWARD* button.
2. In the *Target* section, select *Server* or *Pool* button to assign account to a specific server or a server pool by selecting it in the next step from the *Server*, or *Pool* drop-down list.
3. Select *Forward domain* option to have the domain name included in the string identifying the user.

> **Note**
>
> The 'Forward domain' option utilizes *user's domain settings* as follows:

- If the user has an 'AD Domain' configured, Fudo Enterprise will use it for authentication againts the server.
- If the user doesn't have an 'AD Domain' configured but has a 'Fudo Domain' configured, Fudo Enterprise will use the 'Fudo Domain' for authentication against the server.

4. With the *Authenticate against server* option enabled, Fudo Enterprise does not verify the correctness of user credentials. Login information is forwarded to the target host, which verifies whether the user is allowed to access it. Verification status is returned to Fudo, which establishes monitored connection. To enable this authentication scenario, select the *Authenticate against server* option in the *Credentials* section (available only for MySQL servers, SSH servers and RDP hosts with the *Enhanced RDP Security (TLS) + NLA* security option selected).

Note

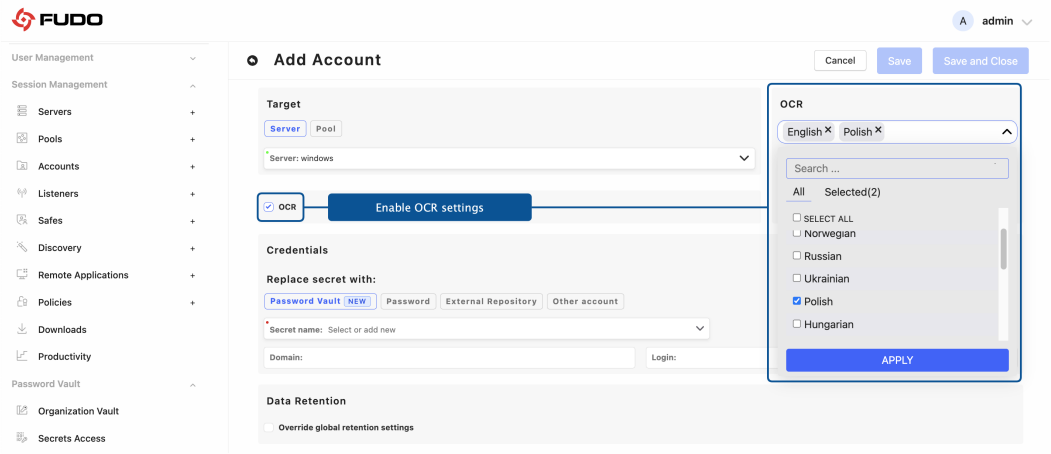
Please note that 2FA/MFA authentication won't work here. If you create a user with OATH+AD authentication the OATH part is bypassed and only the password is used and sent to the server – Fudo won't ask for the OATH token in this situation. The same goes for Duo, SMS an any other 2FA user authentication scheme that can be configured in Fudo. This restriction is specific only to forward account types.

5. Select *SSH Agent forwarding* option to authenticate the user against the target host using client's SSH key.

Note

This option is available only after selecting an SSH server. Use -A option for connecting to SSH server.

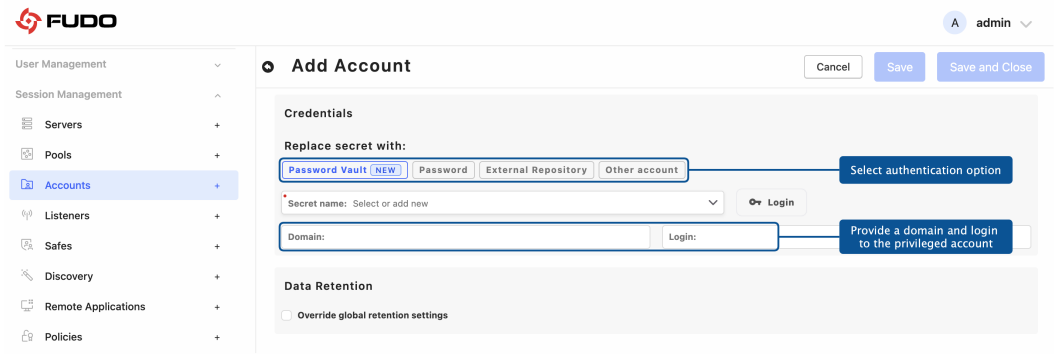
6. To have RDP, VNC or rendered HTTP sessions automatically processed, you can enable *OCR session* option for this account and select the language of processed data.



Note

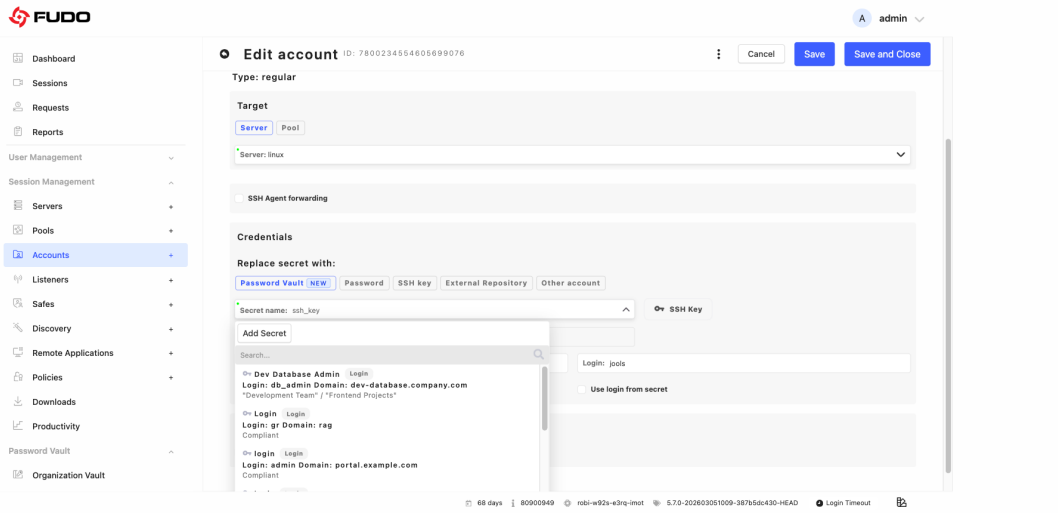
The *OCR* option is available only after selecting an RDP, VNC or HTTP server.

7. In the *Credentials* section, select a method for replacing the secret. Click the button corresponding to one of the desired options.



Password Vault

- Click the *Secret name* dropdown to view available secrets.
- Select secret from the list.
- Optionally, enable checkboxes:
  - *Use domain from secret* - Uses the domain stored in the secret
  - *Use login from secret* - Uses the login name stored in the secret



Note

The *Add Secret* button in the secret selection dropdown allows you to create a new secret directly from the account configuration interface if the required secret doesn't exist yet.

Password

- Provide account password in the *Secret* field.

Note

Two-fold authentication

With two-fold authentication enabled, user is being prompted twice for login credentials. Once for authenticating against Fudo Enterprise and once again for accessing target system.

To enable two-fold authentication, select `Password` from the *Replace secret with* section and leave the password and login fields empty.

SSH key

- Click the *Generate* button and select the key algorithm.
- Or click the *Upload* button and browse the file system to find the key definition file. Provide the *Key passphrase* if needed for the uploaded file.

Repository

- Select external repository name.

Note

To learn more about defining an external password repository, please refer to the *External Passwords Repositories* section.

Other account

- From the *Account* drop-down list, select account object, whose credentials will be used to authenticate user when establishing connection with monitored server.

Note

The list contains only objects to which you have been given access permissions.

None

- In this case no credentials will be forwarded.

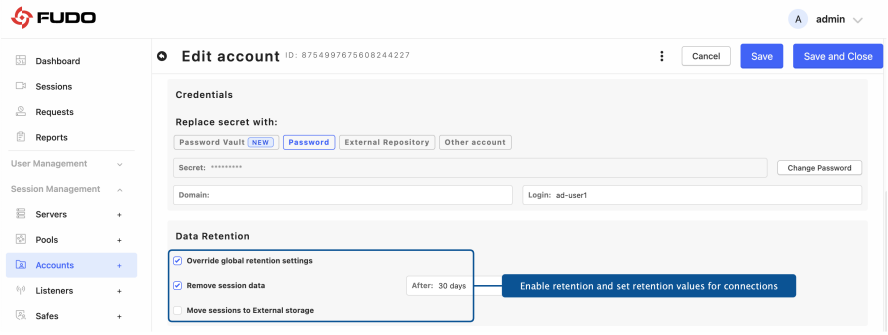
8. In the *Domain* field, enter privileged account domain.

Note

If a domain is entered in the *Domain* field, Fudo Enterprise will always use it to authenticate against the server. The domain will be added automatically to the user's login.

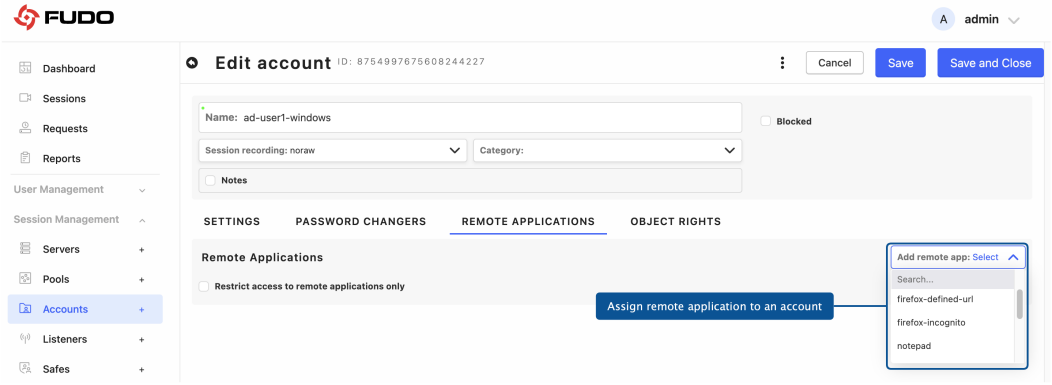
9. In the *Data retention* section, define automatic data removal settings.
    - Select *Override global retention settings* option to set other than *global retention values* for connections established using this account.
    - Check the *Remove session data* option to exclude sessions from retention mechanism.

- Next to the *Remove session data* field, define the number of days after which the session data will be moved to external storage device. Default value when the option is checked, is 30 days.



REMOTE APPLICATIONS TAB

In the *REMOTE APPLICATIONS* tab you can assign the desired remote application entries to an account, enabling direct RDP connections to those applications.



Note

To learn more about defining remote applications and restricting access to the full desktop, see the *Remote Applications* section.

Note

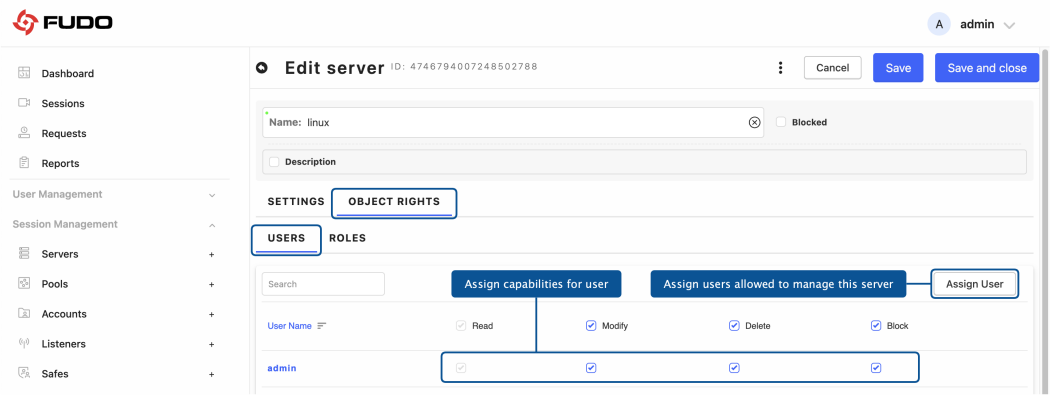
The *REMOTE APPLICATIONS* tab is active only when creating a regular or forward account with an RDP server or pool assigned.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.

4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



Note

- The *Remote applications* tab is active only when creating a regular or forward account with an RDP server or pool assigned.
- The *Secret Changers* tab is active only when creating regular account types.

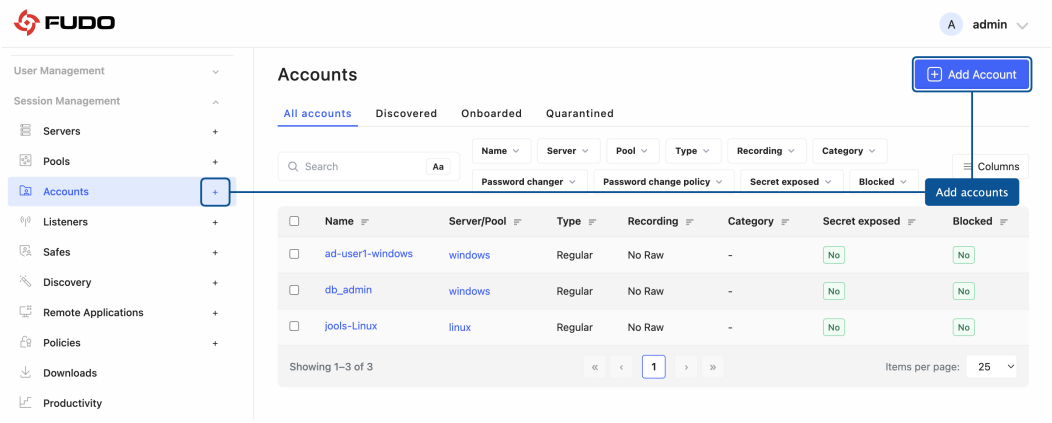
Related topics:

- *Data Model*
- *Deleting an Account*
- *Editing an Account*
- *Unblocking an Account*
- *Blocking an Account*

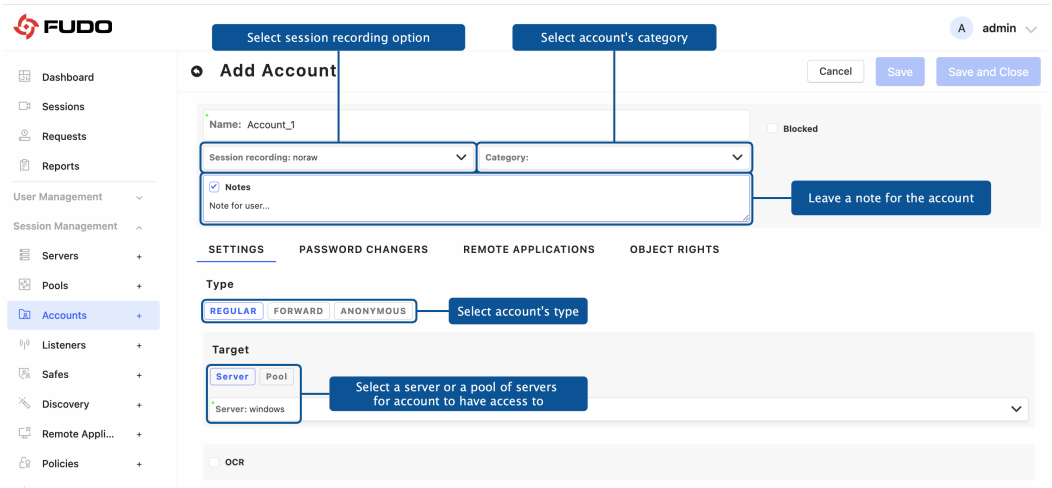
10.3.1.3 Creating a *Regular* Account

To create an account definition, follow the instructions below.

1. Select *Session Management* > *Accounts* and then click *+ Add account*, or
2. Click *+* icon next to the *Accounts* tab.



3. Define object's name.
4. Select *Blocked* option to disable account after it's created (if needed).



5. Select desired session recording option.

    - `all` - Fudo Enterprise saves session metadata (basic session information), records raw network traffic (RAW file) and stores session data in internal file format (FBS). The latter enables session playback using the built-in session player, as well as exporting sessions to a selection of video file formats.
    - `raw` - Fudo Enterprise saves session metadata (basic session information) and records raw network traffic (RAW file). The raw data can be downloaded but it cannot be played back in graphical form using the built-in session player (session player only depicts the networks packet exchange between the client and the target host).
    - `noraw` - Fudo Enterprise records the session data in a non-raw format that could be played back using the built-in session player.
    - `none` - Fudo Enterprise saves only session metadata (basic session information).

Under review

RAW session recording of protocols that support the FBS format is **under**

review and may be removed in a future release. For those protocols the choice would then be reduced to recording the session or not recording it at all, and the `all` and `raw` options would stop producing a RAW dump. Database protocols - Oracle, PostgreSQL, MySQL and MSSQL(TDS) - are recorded in RAW only and are **not** affected by this change.

6. From the *Category* drop-down list select `privileged` or `non-privileged` account category.

Note

During manual account creation, assigning the category as *privileged* or *non-privileged* is purely informational, yet during the *Discovery*, it is automatically assigned based on the account's parameters in the source system.

7. Select the *Notes* option to activate the field where you can enter a message for *User Access Gateway* users. If permissions are granted, notes can be also edited.

Note

Account notes can be displayed in the *User Access Gateway*.

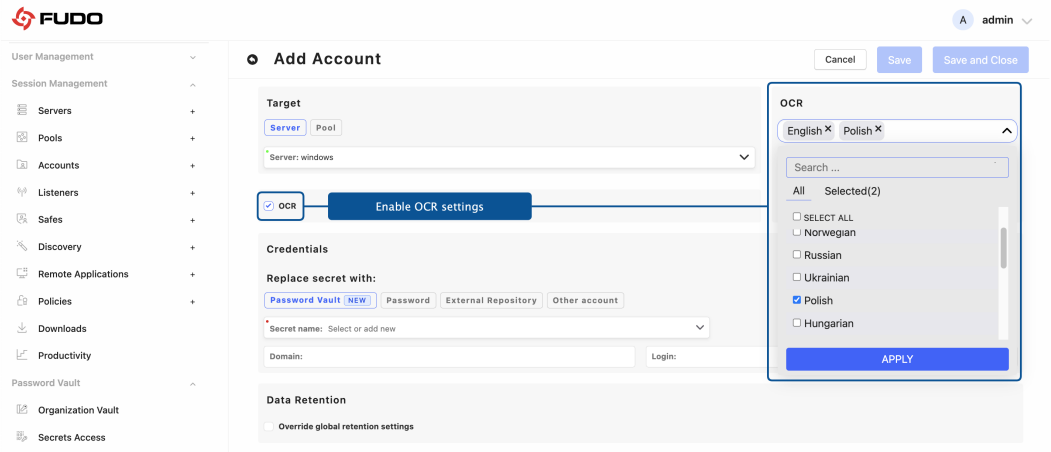
SETTINGS TAB

1. In the *SETTINGS* tab, in the *Type* section, press the *REGULAR* button.
2. In the *Target* section, select *Server* or *Pool* button to assign account to a specific server or a server pool by selecting it in the next step from the *Server*, or *Pool* drop-down list.
3. Select *SSH Agent forwarding* option to authenticate the user against the target host using client's SSH key.

Note

This option is available only after selecting an SSH server. Use -A option for connecting to SSH server.

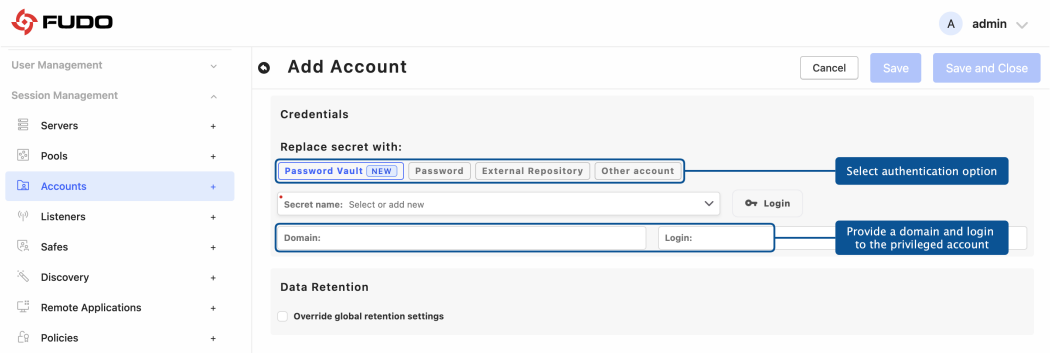
4. To have RDP, VNC or rendered HTTP sessions automatically processed, you can enable *OCR session* option for this account and select the language of processed data.



Note

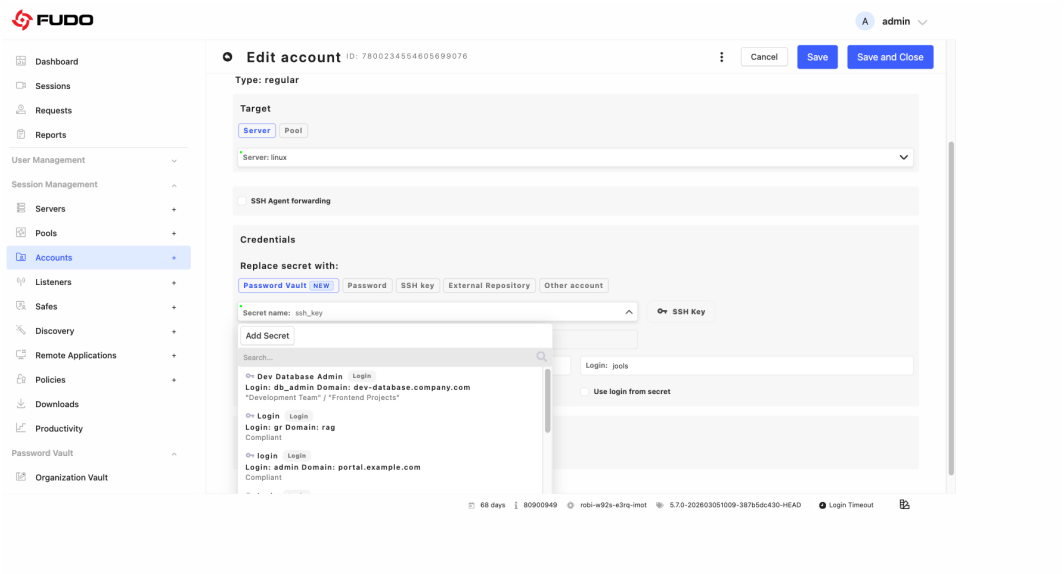
The *OCR* option is available only after selecting an RDP, VNC or HTTP server.

5. In the *Credentials* section, select a method for replacing the secret. Click the button corresponding to one of the desired options.



Password Vault

- Click the *Secret name* dropdown to view available secrets.
- Select secret from the list.
- Optionally, enable checkboxes:
  - *Use domain from secret* - Uses the domain stored in the secret
  - *Use login from secret* - Uses the login name stored in the secret



Note

The *Add Secret* button in the secret selection dropdown allows you to create a new secret directly from the account configuration interface if the required secret doesn't exist yet.

Note

When you assign a secret from the *Password Vault*, its secret changers and verifiers are managed on the secret itself — in Password Vault > Organization Vault, in the secret's CHANGERS tab — not on this account. In that case the account's SECRET CHANGERS tab stays inactive.

If you instead select the *Password* method below, secret changers and verifiers are assigned on the account, in its SECRET CHANGERS tab.

Password

- Provide account password in the *Secret* field.

Note

Two-fold authentication

With two-fold authentication enabled, user is being prompted twice for login credentials. Once for authenticating against Fudo Enterprise and once again for accessing target system.

To enable two-fold authentication, select `password` from the *Replace secret with* drop-down list and leave the password and login fields empty.

SSH key

- Click the *Generate* button and select the key algorithm.
- Or click the *Upload* button and browse the file system to find the key definition file. Provide the *Key passphrase* if needed for the uploaded file.

External Repository

- Select external repository name.

> **Note**
>
> To learn more about defining an external password repository, please refer to the *External Passwords Repositories* section.

Other account

- From the *Account* drop-down list, select account object, whose credentials will be used to authenticate user when establishing connection with monitored server.

> **Note**
>
> The list contains only objects to which you have been given access permissions.

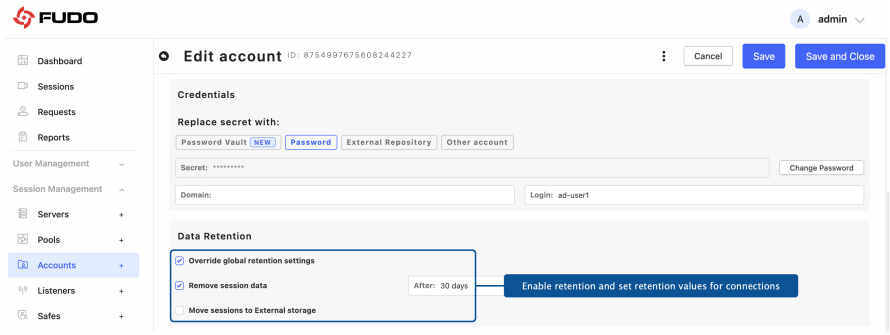
6. In the *Domain* field, enter privileged account domain.

> **Note**
>
> If a domain is entered in the *Domain* field, Fudo Enterprise will always use it to authenticate against the server. The domain will be added automatically to the user's login.

7. In the *Login* field, type in login to the privileged account.

> **Warning**
>
> For regular accounts with an empty login, the **domain attribute is not supported.** Such configurations will trigger an error when saved. If account with this setup already exists, the domain value will be automatically **removed during the upgrade** to the version that includes this validation (Fudo Enterprise 5.5.8 and later).

8. In the *Data retention* section, define automatic data removal settings.
    - Select *Override global retention settings* option to set other than *global retention values* for connections established using this account.
    - Check the *Remove session data* option to exclude sessions from retention mechanism.
    - Next to the *Remove session data* field, define the number of days after which the session data will be moved to external storage device. Default value when the option is checked, is 30 days.



9. If Password option was chosen as an authentication method, provide additional configuration in the *SECRET CHANGERS* tab. Otherwise, go to the chapter describing *Remote Applications configuration*.

Note

The *SECRET CHANGERS* tab is active only when creating a regular account with a *Password* method selected, and an Login to the privileged account provided in the *Credentials* section.

SECRET CHANGERS TAB

1. Select *Secret change policy* from the list of the configured secret change policies.
2. In the *Password checkout time limit* field, define the time after which the password is returned automatically.

Note

Defining the password checkout time limit automatically enables the Secret Checkout feature for the particular Safe.

3. Select *Change secret after last checkin* option to change the password automatically after it has been returned by the last user.

Note

This options is available only for Secret Checkout feature and it's enabled after specifying the *Password checkout time limit*.

4. Select *Change secret after session* option to change the account password remotely after the session is ended.

Note

This option requires to choose at least one *Secret changer* and a *Secret change policy* any other than `Static, without restrictions`.

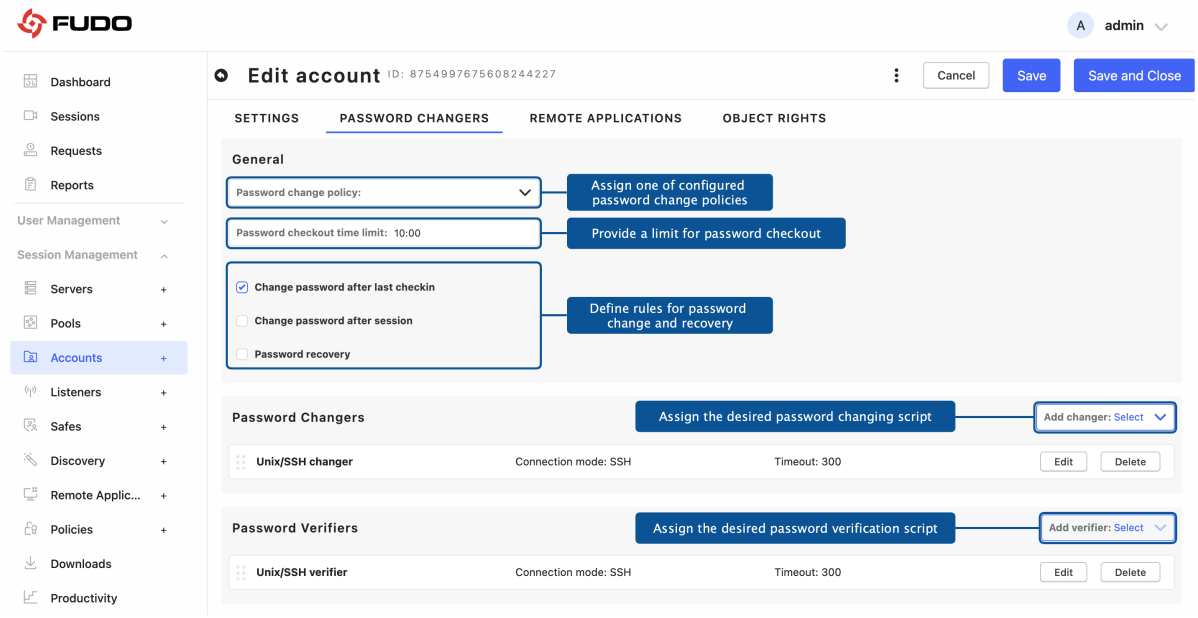
Refer to the *Secret Changers* topic for detailed information on setting up secret changers.

5. Check the *Password recovery* option to set a Secret verifier, to automatically trigger a

secret changer if it verifies that the password for an Account was changed and a new password is not stored in Fudo Enterprise.

Note

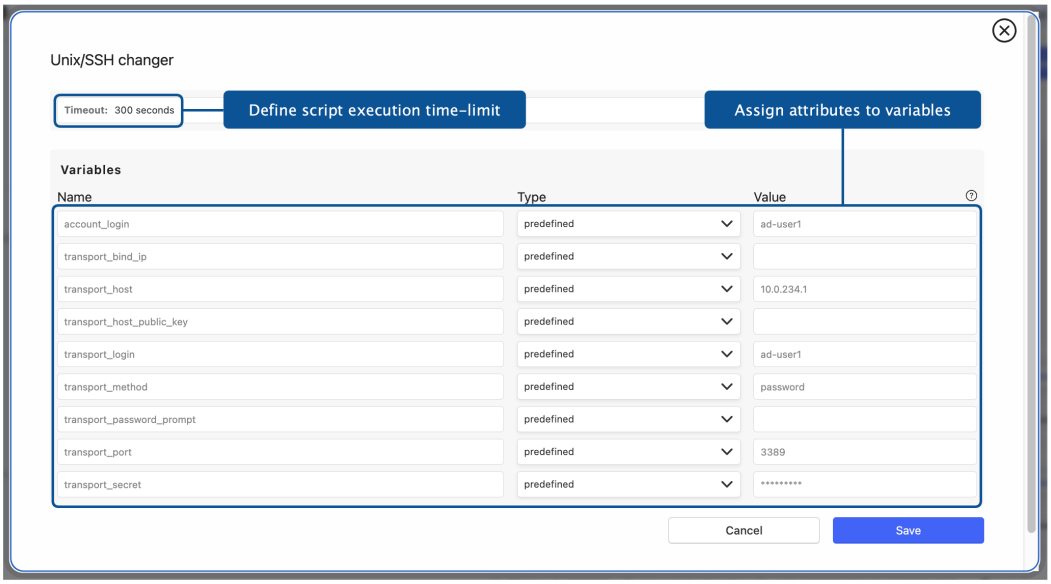
Having the *Password recovery* option enabled, the Secret Verifier spawns "Trigger secret changer" action in the account. When it's disabled, the Secret Verifier only sends event "Unable to verify password for account <account_name>".



6. In the *Secret Changers* field select desired password changing script from the drop-down list, to have the password to the account changed automatically according to the *secret change policy*.
7. In the *Secret Changers* window, in the *Timeout* field, define the script's execution time limit.
8. In the *Variables* section, assign attributes to variables.

Warning

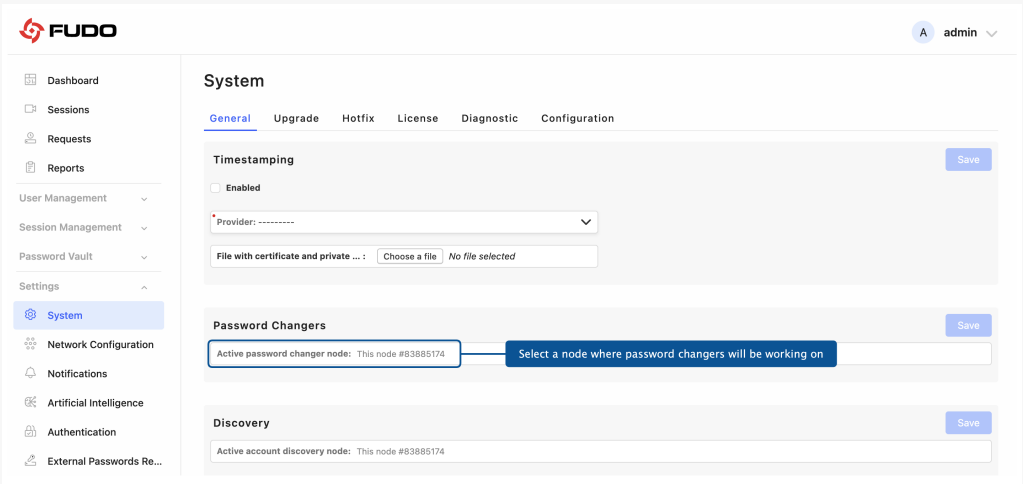
- To handle a password change, you must use an account (`transport_login` and `transport_secret`) that has delegated *Reset user passwords and force password change at next logon* permissions for the *Organizational Unit (OU)* containing the users whose passwords will be changed, or the account must be a member of the *Account Operators* group.



9. Click *Save* to close the window.
10. In the *Secret Verifiers* field select desired Secret verifier from the drop-down list, to have the password to the account verified automatically according to the *secret policy*.
11. In the *Secret Verifiers* window, in the *Timeout* field, define the script's execution time limit.
12. In the *Variables* section, assign attributes to variables.
13. Click *Save* to close the window.

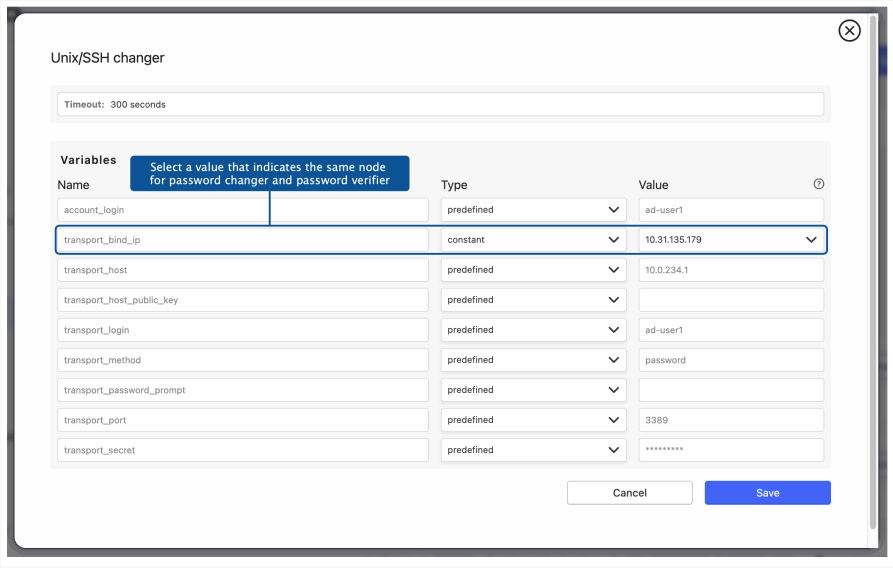
Note

Fudo Enterprise allows changing a password on a different node than the one that set as an *Active cluster node for Secret Changers*.



In order to have this configured, the following condition should be met:

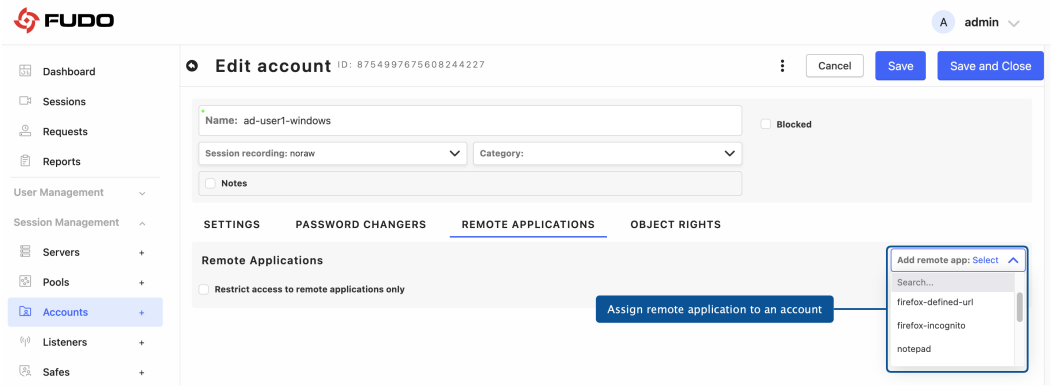
- Setting up a **Secret Changer / Secret Verifier** for an account, a value for `transport_bind_ip` variable should indicate the same cluster node for all secret changers as well as Secret verifiers.



- If the `transport_bind_ip` variable values indicate different cluster nodes, the configured secret changer/verifier will be running on a node that set as an *Active cluster node for Secret Changers*.

REMOTE APPLICATIONS TAB

In the *REMOTE APPLICATIONS* tab you can assign the desired remote application entries to an account, enabling direct RDP connections to those applications.



Note

To learn more about defining remote applications and restricting access to the full desktop, see the *Remote Applications* section.

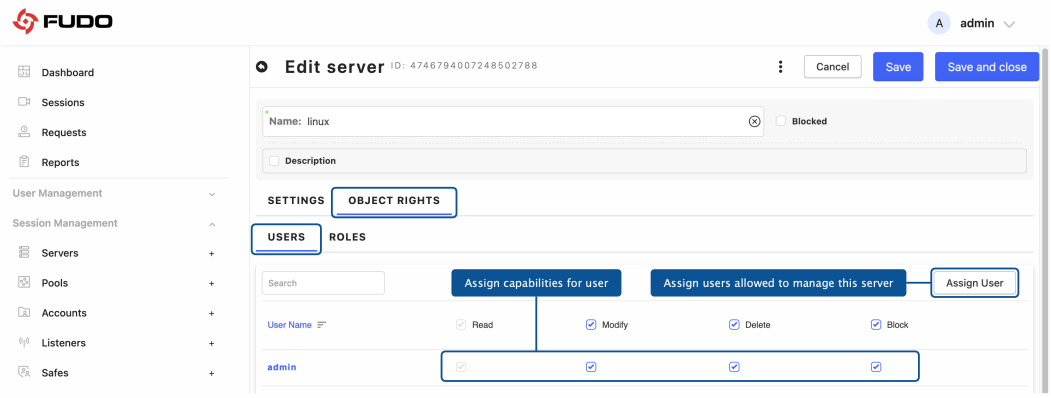
Note

The *REMOTE APPLICATIONS* tab is active only when creating a regular or forward account with an RDP server or pool assigned.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.

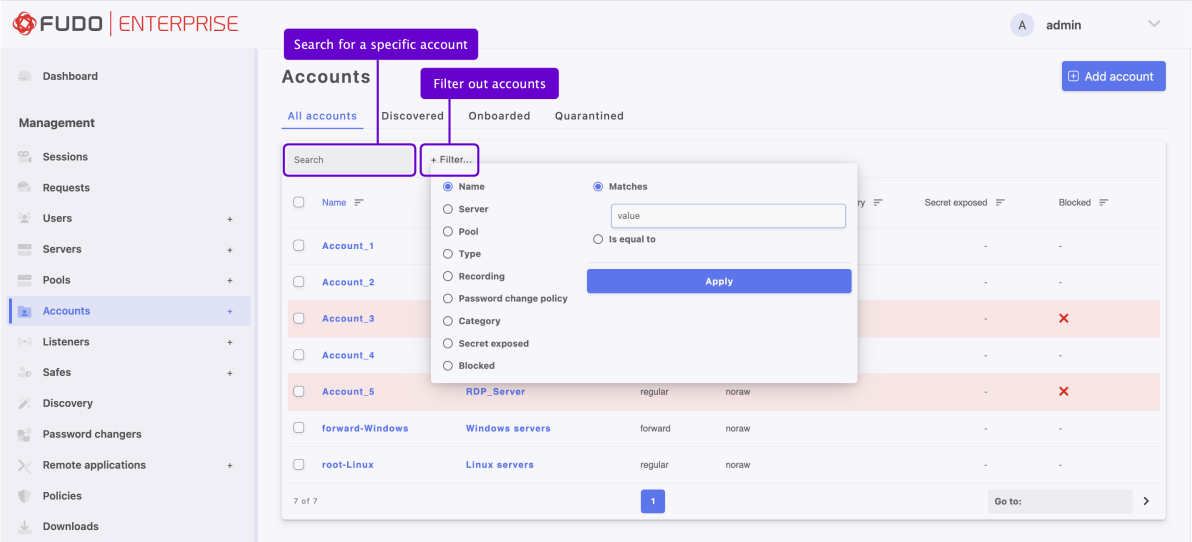


Related topics:

- *Data Model*
- *Editing an Account*
- *Blocking an Account*
- *Unblocking an Account*
- *Deleting an Account*
- *Secret Changers - Active Cluster Node*

10.3.2 Editing an Account

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Find and click desired object's name to open its configuration page.
4. Modify configuration parameters as needed.
5. Click *Save*.

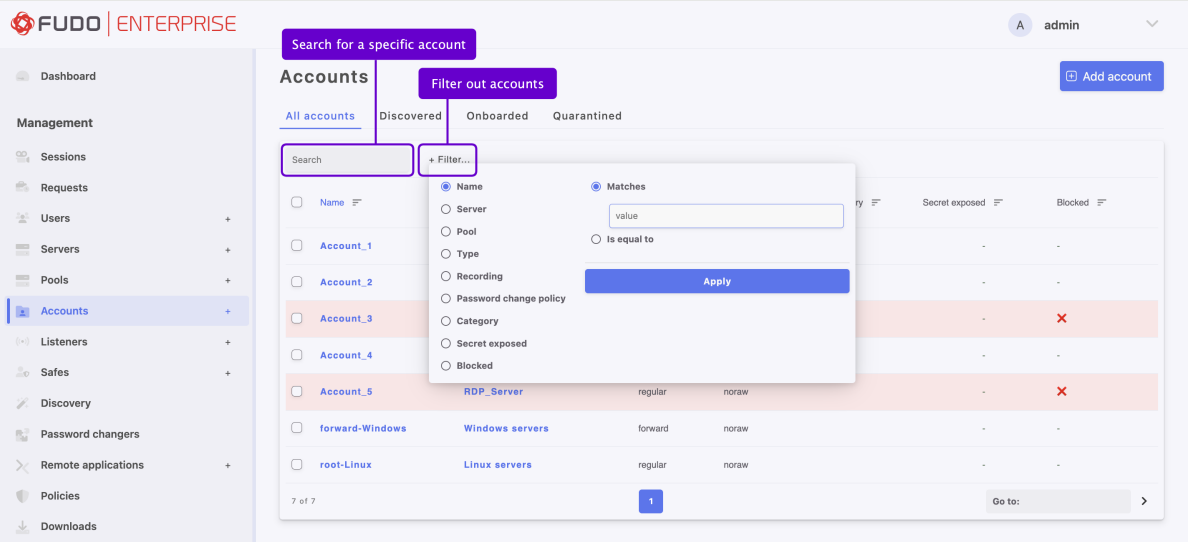
Related topics:

- *Creating an Account*
- *Blocking an Account*
- *Unblocking an Account*
- *Deleting an Account*

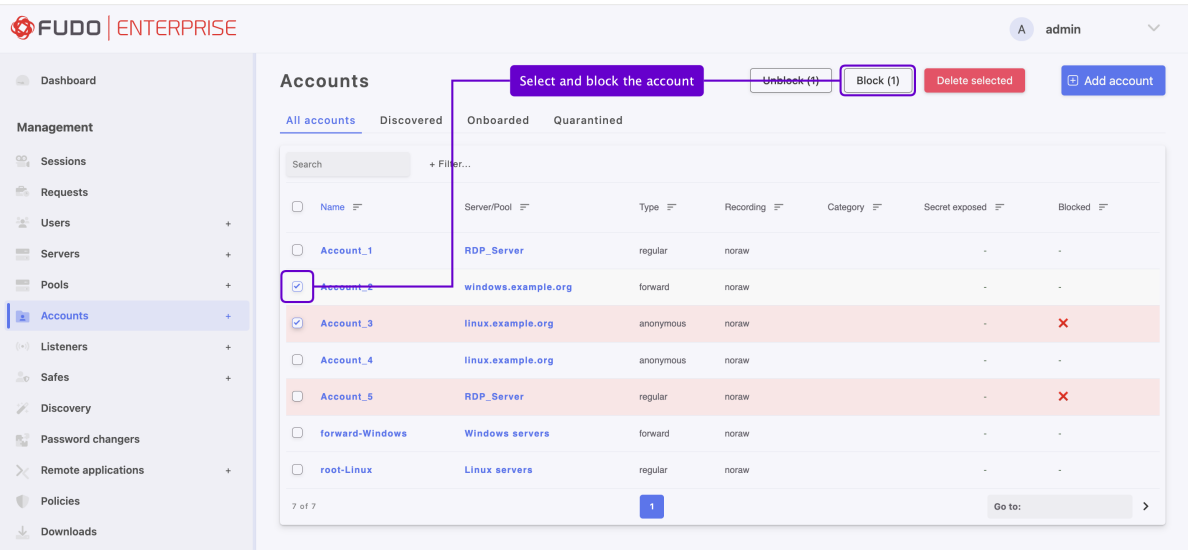
10.3.3 Blocking an Account

> **Warning**
>
> Blocking an accout definition will terminate all current connections to servers which use selected account for accessing those servers.

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Click *Block*.



4. Provide mandatory blocking reason and click *Confirm*.

Note

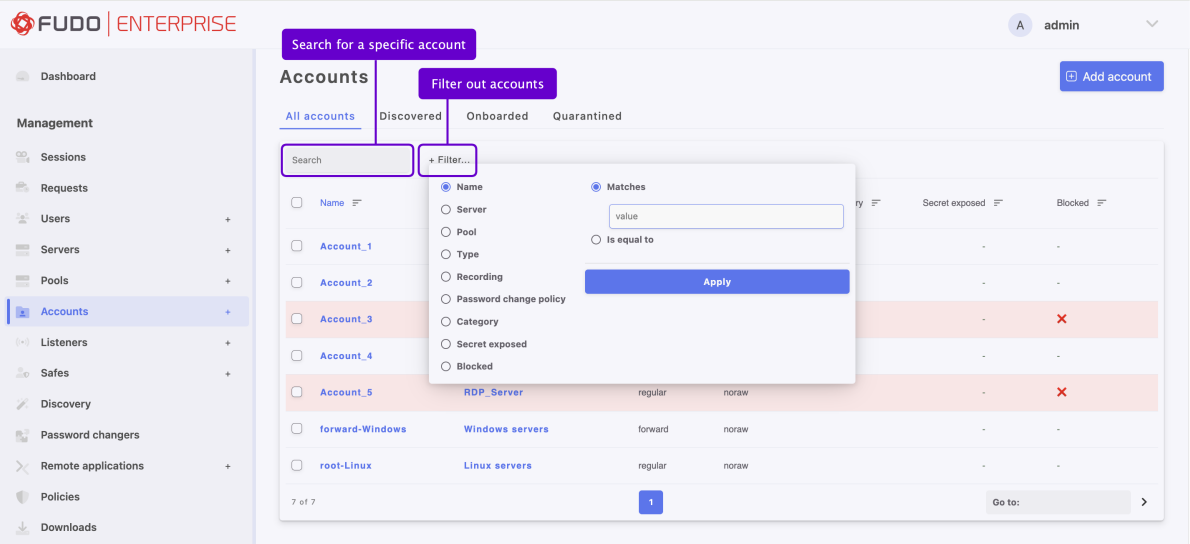
To view the blocking reason, place the cursor over the red cross icon on the accounts list.

Related topics:

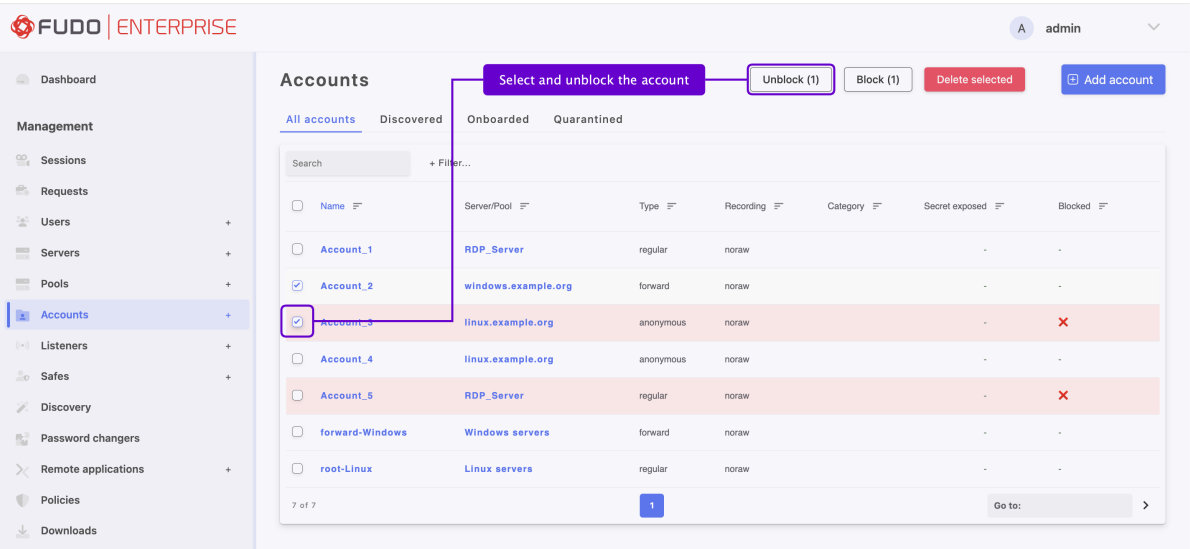
- *Creating an Account*
- *Editing an Account*
- *Unblocking an Account*
- *Deleting an Account*

10.3.4 Unblocking an Account

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Click *Unblock*.



4. Confirm unblocking selected objects.

Related topics:

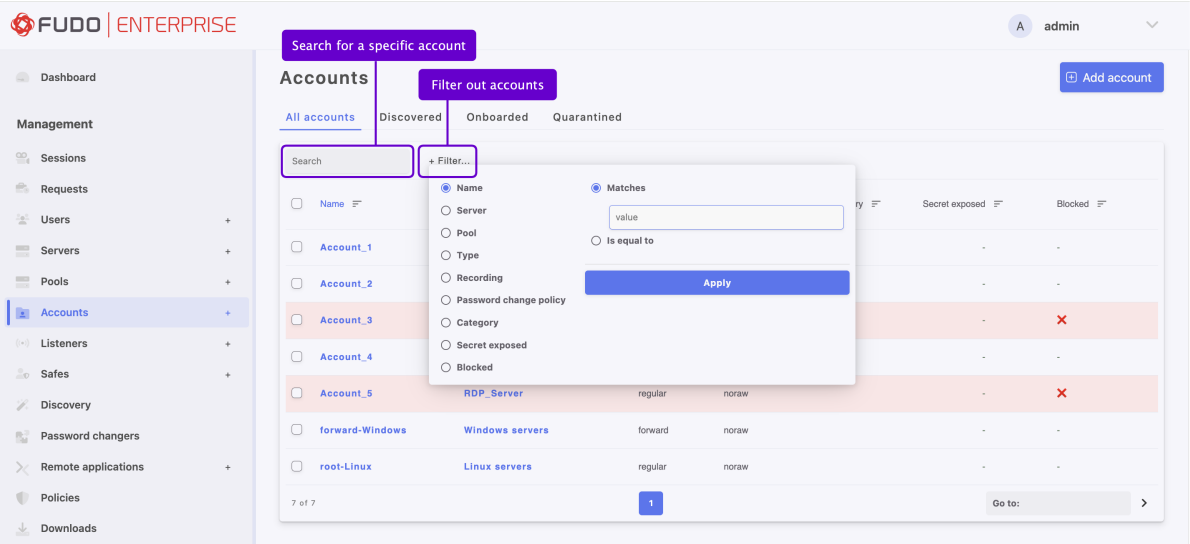
- *Blocking an Account*
- *Creating an Account*
- *Editing an Account*
- *Deleting an Account*

10.3.5 Deleting an Account

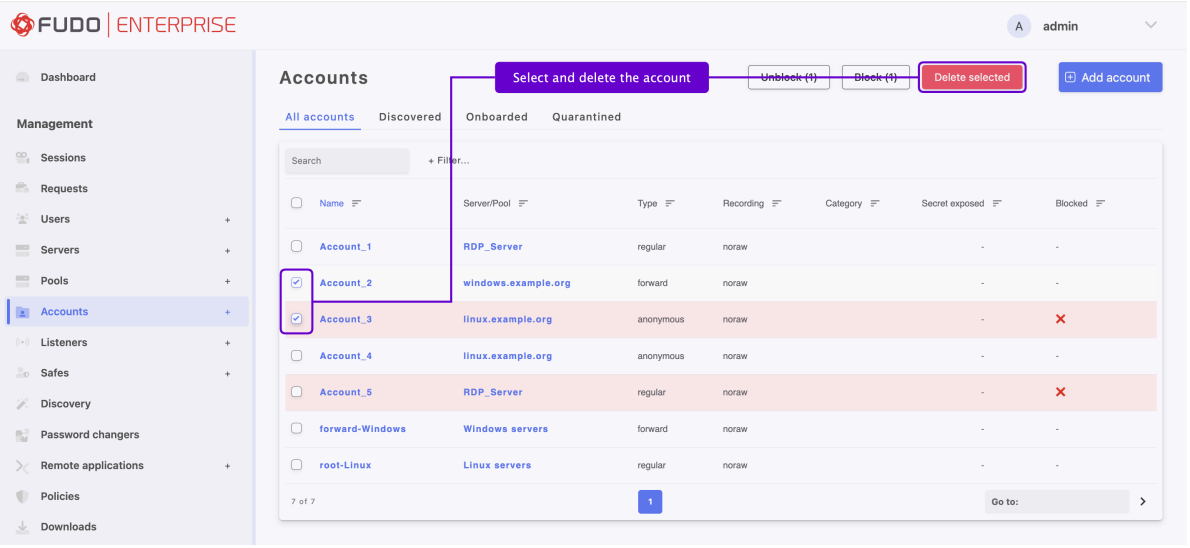
Warning

Deleting an accout definition will terminate all current connections to servers which use selected account for accessing those servers.

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Click *Delete selected*.



4. Confirm deletion of selected objects.

Related topics:

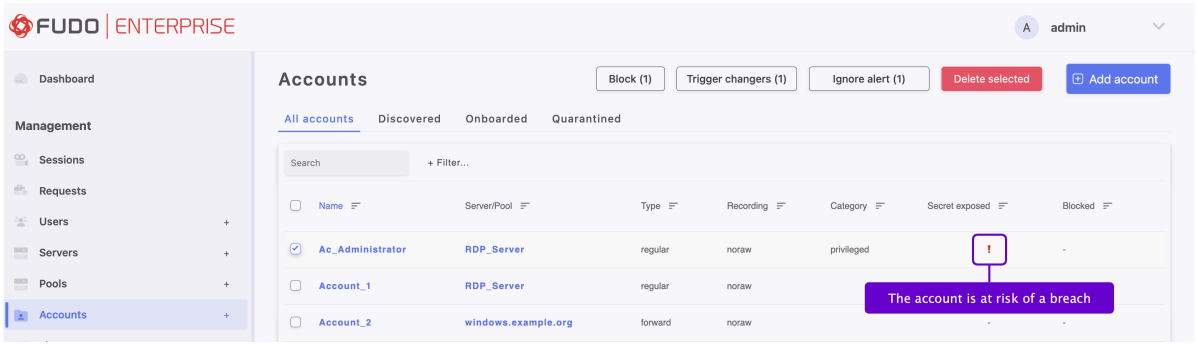
- *Creating an Account*
- *Editing an Account*
- *Blocking an Account*

- *Unblocking an Account*

10.3.6 Managing Security Alerts

Fudo Enterprise tracks user's action in *User Access Gateway* and registers every password viewing. Blocking a user who has seen the current password can help prevent a potential security breach. Fudo Enterprise identifies such events and communicates them to system's administrators.

> **Note**
>
> Triggering a secret change is available only for accounts with an assigned secret changer and secret change policy that has the *Secret change* option active.

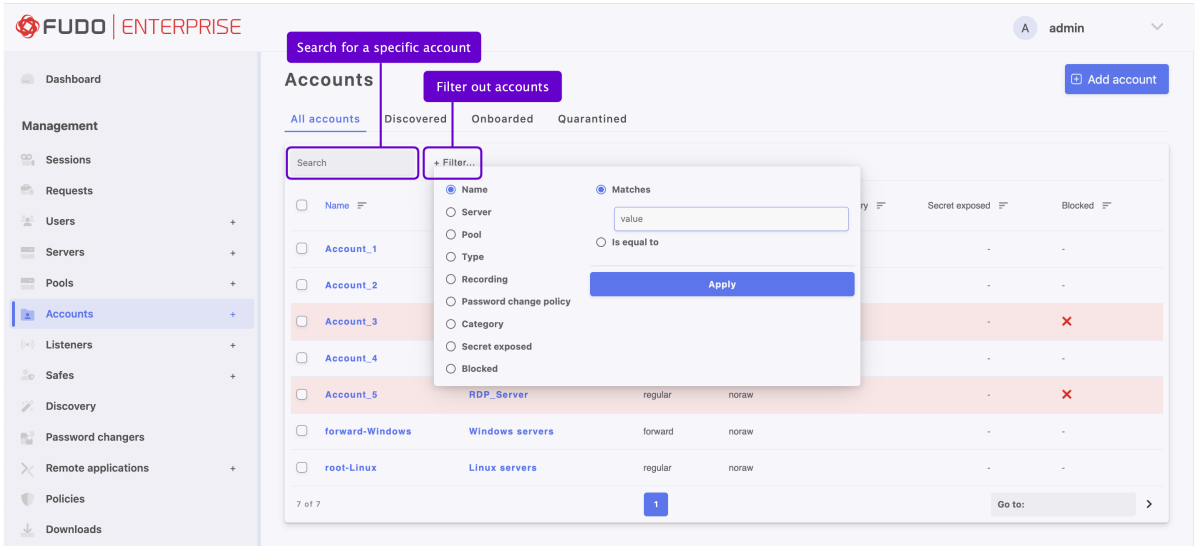


Administrator has an option to ignore the alert or trigger a *secret changer* assigned to the account.

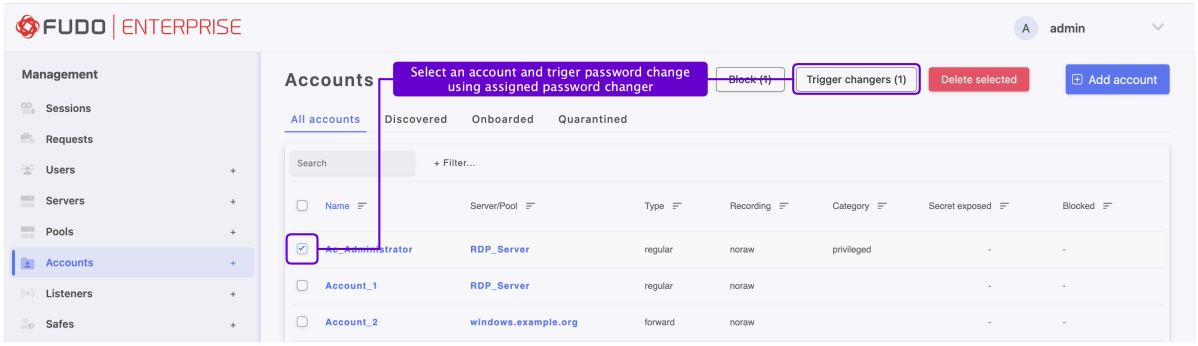
10.3.6.1 Triggering Secret Change

Triggering secret change on the accounts list

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



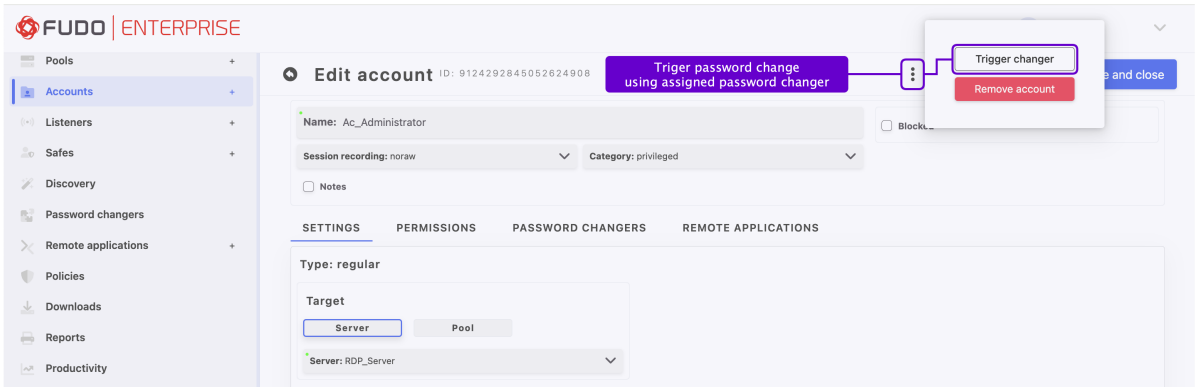
3. Select an account and click *Trigger changers*.



4. Confirm changing secret to selected accounts.

Triggering secret change from account form

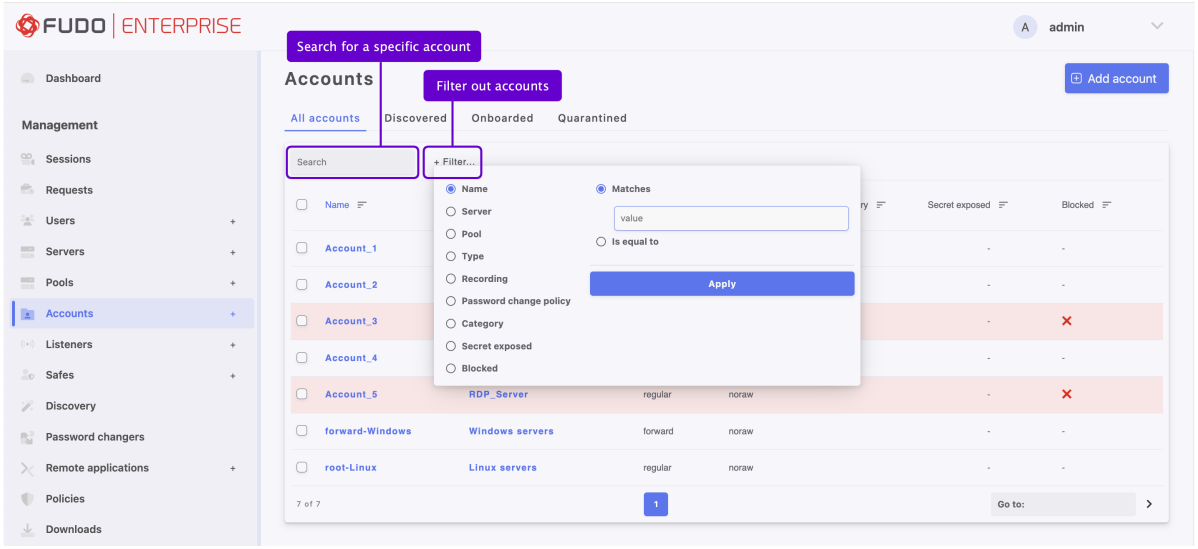
1. Click on the chosen account's name to edit its configuration.
2. Click on the three dots symbol before the *Cancel* and *Save* buttons to reveal the additional menu, and then click *Trigger changer*.



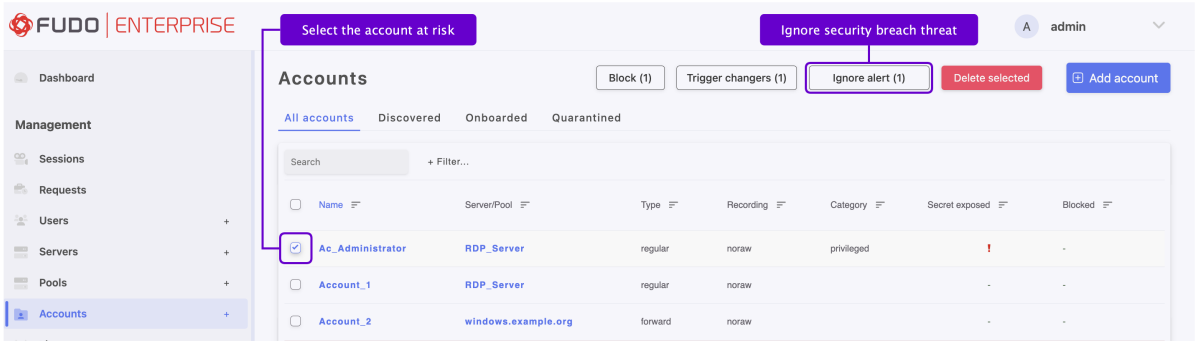
10.3.6.2 Ignoring Security Alert

Ignoring security alert on the accounts list

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



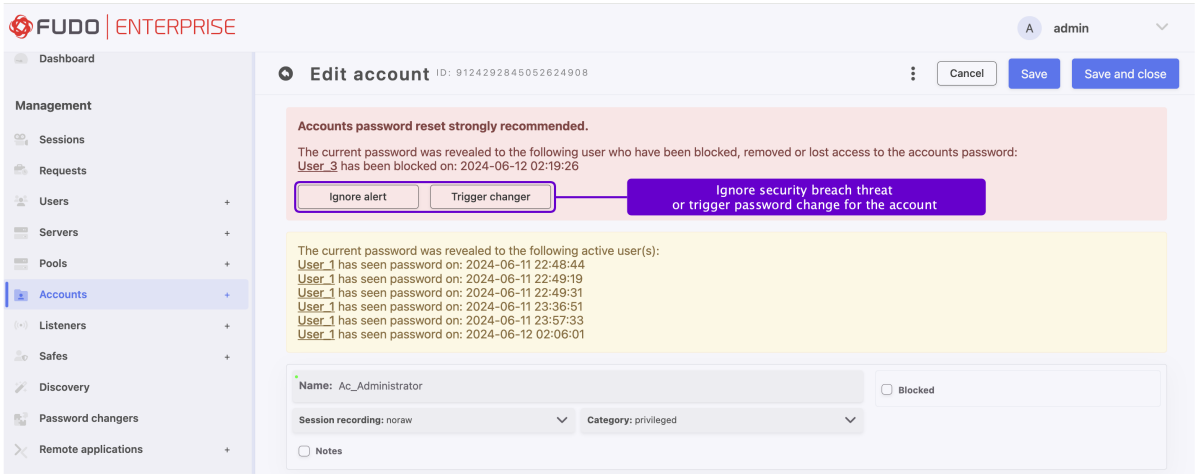
3. Select the account at risk and click *Ignore alert*.



Ignoring security alert from the account form

1. Click on the account's at risk name to edit its configuration.

> **Note**
>
> Account edit form contains a list of blocked users who have seen current password.



2. Click :*Ignore alerts*.

Related topics:

- *Secret Changers*
- *User Access Gateway*

10.4 Listeners

Listener determines server connection mode (proxy, bastion) as well as its specifics.

10.4.1 Creating a Listener

> **Warning**

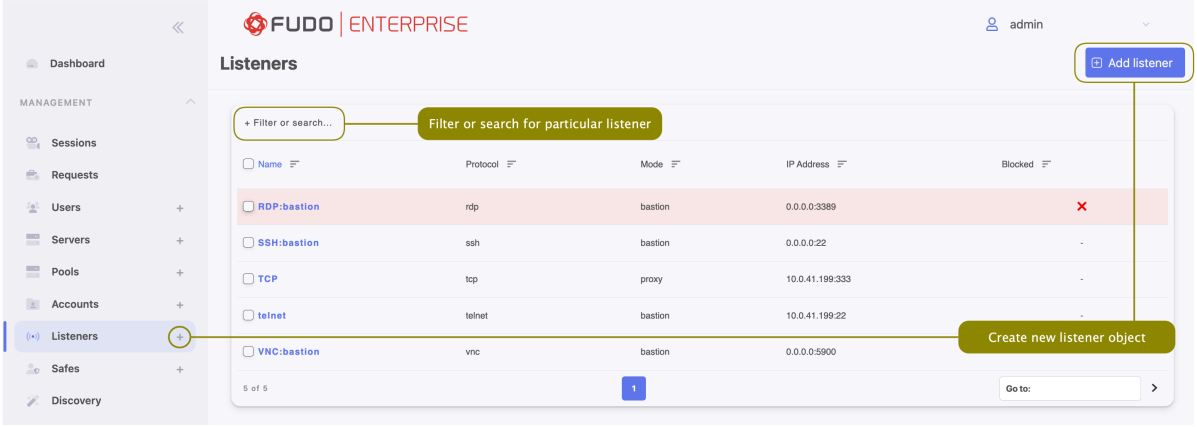
Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances **must not** be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

Note

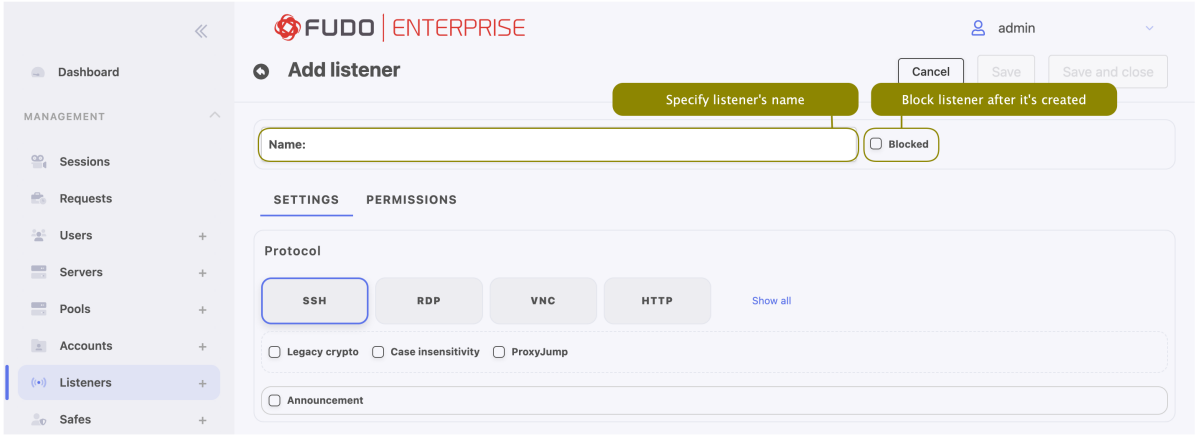
- A listener cannot link to an account that is assigned to a server with a different protocol then the one defined in the listener.
- A *proxy* type listener can link to only one server.
- A *bastion* type listener cannot link to an anonymous account.
- A listener cannot link to the same anonymous account through two different safes.
- A listener cannot link to an *anonymous* and a *regular* or *forward* account to the same server with the same protocol as the listener's protocol.
- A listener cannot link to two *regular* or *forward* type accounts to the same server with the same protocol as the listener's protocol, to which a single user has access.
- For a given linked RDP listener and RDP server, both have to use either *Standard RDP Security* or *TLS* or *NLA*.

In order to create a Listener, follow the instruction:

1. Click + icon in the main menu next to the *Listeners* tab of the *User Management* subsection, or
2. Select *Management* > *Listeners* and then click + *Add listener*.



2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.



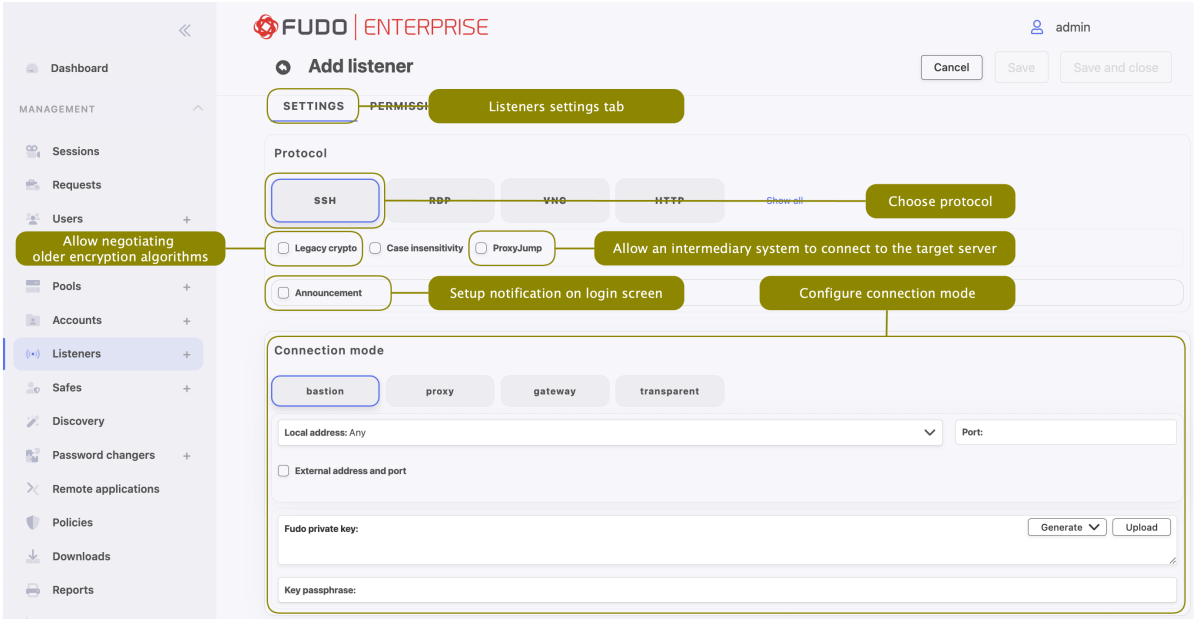
4. Select the appropriate section below to continue configuring the listener for the selected protocol:

- *Setting up the SSH listener*
- *Setting up the RDP listener*
- *Setting up the VNC listener*
- *Setting up the HTTP listener*
- *Setting up the Modbus listener*
- *Setting up the MySQL listener*
- *Setting up the Oracle listener*
- *Setting up the TCP listener*
- *Setting up the MS SQL listener*
- *Setting up the PostgreSQL listener*
- *Setting up the Telnet listener*
- *Setting up the Telnet 3270 listener*
- *Setting up the Telnet 5250 listener*

10.4.1.1 Setting up the SSH Listener

This section describes how to setup SSH listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *Settings* tab and press the `SSH` button in the *Protocol* field.
2. Select *Legacy crypto* option to allow negotiating older encryption algorithms when establishing connections. For the list of these algorithms, see *SSH*.
3. Select the *Case insensitivity* option to disable case sensitivity in the username string when connecting over this listener.



4. Select *ProxyJump* option to allow an intermediary system to connect to the target server.
5. Select *Announcement* option to enable it's field and type in the notification that will be presented to the user on the login screen.
6. In the *Connection mode* section, select desired connection mode.

   Mode: bastion

> **Note**
>
> - User connects to the target host by including name along with account login on the target server and target server address in the login string, e.g. `john_smith#root#192.168.0.110`.
> - For details on bastion connection mode, refer to *Connection modes* topic.

- Select `bastion` button in the *Connection mode* field.
- Select the IP address from the **Local address** drop-down list and enter port number.

> **Note**
>
> - The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
> - Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
> - When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.

- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

- Select *External address* option to enable its field and enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Mode: proxy

Note

User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

- Select `proxy` button in the *Connection mode* field.
- Select the the IP address from the **Local address** drop-down list and enter port number.

Note

- The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

- Select *External address* option to enable its field and enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Mode: tunnel

Note

The user connects to the target server through an SSH tunnel.

- Press the `tunnel` button in the *Connection mode* field.
- From the *Local address* dropdown list, select an IP address and enter the port.

> **Note**
>
> - The **Keys** field displays automatically generated SSH, TLS, and Standard RDP Security keys, as well as the TLS certificate required for "Tunnel"-type listener. You can also upload your own keys and certificate.
> - The *Establishing Connections to Servers via SSH Tunnel in Fudo Enterprise* section provides examples of how to establish such connections for selected protocols.

7. In the *Fudo private key* field, click *Generate key pair* to generate private/public key pair, or click *Upload* to upload it.
8. Click *Save*.

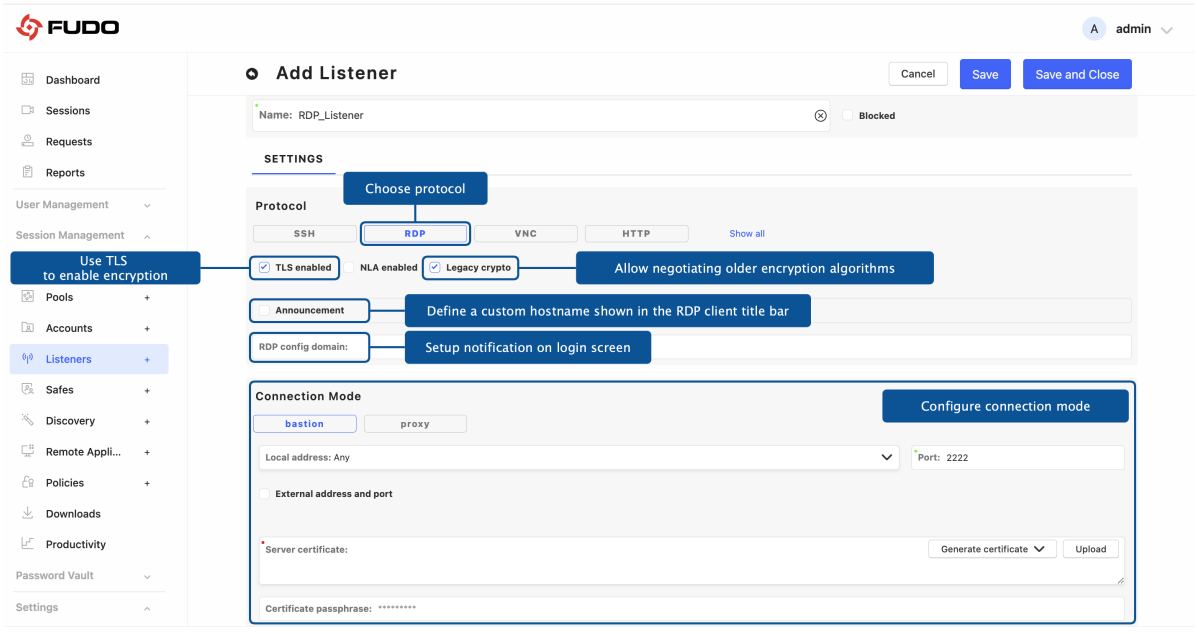
Related topics:

- *Data model*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*

10.4.1.2 Setting up the RDP Listener

This section describes how to setup RDP listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *Settings* tab and press the `RDP` button in the *Protocol* field.
2. Select the *TLS enabled* option to enable encryption.
3. Check the *NLA enabled* option for additional security.



Note

Security mode must match the security mode setting in the *RDP server configuration*.

In case the *TLS enabled* option is chosen, select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing RDP connections.

Selecting the RDP implementation

Starting with version 6.2, Fudo Enterprise handles RDP connections with a new implementation of the protocol, which additionally records the video stream sent by the server and the sound of the session. The previous implementation is still available and is selected per listener with the *Use legacy RDP implementation* option, placed under *Legacy crypto*.

Note

A newly created listener uses the new implementation - the *Use legacy RDP implementation* option is cleared by default. Listeners that already existed before the upgrade keep the option **selected**, so their behaviour does not change until you clear it.

Warning

The new implementation does not support three cases, and they behave differently:

- **Standard RDP Security**, that is connections with the *TLS enabled* option cleared. Fudo Enterprise does not allow such a listener to be saved with *Use legacy RDP implementation* cleared, so the previous implementation is enforced here.
- **Kerberos authentication to the monitored server.** This case is **not** enforced - select the *Use legacy RDP implementation* option yourself on such listeners, otherwise their connections will stop working.
- **Monitored servers that do not use the RDP graphics pipeline (RDPGFX)**, for example older systems. A session to such a server is ended with a message, because it could not be recorded. Select the *Use legacy RDP implementation* option on the listener used to connect to such servers.

Note

The new implementation records sessions only in the FBS format and does not produce a RAW dump. Recording options that ask for RAW have no effect on listeners that use it, and trusted timestamping, which operates on RAW files, is therefore unavailable for such sessions in version 6.2. See *Trusted Timestamping*.

Note

Recording the sound of a session and video recording are available only with the new implementation. Refer to *the safe functionality options* for the safe options that control them.

4. Select *Announcement* option to enable it's field and type in the notification that will be presented to the user on the login screen.
5. In the *Connection mode* section, select desired connection mode.

   Mode: bastion

   Note

   - User connects to the target host by including name along with account login on the target server and target server address in the login string, e.g. `john_smith#root#192.168.0.110`.
   - For details on bastion connection mode, refer to *Connection modes* topic.

   - Select `bastion` button in the *Connection mode* field.
   - Select the IP address from the **Local address** drop-down list and enter port number.
   - Select *External address* option to enable its field and enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

   Note

   - The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
   - Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
   - When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
   - In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

   Mode: proxy

   Note

   User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

   - Select `proxy` button in the *Connection mode* field.
   - Select the the IP address from the **Local address** drop-down list and enter port number.

Note

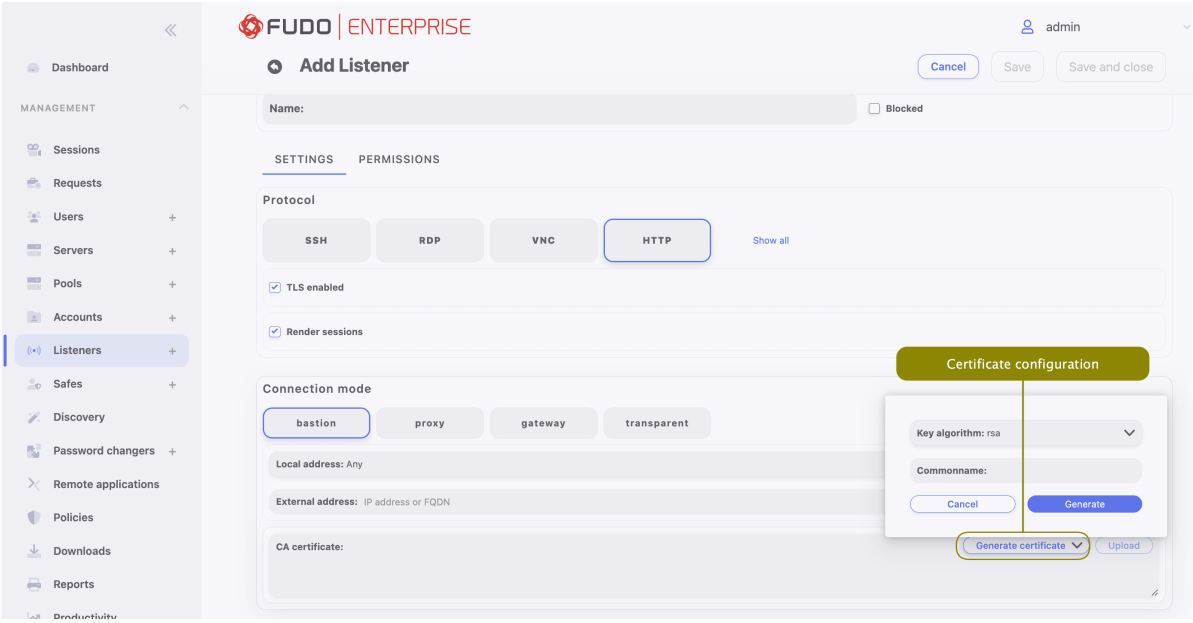
- The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

- Select *External address* option to enable its field and enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Note

The RDP config domain field can be used to define a custom hostname shown in the RDP client title bar for connections started from the User Access Gateway using the native RDP client. For a full configuration example, refer to *Custom RDP Hostname in the Session Title*.

6. In the *Server certificate* field, click *Generate certificate* to generate TLS certificate, or click *Upload* to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.



7. Click *Save*.

Note

The *Server certificate* is also used to sign the connection definition file that the User Access Gateway generates for the *Native client* option. Since the April 2026 Windows update, the Remote Desktop client verifies the signature of such files and warns the user when it is missing.

- If the workstations trust the certificate, the user can dismiss the warning permanently by selecting *Don't ask again for connections to this publisher*.
- With a self-signed certificate the warning still appears, but the user can allow the publisher permanently.
- A listener with no server certificate serves unsigned files, exactly as before.
- The certificate is used only if it is currently valid and has the *Server Authentication* extended key usage. Otherwise the file is served unsigned and the event log shows the reason (FSW1710). A file signed with such a certificate would be rejected by the Remote Desktop client.
- If the *Local address* is *User Access Gateway*, the address in the file is the name that the user typed in the browser to open the User Access Gateway. Such a file is signed only if the *list of Access Gateway allowed hosts* is filled and the name is on the list or is one of the node's User Access Gateway addresses. The file then contains the name from the list. If the list is empty, which is the default, such files are not signed. To have them signed regardless of the name that the user typed, select the *External address* option of the listener.
- The same applies to a listener that a *Reverse Proxy* publishes on `0.0.0.0` or `::` without an external address. To sign its files, add the name that users type to reach the User Access Gateway through the Reverse Proxy to the list of allowed hosts, or set the external address in the listener mapping.
- For a listener with *TLS enabled*, the *User Access Gateway* local address and no external address, the listener form shows whether the files will be signed.
- Signing can be turned off for a safe with the *Sign .rdp files* option in the *safe functionality settings*.

To remove the warning entirely, use a certificate the workstations already trust.

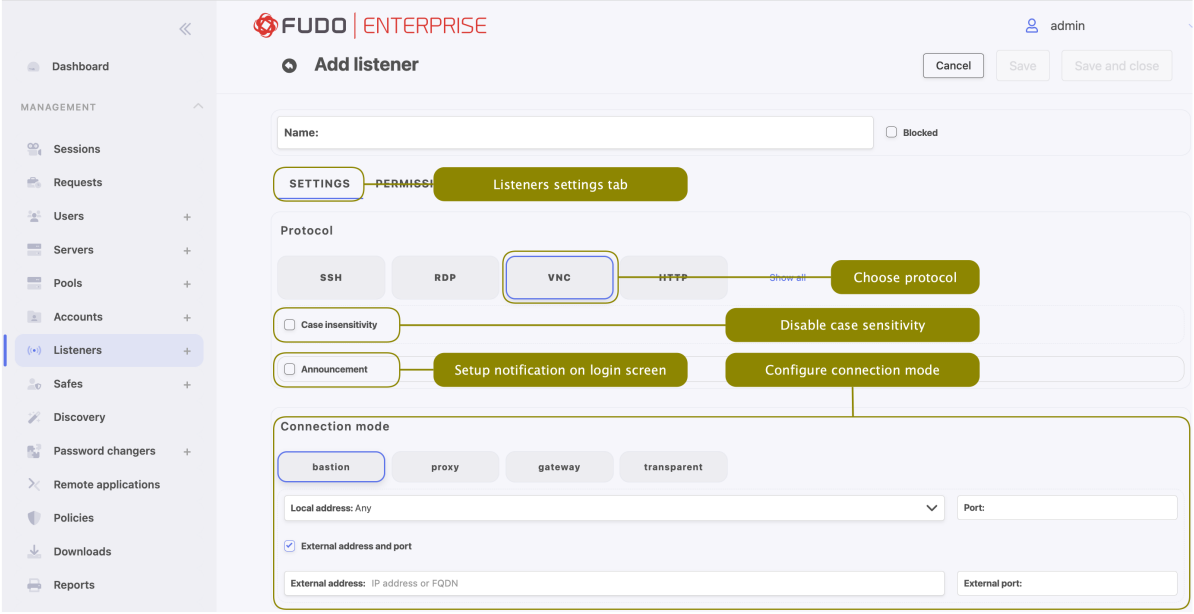
Related topics:

- *Data model*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*

10.4.1.3 Setting up the VNC Listener

This section describes how to setup VNC listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *Settings* tab and press the `VNC` button in the *Protocol* field.



2. Select the *TLS enabled* option to enable encryption.
3. (Optional) Select the *Legacy crypto* checkbox to enable support for older encryption algorithms if your PostgreSQL clients require them.
4. Select the *Case insensitivity* option to disable case sensitivity in the username string when connecting over this listener.
5. Select *Announcement* option to enable it's field and type in the notification that will be presented to the user on the login screen.
6. In the *Connection mode* section, select desired connection mode.

   Mode: bastion

> **Note**
>
> - User connects to the target host by including name along with account login on the target server and target server address in the login string, e.g. `john_smith#root#192.168.0.110`.
> - For details on bastion connection mode, refer to *Connection modes* topic.

   - Select `bastion` button in the *Connection mode* field.
   - Select the IP address from the **Local address** drop-down list and enter port number.

Note

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

Mode: proxy

Note

User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

- Select `proxy` button in the *Connection mode* field.
- Select the the IP address from the **Local address** drop-down list and enter port number.

Note

- The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

- Select *External address* option to enable its field and enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

7. If the *TLS enabled* option was selected, go to the *Server certificate* field and click *Generate certificate* to generate TLS certificate, or click *Upload* to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.
8. Click *Save*.

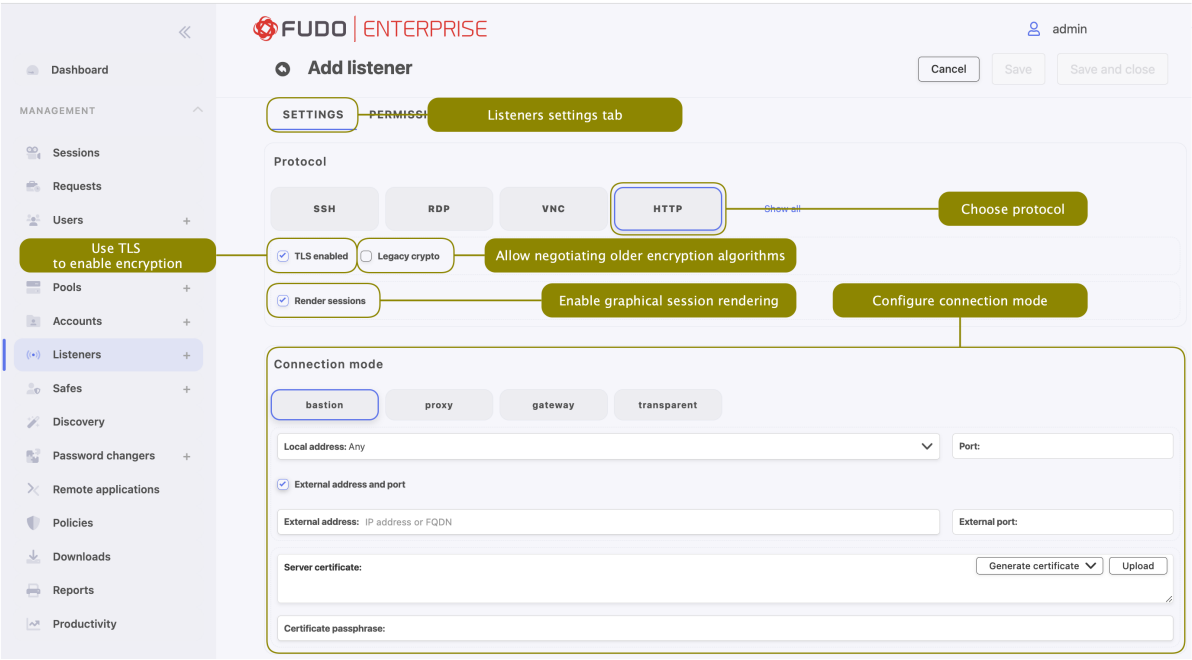
Related topics:

- *Data model*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*

10.4.1.4 Setting up the HTTP Listener

This section describes how to setup HTTP listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *Settings* tab and press the `HTTP` button in the *Protocol* field.
2. Select the *TLS enabled* option to enable encryption.
3. In case the *TLS enabled* option is chosen, select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing RDP connections.
4. Select `Render sessions` to enable graphical session rendering.



Warning

HTTP rendering is a CPU intensive process and may have negative impact on system's performance. A physical appliance is recommended for monitoring rendered HTTP connections with the following limitations regarding the maximum number of concurrent rendered HTTP sessions.

Model	Maximum recommended number of concurrent HTTP sessions*
F100x	2
F300x	5
F500x	10

* The actual value depends on the Fudo Enterprise instance configuration.

Note

- During rendered HTTP sessions raw protocol data is not recorded.
- *Render sessions* option must be enabled to activate authentication in the HTTP servers (refer to the *Creating an HTTP Server* topic).
- To understand the difference between rendered and raw HTTP sessions, please refer to the *Viewing Sessions* topic.

5. In the *Connection mode* section, select desired connection mode.

   Mode: bastion

   - Select `bastion` button in the *Connection mode* field.
   - Select the IP address from the *Local address* drop-down list and enter port number.

   Note

   - Bastion mode is supported for rendered mode only.
   - User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
   - For details on bastion connection mode, refer to *Connection modes* topic.

   - Select *External address* option to enable its field and enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

   Mode: proxy

   Note

   User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

   - Select `proxy` button in the *Connection mode* field.
   - Select the the IP address from the **Local address** drop-down list and enter port number.

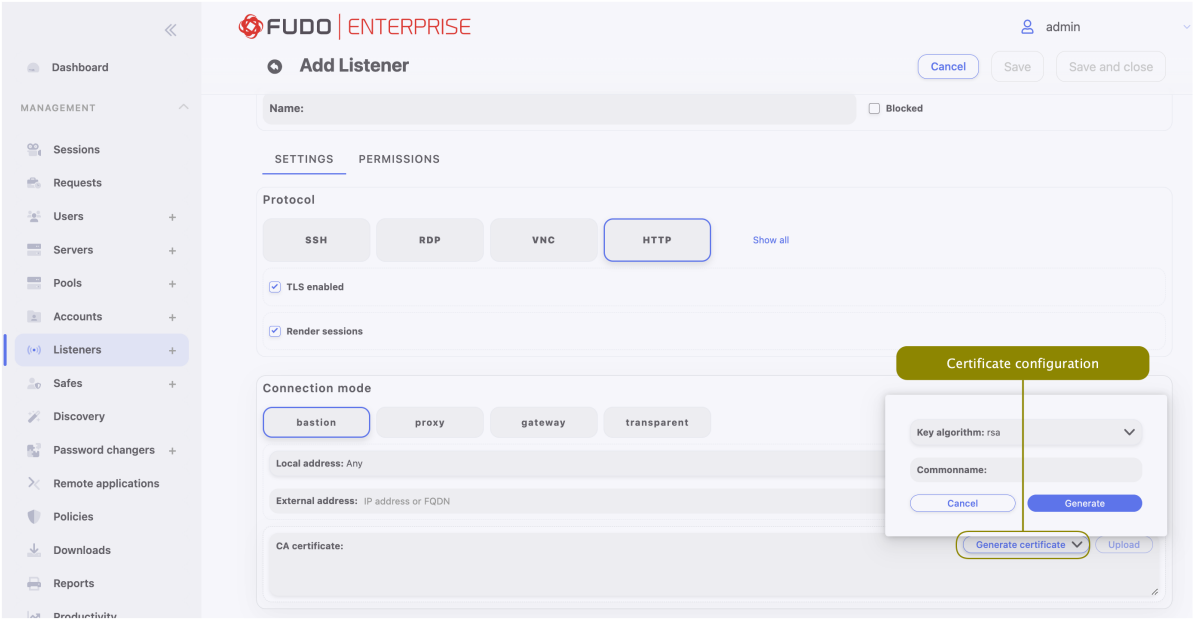
   Note

   - The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).

- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

- Select *External address* option to enable its field and enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

6. In the *Server certificate* field, click *Generate certificate* to generate TLS certificate, or click *Upload* to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.



7. Click *Save*.

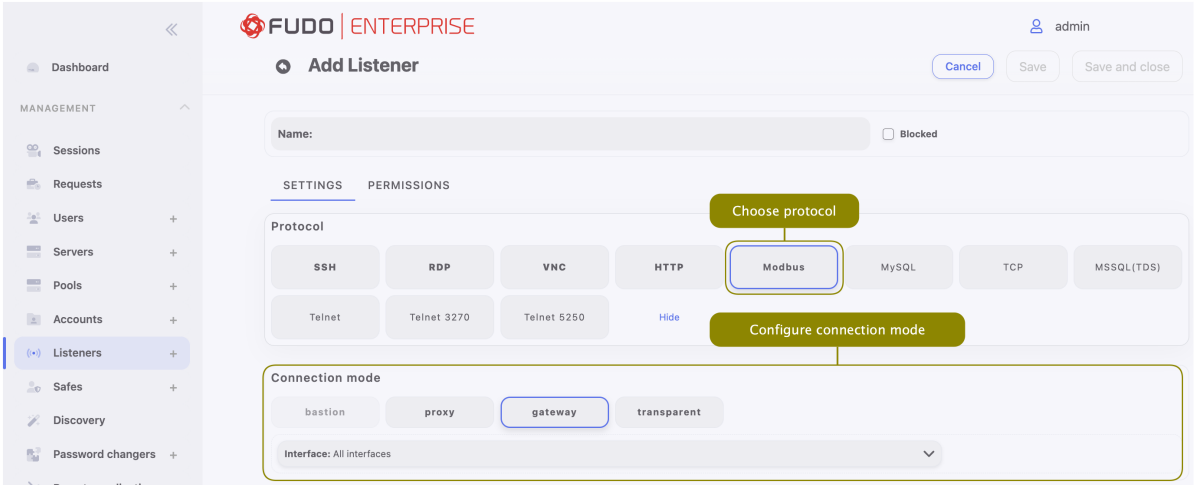
Related topics:

- *Data model*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*
- *Session examples*

10.4.1.5 Setting up the Modbus Listener

This section describes how to setup RDP listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *Settings* tab and press the *Show all* button to expand supported protocols list.
2. Press `Modbus` button in the *Protocol* field.



3. In the *Connection mode* section, select desired connection mode.

   Mode: bastion

> **Note**
>
> - User connects to the target host by including name along with account login on the target server and target server address in the login string, e.g. `john_smith#root#192.168.0.110`.
> - For details on bastion connection mode, refer to *Connection modes* topic.

   - Select `bastion` button in the *Connection mode* field.
   - Select the IP address from the **Local address** drop-down list and enter port number.

   Mode: proxy

> **Note**
>
> User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

   - Select `proxy` button in the *Connection mode* field.
   - Select the the IP address from the **Local address** drop-down list and enter port number.

Note

- The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

4. Click *Save*.

Related topics:

- *Data model*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*

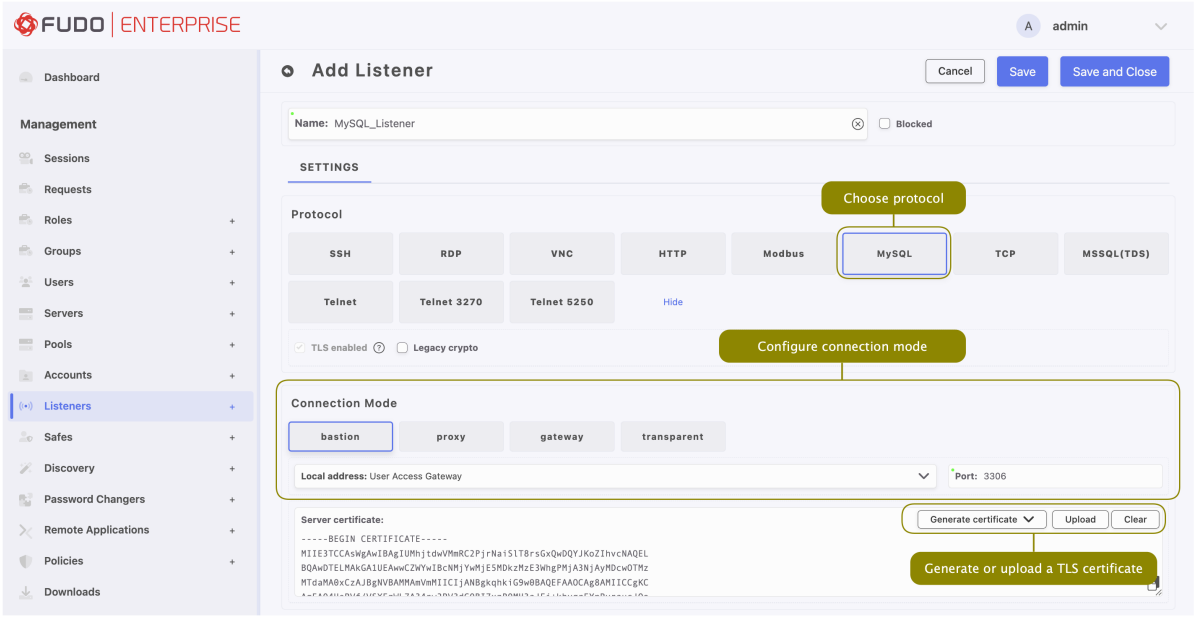
10.4.1.6 Setting up the MySQL Listener

This section describes how to setup MySQL listener. To learn first steps of creating listener, please follow *Creating a listener* section.

Warning

- The following MySQL authentication plugins are supported for communication between Fudo Enterprise and the database server: `mysql_clear_password` `mysql_native_password`, `caching_sha2_password`.
- For communication between the client and Fudo Enterprise, only `mysql_clear_password` plugin is supported, which is why TLS is enforced for MySQL listeners.

1. Go to *Settings* tab, press the `Show all` button to expand supported protocols list.
2. Press `MySQL` button in the *Protocol* field.



Note

TLS is always enabled for the MySQL listener and cannot be disabled.

3. In the *Connection mode* section, select desired connection mode.

   Mode: bastion

   Note

   - User connects to the target host by including name along with account login on the target server and target server address in the login string, e.g. `john_smith#root#192.168.0.110`.
   - For details on bastion connection mode, refer to *Connection modes* topic.

   - Select `bastion` button in the *Connection mode* field.
   - Select the IP address from the **Local address** drop-down list and enter port number.

   Mode: proxy

   Note

   User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

   - Select `proxy` button in the *Connection mode* field.
   - Select the the IP address from the **Local address** drop-down list and enter port number.

Note

- The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

4. In the *Server certificate* field, click *Generate certificate* to generate TLS certificate, or click *Upload* to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.
5. Click *Save*.

Related topics:

- *Data model*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*

10.4.1.7 Setting up the Oracle Listener [BETA]

This section describes how to setup Oracle listener. To learn first steps of creating listener, please follow *Creating a listener* section.

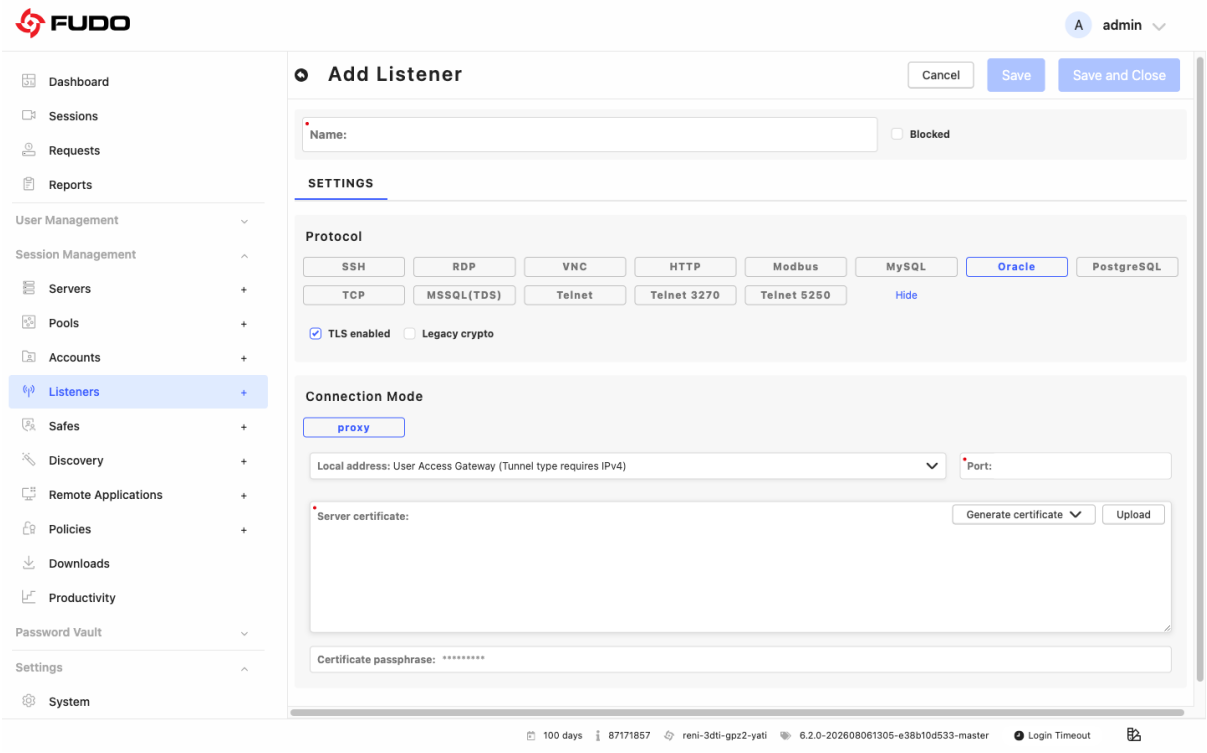
Warning

- Encrypted connections are supported with the Oracle SQL*Plus client. Other client applications do not support TLS with Fudo Enterprise, so do not enable *TLS enabled* if your users connect with a different client.
- Oracle native encryption (Advanced Security Option) is refused. Configure clients so that they do not negotiate it.

Note

The Oracle listener supports the *proxy* connection mode only. In the Bastion mode the user passes the Fudo Enterprise user name and the target server together with the login, and the Oracle protocol has no field that could carry them.

1. Go to *Settings* tab, press the `Show all` button to expand supported protocols list.
2. Press `Oracle` button in the *Protocol* field.



3. Select the *TLS enabled* option to allow clients to connect over TLS.
4. Select the *Legacy crypto* option to allow negotiating older encryption algorithms when establishing connections.

Note

The *Legacy crypto* option is shown only when *TLS enabled* is selected.

5. In the *Connection mode* section, the *proxy* mode is already selected.

   Mode: proxy

   Note

   User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

   - Select `proxy` button in the *Connection mode* field.
   - Select the the IP address from the **Local address** drop-down list and enter port number.

Note

- The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

6. If you enabled TLS, in the *Server certificate* field, click *Generate certificate* to generate TLS certificate, or click *Upload* to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.
7. Click *Save*.

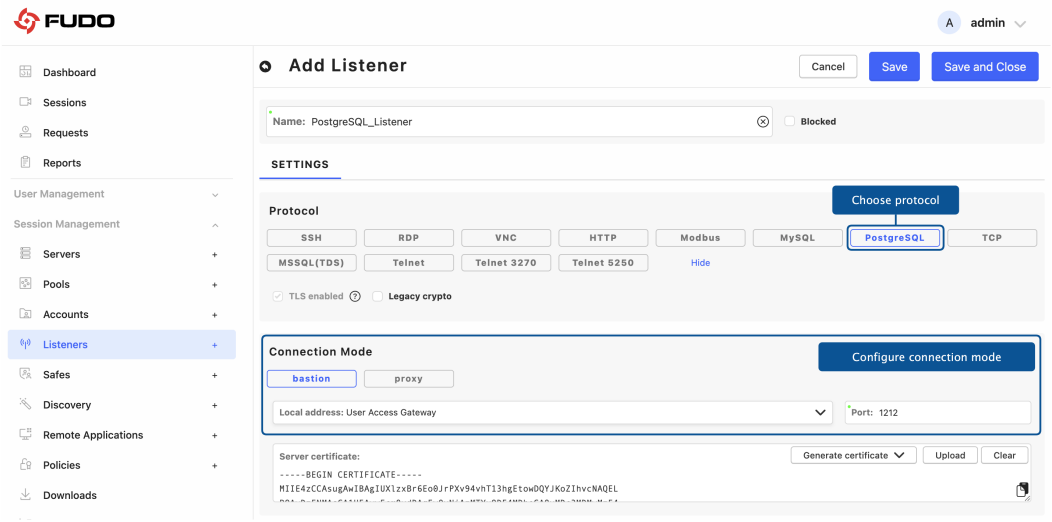
Related topics:

- *Data model*
- *Creating an Oracle Server [BETA]*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*

10.4.1.8 Setting up the PostgreSQL Listener

This section describes how to setup PostgreSQL listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *SETTINGS* tab, press the `Show all` button to expand supported protocols list.
2. Press `PostgreSQL` button in the *Protocol* field.



Note

TLS is always enabled for the PostgreSQL listener and cannot be disabled.

3. (Optional) Select the *Legacy crypto* checkbox to enable support for older encryption algorithms if your PostgreSQL clients require them.
4. In the *Connection mode* section, select desired connection mode.

Mode: bastion

Note

- User connects to the target host by including name along with account login on the target server and target server address in the login string, e.g. `john_smith#root#192.168.0.110`.
- For details on bastion connection mode, refer to *Connection modes* topic.

- Select `bastion` button in the *Connection mode* field.
- Select the IP address from the **Local address** drop-down list and enter port number.

Mode: proxy

Note

User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

- Select `proxy` button in the *Connection mode* field.
- Select the the IP address from the **Local address** drop-down list and enter port number.

Note

- The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

5. In the *Server certificate* field, click *Generate certificate* to generate TLS certificate, or click *Upload* to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.

Warning

For PostgreSQL listener, the certificate's Common Name (CN) should match the hostname that clients will use to connect. Mismatched CN may cause certificate validation errors in PostgreSQL clients.

6. Click *Save*.

Note

- After creating the PostgreSQL listener, users can connect using the native PostgreSQL client, `psql`.
- The command used to establish the connection is available to the user after logging in to the User Access Gateway. For example:

```
psql postgres:1/85156504WW4NEopiQ0vePxbIqaXiEYcT:empty@<listener_address>
↪[:port]/<database_name>
```

- The user must replace `<database_name>` with the correct database name.

Related topics:

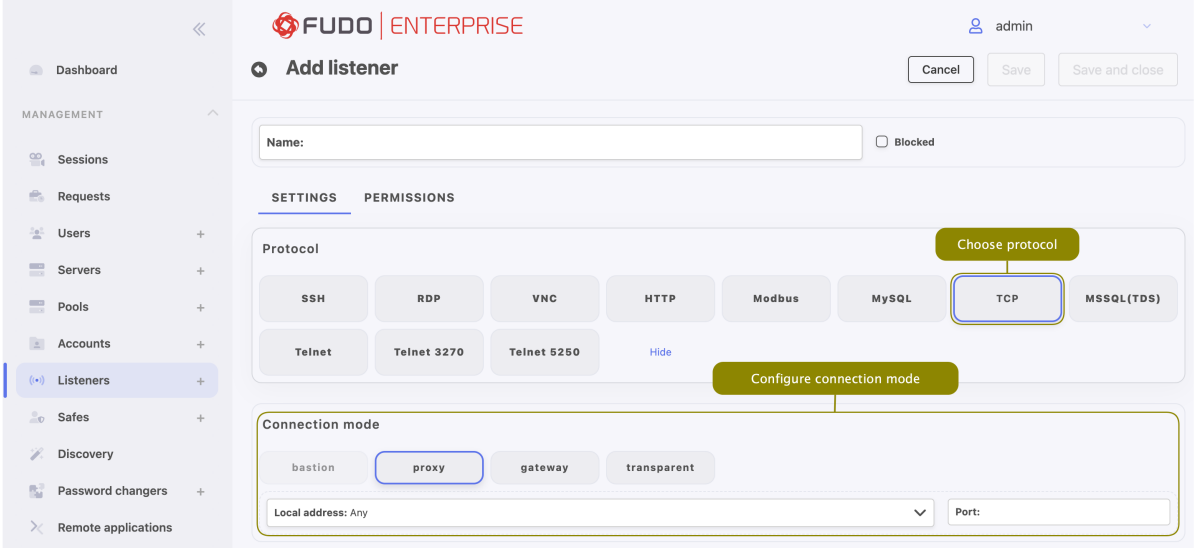
- *Data model*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*
- *Creating a PostgreSQL Server*

- *PostgreSQL*

10.4.1.9 Setting up the TCP Listener

This section describes how to setup TCP listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *Settings* tab, press the *Show all* button to expand supported protocols list.
2. Press `TCP` button in the *Protocol* field.



3. In the *Connection mode* section, select desired connection mode.

   Mode: proxy

> **Note**
>
> User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

- Select `proxy` button in the *Connection mode* field.
- Select the the IP address from the **Local address** drop-down list and enter port number.

> **Note**
>
> - The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
> - Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
> - When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access

Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.

- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

4. Click *Save*.

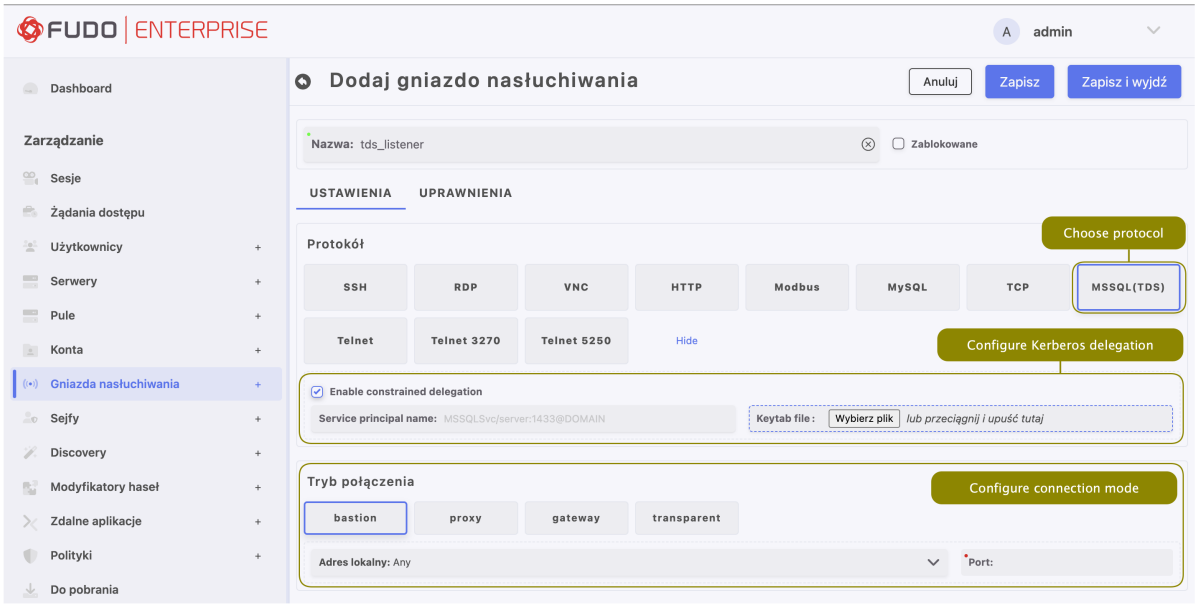
Related topics:

- *TCP*
- *Creating a TCP Server*
- *Data Model*

10.4.1.10 Setting up the MS SQL Listener

This section describes how to setup MS SQL listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *Settings* tab, press the *Show all* button to expand supported protocols list.
2. Press `MS SQL(TDS)` button in the *Protocol* field.
3. If you want to configure the *Kerberos constrained delegation*:
   - Select Enable constrained delegation option.
   - In the *Service principal name* field, enter the name using the following format (e.g., `MSSQLSvc/mgmt.qa.fudo:1433@QA.FUDO`).
   - Upload Keytab file generated for the constrained delegation purpose.



4. In the *Connection mode* section, select desired connection mode.

Mode: bastion

Note

- User connects to the target host by including name along with account login on the target server and target server address in the login string, e.g. `john_smith#root#192.168.0.110`.
- For details on bastion connection mode, refer to *Connection modes* topic.

- Select `bastion` button in the *Connection mode* field.
- Select the IP address from the **Local address** drop-down list and enter port number.

Mode: proxy

Note

User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

- Select `proxy` button in the *Connection mode* field.
- Select the the IP address from the **Local address** drop-down list and enter port number.

Note

- The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

5. Click *Save*.

Related topics:

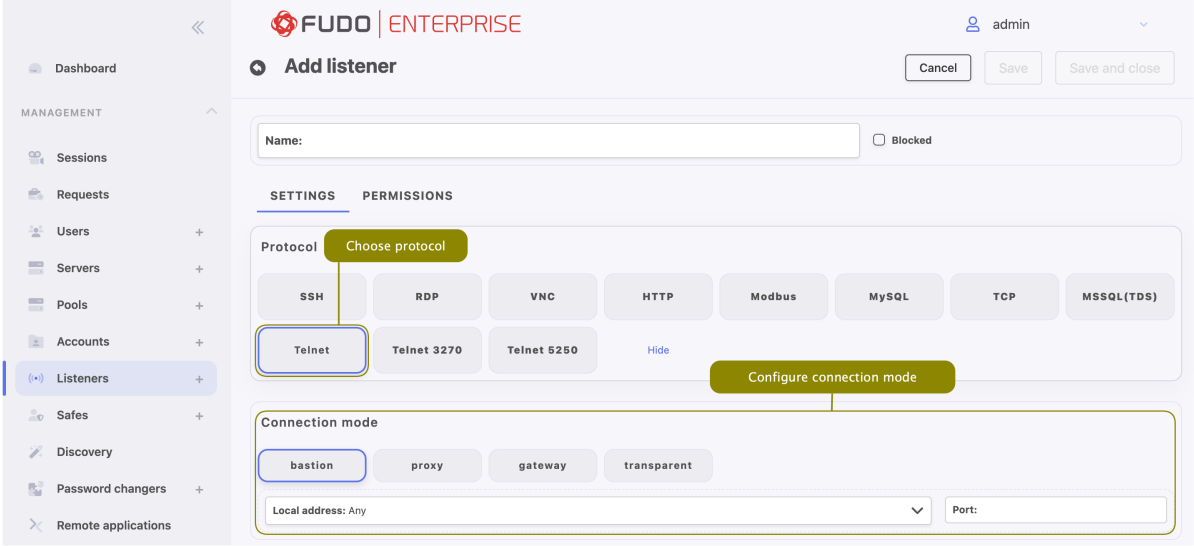
- *Data model*
- *Editing a Listener*
- *Deleting a Listener*

- *Blocking a Listener*
- *Unblocking a Listener*

10.4.1.11 Setting up the Telnet Listener

This section describes how to setup Telnet listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *Settings* tab, press the *Show all* button to expand supported protocols list.
2. Press `Telnet` button in the *Protocol* field.



3. In the *Connection mode* section, select desired connection mode.

   Mode: bastion

> **Note**
>
> - User connects to the target host by including name along with account login on the target server and target server address in the login string, e.g. `john_smith#root#192.168.0.110`.
> - For details on bastion connection mode, refer to *Connection modes* topic.

   - Select `bastion` button in the *Connection mode* field.
   - Select the IP address from the **Local address** drop-down list and enter port number.

   Mode: proxy

> **Note**
>
> User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

- Select `proxy` button in the *Connection mode* field.
- Select the the IP address from the **Local address** drop-down list and enter port number.

> **Note**
>
> - The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
> - Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
> - When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
> - In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

4. Click *Save*.

Related topics:

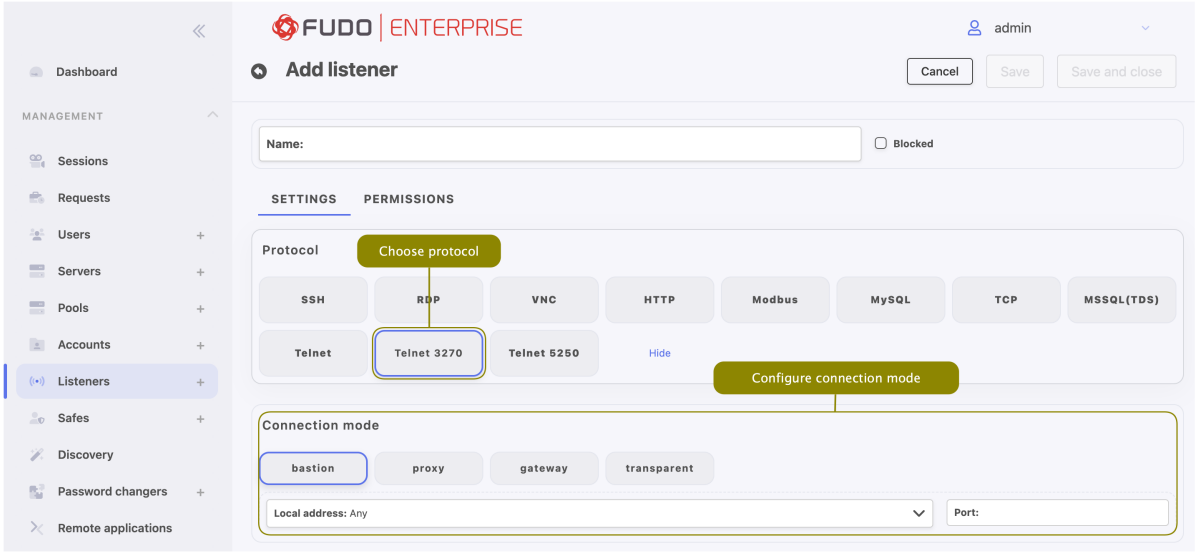
- *Data model*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*

10.4.1.12 Setting up the Telnet 3270 Listener

> **Under review**
>
> Support for the **Telnet 3270** protocol is **under review** and may be removed in a future release. If this protocol is critical to your environment, please contact Fudo Support for more information.

This section describes how to setup Telnet 3270 listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *Settings* tab, press the *Show all* button to expand supported protocols list.
2. Press `Telnet 3270` button in the *Protocol* field.



3. In the *Connection mode* section, select desired connection mode.

   Mode: bastion

   Note

   - User connects to the target host by including name along with account login on the target server and target server address in the login string, e.g. `john_smith#root#192.168.0.110`.
   - For details on bastion connection mode, refer to *Connection modes* topic.

   - Select `bastion` button in the *Connection mode* field.
   - Select the IP address from the **Local address** drop-down list and enter port number.

   Mode: proxy

   Note

   User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

   - Select `proxy` button in the *Connection mode* field.
   - Select the the IP address from the **Local address** drop-down list and enter port number.

   Note

   - The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
   - Selecting the `Any` option will result in Fudo listening on all configured IP addresses.

- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

4. Click *Save*.

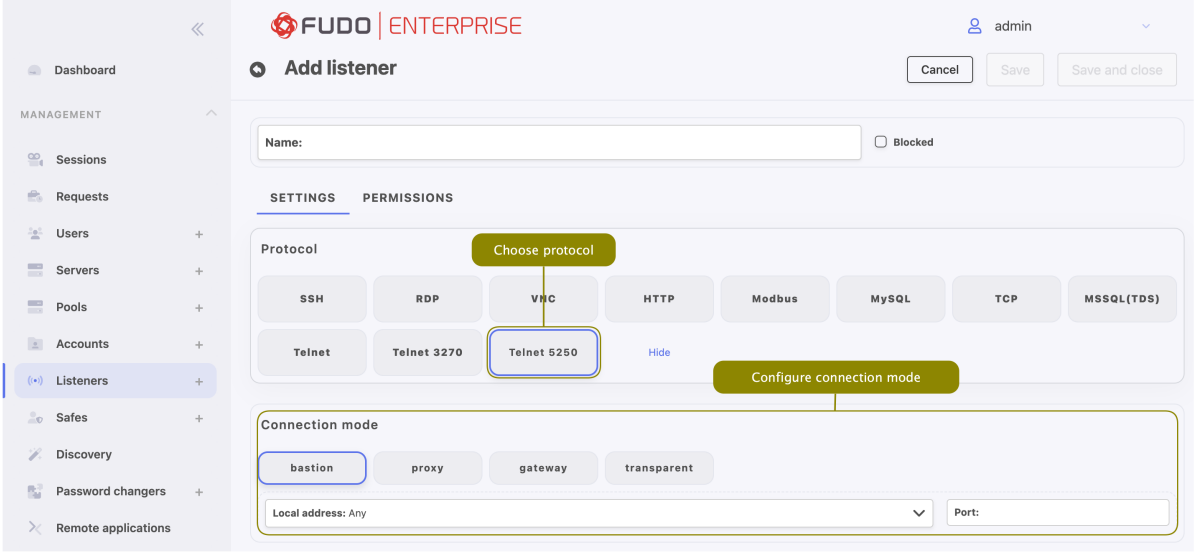
Related topics:

- *Data model*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*

10.4.1.13 Setting up the Telnet 5250 Listener

This section describes how to setup Telnet 5250 listener. To learn first steps of creating listener, please follow *Creating a listener* section.

1. Go to *Settings* tab, press the *Show all* button to expand supported protocols list.
2. Press `Telnet 5250` button in the *Protocol* field.



3. In the *Connection mode* section, select desired connection mode.

   Mode: bastion

Note

- User connects to the target host by including name along with account login on the target server and target server address in the login string, e.g. `john_smith#root#192.168.0.110`.
- For details on bastion connection mode, refer to *Connection modes* topic.

- Select `bastion` button in the *Connection mode* field.
- Select the IP address from the **Local address** drop-down list and enter port number.

Mode: proxy

Note

User connects to the target host by providing Fudo Enterprise IP address and port number which unambiguously identifies target host.

- Select `proxy` button in the *Connection mode* field.
- Select the the IP address from the **Local address** drop-down list and enter port number.

Note

- The **Local address** drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- When a Listener is configured with *User Access Gateway* as the local address, only one connection option is displayed after login to User Access Gateway for clarity, and the connection uses the address from the browser's address bar together with the listener's configured port.
- In case of cluster configuration, select a labeled IP address from the **Local address** drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

4. Click *Save*.

Related topics:

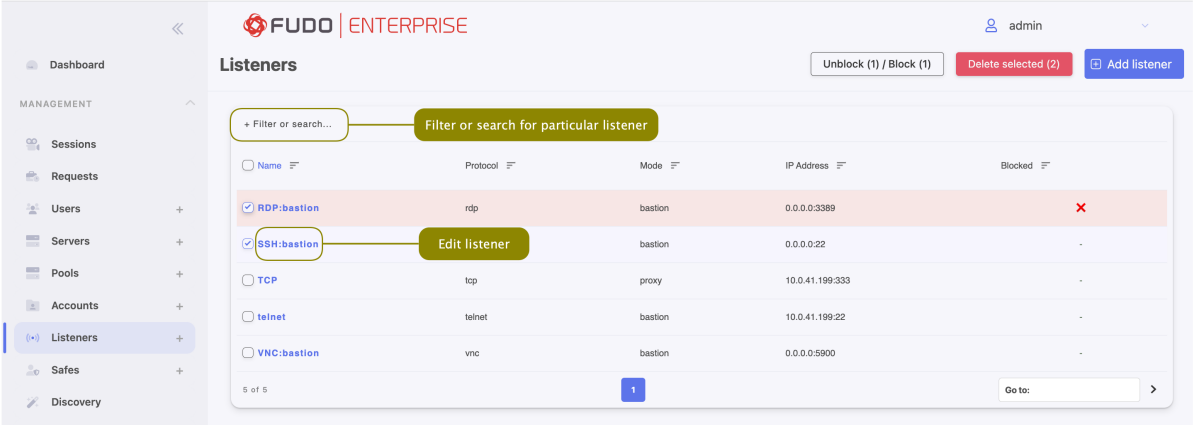
- *Data model*
- *Editing a Listener*
- *Deleting a Listener*
- *Blocking a Listener*
- *Unblocking a Listener*

Note

Starting from release 5.6, the **configuration of listeners for the User Access Gateway** has been **enhanced.** When **User Access Gateway** is selected as the **local address**, only one connection option will be displayed after logging in to the User Access Gateway for clarity. The connection will then use the address from the browser's address bar together with the listener's configured port.

10.4.2 Editing a Listener

1. Select *Management* > *Listeners*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Find and click on a name of the desired listener to access its configuration parameters.
4. Modify configuration values as needed.
5. Click *Save*.

Related topics:

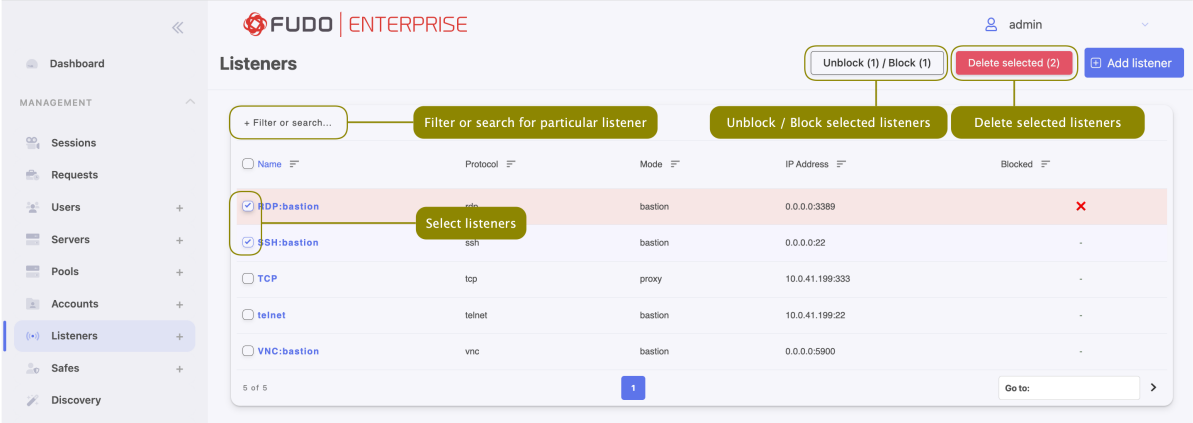
- *Data model*
- *System initiation*
- *Servers*

10.4.3 Blocking a Listener

Warning

Blocking a listener will terminate current connections with server which uses it.

1. Select *Management* > *Listeners*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Select one or more listeners to block by checking the box next to listener's name.
4. Click *Unblock / Block* button to disable access to hosts over selected listeners.
5. Provide descriptive reason for blocking given resource (required) and click *Block* in displayed dialog box.

Note

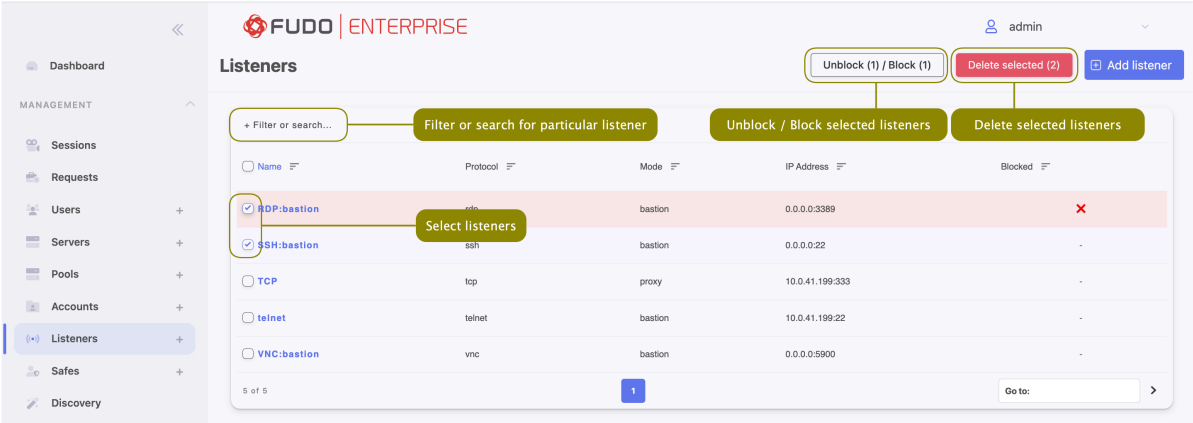
To view the blocking reason, place the cursor over the red cross icon on the listeners list.

Related topics:

- *Data model*
- *System initiation*
- *Servers*

10.4.4 Unblocking a Listener

1. Select *Management* > *Listeners*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Select one or more listeners to unblock by checking the box next to listener's name.
4. Click *Unblock / Block* button to enable access to hosts over selected listeners.
5. Click *Unblock* button in displayed dialog box to confirm unblocking selected objects.

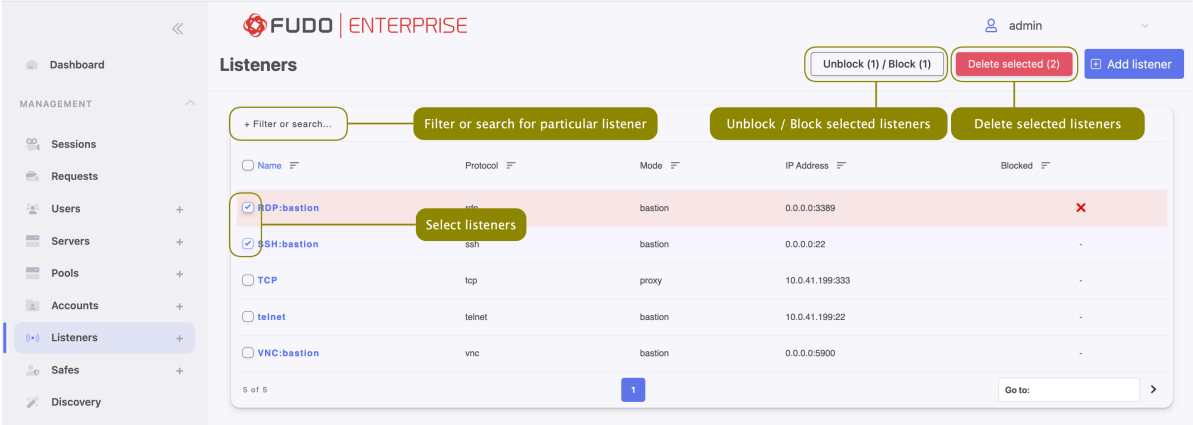
Related topics:

- *Data model*
- *System initiation*
- *Servers*

10.4.5 Deleting a Listener

> **Warning**
>
> Deleting a listener will terminate current connections with server which uses it.

1. Select *Management* > *Listeners*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



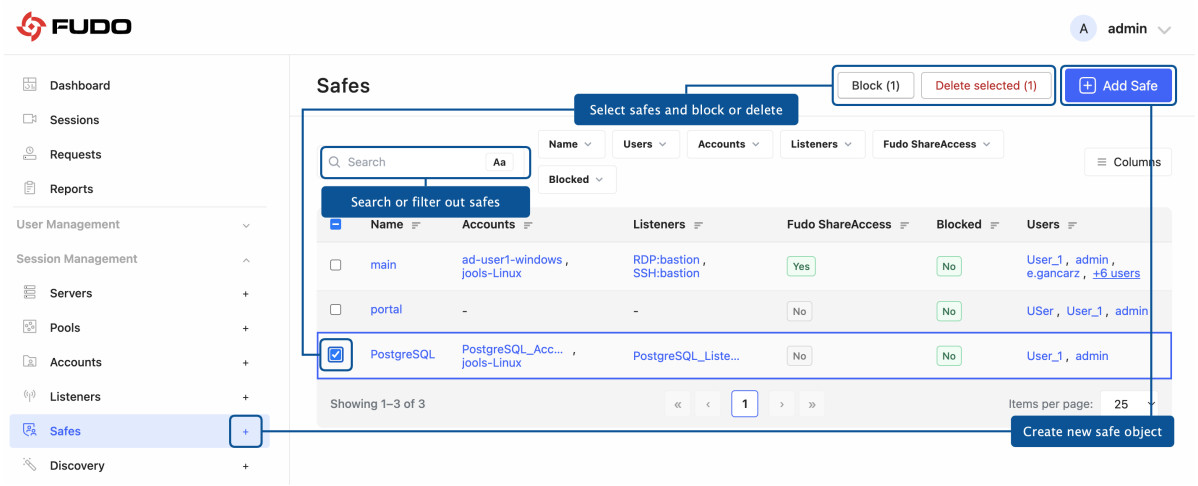
3. Select one or more listeners to delete by checking the box next to listener's name.
4. Click *Delete selected*.
5. Confirm deleting selected objects by choosing *Confirm* button in displayed dialog box.

Related topics:

- *Data model*
- *System initiation*
- *Servers*

10.5 Safes

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

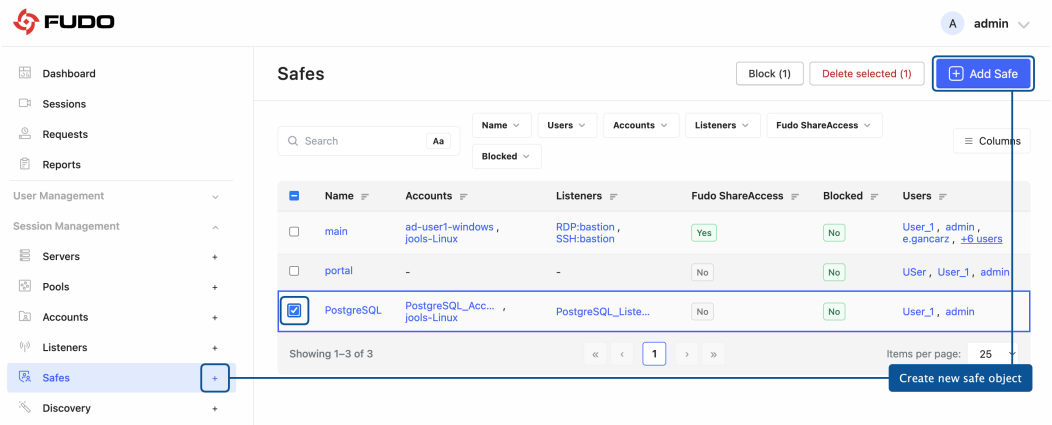


10.5.1 Creating a Safe

Warning

Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances **must not** be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

1. Click + icon in the main menu next to the *Safes* tab of the *Session Management* subsection, or
2. Select *Session Management* > *Safes* and then click + *Add safe*.



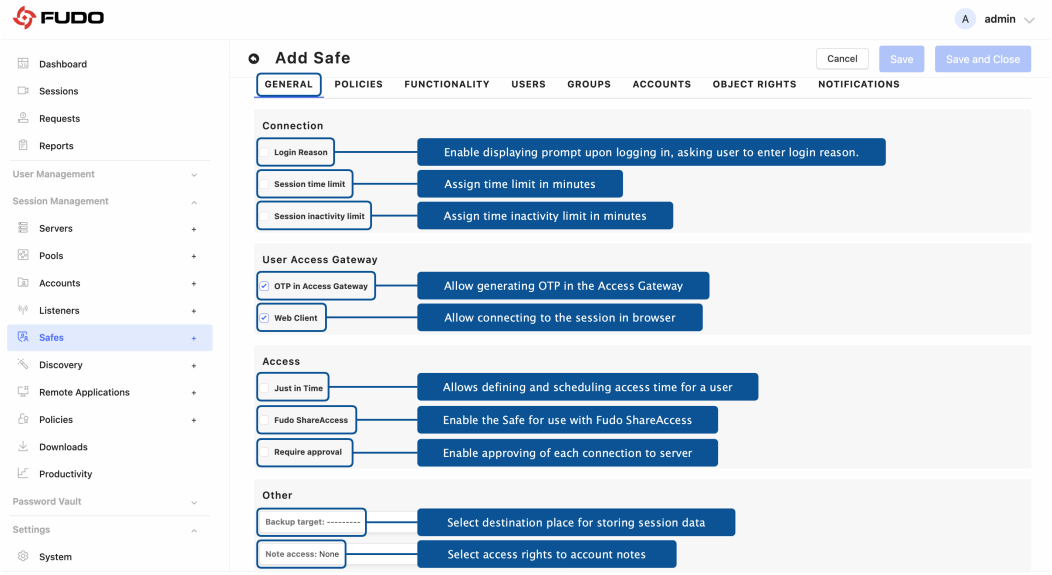
3. Enter object's name.
4. Select *Blocked* option if you want to disable access to object after it's created.
5. Click *Save* to save the object and proceed with further configuration.

GENERAL TAB

1. In the *GENERAL* tab, in the *Connection* field, select *Login reason* option, to display prompt upon logging in, asking user to enter login reason.

Note

Login reason is not supported in *HTTP* connections.

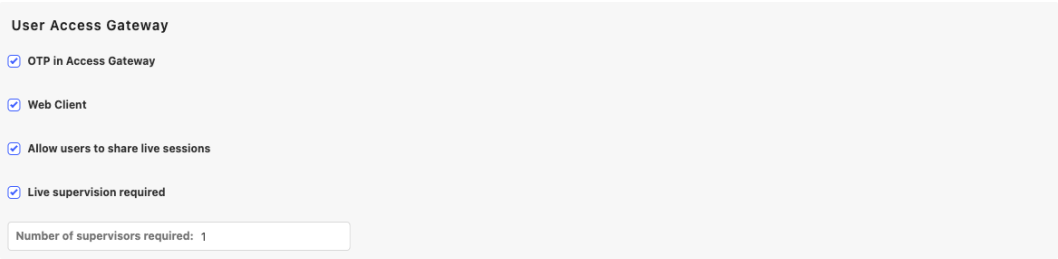


2. Select *Session time limit* option and enter a value in minutes after which the session will be terminated.
3. Select the *Session inactivity* limit option and enter the number of minutes of inactivity after which the session will be terminated.
4. The *OTP in Access Gateway* option is enabled by default and is responsible for generating OTP in the User Access Gateway.

Warning

Disabling the *OTP in Access Gateway* option makes it impossible to connect via the Native Client through the User Access Gateway. Access via the *Access Requests* would be possible only.

5. For RDP, VNC and SSH-based safes, select *Web Client* option to allow connecting to the session using the built-in browser client.
6. Select *Allow users to share live sessions* option to let users share their own running sessions directly from the User Access Gateway, without involving an administrator. Links created this way always require the recipient to sign in and expire when the session ends. For more information, refer to the *Sharing Sessions* section.



With this option enabled, you can additionally select *Live supervision required* and provide the *Number of supervisors required*, so that sessions established through this safe are watched by the given number of signed-in supervisors invited with a share link.

7. Select *Just in Time* option and provide a number of the voters (at least `1`). This feature allows defining and scheduling the time when a user is allowed to access specific resources for a set period of time. The user sends requests via the Access Gateway, and the voters accept or reject them on in the Admin Panel. Read more about the Just-in-Time feature in a *Access Requests* section.

   Optionally, select the *Skip approval during Daily Access Policy hours* sub-option to make the approval requirement time-based: inside the time windows defined by the user's daily access policy the user connects directly, and outside them an approved access request is required. For details, refer to the *Time-Based Access Requests* section.

8. Select *Require approval* option to have the administrator approve each connection to servers accessed through configured safe. Provide how many minutes the administrator has to approve or reject a request.

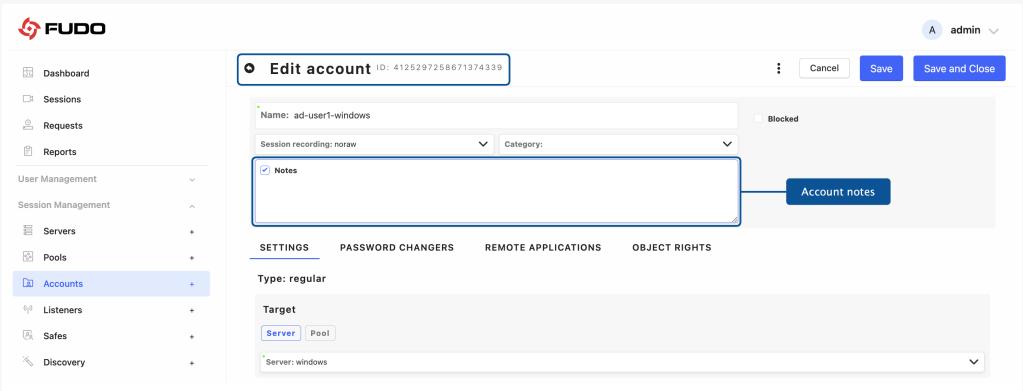
9. Select *Block concurrent sessions through other safes* to prevent users from having simultaneous sessions through this safe and any other safe. For details, refer to *Blocking Concurrent Sessions Through Other Safes*.

10. In the *Other* field, select a *Backup target* as a destination place for storing data. To create a backup target, please refer to the *Backup and Retention* section.

11. From the *Note access* drop-down list, select access rights to account related notes: `read`, `write` or `none`.

Note

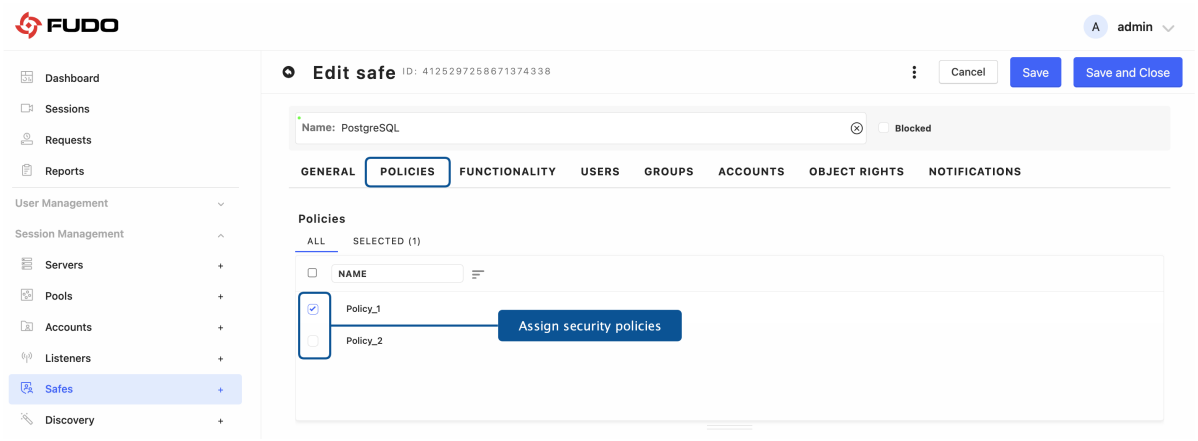
Notes can be accessed either from the account edit form



or in the *User Access Gateway*.

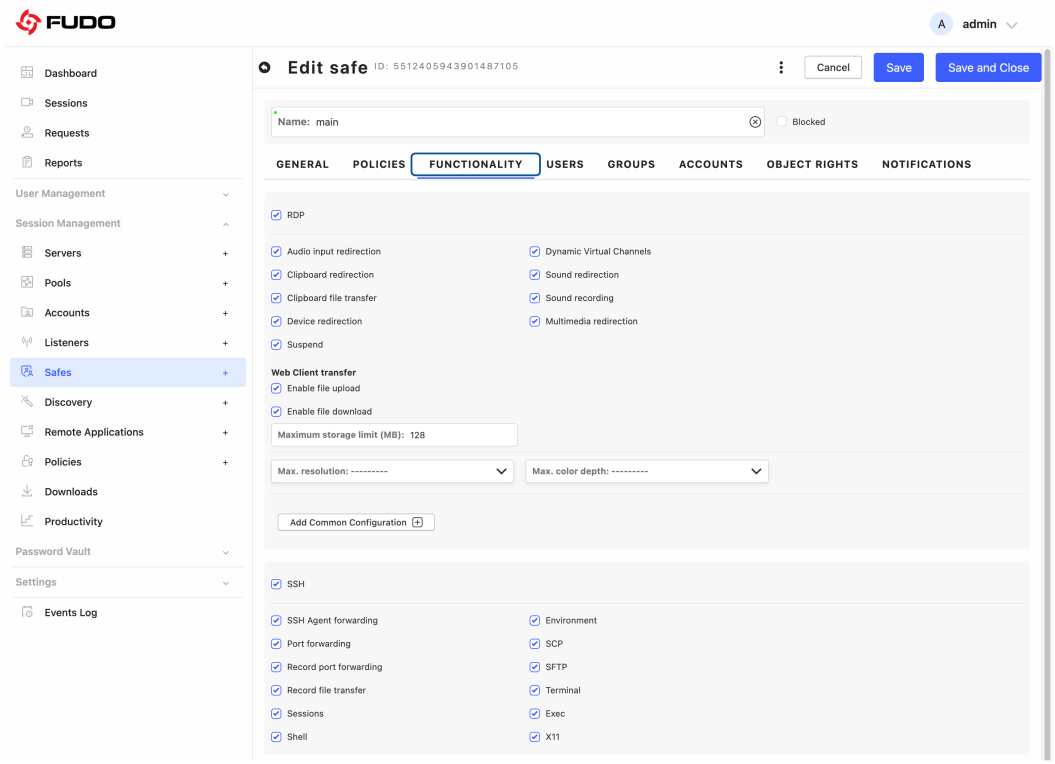
POLICIES TAB

Go to the *POLICIES* tab, and assign desired *security policies* by selecting checkboxes in front of the policies names.



FUNCTIONALITY TAB

Go to the *FUNCTIONALITY* tab, and select allowed protocols' features.



Note

Protocol functionality options overview:

- RDP
  - **Audio Input Redirection** - Redirects audio input from the client device to the remote desktop, allowing voice input applications to function.
  - **Dynamic Virtual Channels** - Enables support for the feature of multiple virtual channels over a single RDP session. DVC is directly related with GFX driver support. Turn off this option to disable GFX support if you experience performance issues. Disabling this option is also required to restore xrdp compatibility.
  - **Clipboard Redirection** - Shares clipboard contents between the client and remote desktop, enabling copy-paste functionality.
  - **Clipboard File Transfer** - Allows files to be copied through the clipboard. Clearing this option blocks copying files while ordinary copying and pasting of text remains available. The option is selected by default and requires *Clipboard Redirection* to be enabled.
  - **Sound Redirection** - Redirects audio output from the remote desktop to the client device.
  - **Sound Recording** - Saves the sound of the session in the recording. This option is independent of *Sound Redirection*: with *Sound Recording* cleared and *Sound Redirection* selected, the user still hears the sound of the remote desktop, but nothing is saved in the recording. The option is selected by default and works only on listeners using the new RDP implementation (refer to *Selecting the RDP implementation*).

  - **Device Redirection** - Allows peripherals (e.g., printers, USB devices, smart cards) connected to the client device to be used within the remote desktop session. In RDP Web Client sessions, this option is also required for **file upload and download**, which is configured in the **Web Client transfer** section below.
  - **Web Client transfer** - Available only when **Device Redirection** is selected. Controls file transfer in RDP Web Client sessions through the shared session drive; native RDP clients are not affected.
    * **Enable file upload** - Allows users to upload files from their local device to the session.
    * **Enable file download** - Allows users to download files from the session to their local device.
    * **Maximum storage limit (MB)** - Sets the space available on the shared session drive for uploaded and downloaded files combined.
  - **Multimedia Redirection** - Improves multimedia playback by offloading the decoding process to the client device for smoother video and audio.
  - **Suspend** - Pauses and saves the current session, allowing it to be resumed later without restarting. With the *Suspend* option enabled, the session content will not be available for viewing when the user minimizes the client application.
  - **Max. Resolution** - Sets the maximum resolution for the remote desktop session, affecting display quality and bandwidth usage.
  - **Max. Color Depth** - Sets the maximum color depth for the remote desktop session, affecting visual quality and bandwidth usage. **Caution:** Older Windows systems require a color depth lower than 32 bpp, whereas newer versions need 32 bpp. To ensure compatibility, you can assign servers with older Windows versions to separate safes and configure a lower color depth for them while maintaining a 32 bpp limit for newer systems.
  - **Native client .rdp file** - Settings of the .rdp file that the User Access Gateway generates for the *Native client* option:
    * **Common configuration** - Allows custom content to be added to the RDP configuration file. For example, to share the `/tmp` directory, the following line can be included in the generated .rdp file: `drivestoredirect:s:/tmp`.
    * **Sign .rdp files** - Selected by default, also for safes created before the upgrade. Signs the generated .rdp file with the server certificate of the RDP listener, so that the Remote Desktop client can verify its publisher. Clear the option to serve unsigned files for this safe. For the certificate requirements, refer to the *RDP listener* topic.
- SSH*
  - **SSH Agent Forwarding** - Enables the User to utilize the SSH Agent Forwarding option during authentication.
  - **Environment** - Disabling this option will prevent the passing of environment variables to the server using `-o SendEnv=`. This option does not block the use of environment variables on the destination server.

  - **Port Forwarding** - Enables redirecting network traffic from one port to another, allowing secure connections to services behind firewalls or NAT.
  - **Record port forwarding** - Enabled by default. Fudo records the nested sessions created by SSH port forwarding (tunnelled connections). Disable this option to stop recording port-forwarding subsessions and reduce the system load caused by creating database entries and file directories for them. The master SSH session is still recorded.
  - **Record file transfer** - Enabled by default. Fudo records SCP and SFTP file transfers performed within an SSH session as nested sessions. Disable this option to stop recording file-transfer subsessions and reduce the system load. The master SSH session is still recorded.
  - **SCP (Secure Copy Protocol)** - Enables secure file transfer between local and remote systems using SSH.
  - **Sessions** - Disabling this option will prevent the initiation of interactive sessions and the execution of remote commands. Nevertheless, certain options, such as port forwarding, will remain available.
  - **SFTP (Secure File Transfer Protocol)** - Enables secure file transfer and management over SSH.
  - **Shell** - Disabling this option will prevent the initiation of interactive sessions. However, it will still be possible to execute remote commands and forward ports.
  - **Terminal** - Enables *pseudo-terminal* functionality.
  - **X11** - Enables support for X11 protocol.
  - **Exec** - Enables executing a single command on the remote server without starting an interactive shell session.

- VNC
  - **Client Cut Text** - User is allowed to paste text into the VNC server computer.
  - **Server Cut Text** - User is allowed to copy and paste text from the VNC server computer into the user's computer.

- Rendered HTTP
  - **Kiosk browser** - Runs the rendered HTTP session in a controlled browser with optional URL navigation and a configurable tab limit.
  - **Full browser access** - Provides a full browser experience: a multi-tab browser with back/forward navigation and an address bar. This option does not grant access to Chrome developer tools, settings, or other restricted browser tools.
  - **Address bar** - For **Kiosk browser**, sets how the URL bar is presented: *Hidden*, *Read-only*, or *Editable*.
  - **Limit number of tabs** - For **Kiosk browser**, limits the number of open tabs. When the limit is reached, the user is notified and can choose whether to open the requested link in the current tab. The maximum is set with **Maximum tabs**.
  - **Convert popups to tabs** - For **Full browser access**, opens pop-up windows as new browser tabs. Selected by default. When the option is cleared, pop-up

windows may open outside the browser view and cover the session content.

- Data transfer
  - **Enable file upload** - Allows users to upload files from their local device to the rendered HTTP session.
  - **Enable file download** - Allows users to download files from the rendered HTTP session to their local device.
  - **Total file storage quota (MB)** - Sets the maximum storage space available for files uploaded and downloaded during rendered HTTP sessions. Required when file upload or file download is enabled. The default value is 500 MB, the minimum is 1 MB, and there is no upper limit.

*For detailed information about SSH functionalities please refer to *RFC 4254 - The Secure Shell (SSH) Connection Protocol.*

Note

The VNC protocol supports only clipboard text transfer through the **Client Cut Text** and **Server Cut Text** options. File copying and file transfer are not supported over VNC.

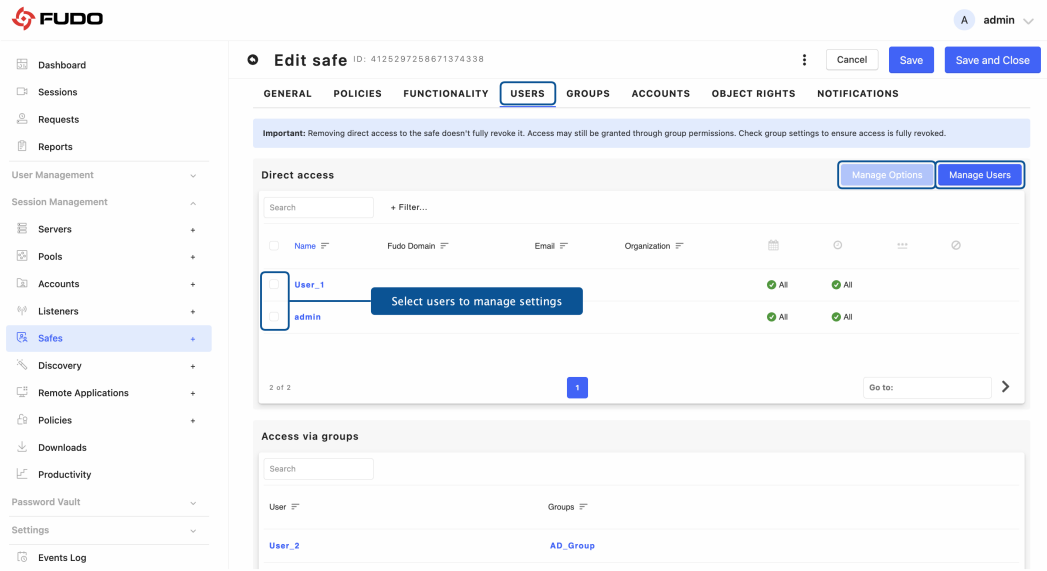
Note

Files transferred in rendered HTTP sessions can be scanned by an antivirus engine. Scanning is not enabled in the safe form but in *Settings* > *System* > *File scanning* - see *File Scanning in Rendered HTTP Sessions*.

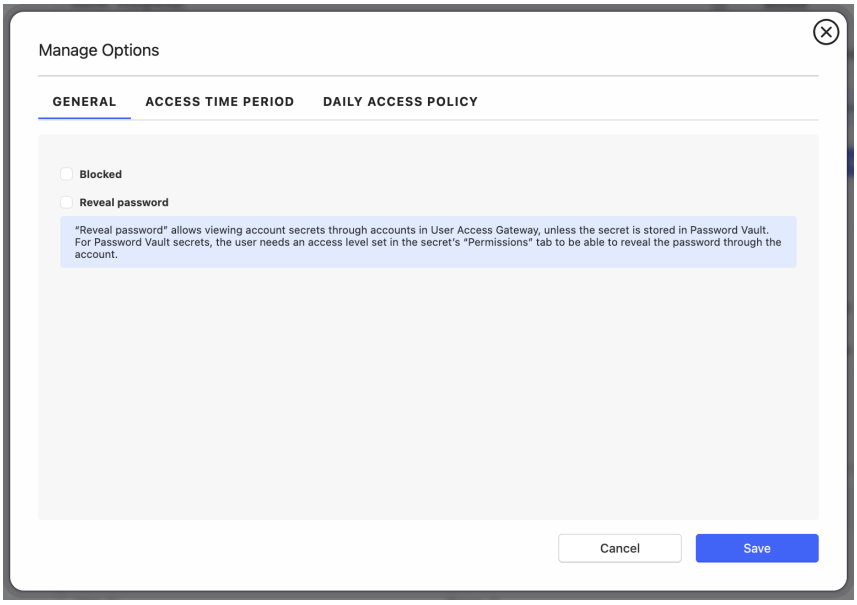
USERS TAB

Go to the *USERS* tab to assign users allowed to access accounts assigned to this safe.

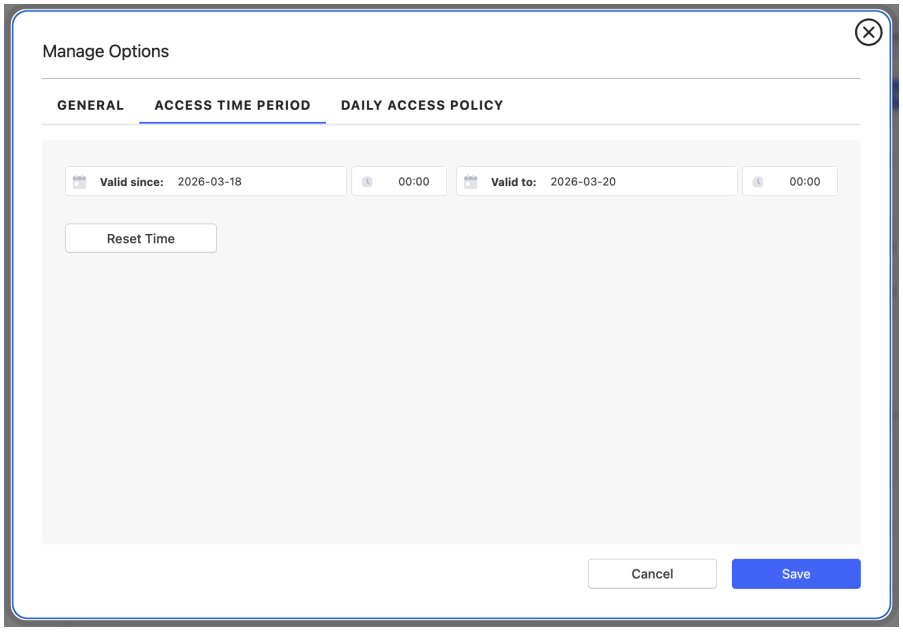
1. Click *Manage Users*.
2. Mark the checkbox in front of the users' names to enable their server access through the monitored safe.



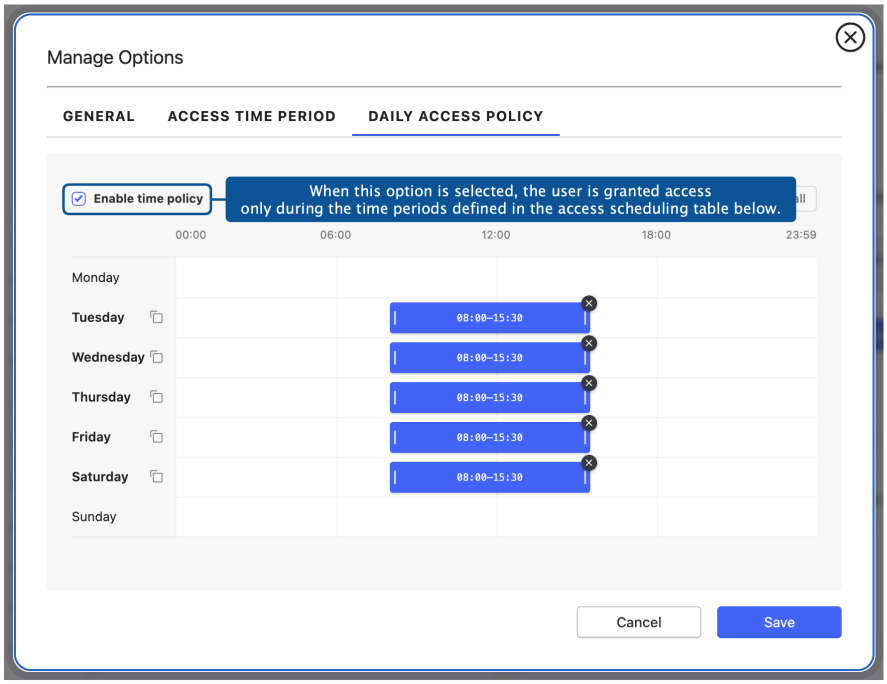
3. Click *Save* to close the modal window.
4. To define safe access options for a user, select the checkbox in front of the desired users' names and click *Manage options*.
    - Go to *General* tab and select *Blocked* option if you want to block the users selected in previous step.
    - Select *Reveal password* to allow selected users to use Secret Checkout feature and view passwords in the User Access Gateway.

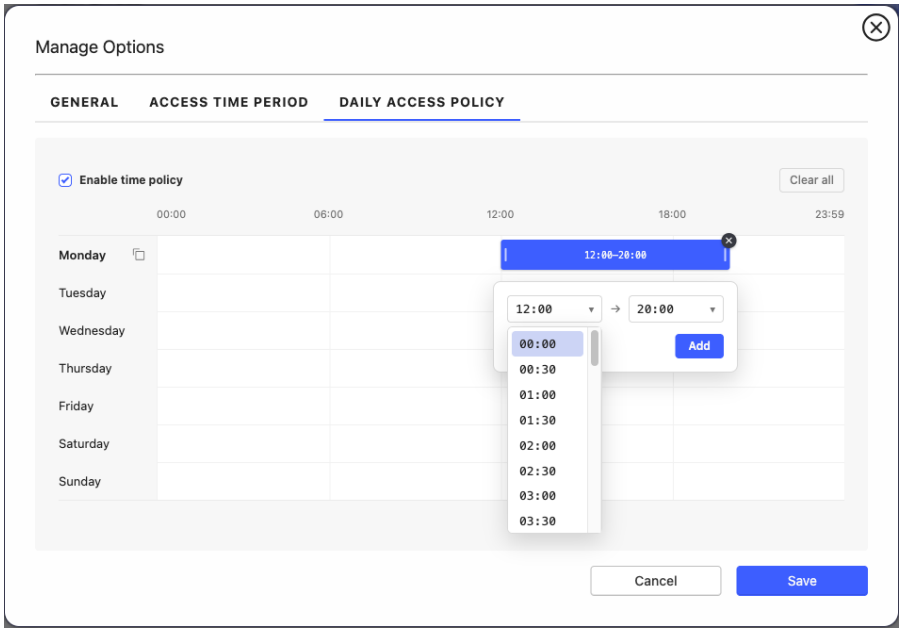


    - Select *ACCESS TIME PERIOD* tab to fill out the *Valid since* and *Valid to* fields with date and time interval when user will be allowed to access servers through the given safe. When defined date and time comes, access to the given safe is granted to the user automatically.



- Select *DAILY ACCESS POLICY* tab to define time intervals during which the user will be allowed to connect to servers. Click the row of the chosen day of the week to add an access window, or drag across the row to draw one; dragging vertically covers several days at once. Windows snap to a 30-minute grid and can be moved or resized by their edges; touching or overlapping windows are merged automatically. Click a window to set exact start and end times, use the copy icon next to a day name to copy that day to all days, and use *Clear all* to remove the whole schedule.





Caution

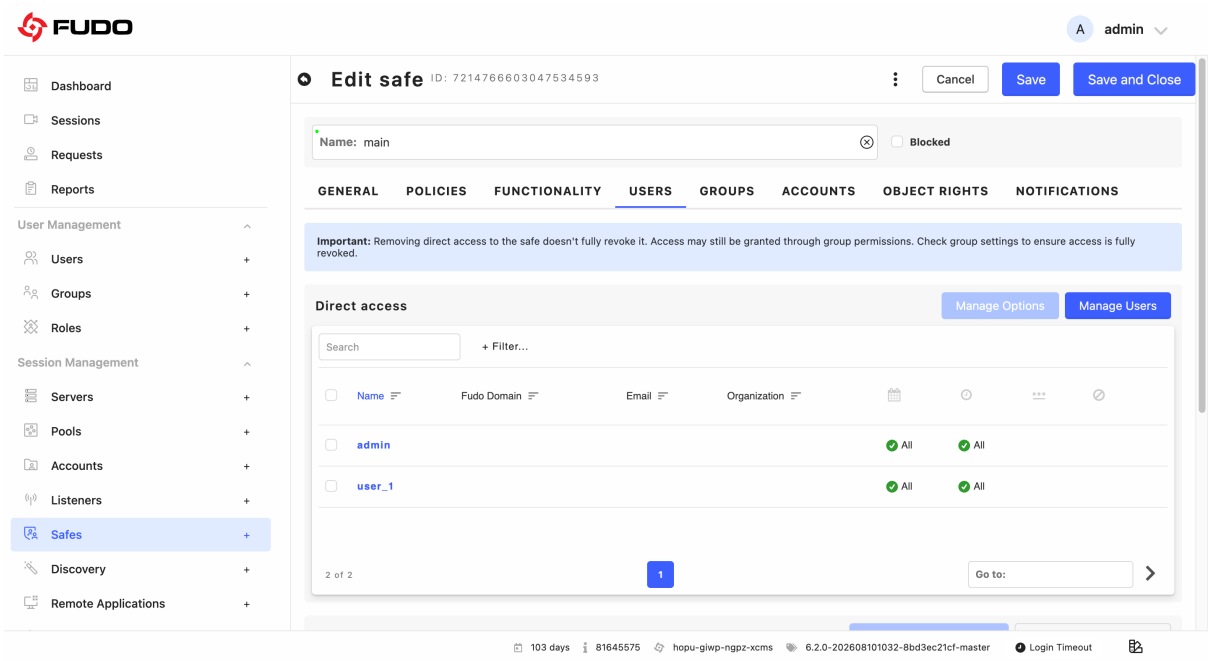
- To make the time policy active, select the *Enable time policy* checkbox above the access scheduling table.

Note

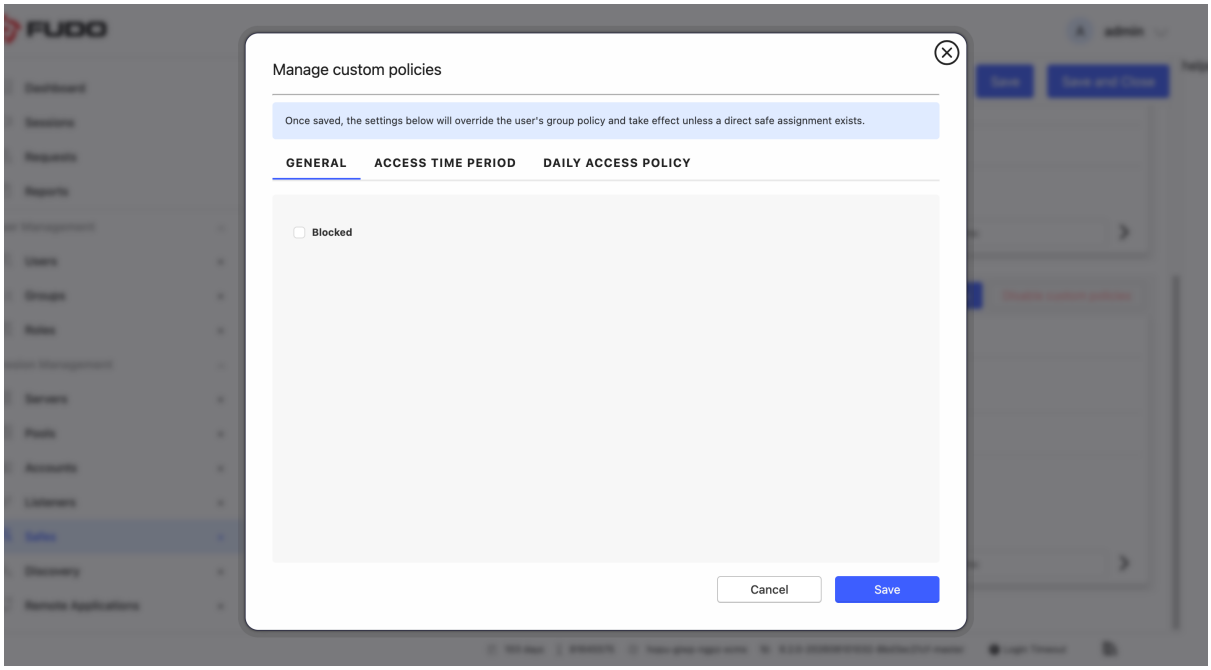
- The daily access policy defined here is always enforced. When the *Just in Time* option is enabled without the *Skip approval during Daily Access Policy hours* sub-option, every connection requires an approved access request and, outside the policy hours, access is denied even when a request has been approved. With the sub-option selected, the daily access policy decides when the user connects directly and when an access request is required - see *Time-Based Access Requests*.

Time Policy for a Single User With Group-Derived Access

The settings above apply to users assigned to the safe directly. A user who reaches the safe through a group can be given a time policy of their own, without being assigned to the safe directly. The *Users* tab lists such users in the *Access via groups* section, together with the groups that grant the access and an indication of whether a policy is already defined for them.



1. Select the users whose access you want to change.
2. Click *Manage custom policies*.
3. Set the options on the *GENERAL*, *ACCESS TIME PERIOD* and *DAILY ACCESS POLICY* tabs. The *GENERAL* tab holds the *Blocked* switch.
4. Click *Save*.



To return a user to the policies of their groups, select them and click *Disable custom policies*. The user is then in exactly the state they were in before any policy was defined for them.

Important

Disable custom policies and the *Enable time policy* checkbox are two different things. Clearing

Enable time policy switches off the weekly schedule but keeps the policy, so its *Blocked* switch and *Access time period* still apply. *Disable custom policies* removes the policy altogether.

Note

Such a policy can only be defined for a user who already reaches the safe through a group - it limits an existing access and does not grant one.

It is tied to the user and the safe, not to a particular group. If the user reaches the safe through several groups, detaching one of them leaves the policy in place.

Warning

When the user loses **every** group path to the safe - the last granting group is detached from the safe, or the user is removed from the last group that grants it - the policy is deleted automatically. Granting group access again later does not restore it; the policy has to be defined once more.

Note

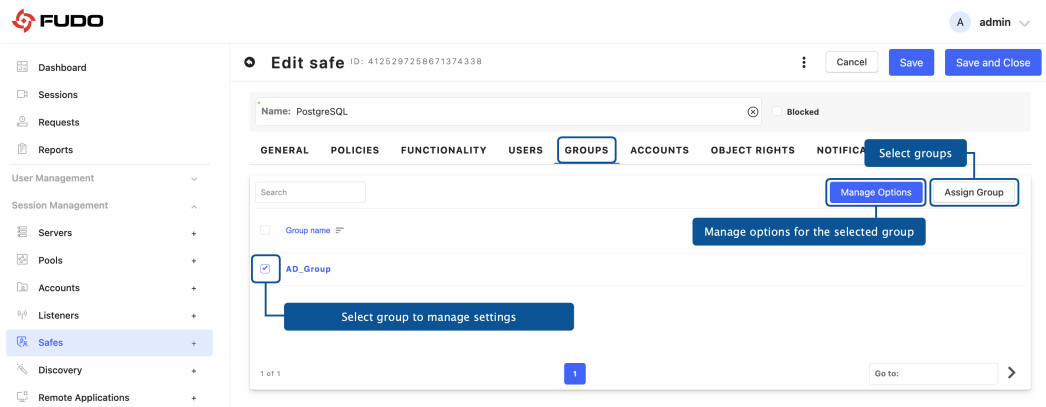
A user denied by such a policy sees the account as unavailable in the User Access Gateway, in the same way as any other denial. If the access time period ends while a session is running, the session is terminated; removing the policy during a session does not terminate it, provided the groups still permit the access.

GROUPS TAB

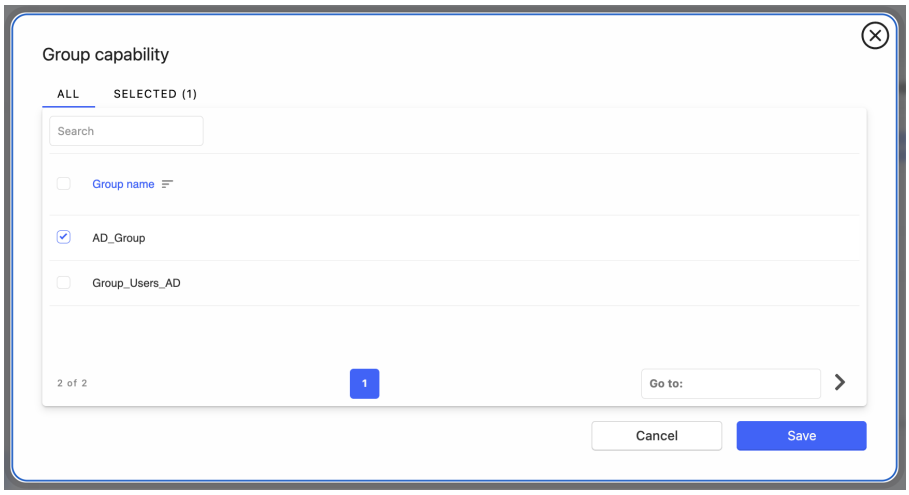
In the *GROUPS* tab, you can specify the user groups that will be allowed to access the accounts assigned to this safe.

Note

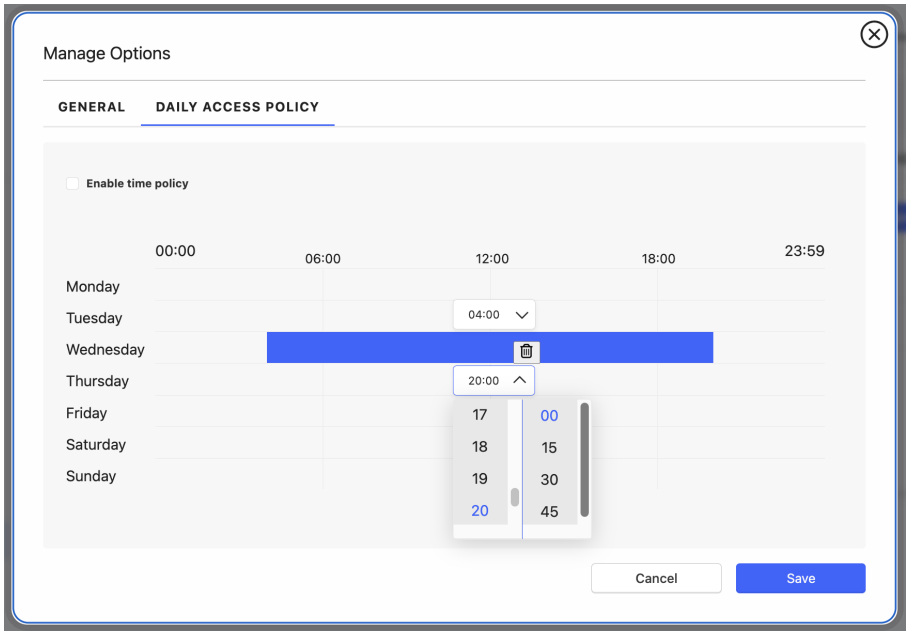
To understand how access for users and groups to the safe is prioritized, see the *Access Resolution and Prioritization* section.



1. Click *Assign Group*.
2. Mark the checkbox in front of the groups' names to add it.



3. Click *Save* to close the modal window.
4. Select desired group and click *Manage Options* to define general settings and daily access rules.



5. Click *Save* to close the modal window.

Note

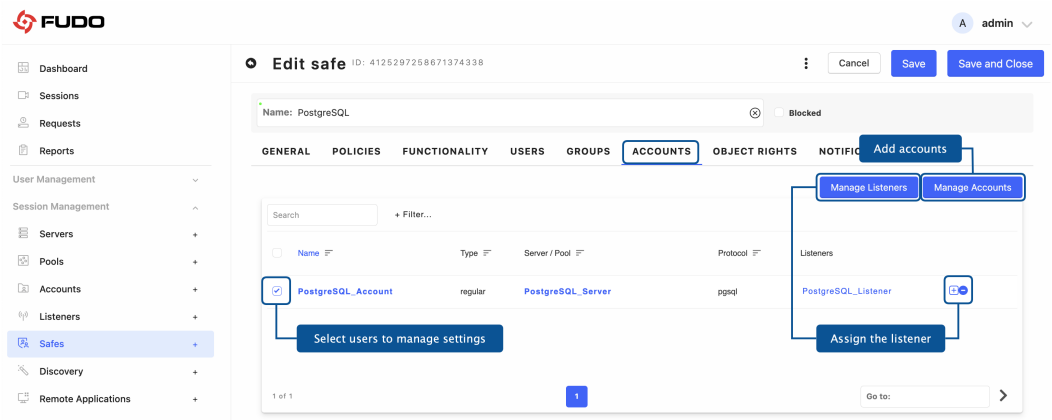
A group that is blocked, or that falls outside its access time period, contributes no access to any of its members for this safe. The same options are available from the group's side, in *User Management* > *Groups*, and show identical values.

ACCOUNTS TAB

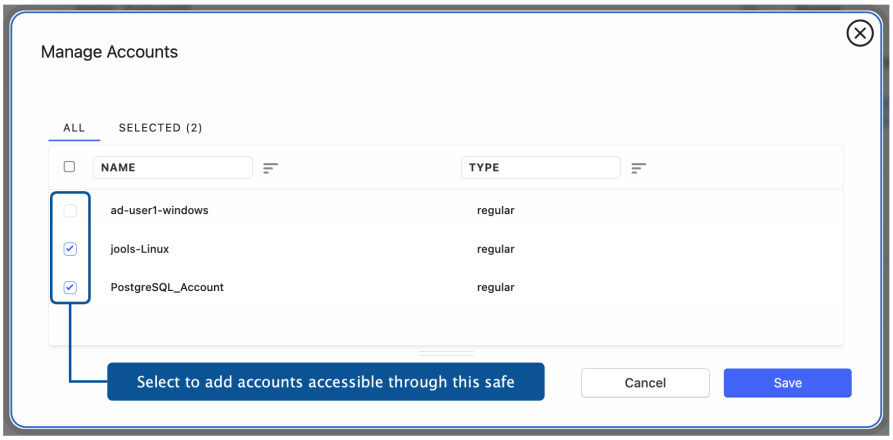
Note

To manage accounts within the safe, the user must also have assigned the *listener-read* privilege.

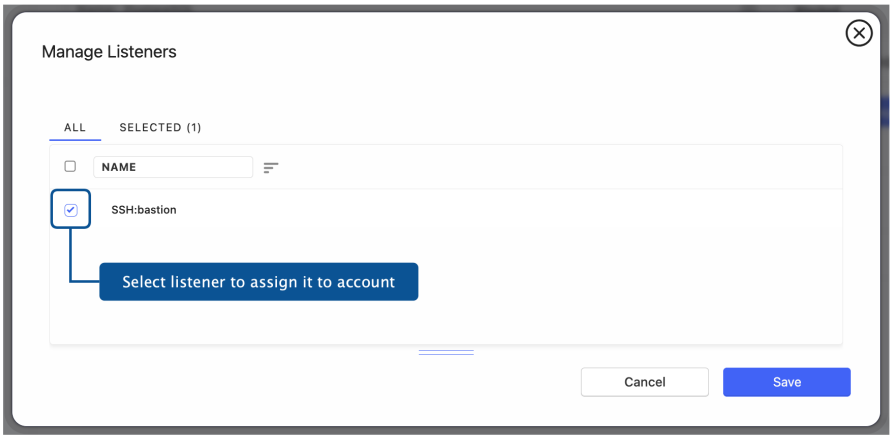
Select *ACCOUNTS* tab to add *accounts* accessible through this safe.



1. Click *Manage Accounts*.
2. Mark the checkbox in front of the accounts' names to add it.



3. Click *Save* to close the modal window.
4. Select desired account and click *Manage Listeners* to assign listeners to accounts.

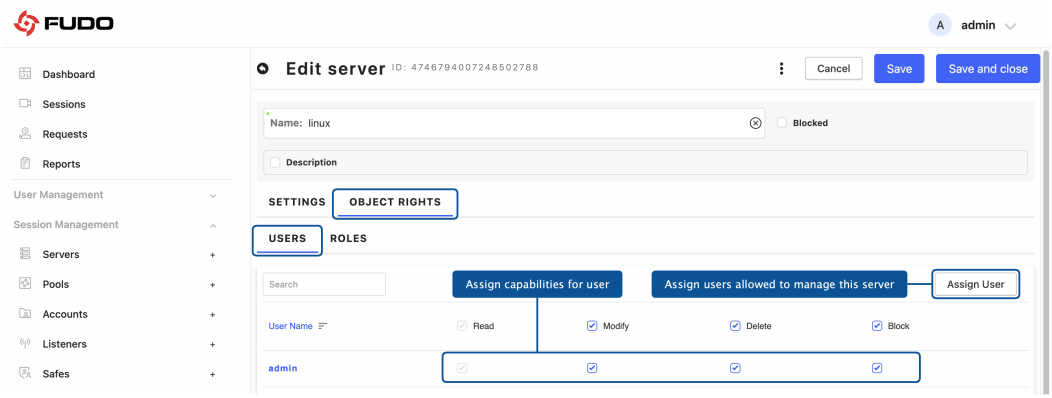


5. Click *Save* to close the modal window.

OBJECT RIGHTS TAB

The **OBJECT RIGHTS** tab is used to define which users and roles are allowed to manage the object and which capabilities (Read, Modify, Delete, Block) are assigned to them.

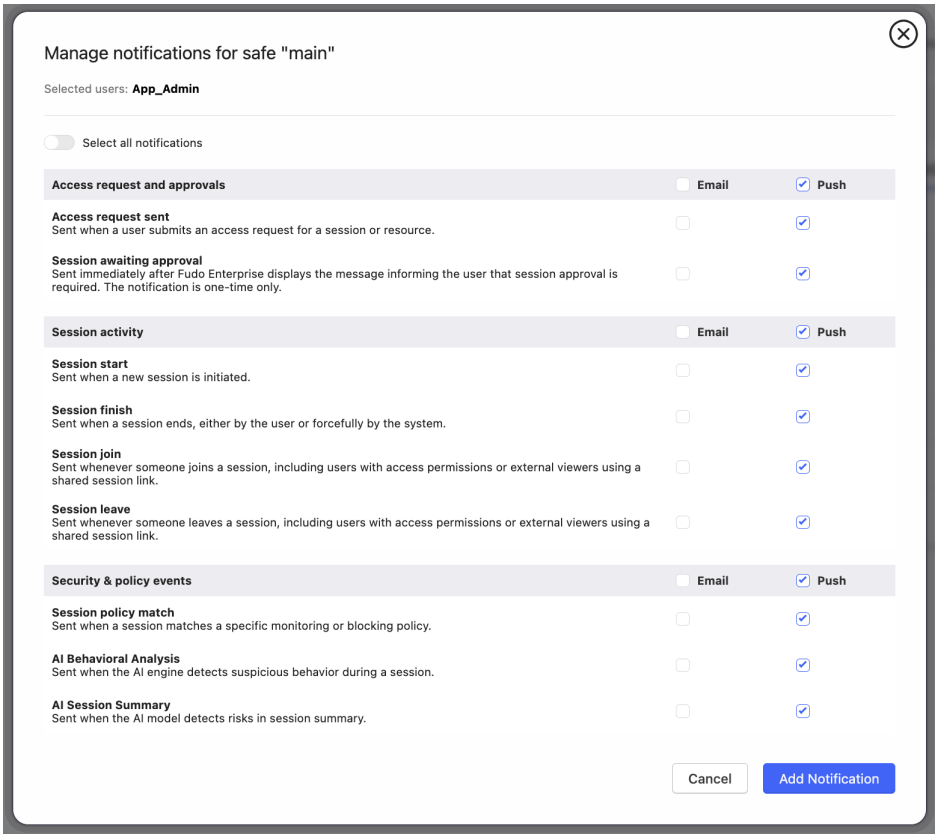
1. Go to the **OBJECT RIGHTS** tab.
2. Open the **USERS** sub-tab.
3. Click **Assign User**, select the users from the list, and click **Save**.
4. In the **Users** list, select the capabilities for each user by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.
5. Open the **Roles** sub-tab.
6. Click **Assign Role**, select the roles from the list, and click **Save**.
7. In the **Roles** list, select the capabilities for each role by enabling the options available for the given object, such as *Read*, *Modify*, *Delete*, or *Block*.



NOTIFICATIONS TAB

Select *NOTIFICATIONS* tab to specify notifications that will be enabled for the particular users. For detailed information about notification types follow the *Notifications* section.

1. To define specific notification types for a user, select the checkbox in front of the desired users' names and click *Manage Notifications*.



2. From the list, select the notification types you want to assign to the user.
3. Click *Add Notification* to close the modal window.
4. Click *Save* or *Save and close* to save the safe configuration.

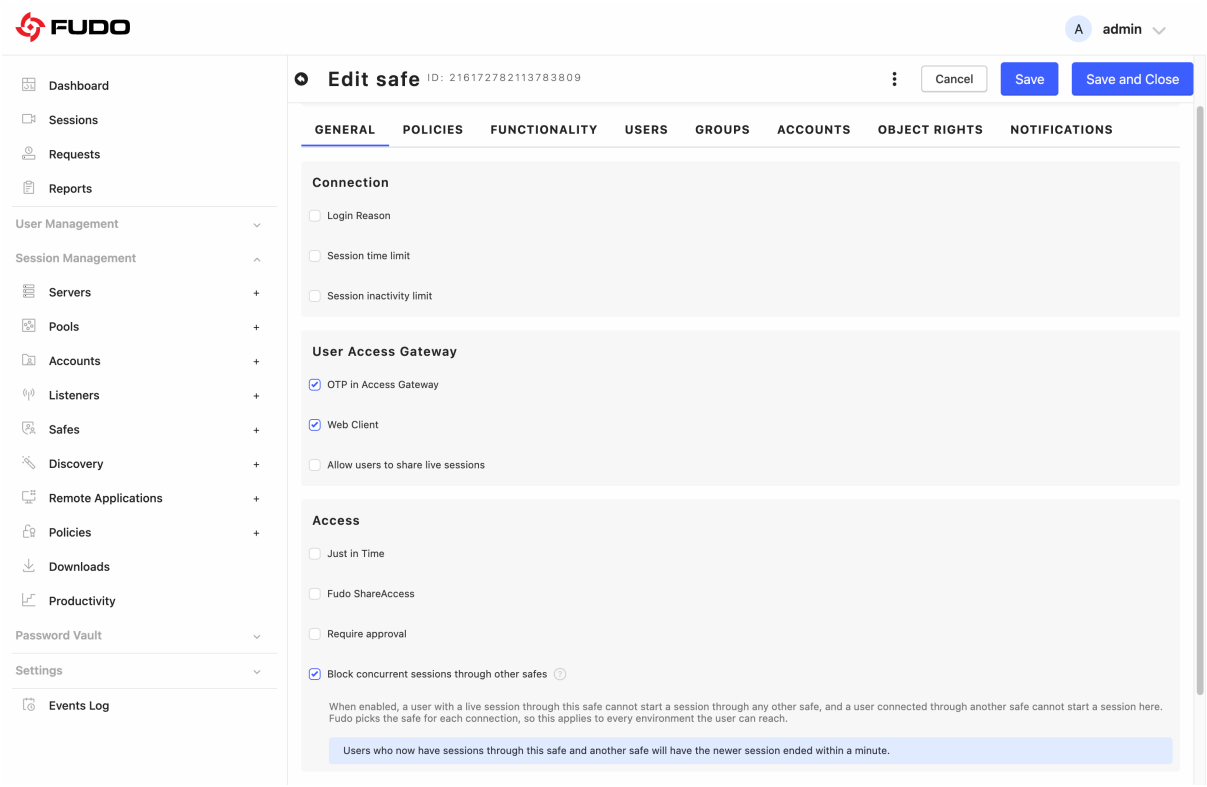
Related topics:

- *Data Model*
- *Editing a Safe*
- *Blocking a Safe*
- *Deleting a Safe*

10.5.2 Blocking Concurrent Sessions Through Other Safes

The **Block concurrent sessions through other safes** option prevents a user from having sessions through two safes at the same time. When the option is enabled for a safe, a user with a live session through this safe cannot start a session through any other safe. A user with a live session through another safe cannot start a session through this safe.

The option is set on the **GENERAL** tab of the safe form, in the **Access** section. It is not available for the built-in portal safe.



How It Works

Fudo Enterprise applies the following rules when checking concurrent sessions:

- A new session is refused if the option is enabled for the safe of the live session or for the safe of the new session.
- A user can have several sessions through the same safe at the same time, even if the option is enabled for that safe.
- A session waiting for approval or for supervisors counts as a live session.
- Secret checkouts are not counted and are not blocked by this option.
- Joining another user's shared session is not checked.

The check is made when the user connects. Two sessions started at the same time can both be established, for example when two connections are opened in parallel. Fudo Enterprise also checks running sessions about every 30 seconds: if a user has live sessions through two safes and one of them blocks concurrent sessions, the **newer** session is ended within a minute. In the session list, such a session has the *Terminated* status.

Note

If you enable the option while a user has sessions through this safe and another safe, the newer session is ended within a minute.

What the User Sees

- In a native client, the connection is refused.
- In the User Access Gateway, the user cannot generate a one-time password or open the session in the Web Client. The message names the account and the server of the session

that is already running, so that the user knows which session to end first.

Anonymous Accounts

A safe that blocks concurrent sessions cannot contain an *anonymous account*. All anonymous connections use the same user, so one anonymous session in such a safe would block anonymous sessions in all other safes.

- The option cannot be enabled for a safe that contains an anonymous account.
- An anonymous account cannot be added to a safe that has the option enabled.

Blocking Concurrent Sessions in a Cluster

In a *cluster*, each node checks for concurrent sessions using the session data replicated from the other nodes, so a session on one node can block a session on another node.

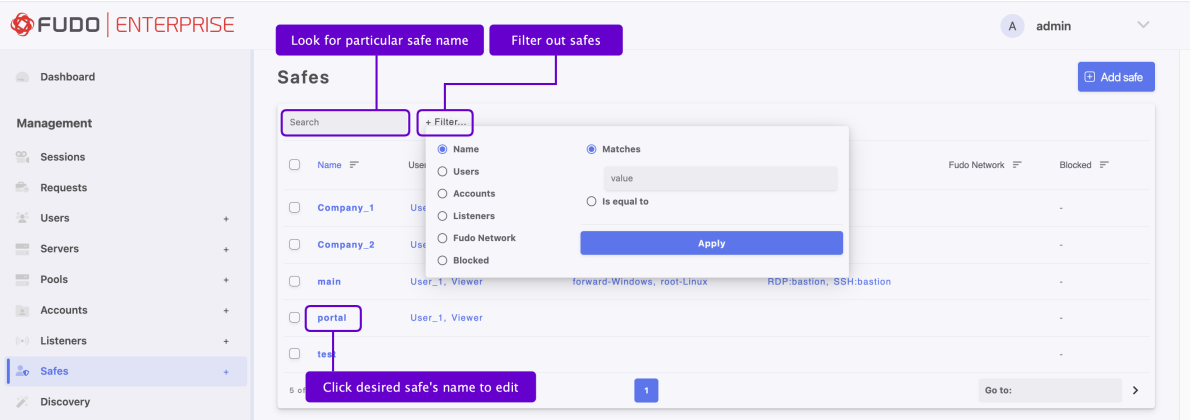
- Configure replication in both directions between all nodes that users connect to. A node that does not receive data from another node does not see the sessions established on that node.
- Because of replication delay, concurrent sessions on two nodes can exist for a short time. They are detected by the periodic check, and the newer session is ended.
- If a node has not replicated its data for more than 2 minutes, for example because it is down, its sessions no longer block new sessions. When replication works again, a conflicting session started in the meantime is ended at the next check.

Related topics:

- *Creating a Safe*
- *Sessions*

10.5.3 Editing a Safe

1. Select *Management* > *Safes*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Find and click desired object's name to open its configuration page.
4. Modify configuration parameters as needed.
5. Click *Save*.

Related topics:

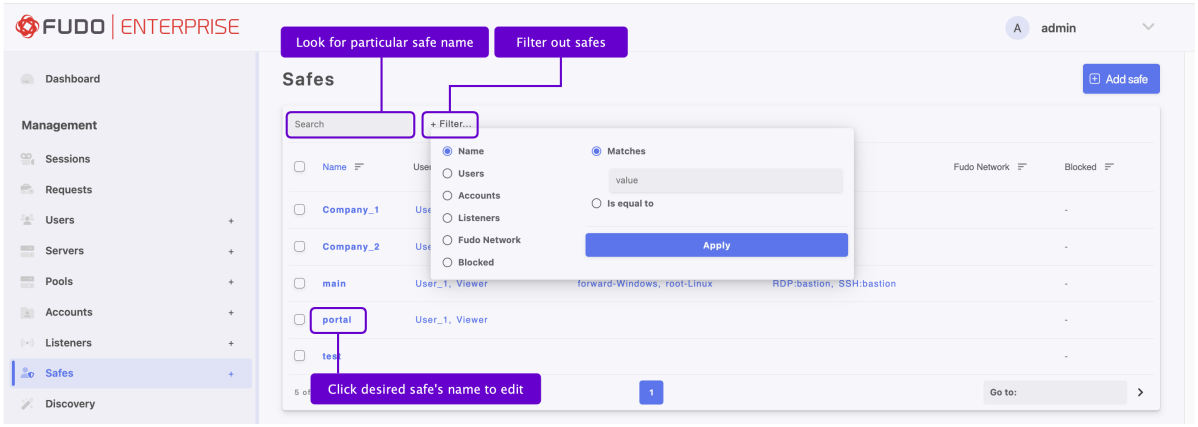
- *Data Model*
- *Creating a Safe*
- *Blocking a Safe*
- *Unblocking a Safe*

10.5.4 Blocking a Safe

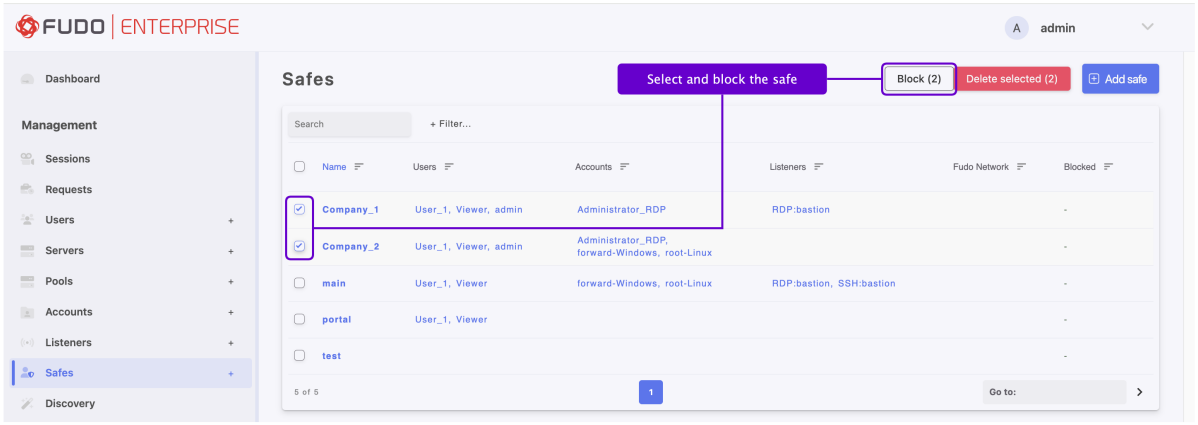
Warning

Blocking a safe definition will terminate all current connections that use accounts assigned to this safe to connect to servers.

1. Select *Management* > *Safes*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Select one or more safes to block by checking the box next to safe's name.
4. Click *Block* button to block selected safes.



5. Provide descriptive reason for blocking given resource (required) and click *Confirm* in displayed dialog box.

Note

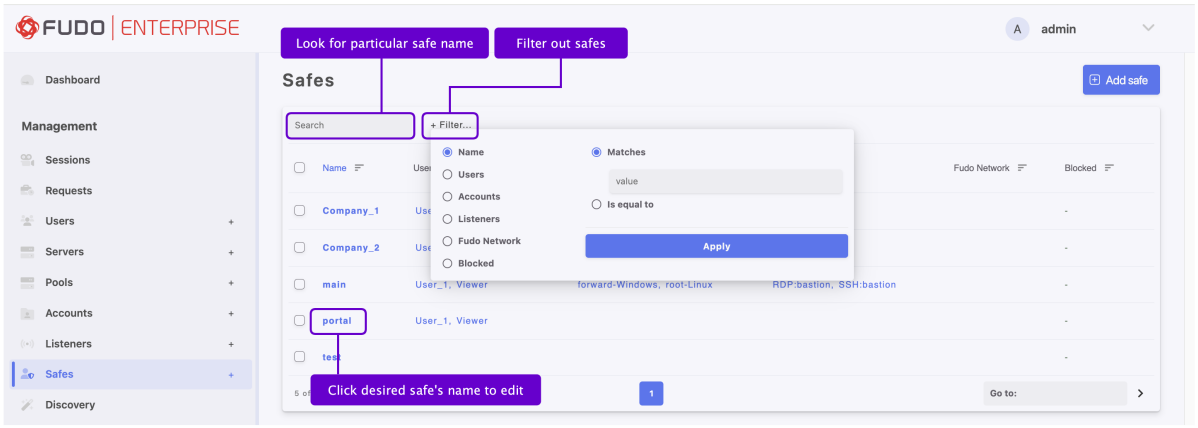
To view the blocking reason, place the cursor over the red cross icon on the listeners list.

Related topics:

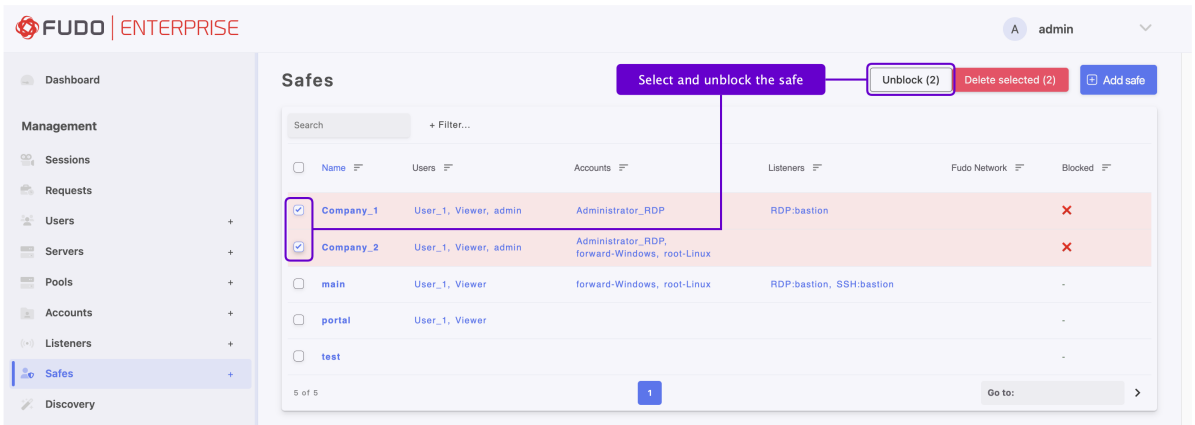
- *Unblocking a Safe*
- *Data Model*
- *Creating a Safe*
- *Blocking a Safe*

10.5.5 Unblocking a Safe

1. Select *Management* > *Safes*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Select one or more safes to unblock by checking the box next to safe's name.
4. Click *Unblock* button to unblock selected safes.



4. Click *Confirm* to unblock selected objects.

Related topics:

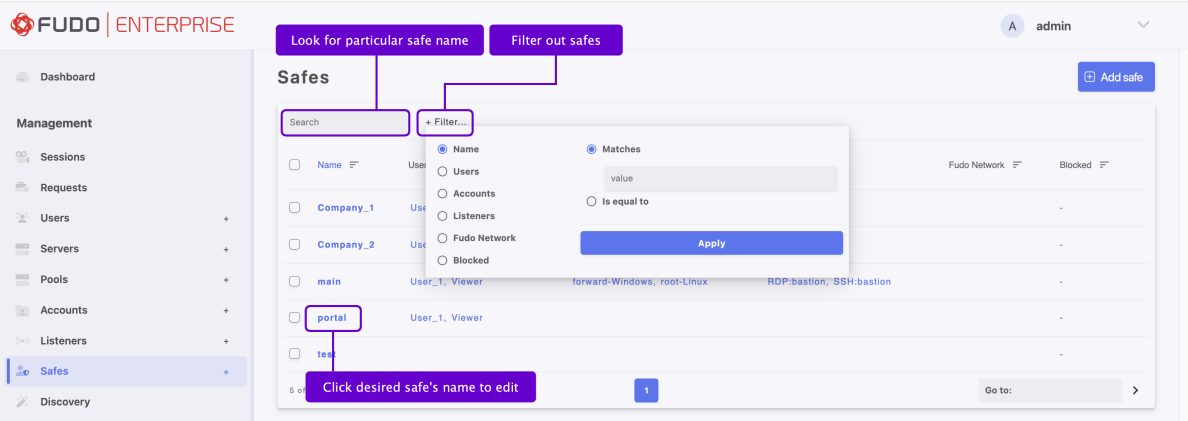
- *Blocking a Safe*
- *Data Model*
- *Creating a Safe*

- *Deleting a Safe*

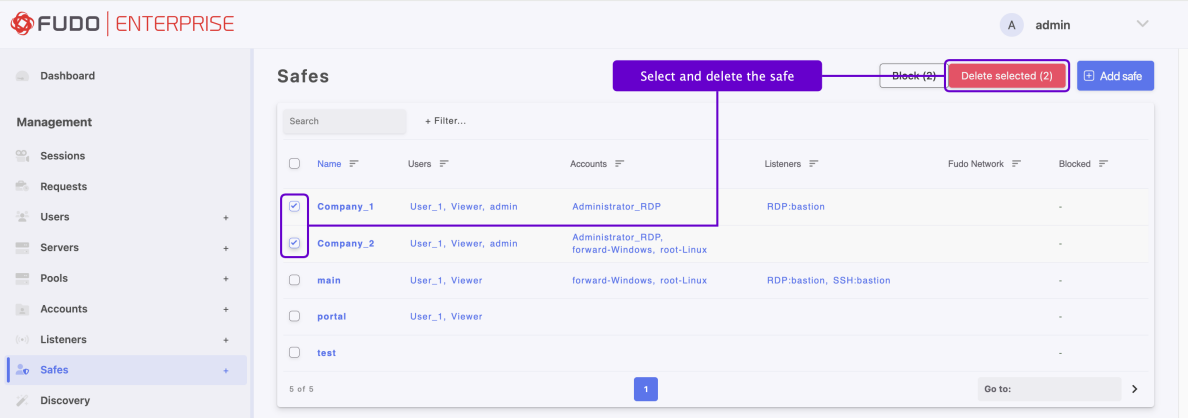
10.5.6 Deleting a Safe

> **Warning**
>
> Deleting a safe definition will terminate all current connections that use accounts assigned to this safe to connect to servers.

1. Select *Management* > *Safes*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



3. Select one or more safes to delete by checking the box next to safe's name.
4. Click *Delete selected* button to delete selected safes.



5. Confirm deleting selected objects by choosing *Confirm* button in displayed dialog box.

Related topics:

- *Data Model*
- *Creating a Safe*
- *Editing a Safe*
- *Blocking a Safe*
- *Unblocking a Safe*

10.6 Discovery

The *Discovery* feature is able to search for accounts with different privilege levels on domain controllers, servers on domain controllers, and local accounts on Windows servers.

Additional nomenclature that comes along with this feature within the *Discovery*, the *Accounts*, and the *Servers* tab:

- *Scanner* - the main component that aims to discover accounts or servers on the target server. The scanner can have a rule that defines an action that follows the discovery. The scanner can be executed manually or automatically according to the schedule.
- *Rule* - allows setting criteria for the objects to be discovered and the actions to be performed after their discovery.
- *Account Category* - is a privilege level of the account.
- *Discovered Accounts* - accounts that were discovered by the scanner.
- *Discovered Servers* - servers that were discovered by the scanner.
- *Onboarded Accounts* - accounts that were unblocked on the target server and optionally added to the listener and / or safe.
- *Onboarded Servers* - servers that were unblocked on the target server and optionally added to the pools.
- *Quarantined Accounts / Servers* - accounts or servers that were blocked on the target server.

Note

- The Discovery feature executes scanning Active Directory by connecting using the LDAP protocol.
- The WinRM protocol is used to connect to the server and scan for local accounts.

The Discovery function needs two objects to provide the most efficient results:

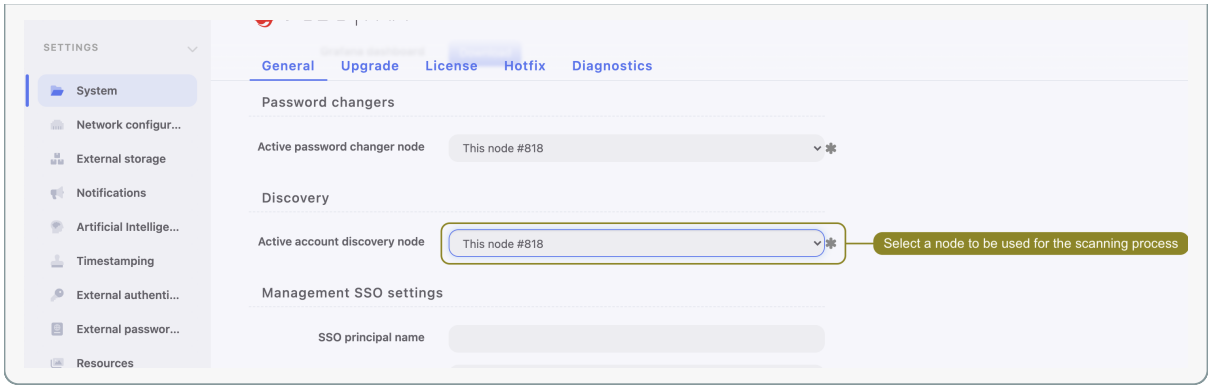
1. A *scanner* with configuration of the target server and an account to connect, and a schedule for running the scanner automatically.
2. A *rule* to specify what the scanner should do in terms of its discovery.

To have the Discovery function fully automatic, it is advised to start its configuration from creating a rule and next, create a scanner.

Although, if you want to onboard or send to quarantine the discovered accounts or servers manually, you can complete *Creating a Scanner* step only, as the scanner can work without the rules being added. Next, discovered accounts or servers can be moved further with the *Managing Discovered Accounts* or *Managing Discovered Servers* option, available in the *Accounts* and *Servers* tab.

Note

The active node, which is used for the scanning process, can be checked under the *Discovery* section in the *Settings* > *System* tab.



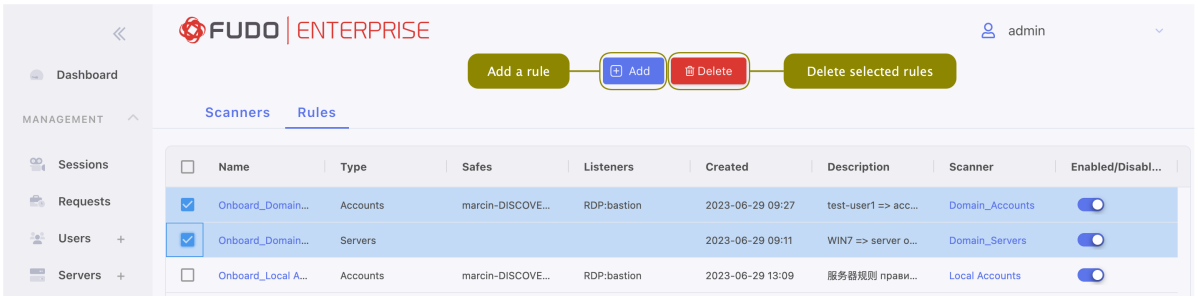
10.6.1 Creating a Rule

Each rule can be enabled or disabled anytime. When a rule is enabled, the system will automatically onboard or send to quarantine matching accounts or servers according to the given rule actions. The rules apply to just discovered elements but not to the elements that are already onboarded or sent to quarantine by the rules. In practice, it means that after a particular rule is changed, its actions will be applied to the accounts or servers that were discovered after the changes are saved.

10.6.1.1 Creating a Rule for Accounts

In order to create a rule for discovered accounts, proceed as follows:

1. Select *Management* > *Discovery* > *Rules*
2. Click + *Add*



3. Enter rule's name.
4. Select *Accounts* from the *Scanner type* drop-down list.
5. Optionally, enter rule's description.
6. In *Configuration* section:

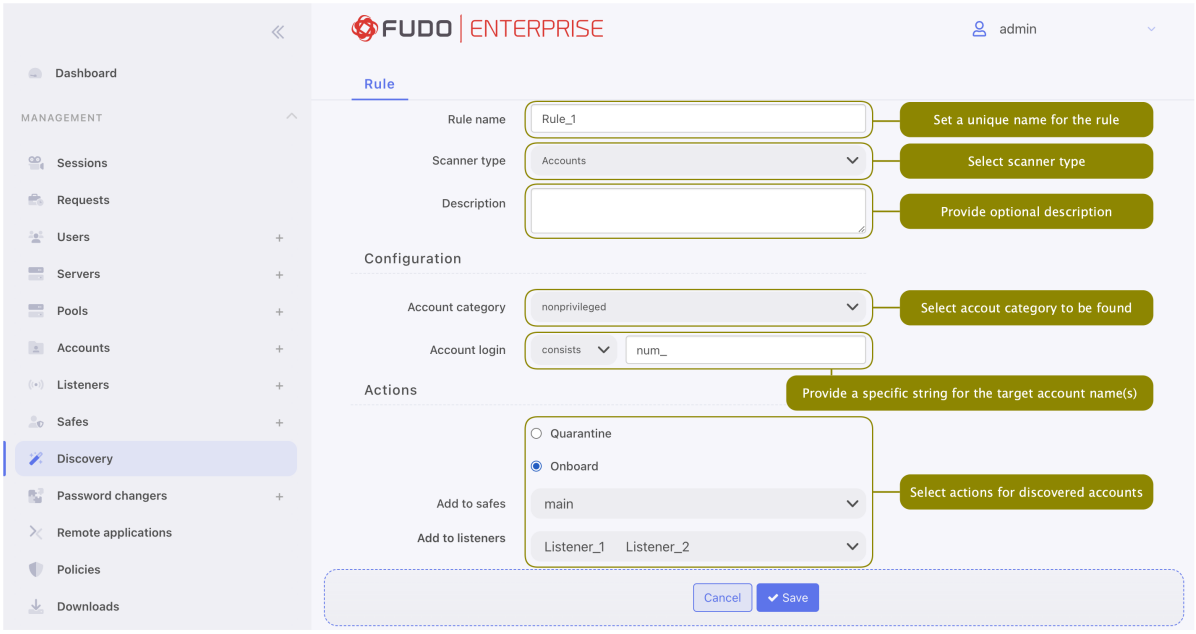
   6.1. Select *Account category* (`privileged`, `non-privileged` or `all`).

   6.2. In the *Account login* field select `consists`, `starts with` or `ends with` and provide a specific string for the target account login(s).

7. Define *Actions*:

   7.1. **Send to quarantine** or

   7.2. **Onboard** by adding the discovered accounts to the Safe and/or Listener. **Please note that listeners with bastion mode are supported only.**



8. Click *Save*.

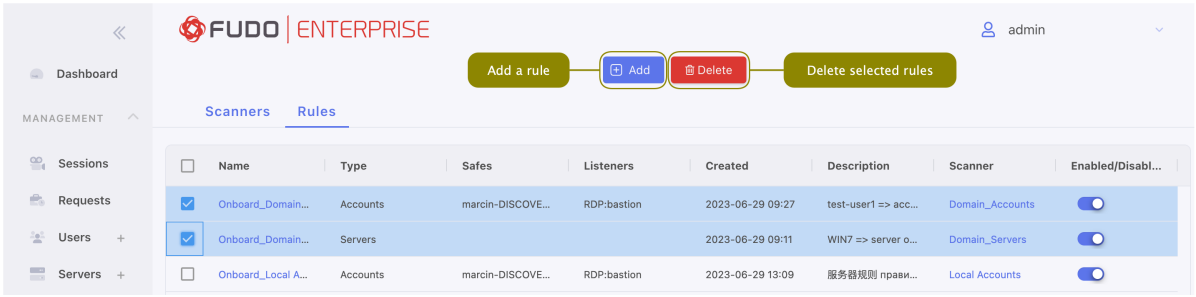
Related topics:

- *Managing Rules*
- *Creating a Scanner*

10.6.1.2 Creating a Rule for Servers

In order to create a rule for discovered servers, proceed as follows:

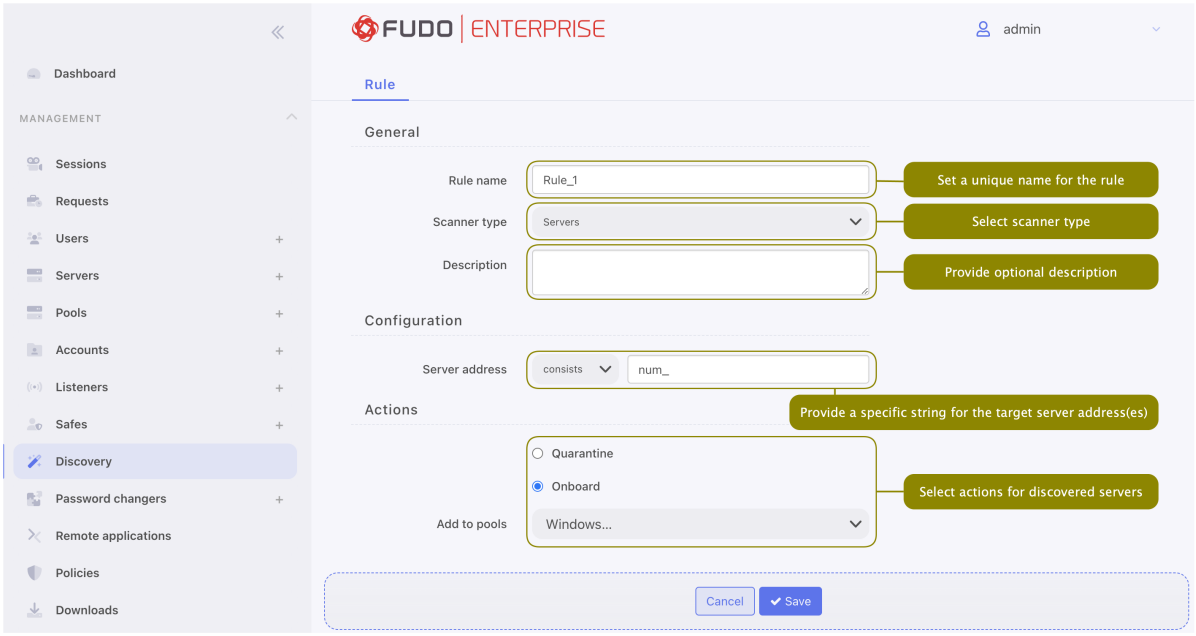
1. Select *Management* > *Discovery* > *Rules*
2. Click *+ Add*



3. Enter rule's name.
4. Select *Servers* from the *Scanner type* drop-down list.
5. Optionally, enter rule's description.
6. In *Configuration* section in the *Server address* field select `consists`, `starts with` or `ends with` and provide a specific string for the target server address(es).
7. Define *Actions*:

   7.1. **Send to quarantine** or

   7.2. **Onboard** by adding the discovered servers to selected Pool.



8. Click *Save*.

Note

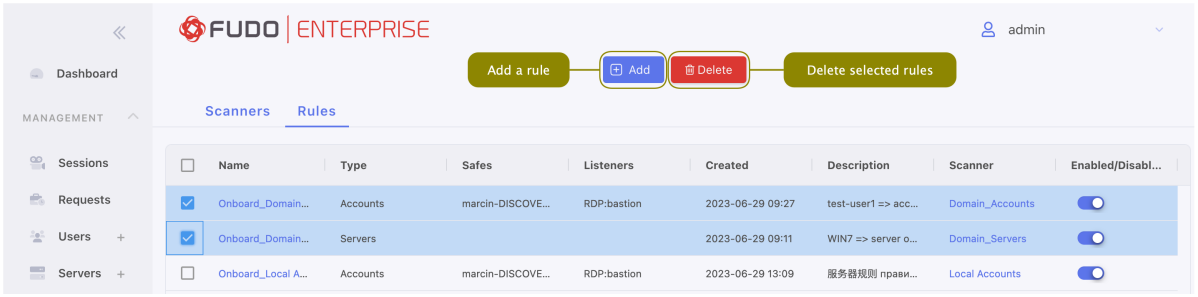
- Server with the same name as the one existing in Fudo Enterprise will not be added after scanning.
- Taking the server on a quarantine will block this server in the domain.
- Onboarding the server unblocks the server in the domain.
- If the server is removed from the domain, it will be removed from Fudo Enterprise after the next scan step.

Related topics:

- *Managing Rules*
- *Creating a Scanner*

10.6.2 Managing Rules

Each rule can be enabled or disabled anytime. When a rule is enabled, the system will automatically onboard or send to quarantine matching accounts or servers according to the given rule actions. The rules apply to just discovered elements but not to the elements that are already onboarded or sent to quarantine by the rules. In practice, it means that after a particular rule is changed, its actions will be applied to the accounts or servers that were discovered after the changes are saved.



Related topics:

- *Creating a Scanner*
- *Managing Discovered Servers*
- *Managing Discovered Accounts*

10.6.3 Creating a Scanner

10.6.3.1 Creating a Scanner for Domain Controller Accounts

The Discovery feature is able to search domain controllers for accounts with different privilege levels and add them to the relevant safes and/or listeners. This *Onboarding* process, which grants the discovered accounts access to connections, is a basis of the *Discovery* feature. Alternatively, the feature can send the accounts to quarantine, which means blocking accounts on the target server.

Note

Before proceeding with creating a scanner, you need to set up:

- a server that will be scanned for accounts - refer to the *Servers* section,
- an administrator's account on that server - refer to the *Accounts* section,
- and a pool to which you want to assign the detected accounts - refer to the *Pools* section.

Secret change policy, secret changer, and Secret verifier can be added later, after saving the scanner.

In order to create a scanner, proceed as follows:

1. Select *Management* > *Discovery* > *Scanners*
2. Click *+ Add*
3. Enter scanner's name.
4. Select `Domain Controller Accounts` from the *Scanner type* drop-down list.
5. Optionally, enter scanner's description.
6. In the *Schedule* section, choose a day and time for your scanner to start automatically on a weekly basis. This field is optional, so you can skip this step to start your scan manually anytime.
7. Fill *Configuration* section with:

7.1. Target server in the *Scan on server* field.

7.2. *Port* number to the target server.

7.3. *CA certificate*.

7.4. Optionally, select *Kerberos authentication* to have the scanner authenticate against the target server using the Kerberos protocol.

> **Note**
>
> Kerberos authentication must be enabled explicitly for each scanner; there is no fallback mechanism. This option is available for LDAP and WinRM connections. See *Kerberos Authentication Settings* for Kerberos configuration (DNS name resolution and optional KDC servers).

7.5. *Base DN* value to indicate the exact location in the domain (optional). Use following format: `cn=##username##,dc=example,dc=com`.

7.6. *Group DN* value to indicate the exact group in the domain (optional). Use following format: `cn=##username##,dc=example,dc=com`.

> **Note**
>
> If only the *Base DN* is provided, the scanner will search the entire domain. Specifying the *Base DN* is required.

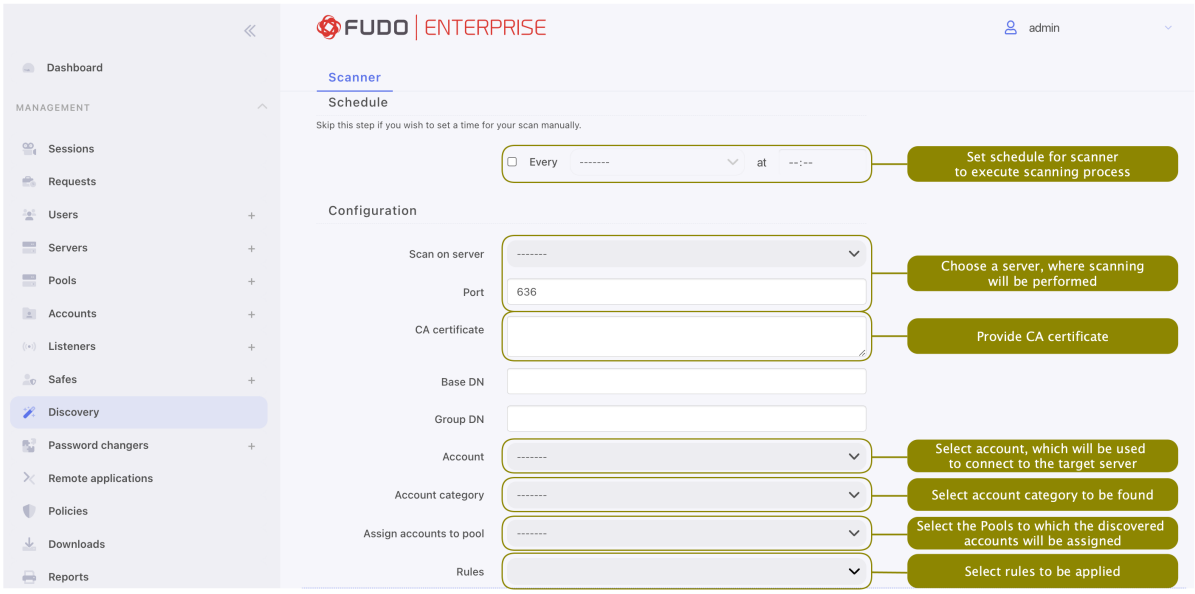
7.7. *Account* to be used to connect to the target server.

7.8. Select *Account category* to be found (`privileged`, `non-privileged` or `all`).

> **Note**
>
> The Discovery feature identifies *privileged* accounts within Active Directory (AD) based on specific group memberships that signify high levels of rights and permissions. To be recognized as *privileged* by the Discovery scanner, accounts must belong to one of four AD's high-privilege groups:
>
> - Enterprise Admins (EA),
> - Domain Admins (DA),
> - Built-in Administrators (BA),
> - Schema Admins (SA).

7.9. Select the *Pools* to which the discovered accounts will be assigned.

7.10. Choose previously defined *Rules* to set the following actions after the scan. **Please note that in case more than one rule is added and their actions overlap, the order of the rules is taken into account: the first matching rule will be applied.**



8. In *Secret Changers* section select *Secret change policy*, *Secret changer*, and *Secret verifier* which will be automatically assigned to discovered accounts.

Note

- Administrator can predefine secret changer variable values in Secret Changers configuration (refer to the *Custom Secret Changers* section).
- Predefining values is optional. If variable is not defined, it will take value from account that secret changer is assigned to.
- Default secret changers don't have predefined variable values.

8. Click Save.

Related topics:

- *Creating a Rule*
- *Managing Discovered Accounts*

10.6.3.2 Creating a Scanner for Domain Controller Servers

The Discovery feature is able to search domain controllers for servers and add them to the relevant pools during the *Onboarding* process. Alternatively, the feature can send the servers to quarantine, which means blocking servers in the domain.

Note

Before proceeding with creating a scanner, you need to set up:

- a server that will be scanned - refer to the *Servers* section,
- a privileged account on that server - refer to the *Accounts* section.

In order to create a scanner, proceed as follows:

1. Select *Management* > *Discovery* > *Scanners*
2. Click *+ Add*
3. Enter scanner's name.
4. Select `Domain Controller Servers` from the *Scanner type* drop-down list.
5. Optionally, enter scanner's description.
6. In the *Schedule* section, choose a day and time for your scanner to start automatically on a weekly basis. This field is optional, so you can skip this step to start your scan manually anytime.
7. Fill *Configuration* section with:

   7.1. Target server in the *Scan on server* field.

   7.2. *Port* number to the target server.

   7.3. *CA certificate*.

   7.4. Optionally, select *Kerberos authentication* to have the scanner authenticate against the target server using the Kerberos protocol.

   Note

   Kerberos authentication must be enabled explicitly for each scanner; there is no fallback mechanism. This option is available for LDAP and WinRM connections. See *Kerberos Authentication Settings* for Kerberos configuration (DNS name resolution and optional KDC servers).

   7.5. *Base DN* value to indicate the exact location in the domain (optional). Use following format: `cn=##username##,dc=example,dc=com`.

   7.6. *Group DN* value to indicate the exact group in the domain (optional). Use following format: `cn=##username##,dc=example,dc=com`.

   Note

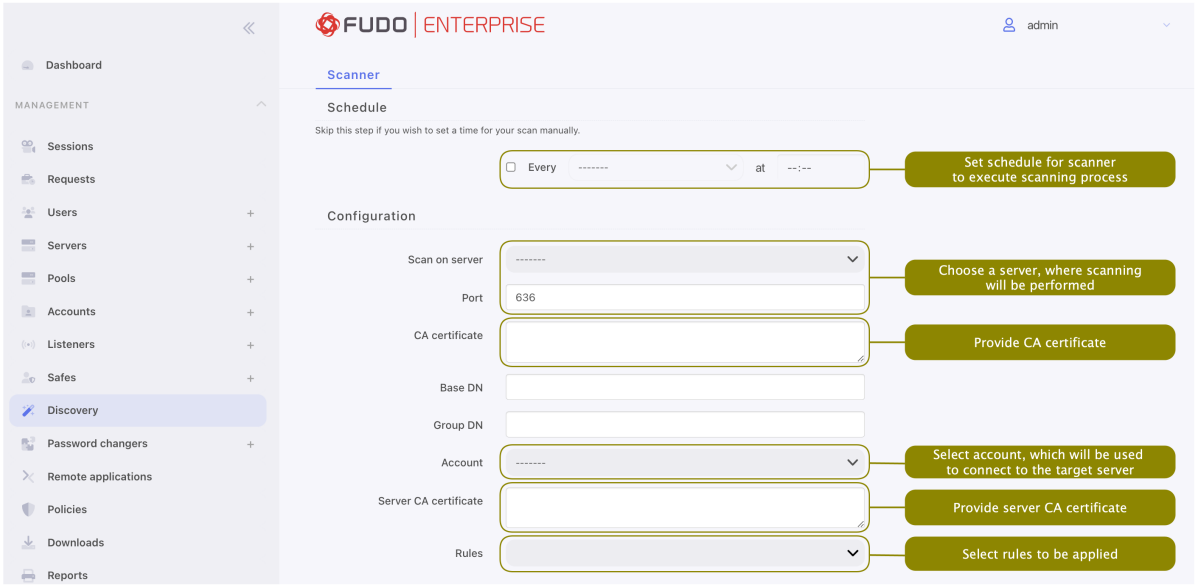
   If only the *Base DN* is provided, the scanner will search the entire domain. Specifying the *Base DN* is required.

   7.7. *Account* to be used to connect to the target server.

   7.8. *Server CA certificate* which will be assigned to the discovered servers.

   7.9. Choose previously defined *Rules* to set the following actions after the scan. **Please note that in case more than one rule is added and their actions**

overlap, the order of the rules is taken into account: the first matching rule will be applied.



8. Click Save.

Related topics:

- *Creating a Rule*
- *Managing Discovered Servers*

10.6.3.3 Creating a Scanner for Local Accounts

The Discovery feature is able to search Windows servers in a pool for local accounts and add them to the relevant safes and/or listeners. Alternatively, the feature can send the accounts to quarantine, which means blocking accounts on the target server.

Note

Before proceeding with creating a scanner, you need to set up:

- a pool of servers that will be scanned for local accounts - refer to the *Pools* section,
- an administrator's account with access to all scanned servers - refer to the *Accounts* section.

Secret change policy, secret changer, and Secret verifier can be added later, after saving the scanner.

In order to create a scanner, proceed as follows:

1. Select *Management* > *Discovery* > *Scanners*
2. Click + *Add*
3. Enter scanner's name.
4. Select `Windows Local Accounts` from the *Scanner type* drop-down list.
5. Optionally, enter scanner's description.

6. In the *Schedule* section, choose a day and time for your scanner to start automatically on a weekly basis. This field is optional, so you can skip this step to start your scan manually anytime.
7. In *Configuration* section:

   7.1. Select the pool of servers, where scanning will be performed.

   7.2. Specify port number in the *Port* field.

   7.3. Provide *CA certificate*.

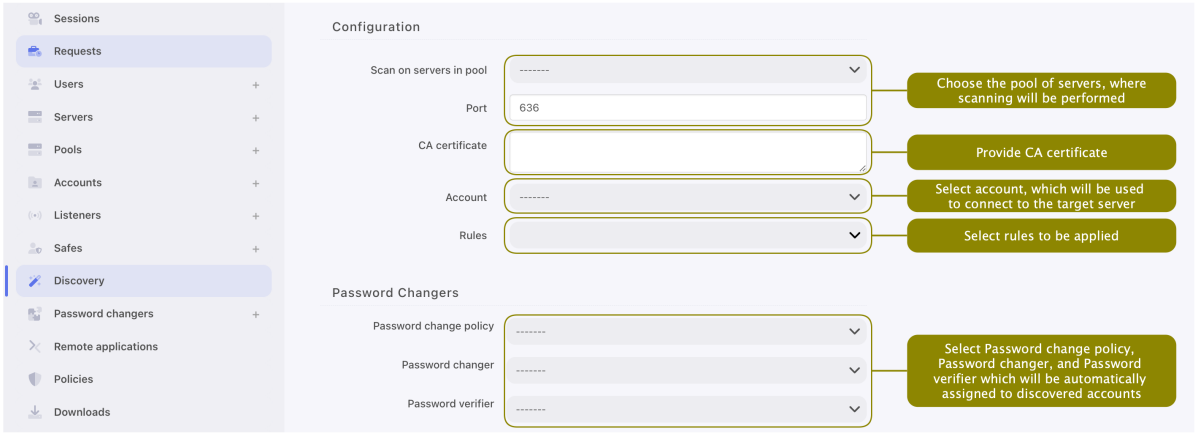
   7.4. Optionally, select *Kerberos authentication* to have the scanner authenticate against the target server using the Kerberos protocol.

> **Note**
>
> Kerberos authentication must be enabled explicitly for each scanner; there is no fallback mechanism. This option is available for LDAP and WinRM connections. See *Kerberos Authentication Settings* for Kerberos configuration (DNS name resolution and optional KDC servers).

   7.5. Select *Account* to be used to connect to the target server.

> **Note**
>
> In order to use one scanner to scan local accounts on multiple Windows servers, an administrator account with exactly the same authentication method must exist on every scanned server.

   7.6. Choose previously defined *Rules* to set the following actions after the scan. **Please note that in case more than one rule is added and their actions overlap, the order of the rules is taken into account: the first matching rule will be applied.**



8. In *Secret Changers* section select *Secret change policy*, *Secret changer*, and *Secret verifier* which will be automatically assigned to discovered accounts.

Note

- Administrator can predefine secret changer variable values in Secret Changers configuration (refer to the *Custom Secret Changers* section).
- Predefining values is optional. If variable is not defined, it will take value from account that secret changer is assigned to.
- Default secret changers don't have predefined variable values.

8. Click Save.

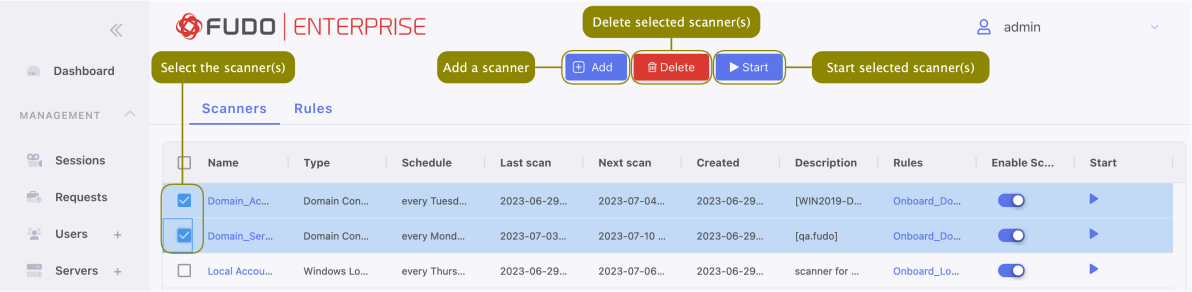
Related topics:

- *Creating a Rule*
- *Managing Discovered Accounts*

10.6.4 Managing Scanners

The scanners with defined schedule can have scheduling enabled or disabled anytime. When a scanner has scheduling enabled, the system will automatically execute the given scanner configuration. When a scanner's scheduling is disabled, the system will wait for the decision from superadmin to start its execution.

Multiple scanners can be started simultaneously or deleted after being selected.

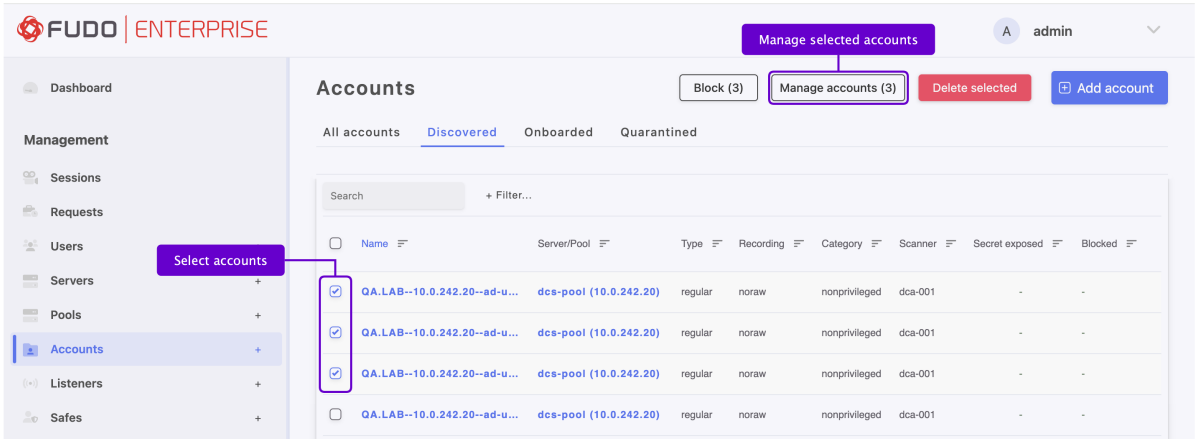


Related topics:

- *Creating a Rule*
- *Managing Discovered Servers*
- *Managing Discovered Accounts*

10.6.5 Managing Discovered Accounts

Discovered, *onboarded* and *quarantined* accounts are available in the main Accounts view.

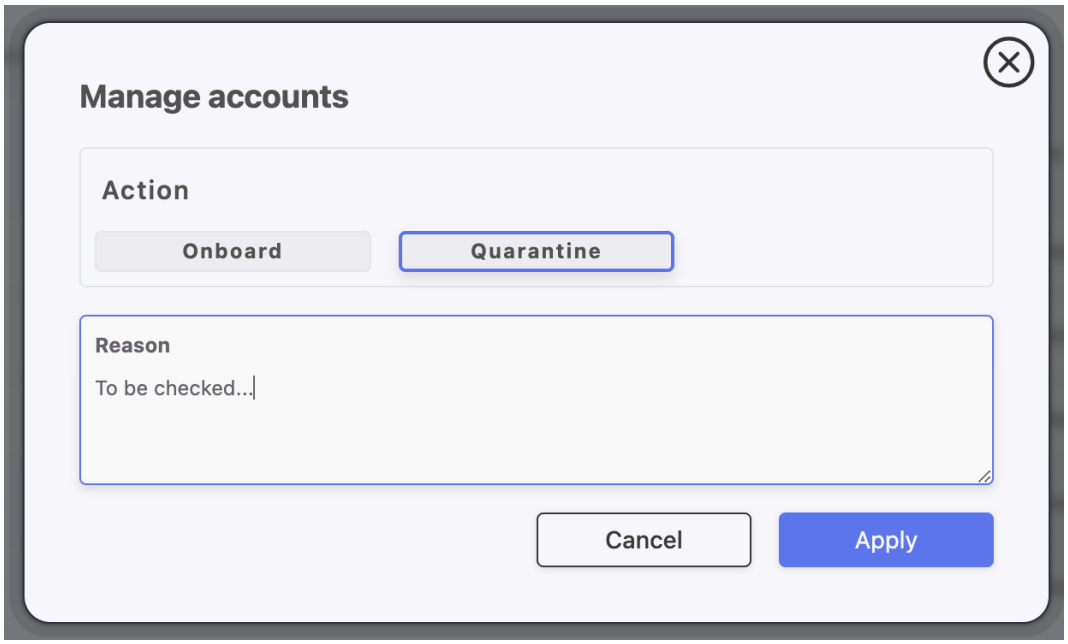


Note

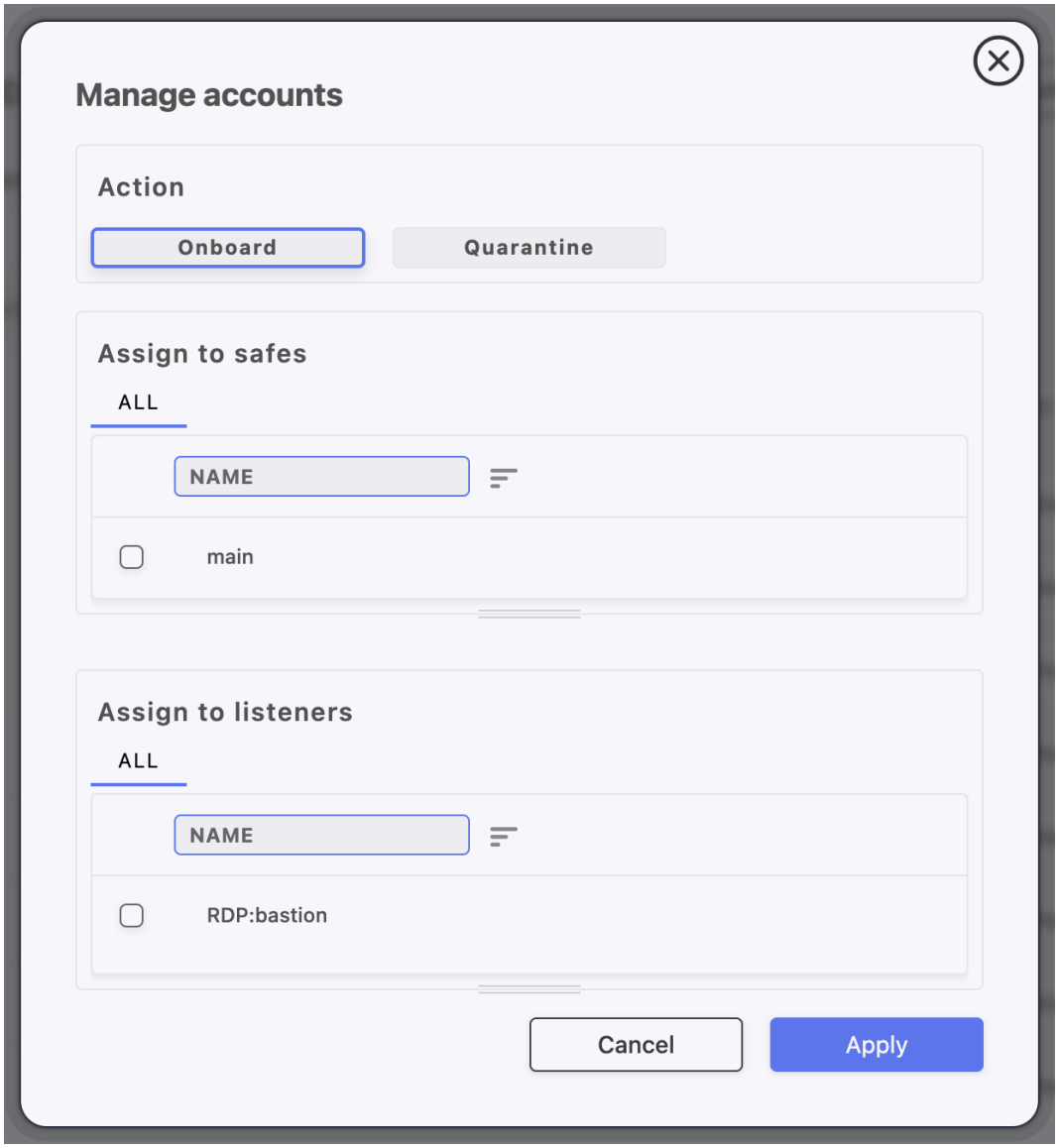
Usually, *discovered* accounts are not onboarded automatically due to a lack of automatic rule in the system. Administrator can manually onboard them by choosing the Manage Accounts option.

1. Select *Management* > *Accounts* and respectful tab: *Discovered*, *Onboarded* or *Quarantined*.
2. Choose the accounts to be onboarded or quarantined by selecting the respective checkboxes next to their names.
3. Click on the *Manage Accounts* option on the top of the functional menu - a modal will pop up.
4. Choose an action:

   4.1 **Send to quarantine** (remember to add a reason) or



   4.2 **Onboard** by adding the discovered accounts to the Safe and/or Listener. Warning: The listeners with bastion mode are supported only.



5. Click on a *Create a rule* checkbox if you want to set the defined actions to be executed automatically by the scanner in the future.
6. Click *Save*.

Related topics:

- *Creating a Rule*
- *Creating a Scanner*

10.6.6 Managing Discovered Servers

Discovered, *onboarded* and *quarantined* servers are available in the main Servers view.

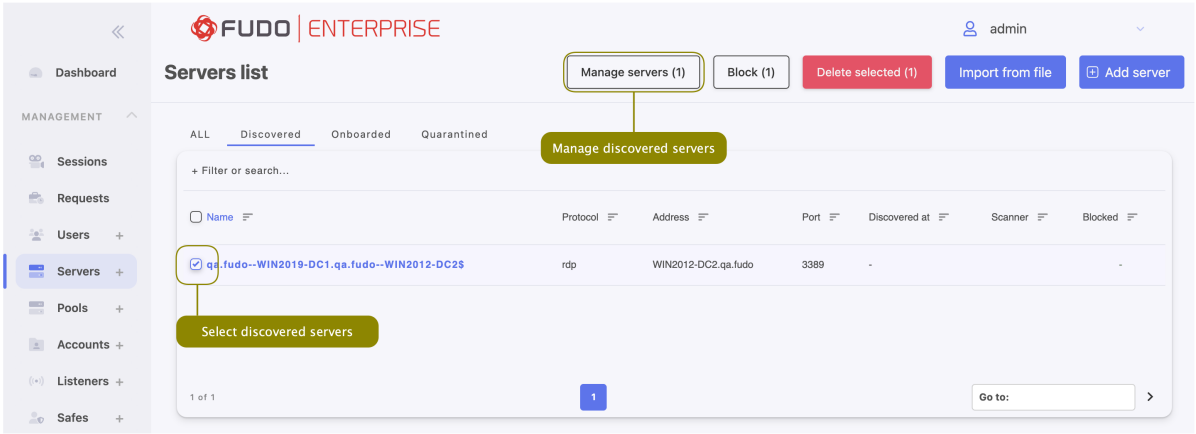
Discovered, *onboarded* and *quarantined* servers are available in the main *Servers* view.

Note

Usually, *discovered* servers are not onboarded automatically due to lack of rule configuration or assignment in scanner. Administrator can manually onboard them by choosing the *Manage*

servers option.

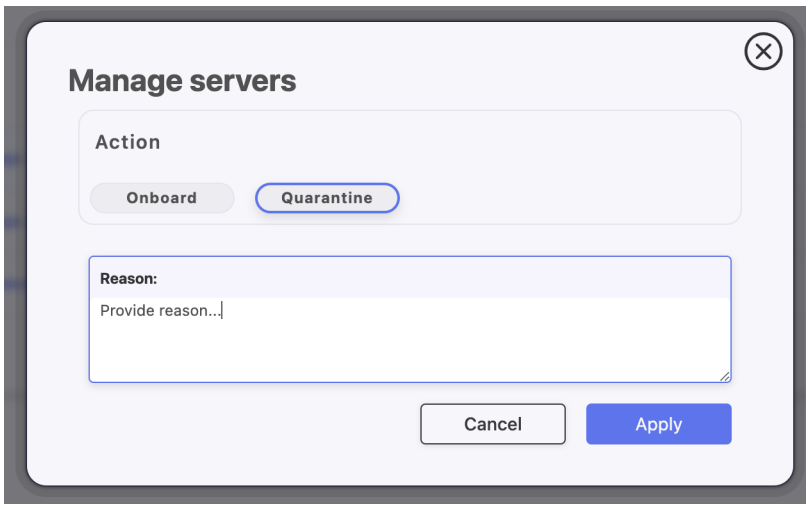
1. Select *Session Management* > *Servers* and respectful tab: *Discovered*, *Onboarded* or *Quarantined*.
2. Choose servers to be onboarded or quarantined by selecting the respective checkboxes next to their names.
3. Click on the *Manage servers* option on the top of the functional menu - a modal will pop up.



4. Choose an action:

   4.1 **Onboard** by adding the discovered servers to specified Pool or

   4.2 **Quarantine** and provide a reason (mandatory) to send chosen servers to quarantine.



5. Click *Apply*.

Related topics:

- *Creating a Rule*
- *Creating a Scanner*

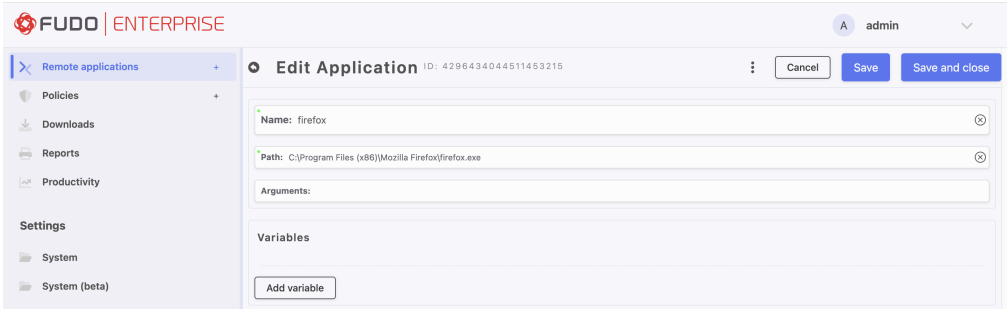
10.7 Remote Applications

Fudo Enterprise enables direct connection over the RDP protocol to a remote application using Remote Applications feature.

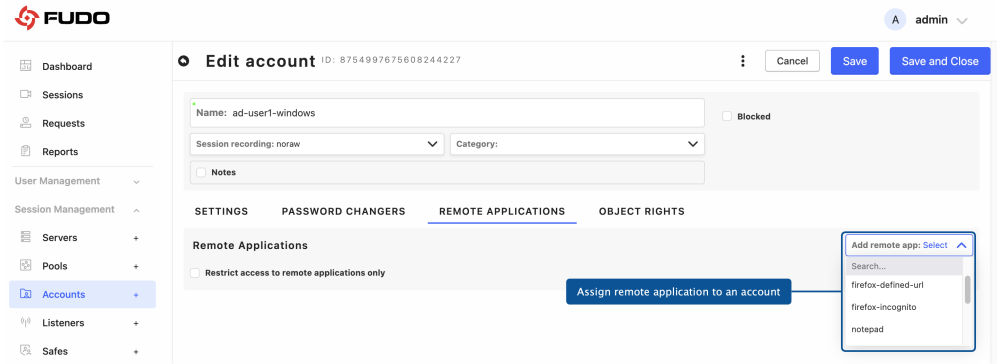
10.7.1 Adding Remote Application

In order to configure a remote application, follow the instruction:

1. Select *Management* > *Remote applications*.
2. Click the *Add remote application* button.
3. Configure the remote application:
    - Enter the application's *Name*.
    - Specify the *Path* to the application's executable file (e.g., `C:\Windows\System32\putty.exe`).



4. Click *Save and close*.
5. Add the created remote application definition to the account that will be used to access the RDP server where the application is located:
    - Select *Management* > *Accounts*.
    - Edit the account that will be used to access the RDP server.
    - In the *REMOTE APPLICATIONS* tab, expand the *Add remote app* drop-down list and select the remote application definition created in the previous steps.
    - Click the *Save* button.



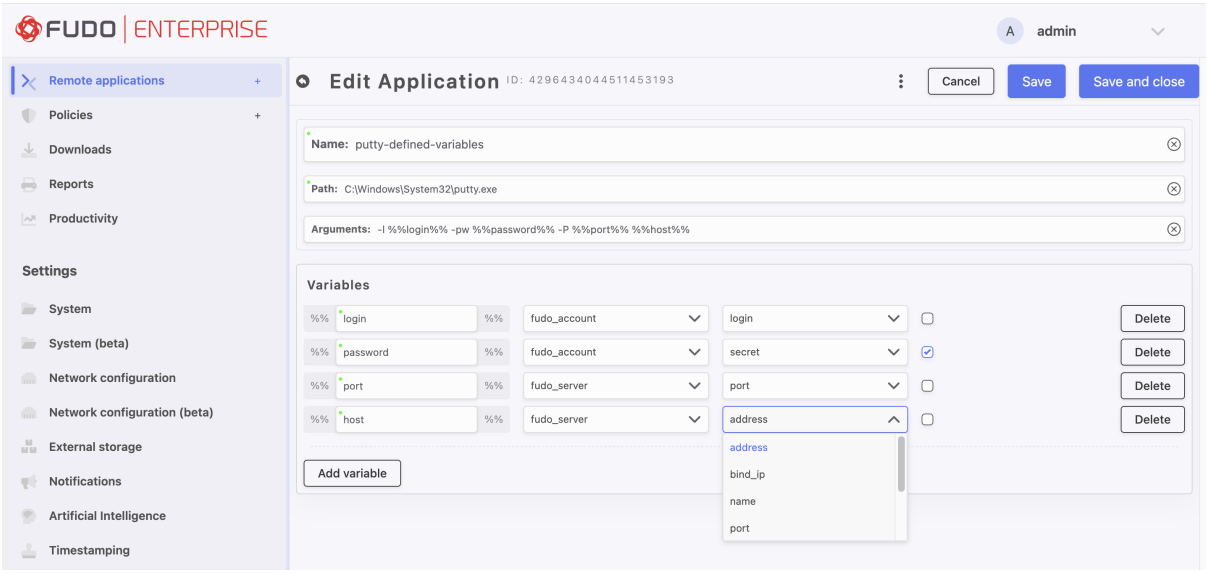
10.7.2 Adding Arguments

Remote Applications allow administrators to set commands that execute automatically at launch, enabling seamless connections with pre-filled login credentials and connection details. Variables can also be created to retrieve data directly from the Fudo Enterprise configuration.

1. Select *Management* > *Remote applications*.
2. Click the *Add remote application* button or edit existing remote application configuration.
3. Go to the *Arguments* field and enter the command to be executed automatically at launch. Here is an example for the *PuTTY* application, using variables: `-l %%login%% -pw %%password%% -P %%port%% %%host%%`.

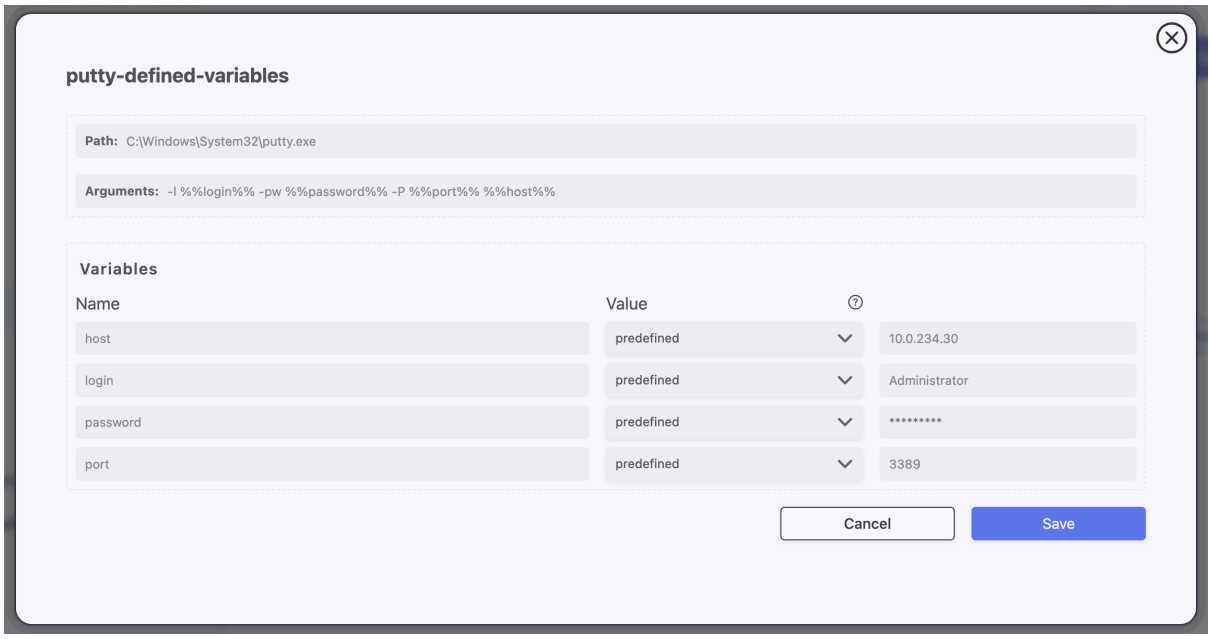
> **Note**
>
> When defining variable you can decide which object and what property of object to use. You can select *Object type* and *Object property* for each of your Arguments, and encrypt given arguments by selecting the checkbox *Encrypt* in the row following the variable name.

4. Using *Add variable* button, add four variables corresponding to the command provided in the *Arguments* field. For example:
   - Variable name: `%%login%%`, Object type: `fudo_account`, Object property: `login`.
   - Variable name: `%%password%%`, Object type: `fudo_account`, Object property: `secret`.
   - Variable name: `%%port%%`, Object type: `fudo_server`, Object property: `port`.
   - Variable name: `%%host%%`, Object type: `fudo_server`, Object property: `address`.



5. Click *Save and close*.
6. Variable values can be verified when adding the remote application to the account:
   - Select *Management* > *Accounts*.
   - Edit the account to which this remote application will be assigned.

- In the *REMOTE APPLICATIONS* tab, expand the *Add remote app* dropdown list and select the remote application definition created in the previous steps.
- Variable values will be displayed in a modal window.
- Click the *Save* button.



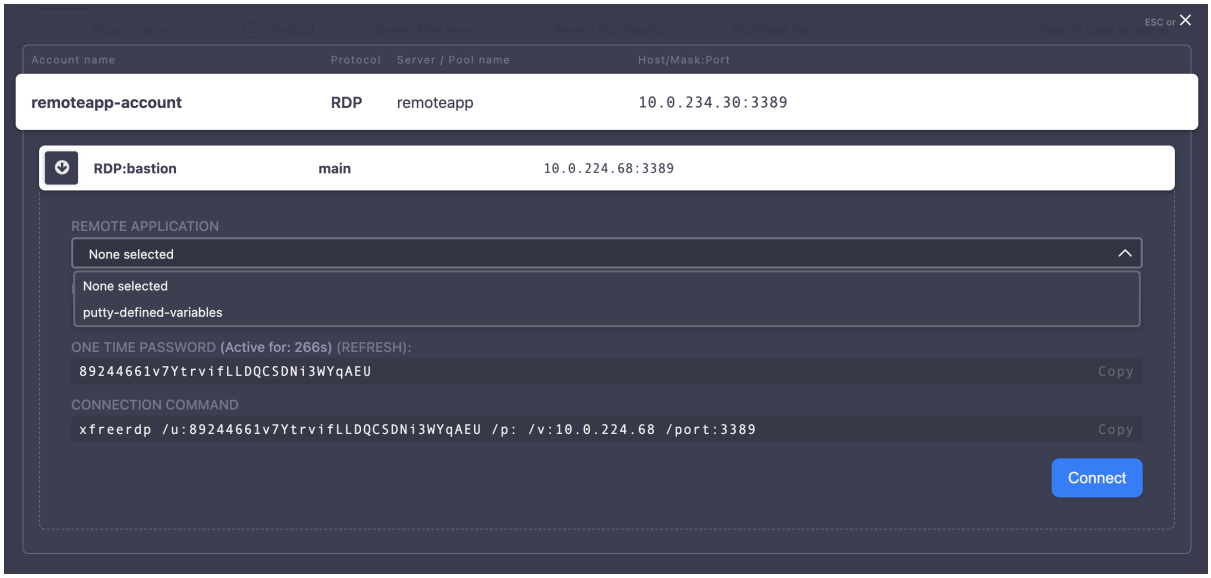
Descriptions of Available Object Types

Object type	Description
`constant`	A variable with a fixed value, editable after assigning the remote application to a specific account.
`special`	The variable will inherit the secret used to establish the session.
`fudo_server`	The variable inherits its value from the server assigned to the account that uses the remote application. Possible properties: • `address` - value from the server's *Address* field, • `bind_ip` - value of the server's bind address, • `name` - value from the server's *Name* field, • `port` - port specified for the server, • `ssh_public_key` - server's public key, • `tls_ca_certificate` - CA certificate, • `tls_certificate` - server's certificate
`fudo_account`	The variable inherits its value from the account to which the remote application is applied. Possible properties: • `description` - account's

10.7.3 Connecting to Remote Application via Access Gateway

In order to establish a connection, sign in to the User Access Gateway and select the respective account and a listener to be connected using the predefined remote application:

1. Select the *Native client* option.
2. Expand the *REMOTE APPLICATION* dropdown list and select the desired remote application to establish a connection.
3. Click *Connect*.



When a session to the specific resource is established by a user, their remote session is connected within the application only. Therefore, the user has no access to the entire desktop, and closing the application terminates the session.

10.7.4 Granular Access to Remote Applications

Warning

Remote applications are **not automatically closed** when a session ends. If you start another session using a different remote application, previously launched ones remain active. This may result in:

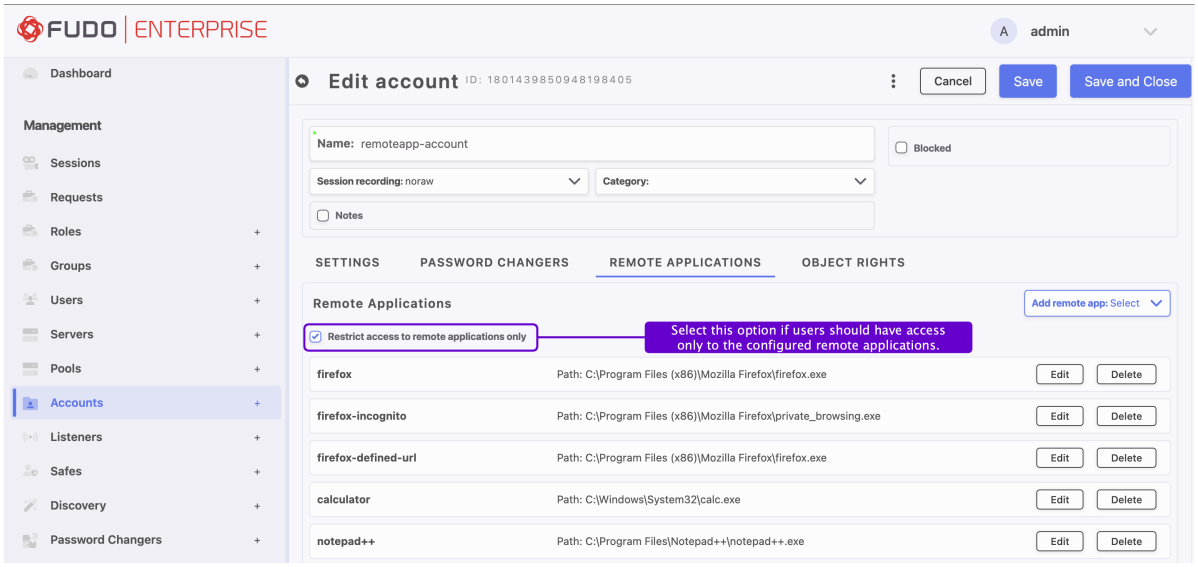
- Data or work from a previous application still being visible.
- An earlier application window overlapping or obscuring the new one.

To improve access control and reduce surface exposure, security admins can restrict users to specific remote applications without granting access to the full desktop environment. This enhancement enables more precise permission management and helps ensure that users interact only with the resources necessary for their roles.

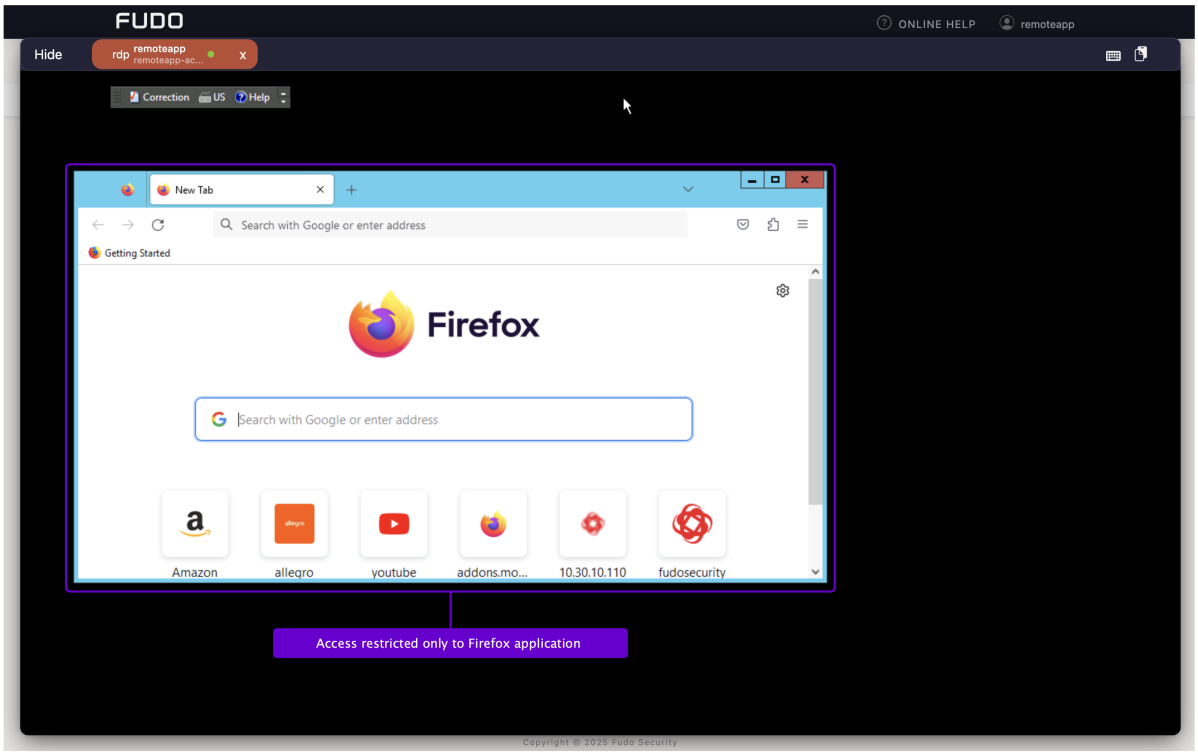
To enable this restriction for a user account:

1. Select *Management* > *Accounts*.
2. Edit the selected user account.

3. Go to the *REMOTE APPLICATIONS* tab.
4. Select the *Restrict access to remote applications only* checkbox.
5. Click the *Save* button.



Once enabled, the user will be able to launch only the remote applications explicitly assigned to their account and will not have access to the full remote desktop session.



10.7.5 Deleting Remote Application

Deleting a Remote Application From the Account Definition

In order to delete a predefined remote application from the Account definition, follow the instructions:

1. Select *Management* > *Accounts*.
2. Select the account that has the predefined remote application configured.
3. In the *REMOTE APPLICATIONS* tab select the *Delete* button following the remote application name to remove it.
4. Click *Save*.

Deleting a Definition of the Remote Application

In order to delete a remote application definition, follow the instructions:

1. Select *Management* > *Remote applications*.
2. Use checkboxes next to the remote application to select it.
3. Click *Delete selected*.
4. Confirm the remote application removal.

Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*
- *Creating an Account*

10.8 Policies

Policies are patterns definitions facilitating proactive session monitoring and control. In case a defined pattern is detected or specific conditions are met, Fudo Enterprise can automatically take respective actions and notify the administrator about the current situation.

Fudo Enterprise supports multiple policy types:

- **Regular Expression** - Triggers when defined patterns are detected in session input or output
- **AI Behavioral Analysis** - Reacts when the *Threat Probability* threshold is reached based on behavioral analysis
- **AI Session Summary** - Triggers actions when risk thresholds are detected in AI-generated session summaries
- **Live Session Analysis** [BETA] - Triggers actions when AI analysis agents report findings during an ongoing SSH session. After the beta stage this feature will be delivered as a separate, separately licensed module
- **Sudo** - Controls and authorizes sudo commands executed during SSH sessions

Note

Policies can trigger various actions depending on their type:

- sending e-mail message,
- sending push notifications to Fudo Officer,
- sending SNMP TRAP notification,
- pausing connection,
- terminating connection,
- blocking the user,
- allowing sudo commands matching created regular expressions (Sudo policies).

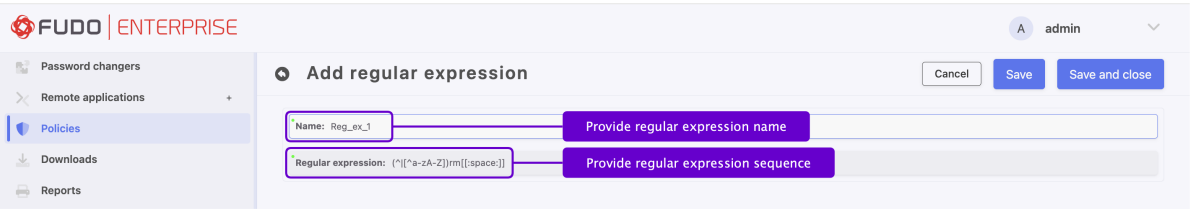
10.8.1 Regular Expression-Based Policy

Note

Fudo Enterprise supports POSIX extended regular expression.

Follow the steps to configure a regular expression-based policy:

1. Select *Management* > *Policies*.
2. Select *Regular expressions* tab.
3. Click *+ Add regular expression*.
4. Enter pattern name.
5. Define the pattern itself.



Note

- Patterns can be defined as regular expressions.
- Fudo Enterprise does not recognize expressions which use backslash character, e.g. `\d`, `\D`, `\w`, `\W`.

6. Repeat steps 3-5 to define additional patterns.
7. Click *Save and close*.

Note

Regular expressions examples

Command `rm`

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

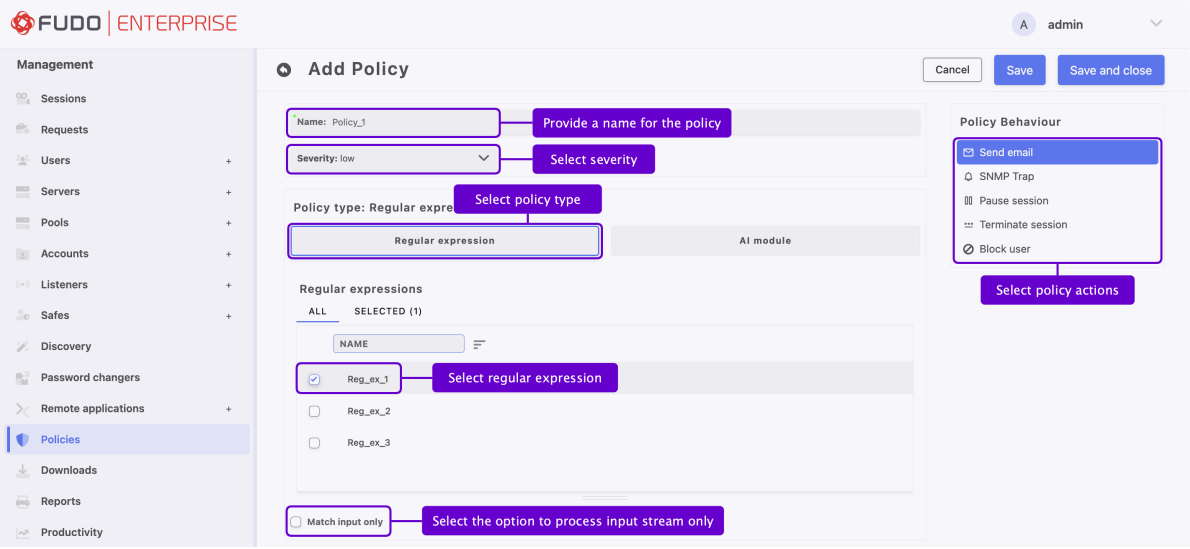
Command `rm -rf` (*also* `-fr`; `-Rf`; `-fR`)

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

Command `rm file`

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

8. Go back to *Policies* tab.
9. Click *Add policy*.



10. Enter policy name.
11. Select policy severity.

Note

Severity parameter value is included in the email notification message.

12. Click the *Regular expression* button in the *Policy type* section.
13. In the *Regular expressions* field, select the previously created monitoring pattern.
14. Select the *Match input only* option to process input stream only.

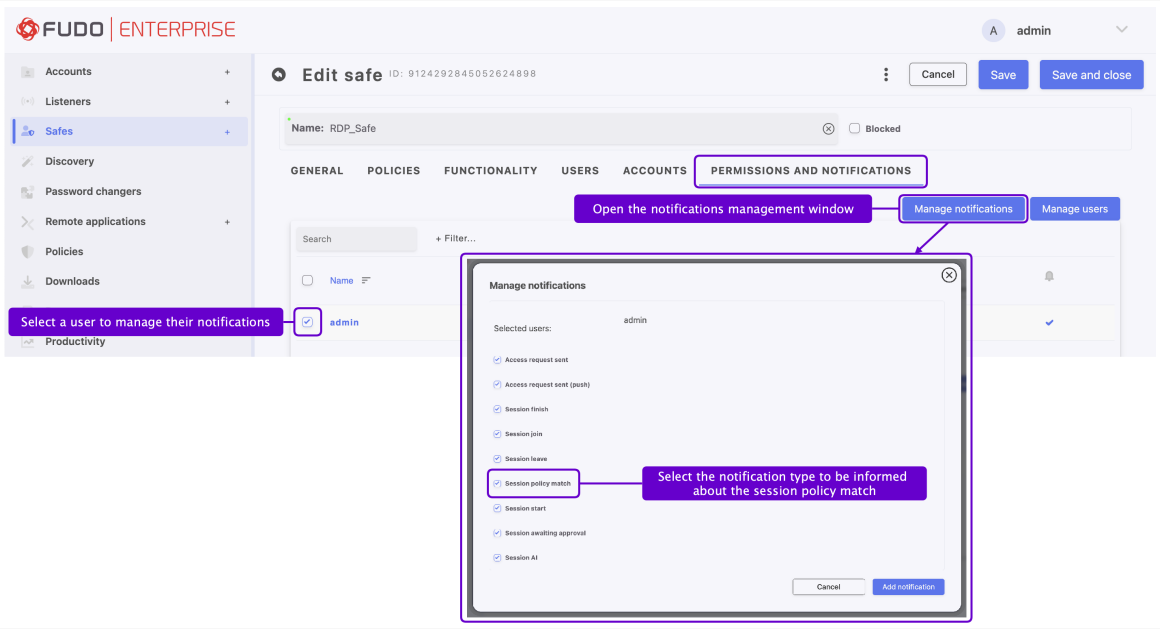
Note

In RDP, VNC and MySQL protocols only input data is processed.

15. In the *Policy Behaviour* field, select desired actions to be taken:
    - *Send email* - send email notification to system administrator,
    - *SNMP Trap* - send SNMP TRAP notification,
    - *Pause session,*
    - *Terminate session,*
    - *Block user.*

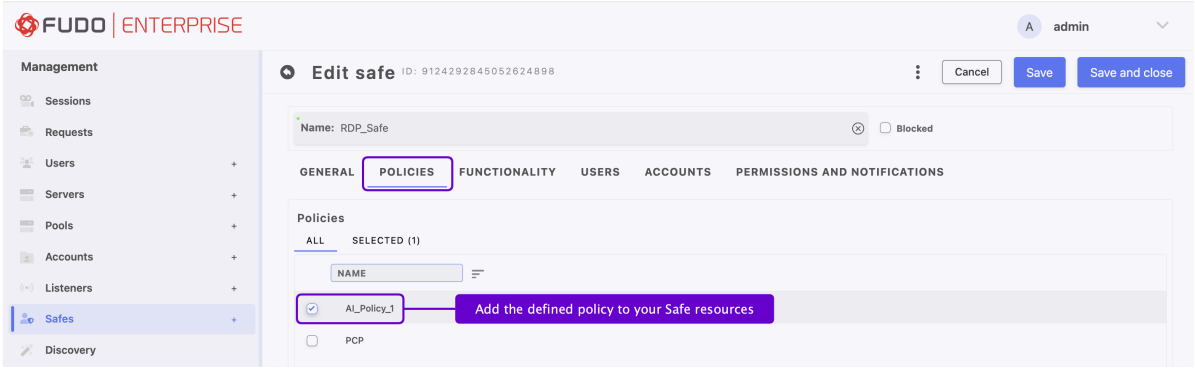
Note

- Sending email notifications requires configuring and enabling *notification service* as well as *Session policy match* notification enabled in *safe configuration*.



- Sending SNMP TRAP notifications requires configuring the SNMPv3 TRAP in the *System* tab. Check the *SNMP* page for more information.
- Note that blocking the user automatically terminates the connection.

16. Click *Save*.
17. After defining a policy, assign it to a *safe* that is used to establish connections to servers.
    - Select *Management* > *Safes*.
    - Edit the selected safe by clicking on its name.
    - Go to the *Policies* tab and select the policy created in the previous step.
    - Click *Save*.



Related topics:

- *Artificial Intelligence (AI)*
- *AI Behavioral Analysis in Sessions*
- *Safes*
- *Terminating connection*
- *Notifications*
- *Security*

10.8.2 Ai Module-Based Policy

In order to configure an AI module-based policy, proceed as the following states:

1. Select *Management* > *Policies*.
2. Click *+ Add Policy*.
3. Provide a name for the policy.
4. Select the Severity. Severity parameter value is included in the email notification message and in the *Events log* with the `FSW0284` code.
5. In the *Policy type* section, select the *AI module* button.
6. Select `min`, `avg` (default) or `max` option for the *Threat Probability Threshold* field and provide the value.

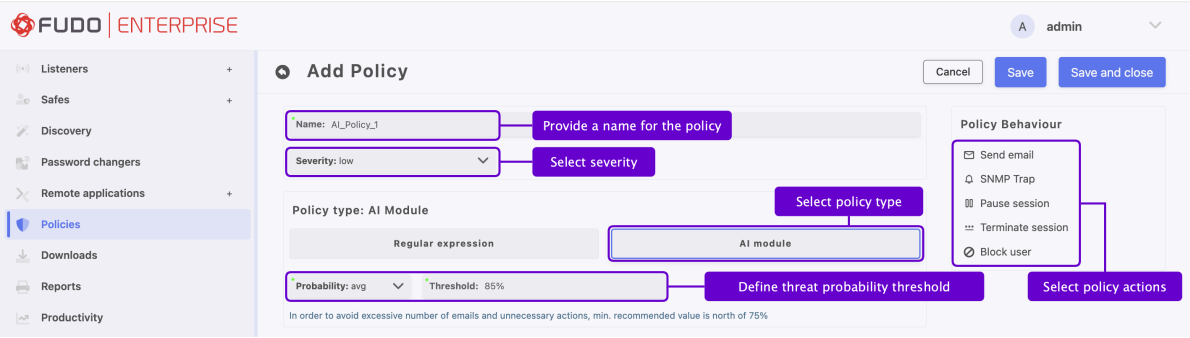
Note

Values for the *Threat Probability* metrics are calculated by the *AI models* for each session segment. The segment evaluations are averaged per model (e.g. Mouse Biometric, Keyboard Biometric) creating a model Threat Probability, thus the AI model delivers one Threat Probability per model for the whole session. These values are used in the policy and the policy actions can be applied to the minimum, average or maximum value of model Threat Probabilities.

In practice, if an administrator wants to decrease sensitivity of the policy so that it reacts to breaching a given threshold by **all the models**, the Threat Probability Threshold should be set to `minimum`. If the situation requires the policy to be more sensitive and react to the threshold breaching by **at least one model**, then the Threat Probability Threshold should be set to `maximum`.

Default value for the Threat Probability Threshold is `average`.

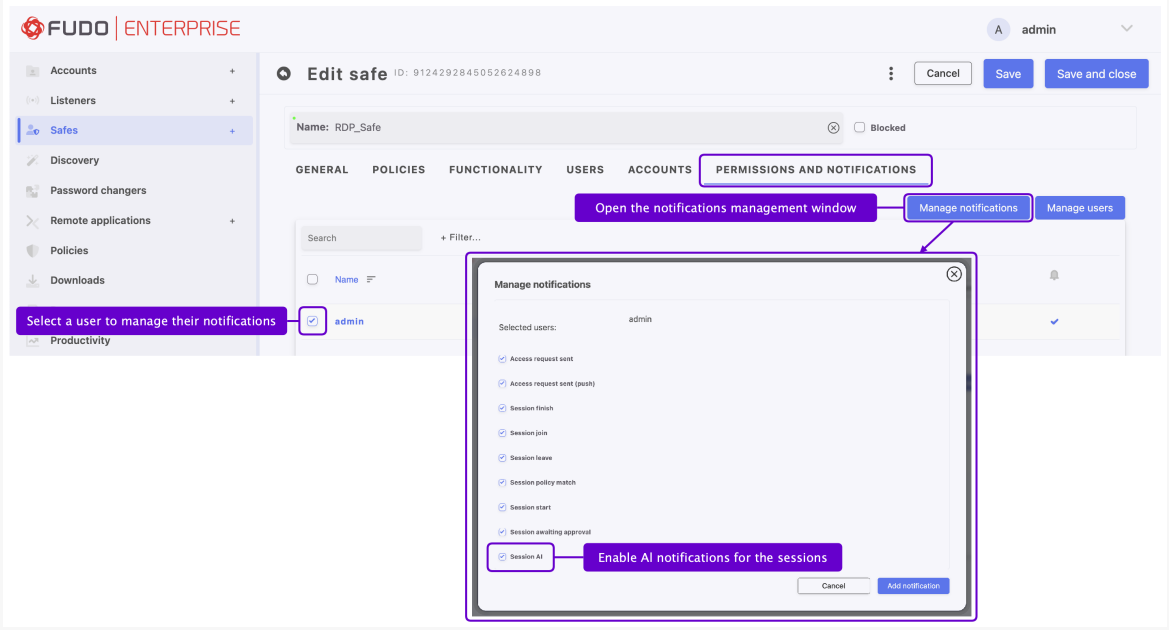
In order to avoid an excessive number of emails and unnecessary actions, min. recommended value is above 75%.



7. Select the actions that will be performed when the policy is breached:
   - send email notification to system administrator,
   - send SNMP TRAP notification to the receiver,
   - pause connection,
   - terminate connection,
   - block user.

Note

- Sending email notifications requires configuring and enabling *notification service* as well as *Session AI* notification enabled in safe configuration.



- Sending SNMP TRAP notifications requires configuring the SNMPv3 TRAP in the System tab. Check the *SNMP* page for more information.

Warning

If SNMP TRAP service is not configured, all notifications on policy violation will be discarded but other options related to the session management will work.

8. Click *Save*.

10.8.3 Ai Module-Based Policy Examples

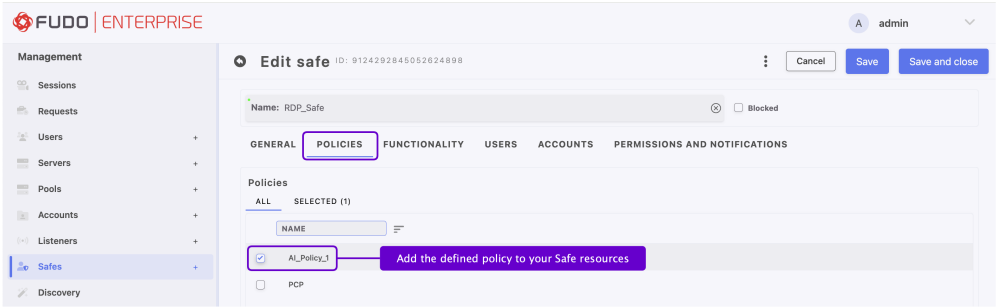
Example 1. Sending SNMP TRAP notifications about suspicious sessions.

To configure the policy to send SNMPv3 TRAP notifications about suspicious sessions, follow the procedure:

1. Create a user for SNMPv3 service:
   - Select *User Management* > *Users*.
   - Create a new one.
   - Enter Login.
   - Choose the `service` in the *Role* field.
   - Select `Static password` in the *Authentication* section and provide your password.
   - Go to the *More* tab, to the *SNMP* section, and define the settings:
     - Enable SNMP.
     - Select `SHA` or `MD5` in the *Authentication Method* field.
     - Select *AES* or *DES* in the *Encryption* field.
   - Click *Save*.
2. Configure SNMPv3 TRAP:
   - Select *Settings* > *System*.
   - Scroll down to the *Maintenance and supervision* section.
   - Select the *SNMPv3 TRAP* option.
   - Configure the SNMPv3 TRAP *server address* and *port*.
   - Select the user with `service` role, created in step 1.
   - Click *Save*.
3. Create policy:
   - Select *Management* > *Policies*.
   - Click *+ Add policy*.
   - Provide a ame for the policy.
   - Select `AI module` in the *Policy type* field.
   - Select the option of the *Threat Probability Threshold* (e.g. `avg`) and add its value (e.g. `90%`).
   - Select the *SNMP TRAP* option in the *Actions* field.

- Click *Save*.

4. Assign the policy to a *safe* that is used to establish connections to servers.
    - Select *Management* > *Safes*.
    - Edit the selected safe by clicking on its name.
    - Go to the *Policies* tab and select the policy created in the previous step.
    - Click *Save*.



Example 2. Terminating suspicious sessions when the Threat Probability Threshold is reached.

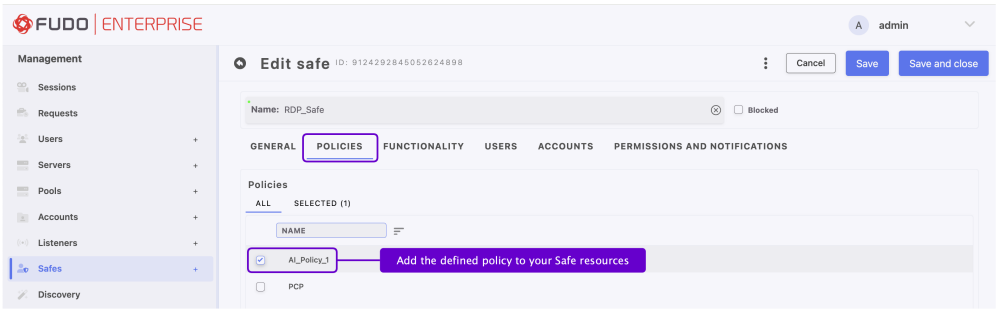
To configure the policy to terminate suspicious sessions when the Threat Probability Threshold is reached, follow the procedure:

1. Create policy:
    - Select *Management* > *Policies*.
    - Click *+ Add policy*.
    - Provide a ame for the policy.
    - Select `AI module` in the *Policy type* field.
    - Select the option of the *Threat Probability Threshold* (e.g. `avg`) and add its value (e.g. `90%`).
    - Select the *Terminate session* option in the *Actions* field.
    - Click *Save*.

Note

For harsh actions like pausing or terminating a session or blocking a user it's advised to use higher max thresholds to minimize consequences of false positives.

2. Assign the policy to a *safe* that is used to establish connections to servers.
    - Select *Management* > *Safes*.
    - Edit the selected safe by clicking on its name.
    - Go to the *Policies* tab and select the policy created in the previous step.
    - Click *Save*.



Related topics:

- *Artificial Intelligence (AI)*
- *AI Behavioral Analysis in Sessions*
- *Safes*
- *Terminating connection*
- *Notifications*
- *Security*

10.8.4 AI Session Summary Policy

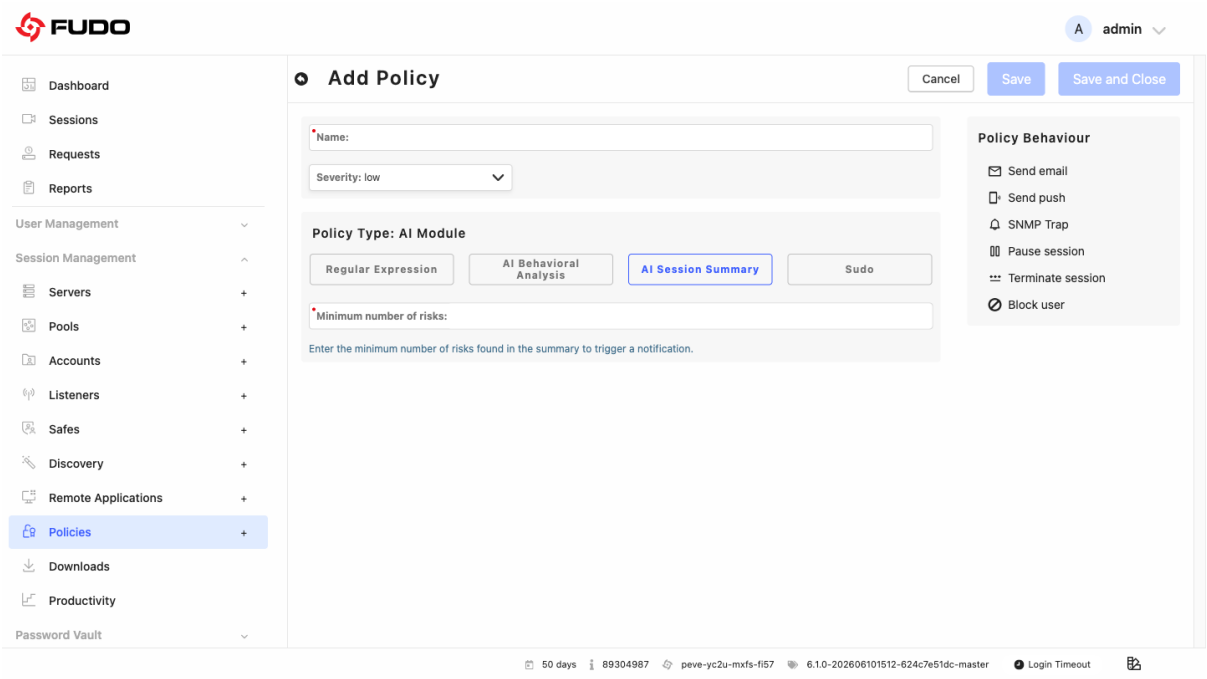
The AI Session Summary policy type monitors AI-generated session summaries for risk indicators and triggers actions when specified risk thresholds are detected. This policy works in conjunction with the AI Session Summary feature (configured separately) to provide automated response to suspicious activities identified in session summaries.

> **Note**
>
> This policy type requires the AI Session Summary feature to be enabled and configured. The summaries themselves are generated independently; this policy only monitors them for risk conditions. See *AI Session Summary* for summary generation configuration.

10.8.4.1 Policy Configuration

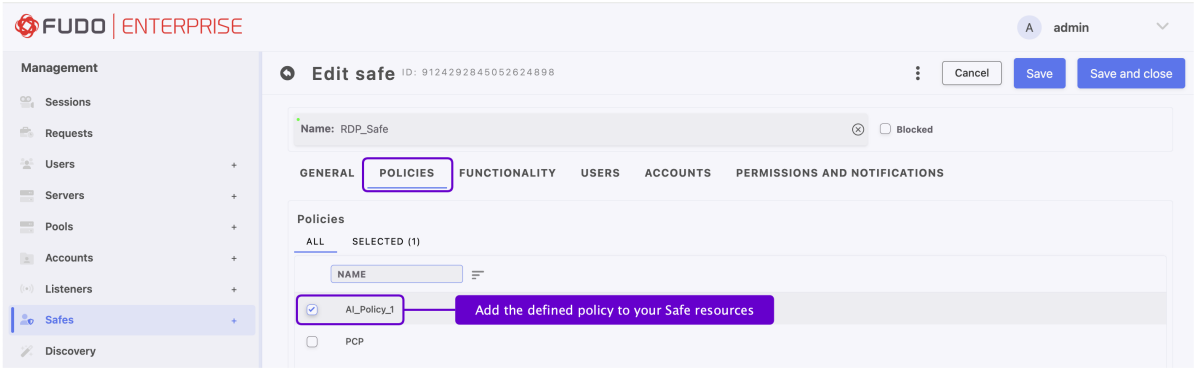
Follow these steps to configure an AI Session Summary policy:

1. Select *Management* > *Policies*.
2. Click *+ Add Policy*.
3. Provide a name for the policy.
4. Select the Severity (low, medium, high, critical). The severity parameter value is included in email notifications and in the Events log.
5. In the *Policy type* section, select *AI Session Summary*.



6. Configure the risk detection thresholds:
   - **Risk Level Threshold** - Minimum risk level to trigger the policy (low, medium, high, critical)
   - **Keyword Detection** - Specific keywords or patterns to monitor in summaries
   - **Activity Categories** - Types of activities to flag
   - **Anomaly Score** - Threshold for anomaly detection based on AI analysis
7. Configure trigger conditions:
   - **Match Type** - ANY (trigger on any condition) or ALL (require all conditions)
   - **Time Window** - Period for evaluating conditions
   - **Occurrence Count** - Number of detections required to trigger
8. Configure Policy Behaviour - select actions to take when risk conditions are detected:
   - Send email - Send notification with risk details to administrators
   - Send push - Send immediate alert to Fudo Officer mobile app
   - SNMP Trap - Send SNMP notification
   - Pause session - Temporarily pause the session for review
   - Terminate session - Immediately end the session
   - Block user - Prevent further access by the user
9. Click *Save*.
10. After defining a policy, assign it to a *safe* that is used to establish connections to servers.
    - Select *Management* > *Safes*.
    - Edit the selected safe by clicking on its name.

- Go to the *Policies* tab and select the AI Session Summary policy created in the previous step.
- Click *Save*.



10.8.4.2 How It Works

The AI Session Summary policy operates through the following workflow:

1. **Summary Generation** - AI generates session summaries based on session activities (configured separately)
2. **Risk Analysis** - The AI analyzes summaries for risk indicators and anomalies
3. **Policy Evaluation** - This policy evaluates the risk analysis against configured thresholds
4. **Action Triggering** - When thresholds are exceeded, configured actions are executed
5. **Alerting** - Administrators receive notifications with risk details and recommended actions

Related Topics

- *AI Session Summary*
- *Policies*
- *Ai Module-Based Policy*
- *AI Behavioral Analysis in Sessions*

10.8.5 Live Session Analysis Policy [BETA]

The Live Session Analysis policy type acts on the findings reported by the AI analysis agents while a session is still running. The policy fires when a single agent reports the configured number of findings at or above the selected severity, and can then notify the administrator, pause or terminate the session, or block the user.

Note

This policy type requires *AI Live Session Monitoring [BETA]* to be enabled and configured. The findings themselves are produced by the analysis agents; this policy only reacts to them.

Like the feature it depends on, this policy type is available in Fudo Enterprise as a **beta version**. Once live session monitoring leaves the beta stage, it will be delivered as a **separate module**, and the availability of this policy type will depend on your *license*.

Important

The policy acts on the verdict of an AI model. Before enabling the *Pause session*, *Terminate session* or *Block user* action, verify on non-critical safes how the selected agents judge the activity typical of your environment.

10.8.5.1 Policy Configuration

1. Select *Management* > *Policies*.
2. Click *+ Add Policy*.
3. Provide a name for the policy.
4. Select the Severity. The severity parameter value is included in email notifications and in the Events log.
5. In the *Policy type* section, select *Live Session Analysis*.
6. Set *Minimum finding severity* - the policy reacts to findings at this level or higher.
7. Set *Minimum number of findings* - how many such findings a single agent must report during one session.
8. Configure Policy Behaviour - select the actions to take:
   - Send email - send a notification with the finding to administrators
   - Send push - send an alert to the Fudo Officer mobile app
   - SNMP Trap - send an SNMP notification
   - Pause session - pause the session for review
   - Terminate session - end the session immediately
   - Block user - prevent further access by the user
9. Click *Save*.
10. Assign the policy to a *safe* used to establish the monitored connections.

- Select *Management* > *Safes*.
- Edit the selected safe by clicking on its name.
- Go to the *Policies* tab and select the Live Session Analysis policy created in the previous step.
- Click *Save*.

Note

The *Minimum finding severity* field offers `medium` and `high` only. Findings of a lower level are not stored, so a lower threshold could never be reached.

Warning

Findings are counted **per agent** - the findings of different agents are never added together. A policy requiring three findings is satisfied when one agent reports three of them, not when three agents report one each. Agents have different remits, so their findings are not comparable.

Note

A policy that has already fired stays quiet until a more serious finding appears in the same session. Only then are the actions executed again, so a single session does not generate a stream of identical alerts.

Findings that arrive after the session has ended can no longer pause or terminate it. In that case Fudo Enterprise performs the actions that remain meaningful - the notification and blocking the user.

10.8.5.2 Notifications

Firing of the policy can be reported with the *Live Session Analysis* notification, which is sent when a live analysis policy fires on an agent's findings during a session. The message contains the finding itself: the agent, the severity and the summary of what was detected.

Related Topics

- *AI Live Session Monitoring [BETA]*
- *Policies*
- *Sessions*

10.8.6 Sudo Command Control Policy

Fudo Enterprise 6.1 introduces sudo command control for Linux environments. The Sudo policy type enables Fudo Enterprise to authorize sudo commands executed by users during SSH sessions.

Important

- This policy type works only with SSH sessions.
- The Fudo sudo plugin must be installed on target Linux systems where sudo command control should be enforced. The plugin is available as a separate download from GitHub.

10.8.6.1 How Sudo Command Control Works

When sudo command control is enabled:

1. **Command Interception** - The Fudo sudo plugin intercepts all sudo commands on the target system
2. **Policy Evaluation** - Commands are sent to Fudo Enterprise for evaluation against configured policies

3. **Authorization Decision** - Commands matching whitelist expressions are allowed; others are blocked
4. **Audit Trail** - All sudo command attempts are logged with full context and shown in the **Commands** list of the session player (see *Viewing Sessions*)
5. **Real-time Notifications** - Administrators receive alerts based on policy configuration

10.8.6.2 Setting up Fudo for Sudo Control

Complete these steps in Fudo Enterprise to enable sudo command control:

Step 1: Configure API Access

Create user with an *API Key* authentication method and ALL required privileges:

- `user-read`
- `policy-read`
- `regexp-read`
- `session-read`
- `sudo-approval`

> **Warning**
>
> Missing any single privilege causes every sudo command to be denied.

Step 2: Configure Server Infrastructure

1. Add the target Linux server:
   - Navigate to *Session Management* > *Servers*
   - Click *+ Add server*
   - Select SSH protocol
   - Configure server connection details
2. Create an Account on that server:
   - Navigate to *Session Management* > *Accounts*
   - Click *+ Add account*
   - Select the server created in step 1
   - Configure account credentials
3. Create a Safe:
   - Navigate to *Session Management* > *Safes*
   - Click *+ Add safe*
   - Link the Fudo user to the account created in step 2

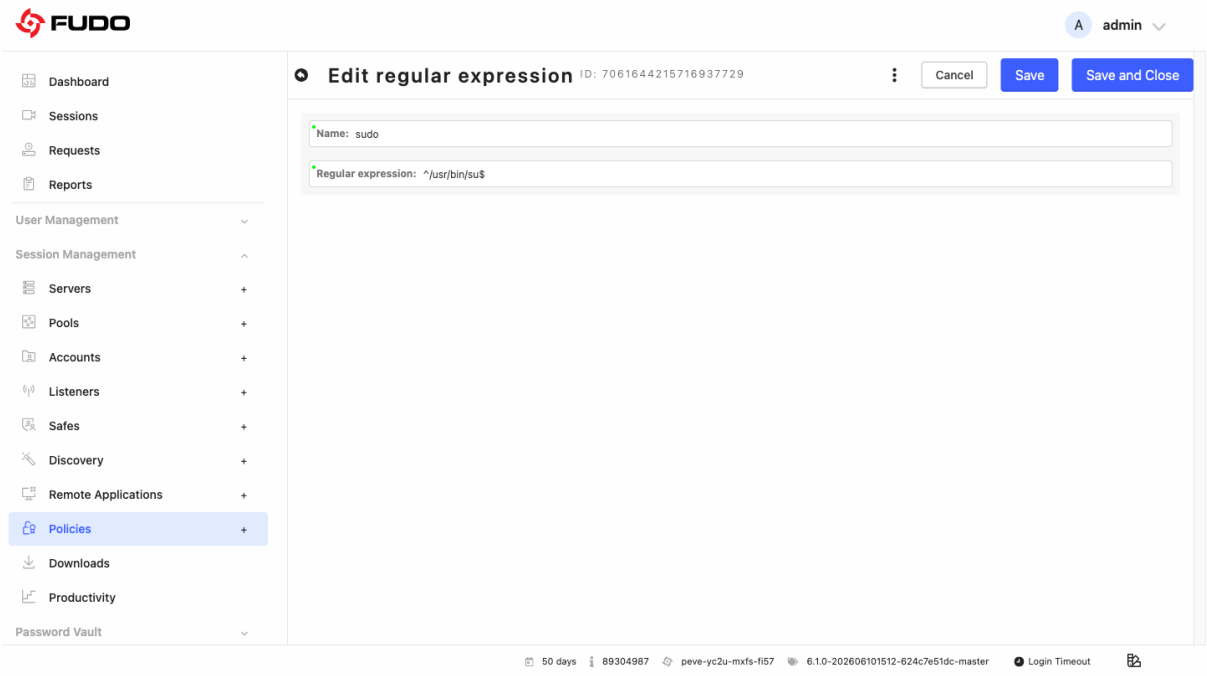
10.8.6.3 Sudo Policy Configuration

Important

Before creating a Sudo policy, you must first define regular expressions that will match the sudo commands you want to allow. Sudo policies work exclusively with a whitelist approach - only commands matching the defined expressions will be permitted. The regular expressions must specify full binary paths (e.g., `^/usr/bin/sudo`, `^/usr/bin/su$`).

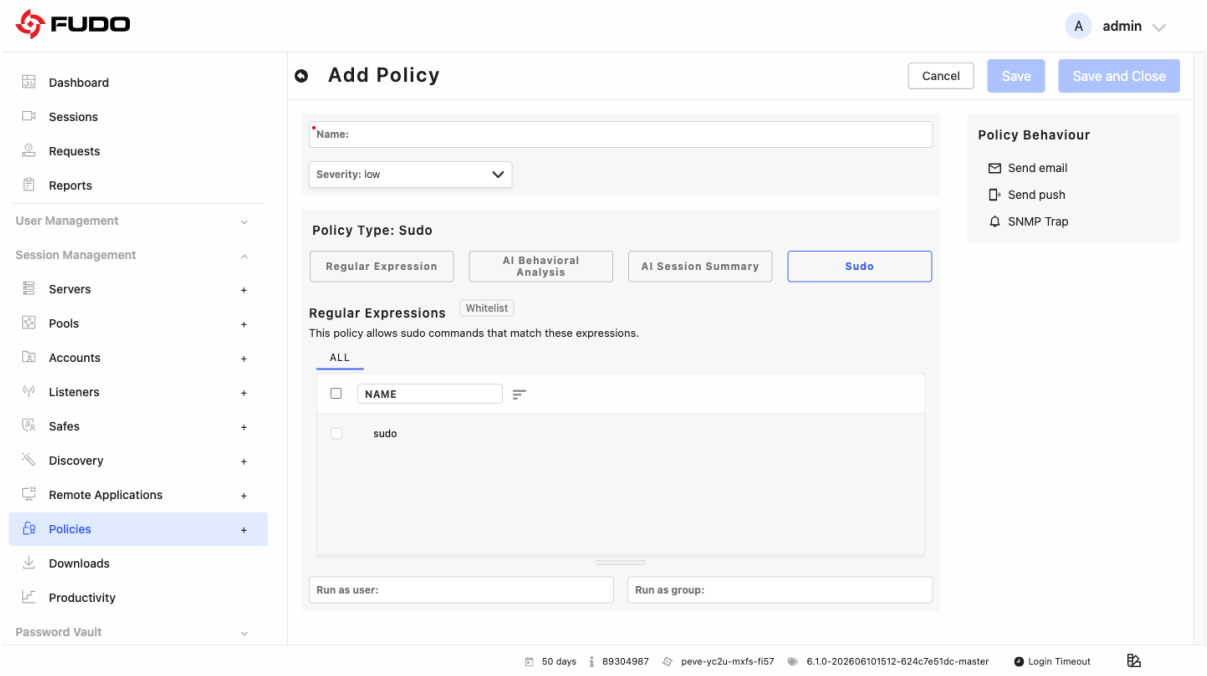
Create regular expressions:

1. Select *Session Management* > *Policies*.
2. Navigate to the *Regular Expressions* tab.
3. Click *+ Add regular expression*.
4. Enter a name for the expression (e.g., `sudo_systemctl`, `sudo_apt_update`).
5. Define the pattern for allowed sudo commands. **Important:** Use full binary paths in your patterns (e.g., `^/usr/bin/su$`, `^/usr/bin/sudo`).
6. Click *Save*.



After creating the necessary regular expressions, follow these steps to configure a Sudo policy:

1. Select *Session Management* > *Policies*.
2. Return to the *Policies* tab.
3. Click *+ Add Policy*.
4. Provide a name for the policy.
5. Select the Severity (low, medium, high, critical). The severity parameter value is included in email notifications and in the Events log.
6. In the *Policy type* section, select *Sudo*.



7. Configure the Regular Expressions:
   - The policy type is **Whitelist** - sudo commands that match the selected expressions will be **allowed**
   - Select from the previously created regular expressions that define allowed sudo commands
   - Only expressions marked with checkboxes will be used in the policy
   - If no expressions are available, you must first create them in the Regular Expressions tab
8. Configure command execution context (optional):
   - **Run as user** - Specify which user the sudo command can run as (e.g., root, www-data)
   - **Run as group** - Specify which group the sudo command can run as
9. Configure Policy Behaviour - select actions to take when a sudo command is executed:
   - Send email - Send email notification to administrators
   - Send push - Send push notification to Fudo Officer mobile app
   - SNMP Trap - Send SNMP TRAP notification
10. Click *Save*.

Note

Fudo Officer 2.3.32 and later can notify users when sudo commands matching the configured policy are executed. This provides real-time visibility into privileged operations across your infrastructure.

10.8.6.4 Sudo Plugin Installation

The Fudo sudo plugin is required on each Linux system where you want to enforce sudo command control.

Requirements

- Target Linux server with sudo 1.9 or newer (verify with `sudo -V`)
- Root access on the target server

> **Warning**
>
> **Critical Installation Precautions:**
>
> 1. **Create a VM snapshot first** - A misconfigured installation will deny ALL sudo commands on the server. A snapshot is the safest rollback method.
> 2. **Keep a second root SSH session open** - Maintain a second SSH session logged in as root during installation. If the plugin breaks sudo, this is your only way to revert without restoring the snapshot.
> 3. **The plugin blocks ALL non-Fudo sudo** - Local console sudo and direct (non-Fudo) SSH sudo are always denied as no Fudo session mapping exists for them. This is by design.
> 4. **Sudo 1.9+ required** - The plugin requires sudo version 1.9 or newer. Ubuntu 20.04 LTS ships with sudo 1.8.31 and is incompatible. Verify your version with `sudo -V` before installation.

Setting Up the Target Linux Server

Complete the following steps in the specified order.

> **Warning**
>
> Steps 1 and 2 are **required** recovery safeguards and must not be skipped.

1. **Open a second SSH connection** to the target server as root and keep it open. This connection provides a recovery path if the plugin installation or configuration fails.
2. **Create a VM snapshot.**
3. Check the installed sudo version:

   ```
   sudo -V | head -1
   ```

   The output must show sudo version 1.9.x or later.
4. Copy the plugin file to the sudo plugin directory used by your Linux distribution:
   - Ubuntu/Debian: `/usr/lib/sudo/`
   - RHEL/Rocky/CentOS: `/usr/libexec/sudo/`

   Copy the `fudo_approval.so` file to the appropriate directory and make it readable by all users.

5. Register the plugin in `/etc/sudo.conf` by adding the following line:

```
Plugin fudo_approval fudo_approval.so api_url=https://<fudo_ip>
```

6. Store the API key in `/etc/fudo/approval.key`.

   The plugin strictly validates the key file ownership and permissions. The file must be owned by root and its permissions must be set to exactly 0600. Otherwise, sudo commands are denied.

7. Add the Fudo TLS certificate to the system trust store.

   Use the certificate trust mechanism required by your distribution, for example:

   - Debian-based distributions: `update-ca-certificates`
   - RHEL-based distributions: `update-ca-trust`

8. Verify the configuration:

```
sudo -V
```

   The `fudo_approval` plugin should appear in the sudo plugin list.

Warning

Do not close the recovery SSH connection until the plugin is visible in the sudo plugin list and sudo command execution has been verified.

Warning

The sudo plugin must be properly configured and tested before deploying to production systems. Misconfiguration can prevent legitimate sudo commands from executing.

Note

Direct sudo commands on the target server (outside of Fudo sessions) will always be denied. This is intentional - only commands executed through Fudo Enterprise sessions can be authorized.

Related topics:

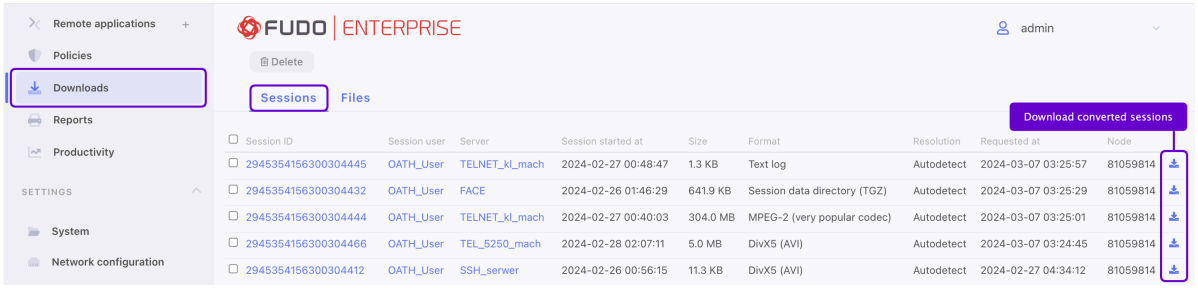
- *Policies*
- *Regular Expression-Based Policy*
- *Notifications*

10.9 Downloads

The **Downloads** tab allows for tracking the conversion progress of session recordings and files transferred during SFTP sessions, previously selected for download.

10.9.1 Sessions

Fudo Enterprise allows converting stored session data to one of supported formats. The **Sessions** tab is designated for managing session recordings that were previously selected for download in Sessions. For detailed instructions on how to export a session, and available file formats, please refer to the *Exporting Sessions* section of this manual.



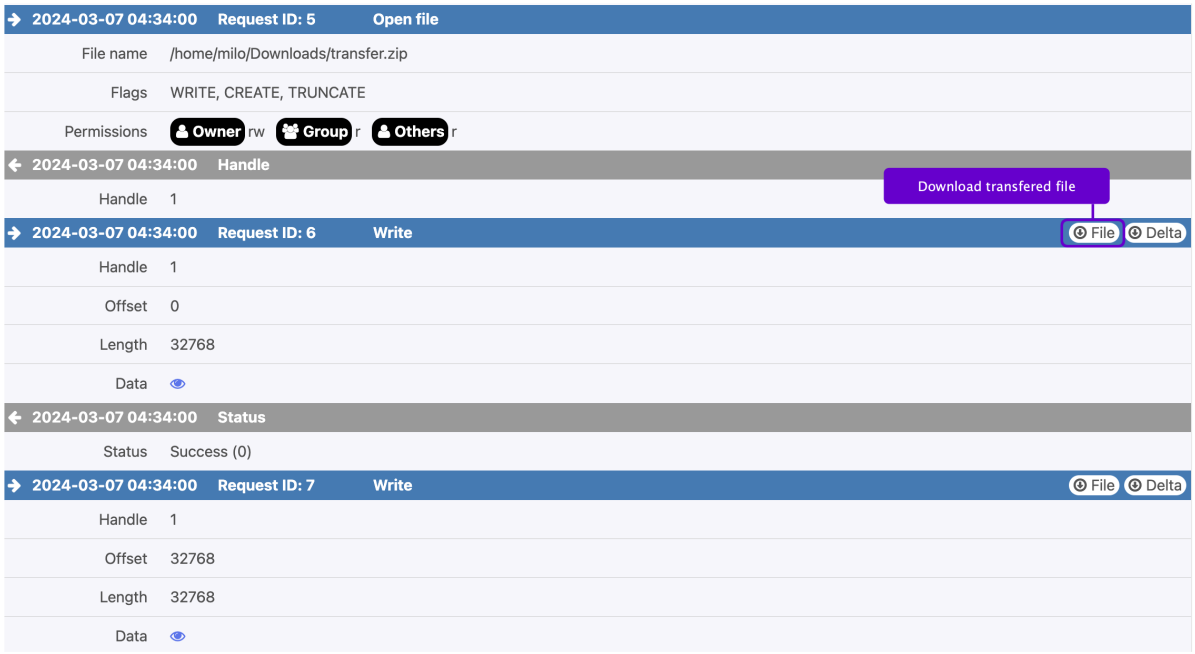
10.9.2 Files

The **Files** tab is designated for managing the downloads of large files that originate from recorded sessions via the SFTP protocol. If the selected file exceeds the 50 MB threshold, it undergoes an encoding process and subsequently appears in the **Files** tab, ready for download. Files smaller than 50 MB are directly downloaded through the browser without encoding.

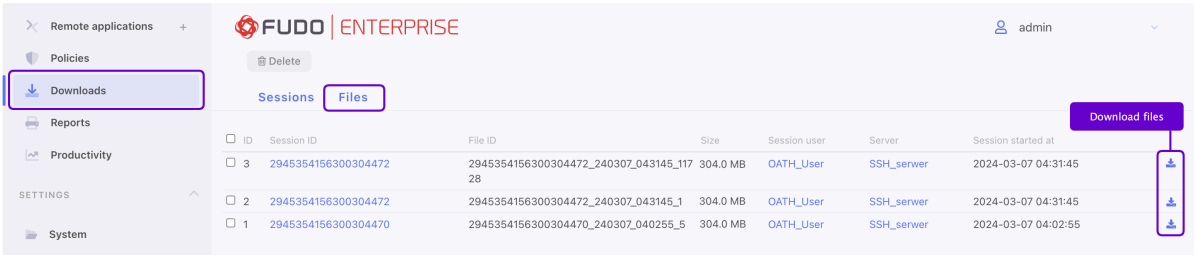
To download a file transfered during SFTP session, users must initiate the download from the session player interface. To view a session, proceed as follows:

1. Select *Select* > *Sessions*.
2. Find desired SFTP session and click the play icon next to it.
3. In the session player window, navigate through the SFTP session history to locate the desired file for download, then click the **File** button to initiate the encoding process.

> **Note**
>
> To ensure the download of the entire file, please use the **File** button.



4. Select *Management* > *Downloads*.
5. Go to the **Files** tab.
6. Click the *Download* icon to download encoded file.



Related topics:

- *Exporting Sessions*
- *Sessions*

10.10 Productivity

Fudo Enterprise features a productivity analysis component which tracks users' activities and can provide precise information on activity and idle times.

> **Note**
>
> Productivity analysis can be disabled at the customer's request. This allows compliance with legal requirements in countries that restrict the monitoring of employee productivity. The feature is disabled through the license file — it is enabled by default. To obtain a license file with productivity analysis disabled, contact the Fudo Presales team.
>
> When productivity analysis is disabled, the following are not available:
>
> - the **Productivity** tab and all of its subpages,

- the **Activity** column in the sessions list, along with filtering and sorting by this value,
- the **Activity** column in the system report,
- the `productivity-read` privilege in role configuration.

Refer to the *Licensing Model and License Limits* section for more information.

10.10.1 Overview

Overview displays data on users' activity in selected time interval.

Note

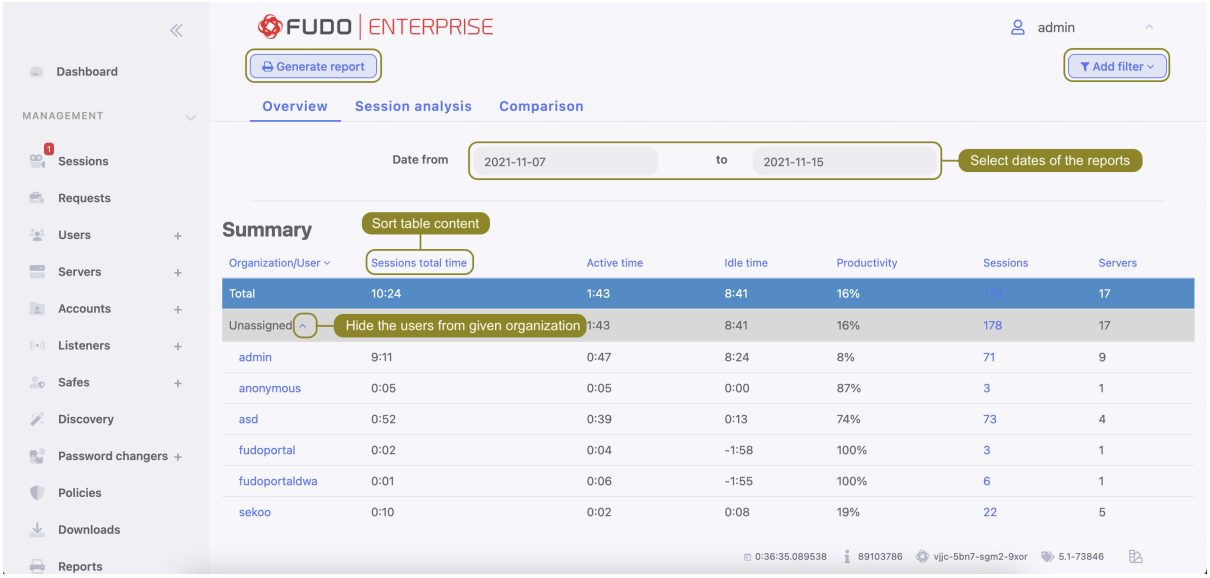
Activity rating is based on the user's interaction with the monitored system. Fudo Enterprise divides the time into 60 seconds long time intervals and monitors the activity within the interval. Lack of any actions in a given time period accounts such as a non-productive time.

To view the users' activity rundown, proceed as follows.

1. Select *Management* > *Productivity*.
2. Select the *Overview* tab.
3. Define the users' list filtering.
4. Click *Generate report* to generate rundown of the displayed data in HTML, CSV or PDF format.

Note

The report can be accessed in the *Reports* section.



Related topics:

- *Productivity analysis - Sessions analysis*

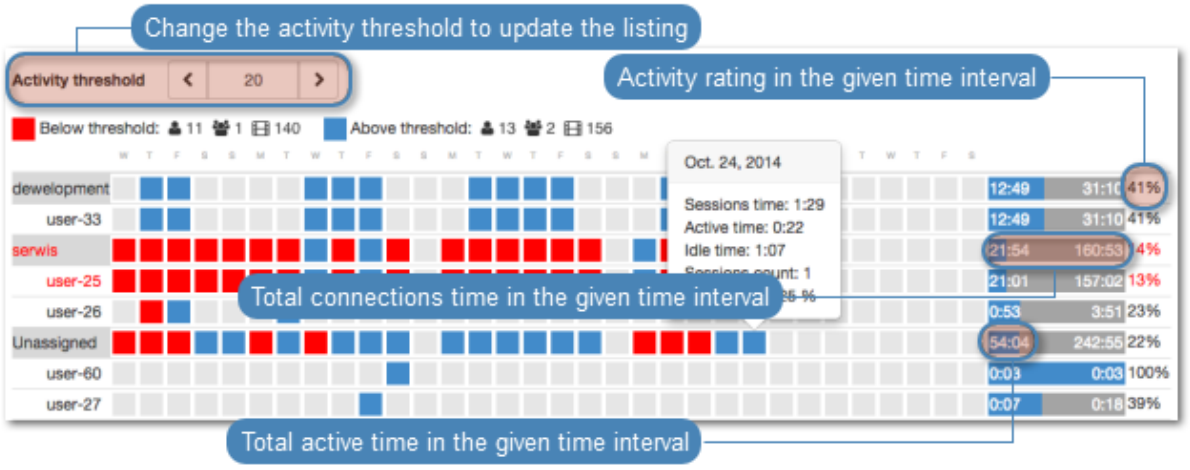
- *Productivity analysis - Comparison*
- *Sessions*

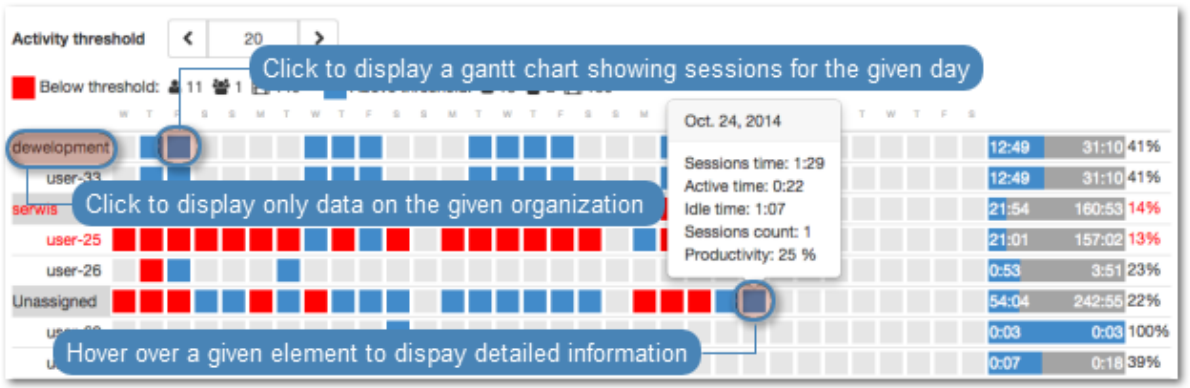
10.10.2 Sessions Analysis

Sessions analysis shows in detail users/organizations productivity in the given time period. The activity threshold parameter allows identifying sessions, users and organisations which do not exceed the required user activity rating and helps establishing the threshold value attainable for a given number of users or sessions. **Users activity rating**

Users activity rating allows identifying sessions which do not exceed the required user activity level. Further material analysis helps determining the reason for low activity in the given session and draw relevant conclusions.

> **Note**
>
> The listing does not cover time periods longer than 31 days. In case the defined time interval is longer than that, only data from the first 31 days is presented.





Related topics:

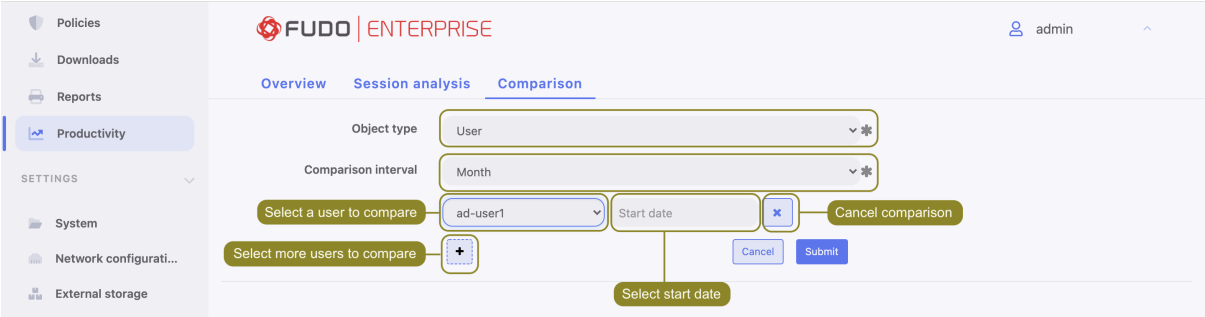
- *Productivity analysis - Overview*
- *Productivity analysis - Comparison*

10.10.3 Activity Comparison

Productivity module enables comparing users/organizations activity in given time periods.

To compare users/organizations, proceed as follows.

1. Select *Management* > *Productivity*.
2. Select the *Comparison* tab.
3. Select object types being compared: `User` or `Organization`.
4. Select the time interval: `Month`, `Quarter`, `Half year`, or `Year`.
5. Add objects to the comparison and define starting date for each object.



6. Click *Confirm* to compare selected objects.

Related topics:

- *Productivity analysis - Sessions analysis*
- *Productivity analysis - Overview*
- *Sessions*

CHAPTER 11

Password Vault

11.1 Overview

Password Vault is a credential management module within Fudo Enterprise that extends traditional Privileged Access Management (PAM) capabilities. It provides encrypted storage, lifecycle management, controlled access, and full auditability of sensitive credentials and other secret data.

The module supports secure storage and management of:

- Passwords
- SSH keys
- X.509 certificates
- API keys
- Notes and structured secret data

Password Vault is designed for enterprise environments and supports hierarchical organization, role-based access control, time-limited access workflows, secret rotation, and full integration with other Fudo Enterprise components.

Key capabilities include:

- Multi-type secret storage
- Hierarchical collections (up to 5 levels)
- Role-based object rights with inheritance
- Just-in-Time access requests and approvals

- Secure secret sharing
- Complete audit trail and immutable history
- Integrated password and key generation
- Automated credential rotation

The following chapters describe the structural, security, and auditing components of the Password Vault module.

11.1.1 Architecture Overview – Security Model

Password Vault is built on a multi-layer security architecture designed to protect data at rest, in transit, and during processing.

Encryption

Data stored in the system is encrypted at rest using AES-256.

Communication between system components is protected using TLS encryption.

Secrets are decrypted only when required to perform an authorized operation.

Access Control

Access control is enforced through a two-layer model:

- Role-Based Access Control (RBAC) – defines who can manage collections and secrets and what operations they can perform on them in the Admin Panel.
- Access Policies – define the conditions and workflow rules for granting access to secrets, such as approvals and time limits, for users accessing secrets through User Access Gateway.

Key characteristics:

- Permission inheritance across collection hierarchy
- Policy override capability at lower levels
- Just-in-Time access requests

Access decisions are evaluated in real time and logged.

Audit

Note

- Operations on secrets (view, checkin / checkout) can be tracked in the **Password Vault** > **Secret Access** tab.
- To preview all logs related to Password Vault, go to the Event Logs tab.

The system tracks:

- Permission changes
- Access requests and approvals
- Checkout and checkin operations
- Secret usage events
- Rotation operations

> **Note**
>
> Each secret maintains immutable version history. To preview logs for a specific secret, edit the secret and open the Activity logs subtab.

11.1.2 Password Vault Structure

The logical structure of Password Vault is based on secrets and collections.

Secrets

A secret is an individual credential or confidential data object stored in encrypted form.

Supported secret types include:

- Password
- SSH key (RSA, ECDSA, Ed25519)
- X.509 certificate
- API key / token
- Encryption key
- Note

Each secret maintains immutable change history and supports access tracking.

> **Note**
>
> Availability of specific secret types depends on your *license*.

Collections

Collections provide hierarchical organization of secrets. They allow grouping of related credentials based on business logic, departments, systems, or environments.

Characteristics:

- Tree-based structure
- Maximum nesting depth: 5 levels

- Permission inheritance model
- Separate permission scope per collection

Collections are the primary boundary for access control enforcement.

Vault Scopes

Password Vault operates in two logical scopes:

- Personal Vault – individual user-managed secrets
- Organization Vault – centrally managed enterprise secrets

11.1.3 Event Logging and Audit Trail

Password Vault provides comprehensive logging and traceability for access to collections and secrets.

Logged events include:

- Authentication and authorization attempts
- Secret access (view, copy, download)
- Secret checkout and automatic checkin
- Secret generation events
- Password/key rotation operations
- Policy changes
- Administrative actions

> **Note**
>
> To preview all logs, go to the Event Logs tab. To preview logs for a specific secret, edit the secret and open the Activity logs subtab.

Checkout / Checkin Tracking

When a secret is checked out:

- The secret can be locked for exclusive use
- The operation is recorded with user identity, timestamp, and scope
- Automatic checkin may occur after inactivity timeout

All checkout and checkin events are stored in the audit trail.

Compliance Support

The audit functionality enables:

- Complete operational history
- Immutable change tracking
- External log forwarding (e.g., SIEM integration)

The audit trail ensures accountability of all privileged credential operations within the system.

11.2 Collections

11.2.1 Creating Collections

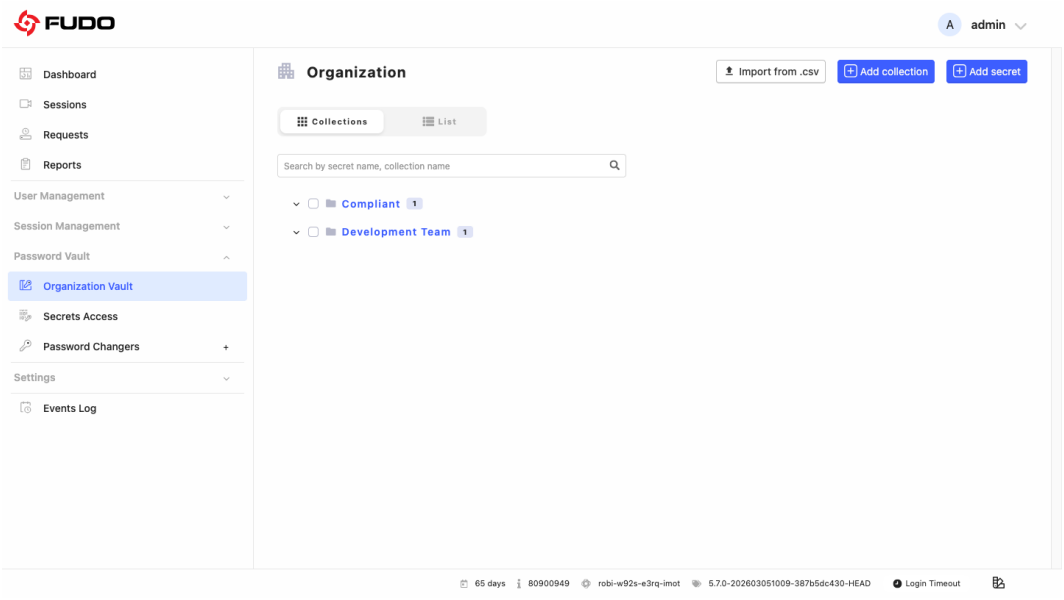
Collections in Password Vault allow you to organize and group secrets in a structured way. This helps with managing access permissions and keeping related secrets together.

Note

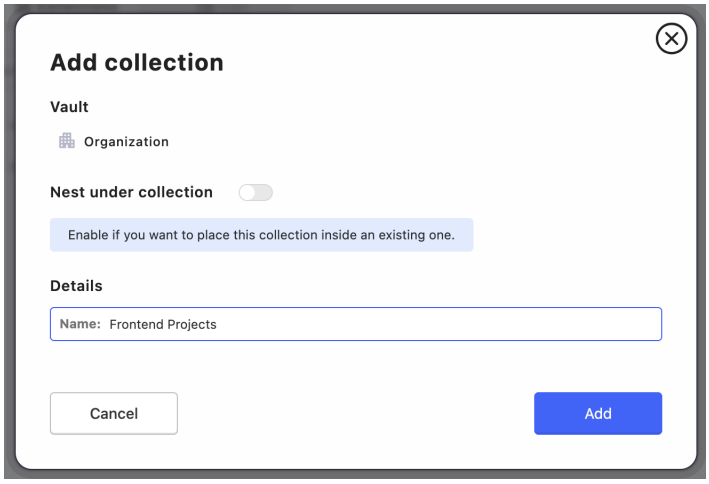
Collection Features:

- **Organization**: Collections help organize secrets by project, team, or purpose
- **Nested Structure**: Collections can be nested within other collections for hierarchical organization
- **Access Control**: Different permissions can be assigned to different collections

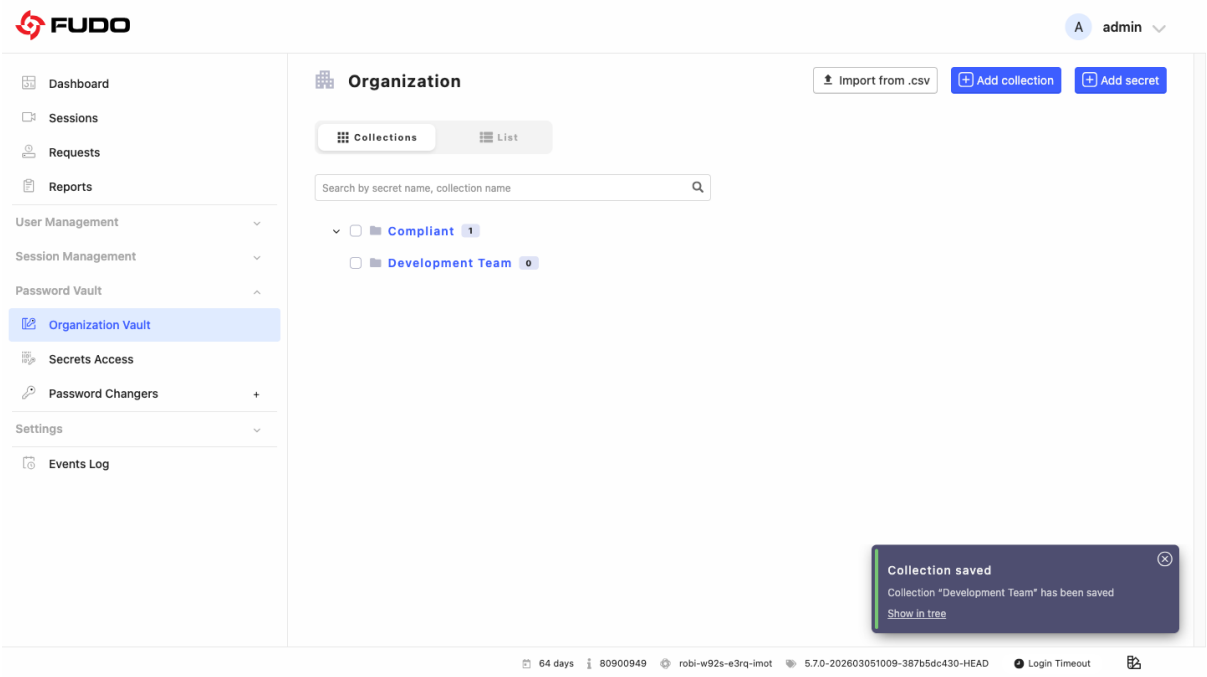
1. Select *Password Vault* > *Organization Vault*.
2. Click *+ Add collection*.



3. In the modal window, enter the collection name in the *Name* field.
4. Optionally, enable *Nest under collection* if you want to place this collection inside an existing one.
5. Click *Add* to create the collection or *Cancel* to abort.



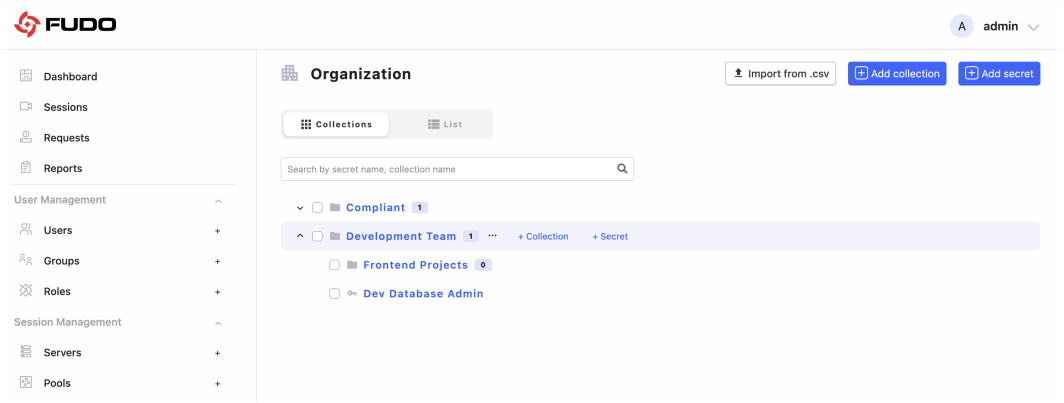
After successfully creating the collection, you will see a confirmation message and the new collection will appear in the collections list.



Alternative Creation Methods:

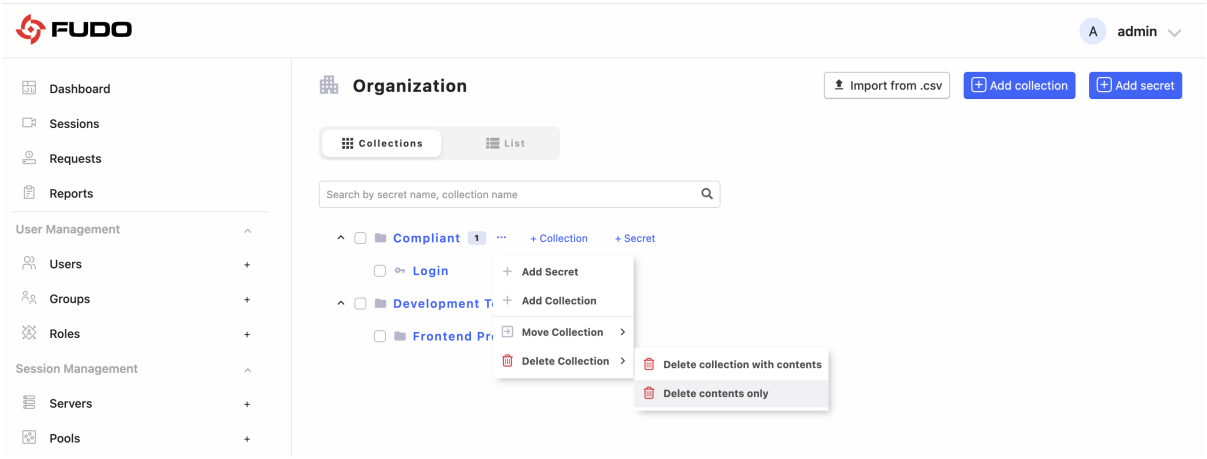
You can also create collections using the quick action menu:

1. Hover over an existing collection to reveal the action buttons
2. Click *+ Collection* to create a nested collection within the selected collection



Or use the three-dot context menu:

1. Hover over a collection and click the three dots (...) button
2. Select **Add Collection** from the context menu



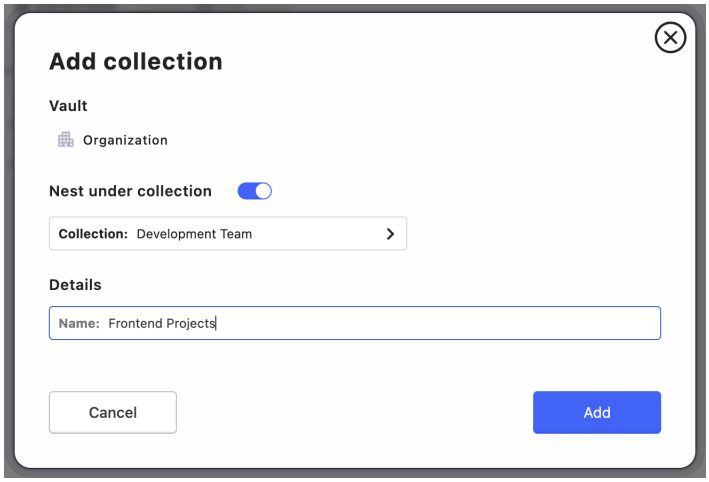
Related topics:

- *Accessing Collection Editing*
- *Nesting Collections*
- *Overview*

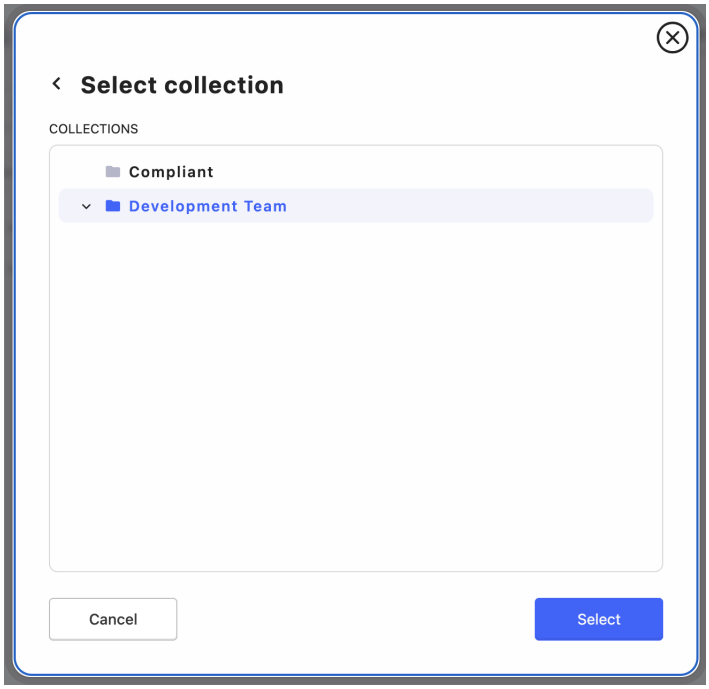
11.2.2 Nesting Collections

Collections can be organized in a hierarchical structure by nesting them within other collections. This feature allows you to create logical groupings and sub-groupings of secrets for better organization and access control.

1. Select *Password Vault* > *Organization Vault*.
2. Click *Add collection*.
3. In the modal window, enable the *Nest under collection* option.

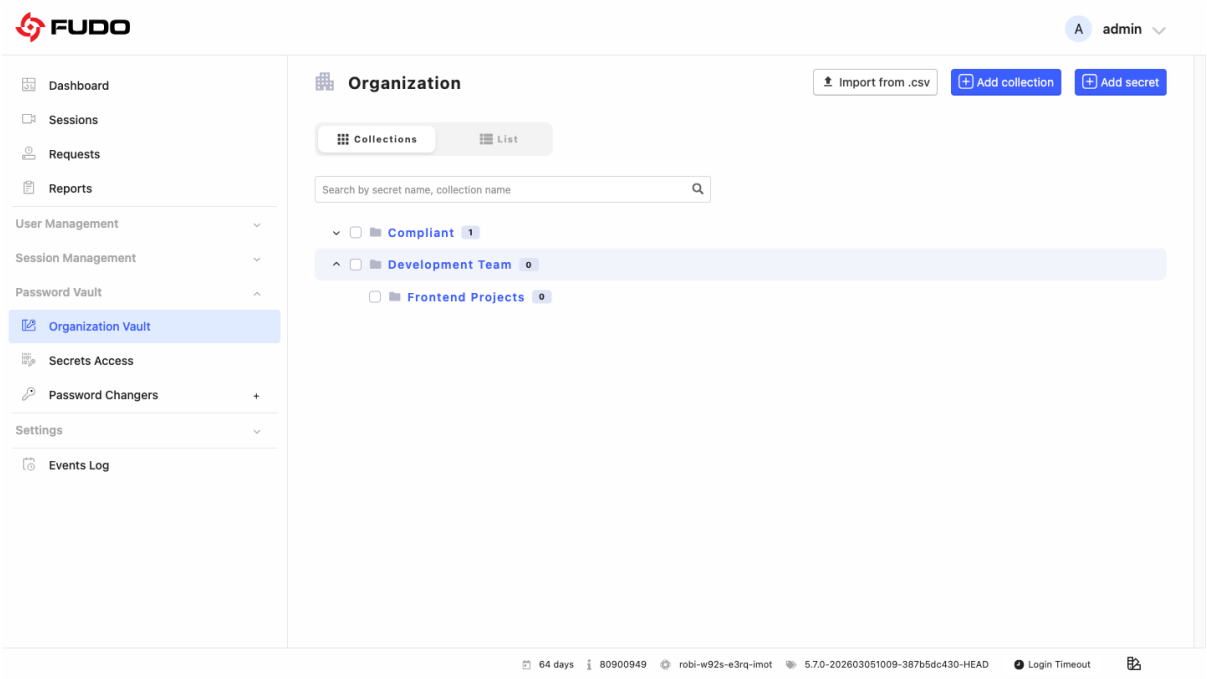


4. Click on the *Collection* dropdown to select a parent collection.
5. Select the desired parent collection from the list and click *Select*.



6. Enter a name for the nested collection in the *Name* field.
7. Click *Add* to create the nested collection.

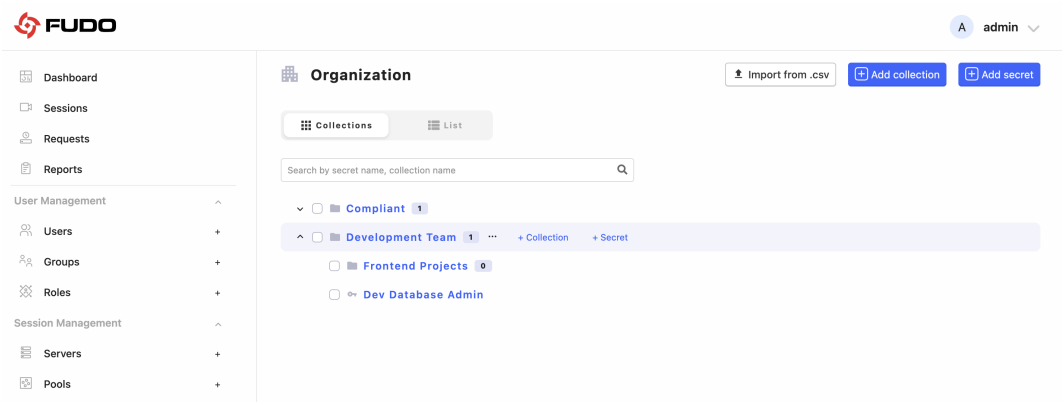
After creating the nested collection, you will see it displayed in the hierarchical tree structure. To view nested collections, expand the parent collection by clicking the arrow next to it.



Alternative Nesting Methods:

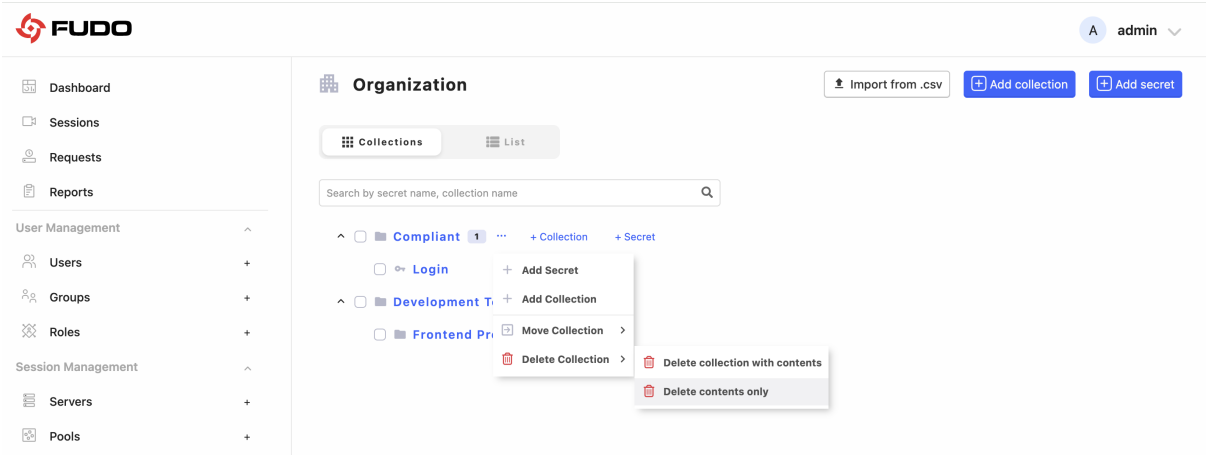
You can also nest collections using the quick action menu:

1. Hover over an existing collection to reveal the action buttons
2. Click + *Collection* to create a nested collection within the selected collection



Or use the three-dot context menu:

1. Hover over a collection and click the three dots (...) button
2. Select **Add Collection** from the context menu



Use Cases:

- **Project-based Organization**: Group secrets by main project with sub-collections for different environments (dev, staging, production)
- **Team Structure**: Mirror your organizational hierarchy with team-based collections and sub-team collections
- **Service Categories**: Group by service type with nested collections for specific applications

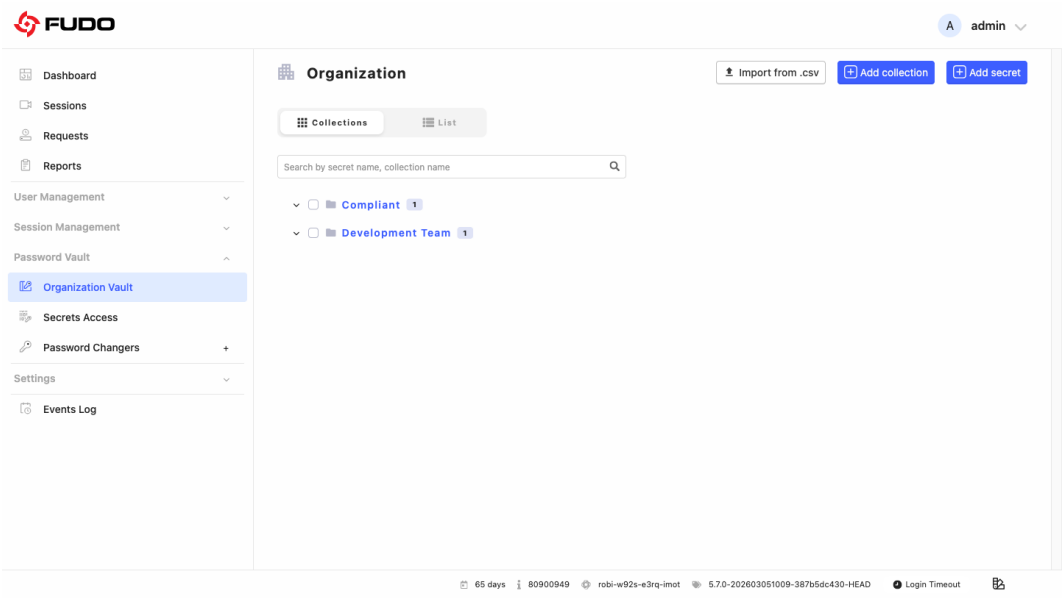
Related topics:

- *Creating Collections*
- *Overview*
- *Secrets*
- *Collections*

11.2.3 Accessing Collection Editing

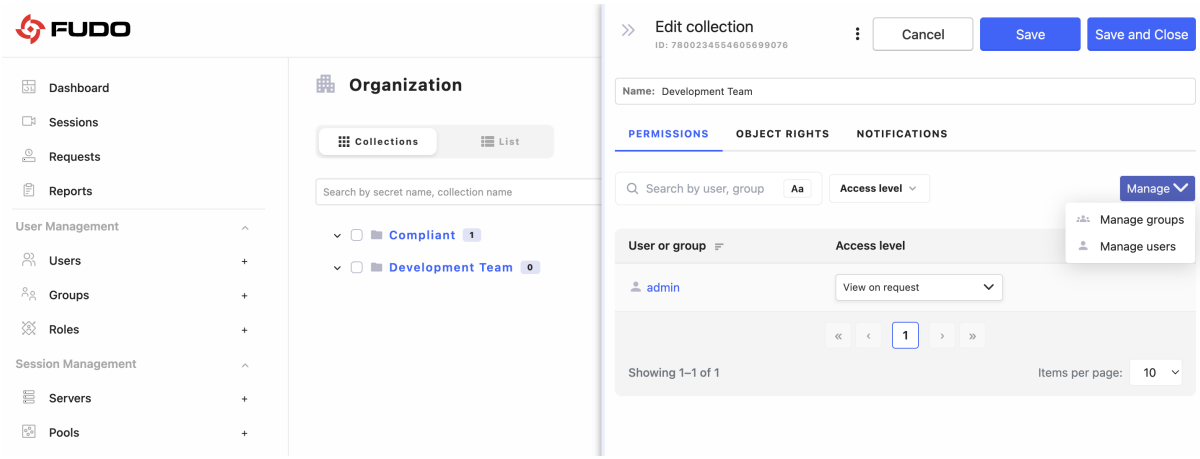
Collections can be edited to modify their properties, manage permissions, assign users and roles, and configure notifications. There are multiple ways to access the collection editing interface.

1. Select *Password Vault* > *Organization Vault*.
2. Click on the collection name you want to edit.



11.2.3.1 Edit Collection Panel

Clicking on a collection name opens the comprehensive edit panel with the following tabs:



GENERAL SETTINGS

In the general view you can modify the collection name and view the unique collection identifier (read-only).

PERMISSIONS TAB

The *PERMISSIONS* tab allows you to assign users and groups to the collection and define how they can access the secrets stored in it through the User Access Gateway.

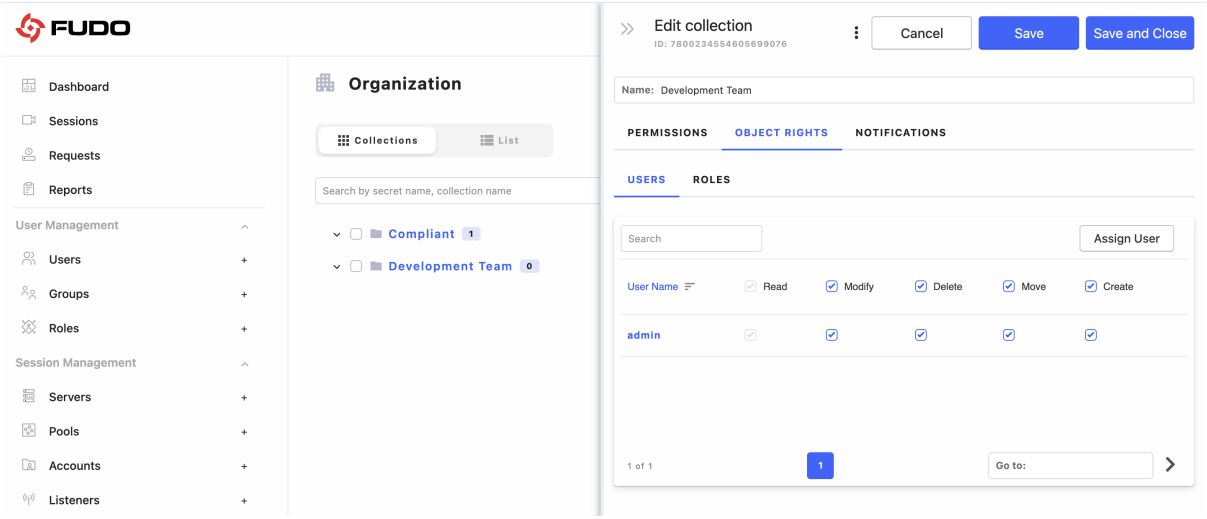
Note

Permissions control visibility of the collection in the User Access Gateway and define what users can do with the secrets stored in it. Depending on the assigned permission level, users can view secrets on request, view secrets directly, edit existing secrets, and add new secrets to the collection.

Note

A more detailed description of collection permissions is available in the *Assigning Users and Groups to Collections* section.

OBJECT RIGHTS TAB



The Object Rights tab is part of the RBAC model and allows you to manage access to the collection as an administrative object.

Note

Object Rights do not make the collection visible in the User Access Gateway. Instead, they define what users and roles are allowed to do with the collection in the Admin Panel, such as viewing, modifying, deleting, moving, or creating objects. When combined with the appropriate Permissions, Object Rights can also allow users to add secrets from the User Access Gateway, in addition to accessing the secrets stored in the collection.

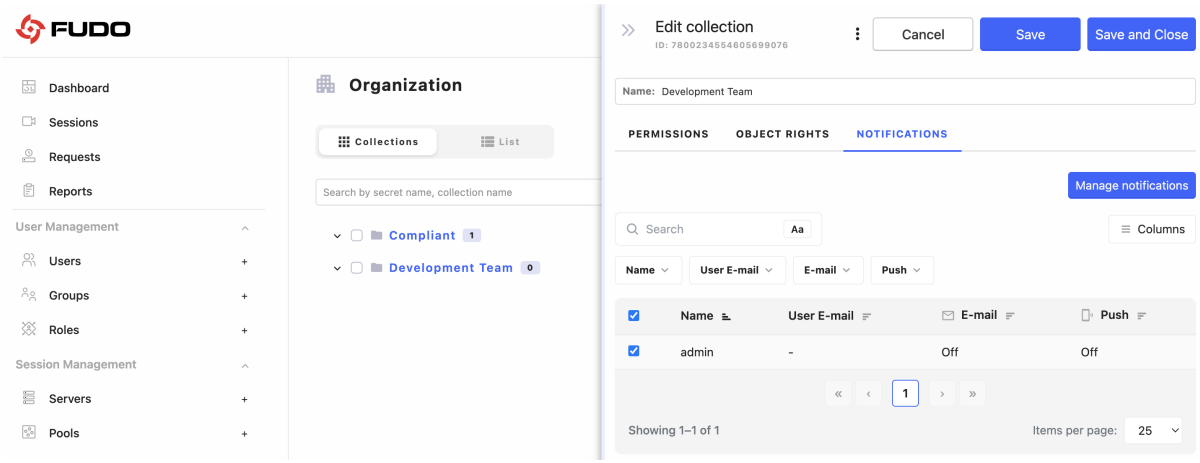
The Object Rights tab provides detailed user and role management:

- **Users Sub-tab**: Assign individual users with specific rights (Read, Modify, Delete, Move, Create)
- **Roles Sub-tab**: Assign organizational roles with appropriate rights

Note

A more detailed description of object rights for collections is available in the *Managing Collection Object Rights* section.

NOTIFICATIONS TAB



In this tab you can configure notification settings for collection activities:

- **User Selection**: Choose which users receive notifications
- **Email Notifications**: Enable/disable email alerts for collection events
- **Push Notifications**: Configure in-app push notifications

Related topics:

- *Creating Collections*
- *Managing Collection Object Rights*
- *Collection Notifications*
- *Deleting Collections*

11.2.4 Assigning Users and Groups to Collections

Collections can have specific users or groups assigned to them, allowing for granular access control over secrets. By assigning users to collections, you can control who has access to which secrets.

> **Warning**
>
> Nested collections can inherit permissions from parent collections. Enabling the **Inherit from parent collection** option removes direct permissions. Any future permissions will be inherited from the parent collection.

The following access levels are available:

- **View on request** – allows the user or group to view the collection and its secrets in the list and request one-time access to preview the secret content. Access requires administrator approval.
- **View** – allows the user or group to view the details of all secrets in the collection at any time. No approval is required.

- **Full edit** – allows the user or group to fully manage all secrets in collection. No administrator approval is required.

1. Select *Password Vault* > *Organization Vault*.
2. Left-click on the collection you want to assign users or groups.
3. Click *Manage* and select either *Manage users* or *Manage groups*, depending on whether you want to assign users or groups to the collection.
4. In the corresponding management modal, search for and select the users or groups you want to assign.
5. Click *Save* to confirm the assignment.
6. Click *Save* to apply the changes.

Related topics:

- *Managing Collection Object Rights*
- *Creating Collections*
- *Overview*

11.2.5 Managing Collection Object Rights

Collection object rights determine which management operations users and roles are allowed to perform on collections. These rights apply to the collection as an object itself, such as viewing, modifying, deleting, moving, and creating collections, and are distinct from access levels used to control access to secrets stored in collections.

Collection object rights are part of the Role-Based Access Control (RBAC) model used in Password Vault. Through RBAC, management rights can be assigned to roles and individual users to control administrative access to collections. For more information about the RBAC model, see *Role-Based Access Control (RBAC)*.

Note

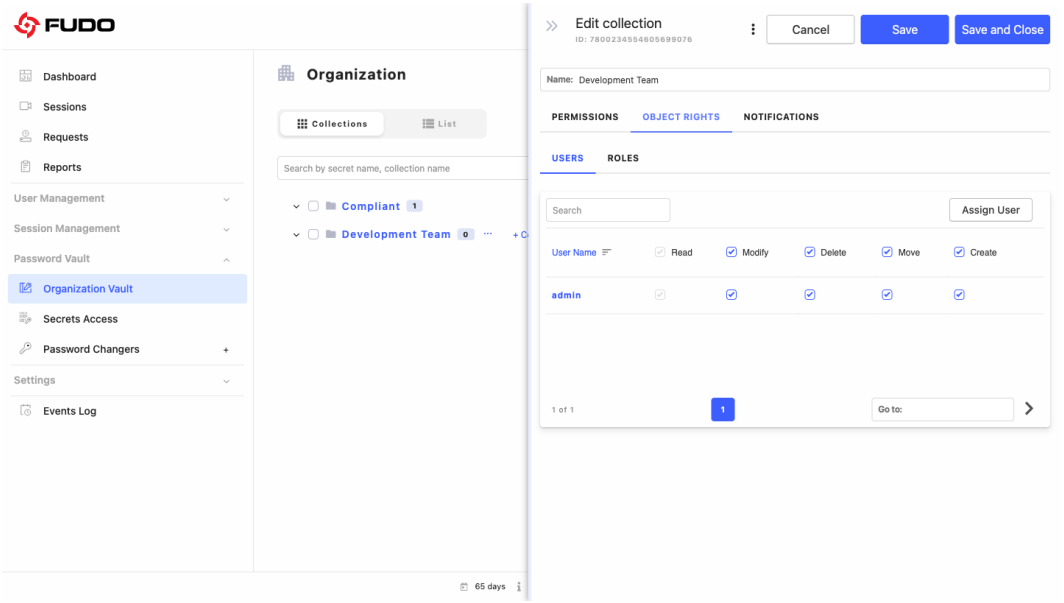
Object Rights vs. Permissions

It is important to understand the difference between object rights and permissions:

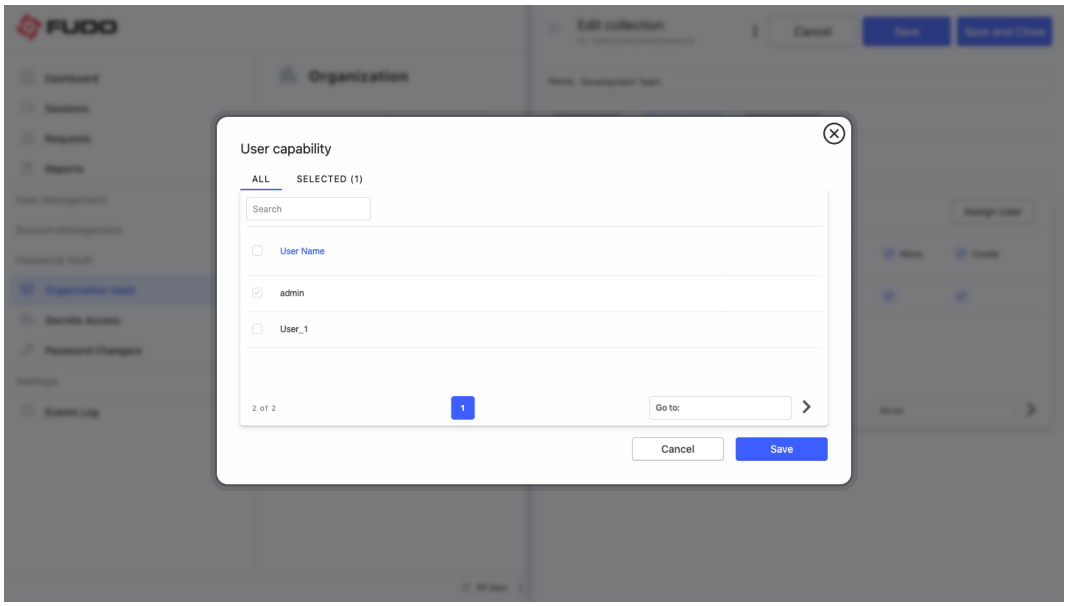
- **Object Rights** control what users can do with the collection itself, such as creating, modifying, deleting, or moving collections.
- **Permissions** control access to the secrets stored within the collection, such as *View on request*, *View*, or *Full edit*.

11.2.5.1 Assigning Object Rights to Users

1. Select *Password Vault* > *Organization Vault*.
2. Left-click on the collection you want to manage.
3. Navigate to the *OBJECT RIGHTS* tab.
4. In the *USERS* sub-tab, click *Assign User*.



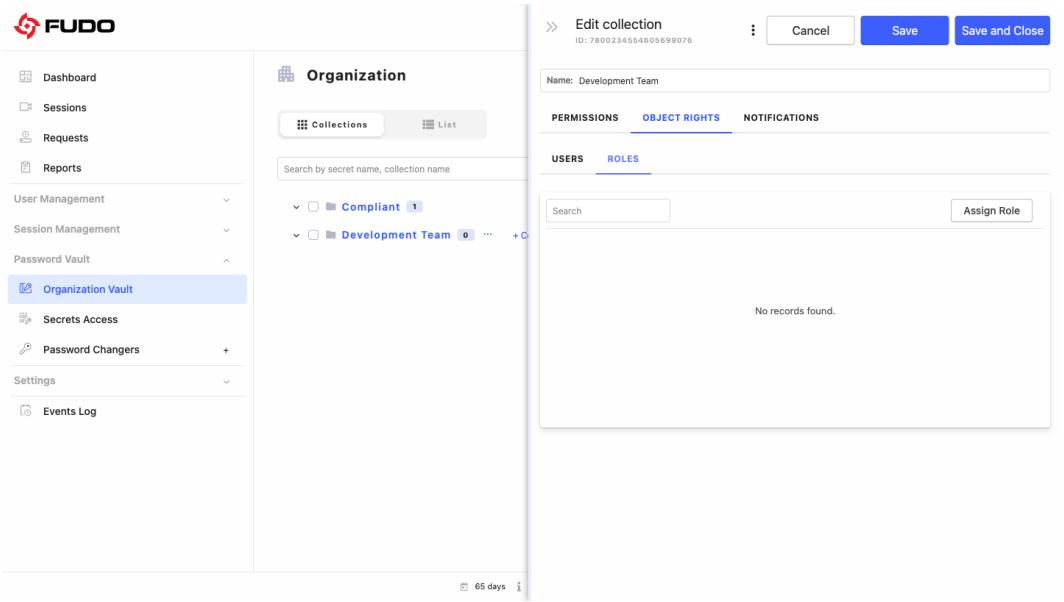
5. Select the users you want to assign and click *Save*.
6. Use the checkboxes to grant specific rights (Modify, Delete, Move, Create) to each user.
7. Click *Save and Close* to apply the changes.



11.2.5.2 Assigning Object Rights to Roles

Role-based access control allows you to assign predefined roles to collections instead of managing individual user permissions. This approach simplifies permission management, especially in larger organizations with established role hierarchies.

1. Select *Password Vault* > *Organization Vault*.
2. Left-click on the collection you want to manage.
3. Navigate to the *OBJECT RIGHTS* tab.
4. In the *ROLES* sub-tab, click *Assign Role*.



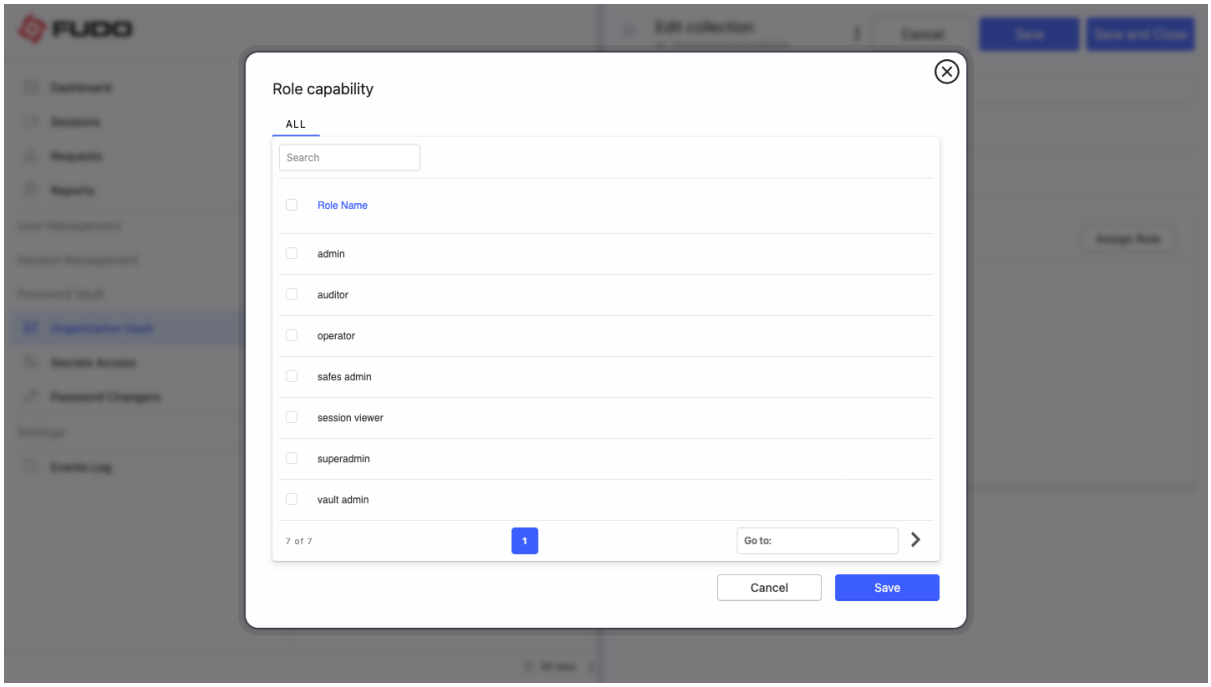
5. Select the roles you want to assign and click *Save*.
6. Use the checkboxes to grant specific rights (Modify, Delete, Move, Create) to each role.
7. Click *Save and Close* to apply the changes.

Note

Users inherit object rights from their assigned roles. If a user belongs to multiple roles, they receive the combined rights from all their roles.

Related topics:

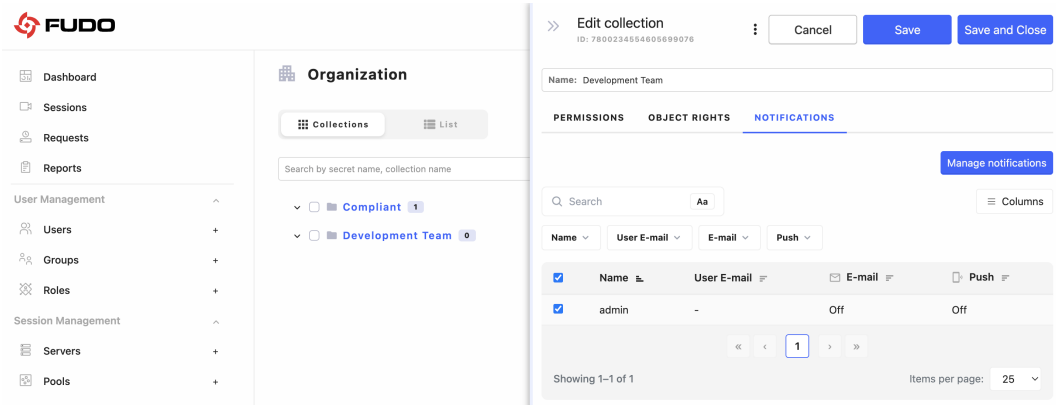
- *Assigning Users and Groups to Collections*
- *Creating Collections*
- *Collections*
- *Overview*



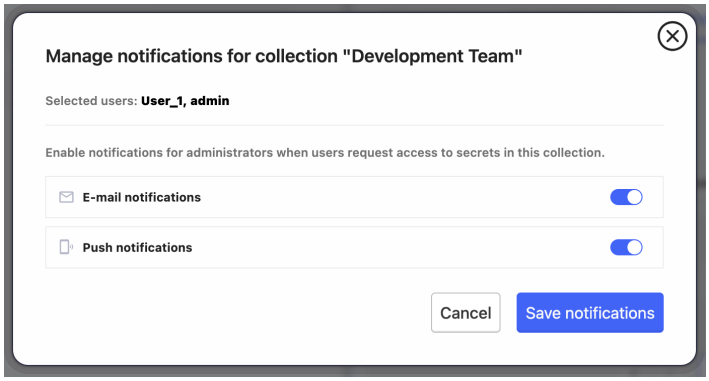
11.2.6 Collection Notifications

Collection notifications keep users informed about important events and changes related to their assigned collections. This feature helps maintain security awareness and ensures proper oversight of secret management activities.

1. Select *Password Vault* > *Organization Vault*.
2. Left-click on the collection for which you want to configure notifications.
3. Navigate to the *NOTIFICATIONS* tab.



4. Select the users for whom you want to configure notifications.
5. Click *Manage notifications*.
6. In the notification settings modal, choose notification delivery methods (Email, Push).
7. Click *Save notifications* to apply the notification settings.



Related topics:

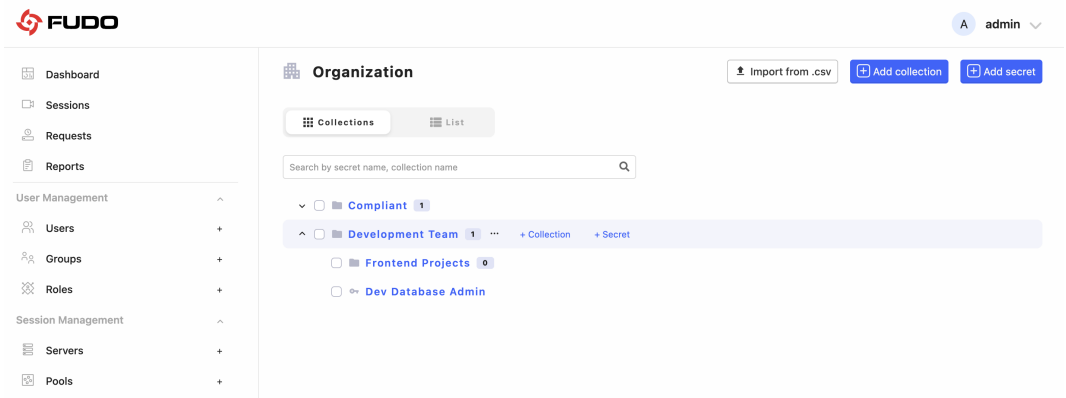
- *Assigning Users and Groups to Collections*
- *Overview*

11.2.7 Deleting Collections

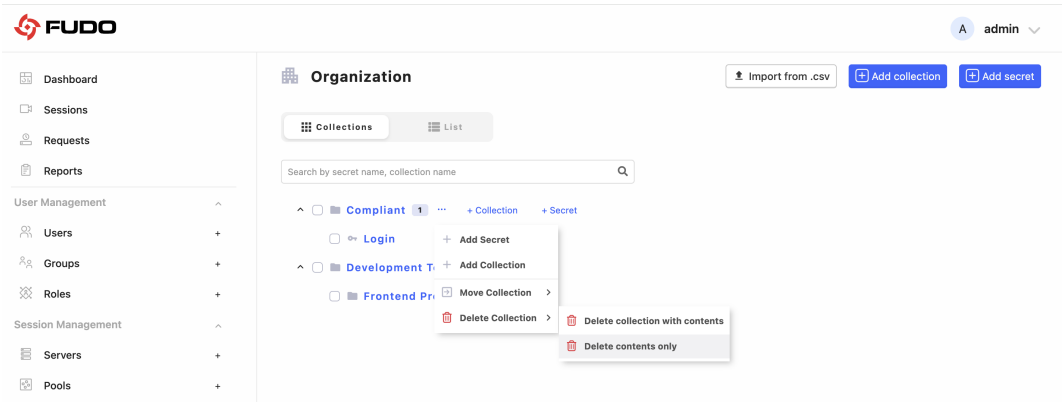
Collections can be deleted when they are no longer needed. Before deleting a collection, ensure that all important secrets are moved to other collections or backed up, as this action cannot be undone.

> **Warning**
>
> Deleting a collection is a permanent action that cannot be undone. All secrets within the collection will also be deleted unless moved to another collection first.

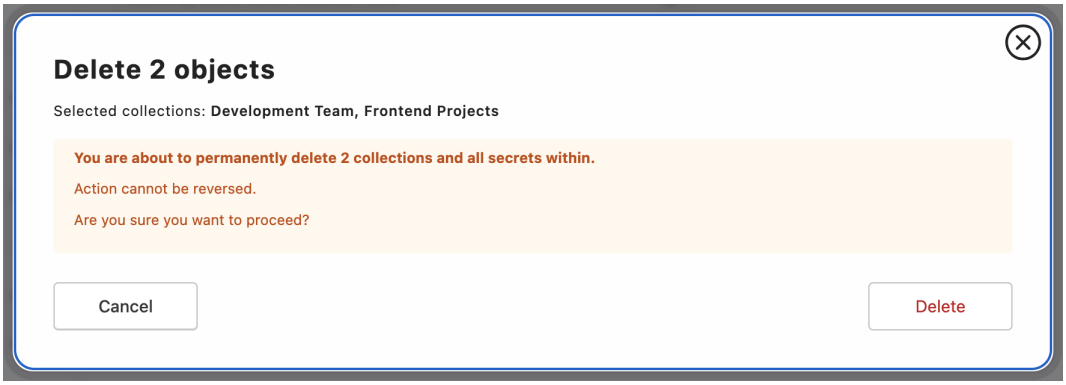
1. Select *Password Vault* > *Organization Vault*.
2. Hover over the collection you want to delete to reveal the options menu.



3. Click the three dots (...) button to open the context menu.
4. Select *Delete Collection* from the context menu.
5. You can then choose whether to delete only the contents of the collection or the collection together with its contents.



6. In the confirmation dialog, review the collection name.
7. Click *Delete* to permanently remove the collection.



Warning

Deleting a parent collection affects all nested collections.

Related topics:

- *Creating Collections*
- *Nesting Collections*
- *Overview*

11.3 Secrets

11.3.1 Creating Secrets

Secrets store sensitive information such as login credentials, API keys, certificates, SSH keys, and notes. Each secret is assigned to a collection for organization and access control.

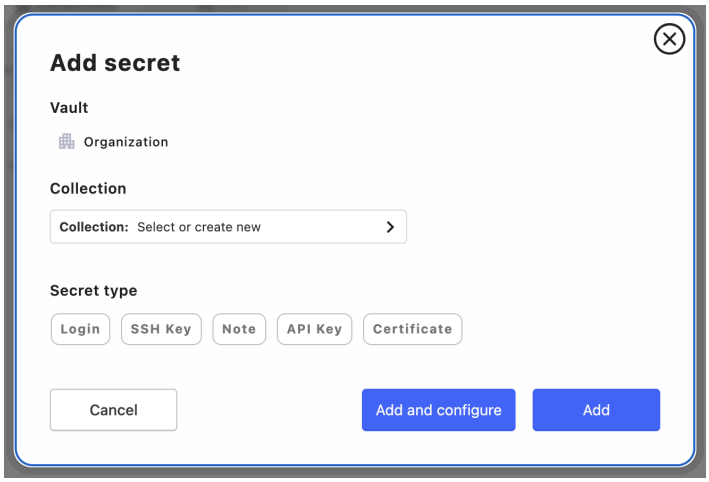
Note

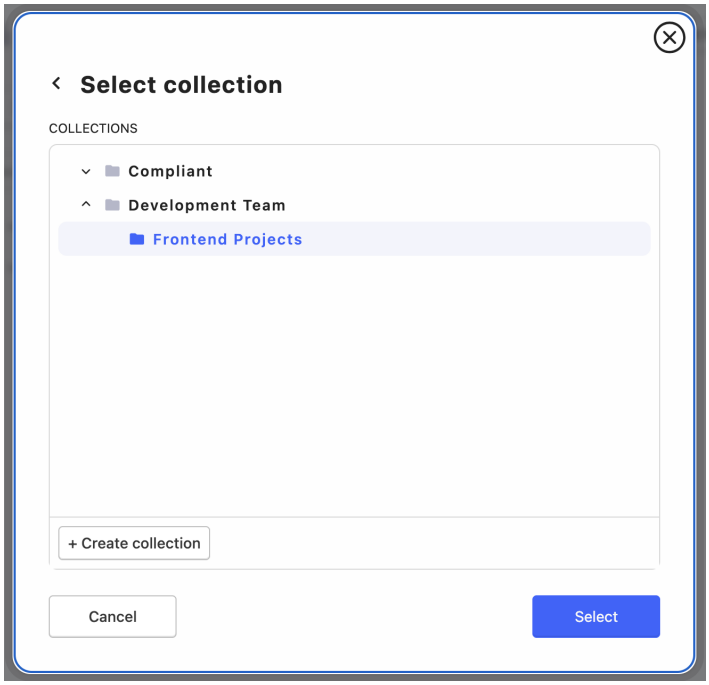
Available Secret Types:

- **Login**: Username/password credentials with domain and URL information

- **SSH Key**: SSH private keys for server access
- **Note**: Plain text notes for storing non-credential information
- **API Key**: API tokens and keys for service authentication
- **Certificate**: Digital certificates and private keys

1. Select *Password Vault* > *Organization Vault*.
2. Click *+ Add secret*.



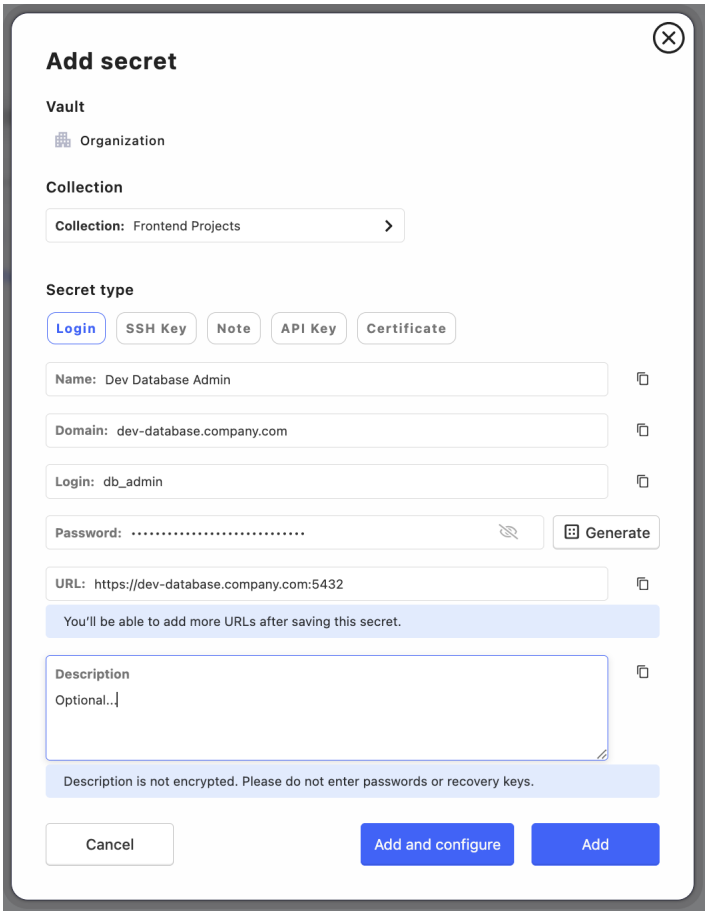


3. Select the collection where the secret will be stored by clicking the *Collection* dropdown.
4. Click *Select*.
5. Choose the appropriate secret type (Login, SSH Key, Note, API Key, Certificate).

For Login Secrets:

- Fill in the required fields:
  - *Name*: Enter a descriptive name for the secret

- *Domain*: Target domain or server address
- *Login*: Username or account name
- *Password*: You can use the *Generate* button for secure passwords
- *URL*: Enter the related website or service URL
- *Description*: Optional additional information (not encrypted)

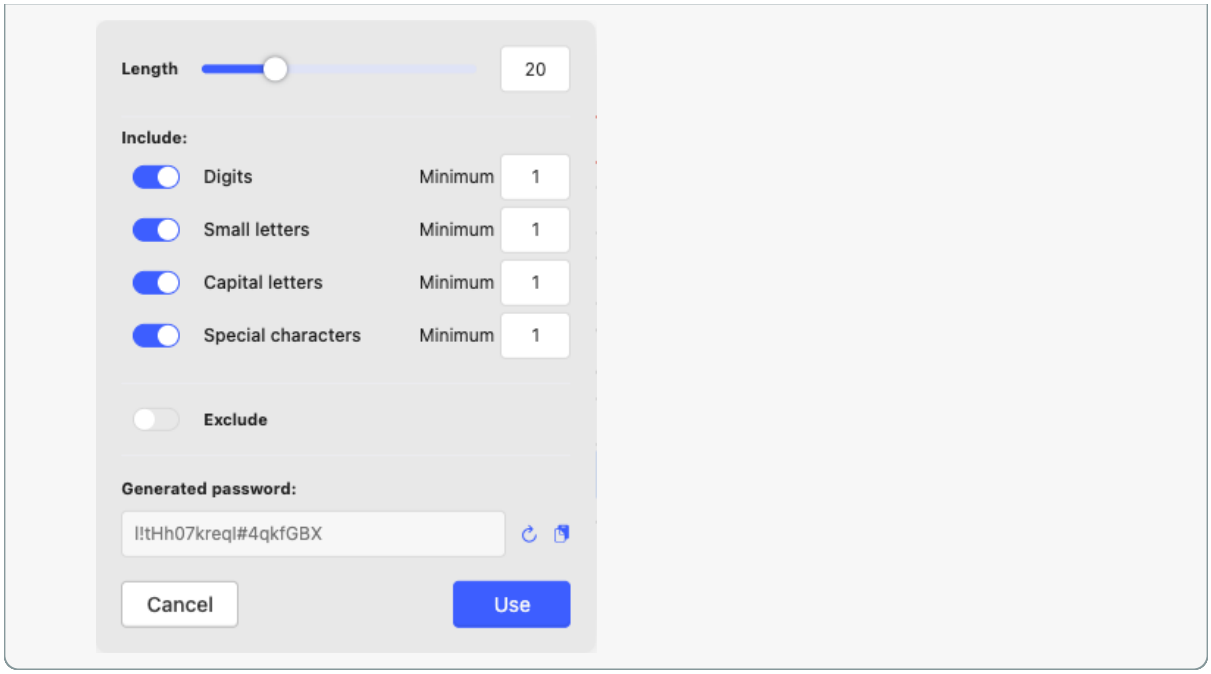


Note

Password Generator:

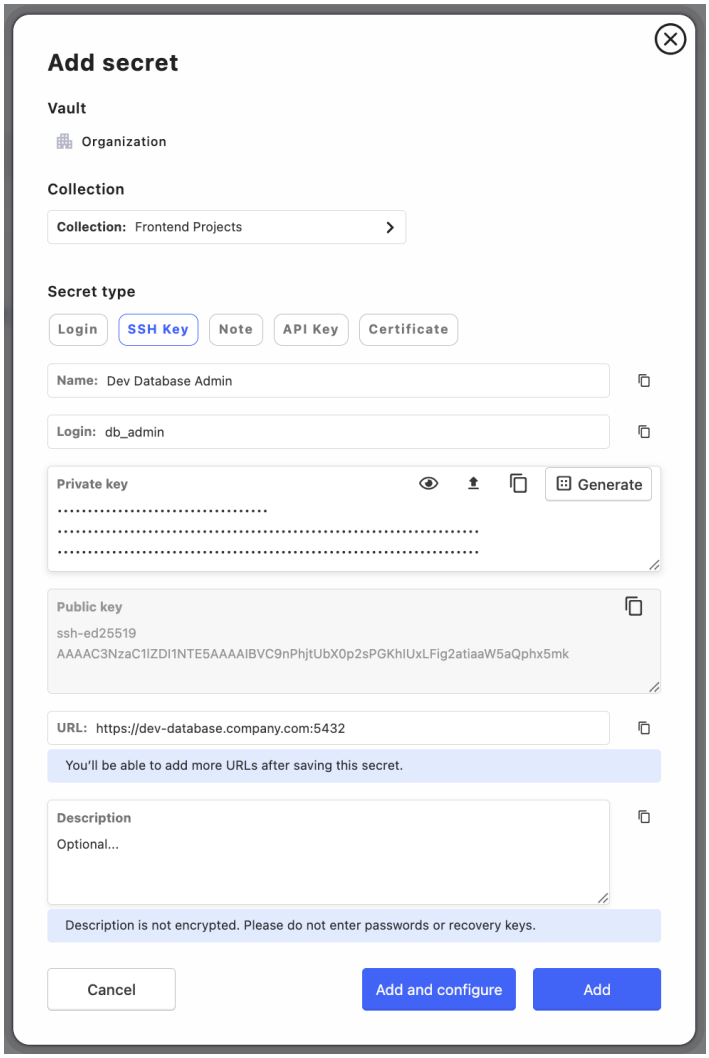
The integrated password generator (*Generate* button) provides secure password creation with customizable options:

- **Length**: Set password length (default: 20 characters)
- **Character Types**: Include digits, small letters, capital letters, special characters
- **Minimum Requirements**: Set minimum count for each character type
- **Exclude Options**: Exclude ambiguous or specific characters
- **Generated Password**: Preview and copy the generated password



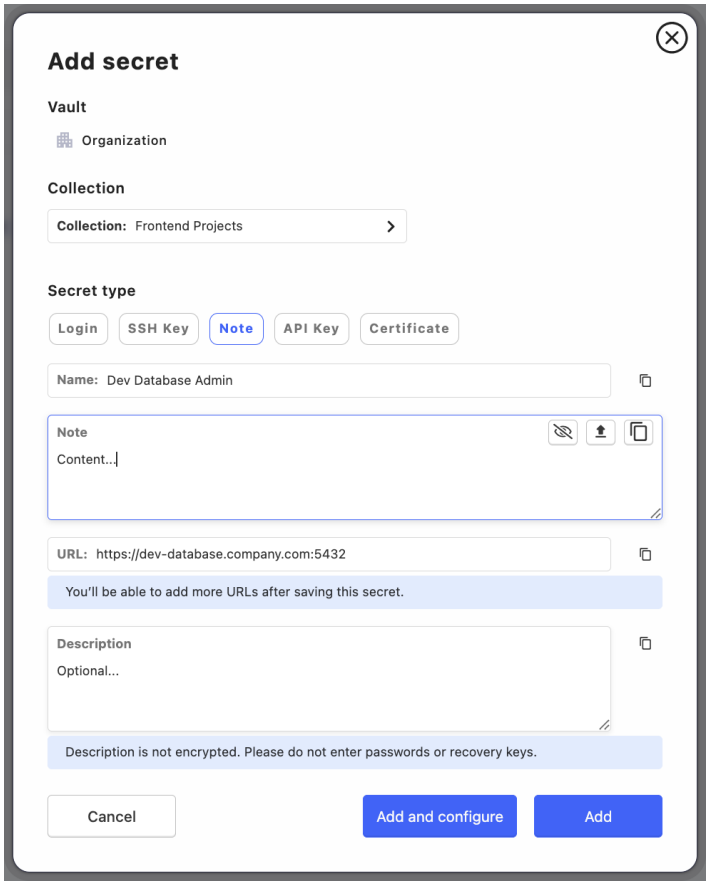
For SSH Key Secrets:

- Fill in the required fields:
  - Name: Enter a descriptive name for the secret
  - Login: Enter the username or account name
  - Private key: Enter the private key, or click *Generate* to generate both private and public keys
  - URL: Enter the related website or service URL
  - Description: Optional additional information (not encrypted)



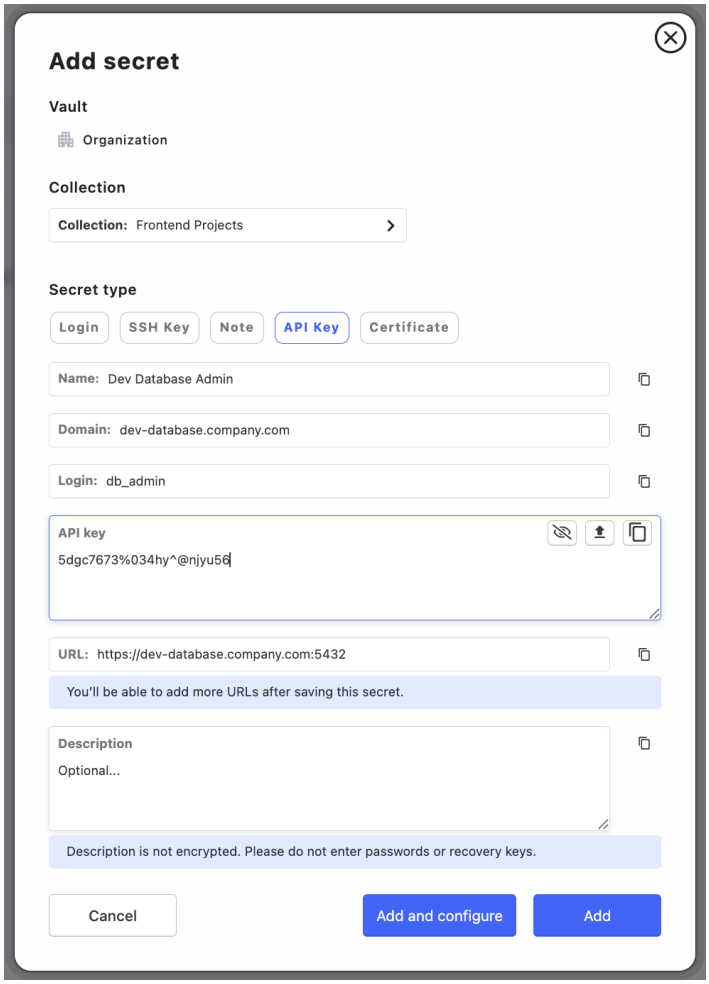
For Note Secrets:

- Fill in the required fields:
  - Name: Enter a descriptive name for the secret
  - Note: Enter the note content
  - URL: Enter the related website or service URL
  - Description: Optional additional information (not encrypted)



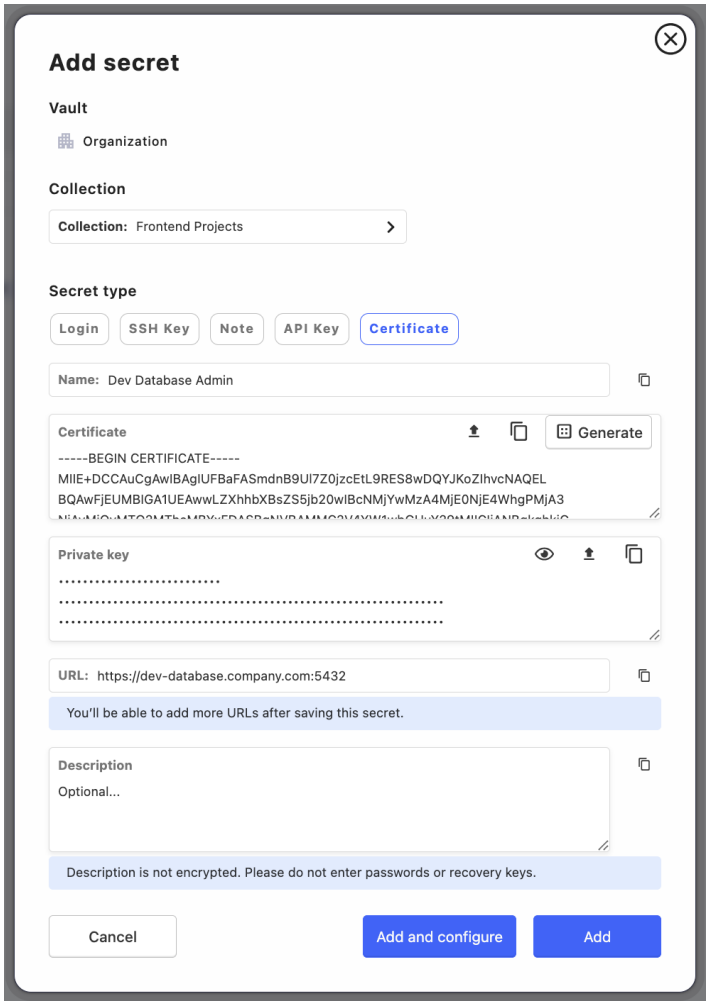
For API Key Secrets:

- Fill in the required fields:
  - Name: Enter a descriptive name for the secret
  - Domain: Enter the target domain or server address
  - Login: Enter the username or account name
  - API key: Enter or upload the API key
  - URL: Enter the related website or service URL
  - Description: Optional additional information (not encrypted)



For Certificate:

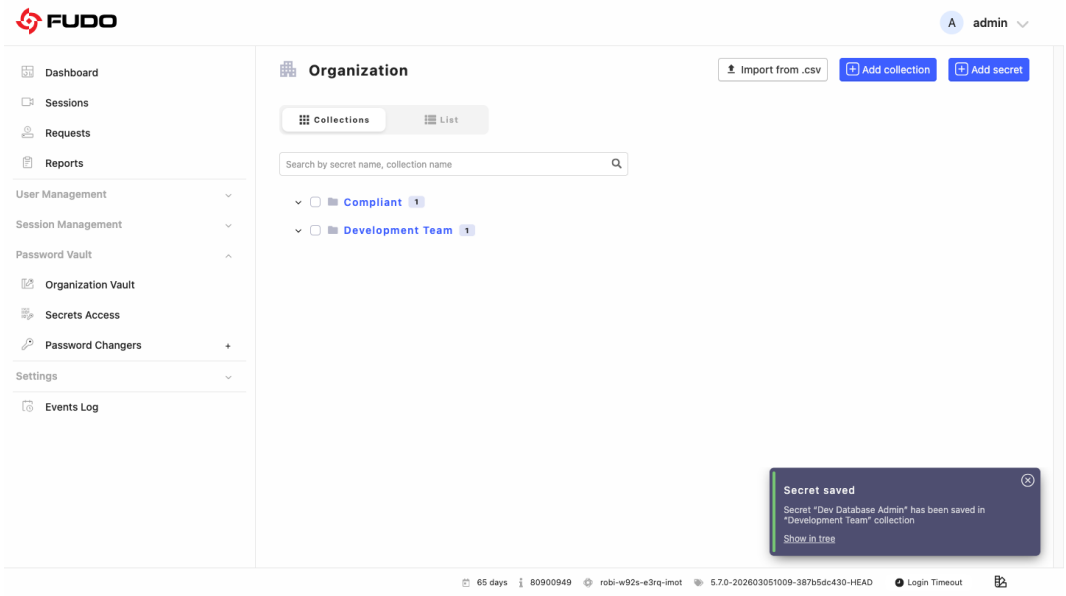
- Fill in the required fields:
  - Name: Enter a descriptive name for the secret
  - Certificate: Upload or generate certificate
  - Private Key: Upload your Private Key
  - URL: Enter the related website or service URL
  - Description: Optional additional information (not encrypted)



7. Click *Add* to create the secret and close the window, or *Add and configure* to create the secret and open its configuration window, where you can continue the setup.

Success Confirmation:

After creating a secret, you will see a confirmation message and the collection's secret count will be updated:



Alternative Creation Methods:

You can also create secrets using quick actions:

1. **From Collection Hover Menu**: Hover over a collection and click + Secret
2. **From Context Menu**: Click the three-dot menu (...) on a collection and select + **Add Secret**

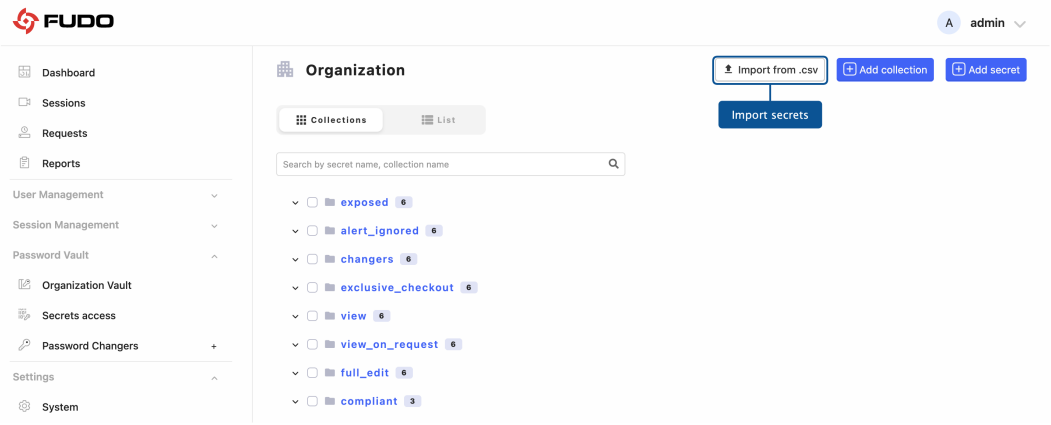
Related topics:

- *Accessing Secret Editing*
- *Creating Collections*
- *Overview*

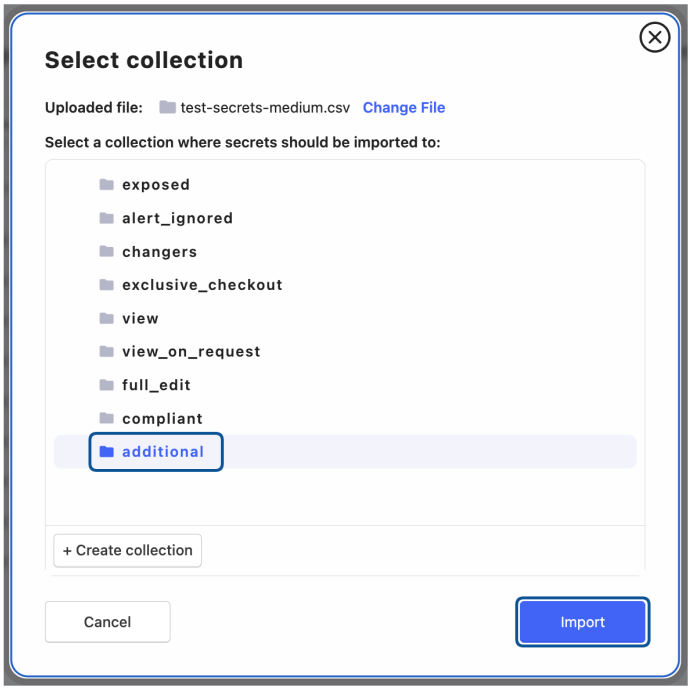
11.3.2 Importing Secrets

> **Note**
>
> The maximum allowed file size for importing secrets from a CSV file is 2 MB.

1. Select *Password Vault* > *Organization Vault*.
2. Click *Import from .csv*.



3. Drag and drop file into the modal window upload area or click *Browse for file* to upload it from local directory.
4. Select or create collection where secrets should be imported to.
5. Click *Import* to upload secrets to Fudo Enterprise configuration or *Cancel* to terminate uploading procedure.



CSV file format

The CSV file must be constructed according to the following rules:

- The first row is a *header row* containing names corresponding to the API fields names (refer to *API Documentation:* API v2: Secrets).
- The *header row* must include all fields that are required when manually creating a secret of specific type. Other fields are optional and can be left empty.
- A comma (,) has to be used as a field separator.

Example CSV file:

```
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,,,,
```

Note

SSH private keys and certificates are typically stored in multi-line PEM format. When importing them from a CSV file, enclose the entire value in double quotes ("") so it is treated as a single CSV field.

Example CSV for a certificate secret:

```
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-----"
```

Related topics:

- *Secrets*
- *Collections*

11.3.3 Accessing Secret Editing

Secrets can be edited to update their information, change passwords, modify URLs, or update descriptions. There are multiple ways to access and edit secrets in the Password Vault.

Method 1: From List View

1. Select *Password Vault* > *Organization Vault*.
2. Click *List* to switch to list view.
3. Click on the secret name to open the edit panel.

Method 2: From Collections View

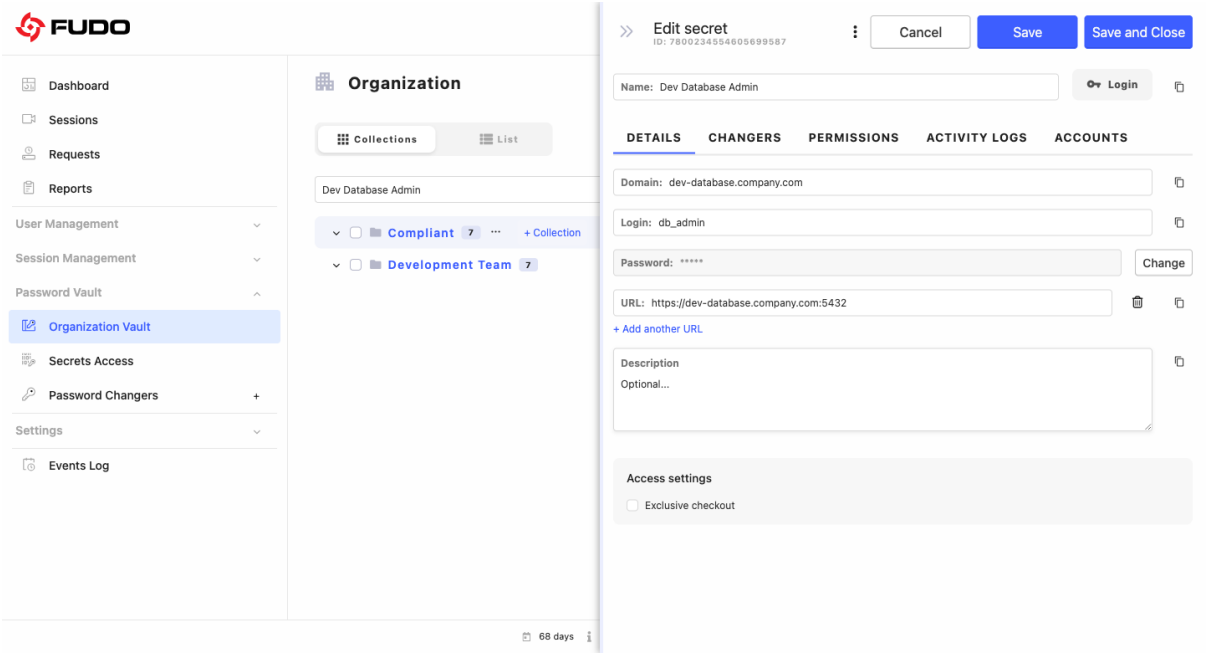
1. Navigate to the collection containing the secret.
2. Expand the collection to view its secrets.
3. Click on the secret name to edit.

11.3.3.1 Edit Secret Panel

The secret edit panel provides comprehensive editing capabilities with the following tabs:

DETAILS TAB

The Details tab is the main editing interface for secret information where you can modify all core attributes of the secret.



Available fields (example for Login type):

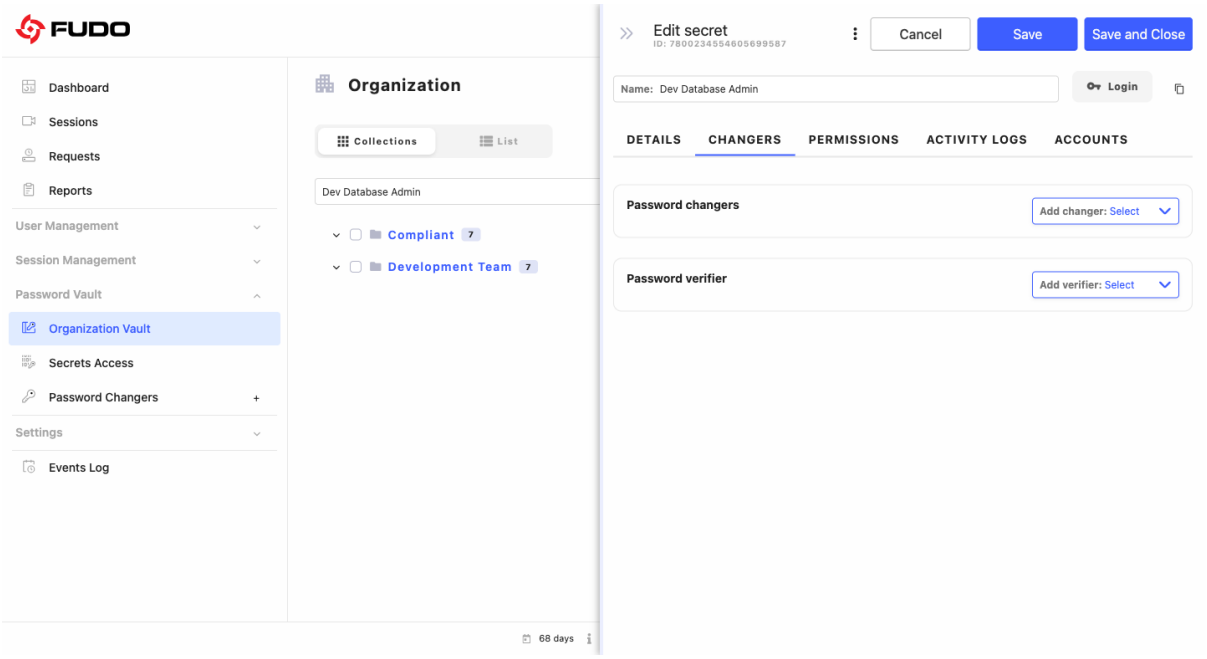
- **Name**: The display name for the secret
- **Domain**: The domain or hostname associated with the credentials
- **Login**: The username or login identifier
- **Password**: The secret password (masked by default with a "Change" button to update)
- **URL**: One or more URLs where these credentials can be used
  - Click + Add another URL to add multiple URLs
  - Click the trash icon to remove a URL
  - Each URL must include the protocol (https://, ssh://, etc.)
- **Description**: Optional notes or additional information about the secret

Access Settings:

- **Exclusive checkout**: When enabled, only one user can access the secret at a time. Other users must wait for the secret to be checked back in.

CHANGERS TAB

The Changers tab allows you to configure automated password management through Secret Changers and Verifiers.



Secret Changers:

Secret changers automate the process of rotating passwords on target systems. You can select a secret changer from the dropdown to automate password rotation.

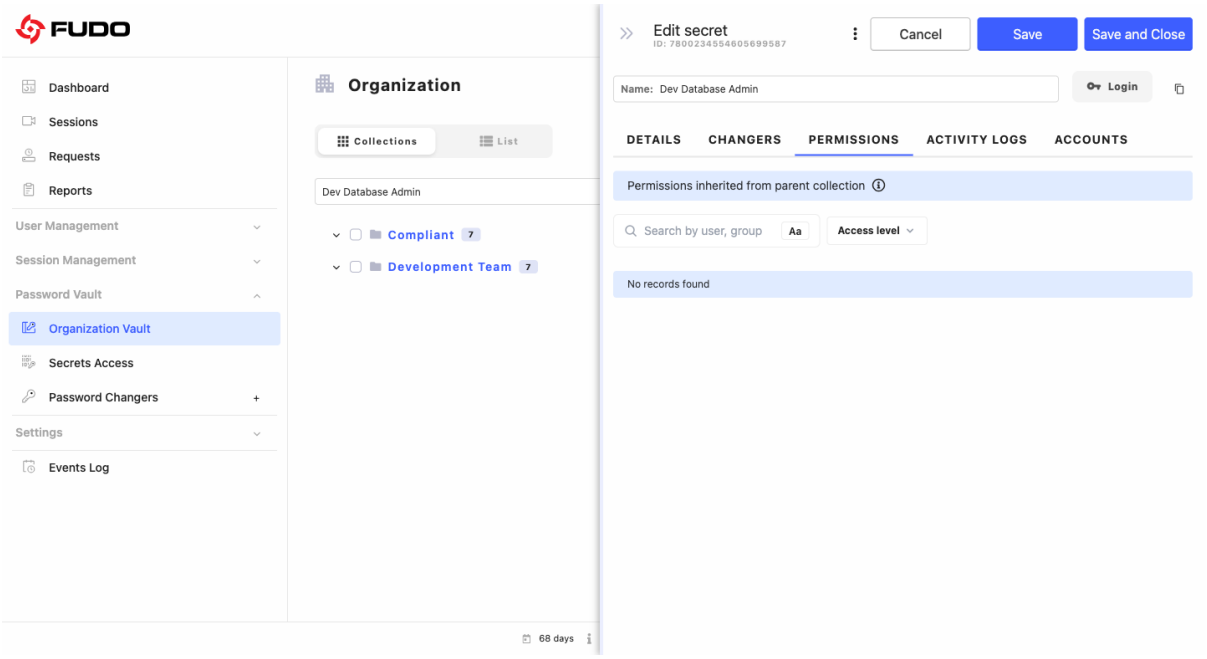
Secret Verifier:

Secret verifiers ensure that the stored credentials match what's configured on the target system. You can select a verifier to periodically validate password accuracy.

> **Note**
>
> A Secret Changer only changes the secret; it never verifies it, even if its change policy includes verification. To also verify the secret, assign a Secret Verifier.

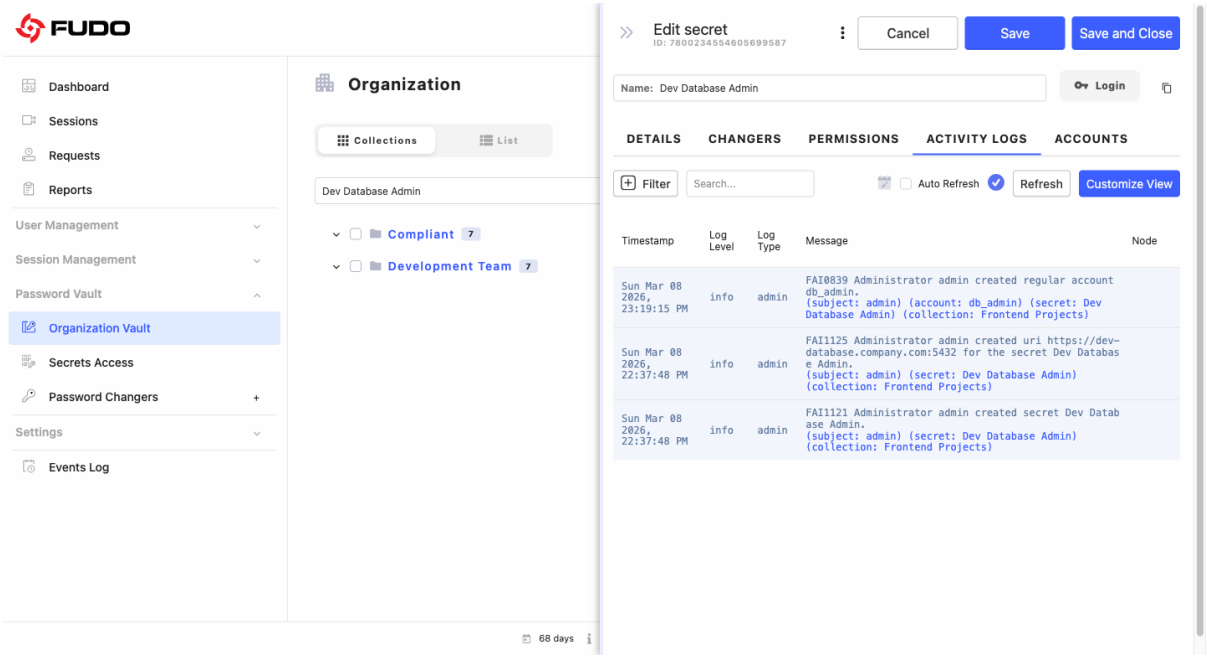
PERMISSIONS TAB

The Permissions tab allows you to preview user or group access to the secret. Secrets inherit permissions from their parent collection.



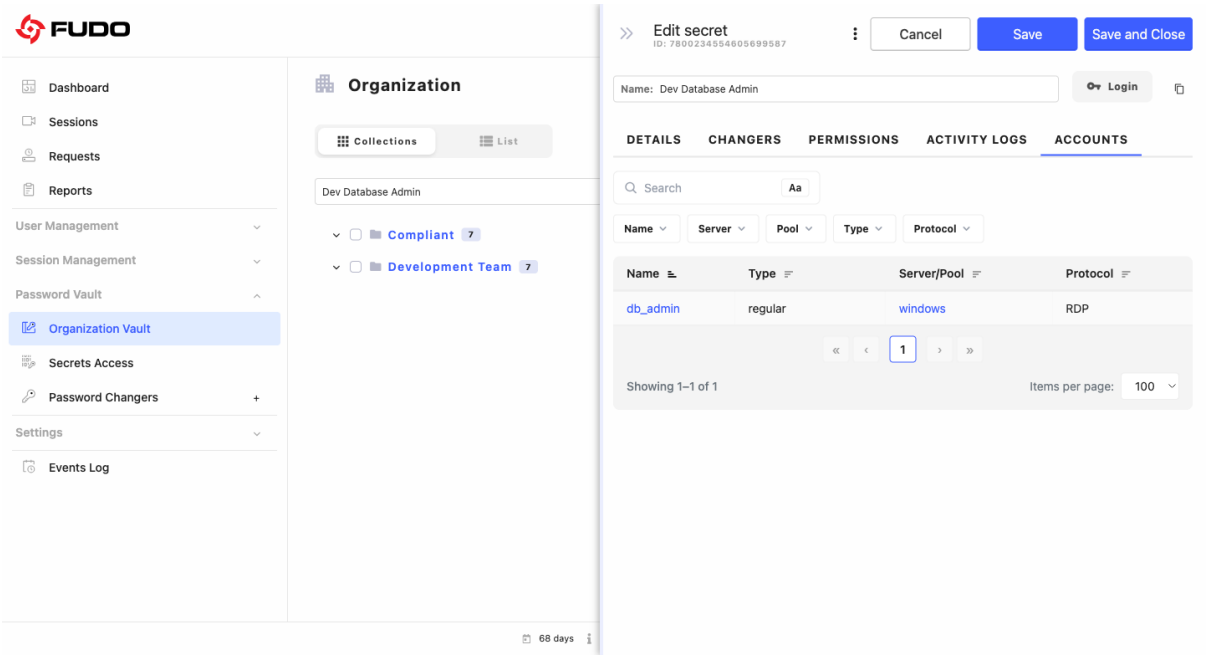
ACTIVITY LOGS TAB

The Activity Logs tab provides a comprehensive audit trail of all actions performed on the secret. You can filter log entries and customize which columns are displayed.



ACCOUNTS TAB

The Accounts tab displays all accounts associated with this secret.



Related topics:

- *Creating Secrets*
- *Deleting Secrets*
- *Accessing Collection Editing*
- *Overview*

11.3.4 Moving Secrets Between Collections

Secrets can be moved between collections to reorganize your password vault structure, adjust access permissions, or reflect changes in team organization. Moving secrets updates their access control based on the target collection's permissions.

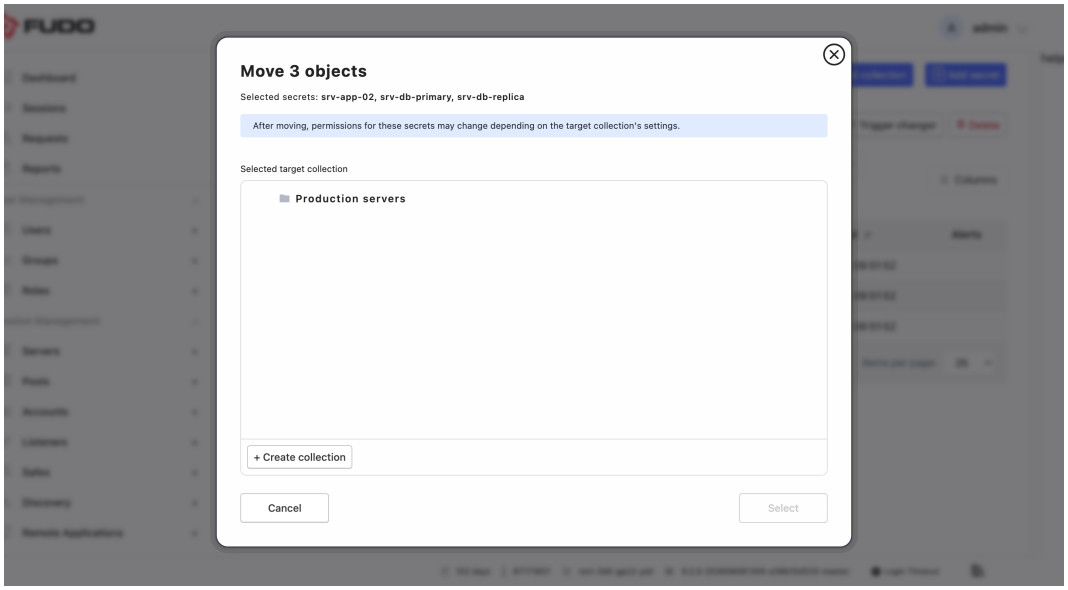
> **Note**
>
> Moving a secret to a different collection will change its access permissions based on the target collection's user and role assignments.

There are several methods to move secrets between collections:

Method 1: Bulk Move in List View

This method allows you to move multiple secrets at once.

1. Navigate to *Password Vault* > *Organization Vault*.
2. Click *List* to switch to list view.
3. Select the checkboxes next to the secrets you want to move.
4. Click the *Move* button that appears in the action bar.
5. Select the target collection from the tree structure.
6. Click *Select* to confirm the move operation.



Note

Objects are moved one by one and the modal reports the progress. If an object cannot be moved, the failure is reported in the modal and the remaining objects are still processed. A running operation can be stopped, in which case the objects already moved stay in the target collection.

Method 2: Bulk Move in Collections View

1. Navigate to *Password Vault* > *Organization Vault*.
2. In *Collections* view, select multiple secrets by checking their checkboxes.
3. Click the *Move* button that appears in the action bar.
4. Select the target collection from the tree structure.
5. Click *Select* to confirm the move operation.

Method 3: Moving During Edit

1. Open any secret for editing.
2. Click the three dots (...) button next to the secret ID In the edit panel and select *Move to*.
3. Select the target collection from the tree structure.
4. Click *Select* to confirm the move operation.
5. Save the secret.

Method 4: Moving Using Context Menu

1. Hover over the secret you want to edit to reveal the options menu.
2. Click the three dots (...) button to open the context menu.
3. Select *Move to*.
4. Select the target collection from the tree structure.

5. Click *Select* to confirm the move operation.

Related topics:

- *Accessing Secret Editing*
- *Creating Collections*
- *Overview*

11.3.5 Deleting Secrets

Secrets can be deleted when they are no longer needed or when credentials have been decommissioned. Before deleting secrets, ensure you understand the impact on users and applications that may depend on them.

Warning

Deleting a secret is a permanent action that cannot be undone. Ensure you have backups or alternative access methods before proceeding with deletion.

There are several methods to delete secrets from the Password Vault:

Method 1: Bulk Delete in List View

This method allows you to delete multiple secrets at once.

1. Navigate to *Password Vault* > *Organization Vault*.
2. Click *List* to switch to list view.
3. Select the checkboxes next to the secrets you want to delete.
4. Click the *Delete* button that appears in the action bar.
5. Review the warning message and confirm the deletion.

Note

Objects are deleted one by one and the modal reports the progress. If an object cannot be deleted, the failure is reported in the modal and the remaining objects are still processed. A running operation can be stopped, in which case the objects already deleted are not restored.

Method 2: Bulk Delete in Collections View

1. Navigate to *Password Vault* > *Organization Vault*.
2. In *Collections* view, select multiple secrets by checking their checkboxes.
3. Click the *Delete* button that appears in the action bar.
4. Review the warning message and confirm the deletion.

Method 3: Delete from Edit Panel

1. Open any secret for editing.
2. Click the three dots (...) button next to the secret ID in the edit panel.

3. Select *Delete* from the dropdown menu.
4. Confirm the deletion in the warning dialog.

Method 4: Using Context Menu

1. Hover over the secret you want to delete to reveal the options menu.
2. Click the three dots (...) button to open the context menu.
3. Select *Delete*.
4. Confirm the deletion in the warning dialog.

Related topics:

- *Creating Secrets*
- *Accessing Secret Editing*
- *Moving Secrets Between Collections*
- *Deleting Collections*
- *Overview*

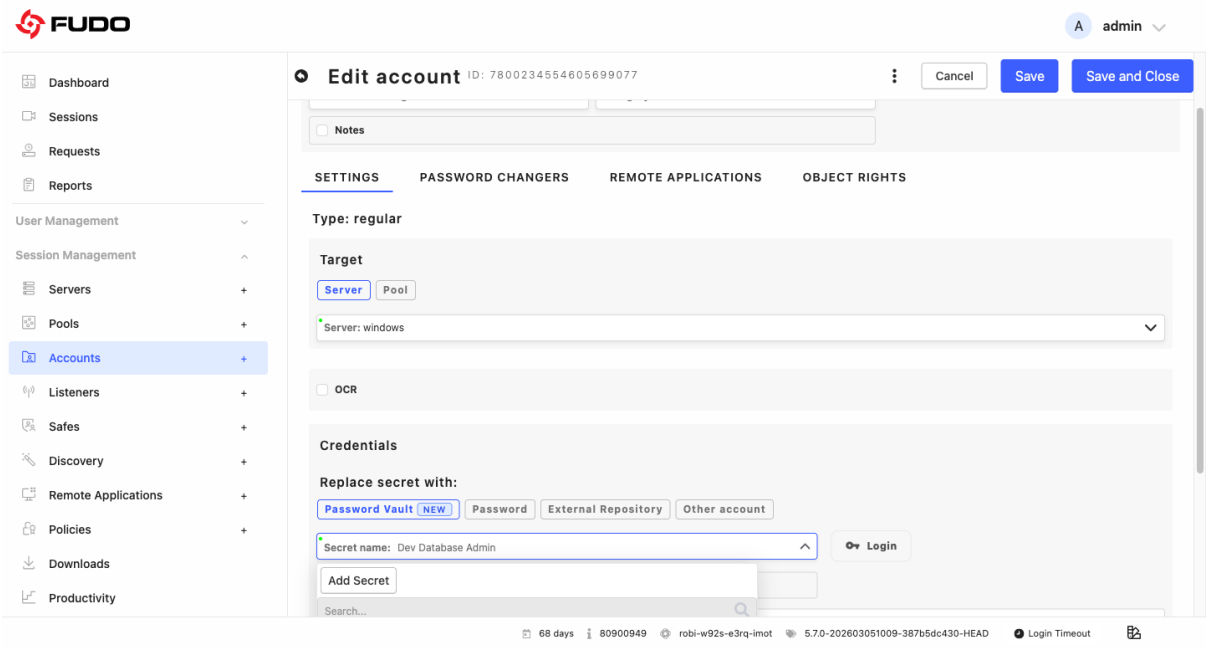
11.3.6 Assigning Password Vault Secrets to Accounts

> **Note**
>
> Before assigning secrets to accounts, ensure that you have appropriate permissions to edit accounts and access to the Password Vault.

Password Vault secrets can be assigned to Fudo Enterprise accounts to provide centralized credential management. This integration allows administrators to use secrets stored in the Password Vault for authenticating connections to target servers.

> **Note**
>
> Two types of secrets can be assigned to accounts: **Login** and **SSH Key** secrets.

1. Navigate to *Session Management* > *Accounts*.
2. Click on the account name you want to edit.
3. In the account settings, locate the *Credentials* section.
4. Under *Replace secret with:*, select *Password Vault*.



5. Click the *Secret name* dropdown to view available secrets.
6. Select secret from the list.
7. The secret details will be displayed, showing the login and domain information.
8. Optionally, enable checkboxes:
   - *Use domain from secret* - Uses the domain stored in the secret
   - *Use login from secret* - Uses the login name stored in the secret
9. Click *Save* or *Save and Close* to apply the changes.

Note

The *Add Secret* button in the secret selection dropdown allows you to create a new secret directly from the account configuration interface if the required secret doesn't exist yet.

Note

- **Permissions**: Users must have appropriate permissions to both the account and the Password Vault secret to establish connections.
- **Audit trail**: All secret access through accounts is logged in both the account activity logs and the Secret Access monitoring.
- **Exclusive checkout**: If a secret has exclusive checkout enabled, only one user can access it at a time through the account.

Related topics:

- *Creating Secrets*
- *Accessing Secret Editing*

- *Secret Access Monitoring*
- *Overview*

11.4 Secret Access Monitoring

The Secret Access tab provides comprehensive monitoring and auditing capabilities for tracking all secret access events within the Password Vault. This centralized view allows administrators to monitor who accessed which secrets, when the access occurred, and whether any security exposures were detected.

Navigate to *Password Vault* > *Secrets access* to access the monitoring interface.

The Secret Access interface displays a comprehensive table with the following information for each access event:

- **User**: The user who accessed the secret (clickable link to user profile)
- **Secret**: The name of the accessed secret (clickable link to secret details)
- **Collection**: The collection containing the secret (clickable link to collection)
- **Start date**: When the secret access began
- **End date**: When the secret access ended
- **Status**: Current status of the access (Ongoing or Ended)
- **Events**: Security events detected during access

11.4.1 Event Types and Status Indicators

Access Status

The system tracks the lifecycle of each secret access:

- **Ended**: The secret access session has been completed
- **Ongoing**: The secret is currently being accessed

Exposure Detection

The Secret Access monitoring includes exposure detection capabilities. When a potential security exposure is detected, it appears in the Events column as "Exposure detected".

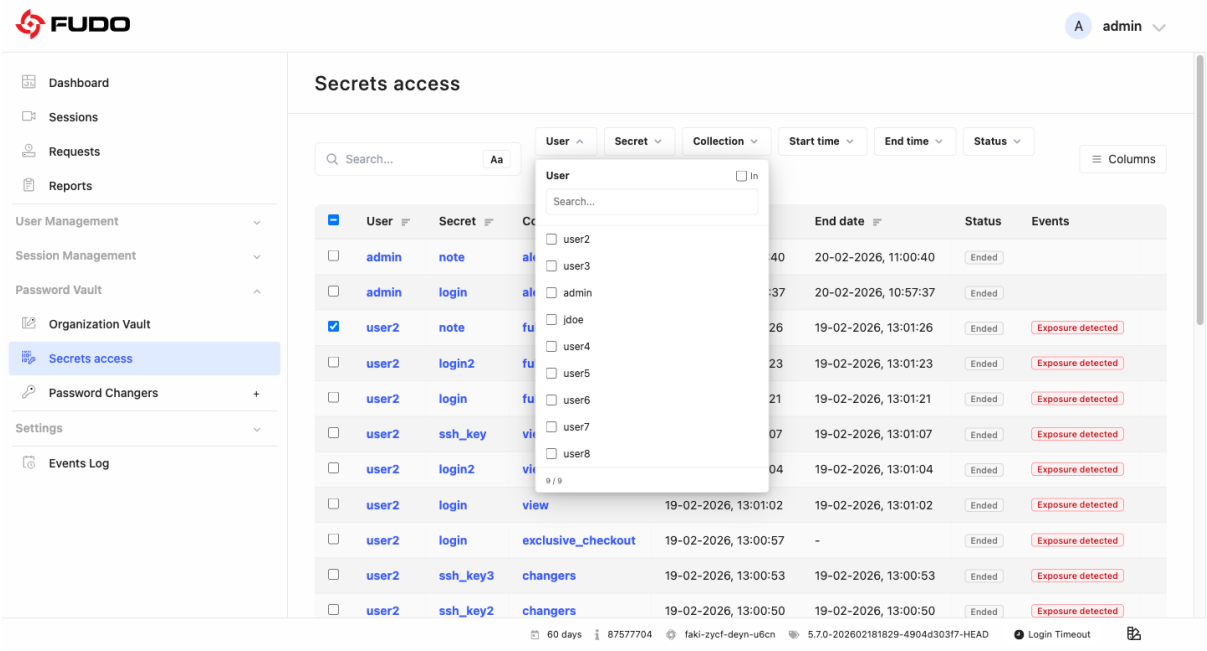
> **Note**
>
> Exposure is detected when a user who has viewed a secret is blocked in Fudo Enterprise.

Hovering over an exposure detection event displays additional information about the exposure reason, such as:

- **User blocked**: The user account has been blocked or deactivated
- **Suspicious activity**: Unusual access patterns detected
- **Policy violation**: Access violated defined security policies

11.4.2 Filtering and Reviewing Events

The Secret Access interface lets you filter events by user, secret, collection, time range, status, exposure, and alert handling.



Search Functionality

The search bar at the top of the interface allows for quick text-based searches across all visible data fields.

> **Note**
>
> The search is case-insensitive by default, with an *Aa* toggle button for case-sensitive searching.

Column Management

Administrators can customize the visible columns using the "Columns" button. This allows for showing or hiding specific columns based on monitoring needs.

Related topics:

- *Overview*
- *Managing Collection Object Rights*
- *Accessing Secret Editing*

11.5 Fudo Password Vault Browser Extension

The Fudo Password Vault browser extension lets users access secrets stored in Fudo Enterprise directly from supported desktop browsers: Chrome, Firefox, and Safari.

After signing in with their Fudo Enterprise user credentials and providing the User Access Gateway address, users can browse available collections, search for secrets, and open linked websites directly from the extension. When a login form is recognized, the extension can suggest autofilling the matching secret, making access to web resources faster and more convenient.

The extension also supports Password Vault access workflows. If a secret requires approval, users can request access directly from the browser. Once access is granted, a notification is displayed on the page. For secrets protected with exclusive checkout, the extension shows how much time remains before the checkout expires.

Users who have a Personal Vault can also create and edit their own secrets and collections directly in the extension, without opening the User Access Gateway in a separate tab.

Note

The extension is available to customers with a Full Password Vault license. It supports desktop browser versions only and is available in English and Polish.

11.5.1 Installation

Install the extension from your browser's official add-on store, then pin it to the toolbar for quick access.

Chrome and other Chromium-based browsers

Install the extension from the Chrome Web Store. If the link is unavailable, search the store for **Password Vault** by Fudo Security.

Firefox

Install the extension from Firefox Add-ons. If the link is unavailable, search the store for **Fudo Password Vault**.

Safari

Install the extension from the Mac App Store, then enable it under *Safari* > *Settings* > *Extensions*. If the link is unavailable, search the store for **Fudo Password Vault**.

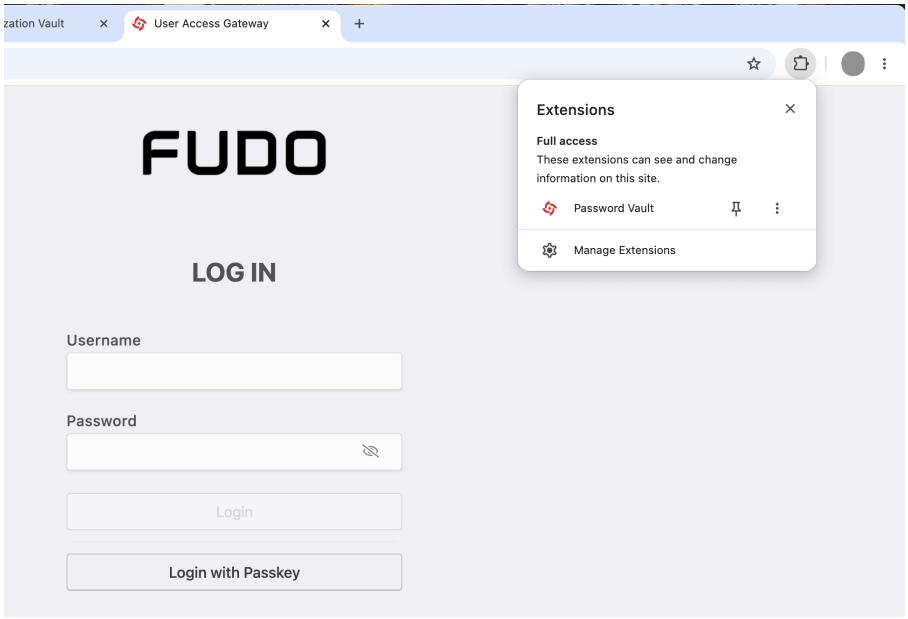
Note

Safari also requires you to grant the extension access to websites. To grant access:

1. Open *Safari* > *Settings* (*Cmd+,*) > *Extensions*.
2. Select **Password Vault** in the left sidebar.
3. Click **Edit Sites...**.
4. At the bottom of the list, set **When visiting other sites:** to **Allow**.
5. Close Settings.

11.5.2 Opening the Extension

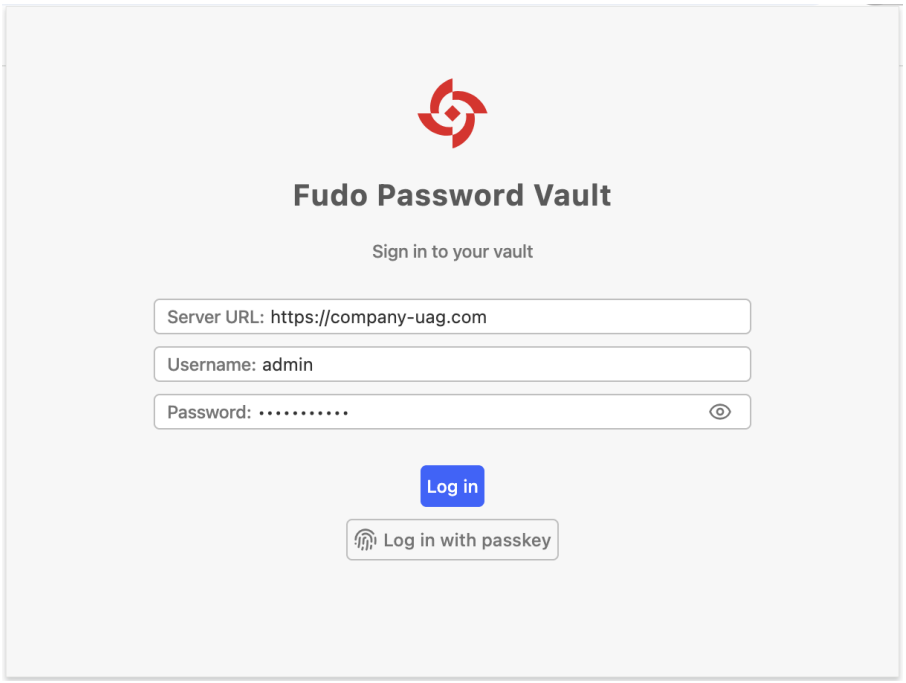
After installation, open the extension from the browser toolbar. In Chrome, click the **Extensions** (puzzle) icon, then select **Password Vault**; you can also pin it to the toolbar for quicker access.



11.5.3 Signing In

To start using the extension:

1. Open the extension from the browser toolbar.
2. Enter the User Access Gateway address of your Fudo Enterprise instance in the **Server URL** field.
3. Enter your Fudo Enterprise user **Username** and **Password**.
4. Click **Log in**.



Note

The connection to the User Access Gateway must use HTTPS with a publicly trusted certificate (issued by a public certificate authority).

Once signed in, the extension connects to User Access Gateway Fudo Enterprise and displays the secrets you are allowed to access.

Signing in with a passkey

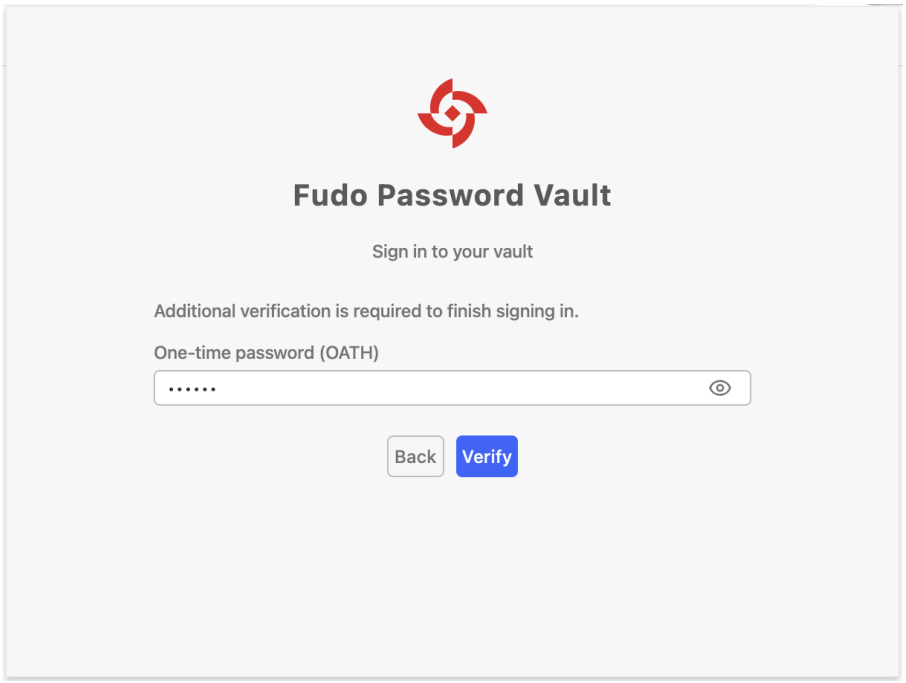
If your account is configured for FIDO2/Passkey authentication, click **Log in with passkey** below the **Log in** button instead of entering a password. The browser then prompts you for your passkey and completes the sign-in.

Note

Passkey sign-in works only when the **Server URL** is a hostname (FQDN), not an IP address - a browser will not use a passkey for an address such as `https://192.168.1.10/`. For details, see the FIDO2/Passkey authentication chapter.

Providing a second authentication factor

If your account requires a second authentication factor, the extension replaces the login form with a verification screen after you submit your credentials. The screen names the method the server expects - for example **One-time password (OATH)** - and provides a field for your response. Methods that require token enrollment additionally display an enrollment QR code.



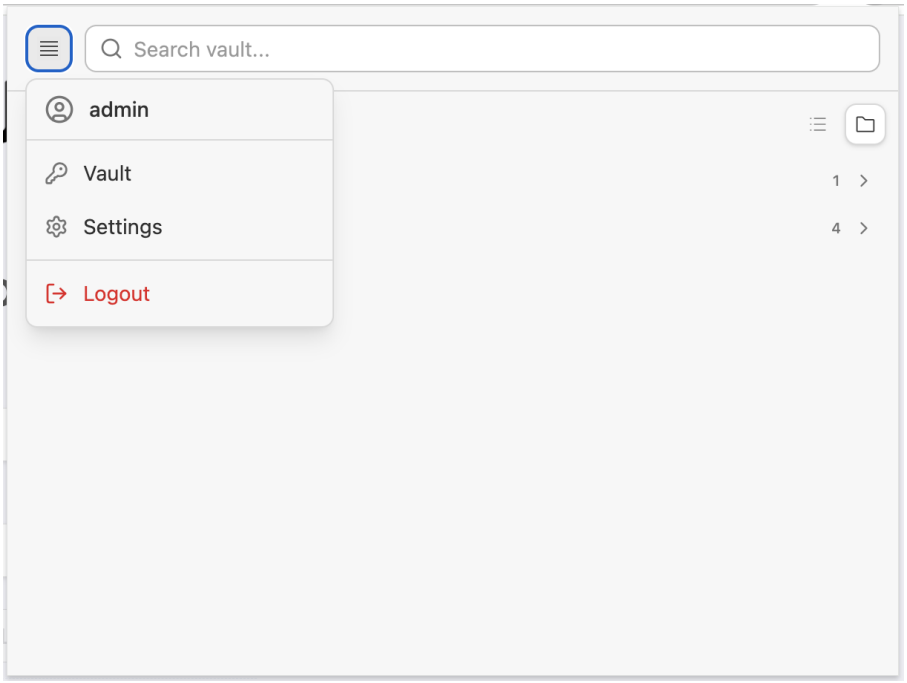
Enter the code provided by your authentication method and click **Verify**, or click **Back** to return to the login form. If the code is not accepted, the sign-in attempt is cancelled and you have to start over with **Back to sign in**.

Important

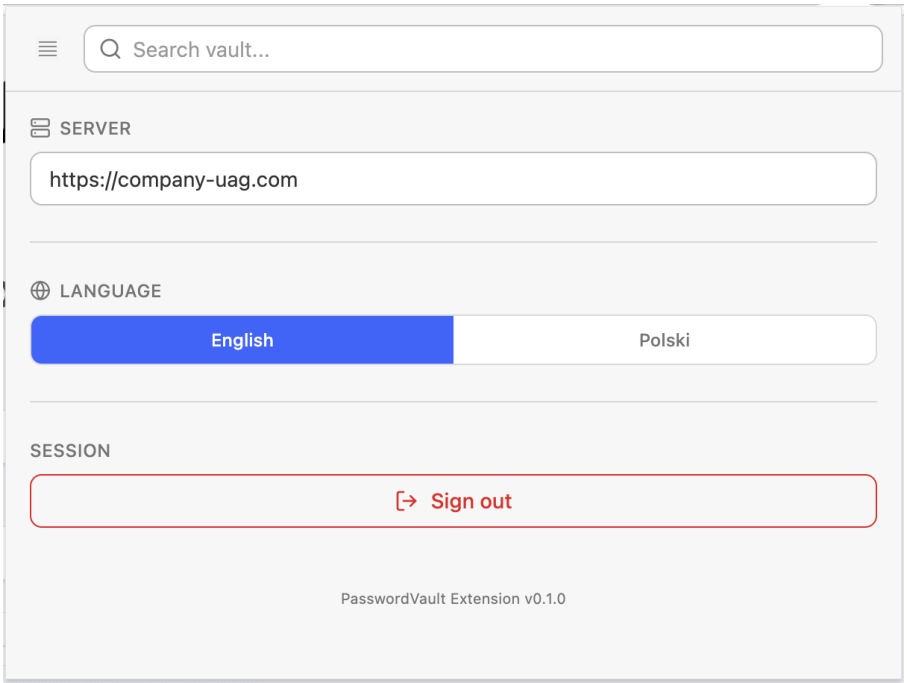
The available second-factor methods come from your user configuration in the Fudo Enterprise Admin Panel. The extension does not configure authentication - it only follows what the server requires.

11.5.4 Extension Menu and Settings

The menu button in the top-left corner opens the extension menu, which provides access to the **Vault**, the **Settings**, and the **Logout** option.

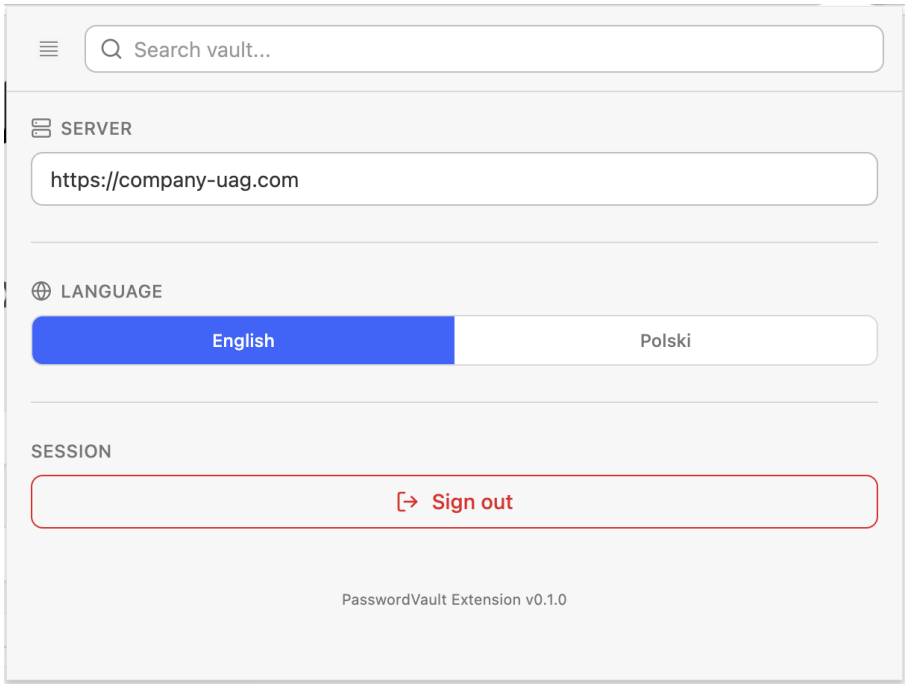


On the **Settings** screen you can review the **Server** (User Access Gateway) address and switch the interface **Language** between English and Polish.



11.5.5 Signing Out

To end your session, open the extension menu and select **Logout**, or click **Sign out** in the **Session** area of the **Settings** screen.



11.5.6 Browsing Collections and Secrets

After signing in, you can switch between a **collection view** and a **secret list view** using the buttons in the top-right corner, limit the list to a single vault with the **All** / **Organization** / **Personal** buttons, and use the **Search vault** field to find a secret by name.

Important

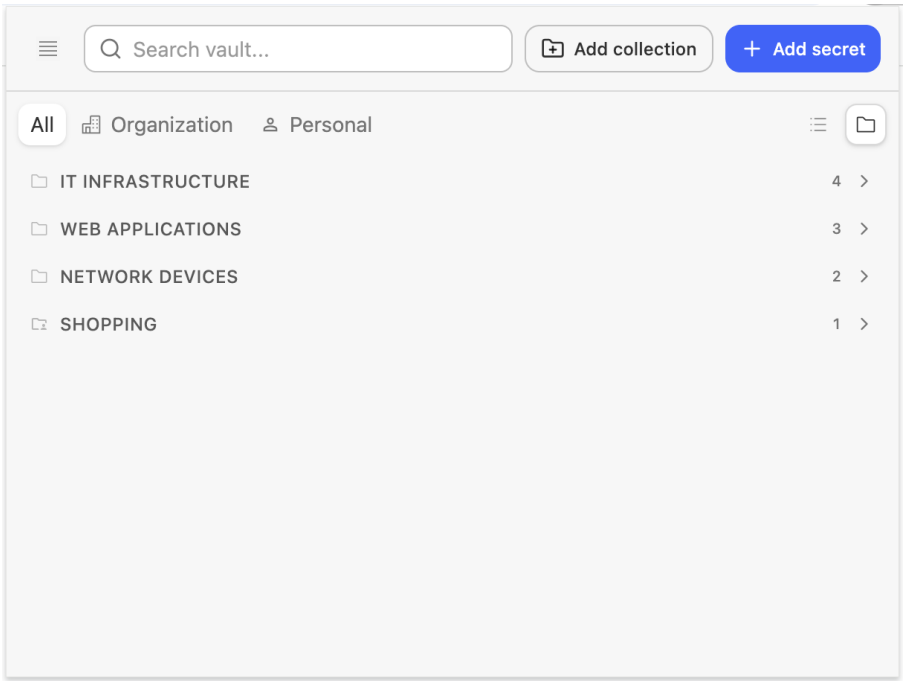
The extension reflects the same permissions configured in the Password Vault: you see only the collections and secrets you have been granted access to through object rights.

Filtering by vault

The buttons above the list limit it to secrets from one vault:

- **All** - secrets from both vaults. This is the default.
- **Organization** (building icon) - only secrets from the Organization Vault.
- **Personal** (person icon) - only your own secrets from the Personal Vault.

With the **All** filter active the two kinds can still be told apart: in the list view each secret carries the icon of its vault, and in the collection view personal collections use a different folder icon than organization ones.

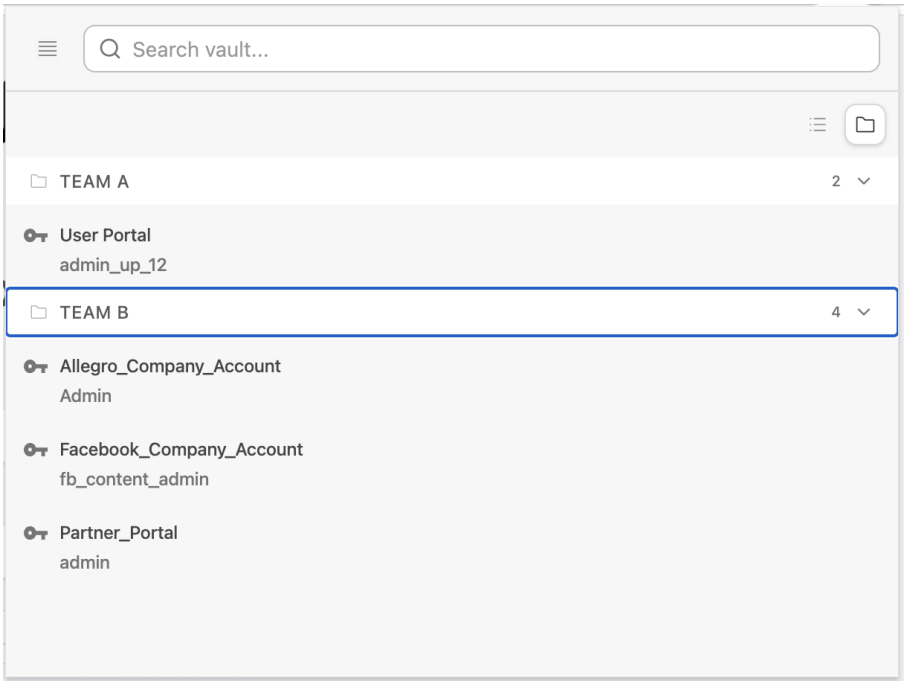


Important

The **Search vault** field searches **only within the selected vault**. With **Personal** selected you will not find an organization secret, and the other way round. If a secret you expect is missing from the results, switch the filter back to **All**.

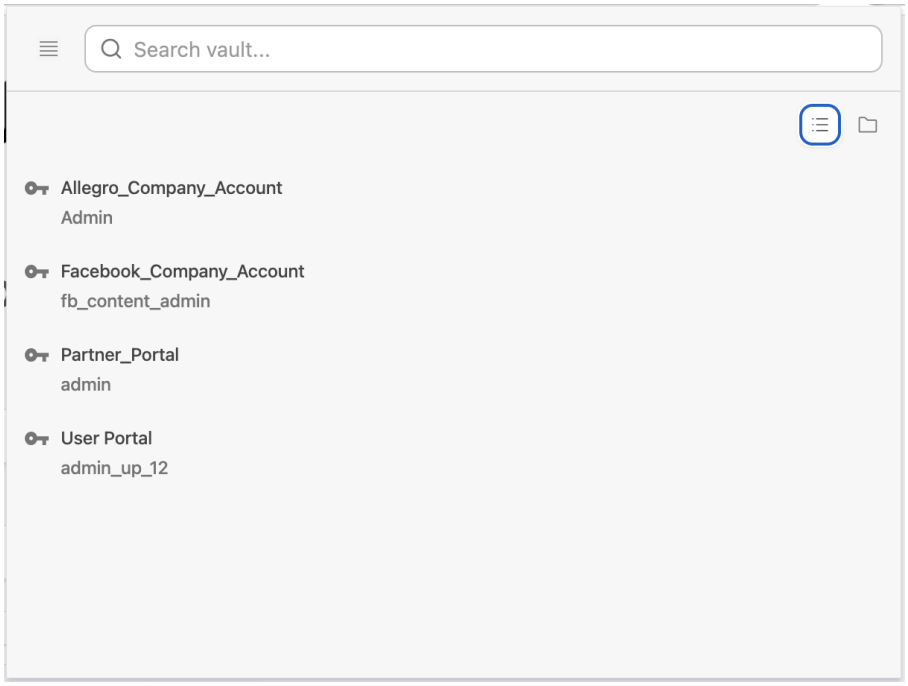
Collection view

The collection view groups secrets under the collections they belong to.



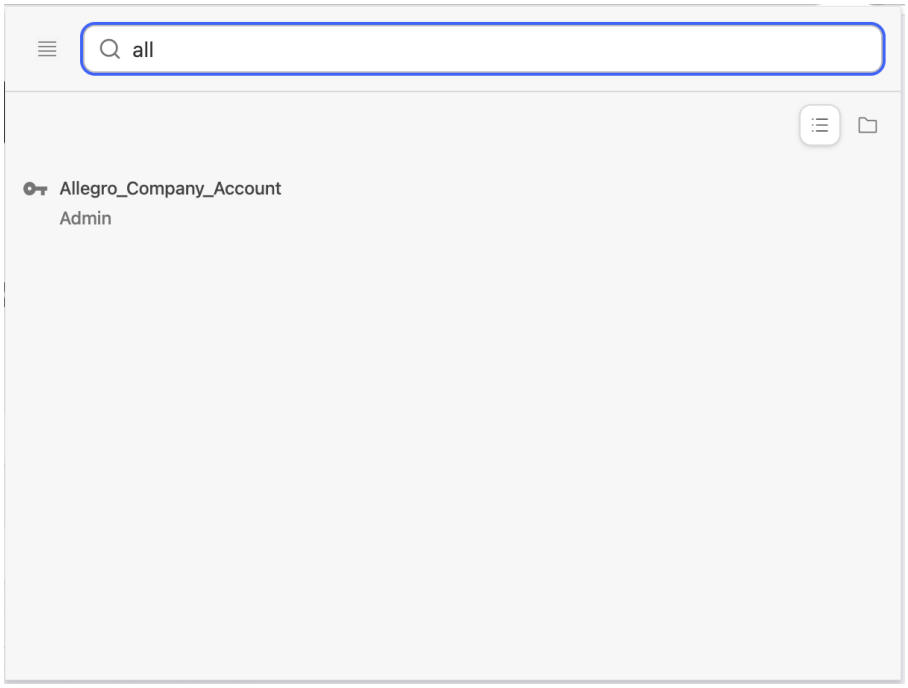
Secret list view

The list view shows all available secrets in a single flat list.



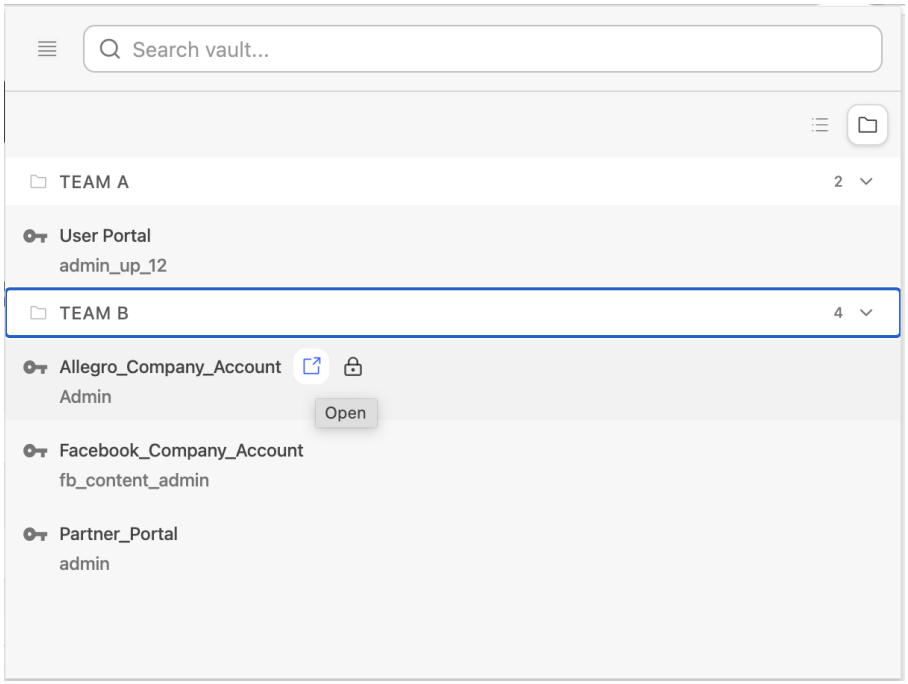
Search

Type in the **Search vault** field to filter secrets by name. The search covers only the vault selected with the **All** / **Organization** / **Personal** buttons.



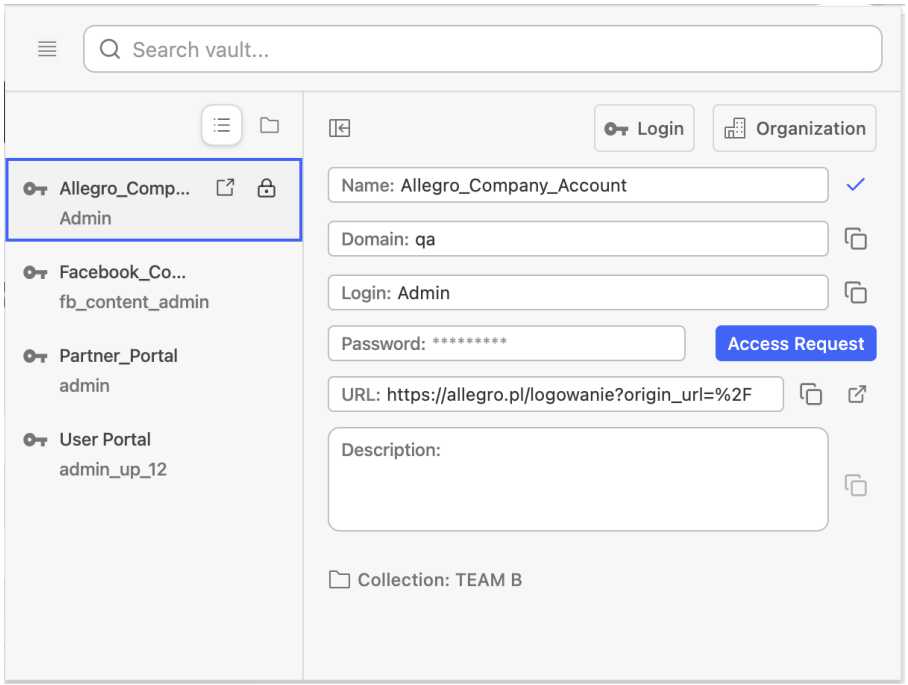
Opening a linked website

Each secret shows an **Open** icon that links to the website the secret is associated with. Selecting it opens the linked website directly in the browser.



Viewing secret details

Selecting a secret opens its details, where you can review fields such as **Name**, **Domain**, **Login**, **Password**, **URL**, and **Description**, and copy individual values to the clipboard.



Note

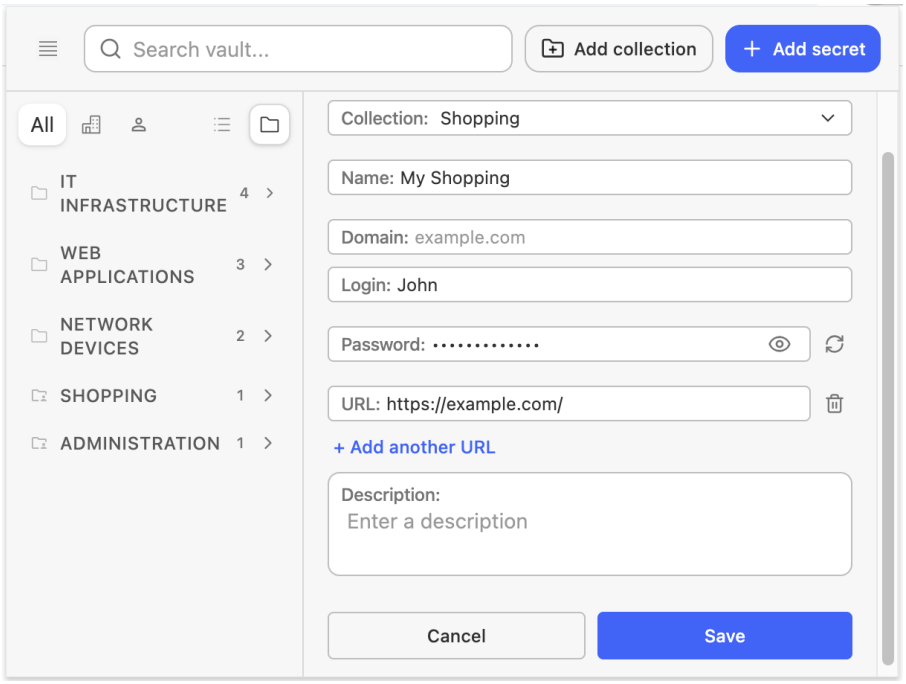
When a password is copied to the clipboard, it is automatically cleared after 30 seconds.

11.5.7 Creating and Editing Personal Secrets

Secrets and collections created in the extension always go to your **Personal Vault**. Organization Vault content is managed by administrators in the Fudo Enterprise Admin Panel and cannot be created or edited from the browser.

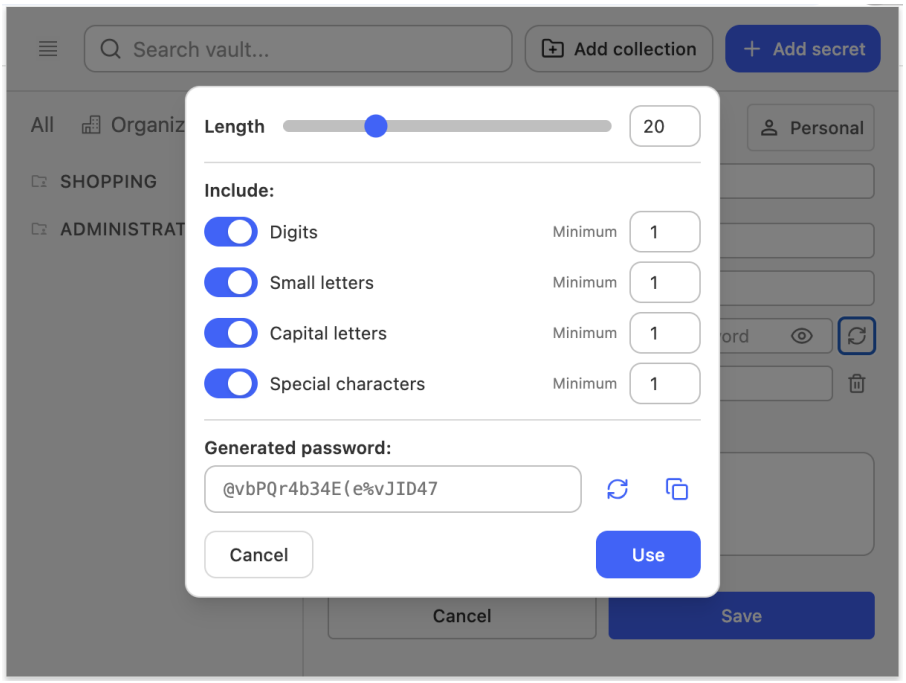
Creating a secret

1. Click **Add secret** in the top bar.
2. Select the **Collection** the secret belongs to. Only personal collections are listed. If you do not have any yet, the form shows **No personal collections available** - create a collection first.
3. Fill in the secret fields:
   - **Name** (required) - the name the secret is listed under.
   - **Domain** - the domain the credentials belong to.
   - **Login** (required) - the user name stored in the secret.
   - **Password** (required) - the password stored in the secret.
   - **URL** - the address the secret is matched against when autofilling. Click + **Add another URL** to store more addresses.
   - **Description** - optional notes.
4. Click **Save**.



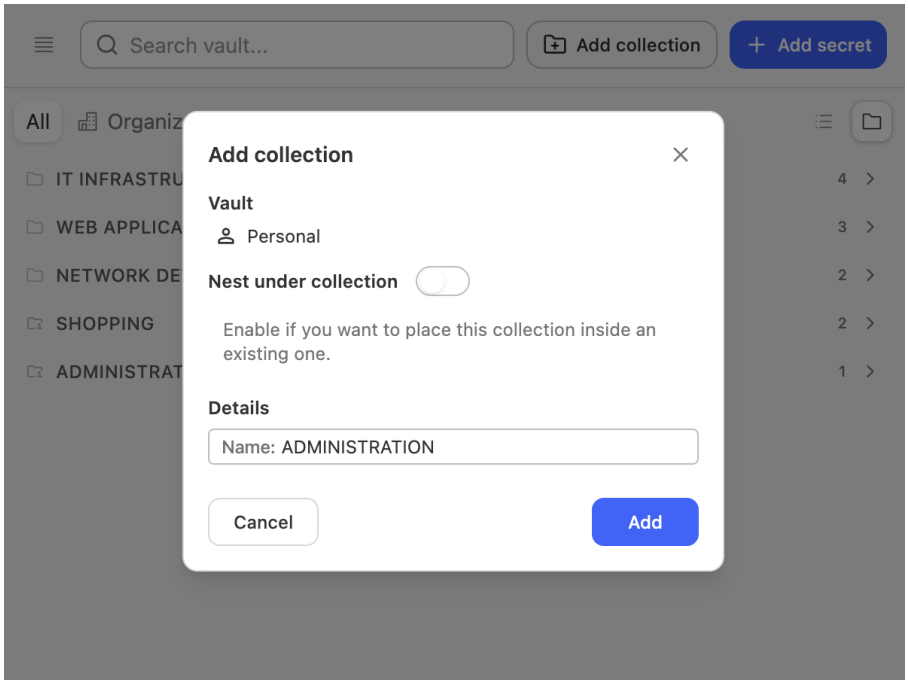
Generating a password

Instead of typing a password, click the generator icon next to the **Password** field. In the dialog that opens set the **Length**, switch on the character groups to **Include** (**Digits**, **Small letters**, **Capital letters**, **Special characters**) and the **Minimum** number of characters from each of them. The result appears under **Generated password** - use the icons next to it to draw another password or copy it to the clipboard, then click **Use** to insert it into the form.



Creating a collection

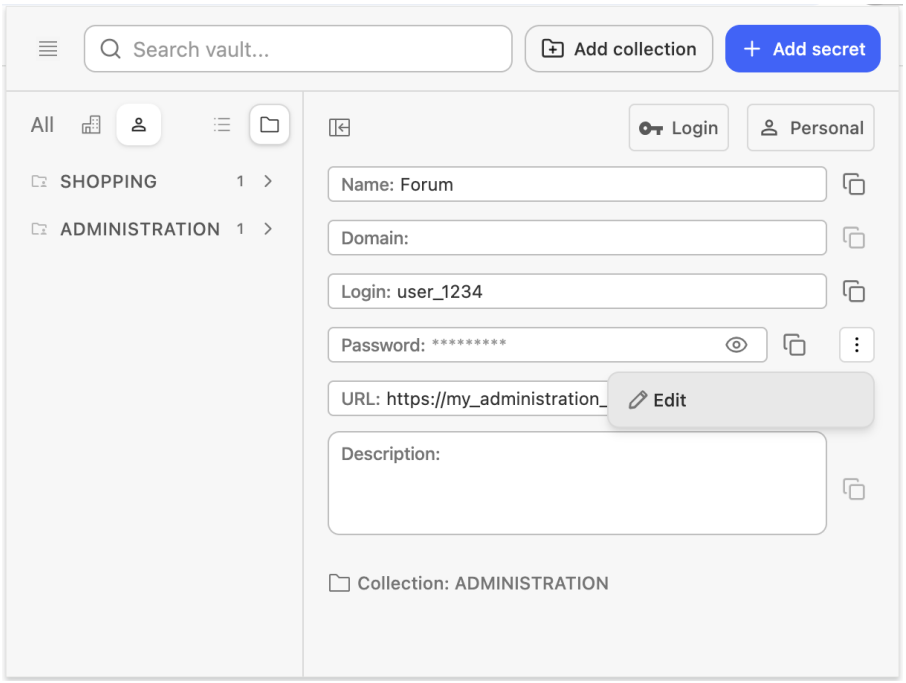
1. Click **Add collection** in the top bar.
2. The **Vault** is always **Personal** and cannot be changed.
3. To place the new collection inside an existing one, enable **Nest under collection** and select the parent collection.
4. Under **Details**, enter the collection **Name**.
5. Click **Add**.



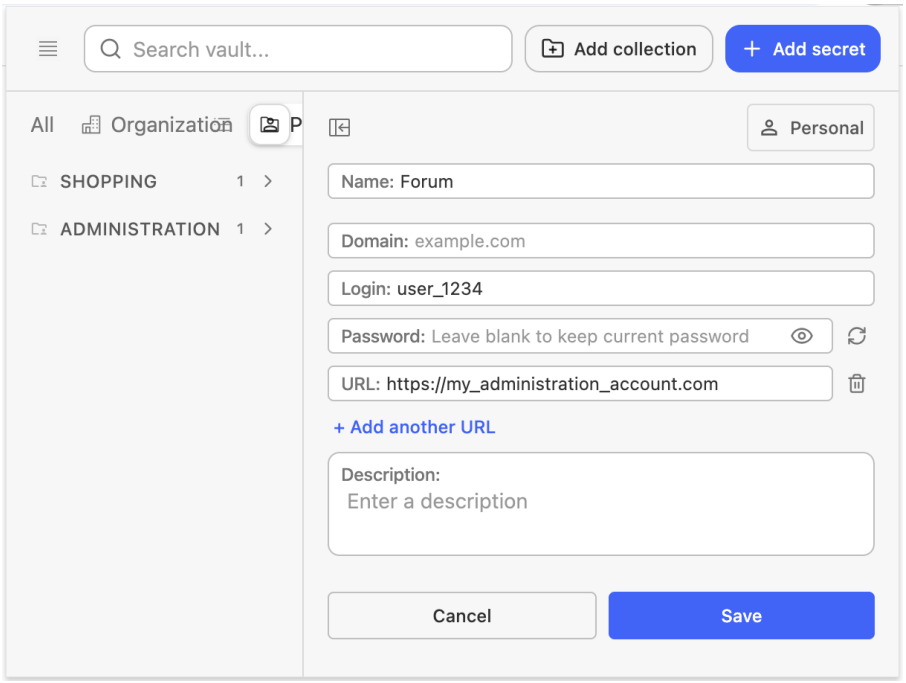
Editing a secret

Open a personal secret, click the three-dot (**More actions**) button next to the **Password** field

and select **Edit**.



The form is the same as when creating a secret, except that the collection cannot be changed. Leave the **Password** field empty to keep the current password.

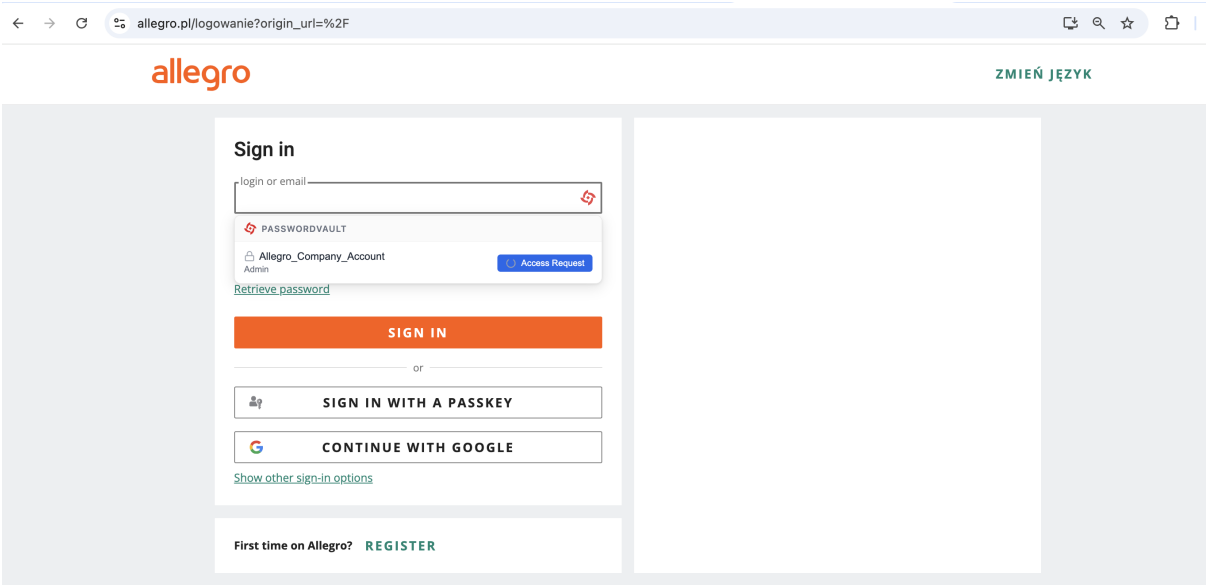


Note

Edit is available only for secrets from the Personal Vault. For organization secrets the **More actions** menu has no **Edit** entry.

11.5.8 Autofilling Credentials on Websites

When you open a page whose login form is recognized, the extension displays a suggestion bar offering to autofill the matching secret. Selecting the suggestion fills in the stored credentials, making access to web resources faster and more convenient.

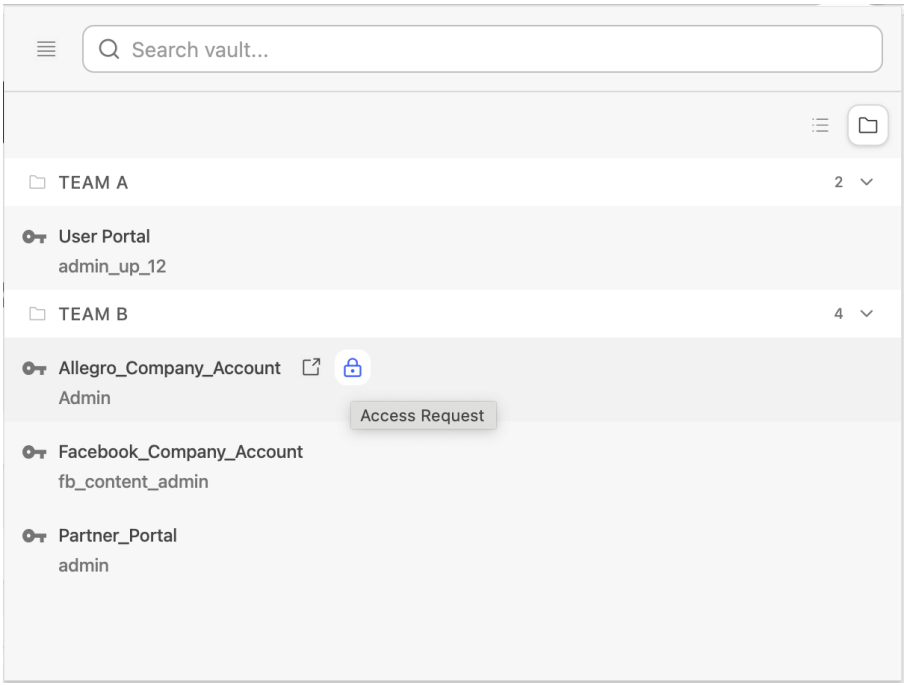


11.5.9 Access Requests, Exclusive Checkout, and Revoked Access

The extension supports Password Vault access workflows directly from the browser.

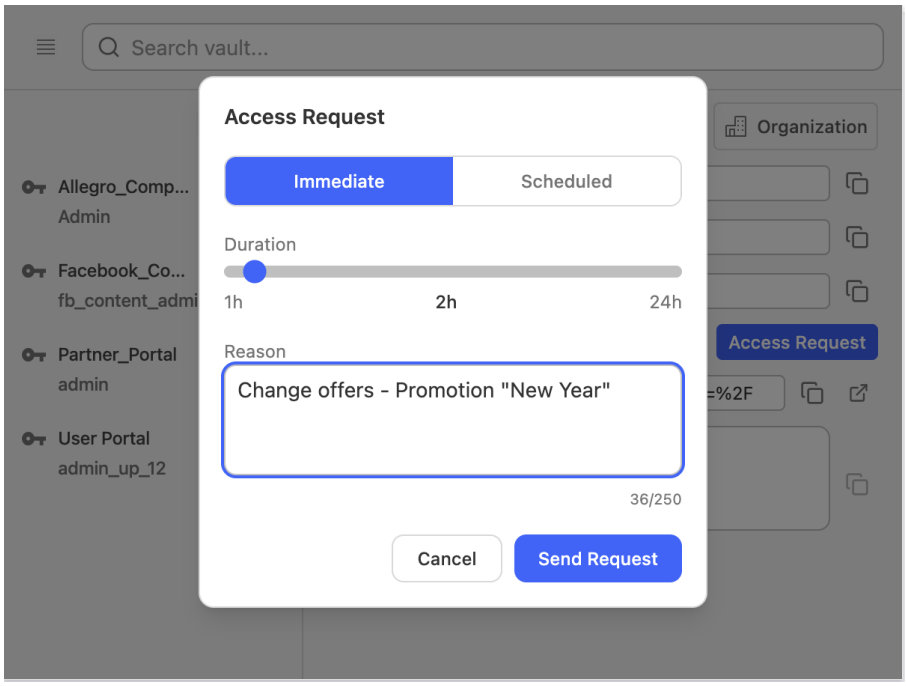
Requesting access

If a secret is configured for access on request, it is marked with a padlock (**Access Request**) icon. Hover over the secret and click the icon to request access.

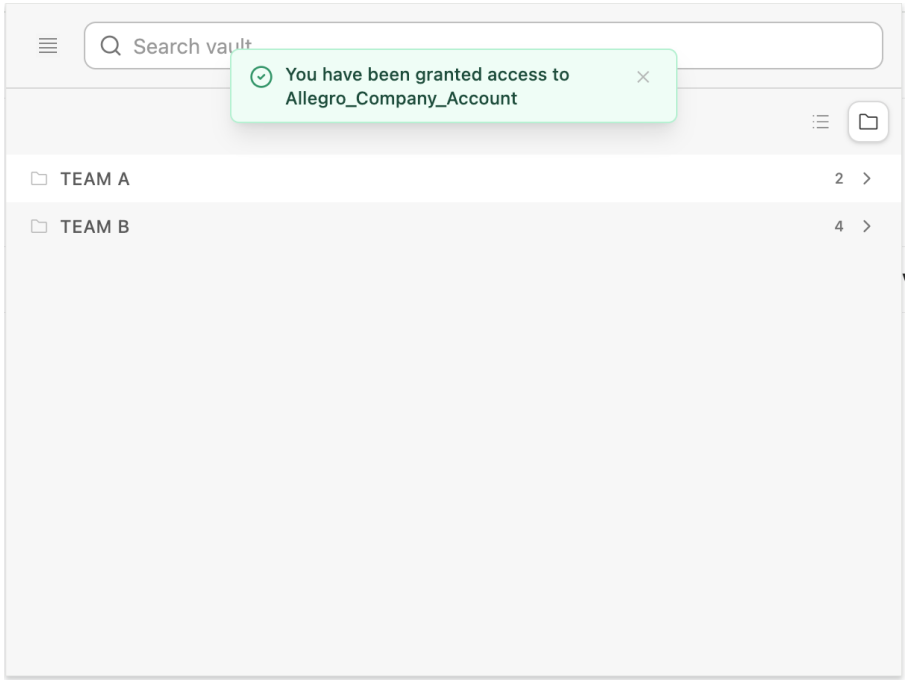


In the **Access Request** form, choose whether access should be granted **Immediate**ly or

Scheduled for later, set the **Duration**, enter a **Reason** for the request, and click **Send Request**.

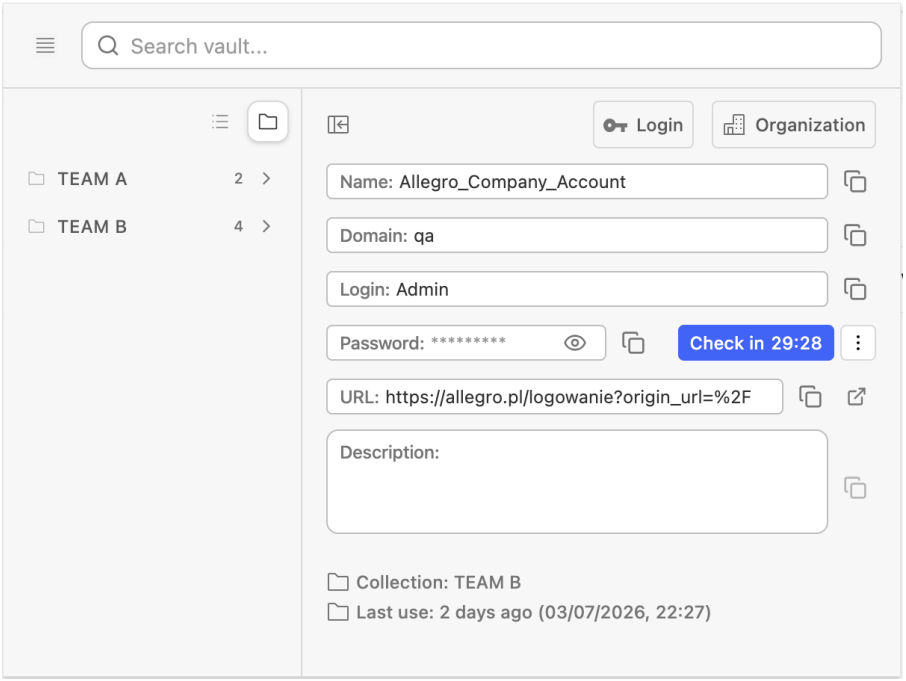


Once access is granted, the extension displays a confirmation notification.



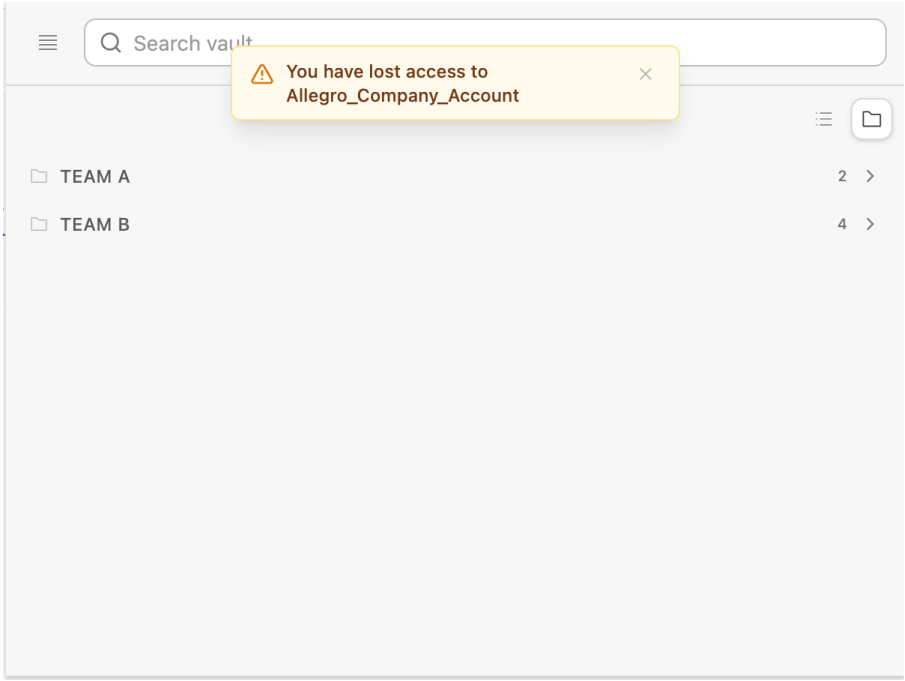
Exclusive checkout

For secrets protected with exclusive checkout, the **Check in** button in the secret details displays a countdown showing how much time remains before the checkout expires.



Revoked access

If your access to a secret is revoked, a crossed-out icon appears next to it and the secret is marked with an **Access refused** button in the list. The extension also displays a notification informing you that access has been lost.



Related topics:

- *Overview*
- *Managing Collection Object Rights*
- *Secret Access Monitoring*

11.6 Compromised Passwords

The Compromised Passwords feature in Password Vault allows administrators to upload lists of known compromised passwords to automatically detect and flag vulnerable credentials stored in the system. This proactive security measure helps organizations identify and replace passwords that may have been exposed in data breaches.

11.6.1 How It Works

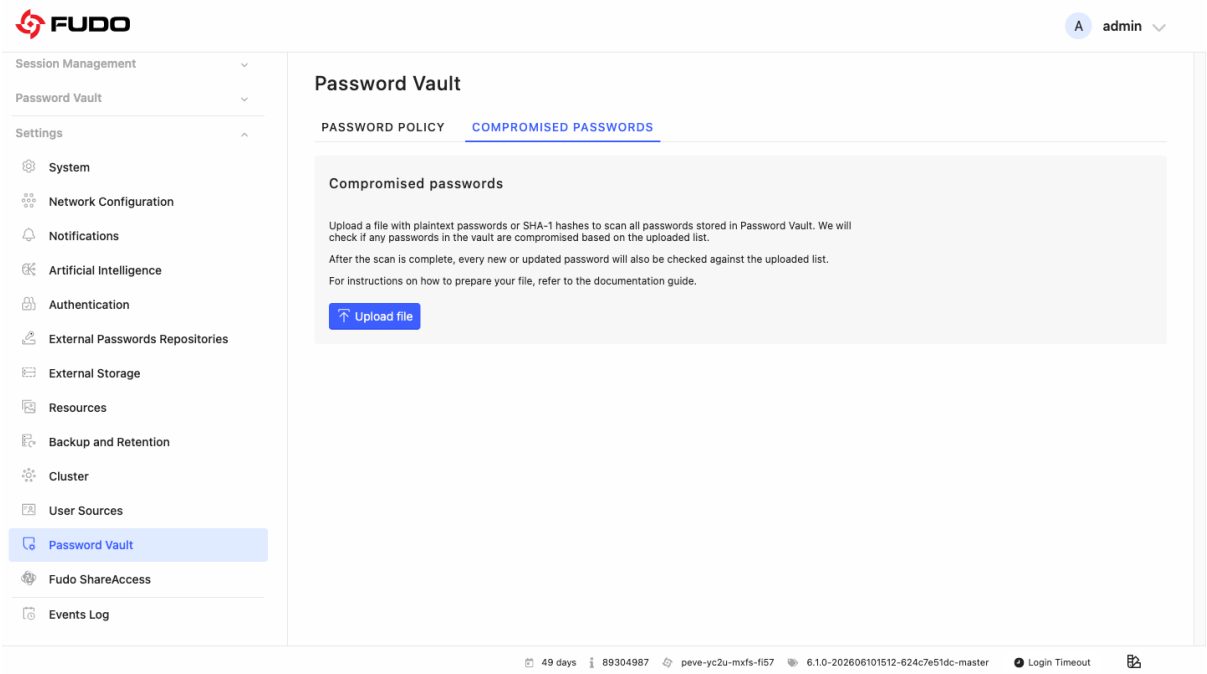
When a compromised password list is uploaded:

1. **Immediate Scan** - All existing passwords in Password Vault are automatically scanned against the uploaded list
2. **Continuous Monitoring** - Every new or updated password is checked against the compromised list
3. **Visual Indicators** - Compromised passwords are flagged with warning indicators in the Password Vault interface
4. **Security Reports** - Administrators can view reports of all compromised credentials

11.6.2 Accessing Compromised Passwords Settings

To access the Compromised Passwords feature:

1. Navigate to **Settings** > **Password Vault**.
2. Click on the **Compromised Passwords** tab.

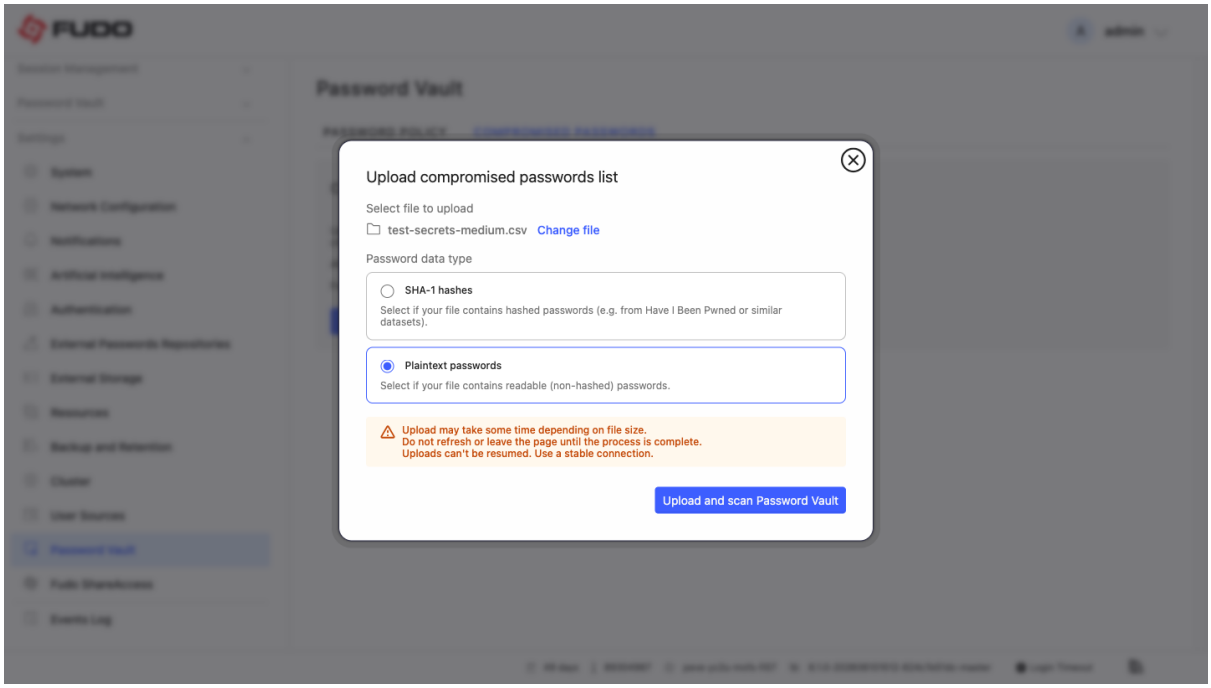


11.6.3 Uploading a Compromised Password List

To upload a list of compromised passwords:

1. Click the **Upload file** button.
2. Select your prepared file containing compromised passwords.

3. Choose the appropriate data type:
   - **SHA-1 hashes** - For files containing hashed passwords (e.g., from Have I Been Pwned)
   - **Plaintext passwords** - For files containing readable passwords
4. Click **Upload and scan Password Vault**



> **Note**
>
> The upload process may take some time depending on the file size. Do not refresh or leave the page until the process completes.

11.6.4 File Format Requirements

The system supports two types of compromised password files:

11.6.4.1 Plaintext Password Files

For plaintext password files, each entry should be placed on a separate line.

```
password
password123
asd
tajny-sekret
root
!! &lt;3
!! 11QQazx
!! 12Exodia
!! Angela11
```

11.6.4.2 SHA-1 Hash Files

For text files containing SHA-1 hashes, each entry should be placed on a separate line. An entry can contain either the hash only or the hash followed by an occurrence count, separated by a colon.

```
0018A45C4D1DEF81644B54AB7F969B88D65:1
00D4F6E8FA6EECAD2A3AA415EEC418D38EC:2
011053FD0102E94D6AE2F8B83D76FAF94F6:1
012A7CA357541F0AC487871FEEC1891C49C:2
0136E006E24E7D152139815FB0FC6A50B15:2
```

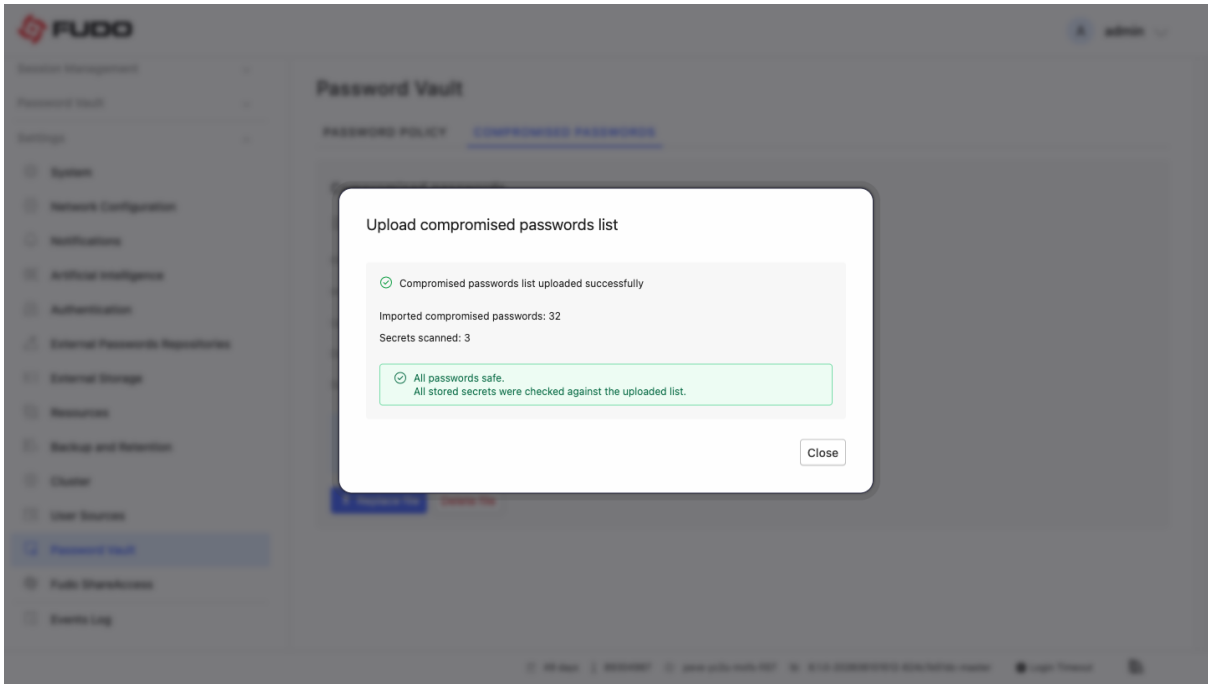
Format Specification:

- Each line contains an uppercase SHA-1 hash
- Optional occurrence count after a colon (e.g., `:1`)
- No headers required
- One hash per line

11.6.5 Scan Results

After uploading and scanning:

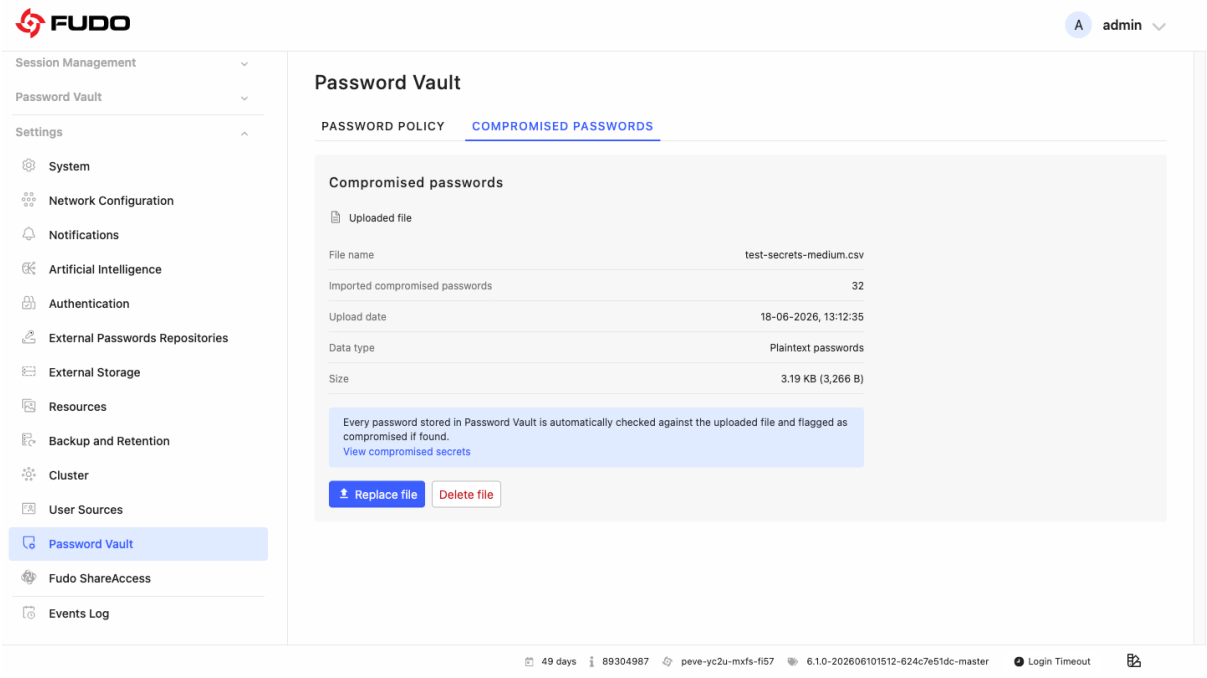
- The system displays the number of imported compromised passwords
- Shows how many secrets were scanned
- Indicates whether any compromised passwords were found
- Provides a link to view all compromised secrets in Password Vault



11.6.6 Managing Uploaded Files

Once a file is uploaded, you can:

- **View Details** - See file information including name, size, upload date, and number of imported passwords
- **Replace File** - Upload a new file to replace the existing compromised password list
- **Delete File** - Remove the compromised password list from the system
- **View Compromised Secrets** - Navigate to Password Vault to see all flagged secrets



Related topics:

- *Creating Secrets*
- *Creating Collections*
- *Overview*

11.7 Secret Changers

Fudo Enterprise features *secret changers*, which enable managing credentials to privileged accounts on monitored servers.

There are two separate secret-changer mechanisms, and which one applies depends on the *Object target* chosen when the changer is created:

- **Account (the classic path)** — Changers are assigned on the account itself, in the account's *SECRET CHANGERS* tab. This path works only for a *Regular* account that uses the *Password* method with a login defined.
- **Password / SSH key (the Password Vault path)** — These changers are assigned to the secret in the *Password Vault*, not on the account. A changer whose *Object target* is *SSH key* can be attached only to an *SSH Key*-type secret, from the secret's *CHANGERS* tab.

Secret verifiers are assigned the same way. For an end-to-end example, see *Configuring SSH Key Rotation for an Account*.

Note

The *Add changer* and *Add verifier* drop-down lists show only the secret changers whose *Object target* matches the type of the secret being edited.

Secret changers run on a separate transport layer: SSH, LDAP, Telnet or WinRM, and you can either use one of the built-in ones or *create your own script*.

The built-in secret changers cover the following scenarios:

- Unix over SSH
- MySQL over SSH
- Cisco over SSH and Telnet
- Cisco Enable Password over SSH and Telnet
- WinRM
- LDAP

11.7.1 Secret Changer Policy

Secret Change Policy defines specifics of how frequently secrets (passwords and SSH keys) should be changed, along with complexity requirements for passwords and configuration settings for SSH keys.

11.7.1.1 Defining a Secret Changer Policy

1. Select *Management* > *Secret Changers*.
2. Go to *Secret Change Policies* tab.
3. Click *+ Add Secret Change Policy*.
4. Enter object name.
5. Enable the *Secret change* option to configure change settings:
   - **Change frequency** - Specify the time interval between each secret change.
6. Configure **Password settings** (for password-based secrets):
   - Set password **Length** (number of characters).
   - Configure password **Complexity** requirements:
     - Select character types to include (Digits, Small letters, Capital letters, Special characters)
     - Define minimum count for required character types
7. Configure **SSH Key settings** (for SSH key-based secrets):
   - Select **SSH Key algorithm** from the dropdown:

  - RSA (default: 4096 bits)
  - ECDSA
  - ED25519

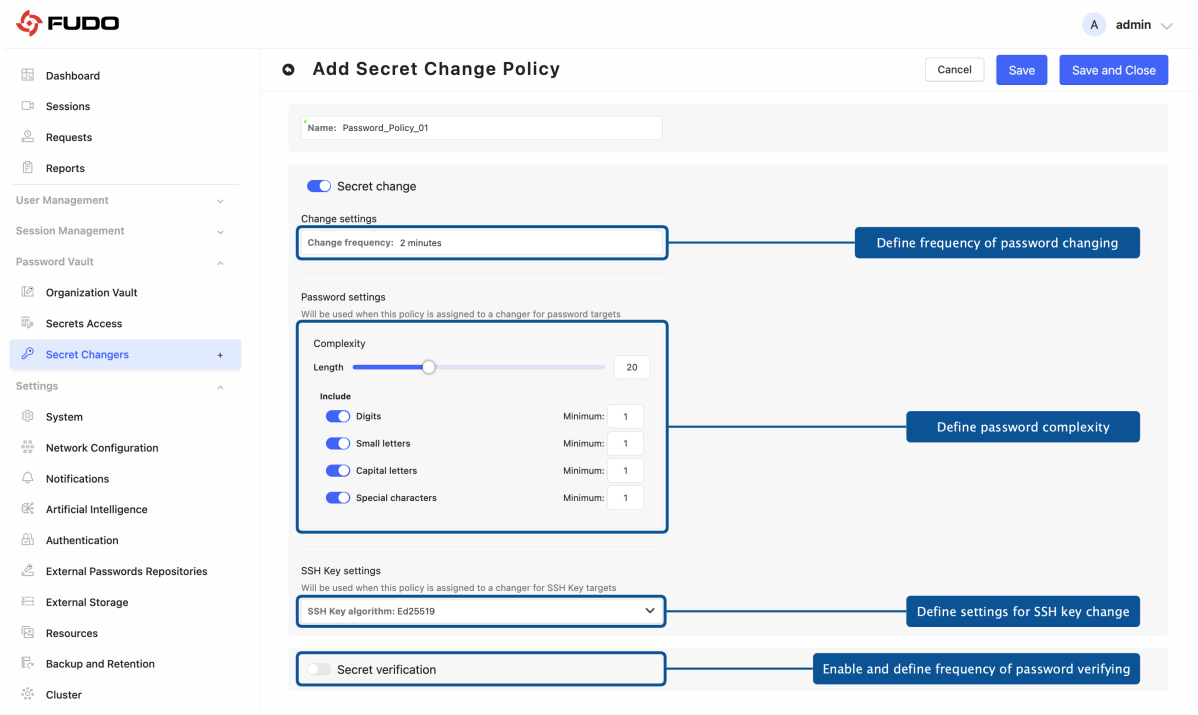
8. Enable the *Secret verification* option to configure verification settings.
9. Specify the time interval between each secret verification.

Parameter	Description
Password Settings	
Length	Provide the number of characters comprising the password.
Small letters	Select to include lowercase characters, define their minimal number.
Capital letters	Select to include uppercase characters, define their minimal number.
Special characters	Select to include special characters, define their minimal number.
Digits	Select to include digits, define their minimal number.
SSH Key Settings	
SSH Key algorithm	Select the algorithm for SSH key generation (RSA, ECDSA, ED25519).
Key size	For RSA keys, the default key size is 4096 bits.

Note

The sum of the enforced password requirements cannot be greater than the specified password length.

9. Click *Save*.

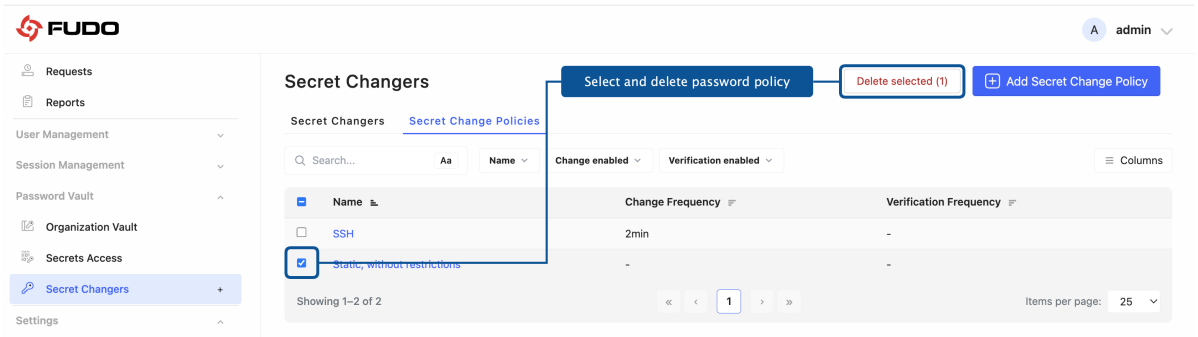


11.7.1.2 Editing a Secret Changer Policy

1. Select *Management* > *Secret Changers* > *Secret Change Policies*.
2. Go to *Secret Change Policies* tab.
3. Find and click desired object to open its configuration page.
4. Modify configuration parameters as needed.
4. Click *Save*.

11.7.1.3 Deleting a Secret Changer Policy

1. Select *Management* > *Secret Changers*.
2. Go to *Secret Change Policies* tab.
3. Find and select desired objects.
4. Click *Delete selected*.
5. Click *Delete object* to confirm deletion of selected objects.



Related topics:

- *Data Model*
- *Accounts*
- *Custom Secret Changers*
- *Setting up Secret Changing on a Unix System*

11.7.2 Custom Secret Changers

Custom secret changers enable defining a set of commands executed on a remote host in case the built-in secret changers cannot handle a specific use case scenario. Secret changers can be configured to manage either user account passwords or SSH keys, depending on the selected object target.

Note

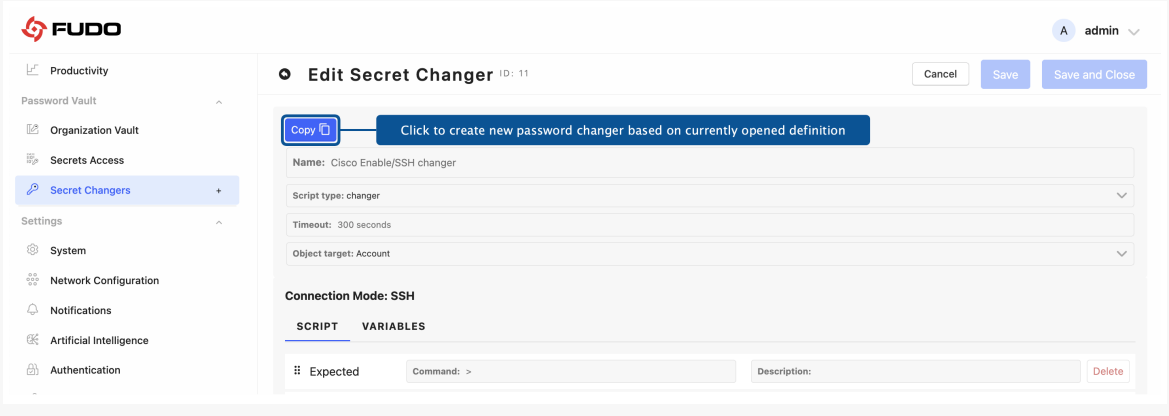
In cluster configuration, the node responsible for changing passwords on monitored systems is configured in system settings. For more information refer to *Secret Changers - Active Cluster Node* topic.

11.7.2.1 Defining a Custom Secret Changer

1. Click + icon in the main menu next to the *Secret Changers* tab, or
2. Select *Management* > *Secret Changers* and click + *Add secret changer*.

Note

Alternatively, you can edit existing secret changer and click Copy to create a new secret changer based on currently opened definition.



3. Define the secret changer's name.
4. From the *Script type* drop-down list, select if the script is a secret changer or Secret verifier.
5. In the *Timeout* field, define the script's execution time limit.
6. From the *Object target* drop-down list, select the target type:
   - **Password** - Manages a *Login* (password) secret stored in the Password Vault.
   - **SSH key** - Manages an *SSH Key* secret stored in the Password Vault.

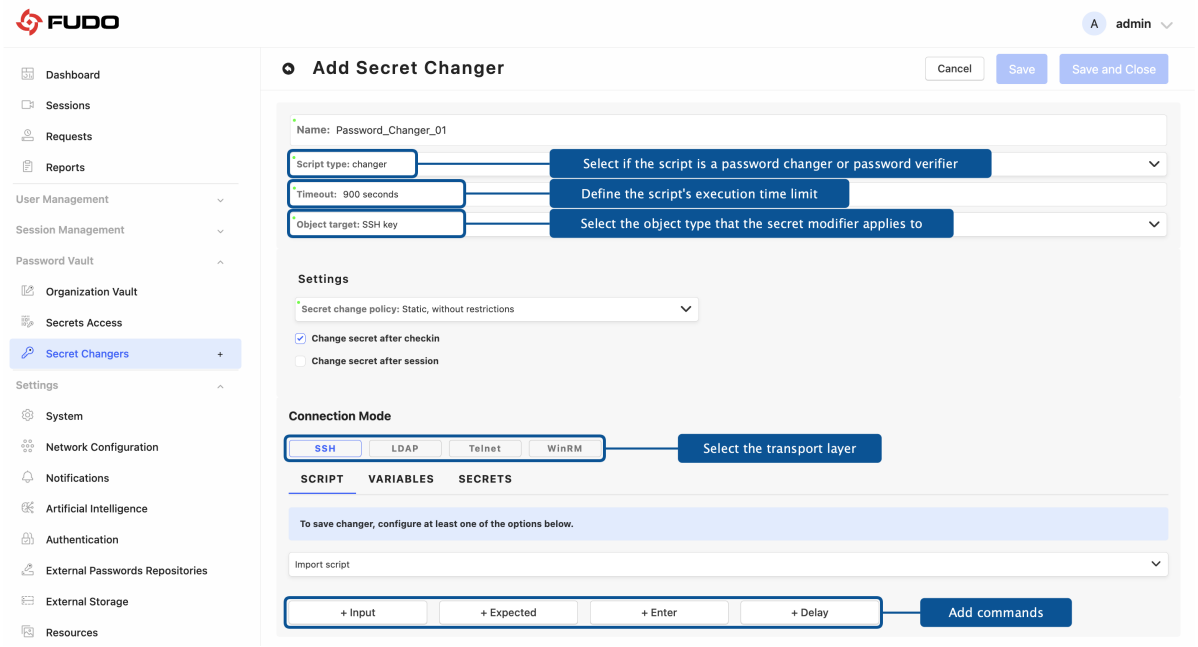
- **Account** - Manages the secret of a monitored account; assigned in the account's *SECRET CHANGERS* tab.

7. If the object target is *Password* or *SSH key*, the *Settings* section appears. From the *Secret change policy* drop-down list, select a policy.
8. Optionally, enable *Change secret after checkin* and *Change secret after session*.

Note

A *Secret change policy* defines settings shared by both changers and verifiers, so one policy can describe how a secret is changed and how it is verified. Selecting a policy here does not enable verification on its own - the secret is verified only when a secret verifier is also assigned to the secret in its *Changers* tab. If only a changer is assigned, the secret is changed but not verified, even when the policy includes verification settings.

9. In the *Connection mode* section, click *SSH, LDAP, Telnet,* or *WinRM* to select the transport layer.
10. In the *SCRIPT* tab, click one of available options to add a command.



Note

Available commands depend on selected transport layer. For more information on connection modes, refer to the *Connection Modes* topic.

- `+Input` - command executed on target host.
- `+Expected` - output that is expected after executing a command.
- `+Enter`
- `+Delay` - delay between commands' execution.
- `DN` - directory service DN (Distinguished Name) parameter.

- `Filter` - directory service user filter.

Warning

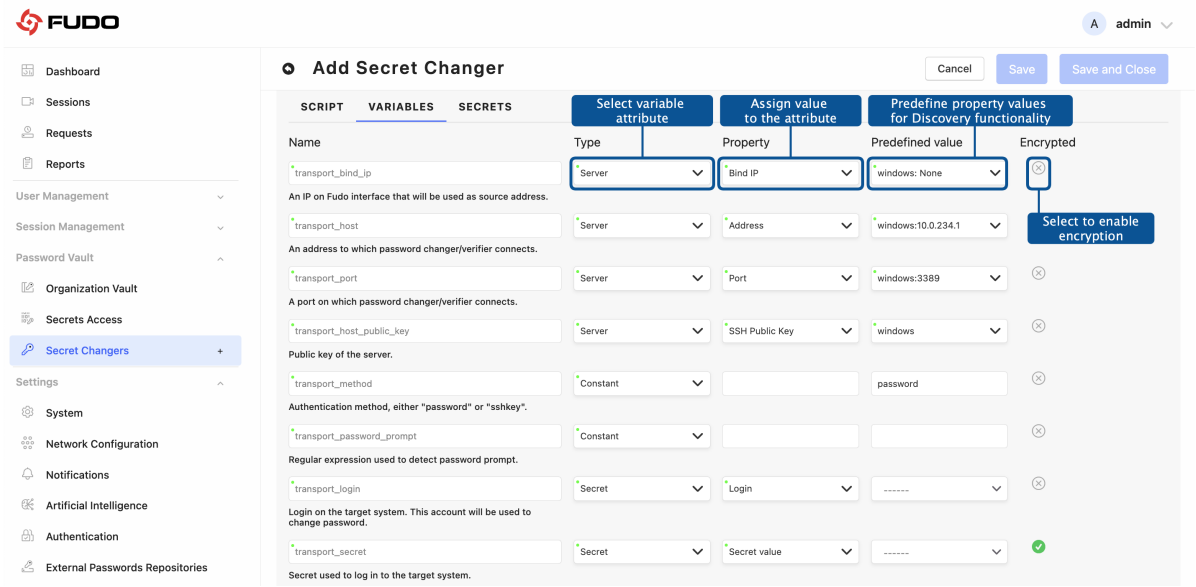
- To handle a secret change, you must use an account (`transport_login` and `transport_secret`) that has delegated *Reset user passwords and force password change at next logon* permissions for the *Organizational Unit (OU)* containing the users whose passwords will be changed, or the account must be a member of the *Account Operators* group.
- To configure **WinRM** secret changers, you need to provide user credentials with the authority to change passwords (typically an admin-level account). However, it's important to avoid using this account to change its own password, as WinRM will return an error that Fudo Enterprise cannot process. **Make sure that the ``account_login`` and ``transport_login`` variables are set to different values.**

11. Enter the command or define action's parameters.

Note

You can use pre-defined transport layer or user defined variables in commands. To use or define a variable, enclose it in %% characters (e.g. `%%transport_host%%`, `%%custom_variable%%`).

12. Repeat steps 10-11 to add more commands.
13. In the *Variables* tab, define variables' attributes.



Note

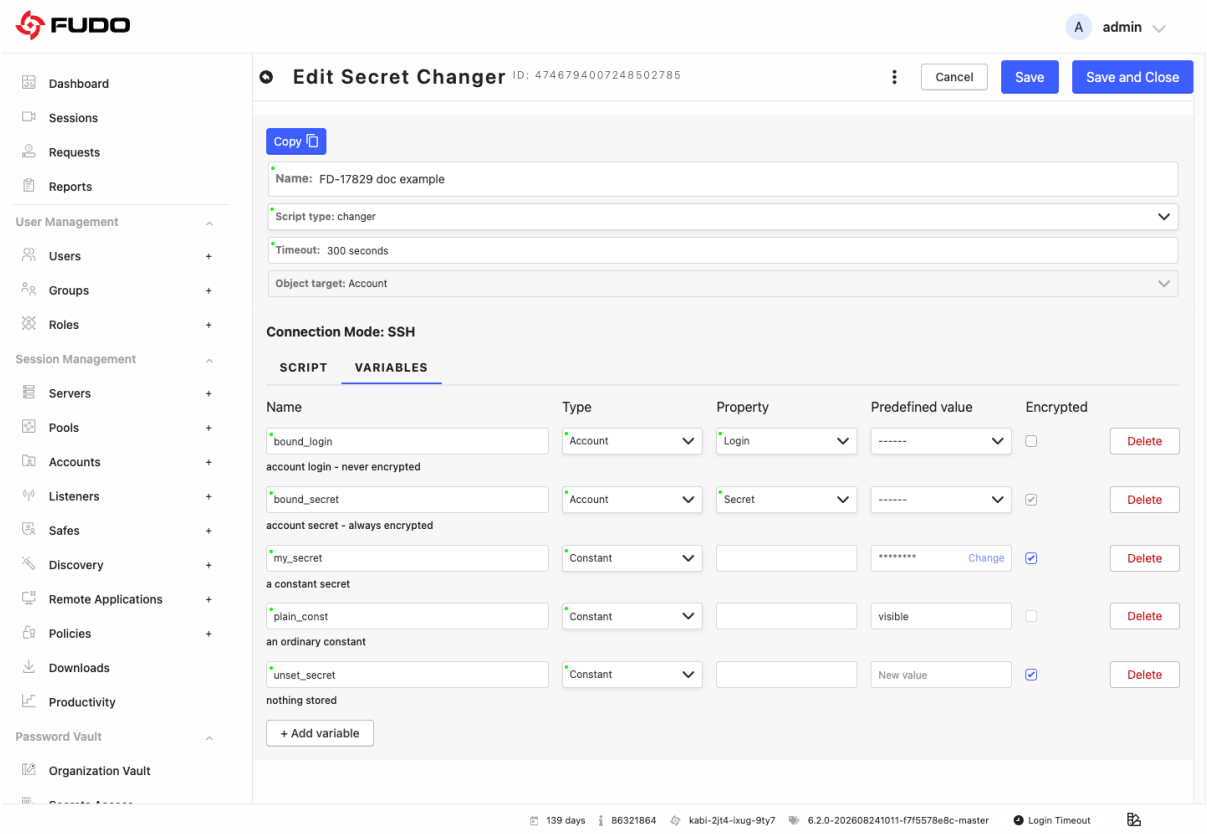
- Variables can be initiated with values referenced from other objects or they can be assigned a constant value.

- Predefine the property values so that the secret changer assigned to the account during the *Discovery* process will not require any additional configuration.
- A variable holding a constant can be encrypted, so that its value is never shown again. For more information refer to the *Encrypted Constant Values* topic.

14. Click *Save*.
15. *Define secret change policy* and *assign the secret changer to account*.

11.7.2.2 Encrypted Constant Values

A variable of type *Constant* can be marked as *Encrypted*. Its value is then stored encrypted with the system master key and is decrypted only on Fudo Enterprise, at the moment the secret changer script runs. Use it for values the script needs but that must not be readable afterwards, such as a shared enable password or an API token.



Note

Encrypted can be set only for variables of type *Constant*.

Once a value has been stored, the *Predefined value* field shows a mask instead of the value, followed by the *Change* button.

Warning

A stored encrypted value cannot be read back. Keep your own copy of any value you may need again.

Replacing a stored value

1. Click *Change* next to the masked value. The mask is replaced by an empty *New value* field.
2. Enter the new value.
3. Click *Save*.

To abandon the replacement and keep the value that is already stored, click the close button next to the *New value* field. It is shown only for a variable that has a value stored.

11.7.2.3 Password Changer Configuration Example

In this secret changer example, the password change is triggered with the `passwd` command executed with *sudo* privileges on a host running FreeBSD operating system.

Commands list

	Action	Content	Comment
1	EXPECTED	`Password`	Expected terminal output with a 'Password' word in it.
2	INPUT	`%%transport_secret%%`	A value of the `transport_secret` variable is a secret for authorizing a privileged account to change the password.
3	EXPECTED	`\[newtd_pc@john-laptop.*\]`	Expected terminal output within given regular expression.
4	INPUT	`sudo passwd %%account_login%%`	Change password for account where `account_login` reflects a login of the user, whose password is being changed.
5	EXPECTED	`Password`	Expected terminal output with 'Password' word in it.
6	INPUT	`%%transport_secret%%`	A value of the `transport_secret` variable is a secret for authorizing a privileged account to change the password.
7	EXPECTED	`Changing local password`	Expected terminal output with 'Changing local password' phrase in it.
8	EXPECTED	`New Password`	Expected terminal output with 'New Password' phrase in it.
9	INPUT	`%%new_secret_value%%`	A value of the `new_secret_value` variable would be a new password.
10	EXPECTED	`Retype New Password`	Expected terminal output with 'Retype New Password' phrase in it.
11	INPUT	`%%new_secret_value%%`	A value of the `new_secret_value` variable would be a new password.
12	INPUT	`echo $?`	
13	EXPECTED	`0`	

Variables

Variable name	Object type	Object property	Encrypted
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	✗

11.7.2.4 Editing a Custom Secret Changer

1. Select *Management* > *Secret Changers*.
2. Click the name of desired secret changer.
3. In the *Script* tab, edit selected commands.
4. Click *Delete* to remove selected command.
5. Click *Save*.

11.7.2.5 Deleting a Custom Secret Changer

1. Select *Management* > *Secret Changers*.
2. Select custom secret changer and click *Delete selected*.
3. Confirm deleting selected objects.

Related topics:

- *Secret Changers - Active Cluster Node*
- *Connection Modes*
- *Accounts*
- *Secret Changer Policy*
- *Setting up Secret Changing on a Unix System*
- *Configuring SSH Key Rotation for an Account*

11.7.3 Importing and Exporting Secret Changers

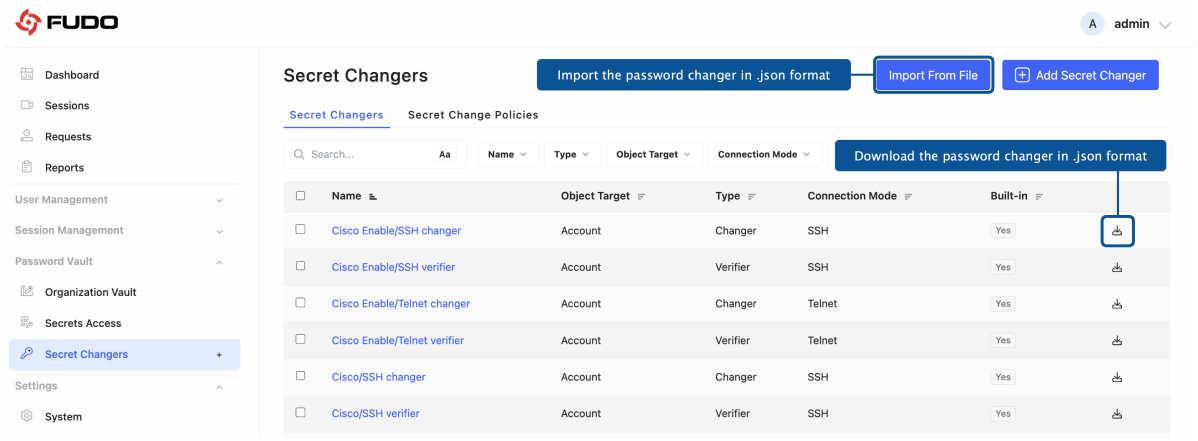
Secret changers created in Fudo Enterprise can be downloaded and imported into another instance of Fudo Enterprise.

11.7.3.1 Exporting a Secret Changer

To download selected secret changer:

1. Select *Management* > *Secret Changers*.
2. Go to *Secret Changers* tab.

3. Click the download icon next to the selected secret changer to download it.



11.7.3.2 Importing a Secret Changer

To import the `.json` file of a secret changer:

1. Select *Management* > *Secret Changers*.
2. Go to *Secret Changers* tab.
3. Click the *Import from file* button to import the file.
4. Drag and drop the file into the import window, or browse the file system to locate the desired `.json` file for a secret changer.
5. Click *Send data* to import the file, or *Clear data* to abort the import.

Related topics:

- *Data Model*
- *Accounts*
- *Custom Secret Changers*
- *Setting up Secret Changing on a Unix System*

11.7.4 Connection Modes

Connection modes specifies transport layer used in the secret change process. The transport layer determines the list of available commands and default variables.

11.7.4.1 SSH

SSH connection mode uses SSH protocol to establish connection with remote host.

Commands

Command	Description
INPUT	Command executed on target host.
EXPECTED	Expected result.
ENTER	
DELAY	Delay between commands' execution.

Variables

Variable	Description
transport_bind_ip	Fudo IP address used to establish connection with the remote host.
transport_host	An IP address of the remote host that the secret changer/verifier connects to.
transport_host_public_key	Public key of the remote host.
transport_login	An account on the target system authorized to change secrets.
transport_method	Transport layer authentication method: `password` or `sshkey`.
transport_password_prompt	Regular expression describing the password prompt. **Note** In case this parameter is defined as *constant* but the user does not explicitly define the value after the secret changer is assigned to the account, the default string will be used to determine the password prompt.
transport_port	A port number that the secret changer/verifier connects to.
transport_secret	Secret used to authorize the account to execute secret change.
account_login	Login of the user whose secret is being changed.
new_secret_value	System default variable initiated with the value automatically generated by Fudo.
account_secret	Password for the account. This password will be verified.
enable_password	Password for raising privileges.
mysql_login	Login for the privileged MySQL account.
mysql_password	Password for the privileged MySQL account.

11.7.4.2 LDAP

LDAP transport layer runs an LDAP query to change the password property of an object defined in the directory service.

Commands

Command	Description
DN	Directory service DN (Distinguished Name) parameter.
FILTER	Directory service user filter.

Note

Secret changers based on the LDAP transport layer can have only one command defined.

Variables

Variable	Description
transport_base	Base distinguished name.
transport_bind_ip	Fudo IP address used to establish connection with the remote host.
transport_ca_certificate	CA certificate of the target system.
transport_domain	Domain used to login to the target system.
transport_encoding	Text encoding used by the target system.
transport_host	An IP address of the remote host that the secret changer/verifier connects to.
transport_kerberos_enabled	Enables Kerberos authentication for this transport layer. Set to `true` to enable (default `false`). Kerberos authentication must be enabled explicitly — there is no fallback mechanism. See *Kerberos Authentication Settings*.
transport_login	An account on the target system authorized to change secrets.
transport_port	A port number that the secret changer/verifier connects to.
transport_secret	Secret used to authorize the account to execute secret change.
transport_server_certificate	Certificate of the target server.
account_domain	Domain of the user whose secret is being changed.
account_login	Login for the account for which password will be changed.
new_secret_value	System default variable initiated with the value automatically generated by Fudo.

Warning

In the LDAP transport layer you can provide both the `transport_ca_certificate` (CA certificate) and `transport_server_certificate` (server certificate) variables at the same time. When both are defined, both are enforced during the TLS handshake. In earlier versions, the CA certificate was ignored if a server certificate was provided. As a result, existing configurations that set both certificates may stop working — keep only the certificate you actually use configured.

11.7.4.3 Telnet

Telnet connection mode uses Telnet protocol to establish connection with remote host and continue to communicate with the server in order to change the secret.

Commands

Command	Description
INPUT	Command executed on target host.
EXPECTED	Expected result.
ENTER	
DELAY	Delay between commands' execution.

Variables

Variable	Description
transport_bind_ip	Fudo IP address used to establish connection with the remote host.
transport_host	An IP address of the remote host that the secret changer/verifier connects to.
transport_login	An account on the target system authorized to change secrets.
transport_port	A port number that the secret changer/verifier connects to.
transport_secret	Secret used to authorize the account to execute secret change.
account_login	Login of the user whose secret is being changed.
new_secret_value	System default variable initiated with the value automatically generated by Fudo.
transport_secret	Secret used to log in to the target system.
enable_password	Password for raising privileges.

11.7.4.4 WinRM

WinRM transport layer uses Windows Remote Management protocol to interface with remote operating system and facilitate secret change. WinRM is compatible with Certificate Revocation List (CRL) so that the used digital certificates are always up to date and valid.

Note

The default settings of WinRM Secret Changer and Verifier allow changing and verifying secrets of *local* users only. If the *domain* users should be included too, add them to the "Allow log on locally" group so that the executing script takes *domain* users' passwords while running, too.

Commands

Command	Description
INPUT	Command executed on target host.
EXPECTED	Expected result.
ENTER	
DELAY	Delay between commands' execution.

Variables

Warning

To configure WinRM secret changers, you need to provide user credentials with the authority to change secrets (typically an admin-level account). However, it's important to avoid using this account to change its own secret, as WinRM will return an error that Fudo Enterprise cannot process. **Make sure that the account_login and transport_login variables are set to different values.**

Variable	Description
transport_bind_ip	Fudo IP address used to establish connection with the remote host.
transport_ca_certificate	CA certificate of the target system.
transport_encoding	Text encoding used by the target system.
transport_host	An IP address of the remote host that the secret changer/verifier connects to.
transport_kerberos_enabled	Enables Kerberos authentication for this transport layer. Set to `true` to enable (default `false`). Kerberos authentication must be enabled explicitly — there is no fallback mechanism. See *Kerberos Authentication Settings*.
transport_login	An account on the target system used to change secrets. It has to be different from the account on which the secret is being changed (account_login variable).
transport_port	A port number that the secret changer/verifier connects to.
transport_secret	Secret used to access the account to execute secret change.
account_login	Login of the user whose secret is being changed.
new_secret_value	System default variable initiated with the value automatically generated by Fudo.
account_domain	Domain of the user whose secret is being changed.

Note

Previously, Kerberos authentication in the WinRM transport was enabled implicitly whenever the `transport_domain` variable had a non-empty value. Since Fudo Enterprise 6.1 it is controlled explicitly by the `transport_kerberos_enabled` variable. During the upgrade, existing changers that used Kerberos (had a domain set) have `transport_kerberos_enabled` set to `true`.

Related topics:

- *Custom Secret Changers*
- *Secret Changer Policy*
- *Setting up Secret Changing on a Unix System*

11.7.5 Setting up Secret Changing on a Unix System

This topic contains an example of setting up secret changing on a Unix system.

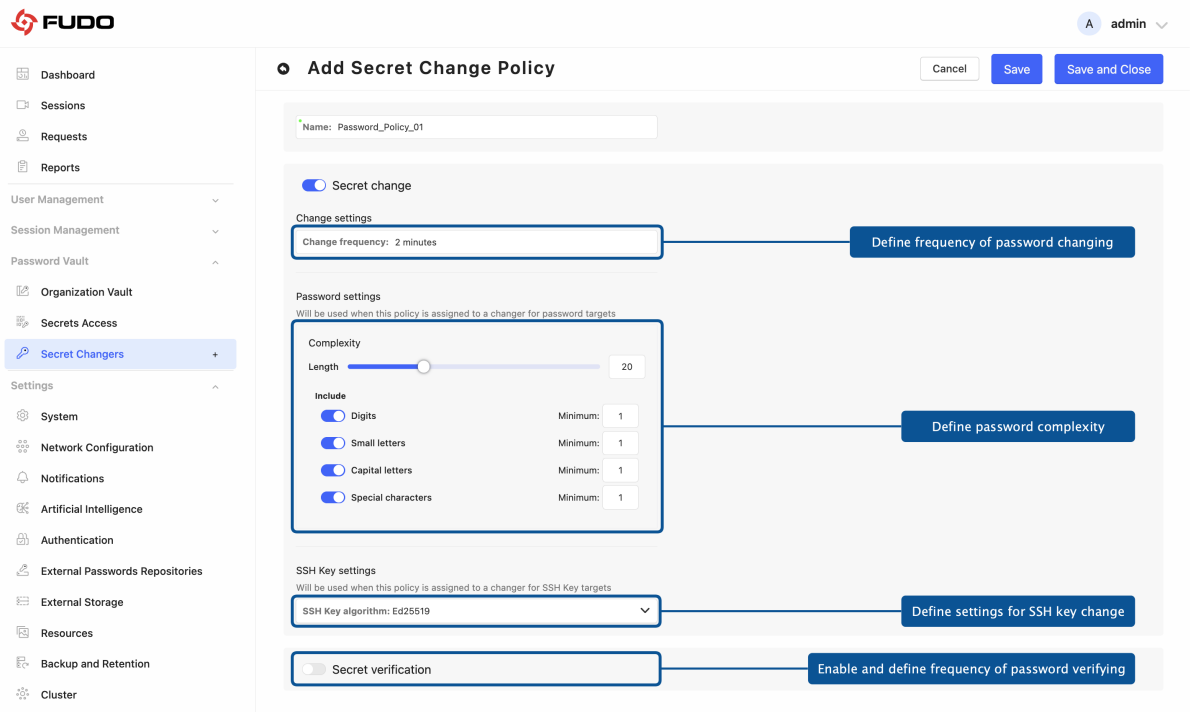
Adding a secret change policy

1. Select *Management* > *Secret Changers*.
2. Go to *Secret Change Policies* tab.
3. Click *+ Add Secret Change Policy* to create a new secret changing policy.
4. Provide secret change policy name.

Note

Provide a descriptive name so that anyone administrating Fudo Enterprise can tell what the policy does at a glance. E.g. `10 minutes, 20 characters, special characters, uppercase`.

5. Select the *Secret change* option and define how frequently the password will be changed.
6. Provide the number of characters comprising the password.
7. Select desired password complexity options and provide the minimal number of characters for each.



8. Select the *Secret verification* option and define how frequently the Secret Manager should verify whether the password has not been changed in any other way but the Secret Manager itself. 7. Click *Save* to store secret changer policy. **Assigning a secret changer and a verifier to the privileged account**

1. Select *Management* > *Accounts*.
2. Find the name of the desired account and click it to edit the account.
3. Go to *SECRET CHANGERS* tab.

Note

Regular account type, password method and login are required to configure secret changers.

4. In the *Secret Changers* field select `Unix/SSH changer` script from the *Add changer* drop-down list.
5. In the *Secret Changers* window, in the *Timeout* field, define the script's execution time limit.

6. Review and modify the default values for the variables according to the table below.

Variable	Value
account_login	`cont_int_mr_jenkins: mr_jenkins`
transport_bind_ip	`cont_int: Any`
transport_host	`cont_int: 10.0.0.12`
transport_host_public_key	`cont_int: ssh-rsa AAA[...]`
transport_login	*Enter manually:* `root`
transport_method	*Enter manually:* `password`
transport_password_prompt	`constant`
transport_port	`cont_int: 22`
transport_secret	`cont_int_mr_jenkins: *****`

7. Click *Save* to close *Secret Changers* window.

Note

- Variables starting with `transport_` are the transport layer variables determining connection parameters with the target host.
- Secret changer variables can be assigned values manually or initialized with properties of other objects.

8. In the *Secret verifiers* field select `Unix/SSH verifier` script from the *Add verifier* drop-down list.
9. In the *Secret verifiers* window, in the *Timeout* field, define the script's execution time limit.
10. Review and modify the default values for the variables according to the table below.

Variable	Value
transport_bind_ip	`cont_int: Any`
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	`constant`
transport_port	`cont_int: 22`
transport_secret	`cont_int_mr_jenkins: *****`

11. Click *Save* to close *Secret verifiers* window.
12. Next, click *Save* in the upper right corner to save the changes to the account definition.

Related topics:

- *Connection Modes*
- *Custom Secret Changers*

CHAPTER 12

Settings

This section covers Fudo Enterprise administration topics.

12.1 System

12.1.1 Date and Time

System events registered by Fudo Enterprise (sessions, system log events, etc.) are timestamped. Fudo Enterprise can obtain the time information either from an NTP server or the system clock.

Warning

- It is strongly advised for the date and time settings to be obtained from a reliable NTP server. Changing date and time settings manually may result in system malfunction.
- Date and time synchronization with NTP server is required in *cluster configurations* and for *Fudo ShareAccess*.

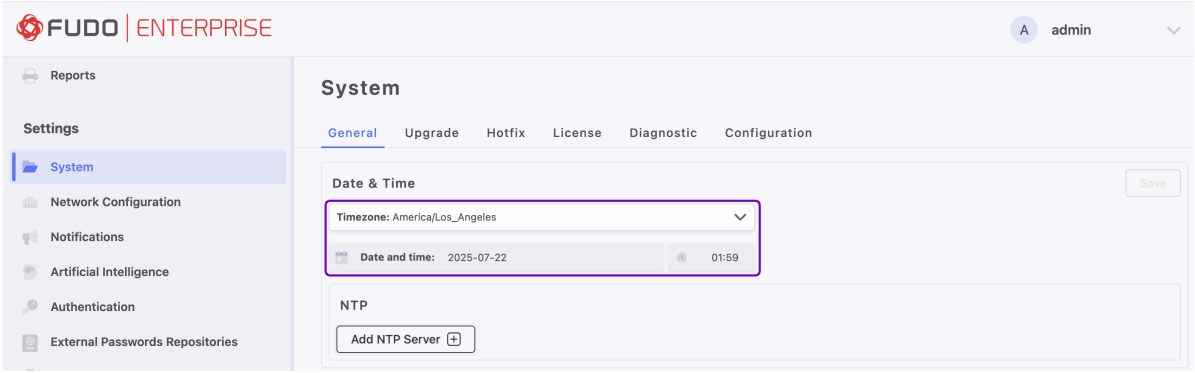
Changing date and time settings

Note

Manual time setting is disabled if there are NTP servers configured.

To change the Fudo Enterprise's system clock settings, proceed as follows.

1. Select *Settings* > *System*.
2. Go to *General* tab.
3. Change date and time parameters in the *Date & Time* section.



4. Click *Save*.
5. Reboot Fudo Enterprise to apply changes (use the link in the message or select the *Reboot* option from the user menu).

Note

To search for a timezone, expand the list and enter a few letters of its name in the *Search...* field.

Time Servers Configuration

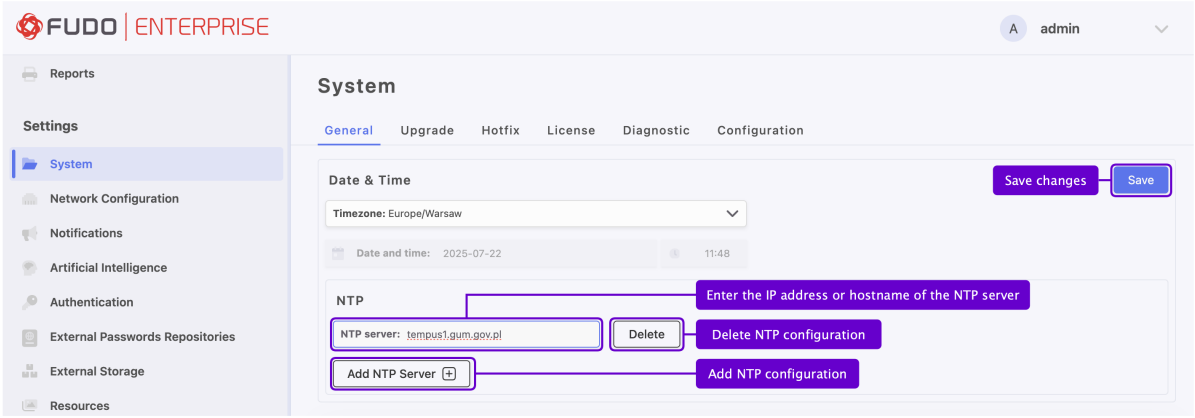
Note

NTP servers ensure that the system time on all IT infrastructure devices is synchronized. Using NTP servers guarantees that the timestamp of the recorded session matches the time settings on the monitored server.

Adding an NTP server:

To add an NTP server, follow the steps below.

1. From the left menu, select *Settings* > *System*.
2. Go to the *General* tab.
3. Click *Add NTP Server* + in the *NTP* section to add a time server definition.
4. Enter the IP address or hostname of the NTP server.



5. Click *Save*.
6. Restart Fudo Enterprise to apply the changes (use the link in the message or select the *Restart* option from the user menu).

Modifying an NTP server:

To modify an NTP server, follow the steps below.

1. From the left menu, select *Settings* > *System*.
2. Go to the *General* tab.
3. Locate and modify the desired entry in the *NTP Servers* section.
4. Click *Save*.
5. Restart Fudo Enterprise to apply the changes (use the link in the message or select the *Restart* option from the user menu).

Removing an NTP server:

To remove an NTP server, follow the steps below.

1. From the left menu, select *Settings* > *System*.
2. Go to the *General* tab.
3. Click *Delete* next to the desired NTP server definition and click *Save*.
4. Restart Fudo Enterprise to apply the changes (use the link in the message or select the *Restart* option from the user menu).

Related topics:

- *Timestamping*

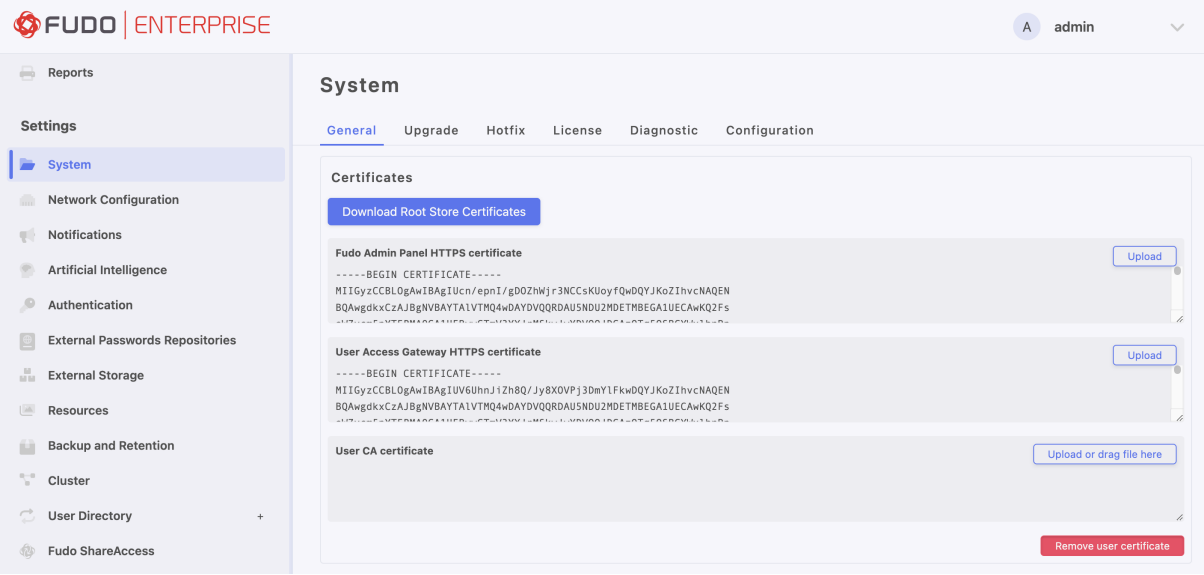
12.1.2 Certificates

Certificates are used to secure HTTPS communication and authenticate users or servers in the Fudo Enterprise environment.

- **Fudo Admin Panel HTTPS certificate** – secures access to the Admin Panel via HTTPS.
- **User Access Gateway HTTPS certificate** – secures the end-user login portal.

- **User CA certificate** – trusted certificate authorities used to validate client certificates during user authentication.

> **Note**
>
> Fudo Enterprise requires the use of unencrypted certificate keys. This way, the user is not prompted to enter the key password on every restart. See: How to decrypt a password-protected RSA private key.



Configuring certificate for Fudo Admin Panel

1. Select *Settings* > *System*.
2. Go to the *General* tab.
3. In the *Fudo Admin Panel HTTPS certificate* section, click the *Upload* button.
4. Click the *Choose a file* button in the *Fudo Admin Panel HTTPS certificate* field and navigate to the location of the certificate file in PEM format.
5. Click the *Choose a file* button in the *HTTPS private key* field and navigate to the location of the private key file.
6. Enter the private key passphrase if the key is encrypted.
7. Click *Save*.

Configuring certificate for User Access Gateway

1. Select *Settings* > *System*.
2. Go to the *General* tab.
3. In the *User Access Gateway HTTPS certificate* section, click the *Upload* button.
4. Click the *Choose a file* button in the *User Access Gateway HTTPS certificate* field and navigate to the location of the certificate file in PEM format.
5. Click the *Choose a file* button in the *HTTPS private key* field and navigate to the location of the private key file.

6. Enter the private key passphrase if the key is encrypted.
7. Click *Save*.

Configuring User CA Certificate

1. Select *Settings* > *System*.
2. Go to the *General* tab.
3. In the *User CA certificate* section, click the *Upload or drag file here* button and navigate to the location of the CA certificate file.

Note

To remove a user CA certificate, click the *Remove user certificate* button below the certificate window.

Related topics:

- *Security Measures*
- *Servers*

12.1.3 Access Gateway Allowed Hosts

The list of allowed hosts defines the host names and IP addresses under which users can open the User Access Gateway. By default the list is empty and the User Access Gateway accepts any name. Once the list is filled, the User Access Gateway rejects every name that is not on it.

The list also determines whether the .rdp files for listeners on the User Access Gateway address are signed - see *Signing .rdp files*.

How It Works

Fudo Enterprise applies the following rules to the list:

- When the list is empty, which is the default, also after an upgrade, the User Access Gateway accepts any name, as in previous versions.
- When the list is filled, the User Access Gateway accepts only the names on the list and the *User Access Gateway IP addresses* of the node. Any other name gets the `421 Misdirected Request` page with the message *This address is not configured for the Access Gateway.*
- Names are compared without regard to letter case, a port number or a trailing dot.
- The list is common to all nodes of a cluster. Each node also accepts its own User Access Gateway IP addresses.
- The list does not affect the Fudo Admin Panel or connections of native clients to listeners.

Before You Fill the List

Once the list is filled, a name that is missing from it stops working. Add all names under which the User Access Gateway is reached, including:

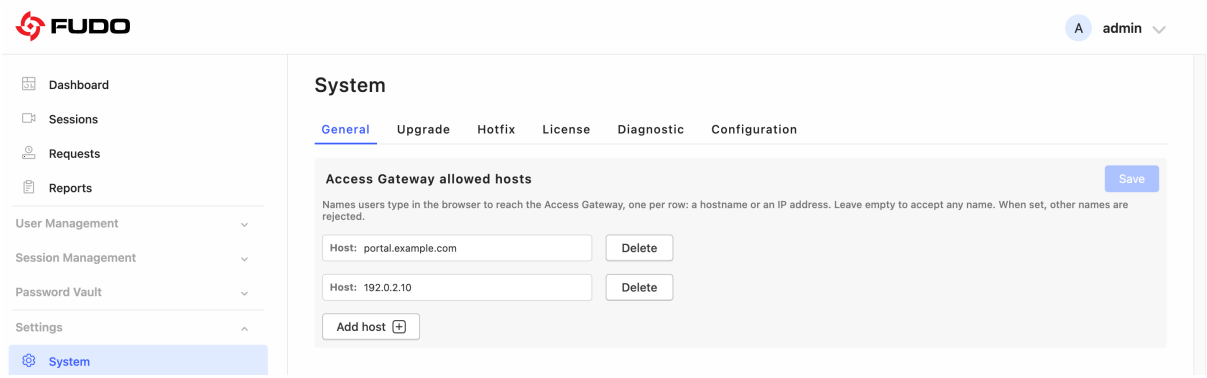
- every host name that users type in the browser, for example the names of individual cluster nodes and the name of a load balancer,
- the host name used for *FIDO2 login* in the User Access Gateway,

- the name under which users reach the User Access Gateway through a *Reverse Proxy*,
- the name that a load balancer sends in its health check. A check without the `Host` header, for example an HTTP/1.0 request, gets the `421` response. Alternatively, let the check use the IP address of the node.

OpenID Connect login, the Web Client and the session player use the address that the user opened, so they keep working without additional entries.

Configuring Allowed Hosts

1. Select *Settings* > *System*.
2. Go to the *General* tab.
3. In the *Access Gateway allowed hosts* section, enter a host name or an IP address in the *Host* field.
4. To add another entry, click *Add host*. To remove an entry, click *Delete* next to it.
5. Click *Save*.



Each row holds one entry: a host name, for example `portal.example.com`, or an IPv4 or IPv6 address. Enter the name without a protocol or a port. Wildcards such as `*.example.com` are not supported. The list can contain up to 32 entries.

To accept any name again, delete all entries and click *Save*.

Required Privileges

The *Access Gateway allowed hosts* section is visible to users with the `uag-hosts-read` privilege (*Access Gateway allowed hosts read*). Changing the list requires the `uag-hosts-modify` privilege (*Access Gateway allowed hosts modify*).

> **Note**
>
> The predefined roles other than **superadmin** do not include these privileges. To let another administrator manage the list, assign them a role with these privileges - see *Creating Role*.

Related topics:

- *Certificates*
- *Setting up the RDP Listener*
- *Reverse Proxy*

12.1.4 SSH Access

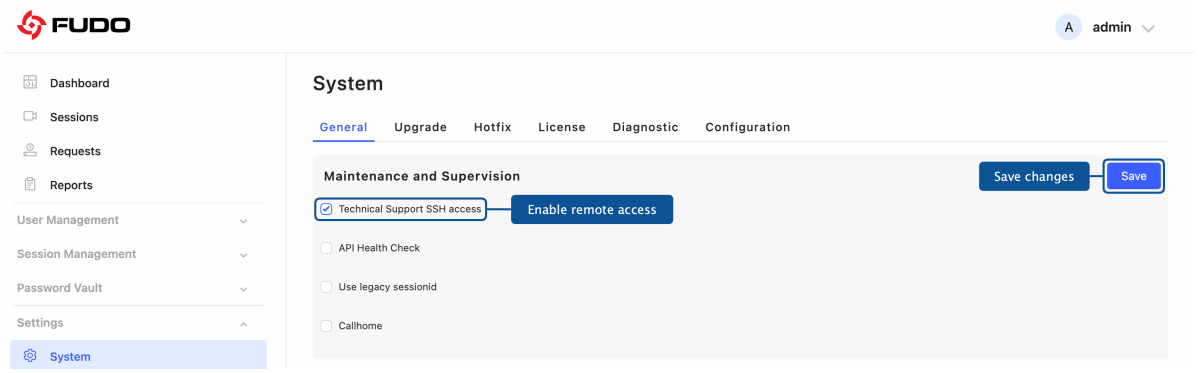
The *Technical Support SSH access* option enables remote access to Fudo Enterprise for servicing and maintenance purposes.

> **Note**
>
> The default port number for service access over SSH protocol is 65522.

Enabling SSH Access

To enable SSH access, proceed as follows.

1. Select *Settings* > *System*.
2. Go to the *General* tab.
3. Select the *Technical Support SSH access* option in the *Maintenance and Supervision* section.



4. Click *Save* button.

Related topics:

- *Callhome*
- *Network Interfaces Configuration*

12.1.5 Legacy Session Cookie

Starting with version 6.3, Fudo Enterprise keeps the session identifier of the Fudo Admin Panel and the User Access Gateway in the `__Host-sessionid` cookie instead of `sessionid`. The browser accepts a cookie with the `__Host-` prefix only from the host that set it and only over HTTPS, so another host in the same domain cannot plant or overwrite it.

If your scripts, integrations or security rules (for example, on a WAF or a reverse proxy) rely on the `sessionid` name, you can temporarily enable the *Use legacy sessionid* option. With the option enabled, Fudo Enterprise also sends the session identifier in the `sessionid` cookie and accepts that cookie when a request does not contain `__Host-sessionid`. The option is disabled by default, also after an upgrade.

> **Note**

Integrations that authenticate with the `Authorization` header, using an API key or a session identifier, are not affected by the cookie name change.

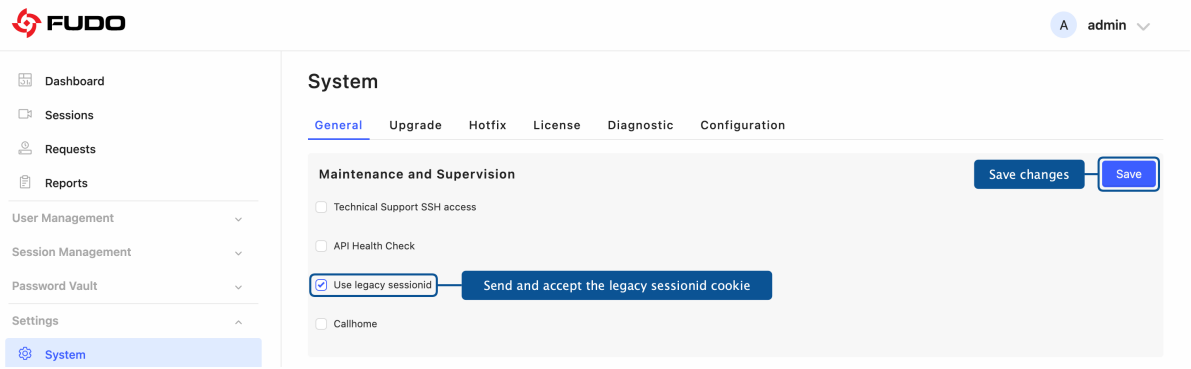
Warning

The `sessionid` cookie is not protected against being planted from another host in the same domain. Enable the option only for the time needed to update your integrations. The option is under review and may be removed in a future version of Fudo Enterprise.

Enabling the Legacy Session Cookie

To enable the legacy session cookie, proceed as follows.

1. Select *Settings* > *System*.
2. Go to the *General* tab.
3. Select the *Use legacy sessionid* option in the *Maintenance and Supervision* section.



4. Click *Save*.
5. Restart Fudo Enterprise.

Note

The change takes effect only after a system restart. After saving, the section displays a message with a link that restarts the system. For more information, see *System Reboot*.

In a cluster, the option is not replicated between nodes. Enable it and restart Fudo Enterprise on each node separately.

Related topics:

- *System Reboot*
- *SSH Access*

12.1.6 Configuration Encryption

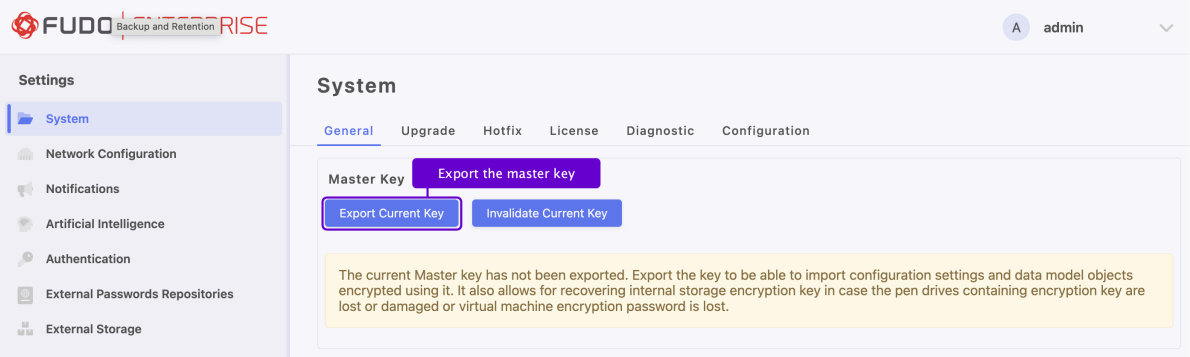
The *Master key* enables encrypting sensitive configuration parameters, system backups and external storage volumes. It also allows for recovering internal storage encryption key in case the pen drives containing encryption key are lost or damaged.

Note

- The Master key is exported to PEM format and it is encrypted with SMIME using administrator's public key/certificate.
- It is essential to have the *Master key* exported and stored in a safe location.
- In case the *Master key* has been compromised, you can invalidate it, which will result in generating a new one and re-encrypting the data.

Exporting Master Key

1. Select *Settings* > *System*.
2. Select the *General* tab.
3. In the *Master Key* section click *Export Current Key*.



4. Click *Choose a file* and browse the file system to find the certificate that will be used to encrypt the *Master key*.

Note

- Generate the keys and the CSR (Certificate Signing Request) using *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.
```

- Sign the CSR:

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

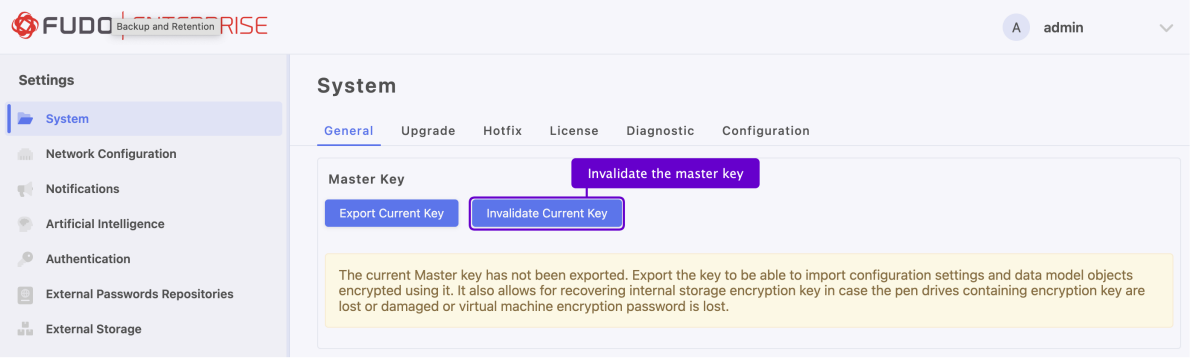
5. Click *Save* to save the the *Master key* file.

Invalidating current master key

In case the current *Master key* has been compromised, you can invalidate it. Invalidating the

current *Master key* generates a new one and triggers data re-encryption.

1. Select *Settings* > *System*.
2. Select the *General* tab.
3. In the *Master Key* section click *Invalidate Current Key*.



4. Confirm invalidating the current key.
5. Make sure to *export the newly generated key*.

Storing the master key in an HSM

Fudo Enterprise can use a Hardware Security Module (HSM) to provide hardware-backed protection for the *Master key*. HSM integration is optional - by default, Fudo Enterprise protects the *Master key* with its standard software-based mechanism.

Enabling HSM integration does not replace the *Master key* with an HSM-generated key. Fudo Enterprise keeps using its own *Master key*, which is protected using key wrapping: a *Key Encryption Key* (KEK) is generated and stored on the HSM as a non-exportable key, and the *Master key* is stored in a wrapped form, encrypted with that KEK. When Fudo Enterprise starts, it contacts the HSM over the PKCS#11 interface to unwrap the *Master key*, and the KEK remains protected within the HSM throughout the operation.

Note

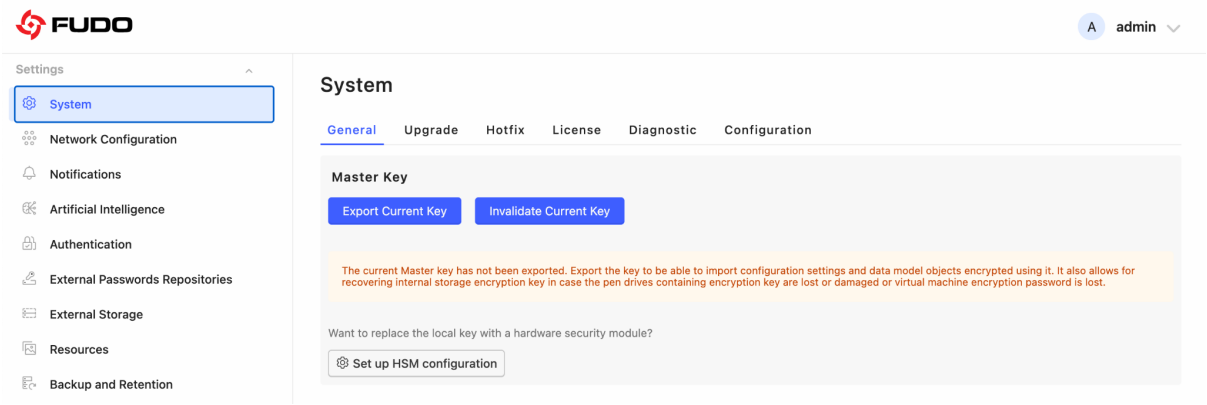
- Fudo Enterprise supports network-accessible HSM providers that provide a Linux x86-64 PKCS#11 client.
- To configure HSM integration you need the PKCS#11 client package prepared for Fudo Enterprise (a `.tar` archive), the token/partition label and the corresponding Crypto Officer (CO) PIN. Preparing the HSM, its application partition, the authentication policy and the client credentials is the responsibility of the administrator of the HSM environment.
- For a step-by-step guide covering the preparation of a Thales Luna Cloud HSM or Thales Luna Network HSM client package, refer to *Master Key Protection with a Thales Luna HSM*.

Enabling HSM protection

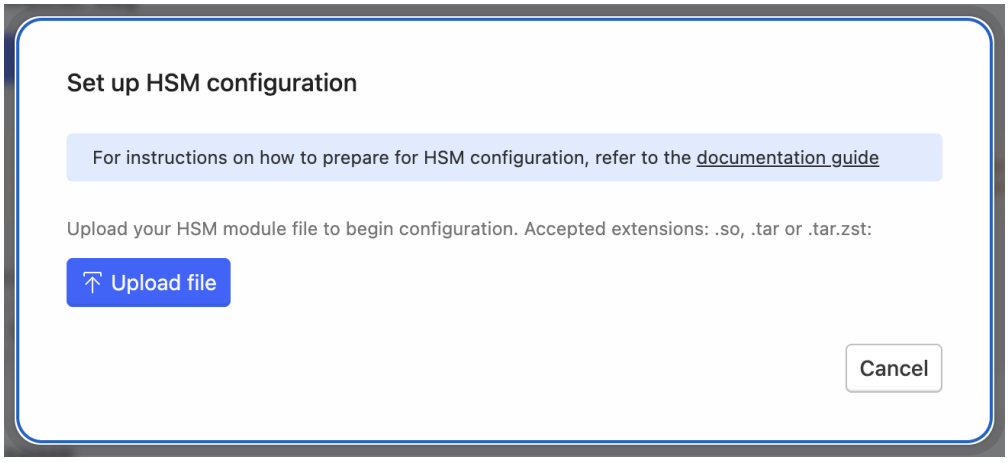
Note

Fudo Enterprise requires a CPU supporting the **x86-64-v2** microarchitecture level (SSE4.2, SSSE3, POPCNT, CMPXCHG16B). Every physical x86 CPU since ~2009 (Intel Nehalem, AMD Bulldozer) supports x86-64-v2. If you are unable to see the *Set up HSM configuration* button in *System* > *Settings*, the hypervisor is presenting a generic vCPU model that masks these instructions.

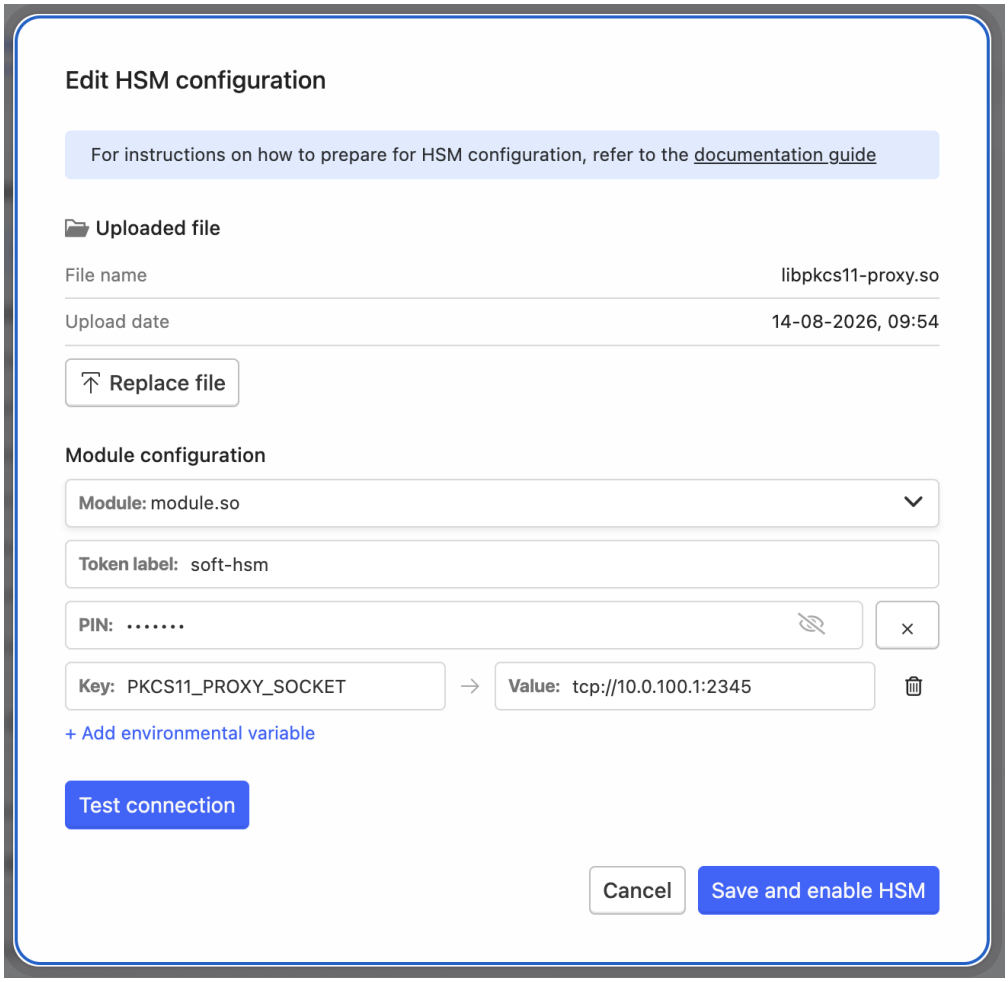
1. Select *Settings* > *System*.
2. Select the *General* tab.
3. In the *Master Key* section click *Set up HSM configuration*.



4. Click *Upload file* and select the archive prepared for your HSM client. Accepted file extensions are `.so`, `.tar` and `.tar.zst`.



5. Configure the following fields:
   - *Module* - select the PKCS#11 library included in the uploaded package. For a standard Luna HSM client this is `libs/64/libCryptoki2.so`.
   - *Token label* - enter the label of the HSM partition prepared for Fudo Enterprise.
   - *PIN* - enter the Crypto Officer (CO) PIN associated with the partition.

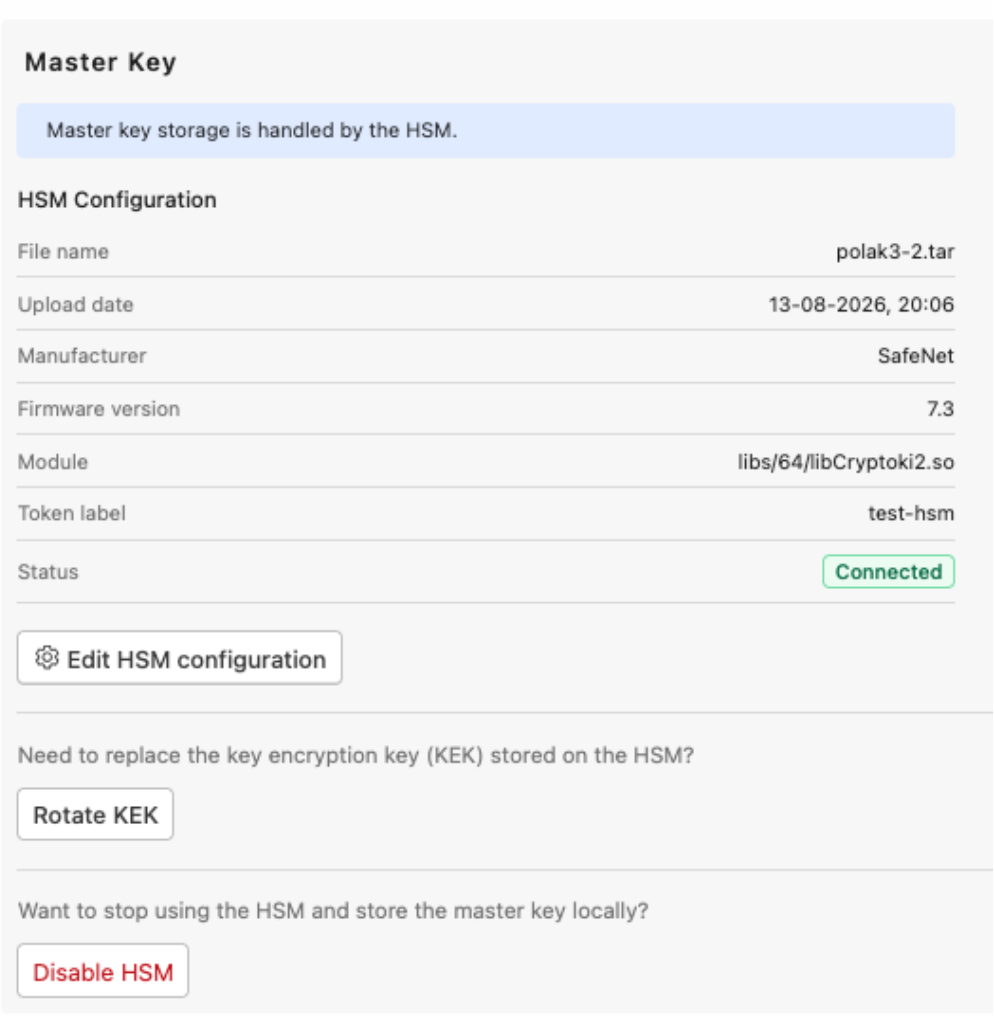


6. If the PKCS#11 module requires environment variables, click *+ Add environmental variable* and provide them as *Key* and *Value* pairs.

> **Note**
>
> The names and values of the environment variables are defined by the documentation of the PKCS#11 module vendor.

7. Click *Test connection* to verify that Fudo Enterprise can reach the HSM with the provided credentials.
8. Once the test succeeds, click *Save and enable HSM*.

The *Master Key* section now displays the details of the uploaded package, the module and token label in use, and the connection status.



Rotating the key encryption key

The *KEK* (Key Encryption Key) is the HSM-protected key used to wrap the *Master key*. Rotating the *KEK* generates a new key encryption key on the HSM and re-wraps the *Master key* with it.

Note

Rotating the *KEK* does not change the *Master key* itself, so the data encrypted with the *Master key* is not re-encrypted.

1. Select *Settings* > *System*.
2. Select the *General* tab.
3. In the *Master Key* section click *Rotate KEK*.

Disabling HSM protection

Disabling HSM protection unwraps the *Master key* and stores it locally again.

Warning

Disabling HSM protection requires access to the currently configured HSM. Do not decommission or disconnect the HSM before HSM protection has been disabled in Fudo Enterprise.

1. Select *Settings* > *System*.
2. Select the *General* tab.
3. In the *Master Key* section click *Disable HSM*.

Related topics:

- *Security Measures*
- *Master Key Protection with a Thales Luna HSM*

12.1.7 SNMP

Fudo Enterprise's status can be monitored over SNMPv3 protocol.

12.1.7.1 Configuring SNMP

1. From the left menu, select *Settings* > *System*.
2. Go to the *General* tab.
3. In the *SNMP* section, enter the username and password for SNMP authentication.
4. From the *Encryption method* drop-down list, select the algorithm used to encrypt SNMP communication (*AES* or *DES*).
5. From the *Authentication method* drop-down list, select either *SHA* or *MD5*.
6. Select the *SNMPv3* option.
7. From the *Source address* drop-down list, select the IP address that will be used for communication with other systems via SNMP.
8. Enter the *port*.
9. Click *Save*.

Note

When listening on *Any,* SNMP will follow the routing from the default routing table 0. When listening on specific IP, SNMP will follow the routing configured on the interface where the IP address is configured.

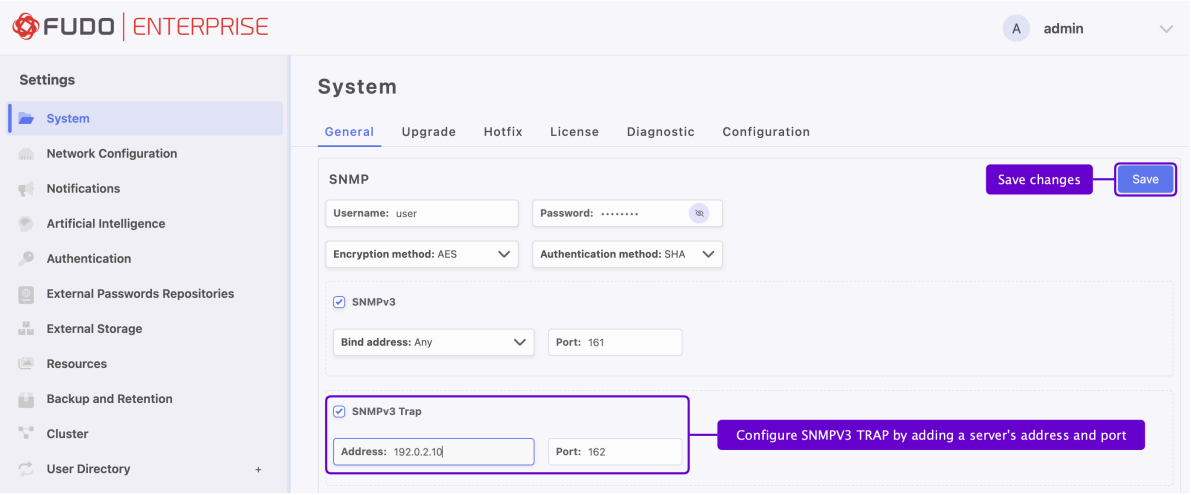
12.1.7.2 Configuring SNMPv3 TRAP

On *Policies* violation, Fudo is able to send a SNMPv3 TRAP, `fudoPolicyViolationNotification` with information containing during which session which user violated which policy. For more details check Fudo's MIB definition in the following section.

To configure SNMP TRAPs, the administrator has to configure the service in the System settings and enable it for a particular policy.

To configure the policy for sending SNMPv3 TRAP notifications about suspicious sessions, follow below procedure:

1. From the left menu, select *Settings* > *System*.
2. Go to the *General* tab.
3. In the *SNMP* section, enter the username and password for SNMP authentication.
4. From the *Encryption method* drop-down list, select the algorithm used to encrypt SNMP communication (*AES* or *DES*).
5. From the *Authentication method* drop-down list, select either *SHA* or *MD5*.
6. Select the *SNMPv3 Trap* option.
7. In the *Address* field, select the IP address that will be used to communicate with other systems via SNMP.
8. Enter the *port*.
9. Click *Save*.



As Fudo Enterprise uses SNMPv3 for sending TRAPs, the manager software (such as `snmptrapd` from *Net-SNMP*) has to know the user's name and password.

Note

The `fudoPolicyViolationNotification` TRAP contains Fudo object identifiers: `sessionId`, `userId` and `policyId`. As all identifiers in Fudo Enterprise are 64-bit integers and SNMP doesn't support 64-bit integers natively, those ids are encoded as big-endian 8-byte arrays.

12.1.7.3 SNMP MIBs

Fudo Enterprise supports following MIBs:

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790) - partly supported
- UCD-SNMP-MIB.

12.1.7.4 Getting SNMP readings using `snmpwalk`

> **Note**
>
> Getting SNMP readings requires installing *Net-SNMP 5.7.3*.

Fetching all SNMP information

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}"          -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1
```

Fetching specific SNMP information

```
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
```

Data specifier	Description
.1.3.6.1.4.1.24410.1.1.1	Disk status (ZFS status)
.1.3.6.1.4.1.24410.1.1.2	Power supply status **Note** This feature is not supported on all Fudo Enterprise units. Contact technical support for more information.
.1.3.6.1.4.1.24410.1.1.3	CPU temperatures
.1.3.6.1.4.1.24410.1.1.4	S.M.A.R.T status

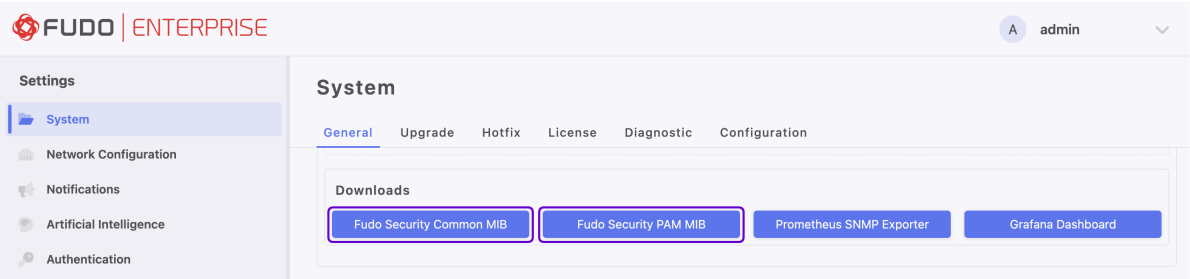
12.1.7.5 Fudo Enterprise Specific SNMP Extensions

Overview

Extensions enable monitoring the number of active sessions, ZFS status, PSU status (if available), CPU temperature on all cores, S.M.A.R.T status such as temperature, health or reallocated sectors.

MIB specification file

MIB specification files (Fudo Security Common MIB and Fudo Security PAM MIB) are available for downloading at the Settings > System in the *Maintenance and supervision* section.



> **Note**

In Fudo Enterprise 5.5.8, the MIB definition has been updated. The `FUDO-SECURITY-COMMON-MIB.txt` file has been modified accordingly, and `smartHealth` now supports only the following states: `ok (1)` and `failed (2)`.

Related topics:

- *Security Measures*
- *Troubleshooting*
- *Policies*

12.1.8 Trusted Timestamping

A trusted timestamp makes recorded session a more convincing evidence in court.

Prerequisites

- Trusted timestamping feature requires signing a contract with an institution providing timestamping services.
- Certificate and private key issued by the timestamping service provider.
- KIR timestamping service requires a DNS server to be configured. Refer to the *DNS Configuration* topic for more information on adding DNS servers.
- Fudo Enterprise must be able to reach the `http://www.ts.kir.com.pl/HttpTspServer` web address in case of the KIR timestamping service.
- Fudo Enterprise must be able to reach the `193.178.164.5` IP address in case of the PWPW timestamping service.

Data Transmitted to Timestamp Provider

When timestamping sessions in Fudo Enterprise, a hash is generated and sent to the timestamp provider. This hash is composed of session data from the `fudo_session` table, and content from the session's RAW dump. It is a one-way hash, ensuring that no session details can be extracted from it.

Note

To ensure the generation of a RAW dump, set the *Session recording* option in Account settings to `all` or `raw` (refer to the *Creating a Regular Account* section to see the example).

Important

This does not apply to sessions handled by the RDP implementation introduced in version 6.2, which records only the FBS format. Such sessions produce no RAW dump and cannot be timestamped, whatever the *Session recording* value is. If you need timestamping for RDP sessions, select the *Use legacy RDP implementation* option on the listener - see *selecting the RDP implementation*. Starting with version 6.3, timestamping will cover both RAW and FBS recordings.

Enabling and Configuring Trusted Timestamping

Note

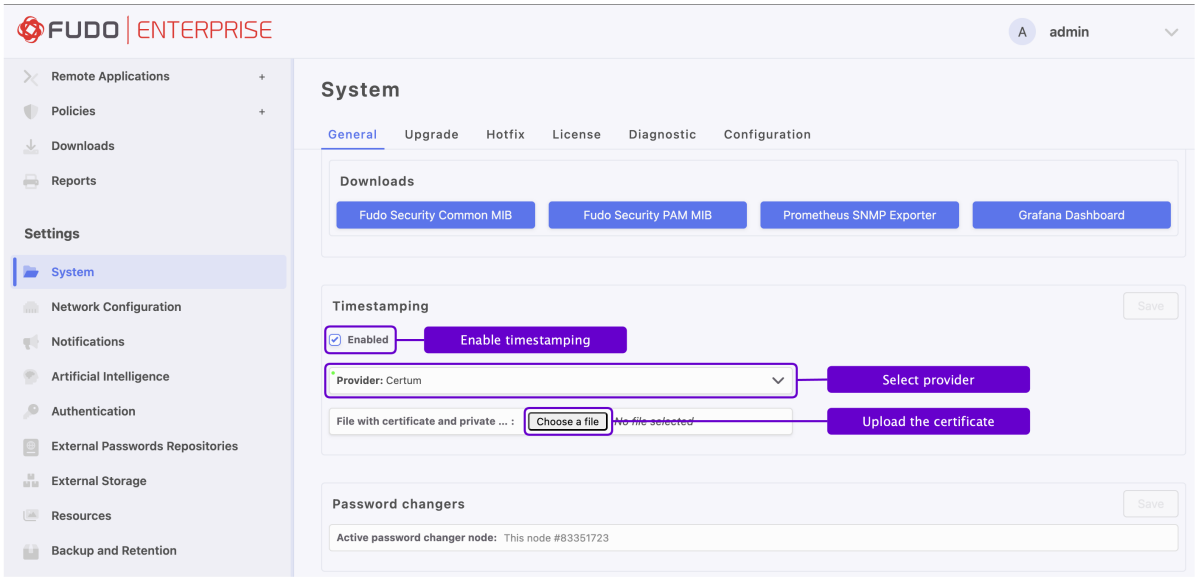
Fudo Enterprise timestamps only those sessions that are completed after the timestamping feature has been enabled.

1. Select *Settings* > *System*.
2. Go to the *General* tab and scroll down to the *Timestamping* section.
3. Select *Enabled* option.
4. From the *Provider* drop-down list, select the institution that provides trusted timestamping services.
5. Upload the certificate and private key issued by the timestamping provider.

Note

The certificate and private key should be provided to you directly by your trusted timestamping service provider.

5. Click *Save*.



Related topics:

- *Security Measures*

12.1.9 File Scanning in Rendered HTTP Sessions

Fudo Enterprise can send files transferred during sessions in selected safes to your antivirus engine over ICAP (Internet Content Adaptation Protocol). A file that the engine rejects is blocked before it reaches the other side.

Note

File scanning covers file uploads and downloads in rendered HTTP sessions only.

Separately from scanning, Fudo Enterprise records every transferred file in the session details, in all safes - see *Recording of Transferred Files*.

How Scanning Works

- **Scanning is enabled per safe.** Providers and timeouts are configured once for the whole system, but no file is scanned until scanning is turned on for a safe.
- **Scanning never fails open.** When scanning is enabled for a safe and the file cannot be scanned - no provider is reachable, the provider returns an error, the scan times out or the file changes while it is being scanned - the transfer is blocked. There is no option to let such files through.
- **Providers are tried in order.** Fudo Enterprise sends each file to the first provider on the list and moves to the next one only if the connection fails. A provider that answers with an error is not skipped - its answer is the result.
- **Files wait for a free slot.** Each provider scans at most *Max concurrent scans* files at a time. Additional files wait in a queue; a file that waits longer than the *Scan timeout* is blocked.

Note

The user sees a message about each blocked file in the browser, for example *Transfer blocked: the scanning service rejected the file (Eicar-Test-Signature). It was not transferred.*

Recording of Transferred Files

Independently of scanning, Fudo Enterprise records every file uploaded or downloaded in a rendered HTTP session, in all safes - also in safes where scanning is turned off.

The record contains the file name, size, location, SHA-256, SHA-1 and MD5 hashes and, if the file was scanned, the scan result. The content of the files is not stored. The records are shown on the *Files* tab of the session details.

Prerequisites

Before you configure file scanning, make sure that the following requirements are met:

- An antivirus engine with an ICAP service that supports the `RESPMOD` method, for example ClamAV with c-icap or OPSWAT MetaDefender.
- The engine's ICAP address, port (`1344` by default) and service path, provided by the antivirus vendor.
- Fudo Enterprise must be able to reach the engine on that port.
- For a TLS connection, the CA certificate that signed the engine's certificate.

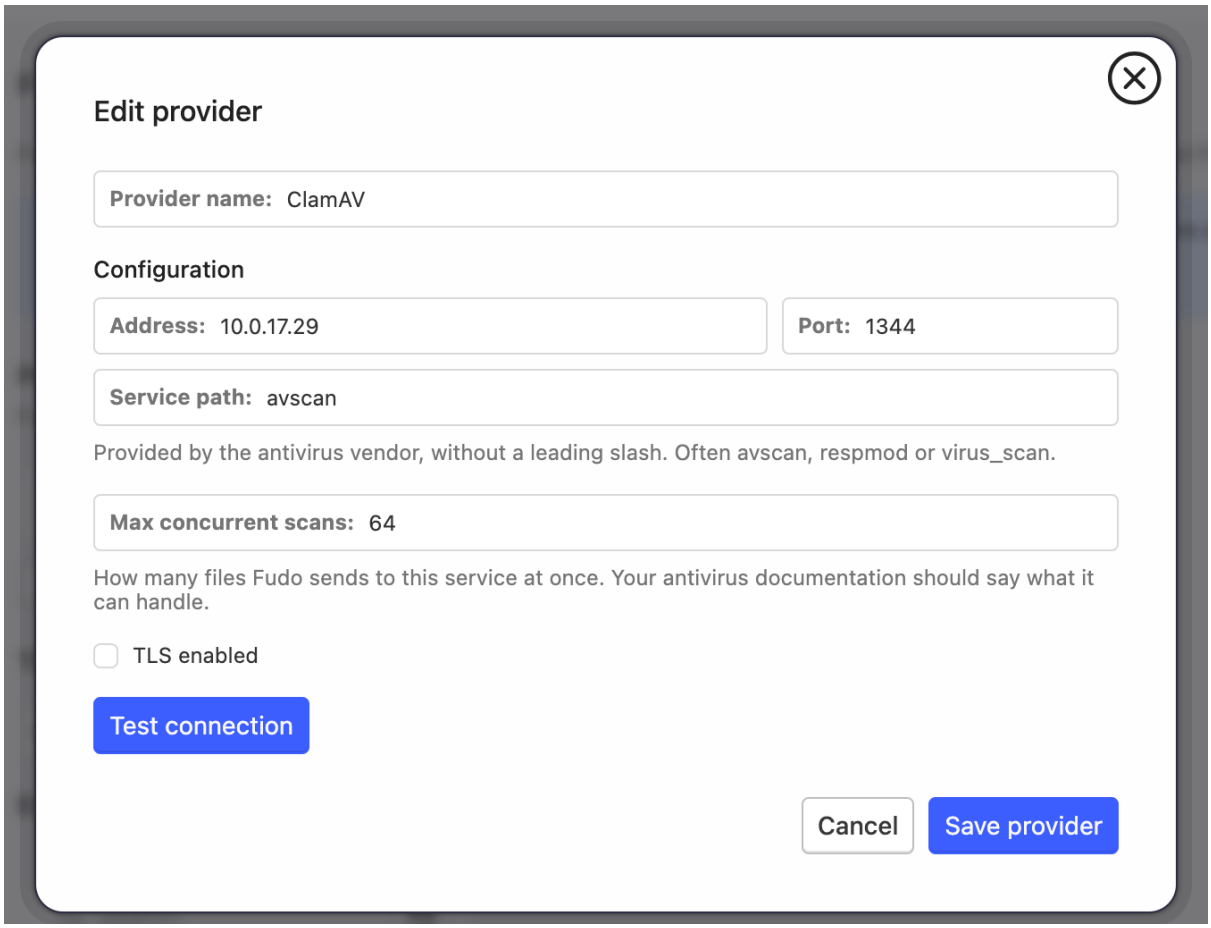
Configure the ICAP service used by Fudo Enterprise so that it scans every file it receives:

- do not set a file size limit lower than the file transfer limit in Fudo Enterprise - for example, c-icap with ClamAV returns files above its maximum size as clean without scanning them,
- turn off content disarm and reconstruction (CDR) - a modified file is treated as a detection,
- review file type exemptions - for example, the default c-icap configuration does not scan PNG, PDF and most media files,

- allow the `204` response for clean files (in c-icap: `allow204=on`), otherwise every clean file is sent back over the network.

Adding a Provider

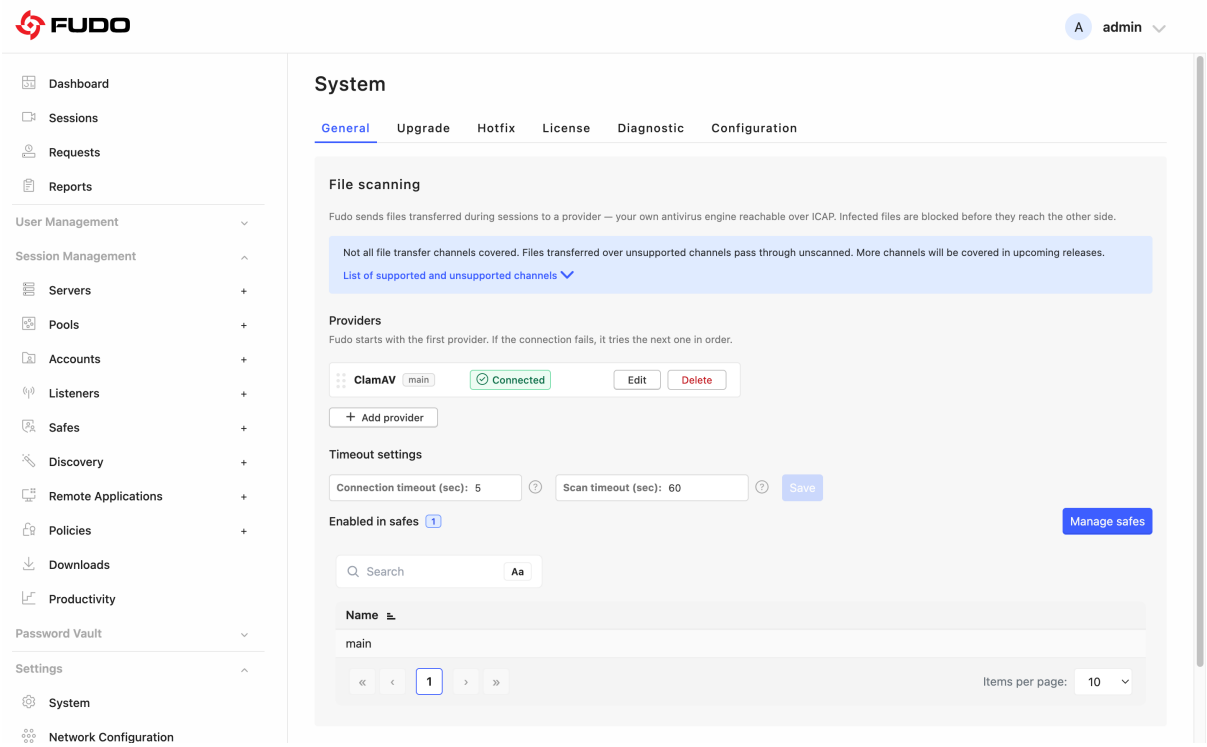
1. Select *Settings* > *System*.
2. Go to the *General* tab and scroll down to the *File scanning* section.
3. Click *Add provider*.
4. Fill in the form:
   - **Provider name** - Name shown on the provider list.
   - **Address** - IP address or host name of the ICAP service.
   - **Port** - ICAP port, `1344` by default.
   - **Service path** - ICAP service name, without a leading slash, for example `avscan`, `respmod` or `virus_scan`.
   - **Max concurrent scans** - Maximum number of files sent to this provider at once, `64` by default. Check the antivirus documentation for the value the engine can handle.
   - **TLS enabled** - Encrypts the connection to the provider. Upload the *CA certificate* that signed the provider's certificate.



5. Click *Save provider*.
6. Click *Edit* next to the provider and click *Test connection* to check that Fudo Enterprise can reach it.

> **Note**
>
> *Test connection* works only for a saved provider. To test changes to a provider, save them first.

The provider list shows the connection status of each provider. The first provider on the list is marked *main*. To change the order, drag a provider by its handle.



Setting Timeouts

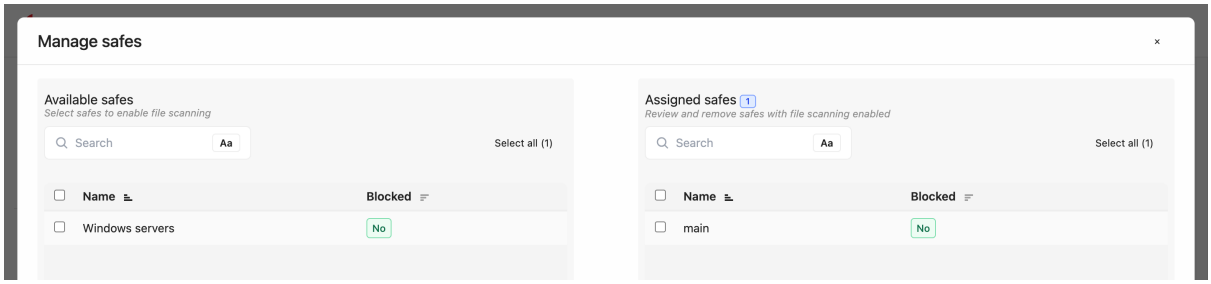
In the *Timeout settings* area, set:

- **Connection timeout (sec)** - How long Fudo Enterprise waits for a provider to accept the connection, from 1 to 60 seconds, `5` by default. After this time, the next provider on the list is tried.
- **Scan timeout (sec)** - How long Fudo Enterprise waits for the scan result, from 1 to 600 seconds, `60` by default. The time includes waiting in the queue and trying subsequent providers. When it runs out, the file is blocked.

Click *Save* to apply the changes.

Enabling Scanning for Safes

1. In the *File scanning* section, click *Manage safes*.
2. In the *Available safes* list, select the safes in which files should be scanned and click the right arrow.
3. To turn scanning off for a safe, select it in the *Assigned safes* list and click the left arrow.



The change takes effect immediately, also for sessions that are in progress. The number of safes with scanning enabled is shown next to *Enabled in safes*.

Note

To check that scanning works, transfer the EICAR antivirus test file in a rendered HTTP session in a safe with scanning enabled. The transfer should be blocked and marked *File blocked by the scanning engine* on the *Files* tab of the session.

File Scanning in a Cluster

In a *cluster*, providers and the list of safes with scanning enabled are replicated to all nodes.

Each cluster node connects to the providers itself: files transferred in a session are scanned through the node that handles the session. The *Test connection* button checks the connection only from the node you are logged in to, so check it on every node, or make sure that every node can reach the providers.

Note

Connections to providers use the default network configuration of the node. The source address and the routing table used for these connections cannot be selected.

Warning

Add, remove and reorder providers only while all cluster nodes are connected, and on one node at a time. The order of providers decides which engine scans the files, so Fudo Enterprise does not resolve conflicting changes automatically.

If providers are changed on different nodes while the connection between them is broken, a conflict remains after the connection is restored:

- each node keeps its own provider list,
- providers added later are no longer replicated to the other node,
- every few seconds, the system log shows `Engine position is already in use` followed by `database commit transaction failure`.

Such a conflict must be resolved manually. Contact technical support.

Required Privileges

The *File scanning* section is visible to users with the `avscan-read` privilege (*AV scanning read*).

Changing the configuration requires the `avscan-modify` privilege (*AV scanning modify*).

> **Note**
>
> The predefined roles other than **superadmin** do not include these privileges. To let another administrator manage file scanning, assign them a role with these privileges - see *Creating Role*.

Related topics:

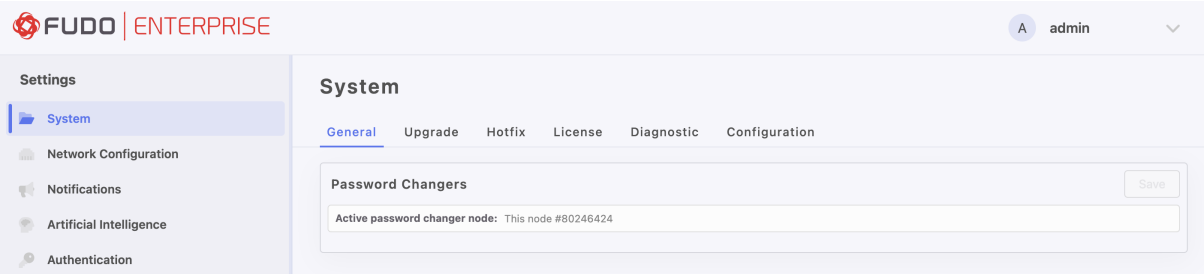
- *Viewing Files Transferred in Rendered HTTP Sessions*
- *Creating a Safe*

12.1.10 Secret Changers - Active Cluster Node

Active cluster node option determines the Fudo Enterprise instance responsible for changing secrets on monitored systems.

> **Note**
>
> Secret changers require at least two active nodes to operate. In a two-node setup, the failure of one node causes secret changers to stop working; therefore, a **three-node setup** is recommended.

1. Select *Settings* > *System*.
2. Select the *General* tab.
3. In the *Secret Changers* section, select the node delegated to secret changing.



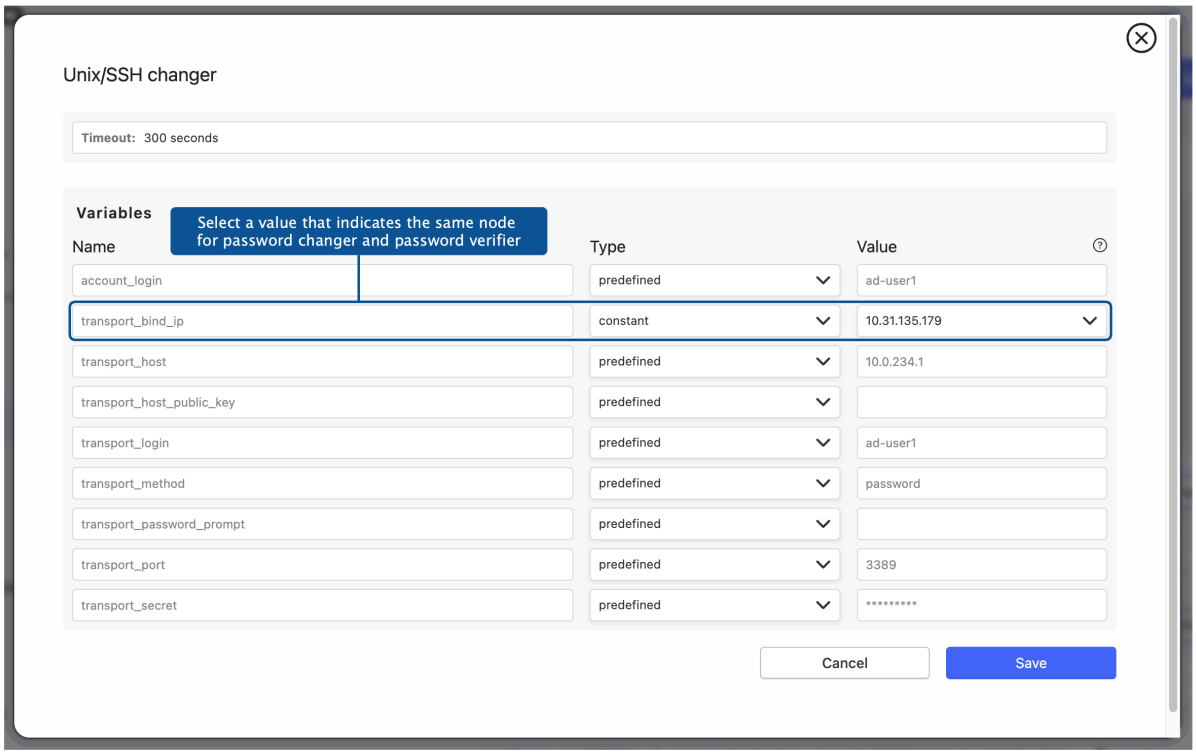
4. Click *Save*.

> **Note**
>
> In case the node responsible for changing secrets fails, the task will not be automatically picked up by another Fudo Enterprise instance. In order to restore automatic secret changing, the system administrator will have to change the active secret changing node or bring back the failed node.

12.1.10.1 Cluster Secret Changers

Fudo Enterprise allows changing a secret on a different node than the one that set as an *Active cluster node for Secret Changers*. In order to have this configured, the following condition should be met:

Setting up a **Secret Changer** / **Secret Verifier** for an account, a value for `transport_bind_ip` variable should indicate the same cluster node for all secret changers as well as secret verifiers.



If the `transport_bind_ip` variable values indicate different cluster nodes, the configured secret changer/verifier will be running on a node that set as an *Active cluster node for Secret Changers*.

Related topics:

- *Secret Changers*
- *Custom Secret Changers*
- *Creating a Regular Account*

12.1.11 Sensitive Features

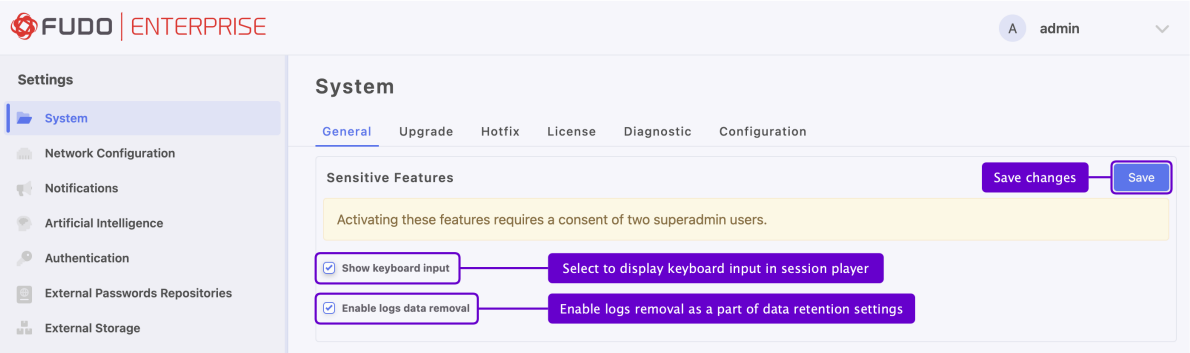
Sensitive features refers to a set of options that require approval from two users who both hold the `sensitive-feature-read` and `sensitive-feature-modify` privileges.

Note

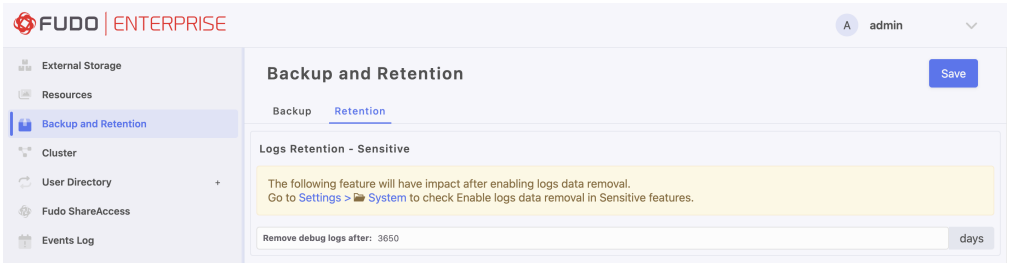
Keystrokes are not displayed in the session player by default. Enabling keystrokes display requires approval from two users who both hold the `sensitive-feature-read` and `sensitive-feature-modify` privileges.

To enable sensitive features, proceed as follows.

1. Select *Settings* > *System*.
2. Go to the *General* tab.



3. Select *Show keyboard input* in the *Sensitive Features* section to initiate the feature.
4. Select *Enable logs data removal* option.
    - this option is combined with Retention settings, where you can specify when logs data should be removed.



5. Click *Save*.
6. Notify another system administrator that the features mentioned above have been initiated and require a confirmation.

Related topics:

- *Viewing Sessions*

12.1.12 Configuring an HTTP Proxy

Fudo Enterprise supports the use of an outbound HTTP proxy to route authentication-related traffic, such as communication with OIDC providers, Microsoft Entra ID, Duo Security, or SMS gateways. It can also be used for integration with timestamping services. This is particularly useful in environments where Fudo Enterprise does not have direct internet access or where all outbound connections must be routed through a controlled proxy server.

You can configure the proxy directly from the Fudo Enterprise web interface.

Note

The HTTP proxy is currently used for the following authentication integrations: **OIDC**, **SMS**, and **DUO**. It can also be used for integration with **timestamping** services. Support for additional components will be added in a future release.

Prerequisites

- An accessible HTTP proxy server (e.g., *tinyproxy*) configured to allow outbound connections.
- Proxy address (hostname or IP) and port.
- Ensure the proxy uses the HTTP scheme.

Configuring the Proxy

1. Select *Settings* > *System*.
2. In the *General* subtab, locate the *Proxy Configuration* section.
3. Select *Enable proxy configuration* option.
4. Enter the proxy address in one of the following formats: `host:port`, or `http://host:port`.

Example:

```
        proxy.example.com:3128
        http://10.0.0.15:8080

5. Click `Save` to apply the configuration.

.. image:: _images/system/5-6-http-proxy.png
```

Note

The `https://` scheme—HTTPS proxies are not supported.

Related topics:

- *Security Measures*

12.1.13 System Update

Note

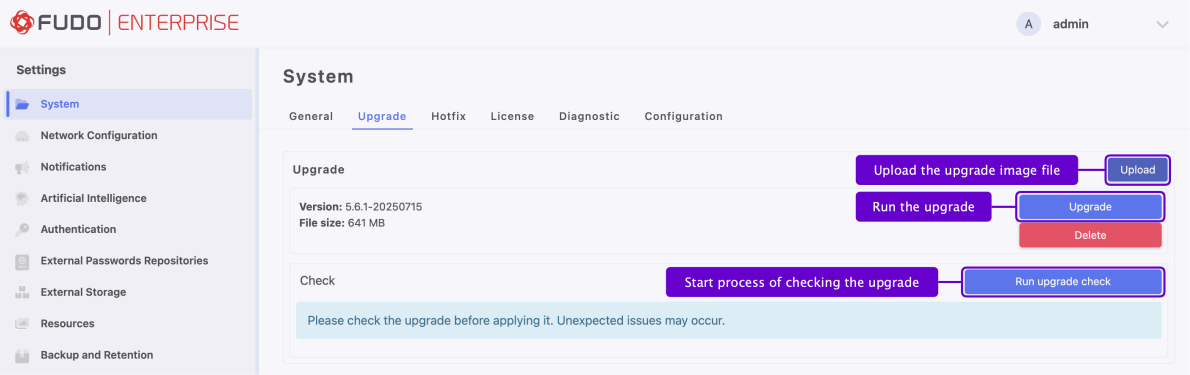
- The system update process does not influence the system configuration or the session data stored on Fudo Enterprise.
- The storage usage may temporarily increase during system update.

12.1.13.1 Updating System

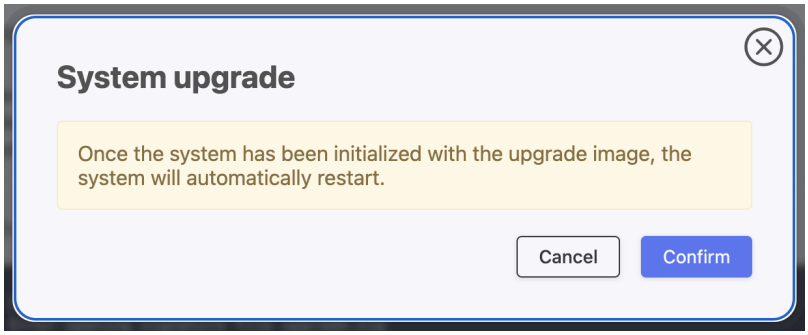
Warning

- Before updating the system it is advised to *run a preliminary check* to ensure that the current system configuration can be successfully upgraded to the new version.
- If the storage usage on the system being updated exceeds 85%, contact Fudo Enterprise technical support before proceeding with upgrading the system.
- During the system update, all current users' connections will be terminated. Use the *Deny new connections* option in the *User authentication and sessions* section of the system settings menu to *limit the number* of active connections before performing system upgrade.
- After running system update, Fudo Enterprise will restart automatically. Connect the USB flash drive containing the encryption key to the USB port before proceeding or have the passphrase ready in case of virtual machine instance. Note that entering incorrect passphrase will restart the machine in previous revision.
- In case of cluster configuration, upgrade slave node first and after successful upgrade, move onto upgrading the master node.
- For clients who are upgrading from 4.x Fudo Enterprise versions, a new masterkey will be generated during the upgrade. Users are encouraged to export and backup the newly generated key. Refer to the *Configuration Encryption* topic to find out more about the system masterkey.

1. Select *Settings* > *System*.
2. Select the *Upgrade* tab.
3. Click *Upload*.
4. Browse the file system to find and upload the update image file (`.upg`).
5. Optionally, click *Run check* to verify if the current configuration and data model objects are compatible with the new system revision.



6. Click *Upgrade*.
7. Click *Confirm* to proceed with system update.

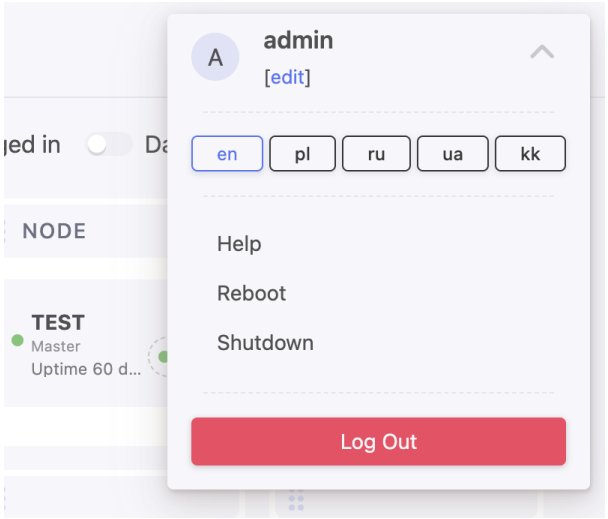


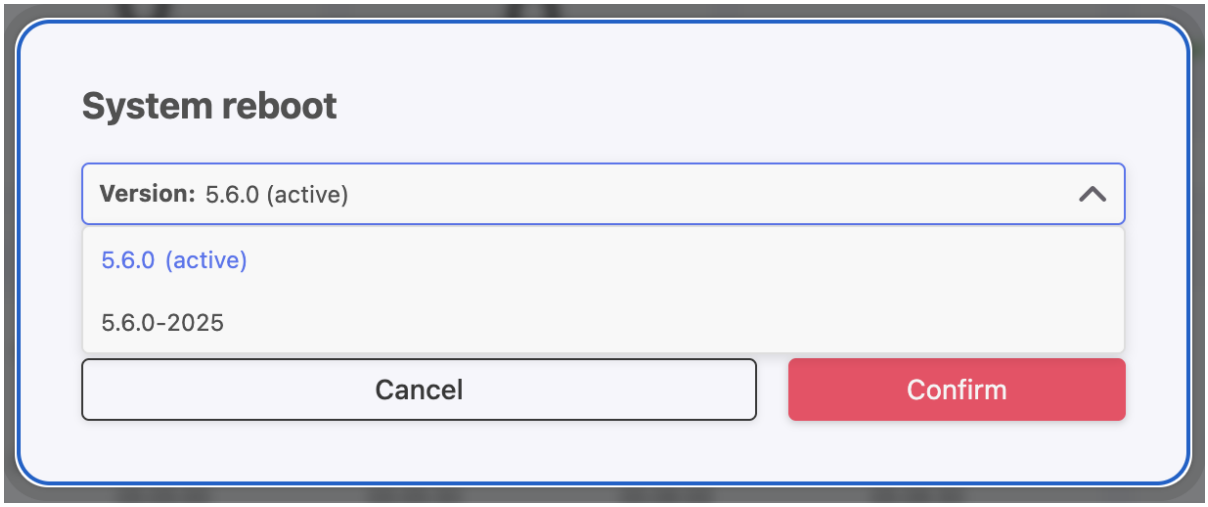
Note

If you *enabled* the *Deny new connections* option before upgrading, make sure to disable it after restarting the system.

12.1.13.2 Restoring Previous System Version

In addition to the current system version, Fudo Enterprise stores the previous revision, allowing for restoring the system to its previous state. In the event of an unsuccessful system update, Fudo Enterprise detects the problem during system restart and restarts itself using the previous system revision. It's also possible to bring the previous version back to the system via the **Reboot** option from the options menu:





Warning

Rollback process will result in the loss of **all sessions recorded** on the new system version and **any system configuration changes**. **All the object configurations** that were created, changed or recorded between the current and the previous system versions will be deleted. This includes the **secret changers** activity. If any passwords were changed during the newer version's usage, restarting Fudo will lead to lost access to corresponding systems.

If the active version is chosen in the modal, the system will be restarted as described at the *Restart* page.

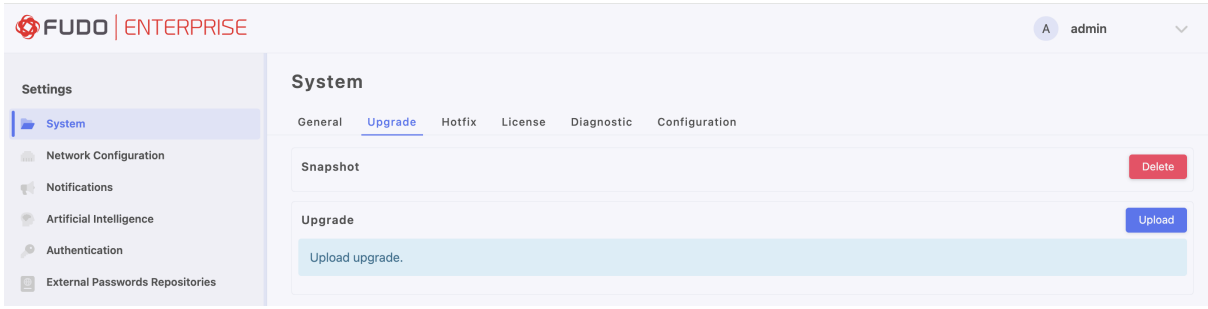
12.1.13.3 Deleting Upgrade Snapshot

Deleting upgrade snapshot will free the storage space occupied by previous system version.

Warning

After deleting the upgrade snapshot it will not be possible to restore the system to previous version.

1. Select *Settings* > *System*.
2. Select the *Upgrade* tab.
3. Click *Delete* in the *Snapshot* section.
4. Confirm deleting previous system version.



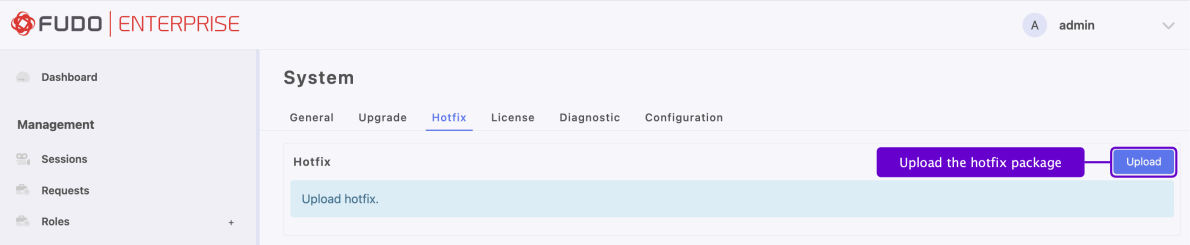
Related topics:

- *System version restore*
- *Restarting system*

12.1.14 Hotfix

The Hotfix feature allows the administrator to upload a minor fix through the Fudo Admin Panel. The fix package is provided by the Fudo Support Team. No additional support actions or system upgrade are required.

The hotfix package uses the Fudo Security HotFix extension (`.fshf`) and can be uploaded by the administrator from the **Hotfix** tab.



Note

Hotfixes cannot be removed or uninstalled, as they are automatically discarded during the next upgrade.

Related topics:

- *System Update*
- *System*

12.1.15 License Information and Management

License Information

The **License** tab displays detailed information about the currently loaded license and the limits applied to individual modules.

General

Field	Description
Serial Number	Unique identifier of the loaded license.
License Owner	Name of the organization to which the license is issued.
License Type	License category (for example *test* or *commercial*).
License Tier	Primary licensed module or feature set.
Cluster Node Limit	The license specifies the number of nodes that can be part of a cluster. If this number is exceeded, the additional nodes will reject connections and log appropriate events in the system logs.

Support

Field	Description
Expiration Date	Date when technical support for the license expires.

Warning

Starting with version 6.1, the license file includes the technical support end date. An expired support end date or *Unknown* support status blocks upgrades to future Fudo Enterprise versions. Before upgrading beyond Fudo Enterprise 6.1, contact Fudo Presales team to obtain a license file that includes the support end date.

Privileged Session Management

Field	Description
Expiration Date	Date when the Privileged Session Management license expires.
Available Servers	Number of servers currently configured in the system compared to the maximum allowed by the license. After exceeding this limit, adding new servers or modifying existing ones is no longer possible. For more details, see the description of the *Accounting Mode*.
Number of Concurrent Sessions	The license also sets a cap on the number of sessions that can be monitored concurrently. When the limit is reached, no new sessions can be initiated until the number of active sessions falls below the licensed value.
Number of Active Users	Number of currently active PSM users compared to the licensed limit. An active user is defined as any user who has established a sessions on Fudo Enterprise within the last 30 days*.
Accounting Mode	Defines how the system accounts for license usage in terms of servers. Possible values are: • *host* – License usage is based on the number of unique IP addresses configured in the system. Port numbers are ignored, meaning multiple servers defined with different ports but the same IP address are counted as a single host. • *unlimited* – The number of defined servers is not limited. In this mode, license enforcement is based solely on the number of concurrently active sessions, not the number of configured servers.

Note

For more information about license limits and active user calculation rules, see the *Licensing Model and License Limits* section.

Password Vault

Field	Description
License Level	Indicates the Password Vault license level (`FULL` or `BASIC`).
Expiration Date	Expiration date of the Password Vault license.
Number of Active Users	Number of users currently using Password Vault functionality compared to the licensed limit.
Number of Available Changers	Maximum number of secret changers that can be assigned to accounts and secrets. Once the limit is reached, no additional secret changers can be assigned to other accounts and secrets.

Note

If no dedicated Password Vault license is installed, the module automatically operates in **Basic** mode with limited functionality.

Available Languages

The license defines which language versions of the product interface are available. Supported languages may include:

- English (en)
- Polish (pl)
- German (de)
- Kazakh (kk)
- Russian (ru)
- Ukrainian (ua)
- Uzbek (uz)
- Italian (it)
- French (fr)

Note

*Logging into the **Admin Panel** is always allowed. This prevents administrators from being locked out of the system due to license limits.

Uploading New License

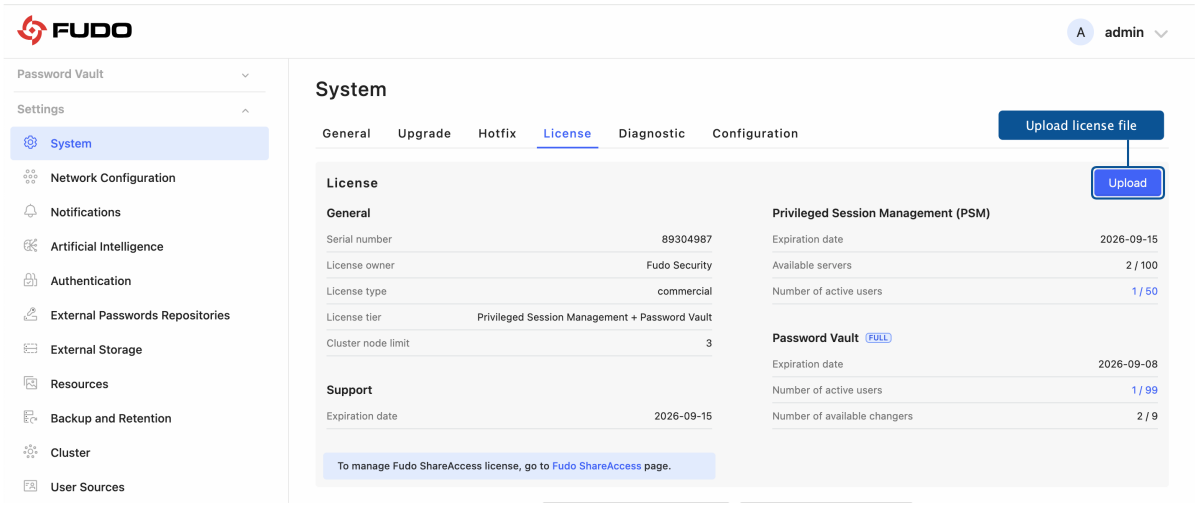
To upload a new license file, proceed as follows.

Note

New license will replace existing one.

1. Select *Settings* > *System*.

2. Select the *License* tab.
3. Click *Upload*.
4. Browse the file system to find the license file and click *OK* to upload and replace current license definition.



Related topics:

- *Licensing Model and License Limits*
- *System Overview*
- *Requirements*
- *System*

12.1.16 Diagnostics

System diagnostics module enables executing basic system command, such as ping, netcat or traceroute.

To run a diagnostic utility, proceed as follows.

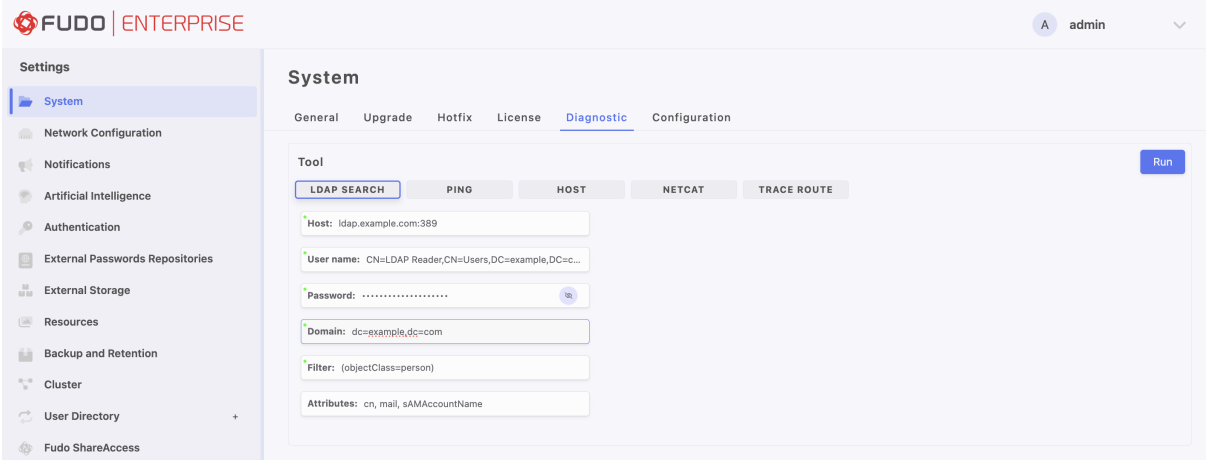
1. Select *Settings* > *System*.
2. Select the Diagnostics tab.
3. Each utility has its own tab. Select the desired one, provide the necessary parameters, and click *Run* to execute the command.

LDAP SEARCH

The LDAP Search utility allows the administrator to query an LDAP server for directory objects using specific filters and attributes.

The table below describes the available parameters required to perform a search.

Command/parameter	Description
Host	LDAP server IP address.
User name	Login of the user allowed to browse the directory.
Password	Password of the user allowed to browse the directory.
Domain	Directory domain to query.
Filter	Objects filtering parameter (eg. `(objectClass=*)`).
Attributes	LDAP search attributes.

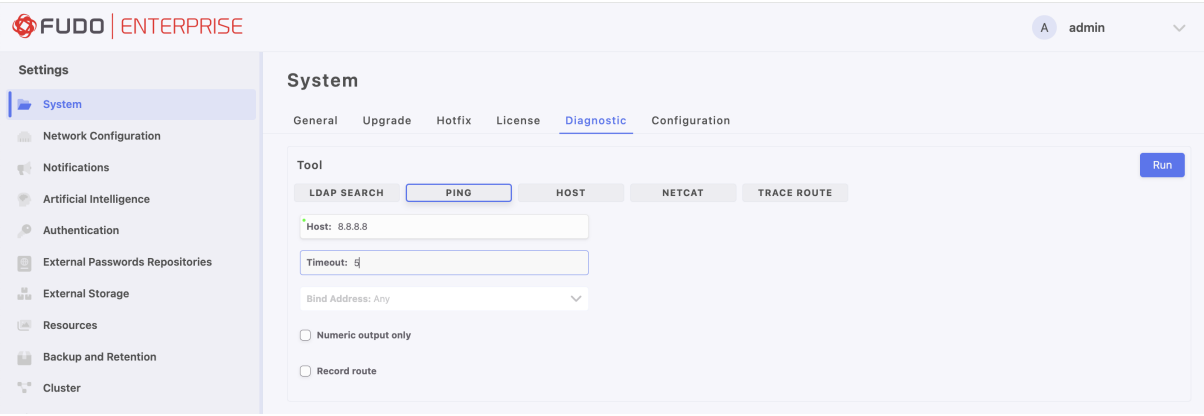


PING

The Ping utility is used to verify the availability of a remote host by sending a series of ICMP packets.

The table below lists the available options for configuring the ping request.

Command/parameter	Description
Host	IP address or hostname of the remote system to be pinged.
Timeout	Maximum time to wait for a response, in seconds.
Bind address	Local IP address to use as the source of outgoing ping packets.
Numeric output only	Does not resolve host's IP address to its mnemonic name.
Record route	Enables tracking packets' route.

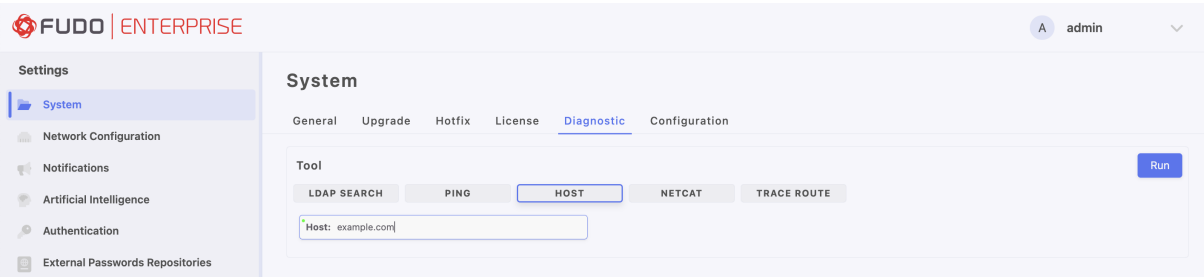


HOST

The Host utility checks whether a DNS server correctly resolves a hostname to its corresponding IP address.

The table below provides details of the available command and its purpose.

Command/parameter	Description
Host	Fully qualified domain name (FQDN) to be resolved via DNS.

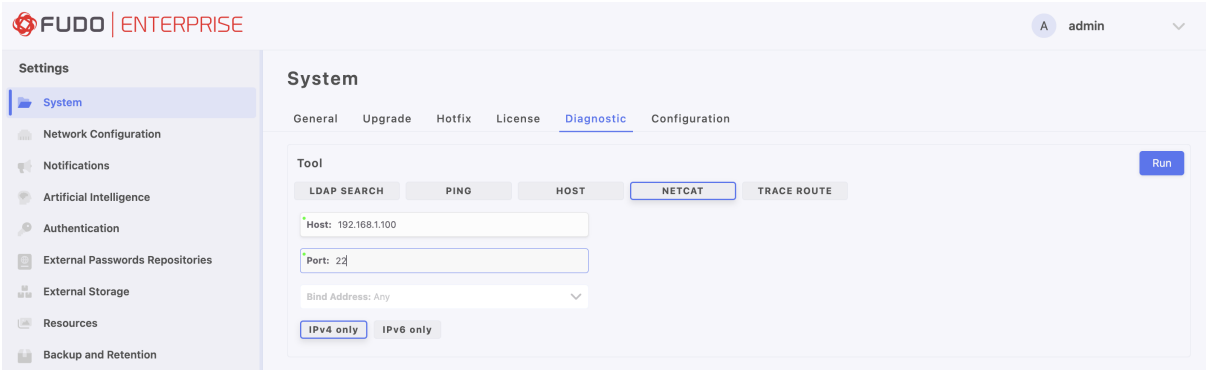


NETCAT

The Netcat utility enables the administrator to establish a TCP connection to a specified host and port.

The table below outlines the available parameter used to perform this check.

Command/parameter	Description
Host	IP address or hostname of the remote system to connect to.
Port	TCP port number on the remote host to be tested.

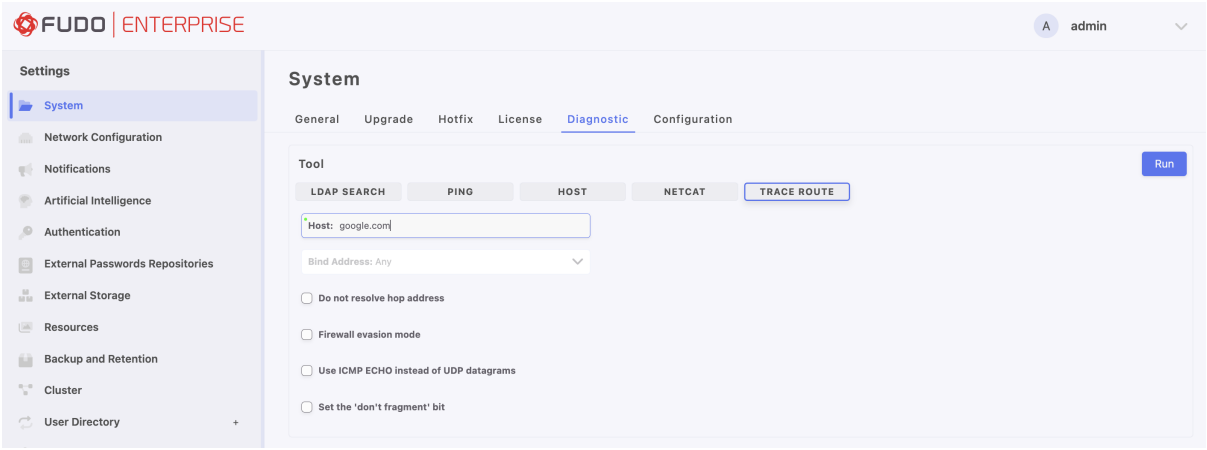


TRACE ROUTE

The Trace Route utility traces the network path taken by packets between Fudo Enterprise and the specified host.

The table below describes the parameters that can be used to customize the trace operation.

Command/parameter	Description
Host	IP address or hostname of the target system for which the packet route should be traced.
Bind address	Local IP address from which the trace operation will be initiated.
Do not resolve hop addresses	Subsequent hop IP addresses are not resolved to mnemonic names.
Use ICMP ECHO instead of UDP datagrams	Enforces `traceroute` to use UDP packets instead of ICMP.
Firewall evasion mode	Enforces the same port numbers for UDP and TCP packets. Target port is not incremented with each packet sent.
Set the "don't fragment" bit	Disables packet fragmentation in case the packet exceeds defined MTU (Maximum Transmission Unit) value defined for the network. Exceeding the MTU value results in an error.



Related topics:

- *Troubleshooting*

12.1.17 Exporting/Importing System Configuration

Fudo Enterprise enables exporting current system state, defined objects and configuration settings, which later can be used to initiate the system.

Warning

Exported configuration data contains confidential information.

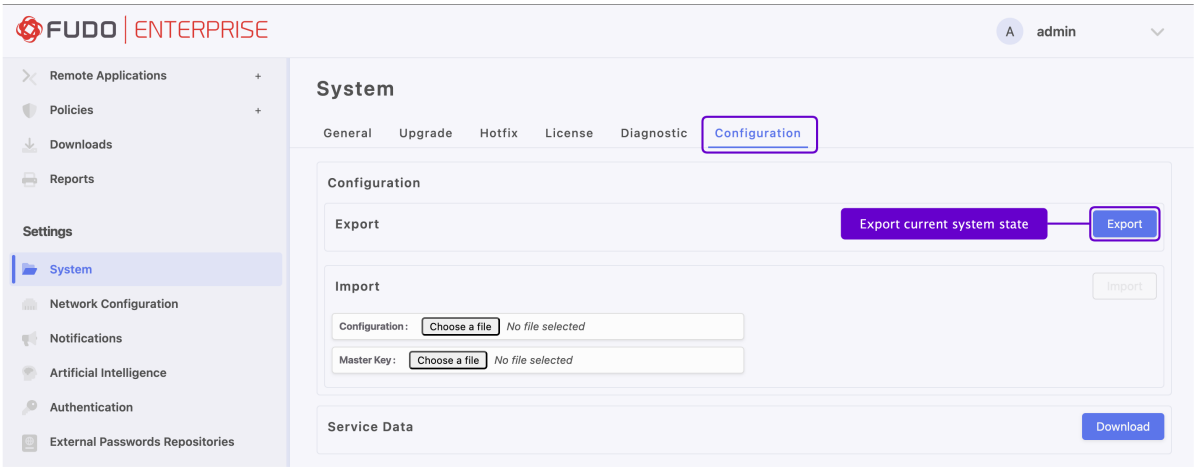
Note

- Configuration export and import options are available only for the *superadmin* users.
- Export/import can be performed only between Fudo Enterprise instances with the same serial number and version.
- It is not possible to export configuration in a clustered setup.

12.1.17.1 Exporting System Configuration

To export system configuration, proceed as follows.

1. Select *Settings* > *System*.
2. Go to the *Configuration* tab.
3. Click *Export* to initiate the download of the `.conf` file.



12.1.17.2 Importing System Configuration

Warning

Importing a configuration file and initiating system with imported data will delete all existing session data.

To import a system configuration file, proceed as follows.

1. Find and decrypt the *Master key file* using *openssl*:

```
openssl smime -decrypt -binary -in path/to/masterkey.pem -inkey privkey.pem -out
masterkey.tar
```

Note

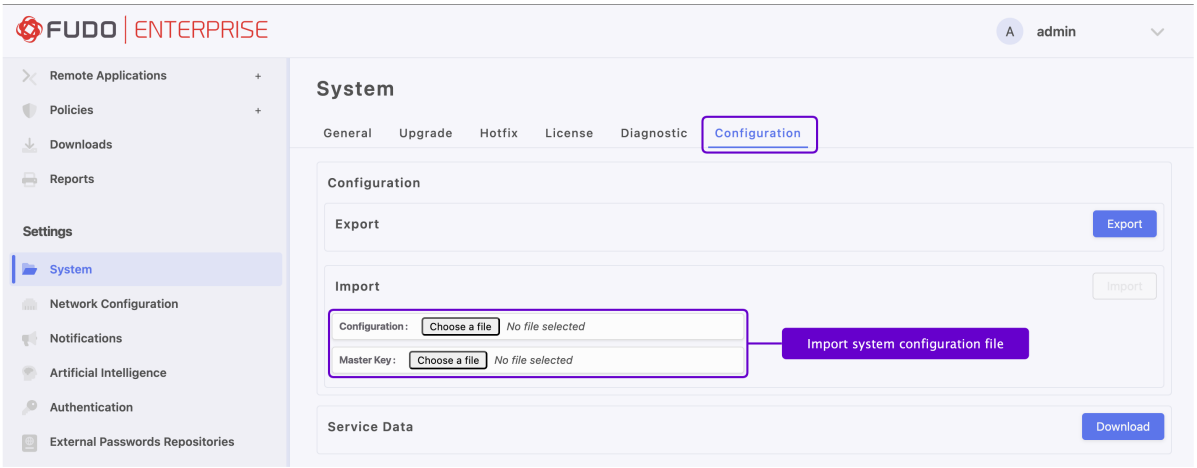
The `-binary` option prevents end-of-line conversion, which may corrupt the decrypted `.tar` archive (notably on Windows). To verify the decrypted file, run: `tar -tvf masterkey.tar`.

2. Select *Settings* > *System*.
3. Go to the **Configuration** tab.
4. Click *Choose a file* in the *Master Key* field and select the *Master key* file.

Note

Master key must be decrypted beforehand.

5. Click *Choose a file* in the *Configuration* field and select the configuration file.



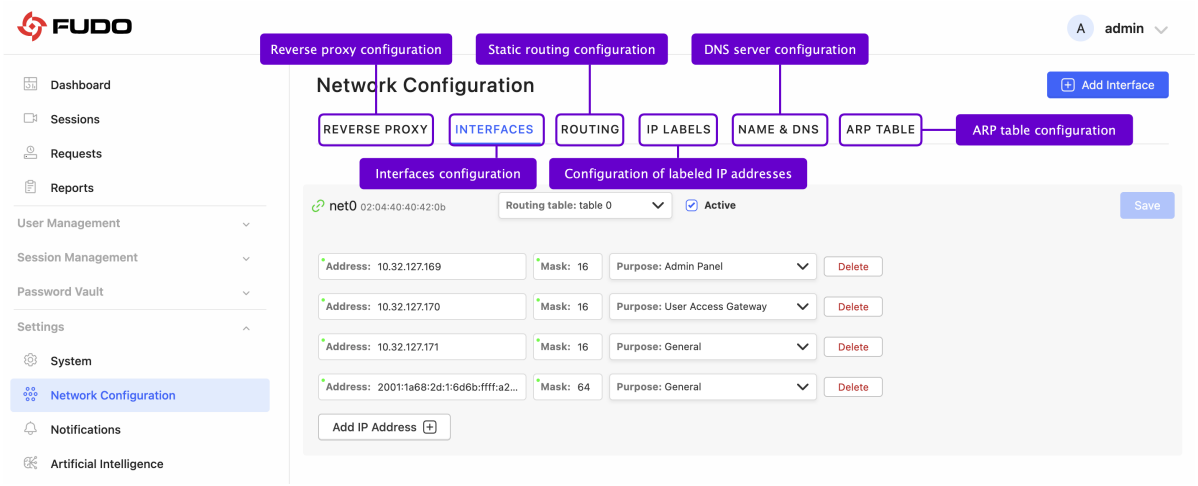
6. Click *Import* to proceed with initiating the system with the imported data.

Related topics:

- *Configuration Encryption*
- *Session Data Backup*
- *System Initiation*
- *System Update*

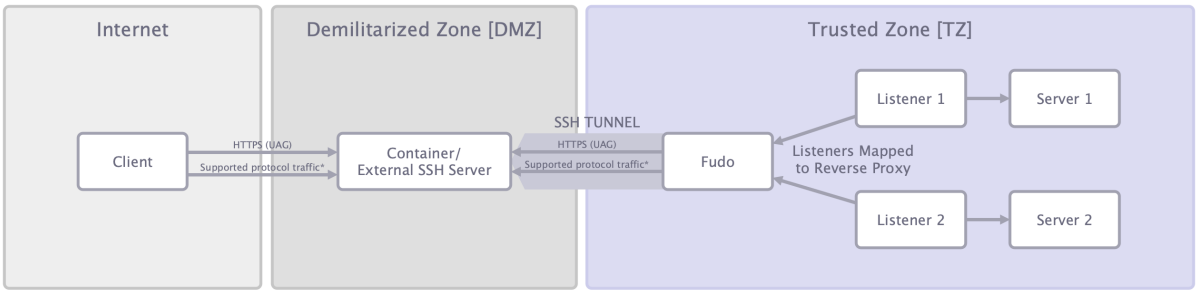
12.2 Network Settings

To change network settings select *Settings* > *Network configuration*.



12.2.1 Reverse Proxy

The Reverse Proxy feature enables reverse SSH tunnels that allow connections from a Demilitarized Zone (DMZ) container or external SSH server to reach internal resources within your infrastructure. This is accomplished by establishing an outbound SSH connection to an external server, which then allows that server to forward traffic back through the tunnel to your internal listeners.



*Supported protocols: HTTP, Modbus, MS SQL (TDS), MySQL, RDP, SSH, Telnet 3270, Telnet 5250, Telnet, VNC, X11, TCP, Secret Checkout.

Note

The external SSH server/container serves as the access point for users connecting through the Reverse Proxy. Instead of connecting directly to Fudo Enterprise, clients establish their connection to this external server, which then forwards traffic through the reverse SSH tunnel into the internal environment. As a result, this server is not just an auxiliary host — it is the endpoint that users will connect to when accessing internal resources.

12.2.1.1 Prerequisites

Before configuring a Reverse Proxy, ensure the following requirements are met.

- **External SSH Server**
  - A proxy server can be a hardware or virtual machine, or a container with SSH enabled that allows tunnel forwarding with the `-R` option.

  - The external SSH server must have the following configuration in its `sshd_config` file: `GatewayPorts clientspecified`. This setting allows the SSH daemon to bind to specific addresses as requested by the client.

- **Authentication Setup**
  - Add the SSH public key (corresponding to the private key you'll use) to the `authorized_keys` file on the external SSH server to enable key-based authentication.
- **Network Requirements**
  - You must select a specific Bind IP address for the outbound connection—labels and Any are not permitted.
  - Each Reverse Proxy configuration must use a unique combination of server address and port.

12.2.1.2 Configuration Steps

For illustration purposes, the example below uses a container-based SSH server.

Example SSH Container Configuration

The following `Dockerfile` defines a minimal SSH server suitable as an External SSH Server for Reverse Proxy tunneling.

Dockerfile

The example uses Ubuntu 22.04 LTS, but any Linux base image with OpenSSH Server installed can be used.

```
FROM ubuntu:22.04

RUN apt-get update && apt-get install -y openssh-server \
    && mkdir -p /var/run/sshd

# Create a dedicated user
RUN useradd -m reverseproxy && mkdir -p /home/reverseproxy/.ssh \
    && chown -R reverseproxy:reverseproxy /home/reverseproxy/.ssh

# Update SSH configuration to allow reverse tunnels
RUN sed -i 's/#GatewayPorts no/GatewayPorts clientspecified/' /etc/ssh/sshd_
↪config

# (Optional) Disable password authentication for security
RUN sed -i 's/#PasswordAuthentication yes/PasswordAuthentication no/' /etc/ssh/
↪sshd_config

EXPOSE 22

CMD ["/usr/sbin/sshd", "-D"]
```

Build the Container

```
docker build -t external-ssh-server .
```

Run the Container

Expose port 22 to your host. You can use any port on the host. Using a non-standard port (e.g., 2222) is recommended for basic hardening.

```
docker run -d -p 2222:22 --name external-ssh external-ssh-server
```

Configure Key-Based Authentication

> **Note**
>
> The public key required for authentication on the external SSH server can be obtained directly from the Reverse Proxy configuration in Fudo Enterprise.

After starting the container, copy the SSH public key that the Reverse Proxy will use.

```
docker exec -it external-ssh bash
```

Inside the container:

```
su - reverseproxy
echo "YOUR_PUBLIC_KEY" > =/.ssh/authorized_keys
chmod 700 =/.ssh
chmod 600 =/.ssh/authorized_keys
```

Validate the Configuration

To verify that the external SSH server accepts key-based authentication and supports reverse SSH connections, you can perform a manual test from any host that will initiate the tunnel (e.g., the Reverse Proxy host).

- SSH Key Authentication

  ```
  ssh -i private_key reverseproxy@<server-ip> -p 2222 true
  ```

- Reverse Port Forwarding

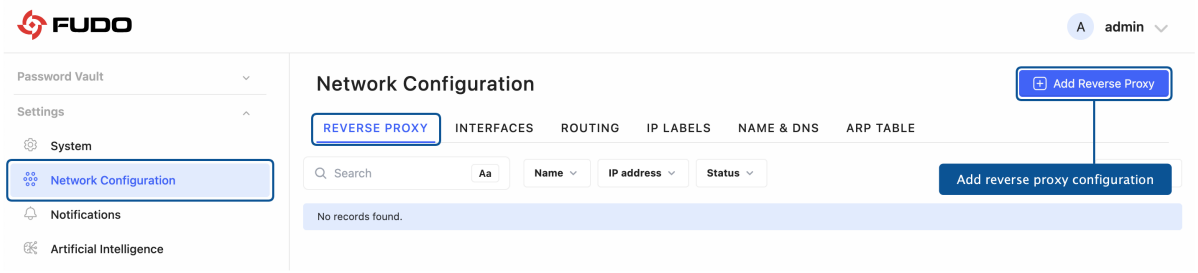
  ```
  ssh -i private_key -R 0.0.0.0:8080:localhost:80 reverseproxy@<server-
  ↪ip> -p 2222
  ```

- If successful, the container is ready to be used as the External SSH Server for Reverse Proxy.

> **Note**
>
> If the key pair was generated in Fudo Enterprise, make sure that the private key was downloaded and stored securely before performing this test.
>
> If the private key is missing, authentication will fail. In this case, generate a new key pair or upload your own public key to Fudo Enterprise.

Configuration Steps in Fudo Enterprise

1. Select *Settings* > *Network Configuration*.
2. Open the *REVERSE PROXY* tab.
3. Click + *Add Reverse Proxy*.



SETTINGS TAB

Note

Settings tab configures the SSH connection parameters and determines whether the User Access Gateway (UAG) is proxied through this connection.

1. In the **Name** field, enter a descriptive name for this Reverse Proxy configuration, for example `Reverse Proxy - DMZ` or `SSH Tunnel to Reporting Server`.
2. In the **IP address** field, provide the hostname or IP address of the external SSH server that Fudo Enterprise should connect to.
3. In the **Port** field, enter the SSH port number on the external server. This is typically 22, unless the server uses a non-standard port.
4. In the **Login** field, enter the SSH username used on the external server (e.g., `fudo`, `tunnel`, `proxyuser`).
5. In the **Private Key** field, paste the private key used for authentication on the external SSH server.

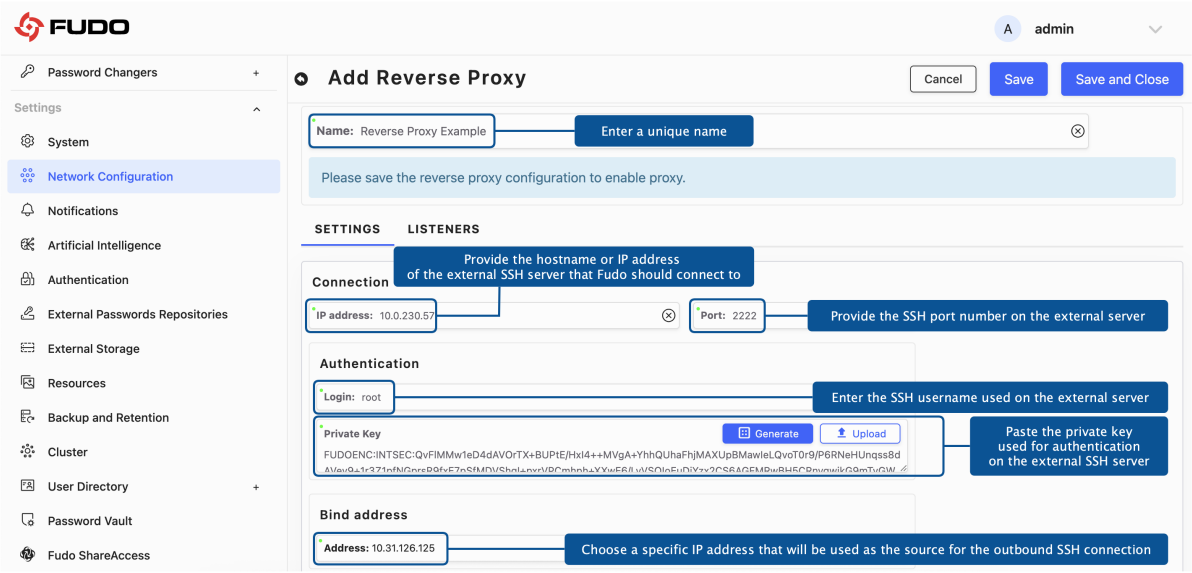
   Note

   Remember that only key-based authentication is supported — password authentication is not available.

6. In the **Bind IP** field, choose a specific IP address that will be used as the source for the outbound SSH connection.

   Note

   You cannot use labels or the Any option. The selected IP determines which node establishes the SSH connection.



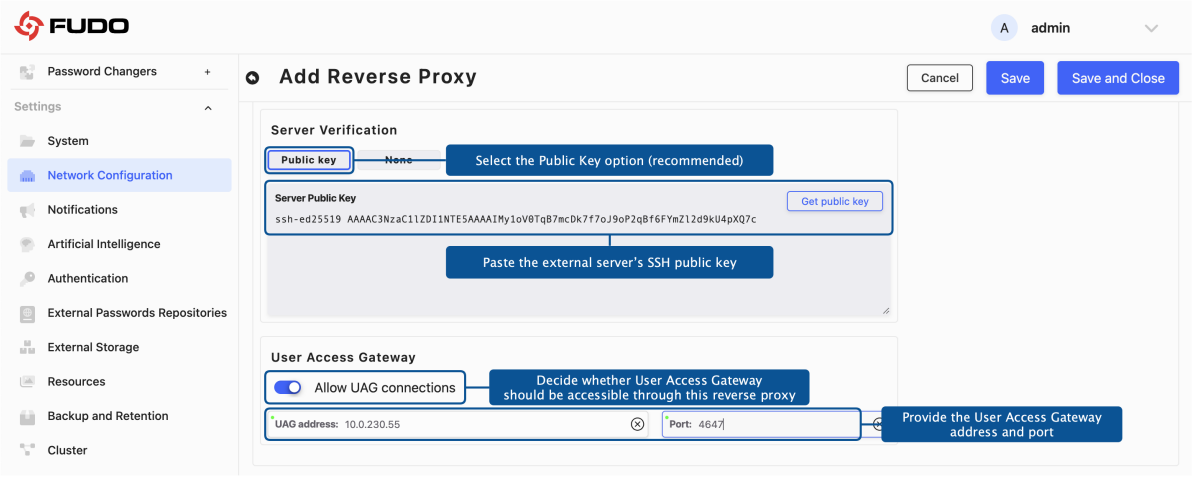
7. In the **Server Verification** section, select the **Public Key** option (recommended) and paste the external server's SSH public key into the **Server Public Key** field.

> **Note**
>
> Although this field is optional, it is strongly recommended to provide the key. If the field is left empty, the key will be retrieved automatically on every tunnel establishment attempt. Providing the key manually is recommended because it reduces the risk of man-in-the-middle attacks and ensures you are connecting to the expected server.

8. In the **User Access Gateway (UAG)** section, decide whether UAG should be accessible through this Reverse Proxy.

   If you enable the **Allow UAG connections** option for this configuration, users connecting through this tunnel will receive a filtered view of resources based on their assigned permissions.

   When UAG access is enabled, provide the UAG address and port.



Note

If the User Access Gateway (UAG) is exposed through the Reverse Proxy under a different hostname or IP address, the TLS certificate used by the UAG must include all such addresses. Otherwise, TLS validation will fail and connections will be rejected.

If the *list of Access Gateway allowed hosts* is filled, add these names to it as well.

LISTENERS TAB

1. Go to the **LISTENERS** tab.

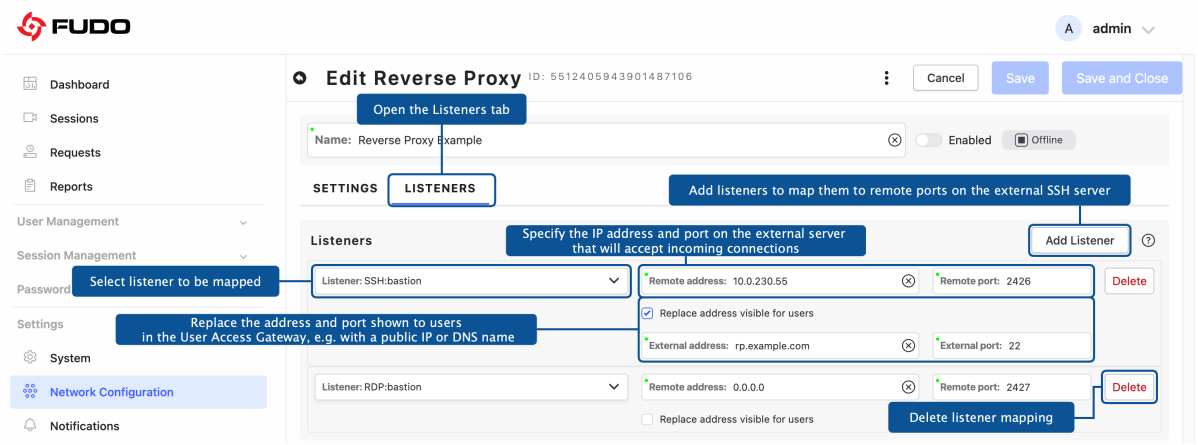
   Note

   Listeners tab allows you to map internal listeners to remote ports on the external SSH server, creating tunnels that forward traffic from the remote server back to your internal resources.

2. Click Add Listener to create listener mapping.
3. From the **Listener** drop-down list, select the Fudo Enterprise listener (identified by its listen IP and listen port) that will receive the tunneled traffic.
4. In the **Remote address** field, specify the IP address on the external server that will accept incoming connections. Enter `0.0.0.0` (IPv4) or `::` (IPv6) to accept connections on all addresses of the external server.
5. In the **Remote port** field, specify the port on the external server that will accept incoming connections. This port must be unique within this Reverse Proxy configuration.
6. Optionally, select **Replace address visible for users** and fill in the **External address** and **External port** fields. Use this option when users reach the external server through a different address, for example a public IP address or a DNS name behind NAT. The User Access Gateway then shows this address and port to users instead of the remote address and port. The tunnel itself does not change.

   Note

   Fudo Enterprise does not verify the external address. Make sure that users can reach the external server at this address and port.



Note

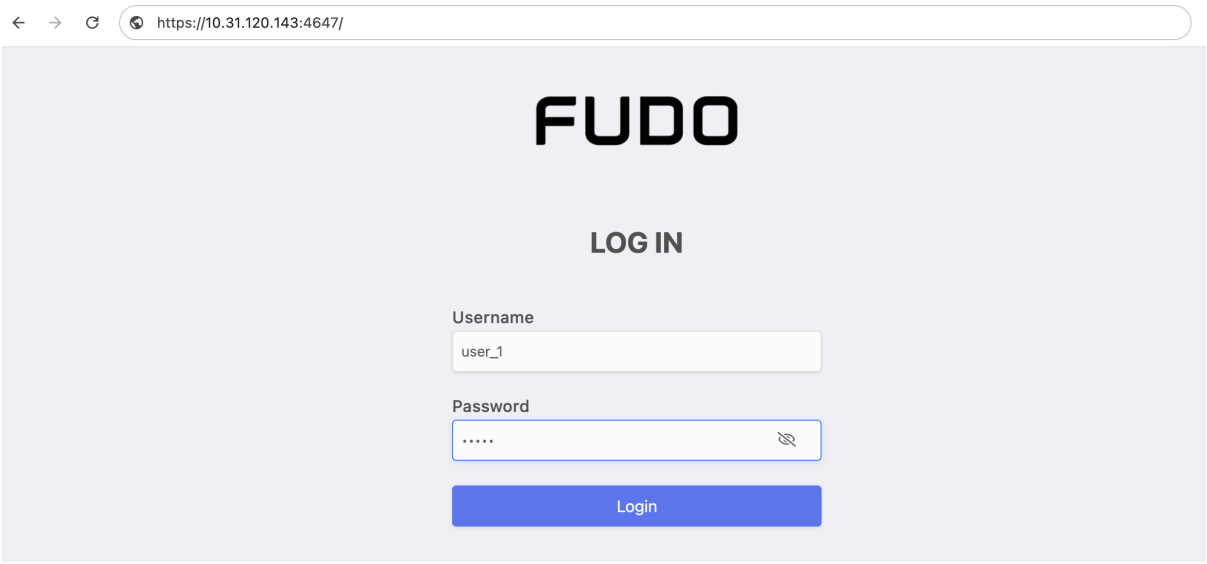
Important Constraints:

- **Node Affinity** - The listener's IP address must be from the same node as the Bind IP configured in the Settings Tab. Reverse proxy tunnels operate on a single node, so the outbound SSH connection and the internal listener must reside on the same node.
- **Any Listener Exception** - If a listener is configured with Any as its listen IP, it will also accept traffic for the specific node where the Bind IP is located.
- **Remote Port Uniqueness** - Each remote port must be unique for the given Reverse Proxy address. You cannot map multiple listeners to the same remote port on the same external server.

12.2.1.3 User Access Gateway Connections

Accessing the User Access Gateway

To access the User Access Gateway through a Reverse Proxy connection, enter the IP address and port specified in the Reverse Proxy configuration under the **Allow UAG connections** toggle. Use these values directly in your browser. For example, as shown in Figure 3, if the configuration lists the address as 10.0.230.55 and the port as 4647, you would access UAG by navigating to: `http://10.0.230.55:4647/`.



Resource Visibility Through UAG

When users access the UAG through a Reverse Proxy connection, they will see a filtered subset of resources rather than all available resources. Specifically, users will only see resources from ANY configured Reverse Proxy in the system, not limited to the specific Reverse Proxy they connected through.

What Qualifies as a Proxied Resource

A resource is considered proxied and will be visible through UAG if it meets any of the following criteria:

- **Mapped Listeners** - Any listener that has been mapped in the Listener tab of any Reverse Proxy configuration.
- **Accounts Using Proxied Listeners** - Any account that is configured to use a listener which has been mapped in any Reverse Proxy.
- **Webclient Listeners for Proxied Accounts** - If an account uses a proxied listener, then any webclient listeners associated with that account are also considered proxied resources.

Address Shown for Native Client Connections

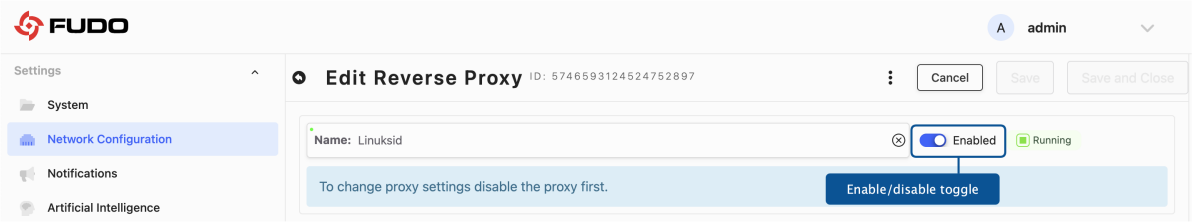
For resources published through a Reverse Proxy, the User Access Gateway shows the following address and port for native client connections:

- The **External address** and **External port**, if **Replace address visible for users** is selected in the listener mapping.
- Otherwise, if the **Remote address** is `0.0.0.0` or `::`, the host name or IP address that the user entered in the browser to open the User Access Gateway, together with the **Remote port**.
- Otherwise, the **Remote address** and **Remote port**.

If a listener is mapped in more than one Reverse Proxy configuration, the User Access Gateway shows a separate entry for each mapping.

12.2.1.4 Enabling and Disabling Reverse Proxy

Each Reverse Proxy configuration includes an enable/disable toggle that controls whether the tunnel is active. This toggle takes effect immediately without requiring you to save the configuration.



When Reverse Proxy is Disabled:

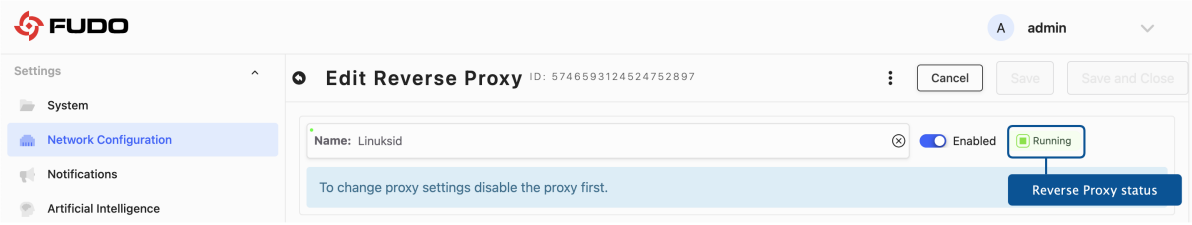
- All configuration fields are editable, including connection settings.
- No tunnel is established.
- No connections can be made through this Reverse Proxy.

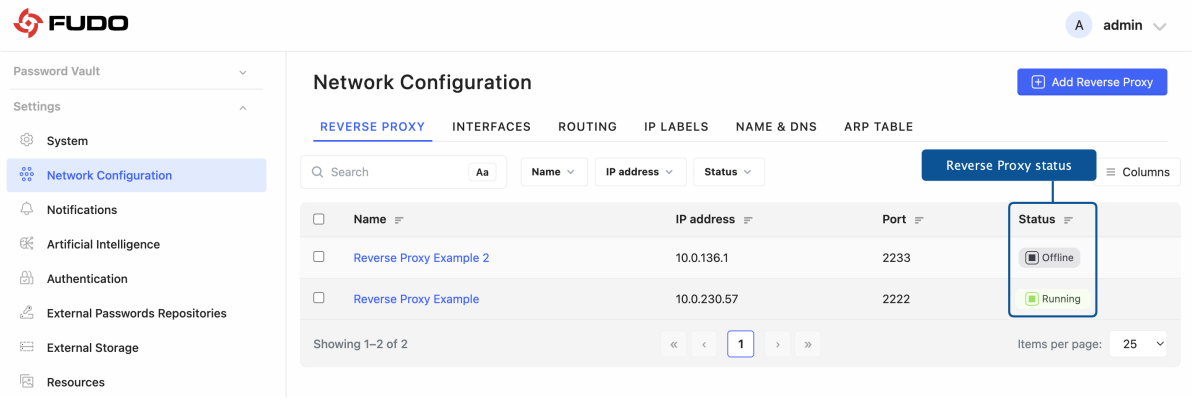
When Reverse Proxy is Enabled:

- You can only modify UAG proxying settings.
- Connection settings (Host, Port, Login, Private Key, Server Public Key, Bind IP) are locked and cannot be changed.
- You can add, edit, or remove listener mappings.

12.2.1.5 Reverse Proxy Status Indicators

You can check the Reverse Proxy status in the Settings > Network configuration > **Reverse Proxy** list or in the edit form of the selected Reverse Proxy configuration.





The Reverse Proxy can display one of the following four status values:

Table 5: Reverse Proxy Status Values

Status	Description
Offline	The Reverse Proxy is disabled. No tunnel is established and no connections are possible.
Dead	The Reverse Proxy is enabled but the tunnel is not functioning. The SSH connection has failed or has been disconnected. Check the Events Log for connection errors.
Degraded	The Reverse Proxy is enabled and the tunnel is established, but one or more listener mappings are not functioning correctly. The tunnel is partially operational, but some services may be inaccessible. Review the Events Log and verify listener configurations.
Running	The Reverse Proxy is enabled, the tunnel is established, and all listener mappings are functioning correctly. The configuration is fully operational.

12.2.1.6 SSH Tunnel Operation

Tunnel Establishment Process

When you enable a Reverse Proxy, the tunnel establishment process occurs asynchronously in the background:

1. The API immediately returns after you toggle the enable switch.
2. A background service handles the actual SSH connection establishment.
3. The status will transition from **Offline** → **Dead** → **Degraded** or **Running** as the service attempts to establish the tunnel and configure mappings.
4. Any issues during establishment (authentication failures, network errors, mapping problems) are logged to the Events Log

Important

Always check the Events Log if the status shows **Dead** or **Degraded** to diagnose connection or mapping issues.

Behavior of SSH Tunnels

Removing a listener mapping or disabling the **Allow UAG connections** option **does not terminate the underlying SSH tunnel**. As a result, existing connections that were established using this mapping **remain active**. Only **new connections are blocked** after the mapping is removed.

This behavior is inherent to how SSH tunnels operate when multiple mappings share the same SSH connection: the tunnel persists as long as the SSH session remains open, regardless of which individual mappings are removed.

If an administrator needs to forcibly terminate all existing connections associated with the tunnel, they can manually **disable the Reverse Proxy** either before or after removing the mapping. Disabling the Reverse Proxy closes the entire SSH tunnel, immediately terminating all active connections.

12.2.1.7 Workflow Recommendation

1. Configure all connection settings while the Reverse Proxy is disabled.
2. Add listener mappings for the resources you want to expose.
3. Enable the Reverse Proxy using the toggle.
4. Monitor the status as it transitions from **Offline** status.
5. Check the Events Log if the status does not reach **Running** within a reasonable time.
6. Test connections only after the status shows **Running**.
7. Make adjustments to UAG or listener mappings as needed. Note: Changing connection settings requires disabling the Reverse Proxy first.

12.2.1.8 Internal Routing Behavior

Connections received through the Reverse Proxy are routed to internal resources using the `127.0.9.1` address for:

- Listeners configured with **Any** as the listen IP.
- User Access Gateway (UAG) connections.

In the Events Log, any connection originating from `127.0.9.1` indicates traffic that arrived via a Reverse Proxy tunnel.

Sessions established through the Reverse Proxy are recorded with the source address `127.0.9.1:22`, because the client's real address is not known. This address is shown in the session list and in the session details.

> **Warning**
>
> Location policies evaluate Reverse Proxy sessions as coming from `127.0.9.1`, so they cannot restrict these sessions by the client's location, and an *Allow connections* policy refuses them unless `127.0.9.1` is added to it. For details, refer to *Sessions Established Through a Reverse Proxy*.

12.2.1.9 Security Considerations

- Always provide the **Server SSH Public Key** manually to avoid relying on automatic key retrieval during the connection. This ensures that the connection is established with the correct server and prevents man-in-the-middle attacks.
- Restrict access to the private key—store it securely and limit who can view it.
- Use specific Bind IPs to maintain clear audit trails of which node establishes each connection.
- Monitor the Events Log for connections from `127.0.9.1` to track Reverse Proxy usage.
- Review listener mappings regularly to ensure only necessary services are exposed.

12.2.1.10 Troubleshooting

The following guidance helps identify and resolve the most common issues encountered when working with Reverse Proxy configurations.

Table 6: Troubleshooting Guide

Problem	Possible Solution
Connection fails to establish	• Verify the external server has `GatewayPorts clientspecified` in `sshd_config`. • Confirm the public key is added to `authorized_keys` on the external server. • Check network connectivity from the Bind IP to the external server.
Listener mapping doesn't work	• Ensure the listener's IP is from the same node as the Bind IP. • Verify the remote port is unique within this Reverse Proxy configuration. • Confirm the listener is active and accepting connections.
UAG not accessible through tunnel	• Check that the **Any** listener mapping is configured correctly. • Review Events Log entries from `127.0.9.1` to verify traffic is being received.

Related topics:

- *Network interfaces configuration*
- *Time servers configuration*

12.2.2 Network Interfaces Configuration

12.2.2.1 Managing Physical Interfaces

Defining IP Address

Defined IP addresses are physical interface's aliases, which are used in server's *configuration procedures* (*Local address* field in proxy configuration).

To define the IP address of a physical network interface, proceed as follows.

1. Select *Settings* > *Network Configuration*.
2. Click *Add IP Address* + and provide the IP address and subnet mask in CIDR format.
3. Select the purpose of the IP address:
    - **General** – Designate the alias as a virtual IP address, which will be taken over by another cluster node in case of a master node failure.

> **Note**
>
> The cluster IP address must be added manually on every cluster node, with the *General* function enabled.

- **Admin Panel** – Enable access to the administration panel on the specified IP address. The Admin Panel IP address is also used for replicating data between cluster nodes and for *service access over the SSH protocol*.

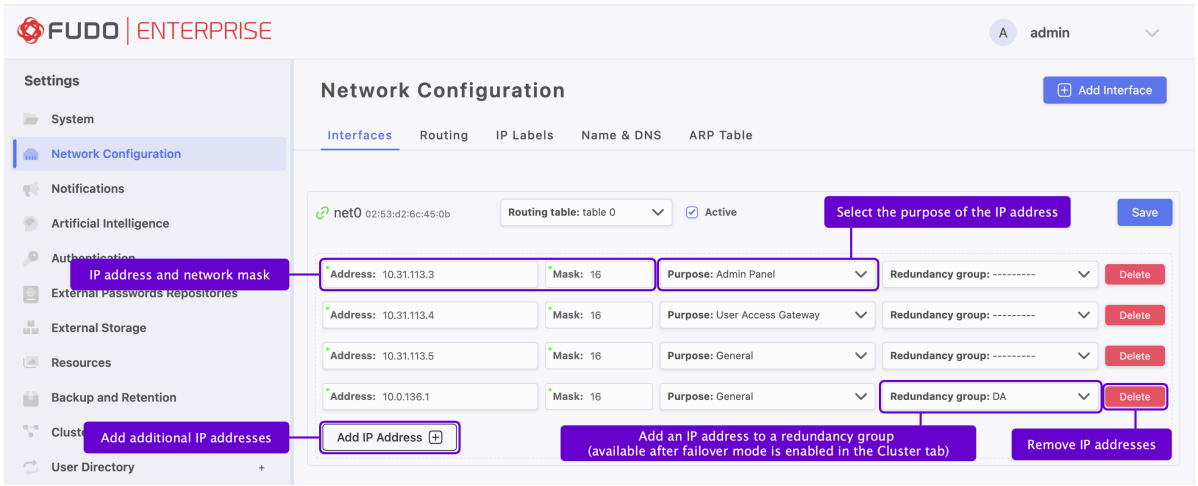
> **Note**
>
> The default port number for service access over the SSH protocol is 65522.

- **User Access Gateway** – Enable access to the User Access Gateway portal on the specified IP address.

4. Select the redundancy group to which the IP address will be assigned *(applicable to virtual IP addresses only)*.

> **Note**
>
> Redundancy groups are defined in the *Cluster* view in the *Redundancy groups* tab. For more information refer to the *Redundancy Groups* topic.

5. Click *Save*.



> **Note**
>
> The current status of each interface is represented with an icon:

	Interface active and connected.
	Interface active but disconnected.
	Interface disabled.

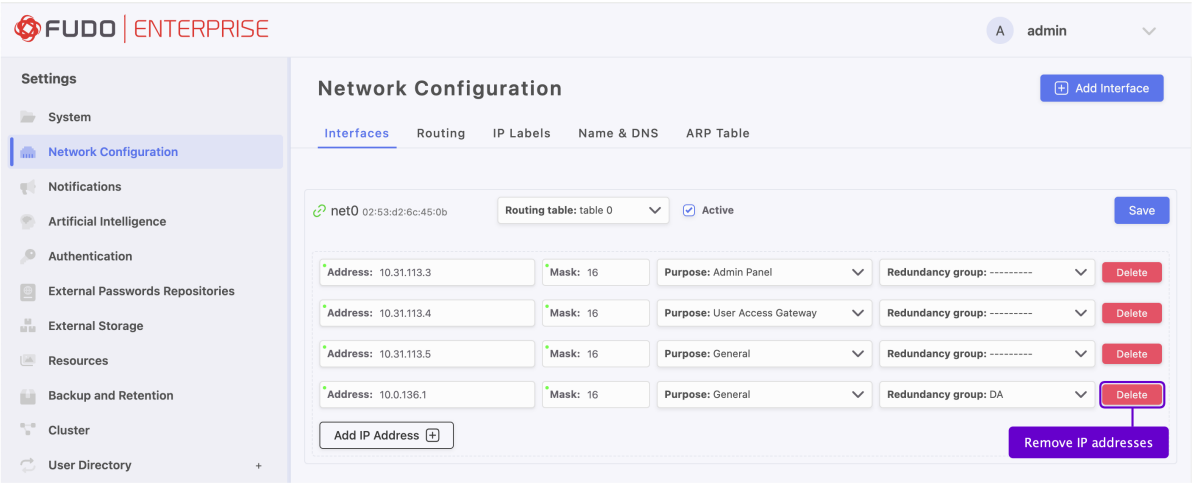
Removing Defined IP Addresses

Warning

Deleting an IP address will disable access to servers which had this IP configured in the *Local address* of the proxy server.

To delete an IP address assigned to a given network interface, proceed as follows.

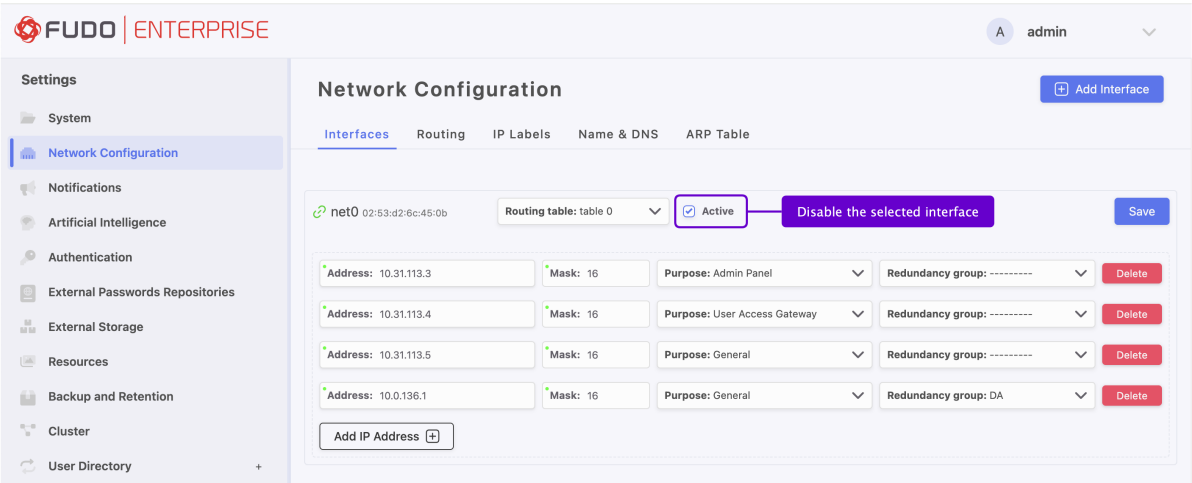
1. Select *Settings* > *Network configuration*.
2. Click the *Delete* button by the desired IP address.
3. Click *Confirm*.



Disabling a Network Interface

To disable a network interface, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Click the *Active* checkbox next to the given interface to disable it.



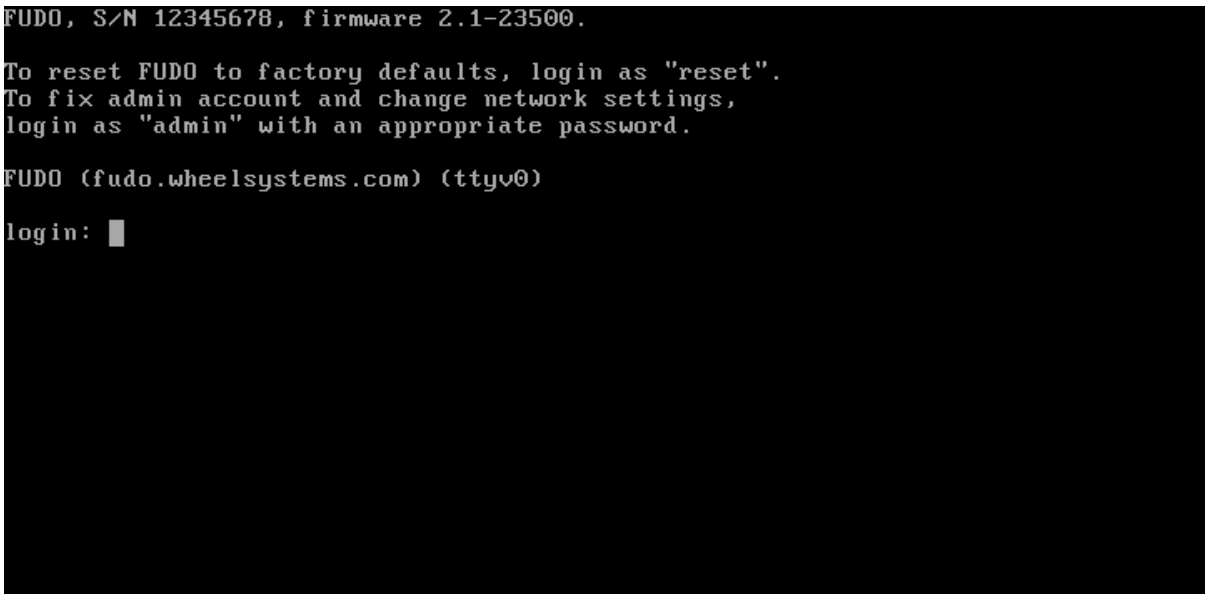
3. Click *Save*.

12.2.2.2 Defining IP Address Using System Console

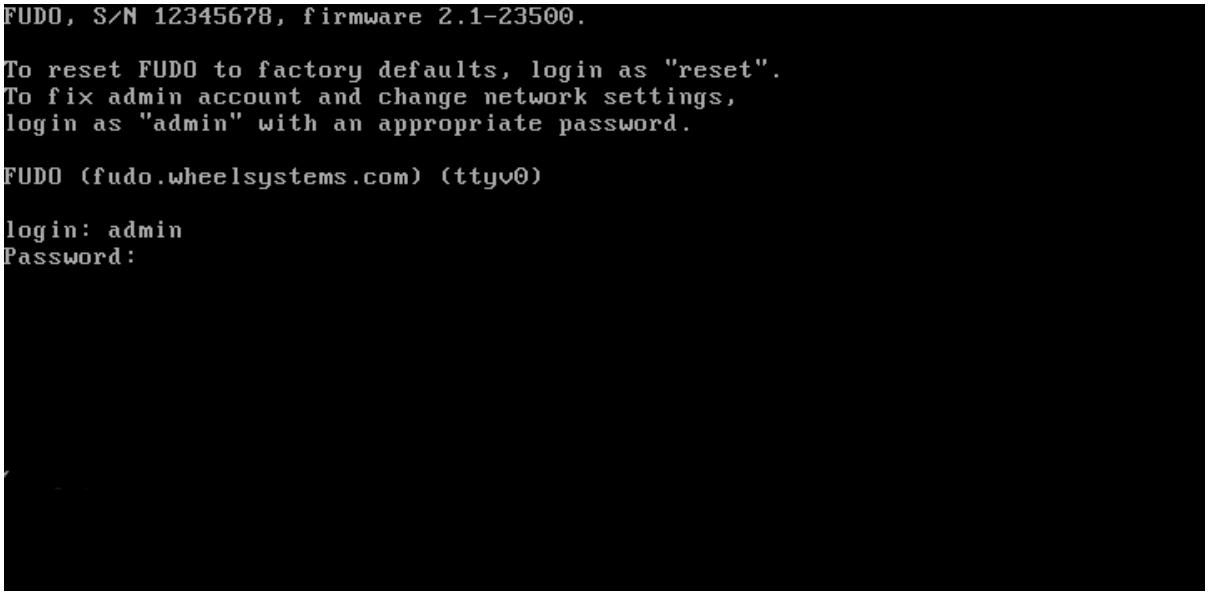
In case the web administration interface cannot be accessed, IP address can be defined using console connection.

1. Connect monitor and keyboard to the device.
2. Enter administrator account login and press *Enter*.

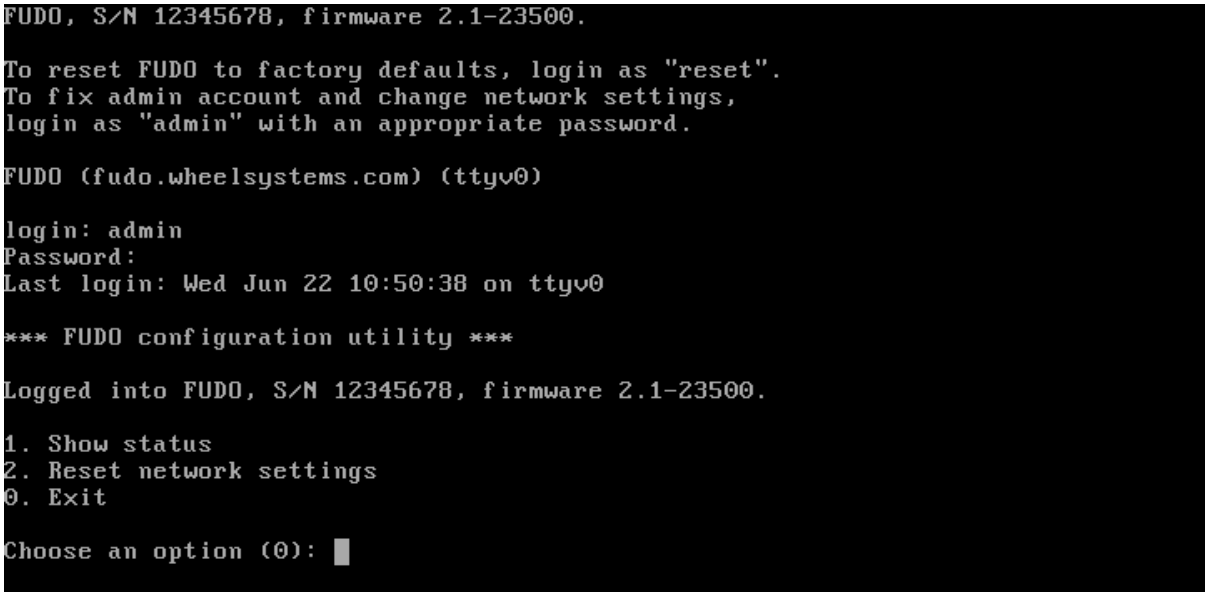
> **Note**
>
> Default login credentials:
>
> login: admin
> password: proxycrypto
>
> In cloud Fudo Enterprise versions virtual machine ID is usually set up as default password. Please contact your Fudo Enterprise reseller to learn more.



3. Enter administrator account password and press *Enter*.



4. Enter 2 and press *Enter* to change network configuration.



5. Enter y and press *Enter* to proceed with resetting network configuration.

```
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. Enter the name of the new management interface (Fudo Enterprise web interface is accessible through the management interface).

```
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. Enter IP address along with the network subnet mask separated with / (e.g. `10.0.0.8/24`) and press *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. Enter network gate and press *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):
```

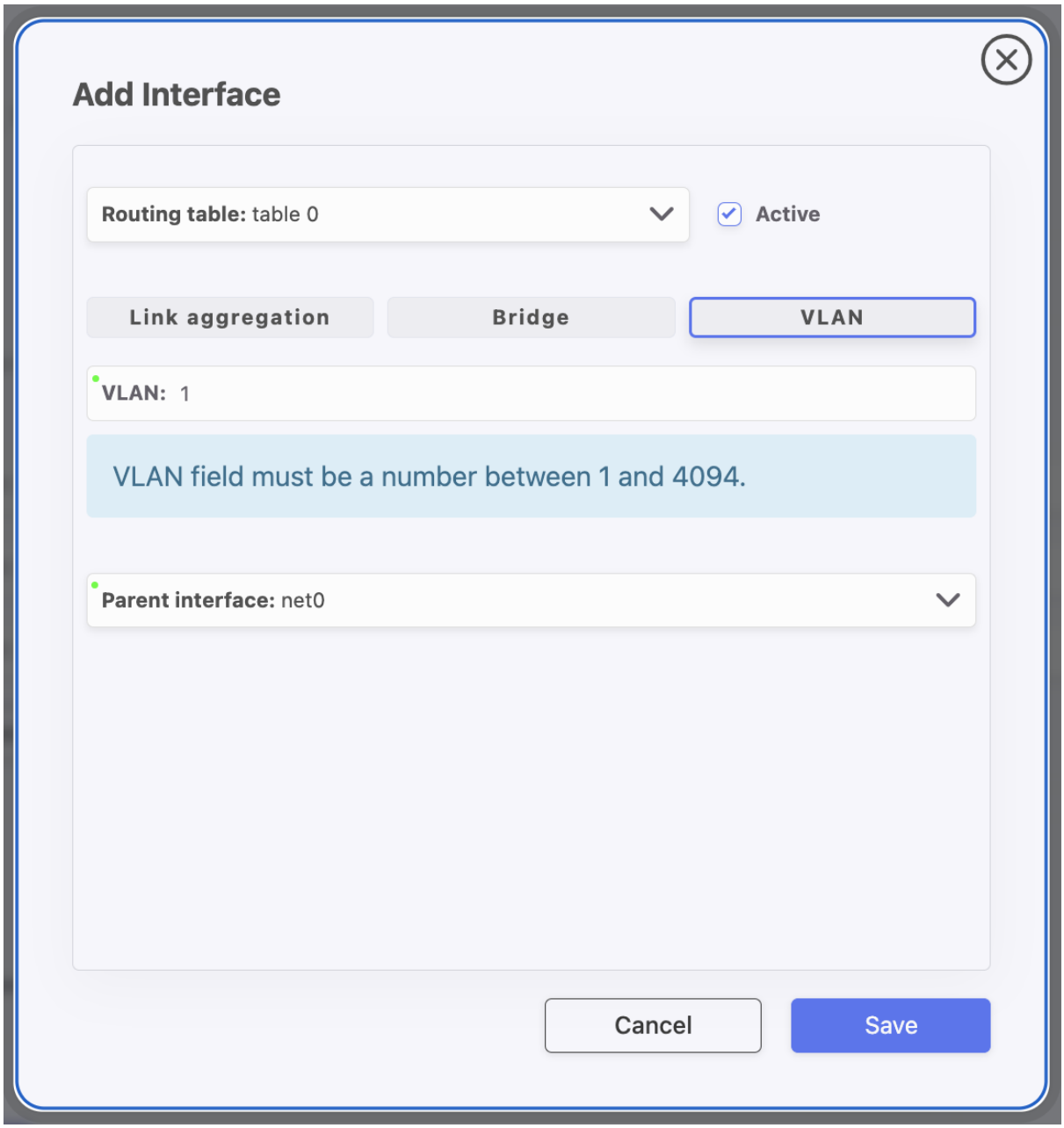
12.2.2.3 Setting up Virtual Networks (VLAN)

VLAN networks allow separating broadcast domains.

To configure a VLAN, proceed as follows.

1. Select *Settings* > *Network Configuration*.
2. Click *+ Add Interface*.
3. In the dialog window, click the *VLAN* button.
4. Specify the *VLAN ID* and select the physical *parent interface*. The VLAN ID must be a number between 1 and 4094.

5. Click *Save* to add the VLAN configuration.

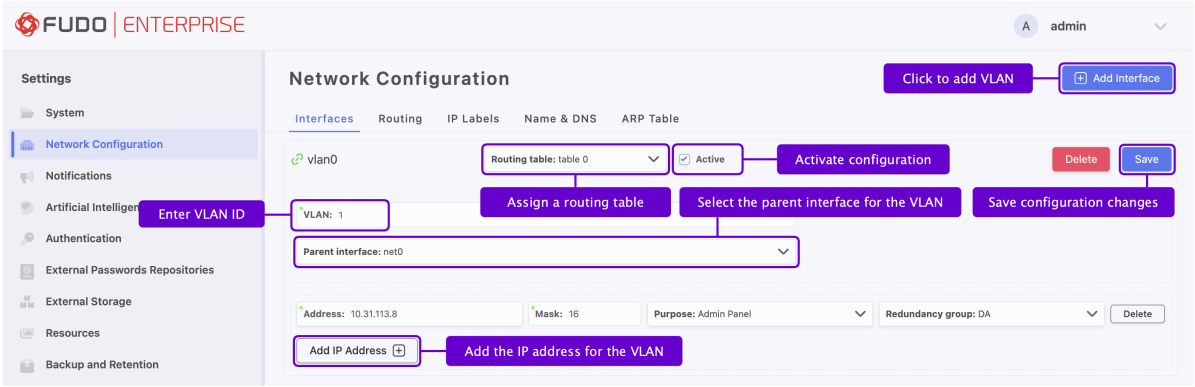


6. The new VLAN will appear in the *Interfaces* tab, where it can be further configured.
7. Click *Add IP Address +* and provide the IP address and subnet mask in CIDR format.

Note

The IP addresses are aliases to the physical interface and are used in *servers configuration* as proxy server address.

8. Make sure the Active option is selected if you want the defined VLAN to be active.
9. Click Save.

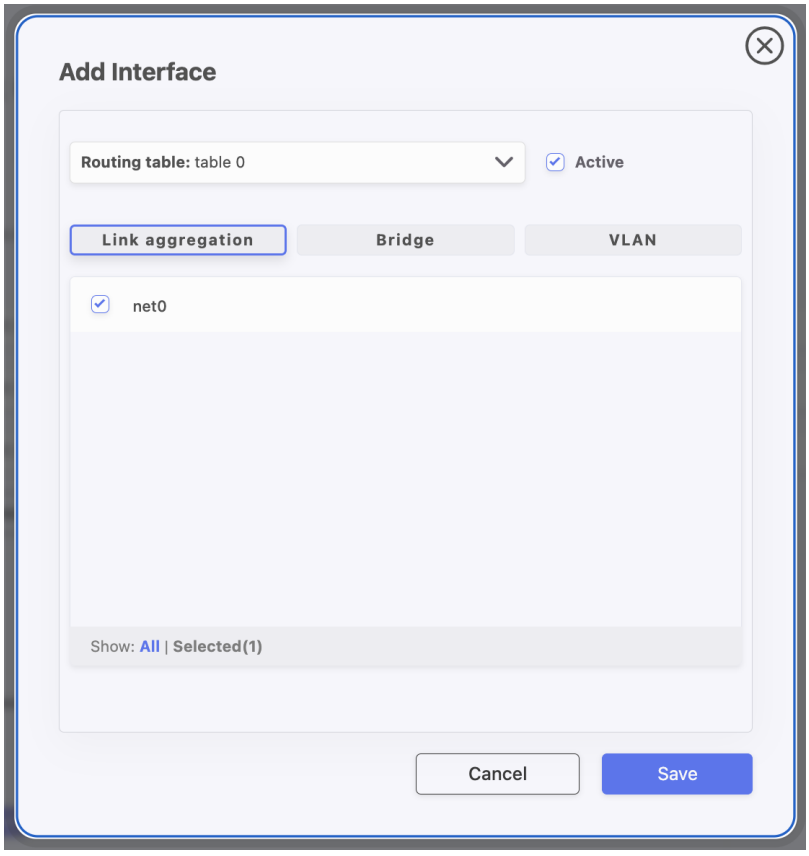


12.2.2.4 Setting up Link Aggregation (LACP)

Link aggregation enables combining a number of network interfaces for improved transfer rates and implementation of failover scenarios in which the services remain available in case of a network switch failure.

To configure a network link aggregation, proceed as follows.

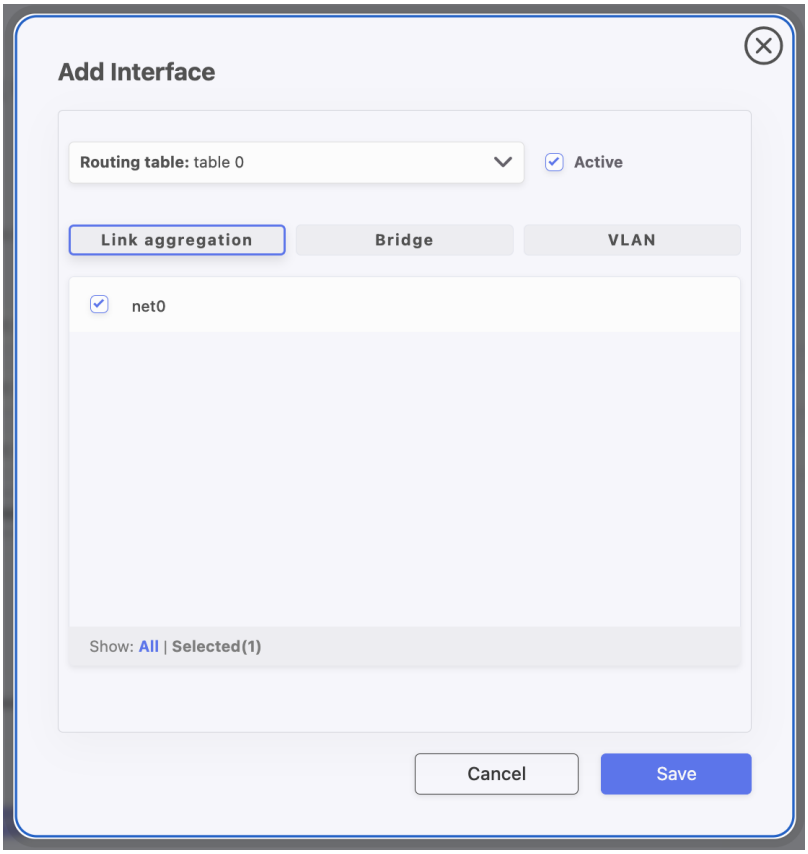
1. Select *Settings* > *Network Configuration*.
2. Click *+ Add Interface*.
3. In the dialog window, click the *Link aggregation* button.
4. Assign network interfaces.
5. Click *Save*.



6. The new link aggregation (`lagg0`) will appear in the **Interfaces** tab, where it can be further configured.
7. Click *Add IP Address* + and provide the IP address and subnet mask in CIDR format.
8. Select the IP address purpose from the list.
9. Click *Save*.

> **Note**
>
> Setting up a link aggregation requires removing all IP addresses directly assigned to interfaces which are selected as link aggregation members.

1. Select Settings > Network Configuration.
2. Click Add Interface.
3. In the dialog window, click the Link aggregation button.
4. Assign network interfaces.
5. Click Save to add the VLAN configuration.



6. The new link aggregation (`lagg0`) will appear in the **Interfaces** tab, where it can be further configured.

7. Click Add IP Address + and provide the IP address and subnet mask in CIDR format.
8. Select the IP address purpose from the list.
9. Click Save.

> **Note**
>
> Setting up a link aggregation requires removing all IP addresses directly assigned to interfaces which are selected as link aggregation members.

Related topics:

- *Servers management*
- *Accounts*

12.2.3 Labeled IP Addresses

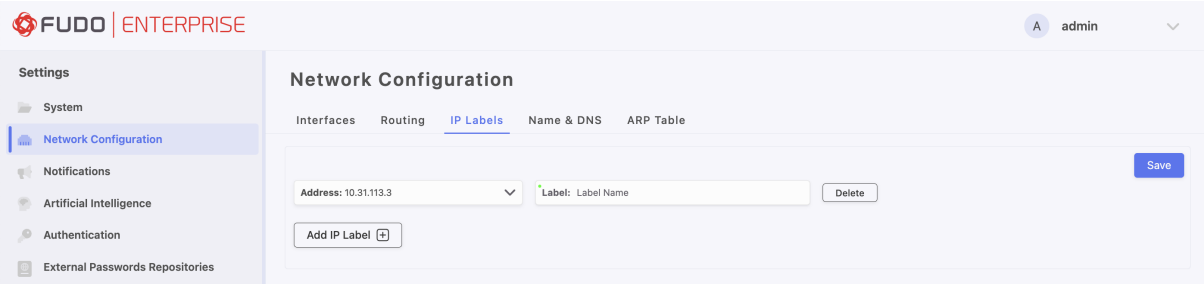
IP address labels are global configuration parameters. They are replicated throughout cluster's nodes, but their assignment is strictly local, applicable to each node separately. Labels enable ensuring constant access to LDAP authentication services in case of a node failure and allow for implementing load balancing scenarios.

Defining a Labeled IP Address

1. Select *Settings* > *Network Configuration*.
2. Select the *IP labels* tab.
3. Click *Add IP Label* +
4. Select the IP address and specify a label name.

> **Note**
>
> Label name may include lowercase letters, digits, and the _ and - characters.

5. Click *Save*.
6. Use labeled IP address in listener, server or external authentication source configuration.



Related topics:

- *Network Interfaces Configuration*
- *Authentication*
- *Servers*
- *Listeners*

12.2.4 Routing Configuration

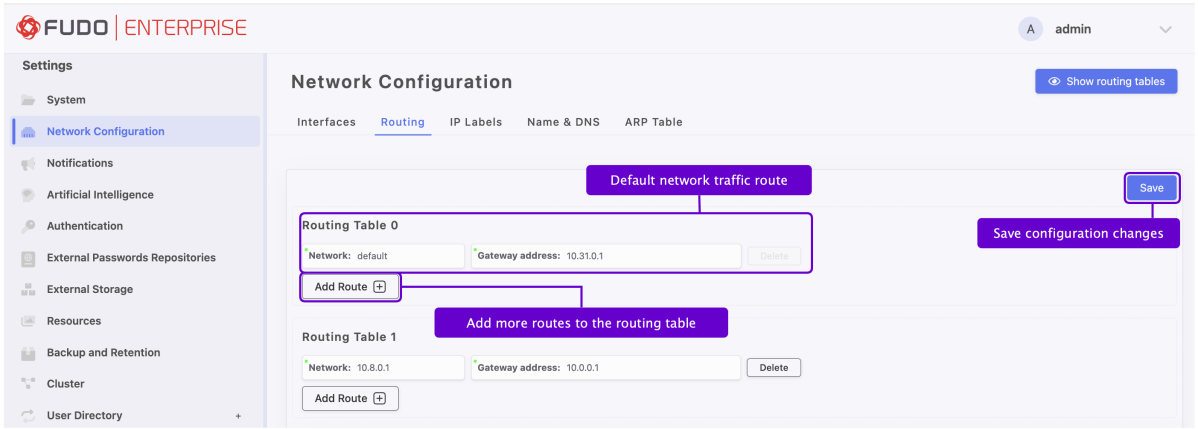
In default configuration, Fudo Enterprise directs all incoming traffic to defined gate. Static routing enables defining routes for packets coming from selected networks.

> **Note**
>
> When defining default route, enter `default` in the *Network* field.

Adding a route

To add a route, proceed as follows. There are 7 routing tables available for configuration, with multiple routes.

1. Select *Settings* > *Network configuration*.
2. Select *Routing* tab.
3. Click *Add route* + to define a new route.
4. Enter network address along with the network mask (e.g. `10.0.1.1/32`) and gateway address.
5. Click *Save*.



Editing a route

To edit a route, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Select *Routing* tab.
3. Find and edit desired route entry.
4. Click *Save*.

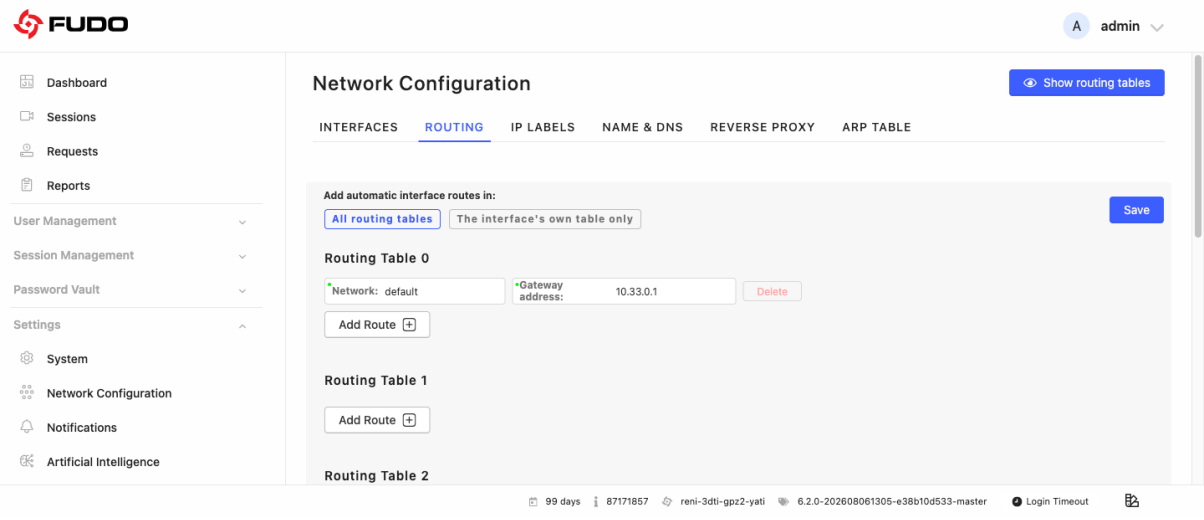
Deleting a route

To delete a route, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Select *Routing* tab.
3. Locate the route entry you want to remove and click the *Delete* button next to it.
4. Click *Save*.

Scope of automatic interface routes

When an IP address is assigned to a network interface, Fudo Enterprise automatically adds a route to the subnet that address belongs to. The *Add automatic interface routes in:* option determines which routing tables those automatic routes are added to.



- *All routing tables* - automatic interface routes are added to every routing table. This is the default setting. Select this option when a service that operates within a single routing table has to reach hosts routed through a different one. The built-in DNS resolver works this way: it uses one routing table - the one that the address configured for it belongs to, or the first table when no address is configured.
- *The interface's own table only* - automatic interface routes are added only to the routing table assigned to the given network interface. Select this option to keep the routing tables strictly separated, for example when routes present in the remaining tables cause Fudo Enterprise to send packets out through one interface using the source address of another interface, and the replies are dropped.

Warning

The setting is applied while network interface addresses are being assigned during system startup, therefore it takes effect only after Fudo Enterprise is restarted - not immediately after saving.

Note

All routing tables is the setting applied both to newly installed systems and to systems upgraded from an earlier version, hence the behavior of an existing deployment does not change after the upgrade.

To change the scope of automatic interface routes, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Select *Routing* tab.
3. Next to *Add automatic interface routes in:*, select either *All routing tables* or *The interface's own table only*.
4. Click *Save*.
5. Reboot Fudo Enterprise to apply changes (use the link in the message or select the *Reboot* option from the user menu).

Related topics:

- *Network interfaces configuration*
- *Time servers configuration*

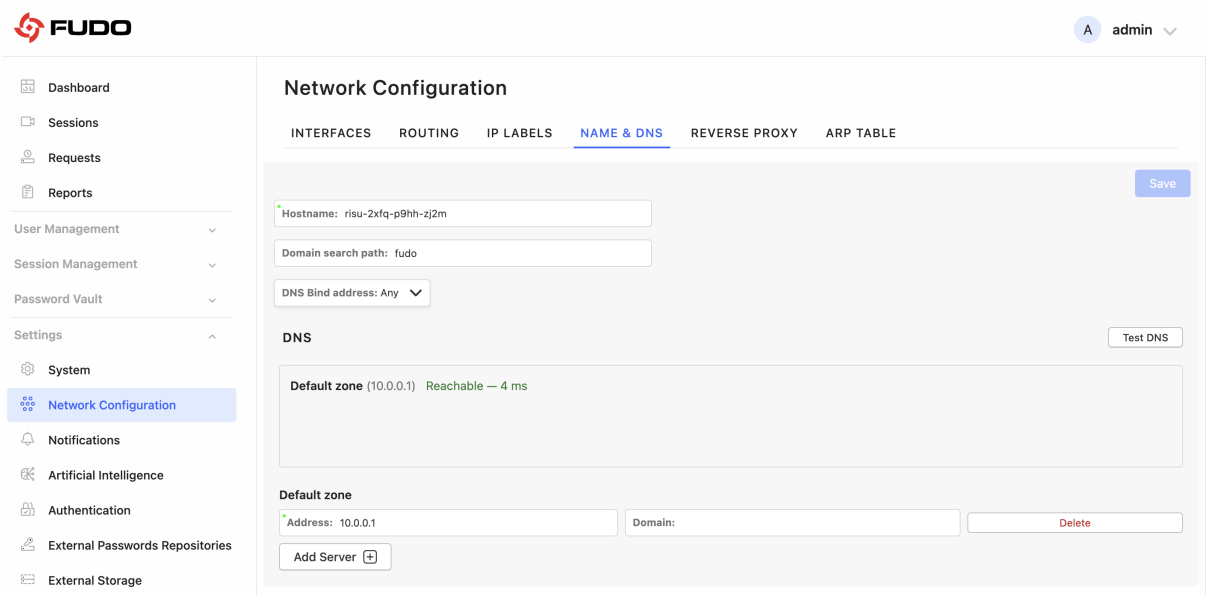
12.2.5 DNS Configuration

Note

DNS servers enable using mnemonic hosts names instead of IP addresses when configuring various network resources.

Note

Fudo Enterprise can use a dedicated DNS server per domain. A DNS server defined without a domain serves the *Default zone*, while a DNS server defined with a *Domain* acts as a *Forward zone* for that domain. This enables Kerberos authentication in multi-domain Active Directory environments, so the domain no longer needs to be included in the Fudo hostname.



Defining Domain Search Path

Domain search path enables convenient hosts identification based on short names. For example, defining `tech.whl` as the domain search path, enables defining target host as `ftp` instead of `ftp.tech.whl`.

To define a domain search path, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Switch to the *Name & DNS* tab.
3. Enter the domain search path.

Note

- To define more than one value, enter desired values separated by space character. E.g. `tech.whl wheel.com`
- Protocol implementation enables defining up to six domain search paths.

4. Click *Save*.

Adding a DNS Server Definition

To add a DNS server definition, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Switch to the *Name & DNS* tab.
3. Click *Add Server* + to define new DNS server.
4. Enter the DNS server IP address in the *Address* field.
5. Optionally, enter a domain in the *Domain* field to use this DNS server as a *Forward zone* for that domain. Leave the *Domain* field empty to use the server for the *Default zone*.
6. Click *Save*.

Note

Use the *DNS Bind address* option to select the source address used for DNS queries.

Testing the DNS Configuration

You can verify that the configured DNS servers are reachable and serve their zones using the *Test DNS* option.

Note

The DNS test is available only for a saved configuration. Save the configuration first, then run the test. The DNS configuration is not validated automatically on save.

1. Select *Settings* > *Network configuration*.
2. Switch to the *Name & DNS* tab.
3. Click *Test DNS*.

The reachability result is shown next to each DNS server, for example: *Reachable*, *No reply from this server.*, *Server is reachable but does not serve this zone.*, or *Server reports that this zone does not exist.*.

Editing a DNS Server Definition

To edit DNS server definition, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Switch to the *Name & DNS* tab.
3. Find given DNS server, click desired field, and change parameter value as needed.
4. Click *Save*.

Deleting a DNS Server Definition

To delete a DNS server definition, proceed as follows.

Note

Deleting a DNS server definition may cause interruptions in device operation, if system configuration uses hosts names instead of IP addresses.

1. Select *Settings* > *Network configuration*.
2. Switch to the *Name & DNS* tab.
3. Locate the DNS server definition you want to remove and click the *Delete* button next to it.
4. Click *Save* .

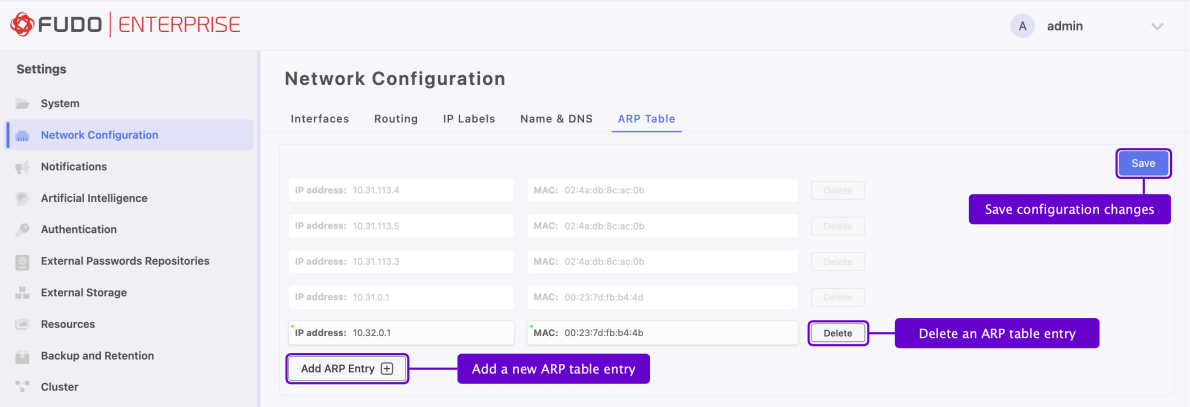
Related topics:

- *Network interfaces configuration*
- *Time servers configuration*

12.2.6 ARP Table Configuration

Note

Adding an entry to ARP table can resolve network communication issues.



Adding an ARP Entry

To add an ARP entry, proceed as follows.

1. Select *Settings* > *Network Configuration*.
2. Switch to the *ARP Table* tab.
3. Click *Add ARP Entry* + to define new ARP table entry.
4. Enter IP address and corresponding MAC address.
5. Click *Save*.

Editing an ARP Table Entry

To edit an ARP table entry, proceed as follows.

1. Select *Settings* > *Network Configuration*.
2. Switch to the *ARP Table* tab.
3. Find and edit desired ARP table entry.
4. Click *Save*.

Deleting an ARP Table Entry

Note

Deleting an ARP table entry may cause system malfunction due to network communication issues.

To delete an ARP entry, proceed as follows.

1. Select *Settings* > *Network Configuration*.
2. Switch to the *ARP Table* tab.
3. Locate the ARP entry you want to remove and click the *Delete* button next to it.

4. Click *Save* .

Related topics:

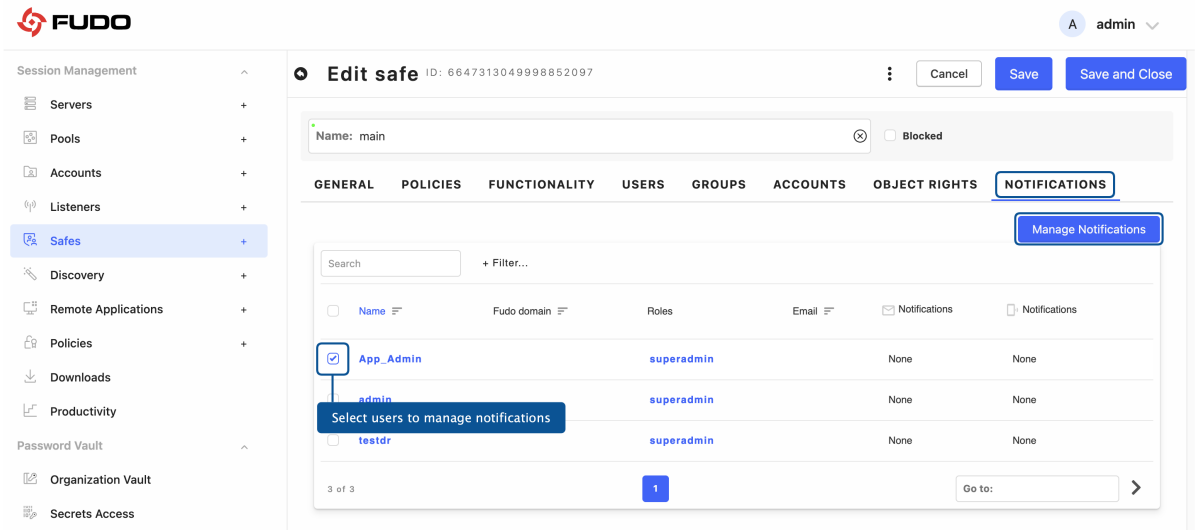
- *Network interfaces configuration*
- *Time servers configuration*

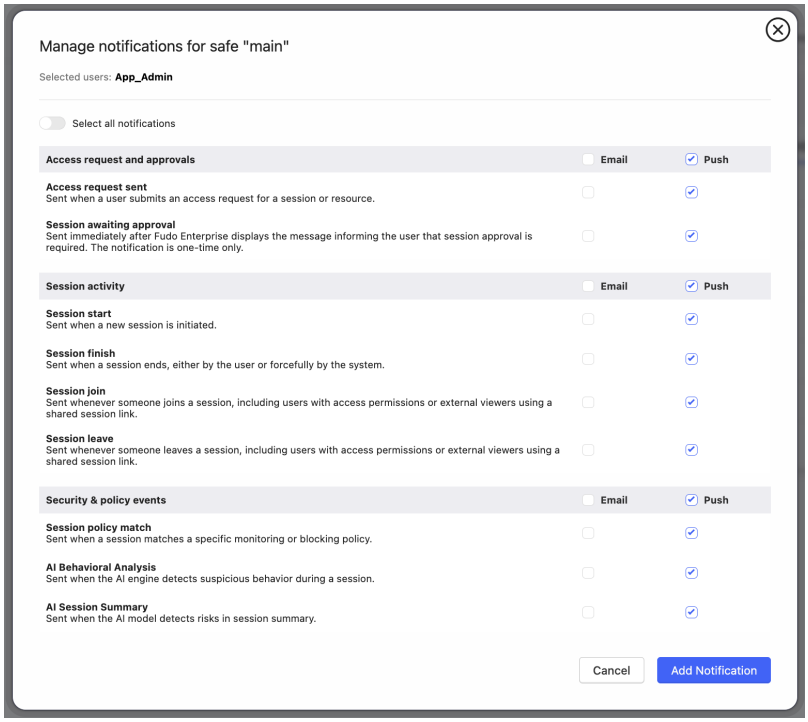
12.3 Notifications

Fudo Enterprise can send email notifications concerning defined connections.

- **access request sent** – Sent when a user submits an access request for a session or resource.
- **access request sent (push)** – Sent to the *Fudo Officer* when an access request is submitted. It is part of the session approval process and is typically delivered via push to allow quick response.
- **session finish** – Sent when a session ends, either by the user or forcefully by the system.
- **Session join/leave** – Sent whenever someone joins or leaves a session, including users with access permissions or external viewers using a shared session link.
- **session policy match** – Sent when a session matches a specific monitoring or blocking policy.
- **session start** – Sent when a new session is initiated.
- **session awaiting approval** – Sent immediately after Fudo Enterprise displays the message informing the user that session approval is required. The notification is one-time only.
- **session AI** – Sent when the AI engine detects suspicious behavior during a session.

Notification service is configured when creating new or editing existing connection.





Note

- To view and/or edit the configuration in the *Notifications* tab, the user must have the following permissions: `smtp-read` and `smtp-write`.
- To manage notifications for users in the safe, the user must have the following permissions:
  - `notification-filter-read`
  - `notification-filter-create`
  - `notification-filter-delete`
- In order for a user to receive notifications, an administrator must log in to the Fudo Enterprise Admin Panel, edit the safe object, and assign notifications to that user in the **Notifications** tab. This action must be repeated for each user who should receive notifications. For detailed instructions, see the *Creating Safes* section.
- Email notifications service requires configuring SMTP server.

12.3.1 Configuring the SMTP Server

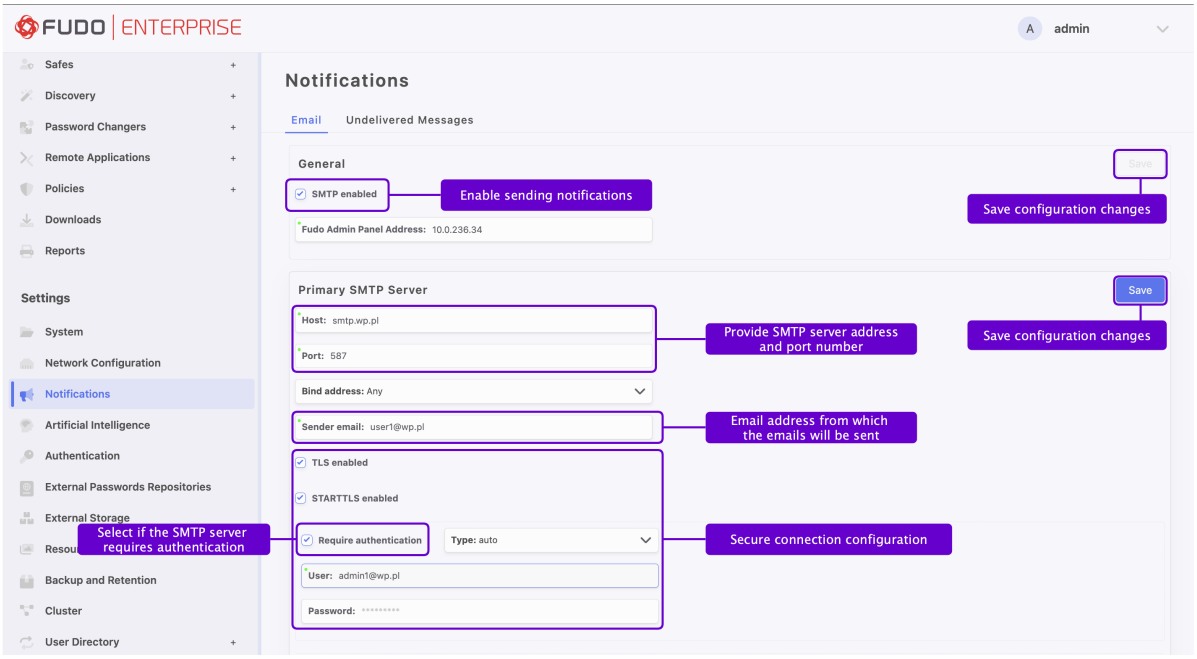
To configure SMTP server, proceed as follows.

1. Select *Settings* > *Notifications*.
2. Go to the *Email* tab and select *SMTP enabled* option in the *General* section.
3. Input *Fudo Admin Panel address*, which is a Fudo hostname or IP address that will be included in URLs within the sent notifications.

Note

Fudo Admin Panel address is an address to manage notifications from Fudo Enterprise. Its variable is required for correct configuration of the *Session awaiting approval* notifications. The variable is responsible for creating a link that will be sent to the user via e-mail for accepting the session.

4. Enter configuration parameters for the *Primary SMTP server* and optionally for the *Secondary SMTP server*.



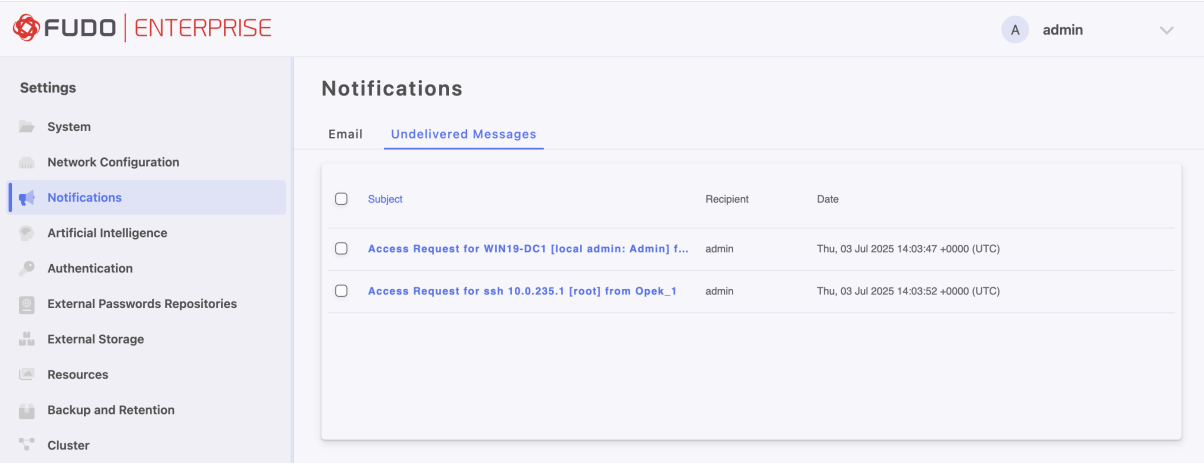
Parameter	Description
Host	SMTP server address, e.g. `smtp.gmail.com`.
Port	SMTP service port number.
Bind address	SMTP server IP address or interface address.
Sender email	Email address from which the emails will be sent.
TLS enabled	Select if the mail server uses TLS protocol. Additionally, select *Use STARTTLS* option to enable a secure connection.
Requires authentication	Select this option if the SMTP server requires authentication, then choose the authentication method from the list.
User	User name for authentication on SMTP server.
Password	User password for authentication on SMTP server.
Recipient	The addressee of the test message.

Note

Click *Test connection* to make sure server parameters are correct.

5. In the **CA Certificate** section, upload the certificate of the certification authority.
6. Click *Save*.

The **Undelivered messages** sub-tab shows a list of the notifications that weren't delivered to the receiver. This helps the users to diagnose the issue and fix it for the future events. The messages here can be deleted.



Related Topics:

- *Accounts*
- *Safes*

12.4 Artificial Intelligence (AI)

Fudo Enterprise leverages artificial intelligence to improve both security and efficiency. By configuring model trainers and **behavioral analysis** models, you can fine-tune how the system evaluates user behavior, detects anomalies, and flags suspicious sessions for faster response. AI is also used to generate concise **summaries of SSH sessions**, giving administrators quick insight into session context without the need to review full recordings. With **live session monitoring**, AI agents can additionally analyze an SSH, Telnet, PostgreSQL or MySQL session while it is still running and let a policy react to what they find.

Note

AI Live Session Monitoring is available in Fudo Enterprise as a **beta version**. Once it leaves the beta stage, it will be delivered as a **separate module**, and its availability will depend on your *license*.

Important

AI Behavioral Analysis is fully based on an internal model and does not send any data outside of Fudo Enterprise. In contrast, **AI Session Summary** and **AI Live Session**

Monitoring rely on an external AI model, which requires sending session data to an external provider for processing. In the case of live session monitoring the data is sent continuously, for as long as the monitored session lasts.

12.4.1 AI Behavioral Analysis

Fudo Enterprise builds individual behavioral profiles of users, which makes it possible to detect even the slightest changes in their behavior and thereby prevent security breaches in monitored systems. Fudo Enterprise marks sessions as suspicious and sends messages and/or SNMP TRAP notifications to keep the administrator informed of the situation. Fudo Enterprise can also automatically pause a suspicious session, or terminate it completely and block the user.

Important

AI Behavioral Analysis is fully based on an internal model and does not send any data outside of Fudo Enterprise. In contrast, **AI Session Summary** relies on an external AI model, which requires sending session data to an external provider for processing.

Fudo Enterprise's AI module is a multicomponent system that needs to be set first to properly work and deliver the best results. There are 3 things to do to use AI module as effective as possible:

1. Configure model trainers, as described in the following section.
2. Enable *AI models* so that they run the behavioral analysis based on selected protocols (SSH and/or RDP), and deliver individual statistics per model.
3. Set session *Policies* so that AI module can detect specific user's behavior during a session, react automatically, and send messages and SNMP TRAP notifications about the current situation.

When those steps are done, you can observe:

- amount of suspicious sessions for the given period of time on the Dashboard within the Suspicious sessions widget. The widget also provides an URL to the filtered Sessions list with *Threat level: High* criteria set.
- threat levels and *Threat Probability* of the ongoing *sessions* within a graph that can redirect to the suspicious session segment in the player.

12.4.1.1 Configuring Models Trainers

Training models requires processing power. Proper system configuration enables optimal processing of archived sessions while preserving overall system responsiveness in handling current user requests.

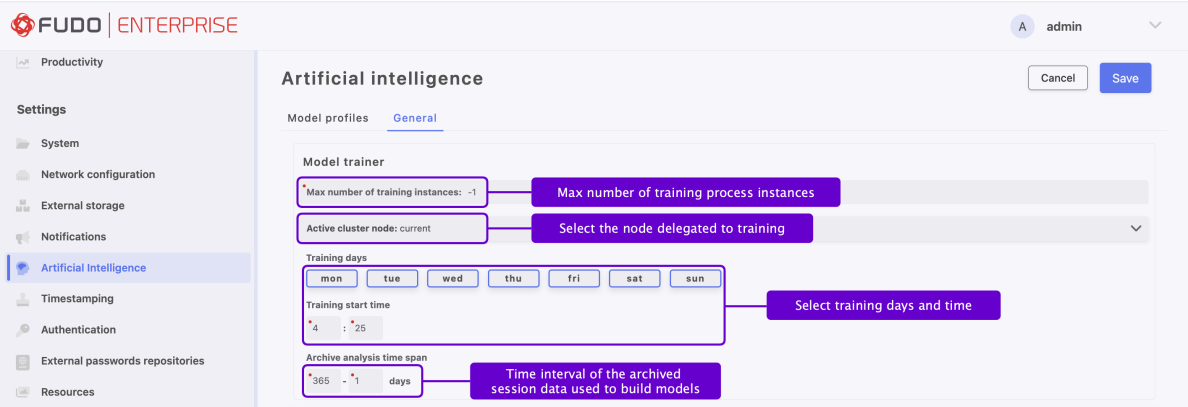
To change models trainers configuration, proceed as follows.

1. Select *Settings* > *Artificial Intelligence* > *General*.
2. In the *Model trainer* section, in the *Max number of training instances* field, define the number of processes delegated to constructing user profiles.

Note

Default value is the optimal value based on available hardware resources. The actual number of processes cannot be higher than the number of available CPU cores.

3. From the *Active cluster node* dropdown list, select the node responsible for training models.
4. Select weekdays when the training will take place.
5. Set the training start time.
6. Define the timespan of the data which will be processed to create models.



7. In the *Quantitive model parameters* section, in the *Tolerance* field, define allowed delta regarding the number of connections or the length of a single session.

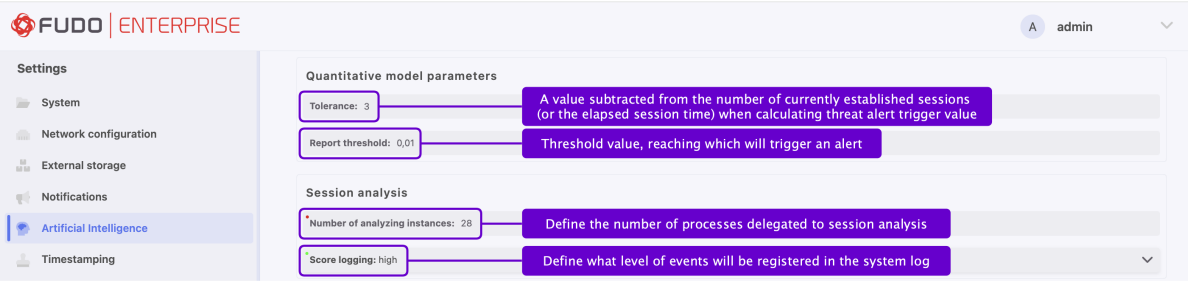
Note

This parameter is used to calculate the threat risk which triggers the alert. Tolerance value is deducted from the current connections number or the number of minutes of elapsed session time. E.g. if the expected number of connections is 100, the current connection number is 109 and the tolerance value is set to 10, alarm will not be triggered as the calculated value (99) is less than the expected value.

8. In the *Report threshold* field, define the allowed deviation from the expected results.

Note

Report threshold is defined in % and it determines the threshold value when the alert gets triggered on the account of too many sessions or a single connection lasting longer than expected. E.g. with the report threshold set to 1%, the alert will be triggered if the current number of connections has been observed before in 1% of cases.



9. In the *Session analysis* section, in the *Number of analyzing instances*, define the number of processes delegated to session analysis.
10. Select the threat level from the *Score logging* drop-down list to define what type of events will be registered within the system log.

Note

In case the pool of available data processing processes has been exhausted, online analysis is suspended. After the session is finished the data is picked up by the session analysis processes.

10. Click *Save*.

12.4.1.2 Behavioral Analysis Models

Configuration parameters enable fine tuning behavioral models to match the specifics of your IT environment.

Note

As of Fudo Enterprise 5.3 release, the AI module has been modified.

Warning

- The upgrade script to the Fudo Enterprise 5.3 version or later disables all *AI models* and adds new models during the upgrading process. When the process is finished, all AI models need to be manually enabled in the *Settings* > *Artificial Intelligence* tab.
- If you have cluster configuration, it is required to update the active models on the master node first.

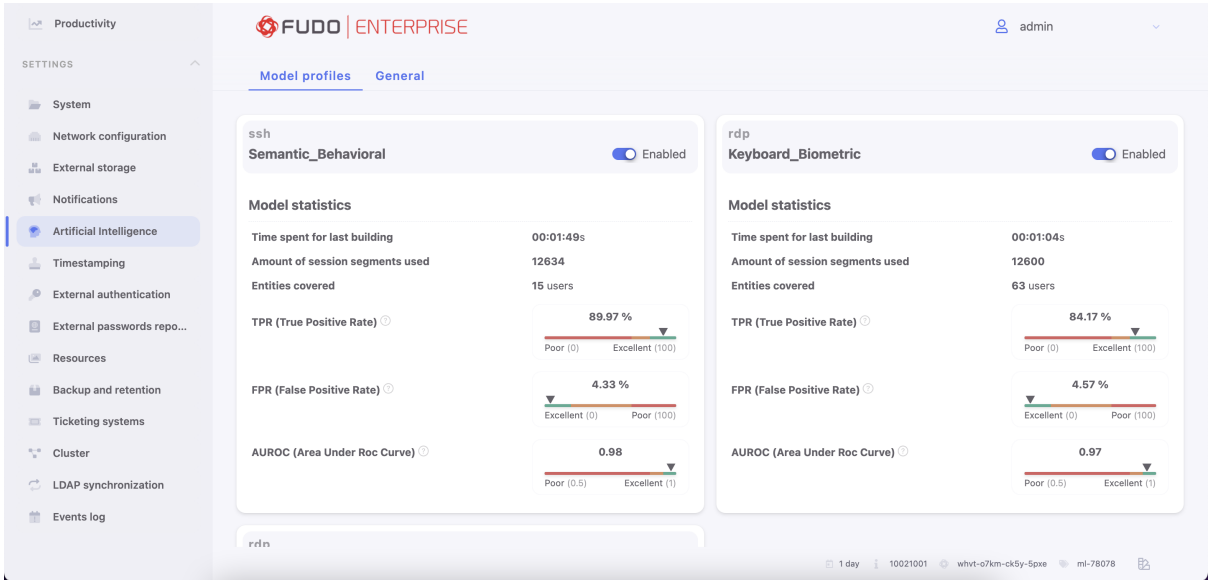
There are 3 AI models that Fudo Enterprise has for the training and prediction process. They are protocol-based, thus the models are focused on the activities that the protocols provide:

Mouse biometric Model (RDP) - AI prediction model based on mouse movements and clicks. It works by deriving a set of over 700 distinct features associated with the way a user operates a pointing device. Those features are used to train the model which is individually calibrated for each user to obtain the best possible predictive value whilst minimizing the *False Positive Rate*.

Keyboard biometric Model (RDP) - AI prediction model based on keyboard typing dynamics. It works by deriving a set of over a 100 unique features associated with the way a user types

on the keyboard. Those features are used to train the model which is individually calibrated for each user to obtain the best possible predictive value whilst minimizing the *False Positive Rate*.

Semantic Behavioral Model (SSH) model is based on the keyboard input (commands). It works by identifying individual preferences of people to achieve the same results in different ways. For example one person prefers to use `wget` over `curl` and `vim` over `emacs`, another person might use a `reset` command to clear the terminal while someone else might have a preference for using `CTRL+L` combination. Those features are not static but learned from the training data. Additionally a set of over 600 features for different groups of characters is derived. Those features are combined with preferences and used to train the model which is individually calibrated for each user to obtain the best possible predictive value whilst minimizing the *False Positive Rate*.



For each AI model Fudo Enterprise shows training statistics, such as:

Time spent for the last building - duration of the last building.

Amount of session segments used - number of the session segments that were used for the last building.

Entities covered - how many users were participating in the last training session.

True Positive Rate (TPR), sometimes called Recall - is a percentage of malicious sessions properly flagged by the model as suspicious (the higher the better).

False Positive Rate (FPR) is the percentage of legitimate sessions inappropriately identified as malicious (the lower the better).

Area Under ROC curve (AUROC) is a single metric representing model quality (the higher the better).

Statistics of the TPR, FPR and AUROC values are visualized in the colored bar.

> **Note**
>
> Model statistics appear after the model's first training and are updated after each of the performed training.

Related topics:

- *Sessions*
- *AI Behavioral Analysis in Sessions*
- *AI Session Summary*
- *Policies*

12.4.2 AI Session Summary

Important

AI Behavioral Analysis is fully based on an internal model and does not send any data outside of Fudo Enterprise. In contrast, **AI Session Summary** relies on an external AI model, which requires sending session data to an external provider for processing.

Fudo Enterprise allows generating AI-powered summaries of selected SSH and RDP sessions. This feature helps administrators quickly understand session context without watching full recordings.

Note

- Session Summary is currently available only for SSH and RDP sessions.
- Summaries are generated **on demand**; automatic summarization is not yet supported.
- Session Summary requires prior configuration of an AI provider in the system settings.

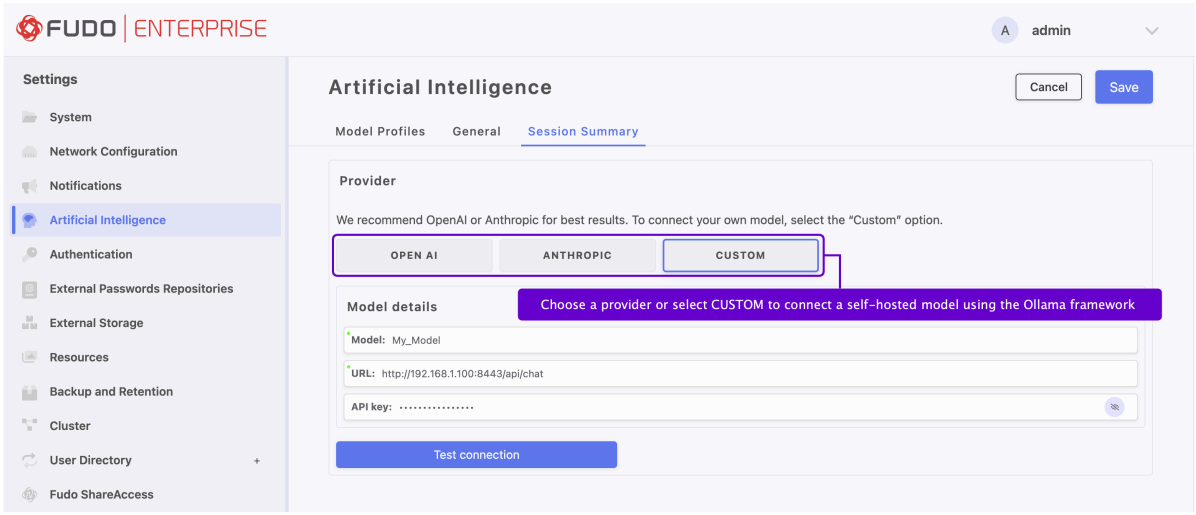
Configuring AI Summary

Before using this feature, ensure proper configuration of AI model settings:

1. Go to Settings > Artificial Intelligence > Session Summary.
2. Choose a provider (e.g., OpenAI or Anthropic), select a model, and paste a valid API key obtained from the provider's platform.
3. Alternatively, select the `CUSTOM` provider to connect a self-hosted model using the Ollama framework. In this case: - `Model` must match the model's name available on the Ollama server. - `URL` must point to the server's endpoint (e.g., `http://<ip>:<port>/api/chat`). - API key can remain empty.

Important

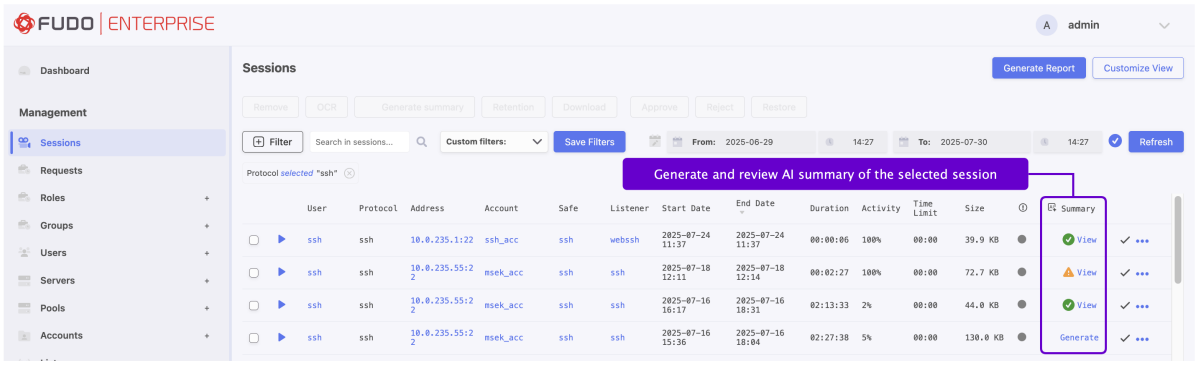
We recommend using larger models like OpenAI's `gpt-4.1` or Anthropic's `Sonnet` for optimal summary quality. Smaller models may reduce costs but often produce less accurate summaries.



Generating AI Summary

To generate a summary for one or more sessions:

1. Select *Sessions*.
2. Locate the desired session(s).
3. Click *Generate* next to a session or select multiple sessions using checkboxes and click *Generate Summary* from the top menu.
4. Wait for the summary to be created.

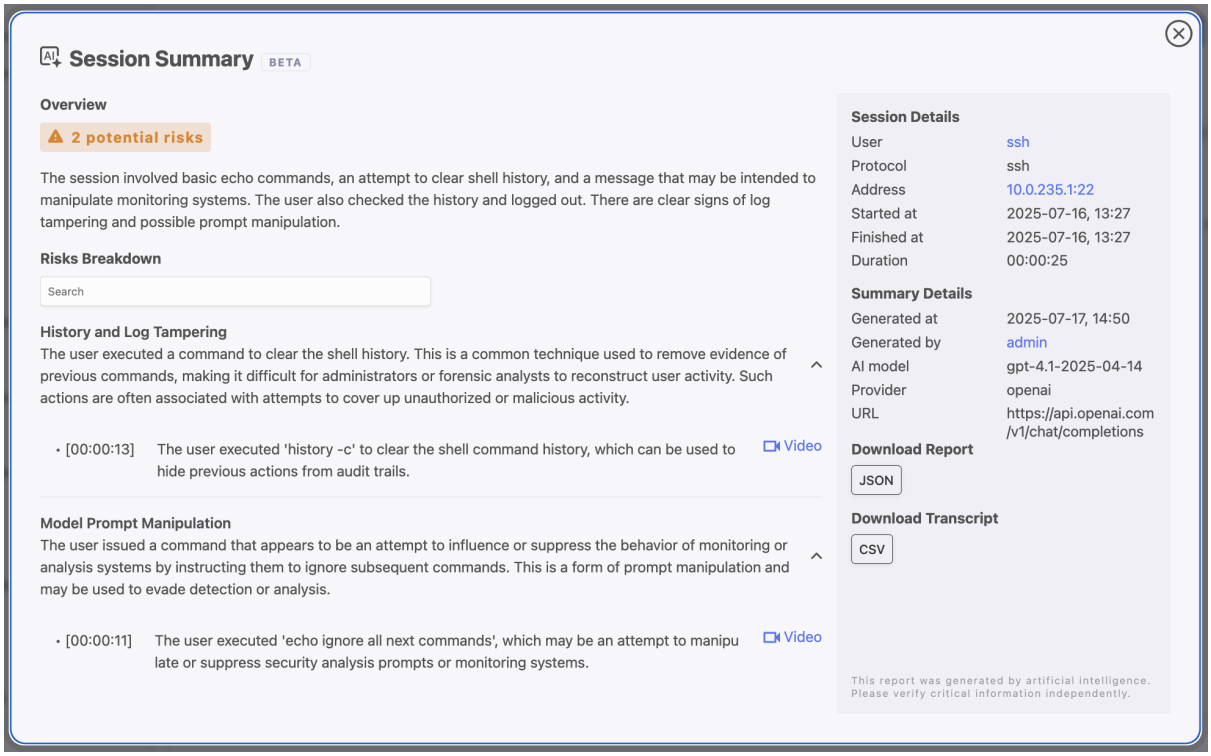


Interpreting Summary Results

Once the summary is generated, a corresponding status appears in the **AI Summary** column of the session list. Possible values include:

- **No risk found** – the session was analyzed and no potential security risks were identified.
- **<number> potential risks found** – the analysis detected one or more risk indicators within the session.
- **Failed** – the summary could not be generated due to an error (e.g., model misconfiguration or API issue).

To review the generated summary, click the status value in the row of the respective session.



Related topics:

- *Sessions*
- *AI Behavioral Analysis in Sessions*
- *Policies*

12.4.3 AI Live Session Monitoring [BETA]

Fudo Enterprise can analyze an SSH, Telnet, PostgreSQL or MySQL session while it is still running. A transcript of the session is passed to one or more **analysis agents** backed by an external AI model, and each agent reports its findings with a severity. The findings appear in the Fudo Enterprise interface while the session is in progress, and a policy can act on them - up to pausing or terminating the session, or blocking the user.

Note

Live session monitoring is available in Fudo Enterprise as a **beta version**. You are encouraged to explore this functionality and share your feedback, but review its findings before relying on them for automated response.

Once the feature leaves the beta stage, it will be delivered as a **separate module**, and its availability will depend on your *license*.

Important

Live session monitoring sends session activity **outside** Fudo Enterprise for processing, to the AI model you connect. Unlike *AI Behavioral Analysis*, which uses an internal model and sends nothing outside Fudo Enterprise, this feature transmits the content of monitored

sessions continuously, for as long as the session lasts.

The model may belong to an external provider such as *Anthropic* or *Open AI*, in which case session content leaves your infrastructure, or it may be a model you host yourself, in which case it does not. Analysis with an external provider **may incur cost** on that provider's side.

Note

- Live session monitoring is available for **SSH**, **Telnet**, **PostgreSQL** and **MySQL** sessions.
- The feature is **disabled by default**. A new installation analyzes nothing until an administrator enables it.

Important

Only recorded sessions are analyzed. In the *account configuration*, set the session recording option to `all` or `noraw` for SSH and Telnet, and to `all` or `raw` for PostgreSQL and MySQL. With the default `noraw` option, PostgreSQL and MySQL sessions are not analyzed.

How it works

1. Fudo Enterprise produces a running text transcript of the monitored session. For SSH and Telnet it is the terminal activity, for PostgreSQL and MySQL the statements run together with a preview of their results.
2. Every analysis agent selected for the session's safe and enabled for the session's protocol receives the transcript, together with the context described for the safe, the server, the account and the user.
3. Each agent returns findings, each with a severity: `LOW RISK`, `MEDIUM RISK` or `HIGH RISK`. A fragment that could not be analyzed at all is marked `UNKNOWN` - this means the AI provider was unavailable or kept returning errors, so that part of the session was not assessed.
4. Findings are shown in the sessions list and in the session player as they arrive.
5. If a *Live Session Analysis policy* is assigned to the safe, reaching its threshold triggers the configured actions.

A session is analyzed only when **all** of the following hold:

- live session monitoring was enabled at the moment the session started,
- the safe used for the connection has at least one analysis agent selected,
- the agent is enabled for the protocol of the session,
- the agent has a provider assigned and that provider works,
- the account records the session in the format required for its protocol.

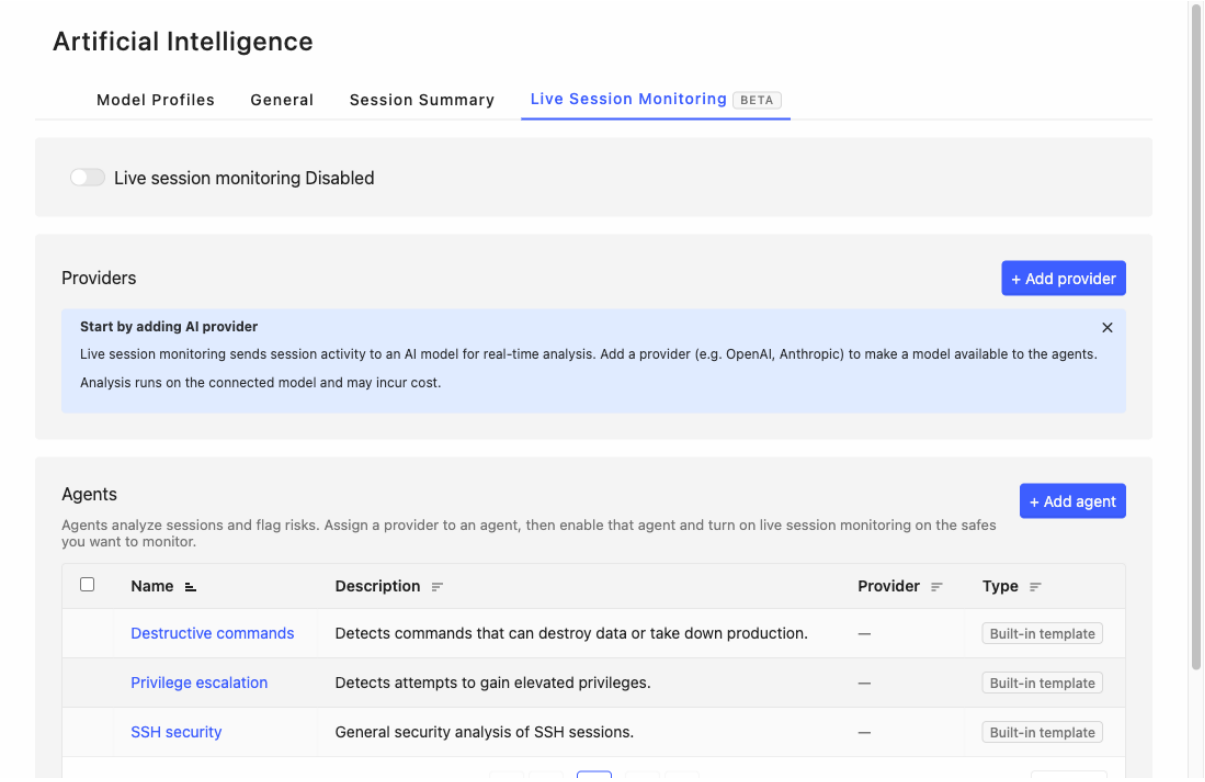
Note

The switch is evaluated when a session starts. Enabling live session monitoring does not pick up sessions that are already running, and disabling it does not interrupt an analysis in progress - such a session is analyzed to its end.

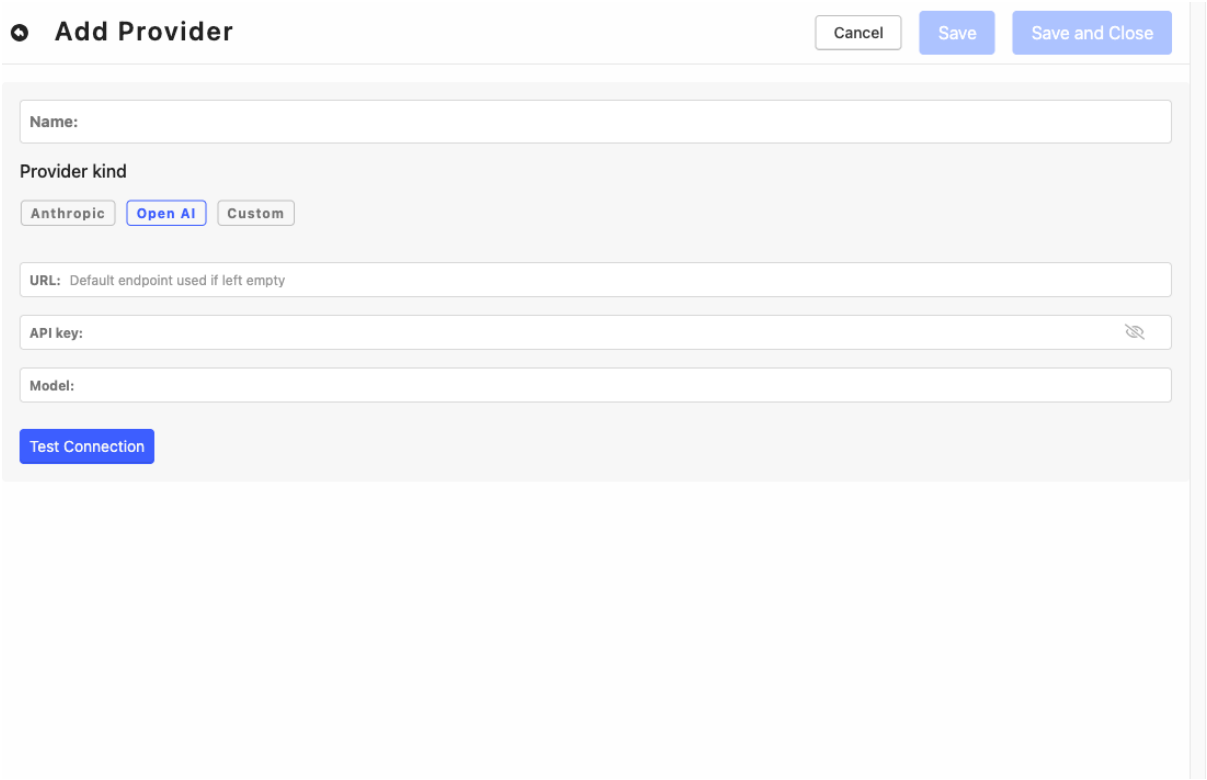
Configuring an AI provider

A provider defines the AI model the agents run on.

1. Select *Settings* > *Artificial Intelligence* > *Live Session Monitoring*.



2. In the *Providers* section, click *Add provider*.
3. Enter the *Name* of the provider.
4. Select the *Provider kind*: *Anthropic*, *Open AI* or *Custom*. Select *Custom* for a self-hosted model.
5. Enter the *URL* of the endpoint. For *Anthropic* and *Open AI* the field may be left empty - the default endpoint of the selected provider kind is then used. **For `Custom` the address is required**, because Fudo Enterprise cannot know which endpoint a self-hosted model exposes.
6. Enter the *API key* used to authenticate against the provider.
7. Enter the *Model* name.



8. Click *Test Connection* to verify the configuration.
9. Click *Save*.

Note

Once saved, the API key is not displayed again. The form shows the message *A key is stored. Enter a new value to replace it.* - enter a new key only when you want to change it.

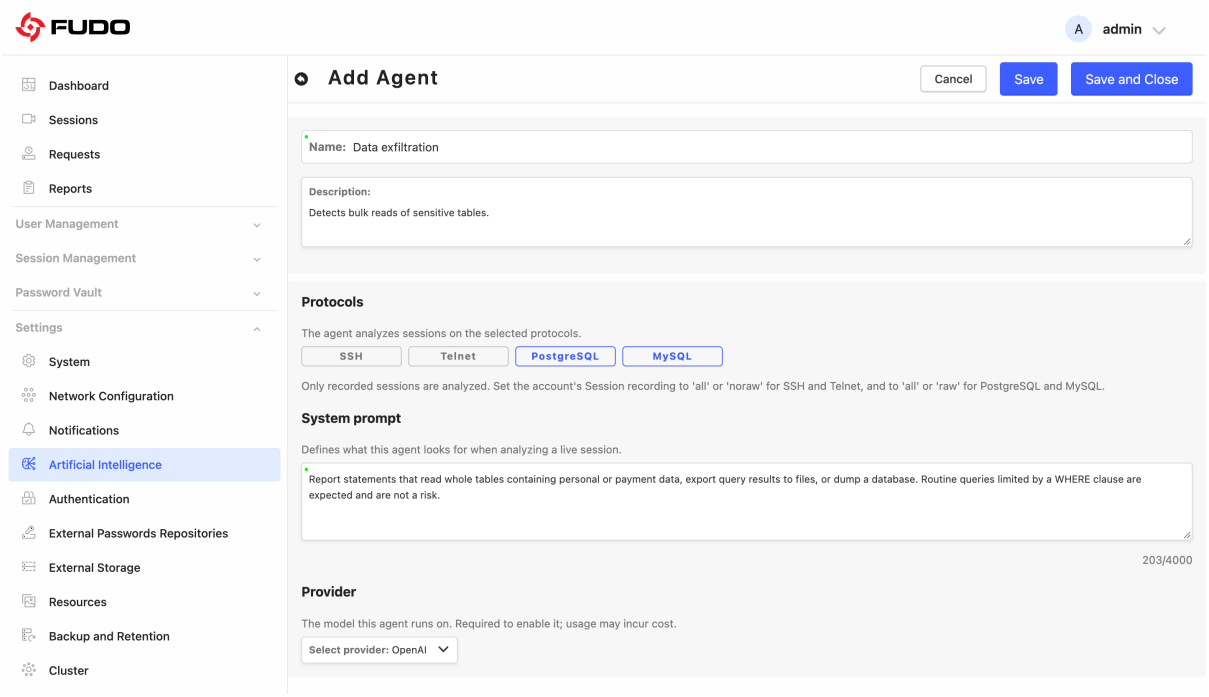
Configuring an analysis agent

An agent is a prompt that defines what to look for in a session, together with the protocols of the sessions it analyzes. Several agents can watch the same session, each with its own remit.

Note

Fudo Enterprise ships three **built-in agents**: *SSH security*, *Privilege escalation* and *Destructive commands*. They analyze SSH sessions. Their name, description, system prompt and protocols cannot be changed, but you can assign a provider to them and select them in safes like any other agent. To adjust a built-in agent, create an editable copy of it.

1. Select *Settings* > *Artificial Intelligence* > *Live Session Monitoring*.
2. In the *Agents* section, click *Add agent*, or click the name of a built-in agent and then click *Copy* to create an editable copy.



3. Enter the *Name* and the *Description* of the agent.
4. In the *Protocols* section, select the protocols of the sessions the agent analyzes: *SSH*, *Telnet*, *PostgreSQL* or *MySQL*. At least one protocol must be selected.
5. In the *System prompt* field, describe what the agent looks for when analyzing a live session. The prompt can be up to 4000 characters long.
6. In the *Provider* section, select the provider the agent runs on.
7. Click *Save*.

Note

- A copy of a built-in agent is created under the name *<agent name> (copy)* and keeps the protocols of the original. Change the name to something meaningful before saving.
- To use a built-in agent without changes, click its name, select the provider in the *Provider* section and click *Save*.

Enabling live session monitoring

Turn the feature on before you select the monitored safes. While live session monitoring is disabled, the *Live Session Monitoring* sections of the safe, server, account and user forms, as well as the *Live Session Analysis* policy type, are hidden.

1. Select *Settings* > *Artificial Intelligence* > *Live Session Monitoring*.
2. Click the *Live session monitoring* switch.
3. Confirm the operation in the *Enable live session monitoring?* window.

Selecting the monitored safes

Sessions are analyzed per safe. An agent watches only the sessions established through the safes it is assigned to.

1. Select *Management* > *Safes* and edit the selected safe by clicking on its name.
2. In the *Live Session Monitoring* section, select the *Enable live session monitoring* option.
3. Select the analysis agents that are to watch sessions in this safe.
4. Click *Save*.

Note

- For a newly created safe the agent list becomes available only after the safe is saved.
- You can also assign an agent to safes in the *Enabled in safes* section of the agent form. The section is available when you edit a saved agent.

Warning

If no agent is selected, sessions in the safe are not analyzed, even when live session monitoring is enabled.

Describing the context

The AI evaluates a session against the context it is given. Without it, routine administrative work is easily reported as a risk. The *AI analysis context* field is available in four places, each under the *Live Session Monitoring* heading:

- on a **safe** - what is normal for connections established through this safe,
- on a **server** - what the server is used for, for example that it is a build machine,
- on an **account** - what the account is normally used for,
- on a **user** - the user's role, for example that the user is an administrator for whom destructive operations are expected.

Note

Describe what is normal rather than what is forbidden. The more accurate the context, the fewer legitimate activities are reported as risks.

Reviewing the findings

Findings are available while the session is running and after it ends.

- The sessions list has an *Analysis* column and a side panel titled *AI live session monitoring*, listing the findings of every agent.
- The session player shows the risk level of the session and marks the moments the findings refer to. Use *Play from this moment* to jump straight to the activity a finding describes. This is also where findings are judged.
- Findings can be filtered by severity and by agent.
- A session with no findings is presented as *NO RISK DETECTED*; a session still being analyzed is presented as *ANALYSIS IN PROGRESS*.

Note

Every report carries the note that it was generated by artificial intelligence and that critical information should be verified independently.

Judging a finding

The AI does not learn from its own findings on its own. It is the operator who decides whether a finding was right, and only findings judged by a person are used to improve later analyses.

Findings are judged in the session player, where each one is marked at the moment of the session it refers to.

1. Select *Sessions* and open the selected session in the player.
2. For the selected finding, click *Risk* to confirm it as a real risk, or *Not a risk* to mark it as a false positive.
3. Optionally click *Add a reason* and describe the decision.

Note

Findings judged by an operator, together with the reasons given for them, are passed to the AI alongside the context described for the safe, the server, the account and the user. They therefore serve as material from which the AI learns what is normal **on that particular server and for that particular user**.

Clicking the same judgment again retracts it together with its reason.

Required privileges

- The `ai-read` privilege is required to manage analysis agents and to select them on a safe. Without it, the safe form informs that the privilege is missing.
- The analysis panel of a session requires the `session-read` privilege. Details of the AI infrastructure - the provider, the model and the token counts - are visible only with the `ai-read` privilege.

Related topics:

- *Live Session Analysis Policy [BETA]*
- *AI Session Summary*
- *AI Behavioral Analysis*
- *Sessions*
- *Safes*

12.5 Authentication

Fudo Enterprise offers a wide range of authentication methods for user verification against the target server. These include:

- External Authentication: *CERB*, *RADIUS*, *TACACS+*, *LDAP*, *Active Directory*

- Other Authentication Methods: *OATH*, *SMS*, *DUO*, *OpenID Connect*, *JWT*, *SSO*, *Kerberos*

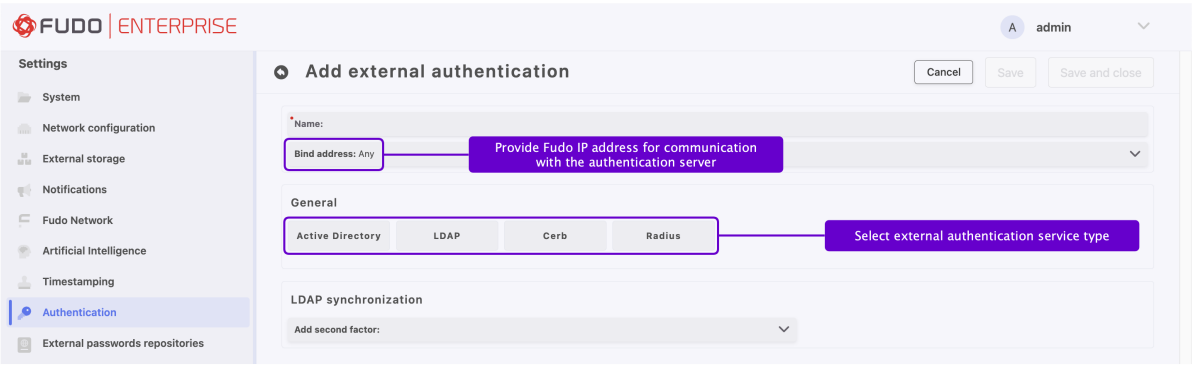
12.5.1 External Authentication Server Definition

To add an external Active Directory, LDAP, Cerb, RADIUS, or TACACS+ authentication server, proceed as follows.

1. Select *Settings* > *Authentication*.
2. Choose **External authentication** tab.
3. Click *+ Add external authentication*.
4. Provide a name for this specific configuration.
5. Select the bind address - IP address used for sending requests to given host.

> **Note**
>
> In case of cluster configuration, select a **labeled IP address** from the *Bind address* dropdown list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

6. In the *General* section, select authentication service type: `Active Directory`, `LDAP`, `CERB`, `RADIUS`, or `TACACS+`.



7. Provide configuration parameters depending on selected external authentication system type. Configuration details are described in the sections below.
8. Click *Save*.

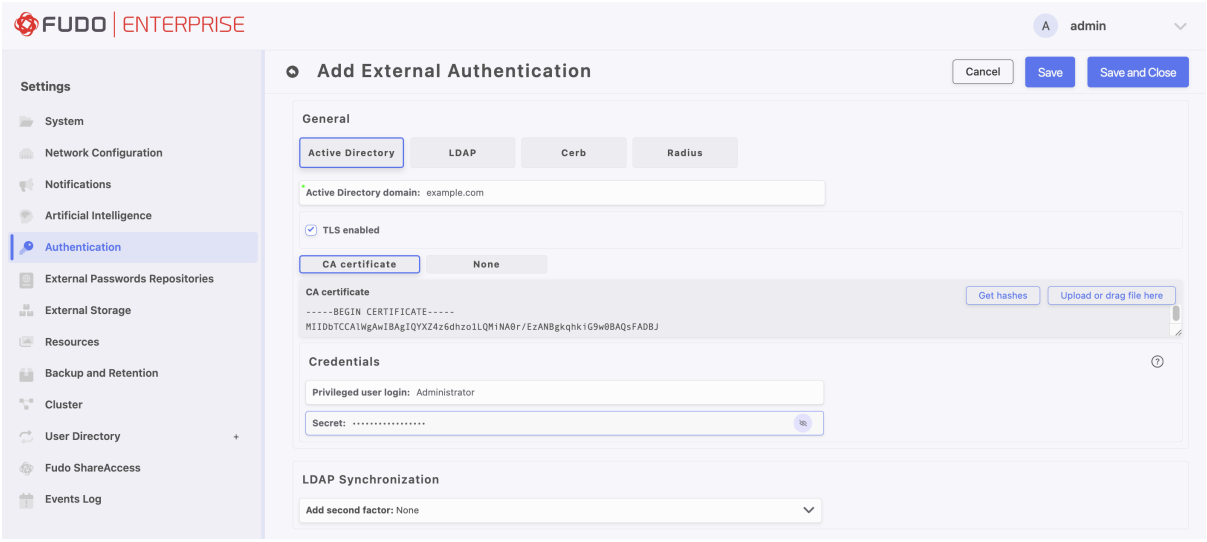
Field Descriptions and Configuration Based on Chosen Method

12.5.1.1 Active Directory

Parameter	Description
Active Directory domain	Domain which will be used for authenticating users in Active Directory.
TLS enabled	This option is required to be checked for the domain users who change their passwords in the User Access Gateway.
CA Certificate	Available when *TLS enabled* option is activated.
Privileged user login	The privileged account's login name to modify a user password on the Active Directory server. The field is located in the *Credentials* subsection.
Secret	Secret used to establish server connection to modify a user password on the Active Directory server. The field is located in the *Credentials* subsection.
Add second factor	Additional verification step with authentication methods `OATH`, `SMS` or `DUO`. Check *Second Authentication Factor* section.

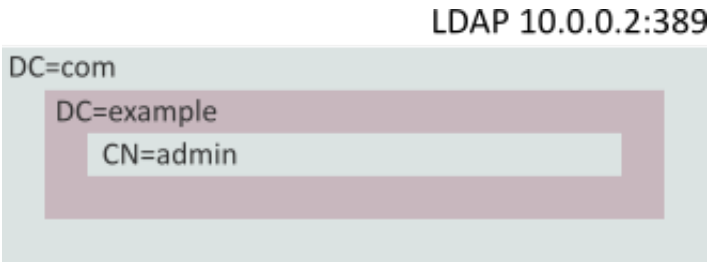
Note

- The **Active Directory** external authentication method uses the Kerberos protocol as the first step.
- This functionality is enabled by default.
- Please refer to *Kerberos Authentication Settings* section to learn how to disable it.
- If **Active Directory** authentication is successfully completed using Kerberos, the configured certificate will not be applied, as it is only utilized when a fallback to LDAP is required.
- To enforce Kerberos-only authentication, you can disable the fallback to LDAP simple bind authentication on the *Kerberos Authentication Settings* page (the *Disable LDAP fallback* option). If Kerberos is then unavailable, **Active Directory** authentication fails.



12.5.1.2 LDAP

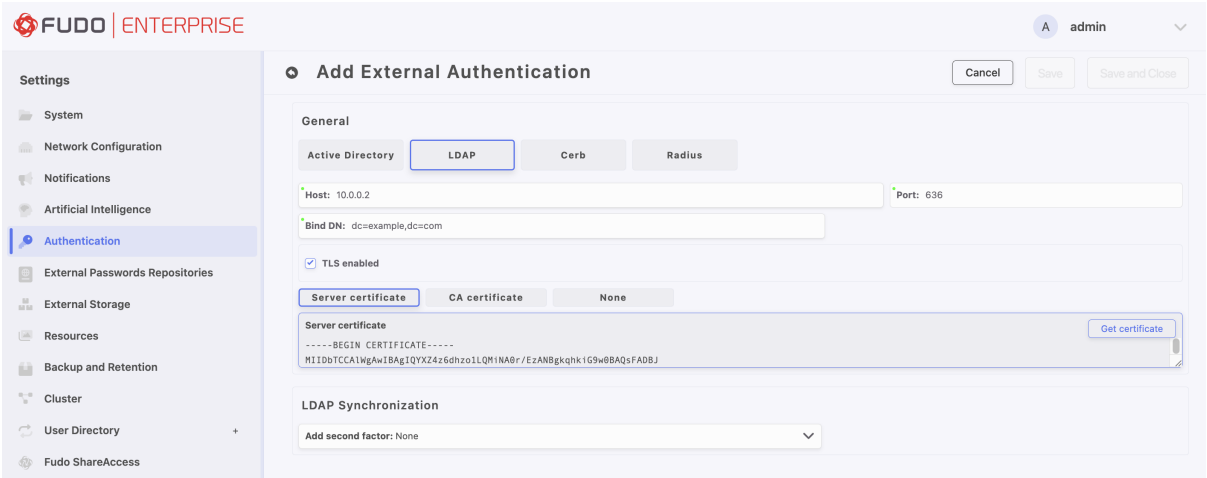
Parameter	Description
Host	Server's host name or IP address.
Port	Port used to establish connections with given server.
Bind DN	Template containing a path which will be used to create queries to LDAP server (for example: `dc=example,dc=com`, `cn=username,dc=example,dc=com`, or, when using variable substitution: `cn=##username##,dc=example,dc=com`).
TLS enabled	This option is required to be checked for the domain users who change their passwords in the User Access Gateway.
Server certificate / CA Certificate	LDAP server certificate or CA certificate. Available when *TLS enabled* option is activated.
Add second factor	Additional verification step with authentication methods `OATH`, `SMS` or `DUO`. Check *Second Authentication Factor* section.



Note

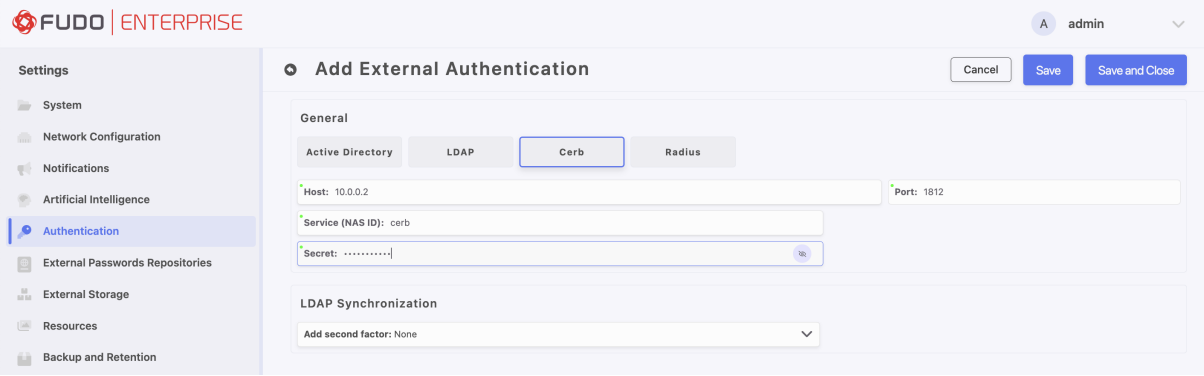
The value of **Bind DN** field may include variable substitution, allowing the DN to be dynamically generated based on the username of the user logging in to the system, for example: `cn=##username##,dc=example,dc=com` In that case, when configuring a user, leave the LDAP Base field empty in **Management** > **Users** > **User Data tab**.

The following description assumes that user's authentication data is stored on LDAP server accessible through `10.0.0.2` IP address and default LDAP service port number - `389`. User definition is stored under `dc=example,dc=com`.



12.5.1.3 Cerb

Parameter	Description
Host	Server's IP address.
Port	Port used to establish connections with given server.
Service (NAS ID)	CERB service used for authenticating Fudo Enterprise users.
Secret	Secret used to establish server connection.
Add second factor	Additional verification step with authentication methods `OATH`, `SMS` or `DUO`. Check *Second Authentication Factor* section.



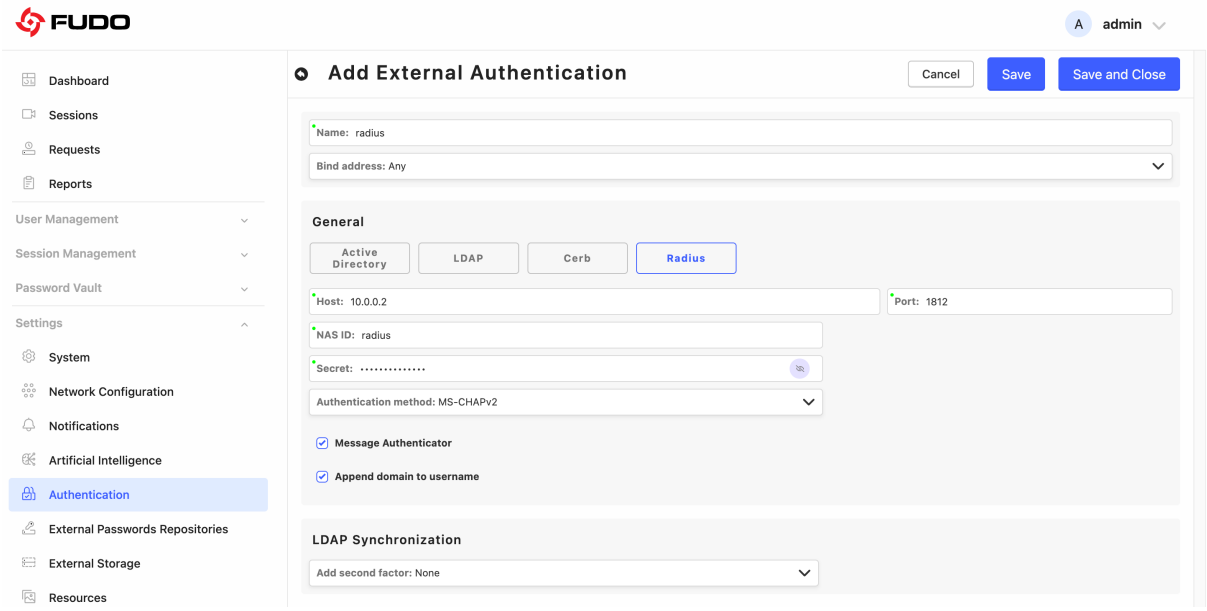
Note

The *AD domain* field from the *user configuration* is included in the initial `Access-Request` packet used to authenticate the user against the **RADIUS/Cerb** server.

- If the *AD domain* is populated:
  - For **RADIUS**, the *AD domain* value is appended to the username in the `User-Name` field, formatted as: `{name}@{ad_domain}`. This behavior is controlled by the *Append domain to username* option described in the *Radius* section. When the option is disabled, the `User-Name` field contains only `{name}`, even if the *AD domain* is populated.
  - For **Cerb**, the `MS-CHAP-Domain` field is set to the value from the *AD domain*, and the `User-Name` field contains only `{name}`. The *Append domain to username* option does not apply to **Cerb**.
- If the *AD domain* is not populated, the `User-Name` field in the `Access-Request` packet for both methods contains only the username: `{name}`.

12.5.1.4 Radius

Parameter	Description
Host	Server's IP address.
Port	Port used to establish connections with given server.
NAS ID	RADIUS server NAS-Identifier parameter.
Secret	Secret used to establish server connection.
Authentication method	Select authentication method *PAP*, *CHAP*, *MS-CHAPv2*
Message Authenticator	Adds the `Message-Authenticator` attribute to the `Access-Request` packet sent to the RADIUS server and requires the server to return it in the `Access-Accept` and `Access-Challenge` responses. When the attribute is missing from the server's response, authentication fails. Leave the option selected unless the RADIUS server does not support the attribute.
Append domain to username	Decides whether the user's *AD domain* is appended to the login sent to the RADIUS server. When the option is selected (default), the `User-Name` field of the `Access-Request` packet contains `{name}@{ad_domain}`. Clear the option if the RADIUS server expects the bare username - the `User-Name` field then contains only `{name}`. The option applies to a single external authentication server definition.
Add second factor	Additional verification step with authentication methods `OATH`, `SMS` or `DUO`. Check *Second Authentication Factor* section.



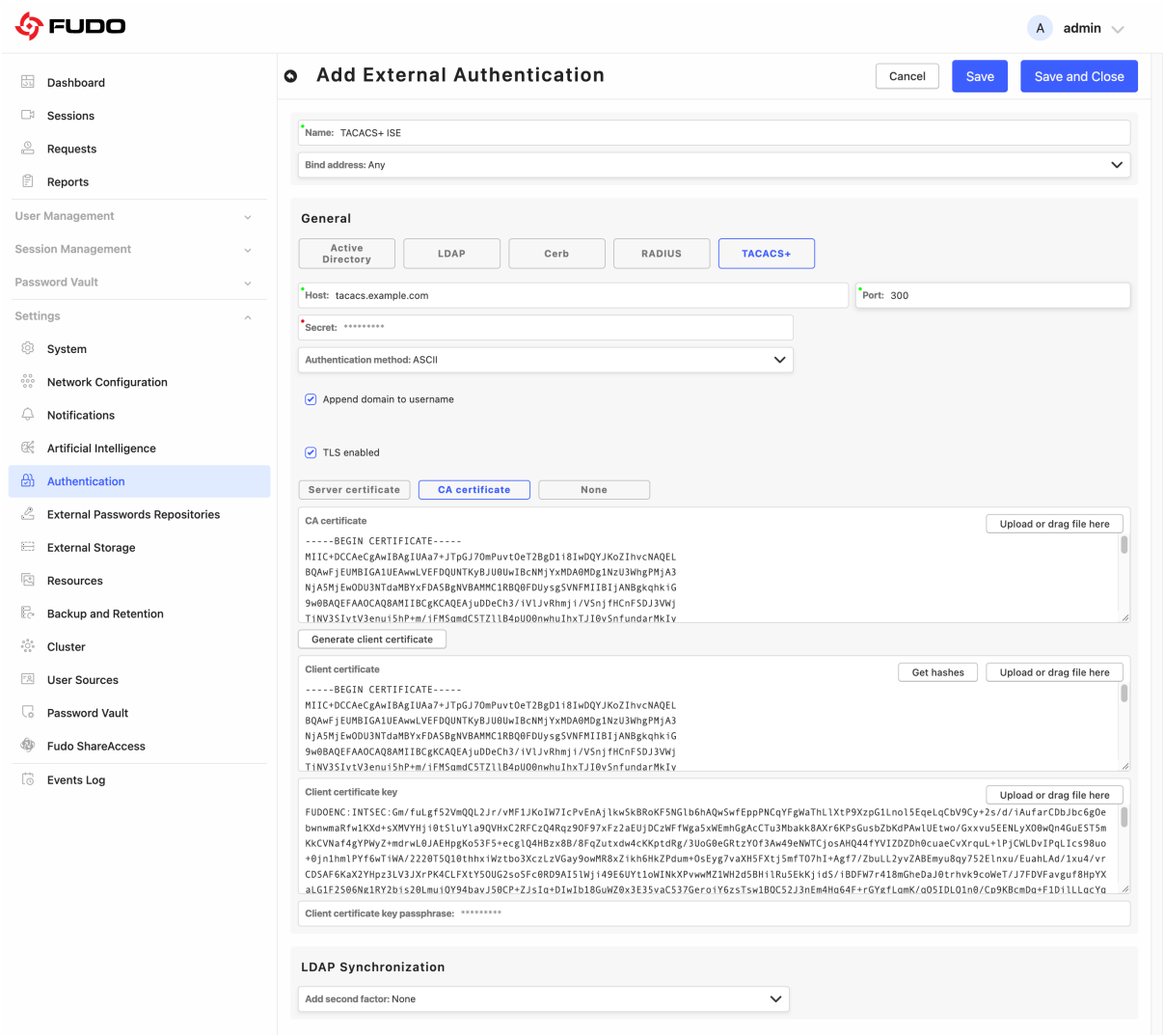
Note

- The **CHAP** authentication method does not work in Windows environments.
- The *Append domain to username* option is selected by default, also for the external authentication server definitions that already existed before the upgrade. The way the username is sent to the RADIUS server does not change until you clear the option.

- Make sure to read the note for the **Cerb** method as well.

12.5.1.5 TACACS+

Parameter	Description
Host	Server's host name or IP address.
Port	Port used to establish connections with the TACACS+ server. Default: `49`, or `300` when *TLS enabled* is selected.
Secret	Shared key defined for Fudo Enterprise on the TACACS+ server. Required when *TLS enabled* is not selected. Over TLS, the key is not used and can be left empty.
Authentication method	Select *ASCII* (default), *PAP*, or *CHAP*.
Append domain to username	Decides whether the user's *AD domain* is appended to the username sent to the TACACS+ server, in the `{name}@{ad_domain}` format. Selected by default. Clear the option if the TACACS+ server expects the bare username.
TLS enabled	Connects to the TACACS+ server over TLS 1.3 (RFC 9887). If the TLS connection fails, Fudo Enterprise does not fall back to an unencrypted connection.
Server certificate / CA certificate / None	Decides how Fudo Enterprise verifies the TACACS+ server: *Server certificate* accepts only the provided certificate, *CA certificate* accepts a certificate issued by the provided CA for the address given in *Host*, *None* does not verify the server. Use *None* for testing only. Available when *TLS enabled* is selected.
Generate client certificate	Generates a self-signed client certificate and its key. Use it when the TACACS+ server trusts this certificate directly. If the server verifies client certificates against a CA, upload a certificate issued by that CA instead. Available when *TLS enabled* is selected.
Client certificate	Certificate that Fudo Enterprise presents to the TACACS+ server. TACACS+ servers usually require it for TLS connections. If the certificate was issued by an intermediate CA, put the client certificate first, followed by the intermediate CA certificates. Available when *TLS enabled* is selected.
Client certificate key	Private key of the client certificate. It must match the client certificate. Available when *TLS enabled* is selected.
Client certificate key passphrase	Passphrase of an encrypted client certificate key. It is used only to decrypt the key and is not stored. Available when *TLS enabled* is selected.
Add second factor	Additional verification step with authentication methods `OATH`, `SMS` or `DUO`. Check *Second Authentication Factor* section.



Note

- Fudo Enterprise uses TACACS+ for user authentication only. TACACS+ authorization and accounting are not used.
- Without TLS, TACACS+ hides the content of the packets but does not protect it against modification. Select *TLS enabled*, or make sure that the connection to the TACACS+ server goes through a trusted network.
- Additional prompts from the TACACS+ server, for example for a token, are supported only with the *ASCII* authentication method. In sessions to servers, they are supported for the SSH, RDP, and VNC protocols.

12.5.1.6 Assigning an External Authentication Method to a User

1. Select *Management* > *Users*.
2. Find and click the user definition for which you want to assign an external authentication method (e.g. `admin`).
3. Go to the **User Data** tab, in the **LDAP Base** field specify the location of this user object in the directory structure (e.g. `cn=admin,dc=example,dc=com`).

Note

Leave the **LDAP Base** field empty if you specified where users are stored in the LDAP server configuration (`cn=##username##,dc=example,dc=com`).

4. To add authentication method, go back to the **Settings** tab and select **External authentication** from the **Add authentication method** drop-down list.
5. Choose method and click *Save*.
6. Click *Save and Close* to save user definition.

12.5.1.7 Second Authentication Factor

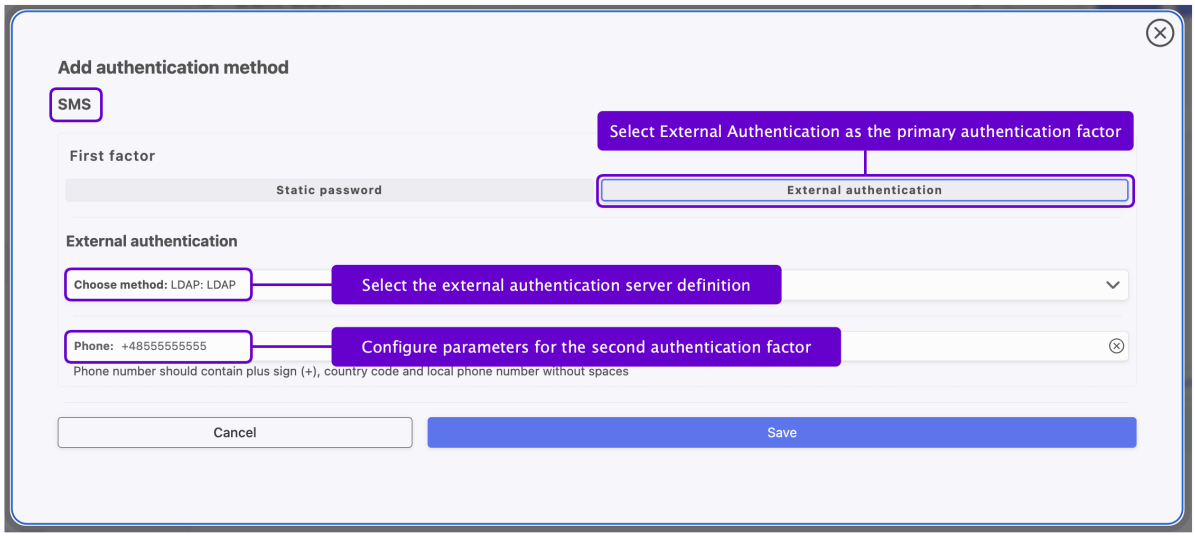
If an additional verification step (the **Add second factor** option) is configured in the external authentication server definition using the OATH, SMS, or DUO authentication methods, the method selected as the second factor must be chosen as the authentication method in the user configuration. Then, in its configuration window, **External Authentication** must be selected as the first authentication factor.

1. Select *Management* > *Users*.
2. Find and click the user definition for which you want to assign an external authentication method (e.g. `admin`).
3. Go to the **User Data** tab, in the **LDAP Base** field specify the location of this user object in the directory structure (e.g. `cn=admin,dc=example,dc=com`).

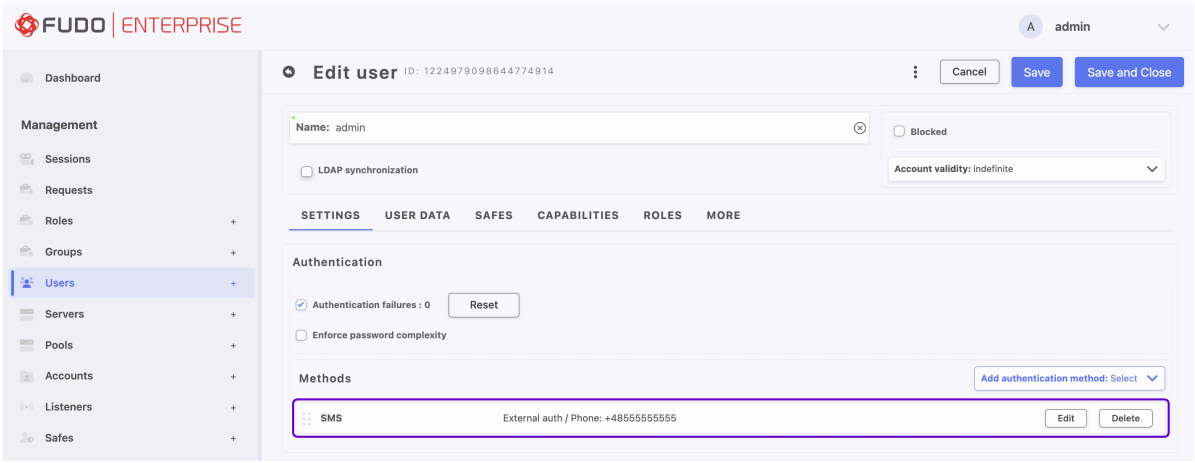
Note

Leave the **LDAP Base** field empty if you specified where users are stored in the LDAP server configuration (`cn=##username##,dc=example,dc=com`).

4. To add external authentication method with second factor, go back to the **Settings** tab and select the name of the method used in the configuration (e.g. SMS) from the **Add authentication method** drop-down list.
5. In the modal window, select **External Authentication** as the first authentication factor.
6. From the **Choose method** list, select the external authentication method configured with a second authentication factor, according to the scenario described above.
7. Configure parameters of the second factor.



8. Click *Save*.
9. Click *Save and Close* to save user definition.



Related topics:

- *User authentication methods and modes*
- *OpenID Connect Authentication Definition with Microsoft Entra (Azure)*
- *System overview*
- *Integration with CERB server*

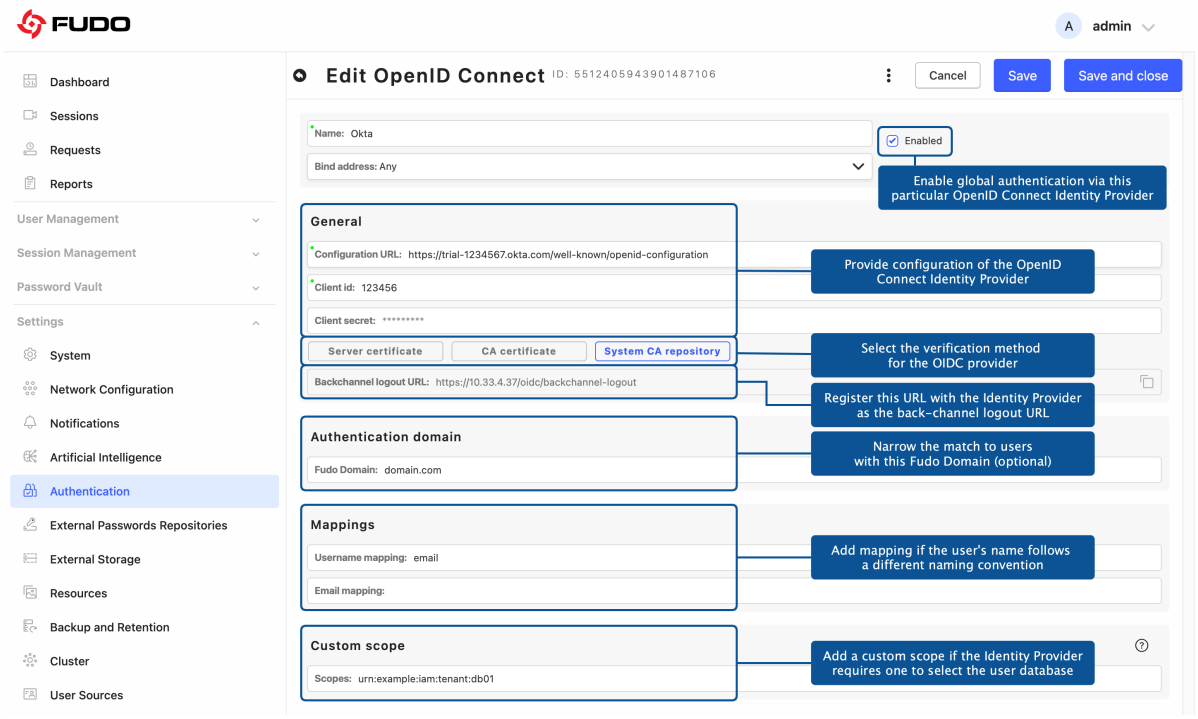
12.5.2 OpenID Connect Authentication Definition

This authentication method is configured globally and is not tied to any particular user. Thus even if a user has no authentication methods configured, they can authenticate using OpenID Connect in Access Gateway and Admin Panel.

Follow the steps to configure the OpenID Connect authentication method:

1. Select *Settings* > *Authentication*.
2. Choose **OpenID Connect** tab.
3. Click *Add OpenID Connect*.

4. Check the *Enabled* option to globally enable OpenID Connect authentication.
5. Provide Name (`Azure`, `Okta` or any other Identity Provider).
6. Provide *Bind address*.



7. In the *General* section, input *Configuration URL*.

Note

This URL is specific for every Identity Provider and allows identifying one for correct configuration. Provide the address of the provider's discovery document, for example `https://accounts.google.com/.well-known/openid-configuration`, or the issuer address alone, for example `https://accounts.google.com` - in that case Fudo Enterprise appends `/.well-known/openid-configuration` on its own.

8. Provide *Client ID*, and *Client secret*. Those values are available after registering with the selected provider.

Note

Please refer to the section *OpenID Connect Authentication Definition with Microsoft Entra (Azure)* for a use case example on configuring OpenID authentication using the Microsoft Entra.

9. Select the verification method for the OIDC provider. Choose:
   - *Server certificate* to upload the provider's certificate,
   - *CA certificate* to specify the signing authority,
   - or *System CA repository* to rely on the default system store.

10. In the *Authentication domain* section, enter the *Fudo Domain* that this OIDC configuration will authenticate against.

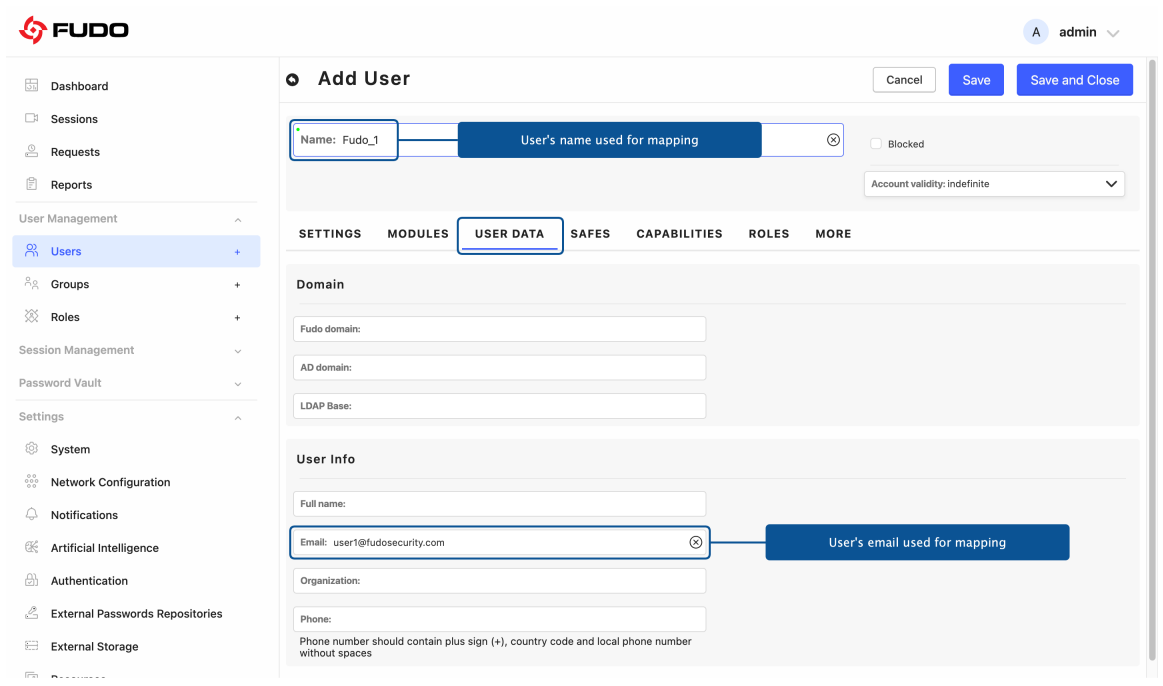
Note

- Use this field if you manage multiple domains or synchronize users from different LDAP/AD sources to avoid conflicts with identical user IDs. The domain is optional.
- The *Fudo Domain* is **not** a part of the user's UPN (User Principal Name). When it is set, only users whose *Fudo domain* matches are taken into account during identification — the value is never appended to the user name to build a UPN. Matching users by their UPN is based on the *AD domain* field of the user account instead.

11. In the *Mappings* field, add *Username mapping* and *Email mapping* in necessary. These fields are useful when the user's name follows a different naming convention.

Note

To ensure proper authentication via Okta external provider, specific mapping configurations are required based on the format of the user's name and the presence of the email address in the User configuration.



1. Username Contains Email Address:

   Scenario: If the *Name* field in the User configuration includes an email address (e.g., `user1@fudosecurity.com`) and the *Email* field in the *User Data* tab is empty.

   Configuration: Set the *Username mapping* to `email`. This ensures that the email address within the username is correctly recognized and used for authentication purposes.

2. Username with Text and Email Field Populated:

Scenario: If the *Name* field in the User configuration contains any text (e.g., `Fudo_1, user1`) and the *Email* field in the *User Data* tab contains the actual email address (e.g., `user1@fudosecurity.com`).

Configuration: Set the *Email mapping* to `email`. This configuration ensures that the email address provided in the Email field is used for authentication, even if the username is a non-email string.

12. In the *Custom scopes* section, provide the *Scopes* required by the Identity Provider (optional).

Note

- Some Identity Providers host several separate user databases behind a single login and select the one to authenticate against based on a custom scope sent in the authorization request. Leave the field empty when the provider does not require it.
- The value is appended to the standard scopes that Fudo Enterprise always sends (`openid`, `profile`, `email`) and is sent only to this provider. A scope defined for one OpenID Connect configuration never affects any other configuration.
- To provide more than one scope, separate them with single spaces. Leading, trailing and repeated spaces are not accepted.
- Example value: `urn:example:iam:tenant:db01`.

13. Click *Save*.

Note

The **algorithm to determine the user's identity** is following:

1. The user is initially identified using the `sub` claim from the OpenID Connect (OIDC) provider.
2. If the user is not identified using the `sub` claim from the OIDC provider, the next step involves checking the autolink setting for the OIDC provider. If this setting is false, the process concludes without finding the user. However, if the autolink setting is true, the search process continues.
3. If *Username mapping* is defined, a search for a corresponding claim in the data is conducted. Once the claim is located in the JSON data, the system then looks for the user with that name.
4. If *Username mapping* is not defined, the claim is not found in the data or the user is not found by name, the next step is to verify if *Email mapping* is defined. If it is defined and exists in JSON data, the process then tries to identify the user based on this email.
5. When neither *Username mapping* nor *Email mapping* is defined, the system will seek to identify the user by their name or email. This is done by searching for the `upn` or `unique_name` claims within the data, in this specified order.
6. If an *Authentication domain* is defined, only users whose *Fudo domain* matches are

considered. When the claim used to identify the user contains `@` (a UPN, for example `jan@domain1.com`), it is matched against the user name combined with the *AD domain* of the user account; a user with no *AD domain* set is never matched this way. Claims without `@` are filtered solely by username and email.

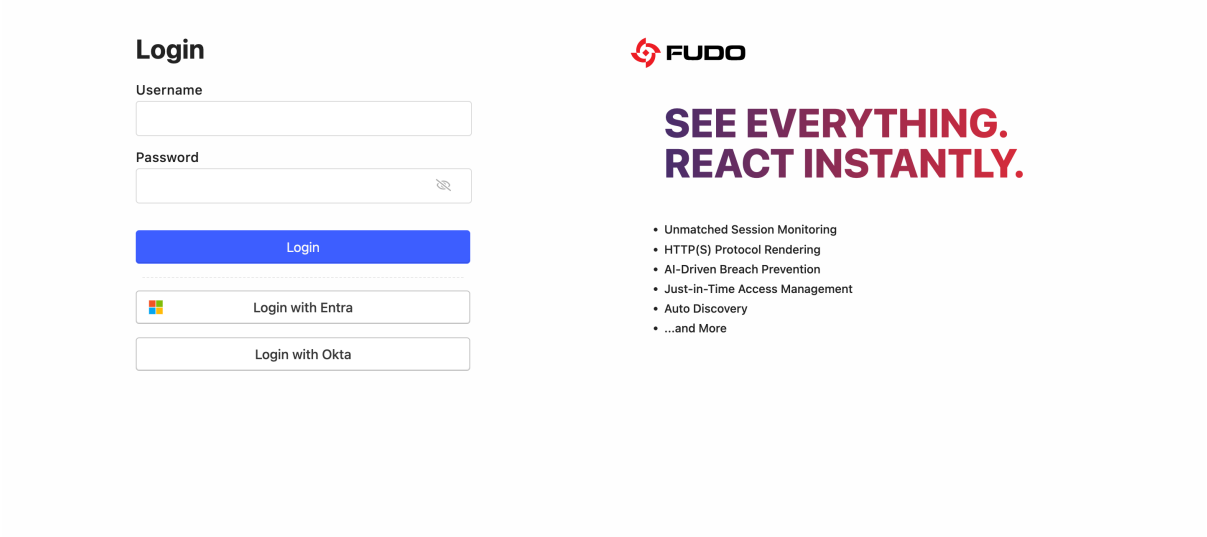
7. When the `email` claim is used for user identification, it is mandatory for the `email_verified` field to be included in the data and set to `true`.
8. The last step checks if the found user has a `sub` claim stored already, but different from the one received from the OIDC provider. If they don't match, it fails.
9. The received user `sub` claim is stored in the database for future use.

Warning

Starting from version 6.2, a claim that contains `@` (a UPN) is matched against the user name combined with the *AD domain* of the user account, and the *Fudo Domain* of the OpenID Connect configuration is no longer treated as the UPN suffix. A user who signs in by name/UPN and has no *AD domain* set — or a value other than the suffix of their UPN — cannot be identified, and their first sign-in fails. Fill in the *AD domain* field of such user accounts with the suffix of their UPN, for example `domain1.com` for `jan@domain1.com`. Refer to the *user specification* to learn how to set this field.

Users who signed in successfully before the upgrade are not affected, because they are identified by the stored `sub` claim. Configurations that identify users by email address are not affected either, as matching by email address does not use domains.

14. Log in using the defined authentication method:



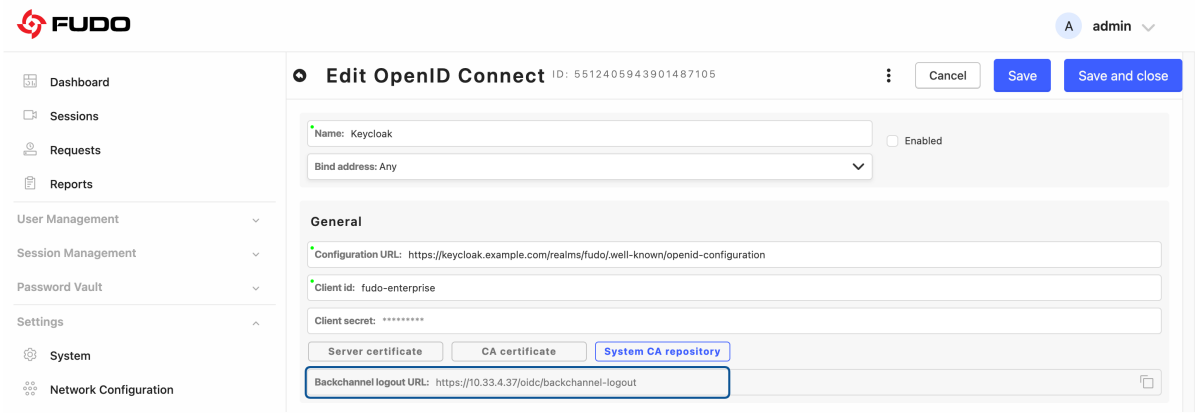
12.5.2.1 Back-Channel Logout

When a user signs out at the Identity Provider, or an administrator ends the user's session there, the provider can notify Fudo Enterprise (OpenID Connect Back-Channel Logout). Fudo Enterprise then ends the matching user sessions in the Admin Panel and in the User Access Gateway, on all cluster nodes that are online.

Important

Back-channel logout is always active. To use it, register the Fudo Enterprise address with the Identity Provider.

1. Select *Settings* > *Authentication*, choose the **OpenID Connect** tab and click the OpenID Connect configuration.
2. In the *General* section, copy the **Backchannel logout URL** value. The field is available after the configuration is saved.
3. In the client configuration on the Identity Provider:
   - set the copied URL as the back-channel logout URL,
   - require the session ID (`sid`) in the logout token,
   - turn off front-channel logout.



Note

- The URL is `https://<Admin Panel address>/oidc/backchannel-logout`. It is the same for all OpenID Connect configurations and also covers sessions in the User Access Gateway. The field shows the address that you used to open the Admin Panel - make sure that the Identity Provider can reach it.
- If the notification identifies a single session at the Identity Provider, only that session ends. If it identifies only the user, all the user's sessions in the Admin Panel and in the User Access Gateway end.
- The user is signed out at their next action in the Admin Panel or in the User Access Gateway.
- Back-channel logout does not end active sessions to servers (SSH, RDP, and other protocols). Signing out of Fudo Enterprise does not sign the user out at the Identity

Provider.

- A cluster node that is offline when the notification arrives does not receive it later. Sessions on that node remain valid until they expire.
- The notification is rejected if two enabled OpenID Connect configurations use the same Identity Provider and the same *Client ID*.
- The logout token must contain the `exp` claim and must not be older than five minutes.

Related topics:

- *User authentication methods and modes*
- *OpenID Connect Authentication Definition with Microsoft Entra (Azure)*
- *System overview*
- *Integration with CERB server*

12.5.3 JWT Authentication Definition

A *JWT provider* lets an upstream token issuer authenticate a Fudo Enterprise user on the request's behalf. When a request carries a signed *JWT* in a configured HTTP header, Fudo Enterprise verifies the token signature against the public keys published by the issuer, checks the standard claims, and maps a claim from the token to an existing user account. The user is not asked for a password and no Fudo Enterprise session is established beforehand — the token is the credential presented with every request.

Warning

The user name carried by the token is mapped directly to a Fudo Enterprise user account, and Fudo Enterprise relies on the issuer to assert that name. Unlike the interactive *OpenID Connect* login, the account is not bound to the provider that authenticated it. Configure a *JWT provider* only for an issuer that your organization controls.

Note

The user account has to exist in Fudo Enterprise before the first request that carries a token. The account is not created automatically — it is usually synchronized from an Active Directory or LDAP service. Refer to the *Users Synchronization - User Directory* section to learn more.

Follow the steps to configure the JWT authentication method:

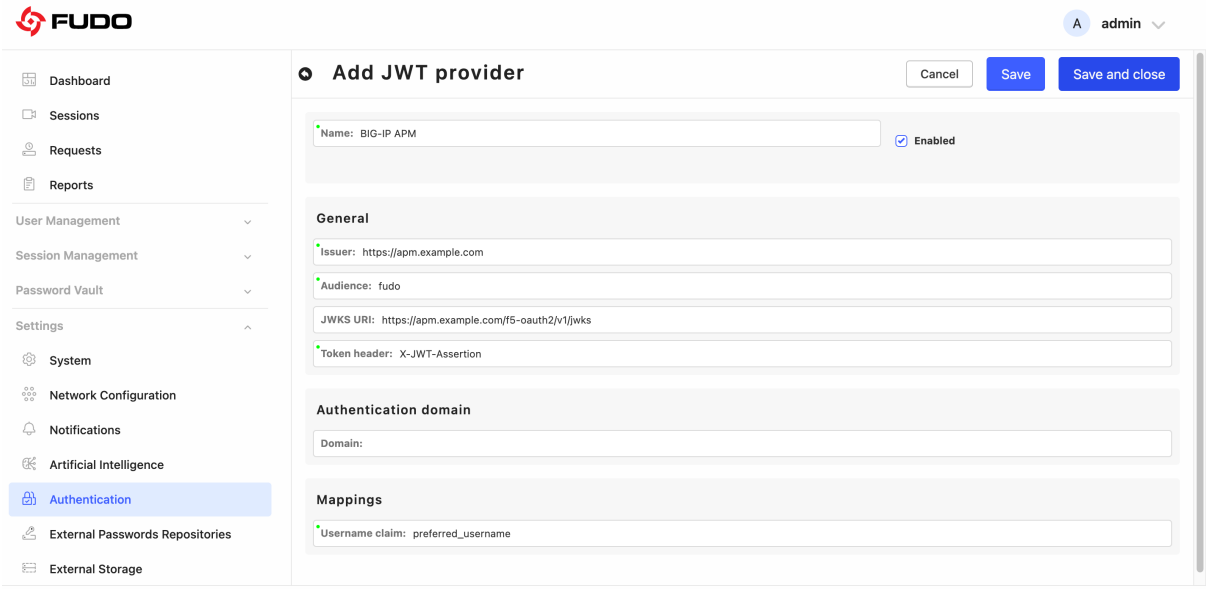
1. Select *Settings* > *Authentication*.
2. Open the *JWT Providers* tab and click *Add JWT provider*.
3. Check the *Enabled* option to activate this provider.
4. Provide *Name*.
5. In the *General* section, input *Issuer* — the exact value of the `iss` claim that tokens from this issuer carry.

6. Provide *Audience* — the exact value of the `aud` claim.
7. Optionally, provide *JWKS URI* — the address of the issuer's *JWKS* document.
8. Provide *Token header* — the name of the HTTP header that carries the token.
9. In the *Authentication domain* section, enter the *Domain* that this provider will authenticate against.
10. In the *Mappings* section, provide *Username claim* — the token claim that carries the user name.
11. Click *Save*.

Note

The values required by the configuration come from the token issuer:

- *Issuer* and *JWKS URI* can be read from the issuer's OpenID configuration document, available at `<issuer address>/.well-known/openid-configuration` - they correspond to its `issuer` and `jwks_uri` fields.
- *Audience* is decided on the issuer's side, when the issuing of tokens for Fudo Enterprise is configured there. It is usually the identifier of the application registered for Fudo Enterprise. The same value has to be entered in this field.
- *Token header* follows from the WAF configuration - it is the header into which the WAF injects the token.
- *Username claim* depends on which claim the issuer fills with the user name.



Note

- *Issuer* must start with `https://` and must be unique among providers. Fudo Enterprise uses it to decide which provider a token belongs to, so it has to match the `iss` claim exactly.

- *Audience* is mandatory. A token whose `aud` claim does not match, or which carries no `aud` claim at all, is rejected. This prevents a token issued for another service by the same issuer from being accepted.
- Leave *JWKS URI* empty to have Fudo Enterprise discover the key set from the issuer's OpenID configuration, at `<issuer>/.well-known/openid-configuration`. When set, the address must start with `https://`.
- *Token header* is `Authorization` by default. Set a custom header, for example `X-JWT-Assertion`, when the token is injected by a *WAF*. A token is accepted only from the header configured on an enabled provider, and the `Bearer` prefix is optional.
- *Domain* narrows the search for the user account to the users of that domain. The field is optional.
- *Username claim* is `sub` by default. Provide a different claim when the issuer does not carry the user name there — with Microsoft Entra ID, for example, `sub` holds an opaque identifier, so use `preferred_username` or `upn` instead.

Editing a JWT Provider

To edit a *JWT provider* definition, proceed as follows.

1. Select *Settings* > *Authentication*.
2. Open the *JWT Providers* tab and click the name of the provider you want to edit.
3. Modify the definition as needed.
4. Click *Save*.

Note

Changing *Issuer*, *JWKS URI* or *Token header*, as well as enabling a provider, makes Fudo Enterprise fetch the signing keys of that provider again.

Deleting a JWT Provider

To delete a *JWT provider* definition, proceed as follows.

1. Select *Settings* > *Authentication*.
2. Open the *JWT Providers* tab.
3. Select the providers you want to delete and click *Delete*.

Note

Requests carrying a token issued by a deleted provider are no longer accepted.

Signing Keys

Fudo Enterprise fetches the public keys used to verify token signatures on its own, over HTTPS, either from the address given in *JWKS URI* or through the issuer's OpenID configuration. Keys are never uploaded to Fudo Enterprise.

The keys are refreshed automatically, once an hour, so a key rotated at the issuer is picked up without any action in the Admin Panel.

The *JWT Providers* list shows the number of keys currently held for each provider. To fetch them again immediately, click *Refresh keys* above the list. The keys of every configured provider are fetched, not only of the one selected on the list.

Warning

Every node of a cluster fetches the signing keys on its own, and the fetched keys are not transferred between nodes. The *JWKS URI* address, or the issuer's OpenID configuration, has to be reachable from **every** node of the cluster.

Requirements for the Token Issuer

Fudo Enterprise does not issue the tokens it accepts, so the following has to be set up on the side of the issuer.

Note

- The signature algorithm must be `RS256`, `RS384`, `RS512`, `ES256`, `ES384`, `ES512` or `EdDSA`. Tokens signed with a shared secret (`HS256` and similar) and unsigned tokens are rejected, because Fudo Enterprise verifies the signature with a public key that it fetched from the issuer.
- Encrypted tokens are not supported. Fudo Enterprise accepts a signed token in the compact serialization form, that is `header.payload.signature`, so when the identity provider issues an encrypted token, the *WAF* has to pass on its signed form.
- The `exp` claim is required, and the claim configured as *Username claim* has to be present. The `nbf` claim is optional. A difference of up to 30 seconds between the clock of Fudo Enterprise and the clock of the issuer is tolerated for `exp` and `nbf`.
- When the issuer publishes more than one key, it is worth setting the `kid` header, as Fudo Enterprise then selects the key by its identifier. This matters while an issuer rotates its keys and publishes the old and the new one at the same time.
- A token must not exceed 8192 bytes. Adding many claims, for example a long list of groups, can cross that limit.

Logging In

When a request to the Admin Panel or to the Access Gateway carries a valid token, the login screen is skipped and the requested page opens right away.

Note

- The authentication methods configured on the user account, such as a password, *OATH* or *DUO*, are not used on this path. The assurance of the sign-in is entirely the one provided by the issuer, so multi-factor authentication has to be enforced by the issuer and not by Fudo Enterprise.
- The user name carried by the token is matched against user accounts regardless of letter

case.

Related topics:

- *User authentication methods and modes*
- *OpenID Connect Authentication Definition*
- *Synchronizing users with AD/LDAP*
- *Events Log*

12.5.4 Location Policies

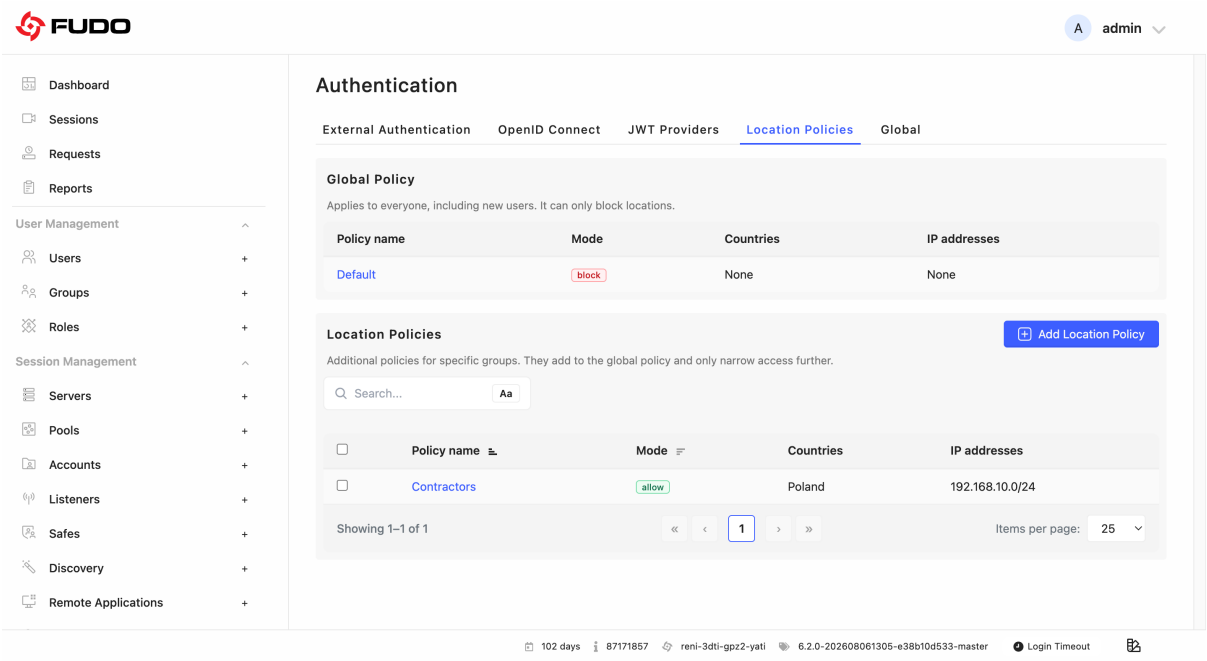
Location policies restrict **where** a user is allowed to authenticate from. A location is expressed as a country, recognised from the source IP address using the built-in GeoIP database, or as an IP address range given in CIDR notation.

Fudo Enterprise distinguishes two kinds of policies:

- the **global policy**, which applies to every user and can only **block** locations,
- **additional policies**, which are assigned to user groups and narrow access down further.

Note

Both kinds are empty after installation and after an upgrade, so no location is restricted until you add the first entry.



12.5.4.1 How Policies Are Combined

A user is never governed by a single policy. Their **effective policy set** consists of the global policy plus the policies of every group the user belongs to. Fudo Enterprise evaluates that whole set on each attempt, in the following order:

1. IP address entries are checked first.
2. Country entries are checked next.

Important

Blocking always wins. If any policy in the effective set blocks the location, access is denied - even when another policy explicitly allows it. An *Allow connections* policy therefore cannot re-open a location that the global policy or another group policy blocks.

This is also why the global policy has no *Allow* mode: it is the baseline that everyone shares, and it can only take access away.

Note

A policy with the *Allow connections* mode restricts the users of its groups to the locations listed in it. A policy with the *Block connections* mode leaves every other location available.

12.5.4.2 Configuring the Global Policy

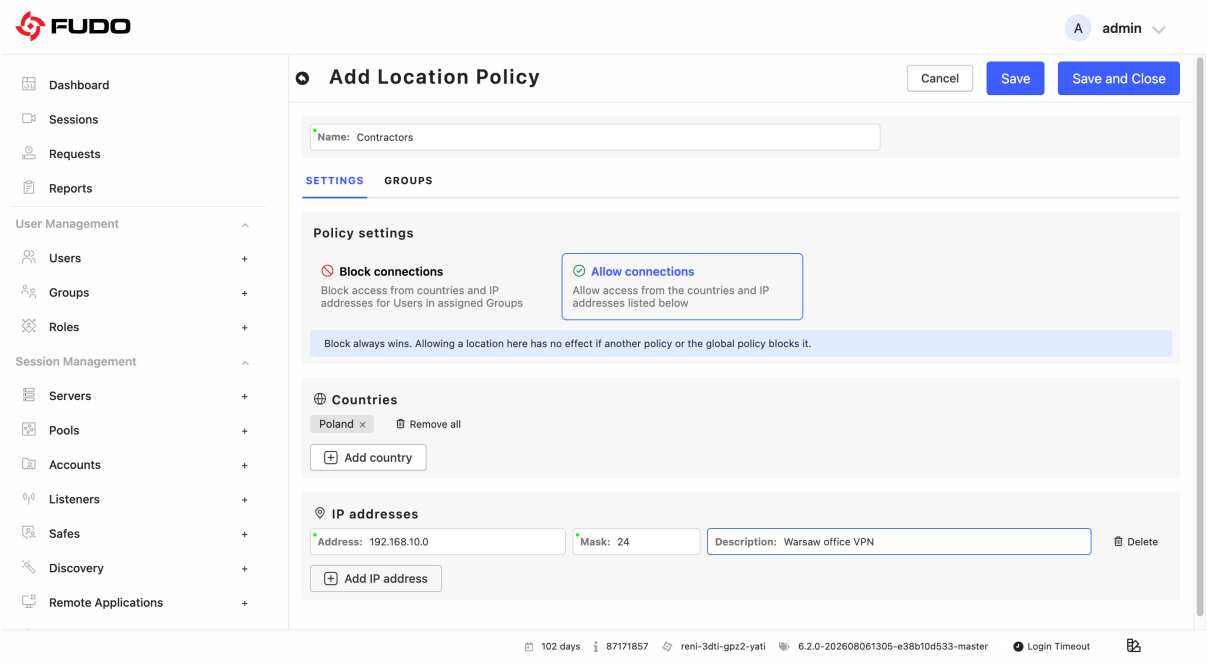
The global policy is a built-in policy named *Default*. It cannot be renamed, deleted or assigned to a group - only its entries can be edited.

1. Select *Settings* > *Authentication*.
2. Go to the *Location Policies* tab.
3. In the *Global Policy* section, click the *Default* policy.
4. Under *Block connections from:*, add the locations to be blocked for everyone:
   - click *Add country* and select the countries,
   - click *Add IP address* and provide the *Address* and *Mask*, optionally with a *Description*.
5. Click *Save*.

12.5.4.3 Adding a Location Policy for a Group

1. Select *Settings* > *Authentication*.
2. Go to the *Location Policies* tab.
3. In the *Location Policies* section, click *Add Location Policy*.
4. Enter the policy *Name*.
5. On the *Settings* tab, choose the mode:
   - *Block connections* - block access from the listed locations,
   - *Allow connections* - allow access only from the listed locations.
6. Add the locations in the *Countries* and *IP addresses* sections.
7. Click *Save*.

8. Go to the *Groups* tab, click *Manage groups*, select the groups in *Available Groups* and move them to *Assigned* with the arrow button.

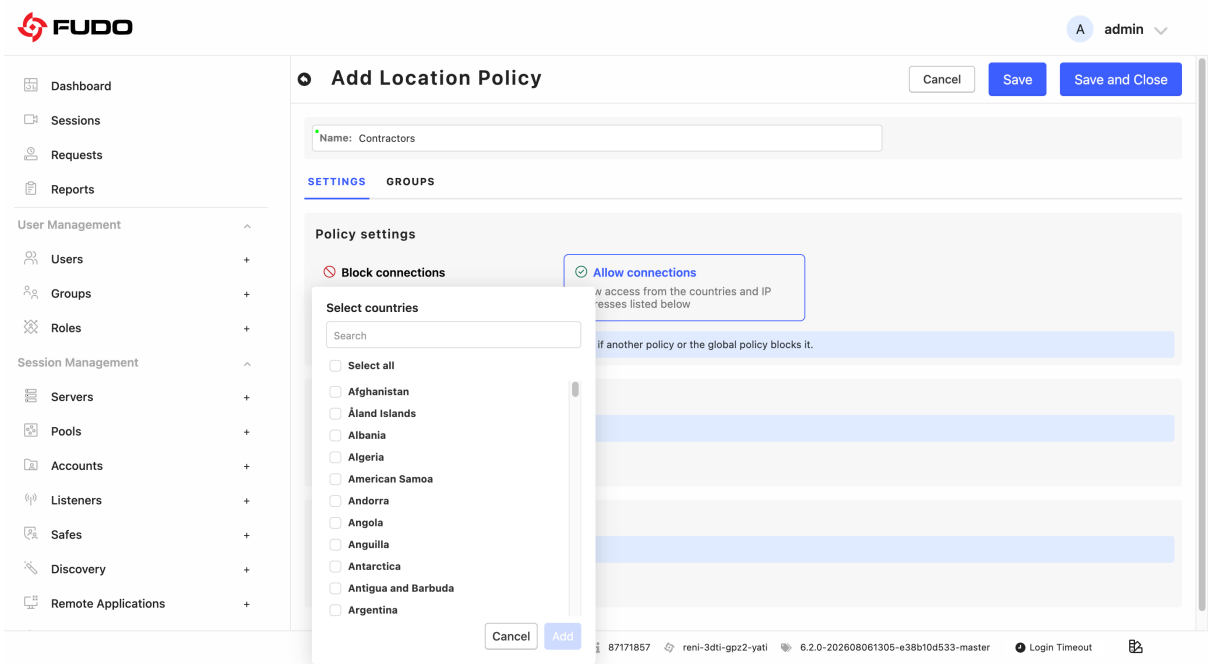


Note

A policy takes effect only once it is assigned to at least one group. When you create a policy, save it first - the *Groups* tab becomes available afterwards.

Selecting countries

The country list comes from the GeoIP database. Use the search field to narrow it down, or *Select all* to take every country at once, then confirm with *Add*. Selected countries are shown as removable chips.



Providing IP address ranges

An IP entry consists of the *Address*, the *Mask* given as a prefix length, and an optional *Description*. The address must be the network address of the range. If it contains host bits - for example `192.168.10.7/24` - Fudo Enterprise reports it and offers the correct network address (`192.168.10.0/24`) to apply with one click.

12.5.4.4 Where Policies Are Enforced

The effective policy set is evaluated at every authentication and on every API request:

- when a user authenticates to establish a session, including the User Access Gateway web client, one-time password logins and tunnels,
- on every request to the Fudo Enterprise API - so a session token acquired from an allowed location and then reused from a blocked one is rejected,
- on SCIM requests used for user provisioning.

Important

Existing sessions are not affected. The location is verified when access is granted, not repeatedly during a session, so changing a policy does not terminate sessions that are already running. The same applies to taking a password out of the password vault.

Note

Requests that carry no source IP address - such as those from the Fudo Officer application - are not subject to location policies.

12.5.4.5 When the Location Cannot Be Determined

If the GeoIP database is unavailable or the source address cannot be resolved to a country, Fudo Enterprise **grants access** and records the event in the events log. This prevents a GeoIP problem from locking every user out.

> **Note**
>
> Private and link-local addresses have no country in the GeoIP database. Users connecting from the local network are therefore matched by IP address entries, not by country entries.

If the country list cannot be loaded while you are editing a policy, the Admin Panel displays a warning and falls back to country codes instead of names. IP address entries remain fully editable.

12.5.4.6 Sessions Established Through a Reverse Proxy

Sessions established through a *Reverse Proxy* are recorded with the source address `127.0.9.1`, not with the address of the client. The tunnel ends inside Fudo Enterprise, so the client's address is not known. Location policies therefore evaluate every such session as coming from `127.0.9.1`:

- An *Allow connections* policy that contains only IP address entries refuses these sessions unless `127.0.9.1` (or `127.0.0.0/8`) is added to it.
- When `127.0.9.1` is added, the policy admits every Reverse Proxy session of the user, regardless of where the client is.
- A policy that also contains country entries admits these sessions even without `127.0.9.1`, because a loopback address has no country.

> **Note**
>
> If you use location policies in **Allow connections** mode, add `127.0.9.1` to them to allow sessions through a Reverse Proxy.

> **Warning**
>
> Location policies cannot restrict sessions established through a Reverse Proxy by the client's location. Do not rely on them for this purpose.

12.5.4.7 Protection Against Locking Yourself Out

Fudo Enterprise verifies every change against the location you are currently connecting from. If saving would deny you access - by adding or editing an entry, switching the mode, assigning a policy to a group, or adding yourself to a group covered by a policy - the change is discarded and an error is displayed.

> **Note**

The check covers only your current location. A policy that leaves your present address allowed can still block you later, from another network - review the effective set before you change your workplace.

12.5.4.8 Required Privileges

Location policies use the same privileges as the rest of the authentication configuration: `authentication-read` to view them and `authentication-modify` to change them. Refer to *Role-Based Access Control (RBAC)* for details on assigning privileges to roles.

Related topics:

- *Authentication*
- *Groups (RBAC)*
- *Role-Based Access Control (RBAC)*
- *Events Log*

12.5.5 Global Authentication Settings

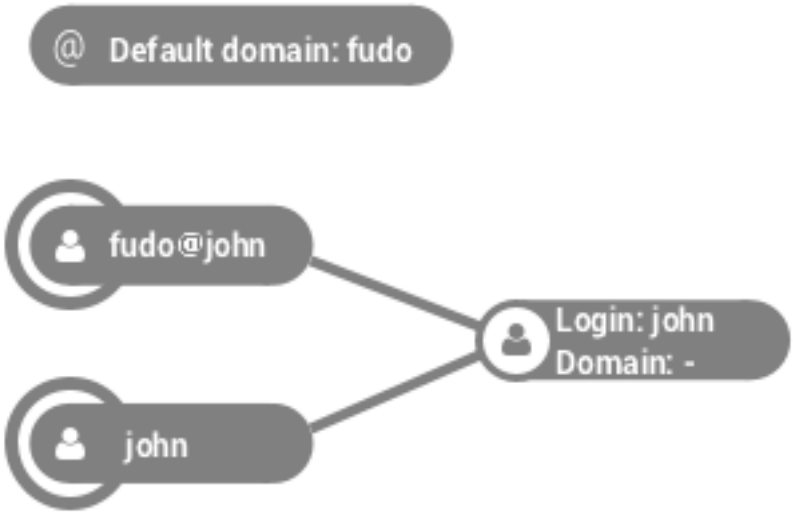
In the *Global* tab, you can configure the default domain, password complexity, the authentication methods that User Access Gateway users are allowed to manage on their own, and a range of authentication methods, including OATH, SMS, DUO, SSO, Kerberos, and FIDO2.

12.5.5.1 Default Domain

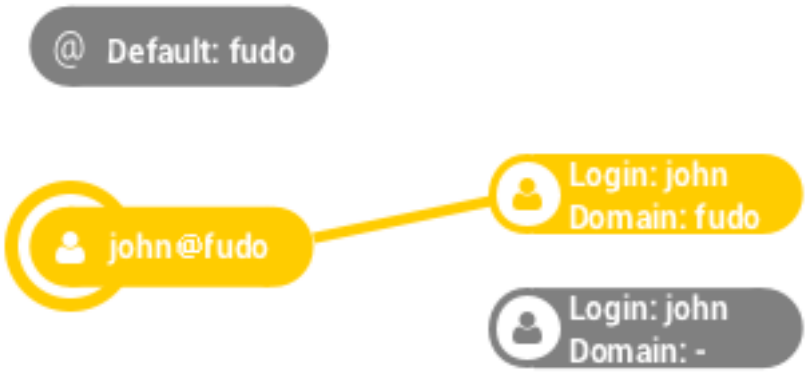
Note

Please remember that the functionality of the *Default Domain* option is closely related to the *Fudo Domain* settings in the *user specification*.

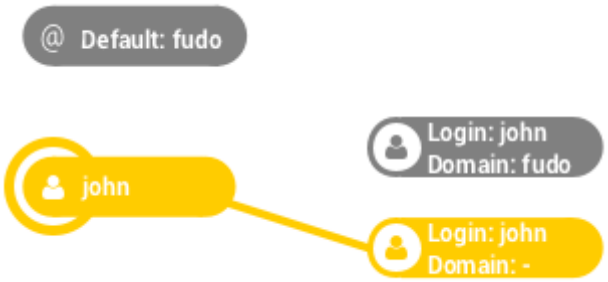
- In case the default domain is specified and the user does not have a *Fudo domain* defined, when logging in to Fudo Enterprise, the user can either include the domain (e.g. `john@domain`) or leave it out (e.g. `john`).



- If there are two users with the same login, one of which has the *Fudo domain* configured the same as the default domain, and the other does not have the *Fudo domain* defined, then:
  - If the user provides the domain during login, Fudo Enterprise will match the user that has the domain explicitly specified.



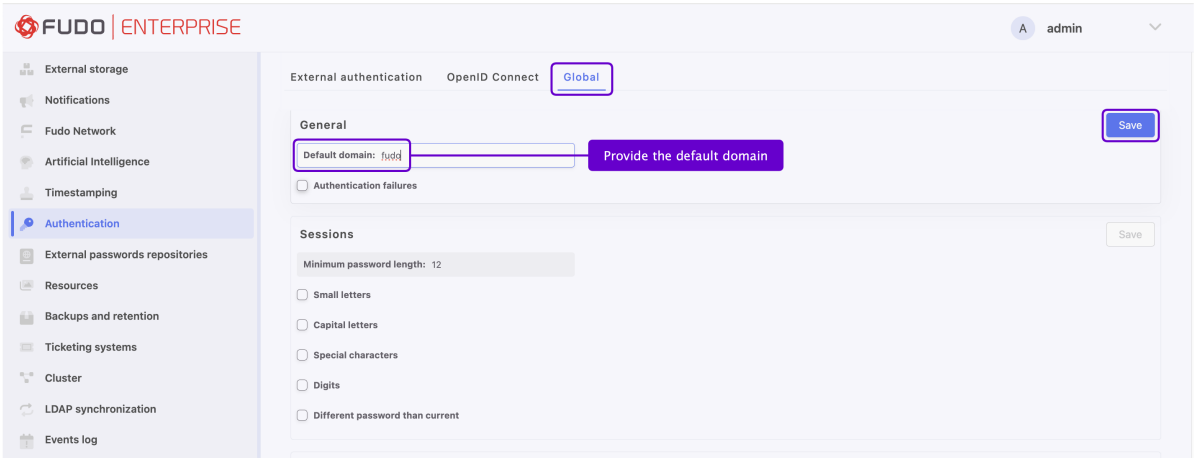
  - In case the user does not provide the domain during login, Fudo Enterprise will match the user that does not have the domain explicitly specified.



  - If the user, which has the *Fudo domain* configured the same as the default domain, will try to login without providing the domain, Fudo Enterprise will report authentication error.

Defining default domain

1. Select *Settings* > *Authentication*.
2. Go to *Global* tab, and provide the default domain in the *General* section.
3. Click *Save* next to the *General* section name.



Related topics:

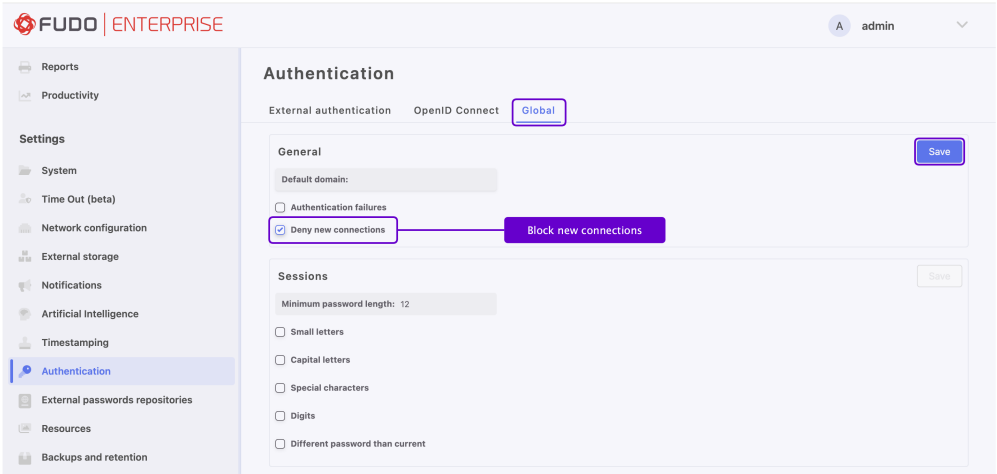
- *Creating a User*
- *Users Synchronization - User Directory*

12.5.5.2 Deny New Connections

Enabling this option results in a denial of all new connections requests.

Blocking new connections

1. Select *Settings* > *Authentication*.
2. Go to *Global* tab, and select *Deny new connections* option in the *General* section.
3. Click *Save* next to the *General* section name.



Related topics:

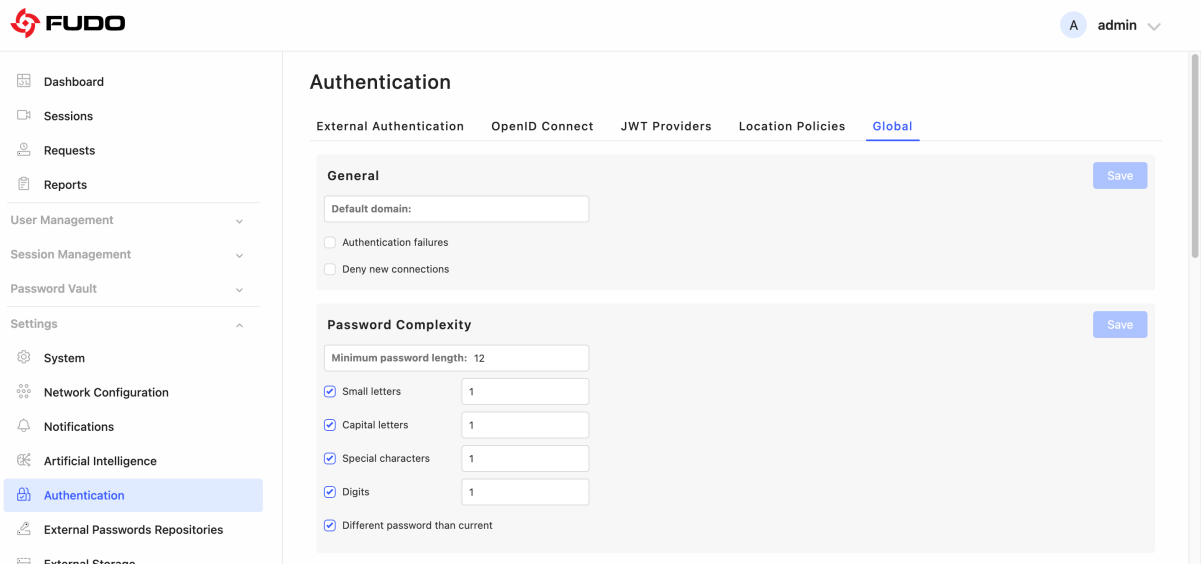
- *Network Interfaces Configuration*

12.5.5.3 Password Complexity

Fudo Enterprise enables the definition of static password complexity, allowing you to enforce passwords that meet your internal regulations.

Defining password complexity

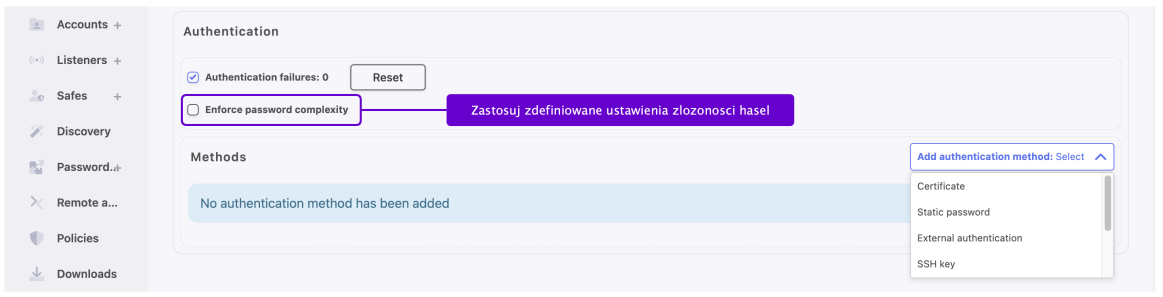
1. Select *Settings* > *Authentication*.
2. Go to *Global* tab, and select *Authentication failures* to set a counter of the login failures.
3. Go to the *Password Complexity* section and define password complexity rules:
   - Define the minimum number of characters.
   - Select *Small letters* and provide the minimal number of small letters in the password.
   - Select *Capital letters* and provide the minimal number of capital letters in the password.
   - Select *Special characters* and provide the minimal number of special characters in the password.
   - Select *Digits* and provide the minimal number of digits in the password.
   - Select the *Different password than current* option to enforce a password different from the current one.



4. Click *Save*.

Note

To enable static password complexity for a particular user, go to *User Management* > *Users*, edit desired user and select the *Enforce password complexity* option in the *Authentication* section.

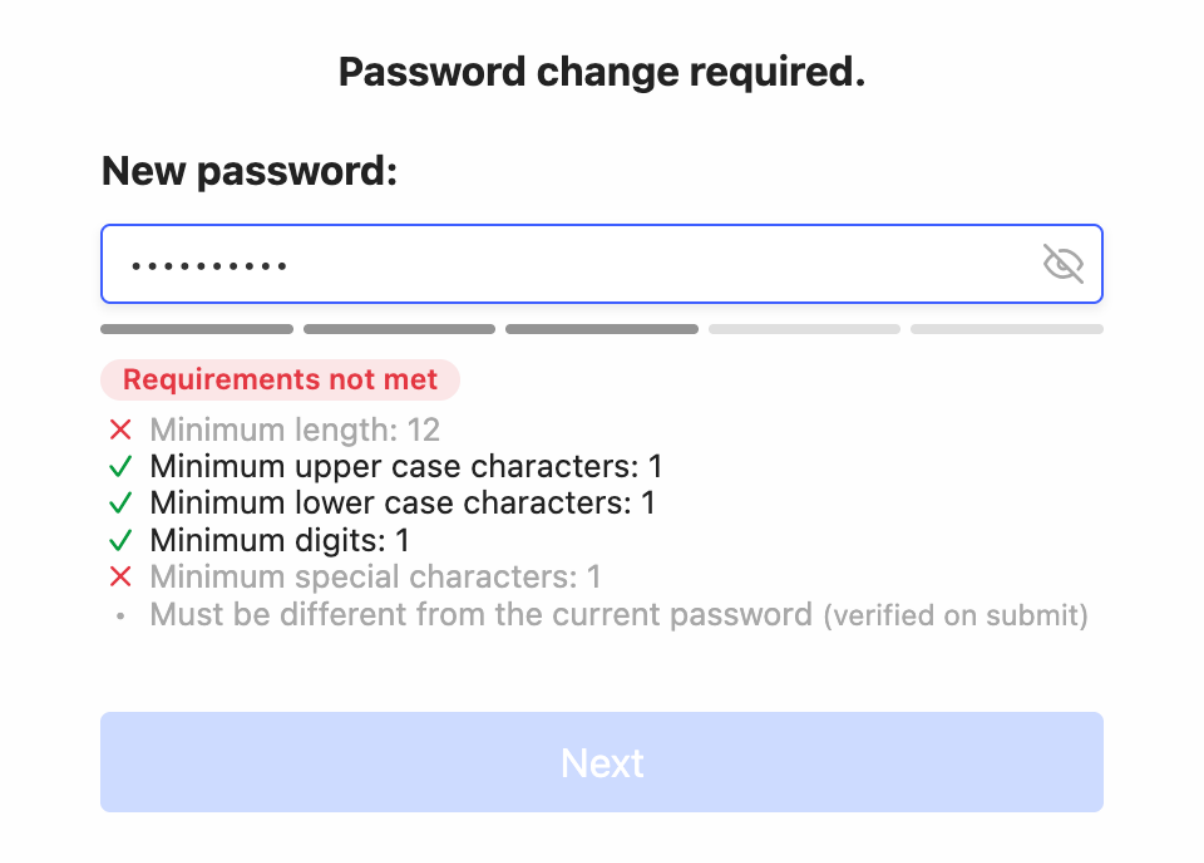


Enabling password complexity will trigger password change for users with the *Enforce pass-*

word complexity option enabled whose passwords do not comply with the complexity settings. The password will have to be changed upon logging into the *Access Gateway*.

Password complexity rules shown to users

For users with password complexity enforced, the rules are listed under every field where a static password is set: in the Admin Panel, in the User Access Gateway and on the password change screen displayed at login. The rules are checked as the user types, and the password can be saved only when all of them are met.



Related topics:

- *Creating a User*
- *Users Synchronization - User Directory*

12.5.5.4 User-Managed Methods in the User Access Gateway

Fudo Enterprise lets you decide which authentication methods a User Access Gateway user is allowed to add or remove on their own. This way you can limit self-service enrollment to the methods approved by your security policy, instead of relying on user training.

Note

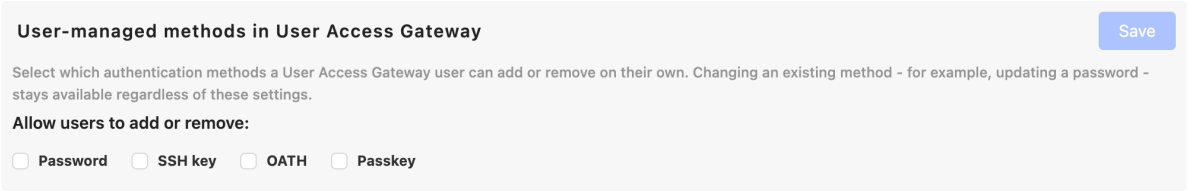
The setting is global - it applies to every User Access Gateway user.

Important

All methods are **disabled by default**. Until you enable a method here, User Access Gateway users cannot add or remove it themselves. Existing authentication methods are not affected - they remain on the list and can still be used to log in.

Selecting User-Managed Methods

1. Select *Settings* > *Authentication*.
2. Go to the *Global* tab and find the *User-managed methods in User Access Gateway* section.
3. Select the methods that User Access Gateway users are allowed to add and remove on their own:
   - *Password*
   - *SSH key*
   - *OATH*
   - *Passkey*



4. Click *Save*.

What the Setting Affects

Each checkbox governs both **adding** and **removing** the given method type in the User Access Gateway.

Action in the User Access Gateway	Method selected	Method not selected
Adding a new method	Allowed	Blocked - the button is greyed out
Removing an existing method	Allowed	Blocked - the button is greyed out
Editing an existing method (for example, changing a password)	Allowed	Allowed
Logging in with an existing method	Allowed	Allowed

Note

Clearing a checkbox never removes methods that users already have. It freezes the set of methods a user holds: no new method of that type can be added, and no existing one can be

removed by the user. To remove such a method, an administrator has to do it in the Admin Panel - see *Creating a User*.

Note

Changing an existing password in the User Access Gateway is an edit, not an addition, so it remains available even when *Password* is not selected. This also applies to password changes enforced by the password complexity policy.

Passkey and FIDO2 Configuration

The *Passkey* checkbox only decides whether users may enroll passkeys themselves. Before a passkey can be created at all, FIDO2 has to be configured by an administrator - see *FIDO2 Authentication Settings*.

Note

If FIDO2 is not configured, the *+ Passkey* button is not shown in the User Access Gateway at all, even when the *Passkey* checkbox is selected. For the same reason, the *Login with Passkey* button on the login page is displayed only when FIDO2 is configured for the given interface.

Related topics:

- *FIDO2 Authentication Settings*
- *Password Complexity*
- *Creating a User*

12.5.5.5 OATH Authentication Definition

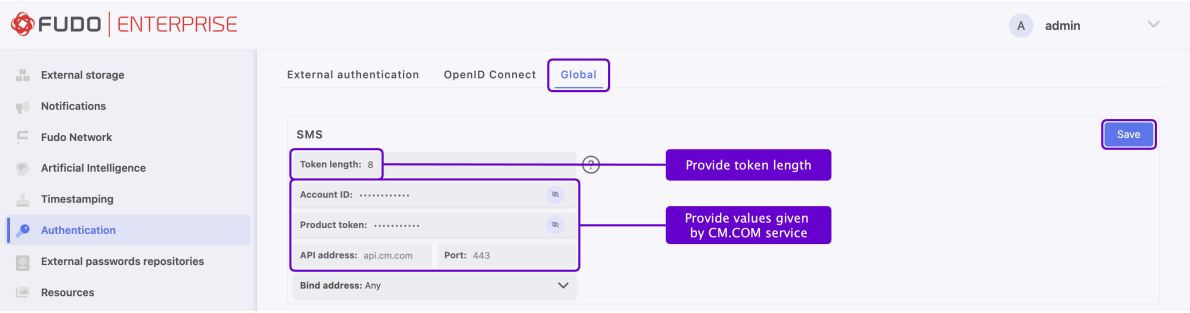
Refer to the *Two-Factor OATH Authentication with Google Authenticator* page.

Related topics:

- *User authentication methods and modes*
- *OpenID Connect Authentication Definition with Microsoft Entra (Azure)*
- *System overview*
- *Integration with CERB server*

12.5.5.6 SMS Authentication Definition

1. Select *Settings* > *Authentication* > *Global* tab.
2. Go to *SMS* section.



3. Input *Token length*.

Note

The token's length should be in the range of 4-16.

4. Input *Account ID*.
5. Input *Product token*.
6. Input *API address* and its *port*.

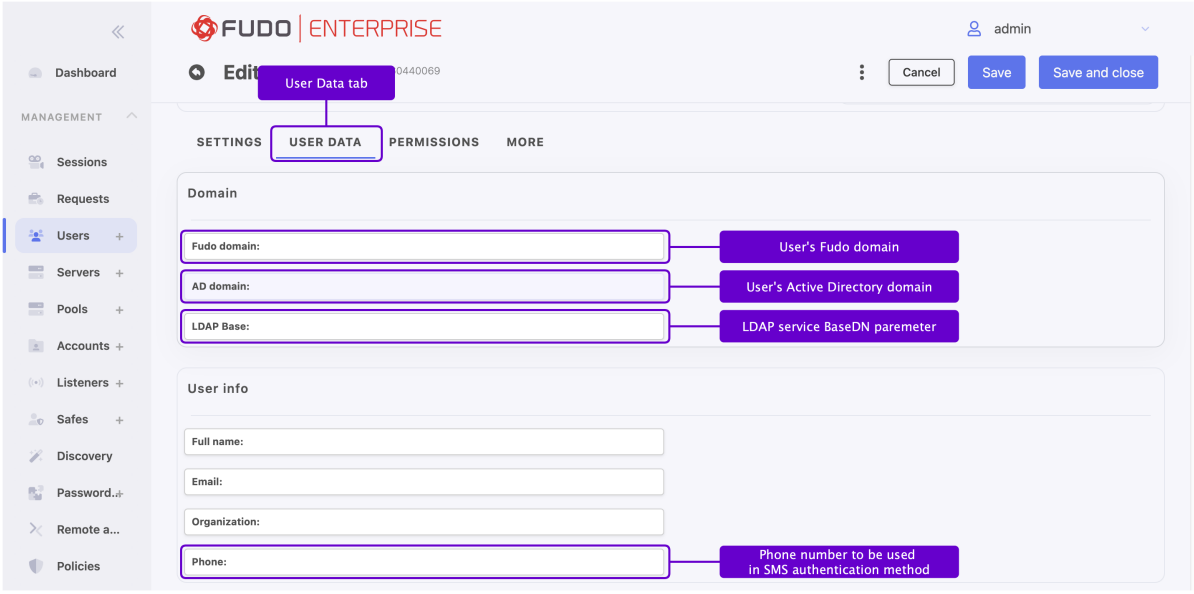
Note

The values for *Account ID*, *Product token* and *API address* are given by CM.COM service. You need to have a registered account there to be able to obtain the required information.

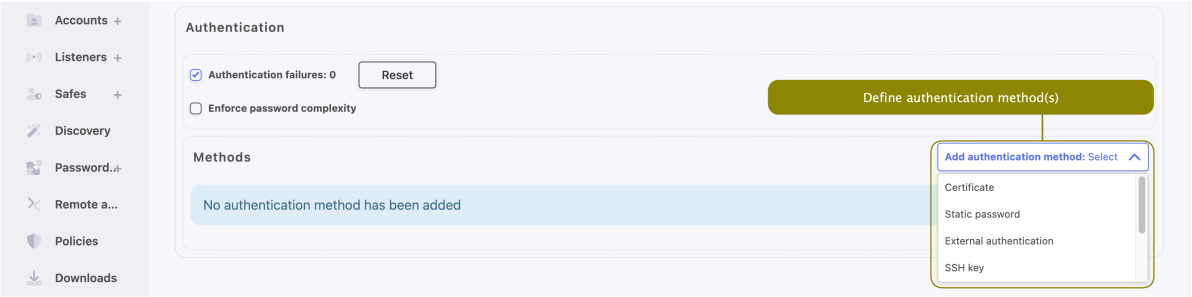
7. Select the *Bind address*.
8. Click *Save*.

Next, configure SMS authentication method for the User:

1. Go to *Management* > *Users*.
2. Find and select the user for whom you want to enable SMS authentication.
3. Input a phone number in the *User data* tab, in the *Phone* input field.



4. In the *Settings* tab, under the *Authentication* section choose `SMS` type from the *Add authentication method* drop-down list.



5. Choose `Static password` or `External authentication` (AD or LDAP) as a *First factor*.
6. Provide static password or external authentication source.
7. Select *Required password change on next login* option if needed.
8. Click *Save*.
9. Log in to the User Access Gateway with SMS code.

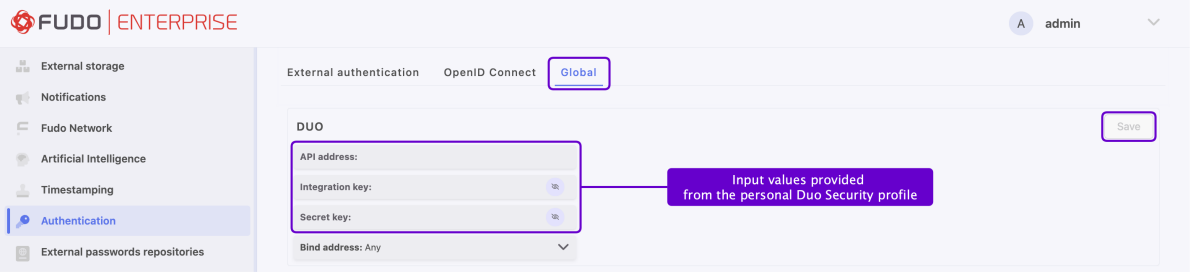
Related topics:

- *User authentication methods and modes*
- *OpenID Connect Authentication Definition with Microsoft Entra (Azure)*
- *System overview*
- *Integration with CERB server*

12.5.5.7 DUO Authentication Definition

1. Download and install Duo Mobile phone application.
2. Sign up for a personal account on Duo Security.
3. Select *Settings* > *Authentication* > *Global* tab.

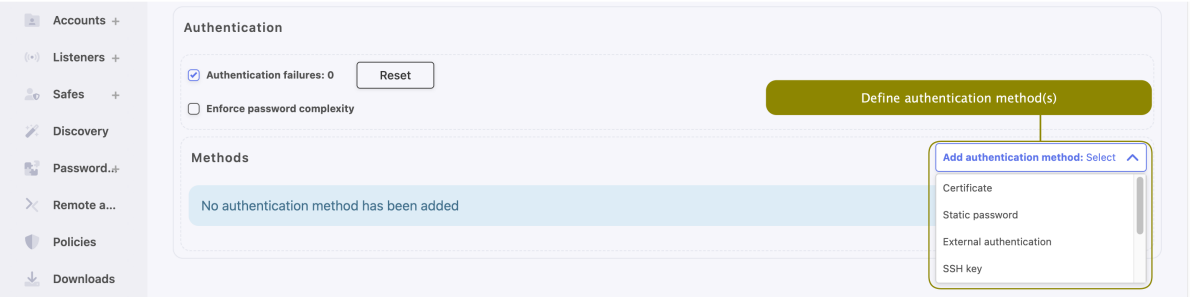
4. Go to *DUO* section.



5. Input values provided from the personal Duo Security profile: *API address*, *Integration key* and *Secret key*.
6. Select the *Bind address*.
7. Click *Save*.

Next, configure DUO authentication method for the User:

8. Go to *Management* > *Users*.
9. Find and select the user for whom you want to enable DUO authentication.



10. In the *Settings* tab, under the *Authentication* section choose `DUO` type from the *Add authentication method* drop-down list.
11. Choose `Static password` or `External authentication` (AD or LDAP) as a *First factor*.
12. Provide *DUO User*.
13. Provide *DUO User Id*.
14. Click *Save*.
15. Log in to the User Access Gateway by tapping *Accept* on push notification from Duo Mobile application.

Related topics:

- *User authentication methods and modes*
- *OpenID Connect Authentication Definition with Microsoft Entra (Azure)*
- *System overview*
- *Integration with CERB server*

12.5.5.8 Single Sign On

Single Sign On allows to automatically authenticate the user when logging into the system. Fudo Enterprise allows to set the Single Sign On functionality for both Admin Panel and User Portal (Access Gateway).

> **Note**
>
> For more detailed information on configuring SSO with Active Directory, please refer to the *Configuring the Single Sign On (SSO)* use case.

Setting up Fudo Enterprise for SSO

1. Set Fudo Enterprise hostname to `hostname.yourdomain.local`.
    - Select *Settings* > *Network configuration*.
    - Switch to the *Name & DNS* tab.
    - Enter `hostname.yourdomain.local` in the *Hostname* field.
2. Configure DNS server to point to a DNS server in the *yourdomain.local* domain.
    - Click *Add new* to define new DNS server.
    - Enter DNS server IP address.
    - Click *Save*.
3. Add user, that has an AD domain account.
    - *Set up LDAP users synchronization* or
    - *add user account manually*, with Active Directory external authentication method.

Setting up Domain Controller

1. Add user account, which will be used by the *User Portal* or *Admin Panel* to communicate with the *yourdomain.local* domain.

> **Note**
>
> When adding the account, enable the *Password does not expire* option.

2. On the DNS server add forward and reverse DNS entries for *hostname.yourdomain.local*.
3. Create a Kerberos ticket for Fudo Enterprise running the following command in the Powershell or CMD console:

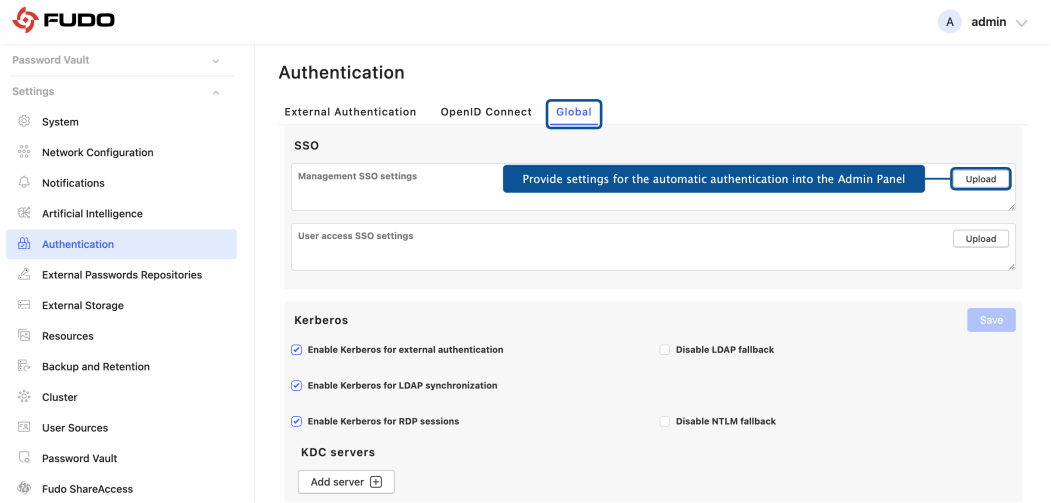
```
ktpass -princ HTTP/hostname.yourdomain.local@yourdomain.local -mapuser
netbios_domain_name\username -pass password       - ptype KRB5_NT_PRINCIPAL -out
hostname.yourdomain.local.keytab
```

Single Sign On in Admin Panel

> **Warning**
>
> **Single Sign On in Admin Panel** is available to set for a user with `superadmin` role only, and can be used by the users with `operator`, `admin` and `superadmin` roles.

In order to define SSO service parameters in system settings, follow the steps:

- Select *Settings* > `*Authentication* > *Global* tab.
- In the *SSO* section, click *Upload* button in the *Management SSO settings* field to access Admin Panel SSO configuration.



- Provide service identifier that will match the user account with the service instance.
- Upload the keytab file containing admin's ID and encryption keys for encrypting and decrypting Kerberos tickets.

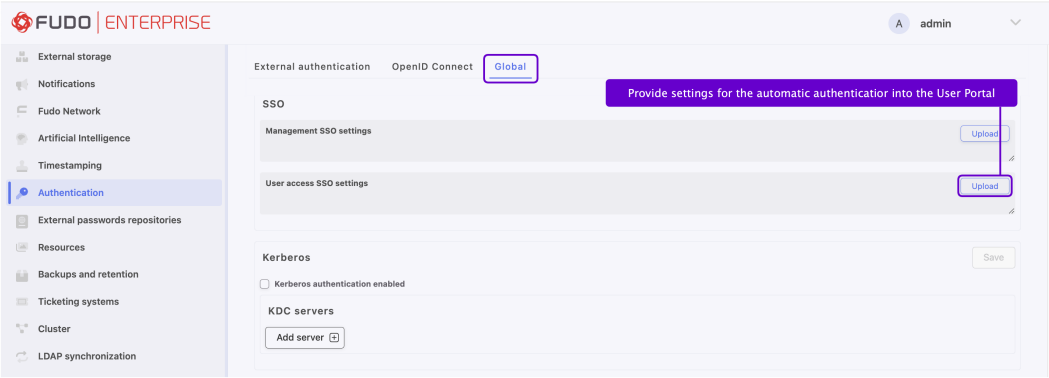
- Click *Save*.

Single Sign On in User Portal

In order to define SSO service parameters in system settings, follow the steps:

- Select *Settings* > `*Authentication* > *Global* tab.

- In the *SSO* section, click Upload button in the *User access SSO settings* field to access Access Gateway SSO configuration.



- Provide service identifier that will match the user account with the service instance.
- Upload the keytab file containing user's ID and encryption keys for encrypting and decrypting Kerberos tickets.

- Click *Save*.

Related topics:

- *Configuring the Single Sign On (SSO)*
- *Creating a User*
- *Users Synchronization - User Directory*

12.5.5.9 Kerberos Authentication Settings

Note

- Kerberos is used by the following components: **Active Directory** external authentication, user synchronization with the directory service (*User Directory*), *Discovery* operations, secret changers and secret verifiers, and authentication against the server during RDP sessions.
- The **Active Directory** external authentication method uses the Kerberos protocol as the first step.
- If **Active Directory** authentication is successfully completed using Kerberos, the configured certificate will not be applied, as it is only used when a fallback to LDAP is required.

- You no longer need to specify the domain in the Fudo hostname for Kerberos authentication to work correctly. This also allows Kerberos authentication to be used across multiple domains.

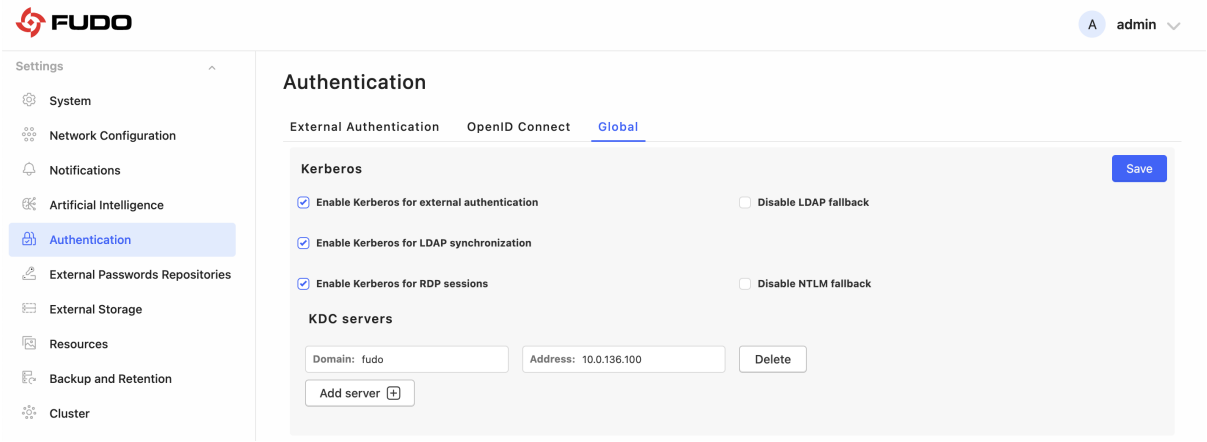
Configure Kerberos Authentication

The *Kerberos* section on the *Global* tab lets you enable Kerberos authentication independently for individual components and disable fallback to less secure protocols.

Note

Enabling the *Enable Kerberos for external authentication* option together with disabling the fallback mechanisms is particularly useful when authenticating members of the Active Directory **Protected Users** group. For accounts in this group, less secure protocols (such as NTLM) are blocked by the Windows domain controller and Kerberos authentication is required, so disabling the fallback in Fudo Enterprise aligns its behavior with the policy enforced by the domain.

Select *Settings* > *Authentication* > *Global* tab and go to the *Kerberos* section.



Option	Description
Enable Kerberos for external authentication	Uses the Kerberos protocol as the first authentication step in the **Active Directory** external authentication method.
Disable LDAP fallback	Disables the fallback to LDAP simple bind authentication when Kerberos is unavailable. **Active Directory** authentication then fails. See *Disable Authentication Fallback*.
Enable Kerberos for LDAP synchronization	Uses the Kerberos protocol when synchronizing users with the directory service (**User Directory**).
Enable Kerberos for RDP sessions	Uses the Kerberos protocol to authenticate against the RDP server when establishing a session.
Disable NTLM fallback	Disables the fallback to NTLM authentication in RDP (NLA) sessions when Kerberos is unavailable. See *Disable Authentication Fallback*.

To save the changes, click *Save* in the *Kerberos* section.

> **Note**
>
> To **completely disable** Kerberos authentication for a given component, deselect the corresponding option (e.g. *Enable Kerberos for RDP sessions*) and save the changes.

Disable Authentication Fallback

To enforce the use of the Kerberos protocol only, you can disable the fallback to less secure authentication protocols:

- **NTLM (RDP sessions)** — select the *Disable NTLM fallback* option. If Kerberos is unavailable, authentication fails and the following message appears in the debug log:

  ```
  Kerberos authentication failed, NTLM fallback is disabled.
  ```

- **LDAP simple bind (Active Directory authentication)** — select the *Disable LDAP fallback* option. If Kerberos is unavailable, authentication fails and the following message appears in the debug log:

  ```
  Kerberos authentication failed for user %s (domain %s), LDAP fallback is␣
  ↪disabled.
  ```

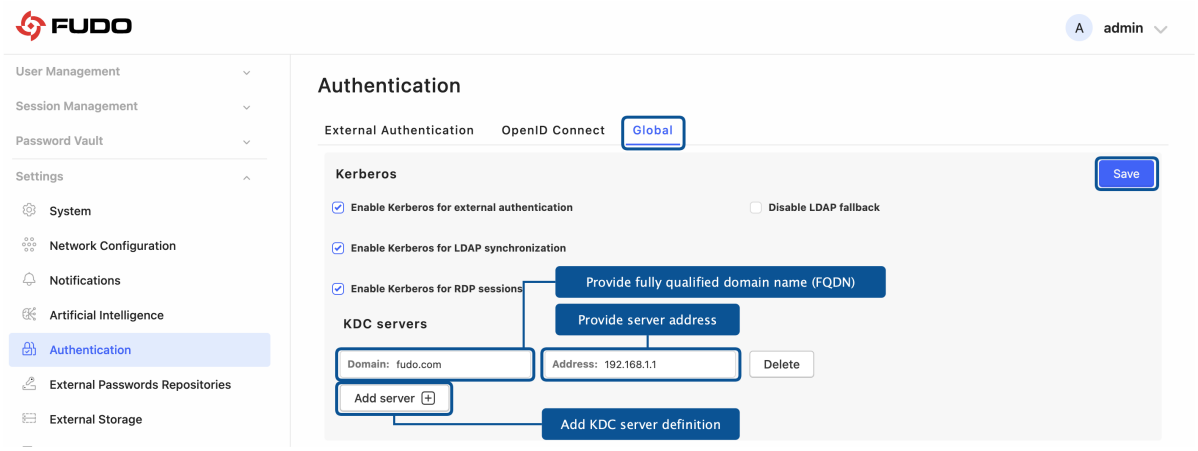
Add KDC Servers

Fudo Enterprise supports configuring Key Distribution Servers (KDC) and mapping domains to KDC servers. Kerberos authentication in multi-domain Active Directory environments is also supported.

> **Note**
>
> Configuring KDC servers is **optional**. In multi-domain Active Directory environments you do not need to add KDC entries manually or include the domain in the Fudo hostname. See *DNS Configuration*.

To add a KDC server:

1. Select *Settings* > *Authentication* > *Global* tab.
2. Go to the *Kerberos* > *KDC servers* section.
3. Click *Add server*.



4. Provide the fully qualified domain name (FQDN) in the *Domain* field (e.g., `fudo.com`, `.fudo.com`).
5. Provide the KDC server address in the *Address* field (e.g., `192.168.1.1`, `foo.bar`, `tcp/foo.bar`, `udp/192.168.1.1:88`).

Related topics:

- *User authentication methods and modes*
- *External authentication server definition*
- *OpenID Connect Authentication Definition with Microsoft Entra (Azure)*
- *System overview*
- *Integration with CERB server*

12.5.5.10 FIDO2 Authentication Settings

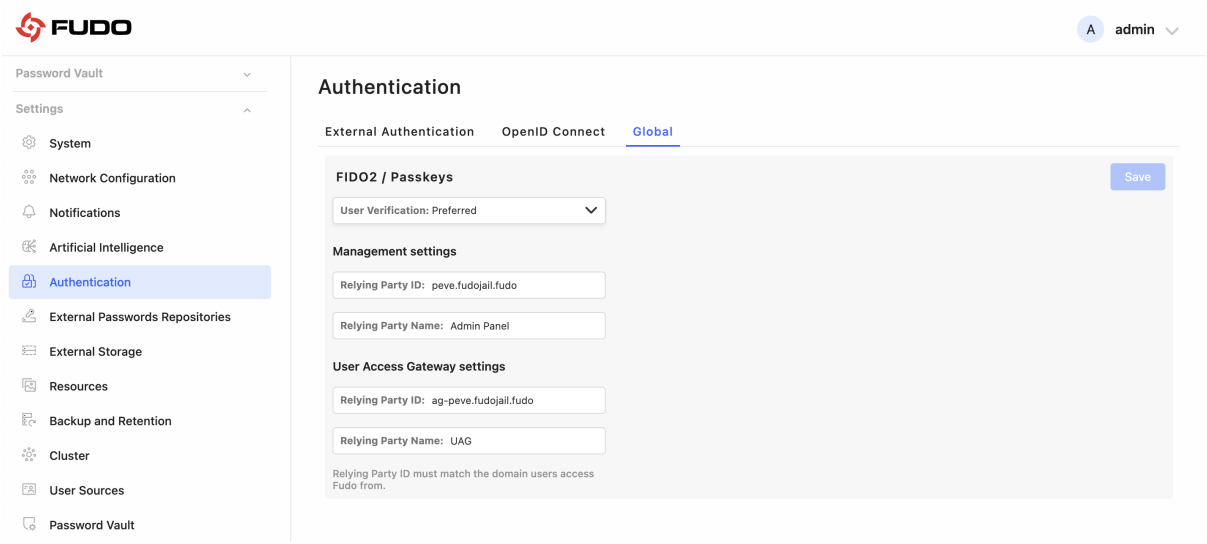
Note

- *FIDO2 authentication* functionality enables secure passwordless login using hardware keys, biometrics, or device-based methods.
- FIDO2 is supported for logging into the Admin Panel and User Access Gateway.
- Each user can only configure the FIDO2 method for their own account.

Configure Global FIDO2 Settings

To configure FIDO2 settings:

1. Select *Settings* > *Authentication* > *Global* tab.
2. Go to the *FIDO2* section.
3. In the *User Verification* field, select the user verification level:
   - **Preferred** - The system prefers user verification but will accept authentication without it
   - **Required** - User verification is mandatory (fingerprint, PIN, key touch)



4. In the *Relying Party* field, enter the full hostnames for which the SSL certificate is issued.
5. Click *Save*.

Warning

The HTTPS certificate **must be valid for all hostnames** used to open the Admin Panel and the User Access Gateway. Certificates are uploaded under *Settings* > *System*, in the *Fudo Admin Panel HTTPS certificate* and *User Access Gateway HTTPS certificate* fields (see *Certificates*).

If **floating IP addresses** are used, the certificate must include **all hostnames** under which the system may be reachable - otherwise FIDO2 login will only work for some of the addresses.

For clusters, deploy the same certificate to all nodes - it is not automatically copied.

If the *list of Access Gateway allowed hosts* is filled, the host names used for FIDO2 login in the User Access Gateway must be on it.

Note

FIDO2/Passkey works only when the login page is opened using a hostname (FQDN), **not an IP address**. For example, it works at `https://fudo.example.com/` but not at `https://192.168.1.10/` - an IP address is not a valid *Relying Party* ID, so the browser will not register or use a Passkey.

The value in the *Relying Party* field (Relying Party ID) must be **identical to the hostname the user opens the login page on** in the browser, or a parent domain of it. Enter the hostname only, without the *https://* prefix and without a port number (e.g. *fudo.example.com*).

If the *Relying Party* value does not match the current address, the browser rejects the login with a message similar to:

"The relying party ID is not a registrable domain suffix of, nor equal to the current domain."

In this case, adjust the *Relying Party* field to match the address the login page is actually served from.

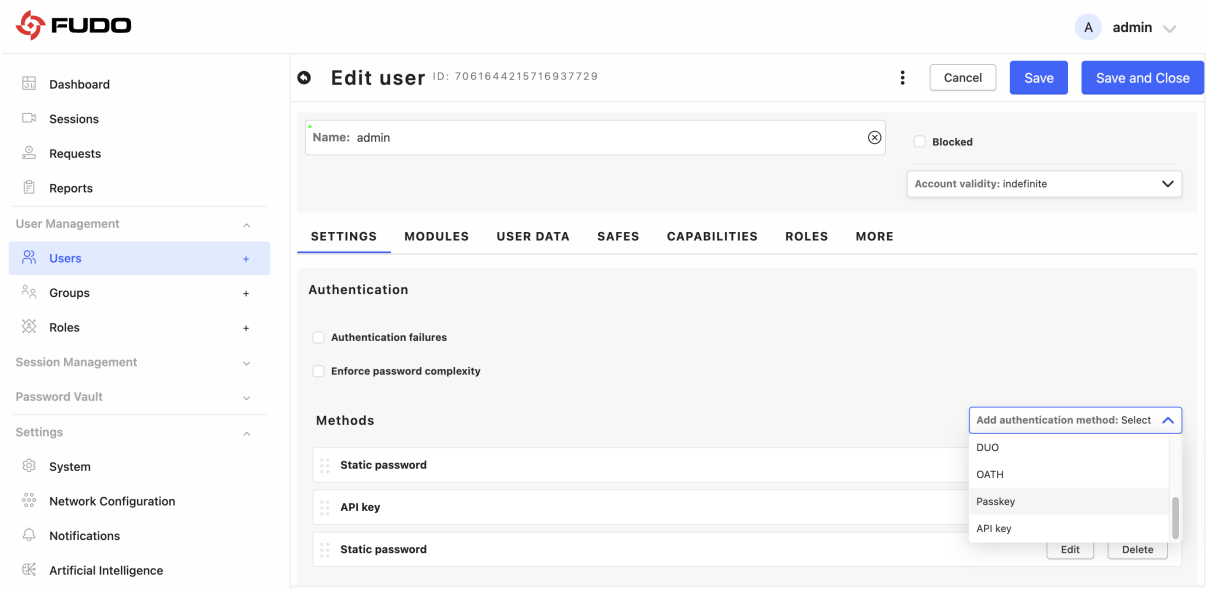
Warning

Changing the *Relying Party* value **invalidates all previously registered Passkeys** - they are cryptographically bound to the previous Relying Party ID. After changing the address, users must register their keys again.

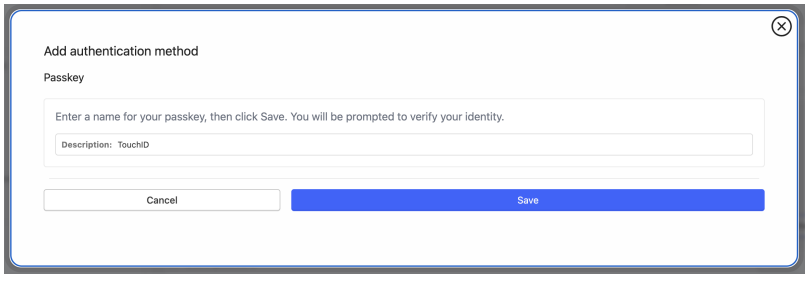
Add Passkey Method for User

To add a FIDO2/Passkey method for a user:

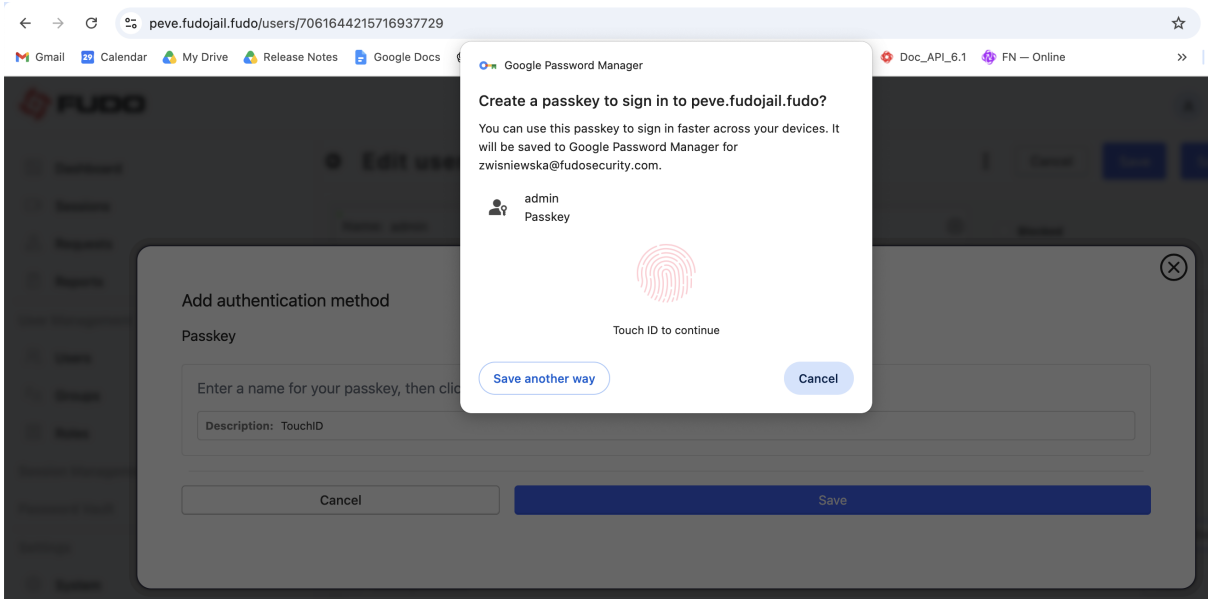
1. Navigate to *Users management* > *Users*.
2. Edit the user account.
3. In the authentication methods section, click *Add authentication method*.
4. Select *Passkey*.



5. Enter a name for the authentication method being added and click *Save*. You will be prompted to verify your identity.



6. Follow the browser instructions:
   - Choose your authentication method (hardware key, biometrics, password manager)
   - Confirm your identity (touch the key, use fingerprint, Face ID)
   - Save the Passkey

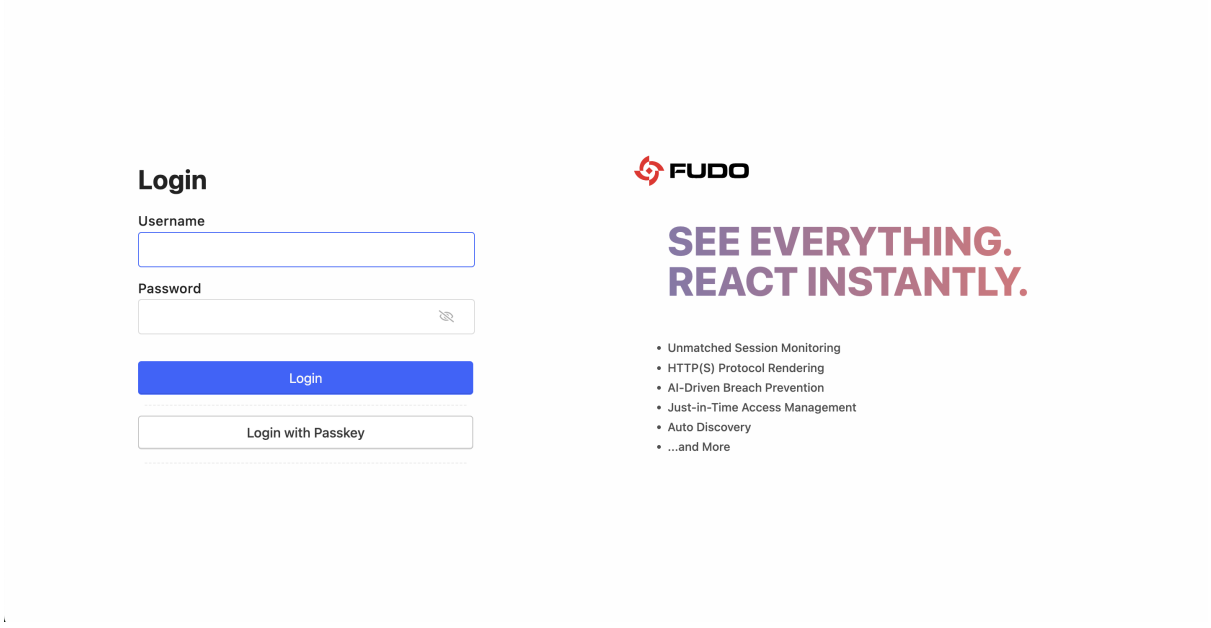


7. Click Save and close to save the configuration of the new authentication method for the user.

Log in Using FIDO2

After configuring a FIDO2 method:

1. On the login page, enter your username.
2. Click the *Login with Passkey* button.



3. Confirm your identity using the configured method.
4. The system will automatically verify the cryptographic signature and grant access.

Note

- The *Login with Passkey* button only appears when the user has a FIDO2 method configured.
- Users can only configure FIDO2 for their own accounts.
- Passkeys created in the Admin Panel cannot be used in the User Access Gateway.

Related topics:

- *User authentication methods and modes*
- *Global Authentication Settings*

12.6 External Passwords Repositories

Fudo Enterprise supports external passwords repositories for managing passwords to monitored servers.

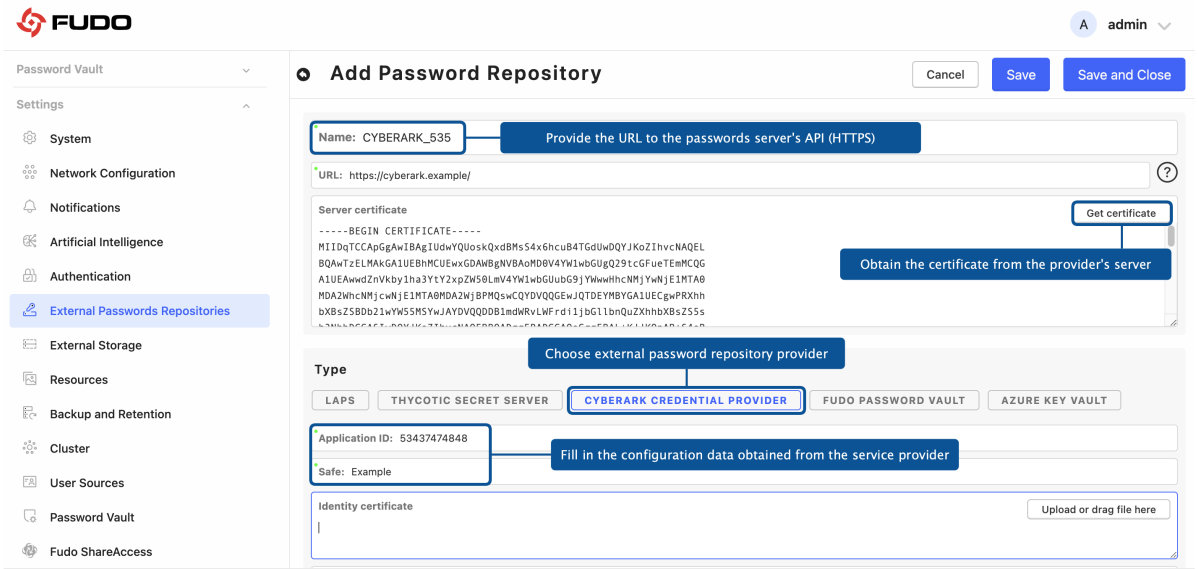
12.6.1 CyberArk Credential Provider

Adding a new passwords repository

1. Select *Settings* > *External passwords repositories*.
2. Click *+ Add password repository*.
3. Specify object's name.
4. Provide the URL to the passwords server's API (HTTPS).
5. In the *Server certificate* field, provide the server certificate, or click the *Get certificate* button to obtain it from the provider's server.

Warning

If HTTPS is used without providing a server certificate, the connection is not verified and is accepted.



6. Select *CYBERARK CREDENTIAL PROVIDER* button in the *Type* section.
7. Provide application identification (*Application ID*).
8. Provide *Safe* (optional). If *Safe* is not defined, the search will be performed across all CyberArk safes.

Note

The search for a given server/account is performed based on the following attributes from the *CyberArk Credential Provider*, which must be set up according to the rules below:

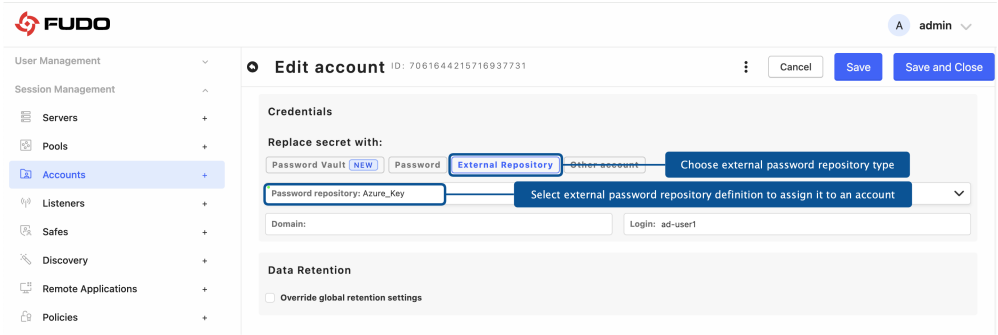
- `Address` - has to match exactly with Fudo server's IP address (required),
- `UserName` - has to match exactly with Fudo account's *Login* (required) - please refer to *Creating a Regular Account* topic,
- `Safe` - has to match exactly with external password repository *Safe* field (optional).

9. When used client certificate authentication *Identity certificate* and *Identity key* fields has to be defined.

Note

-*Identity certificate* and *Identity key* configuration is available only for HTTPS type servers. - Both fields must be filled using PKCS #8 format. - To learn how to generate *Identity certificate* and *Identity key* please follow the next section.

10. Click *Save*.
11. Assign external password repository to an account.
    - Select *Management* > *Accounts*.
    - Browse objects and click an account to access the settings form.
    - In the *Credentials* section, on the *Replace secret with* field, select *Repository* button.
    - From the *Passwords repository* drop-down list select one of the previously defined password repositories.



- Click *Save*.

Generating `CyberArk Credential Provider's` client certificate authorization

1. Generate random Serial Number (e.g. 11223344556677) that will be used by CyberArk to verify the client.
2. Generate *client.key* and *client.crt* files using *openssl*. Example:

```
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. Paste the content of the file *client.crt* in *Identity certificate* field.
4. Paste the content of the file *client.key* in *Identity key* field.
5. Add client serial number to CyberArk server authentication configuration.

Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Locate the repository definition and click on its name to edit its configuration as needed.
3. Click *Save*.

Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find desired repository definition, select it, and click the *Delete selected* button.
3. Click *Save*.

Note

You cannot delete password repository definition if it is assigned to any account.

Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

12.6.2 Thycotic Secret Server

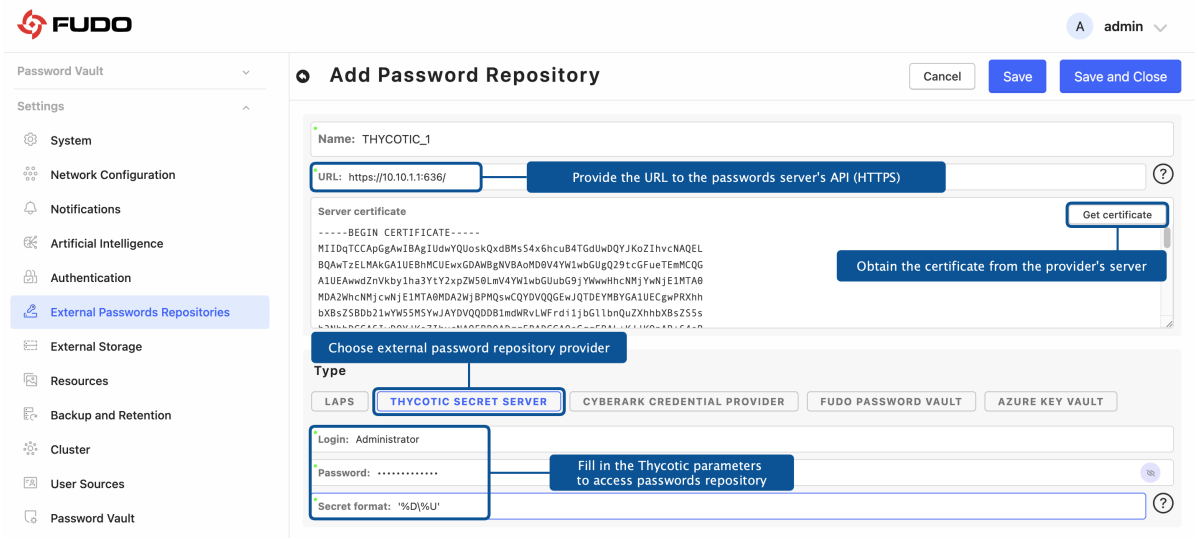
Adding a new passwords repository

1. Select *Settings* > *External passwords repositories*.
2. Click *+ Add password repository*.
3. Specify object's name.
4. Provide the URL to the passwords server's API (HTTPS).

Note

Specify HTTPS protocol within the URL so that communication with the server is encrypted.

5. In the *Server certificate* field, provide the server certificate, or click the *Get certificate* button to obtain it from the provider's server.

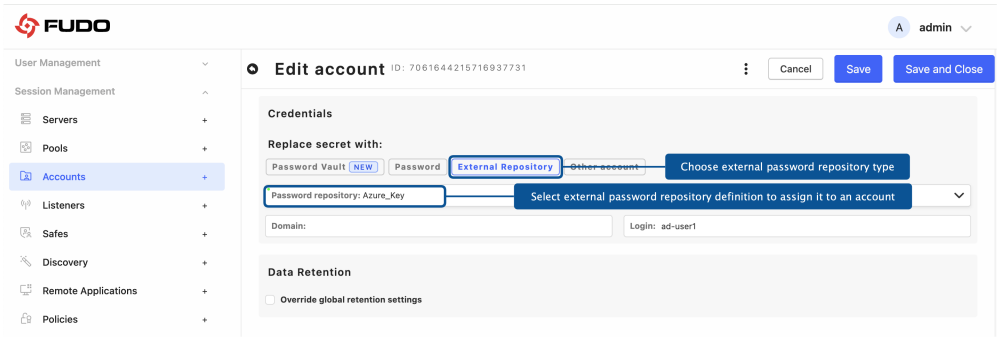


6. Select *THYCOTIC SECRET SERVER* button in the *Type* section.
7. Enter user login allowed to access passwords repository.
8. Provide user password in the *Password* field.
9. Define secret string format used for identifying objects on Thycotic Secret Server.

Note

Secret format can be defined by using variables: `%U - user name, %D - user domain, %S - server name.`, e.g., *'%D%U'*.

10. Click *Save*.
11. Assign external password repository to an account.
    - Select *Management* > *Accounts*.
    - Browse objects and click an account to access the settings form.
    - In the *Credentials* section, on the *Replace secret with* field, select *Repository* button.
    - From the *Passwords repository* drop-down list select one of the previously defined password repositories.



- Click *Save*.

Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Locate the repository definition and click on its name to edit its configuration as needed.
3. Click *Save*.

Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find desired repository definition, select it, and click the *Delete selected* button.
3. Click *Save*.

Note

You cannot delete password repository definition if it is assigned to any account.

Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

12.6.3 Local Administrator Password Solutions (LAPS)

Warning

In some environments, LAPS functionality may be entirely unavailable.

Active Directory/LDAP configuration

The LDAP server should have specified attributes that fall within the `computer` objectClass:

- `dNSHostName` - server name - must be identical with server's unique name specified when creating the server (refer to section about servers creation, ex. *Creating a TCP Server*),

- `sAMAccountName` - login name in that server - must be identical with account's *Login* from *Credentials* section (refer to *Creating a Regular Account* section),
- `ms-Mcs-AdmPwd` - password in plain text,
- `ms-Mcs-AdmPwdExpirationTime` - password expiration date (optional).

Adding a new passwords repository

Note

In order to add LAPS password repository in Fudo Enterprise you have to provide following AD/LDAP parameters:

- URL to AD/LDAP server, e.g., `ldaps://10.10.1.1:636/`,
- *Base DN* to AD/LDAP server, e.g., `dc=company,dc=com`,
- Login and password to AD/LDAP server, e.g., `cn=admin,dc=company,dc=com`,
- CA certificate to validate the encrypted (LDAPS) connection to the AD/LDAP server.

1. Select *Settings* > *External passwords repositories*.
2. Click + *Add password repository*.
3. Specify object's name.
4. Provide the URL to the passwords server's API.

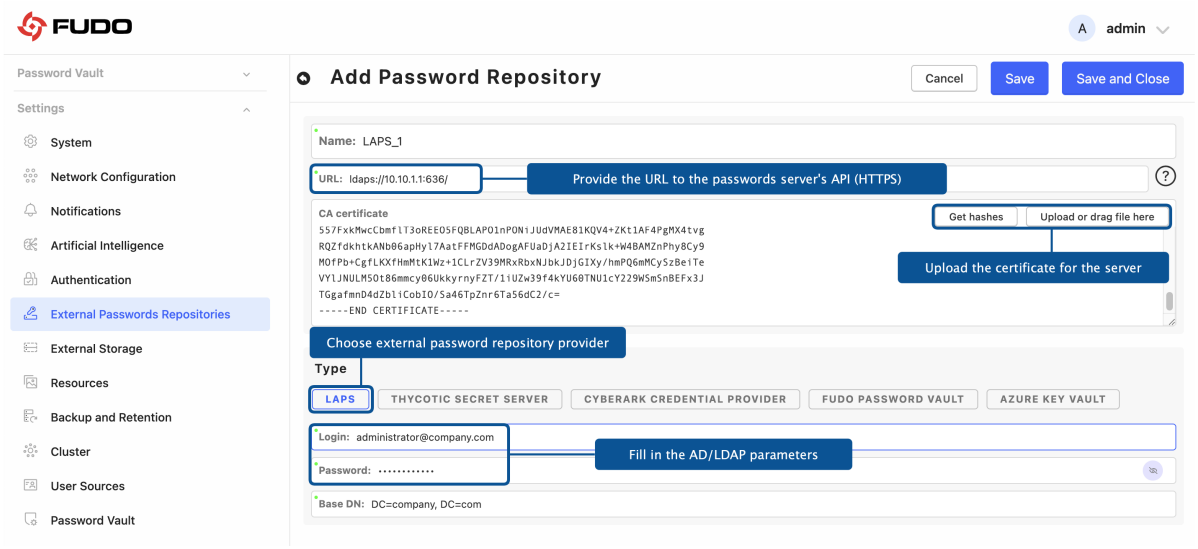
Note

Supported URL format is `ldaps://<server>[:<port>]/` for an encrypted connection.

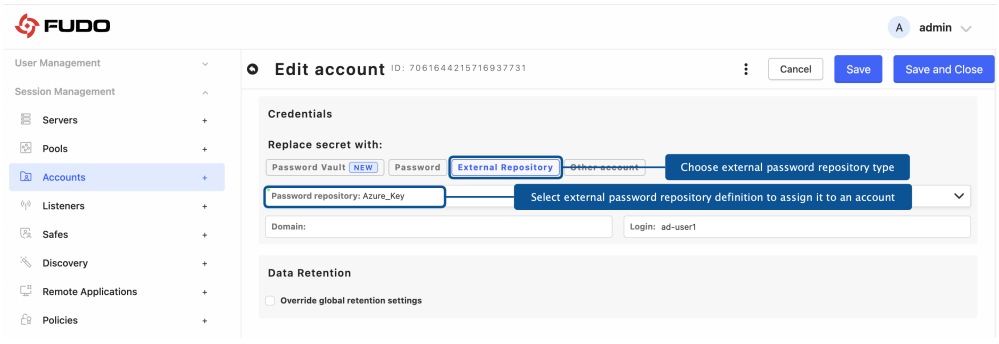
5. In the *Server certificate* field, provide the server certificate, or click the *Get certificate* button to obtain it from the provider's server.

Warning

If LDAPS is used without providing a server certificate, the connection is not verified and is accepted.



6. Select *LAPS* button in the *Type* section.
7. Enter user login allowed to access passwords repository.
8. Provide user password in the *Password* field.
9. Provide *Base DN* to AD/LDAP server.
10. Click *Save*.
11. Assign external password repository to an account.
    - Select *Management* > *Accounts*.
    - Browse objects and click an account to access the settings form.
    - In the *Credentials* section, on the *Replace secret with* field, select *Repository* button.
    - From the *Passwords repository* drop-down list select one of the previously defined password repositories.



    - Click *Save*.

Note

The search for a given server/account is performed based on the following attributes from the *LAPS*, which must be set up according to the rules below:

- `dNSHostName` - server name - has to match exactly with Fudo server's unique name specified when creating the server (refer to *Creating a TCP Server* section),
- `sAMAccountName` - login name in that server - has to match exactly with account's Login from *Credentials* section (refer to *Creating a Regular Account* section).

Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Locate the repository definition and click on its name to edit its configuration as needed.
3. Click *Save*.

Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find desired repository definition, select it, and click the *Delete selected* button.
3. Click *Save*.

Note

You cannot delete password repository definition if it is assigned to any account.

Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

12.6.4 Fudo Password Vault

Fudo Enterprise can retrieve secrets from the *Password Vault* of another (remote) Fudo Enterprise instance and use them as passwords for monitored accounts. The local Fudo Enterprise connects to the remote instance through its User Access Gateway (UAG) API, authenticating with an API key.

Prerequisites on the Remote Fudo

Before adding the repository, create a dedicated user on the remote Fudo Enterprise instance that hosts the Password Vault, and authenticate it with an API key. The repository uses this key to connect to the remote instance.

1. On the remote Fudo Enterprise, select *User Management* > *Users* and click *+ Add user*.
2. Enter a user name.
3. Click *Save* to create the user.
4. From the *Role* drop-down list, select a role that includes Password Vault management permissions.

5. Go to the *Safes* tab and select the safe named *portal* to grant the user access to the User Access Gateway.
6. From the *Add authentication method* drop-down list, select *API key*.
7. Generate the *API key* (or enter your own).
8. Copy the generated key - you will provide it when adding the repository.
9. Click *Save and Close*.

Note

The API key cannot be retrieved after the authentication method is saved, so copy it before saving.

Note

Make sure this user has at least read access (for example, the *View* permission) to the Password Vault collection that stores the secrets you want to use.

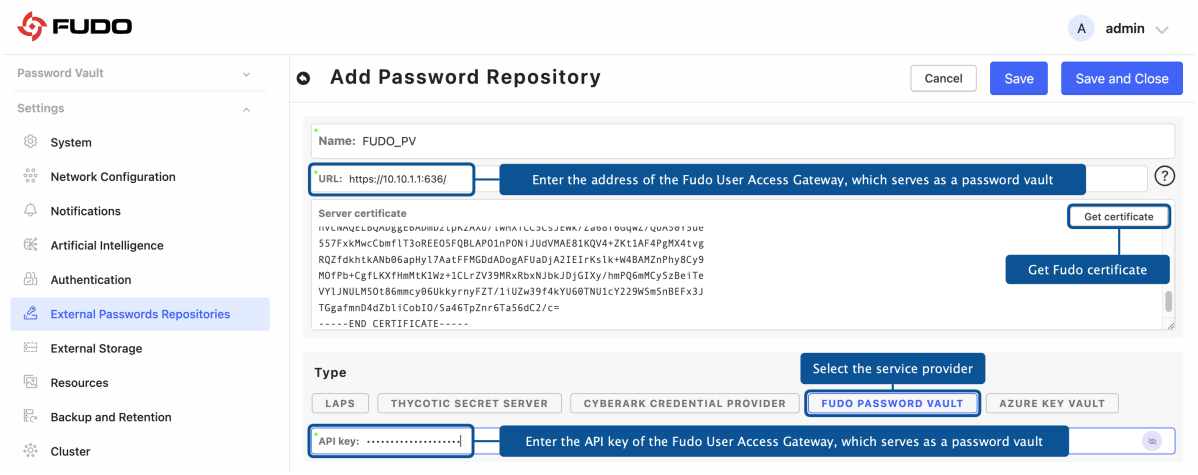
Adding a New Passwords Repository

1. Select *Settings* > *External passwords repositories*.
2. Click *+ Add password repository*.
3. Specify object's name.
4. In the *URL* field, provide the address of the Fudo User Access Gateway, which serves as a password vault (for example, its IP address).
5. In the *Server certificate* field, provide the User Access Gateway (UAG) HTTPS certificate of the remote Fudo, or click the *Get certificate* button to obtain it from the remote server.

Warning

If HTTPS is used without providing a server certificate, the connection is not verified and is accepted.

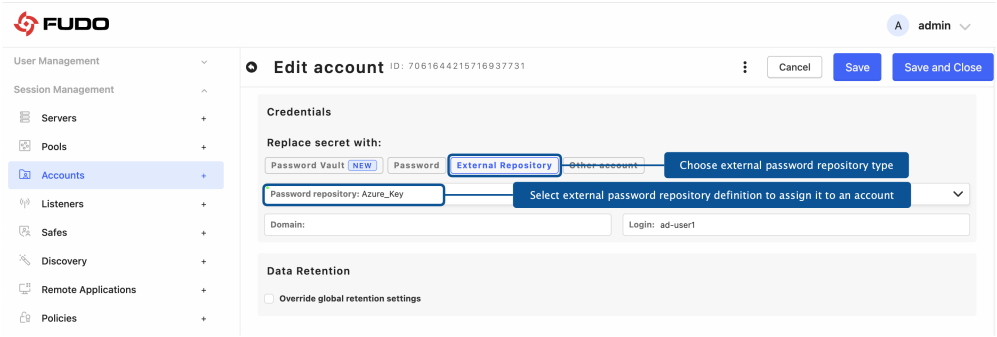
6. Select *FUDO PASSWORD VAULT* button in the *Type* section.



Note

On the remote Fudo Enterprise, the UAG HTTPS certificate is available in *Settings* > *System*, the *General* tab, *Certificates* section (*User Access Gateway HTTPS certificate*).

7. In the *API key* field, provide the API key of the remote Fudo Enterprise UAG user (copied in the prerequisites stage).
8. Click *Save*.
9. Assign the external password repository to an account.
    - Select *Management* > *Accounts*.
    - Browse objects and click an account to access the settings form.
    - In the *Credentials* section, on the *Replace secret with* field, select *Repository* button.
    - From the *Passwords repository* drop-down list select the repository defined above.
    - Provide the *Login* and, optionally, the *Domain* - the same values as in the Secret on the remote Fudo Enterprise.



- Click *Save*.

Matching Secrets from the Password Vault

When a Password Vault repository is assigned to an account, Fudo Enterprise matches the account against the secrets stored in the remote Password Vault. The name of the secret is

irrelevant; matching is based on the account fields.

All fields that are filled in on the account must have the same values in the Password Vault secret. If the account has the following fields filled in, the secret must hold the same values to be matched:

- *Login*
- *Domain*
- *Address* (URL with protocol and port)

For example, an account with login `User_1` used on the SSH server `10.0.100.1` (port `65522`) in the domain `fudo` matches a secret with the following values:

- *Login*: `User_1`
- secret value (password): `pass`
- *Domain*: `fudo`
- *URL*: `ssh://10.0.100.1:65522`

Warning

- If any of these fields is missing in the Password Vault secret, Fudo Enterprise does not match it to the account, and the operation silently fails.
- If the remote Password Vault has a *Basic* tier license, fetching the secret silently fails.

Editing a Passwords Repository

To edit a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Locate the repository definition and click on its name to edit its configuration as needed.
3. Click *Save*.

Deleting a Passwords Repository

To delete a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find desired repository definition, select it, and click the *Delete selected* button.
3. Click *Save*.

Note

You cannot delete password repository definition if it is assigned to any account.

Related Topics:

- *User authentication methods and modes*
- *System overview*

- *Integration with CERB server*

12.6.5 Azure Key Vault

Fudo Enterprise can retrieve secrets from a Microsoft Azure Key Vault and use them as passwords for monitored accounts.

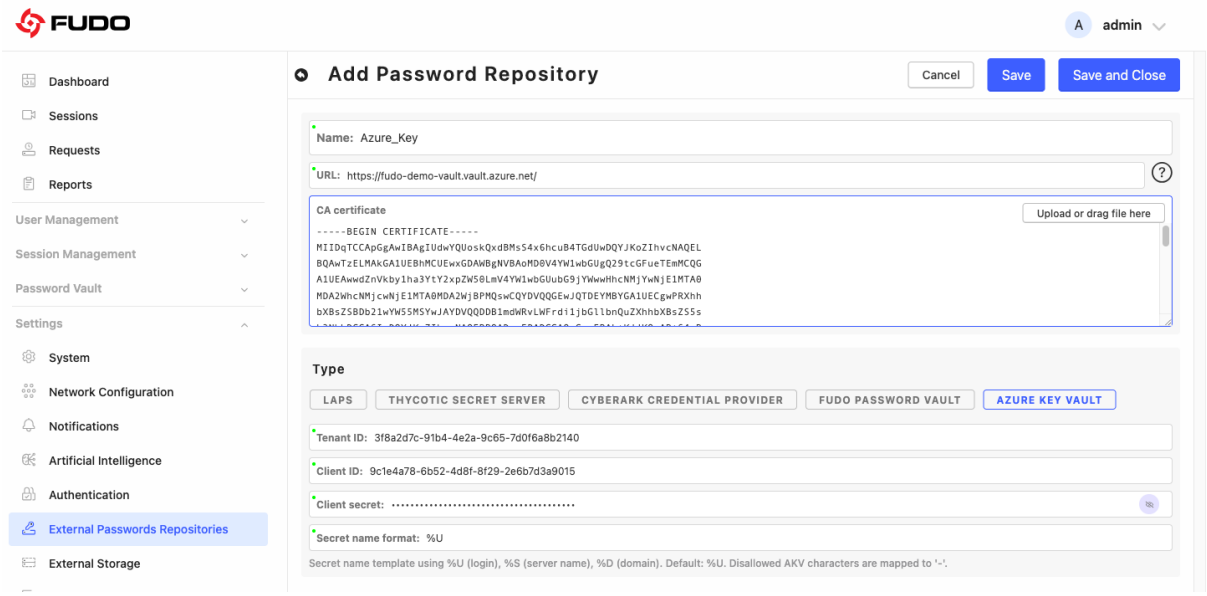
Adding a new passwords repository

Note

In order to add an Azure Key Vault password repository in Fudo Enterprise you have to provide the following parameters:

- the Key Vault *URL*, e.g., `https://<vault-name>.vault.azure.net/`,
- the *Tenant ID* of the Azure Active Directory tenant,
- the *Client ID* of the application (service principal) authorized to read secrets from the vault,
- the *Client secret* generated for that application.

1. Select *Settings* > *External passwords repositories*.
2. Click *+ Add password repository*.
3. Specify object's name.
4. Provide the Key Vault *URL* (HTTPS).
5. In the *CA certificate* field, provide the CA certificate used to validate the HTTPS connection to the Key Vault, or upload it from a file.
6. Select *AZURE KEY VAULT* button in the *Type* section.

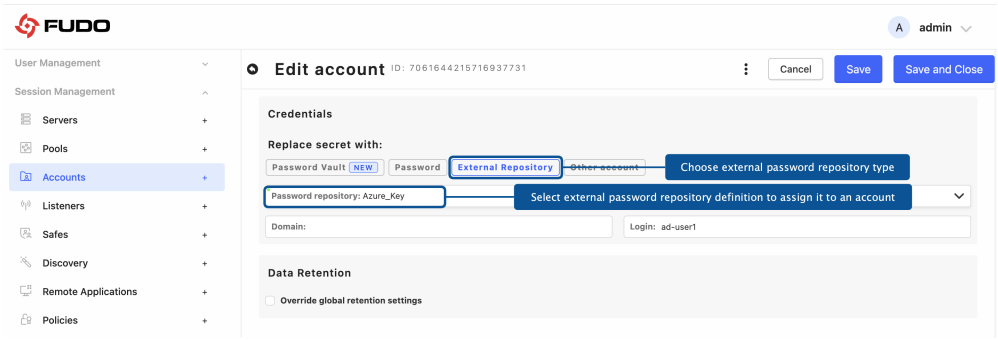


7. Provide the *Tenant ID* of the Azure Active Directory tenant.
8. Provide the *Client ID* of the application (service principal) authorized to read secrets from the vault.

9. Provide the *Client secret* generated for that application.
10. Define the *Secret name format* - the template used to build the name of the secret looked up in the Key Vault.

> **Note**
>
> The *Secret name format* supports the following variables: `%U` (login), `%S` (server name), and `%D` (domain). The default value is `%U`. Characters that are not allowed in Azure Key Vault secret names are automatically replaced with `-`.

11. Click *Save*.
12. Assign external password repository to an account.
    - Select *Management* > *Accounts*.
    - Browse objects and click an account to access the settings form.
    - In the *Credentials* section, on the *Replace secret with* field, select *Repository* button.
    - From the *Passwords repository* drop-down list select one of the previously defined password repositories.



    - Click *Save*.

Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Locate the repository definition and click on its name to edit its configuration as needed.
3. Click *Save*.

Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find desired repository definition, select it, and click the *Delete selected* button.
3. Click *Save*.

Note

You cannot delete password repository definition if it is assigned to any account.

Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

12.7 External Storage

Fudo Enterprise supports storing session data on external storage devices attached through a Fibre Channel interface.

Caution

- External Storage is supported only on physical appliances equipped with Fibre Channel cards. Virtual machines and emulated environments are not supported.
- Fibre Channel cards are not included in the standard hardware configuration and are installed only if ordered with the appliance.

Note

External storage in cluster configuration

- In a cluster configuration, each node must have a dedicated *WWN* object.
- Data stored on external storage is not replicated between cluster nodes.

12.7.1 Configuring External Storage

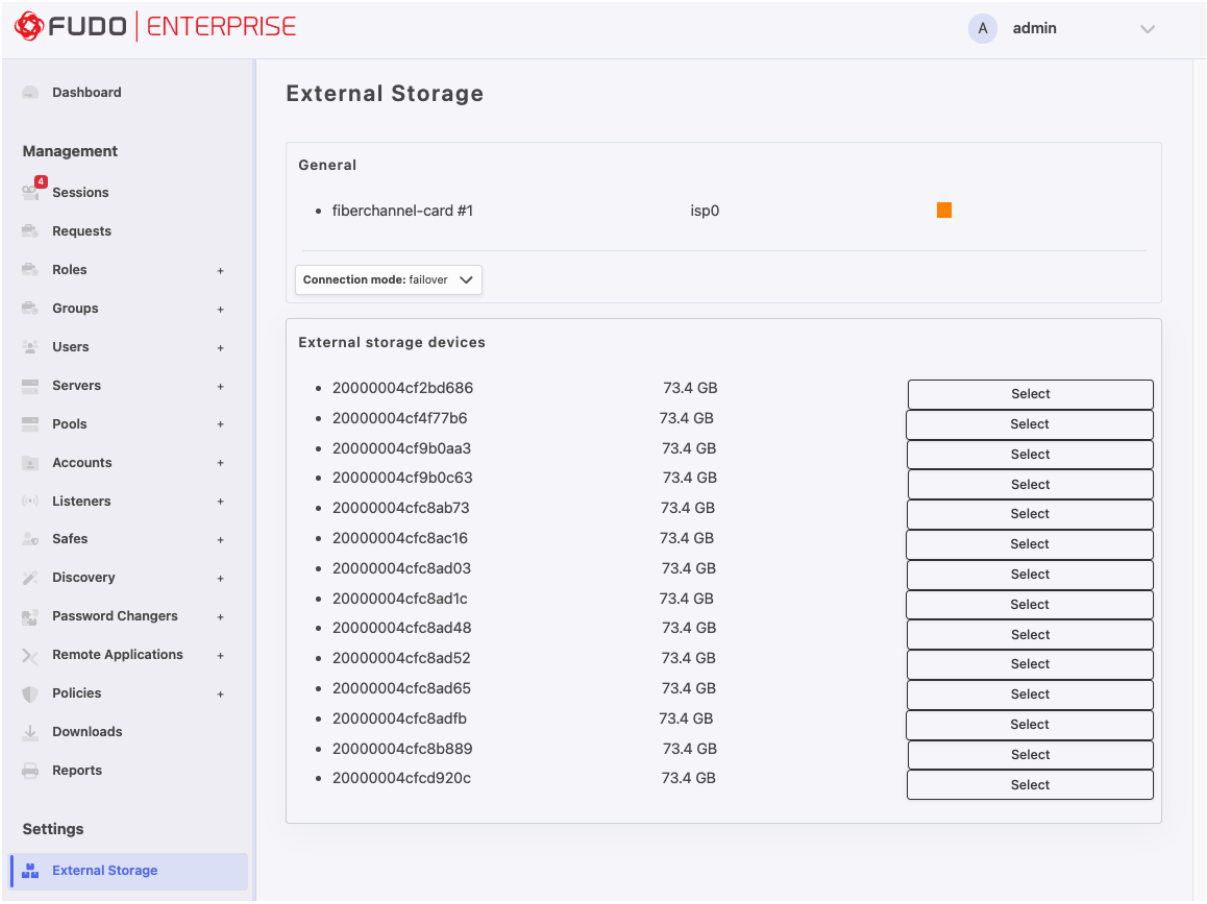
1. Select *Settings* > *External storage*.

Note

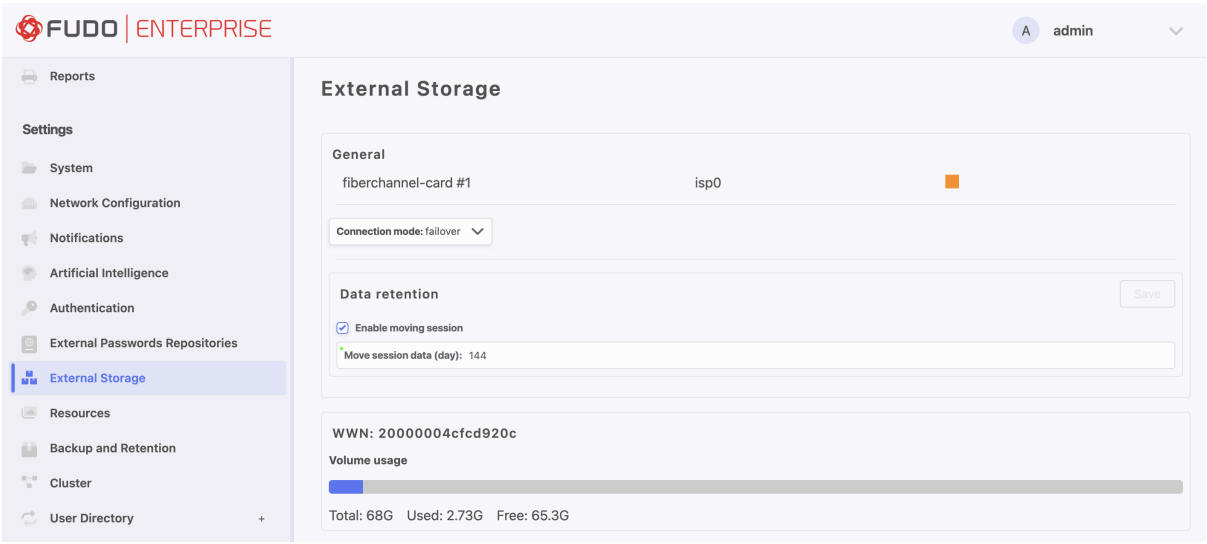
Fiber channel cards status is depicted by the icons.

- ■ - both fiber channel cards are operational.
- ■ - external storage volume is degraded - one of the fiber channel card is down.
- ■ - both fiber channel cards are down.

2. Select fiber channel cards operating mode.
   - Failover - data is transmitted using one fiber channel interface. If the card fails, the other one takes over ensuring continuous availability of the external storage device.
   - Load balancing - both fiber channel interfaces are used to transfer data between Fudo Enterprise and the external storage device.



3. In the *External storage devices* section, select the desired *WWN* object by clicking the *Select* button next to it.



Note

Click the ↻ icon to refresh the list of available storage devices.

4. Proceed with enabling *session data retention*.

Related topics:

- *Session Data Backup*

12.8 Resources

12.8.1 RDP/SSH/VNC Login Screen Configuration

Fudo Enterprise enables customizing RDP, SSH and VNC login screen.

RDP login screen customization

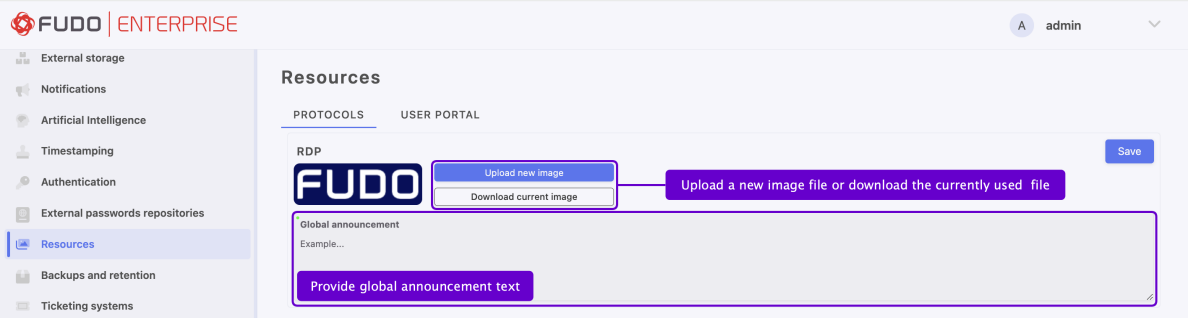
1. Select *Settings* > *Resources*.
2. Select the *Protocols* tab.
3. In the *RDP* section, click *Upload new image* button and select desired image.

Note

Maximum image size is 512 x 512 px.

4. Input the *Global announcement* text to appear as a message on the login screen.

> **Note**
>
> Login screen announcement can be four lines, up to 120 characters.



5. Click *Save*.

SSH login screen customization

1. Select *Settings* > *Resources*.
2. Select the *Protocols* tab.
3. In the *SSH* section, input *Global announcement* text to appear as a message on the login screen.

> **Note**
>
> Login screen announcement can be four lines, up to 120 characters.

4. Click *Save*.

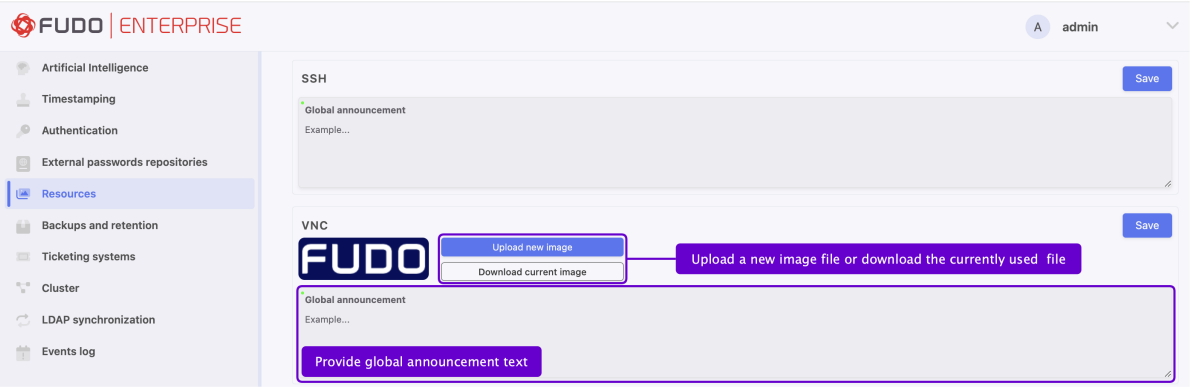
VNC login screen customization

1. Select *Settings* > *Resources*.
2. Select the *Protocols* tab.
3. In the *VNC* section, click *Upload new image* button and select desired image.

> **Note**
>
> Maximum image size is 512 x 512 px.

4. Input the *Global announcement* text to appear as a message on the login screen.

> **Note**
>
> Login screen announcement can be four lines, up to 120 characters.



5. Click *Save*.

12.8.1.1 Keyboard Layouts on the RDP Login Screen

When a user connects with a native RDP client, Fudo Enterprise translates the keystrokes it receives using the keyboard layout that the RDP client reports when the connection is established. There is no setting for this - the layout is detected automatically, and it is independent of the *Predefine Keyboard Layout* option described in *User Portal Configuration*, which applies to browser sessions only.

The detected layout determines:

- the characters produced on the Fudo Enterprise RDP login screen,
- the keystrokes saved in the session recording, and therefore the text found when searching sessions,
- the input matched by regular expression policies.

Fudo Enterprise translates the following keyboard layouts:

- *English (US)*,
- *French* (AZERTY),
- *German*, including the IBM and NEO variants,
- *Norwegian*,
- *Polish*, both the Programmers and the 214 variant,
- *Russian*, including the typewriter variant,
- *German (Swiss)*,
- *Turkish-Q*, and
- *English (UK)*, including the extended variant.

Note

Layouts that are not on the list are handled as *English (US)*. A user typing on such a layout will see different characters than expected on the login screen, and the keystrokes stored in the recording will not match what was typed.

Warning

Dead keys are not supported on the login screen. On layouts that place accents on dead keys - for example the circumflex and the diaeresis on the French and German layouts - the accented character cannot be composed, so a password containing such a character cannot be entered on the Fudo Enterprise login screen. Accented characters available directly on a single key, such as `é`, `è`, `ç`, `à` and `ù` on the French layout, are not affected. This limitation applies to the login screen only, not to the session with the target server.

Related topics:

- *Quickstart - RDP*
- *User Portal Configuration*

12.8.2 *User Portal* Configuration

12.8.2.1 Login Screen Configuration

Fudo Enterprise enables customizing information displayed on the *User portal* login screen.

1. Select *Settings* > *Resources*.
2. Select the *USER PORTAL* tab.
3. Click *Upload new image* button, browse the file system and select a custom logo for the *User portal* login screen.

Note

Maximum image size is 5 MB.

4. Provide the login screen announcement.

Note

Login screen announcement can be four lines, up to 120 characters.

5. Provide seller information.

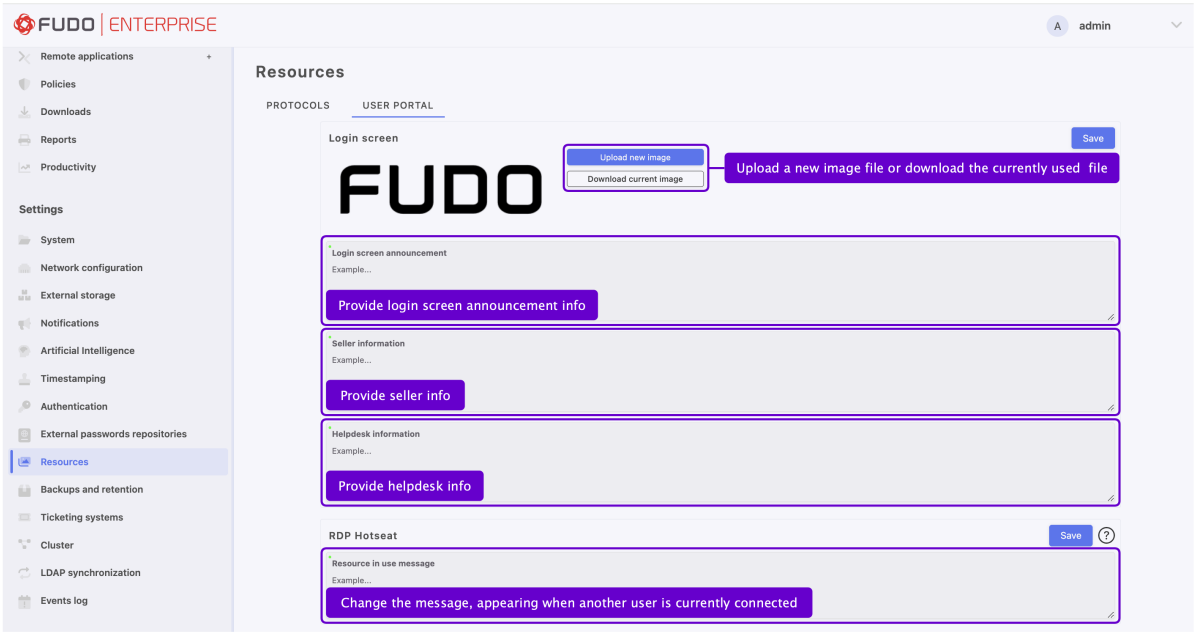
Note

Seller information can be five lines, up to 70 characters.

6. Enter help desk contact information.

Note

Helpdesk contact information can be five lines, up to 70 characters.



7. Provide information in the *Resource in use message* field. This information will be displayed to the user in the User Portal (Access Gateway) when trying to connect to the target server, another user will be already connected to that server via the same account.

Note

You can customize this message by including variables (`organization`, `phone`, `name`, `full_name`, or `email`.), enclosed in double %% symbols. E.g., `%%email%%`.

Warning

Resource in use feature is available for RDP connections only and can be configured while *Creating an RDP Server* by checking the *Inform about existing connection* option.

8. Click *Save*.

12.8.2.2 Predefined Keyboard Layout

Administrators can predefine the keyboard layout globally for the User Access Gateway:

1. Select *Settings* > *Resources*.
2. Select the *USER PORTAL* tab.

The following layouts are available:

- *English (US)*,
- *German*,
- *German (Swiss)*,
- *French* (AZERTY),
- *Norwegian*, and

- *Turkish-Q*.

Note

Each user can customize their keyboard layout individually in the User Access Gateway.

Warning

This setting applies to sessions established in the browser with the Web client. It does not affect connections made with a native RDP client - in that case Fudo Enterprise uses the keyboard layout reported by the client itself. Refer to the *RDP/SSH/VNC Login Screen Configuration* topic for the details.

Related topics:

- *User Access Gateway*
- *RDP/SSH/VNC Login Screen Configuration*

12.8.3 JiT Reason Formats

When sending an access request, the user provides a reason for it. By default this is free-form text, which makes the reason hard to process automatically - for example by an external ticket system that reads reasons submitted in Fudo Enterprise.

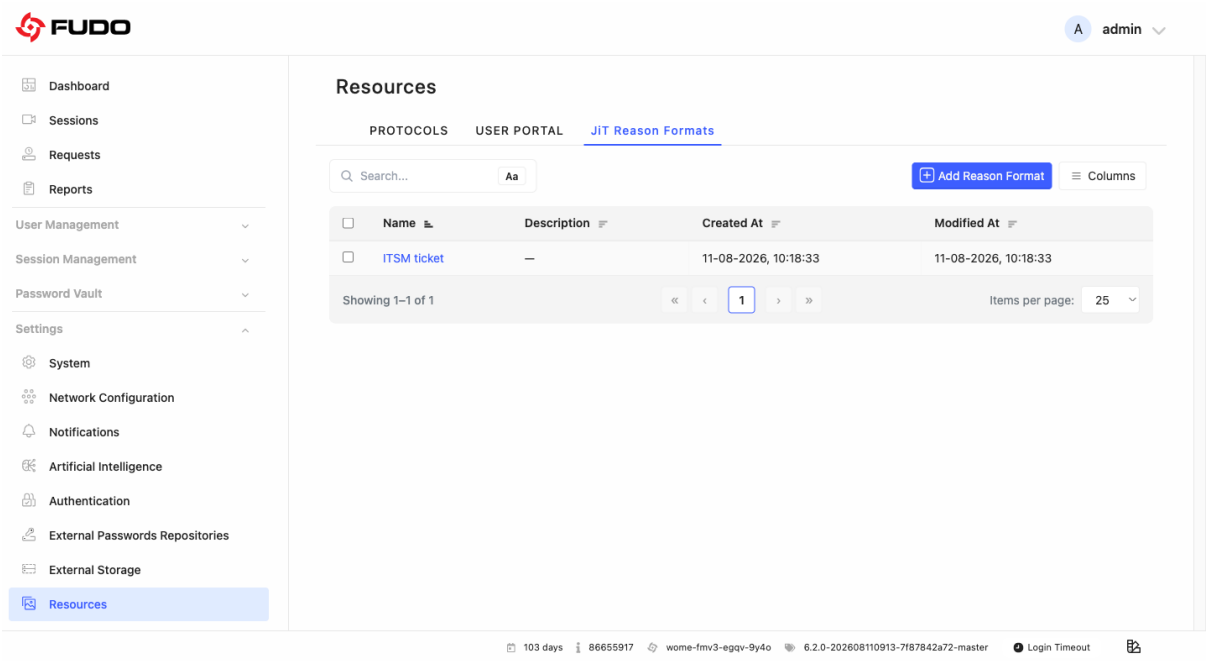
To obtain reasons in a predictable form, define a **reason format** - a named set of fields that the user fills in instead of writing free text. Fudo Enterprise validates the entered values and composes the reason itself, as one *field name: value* line per field.

Note

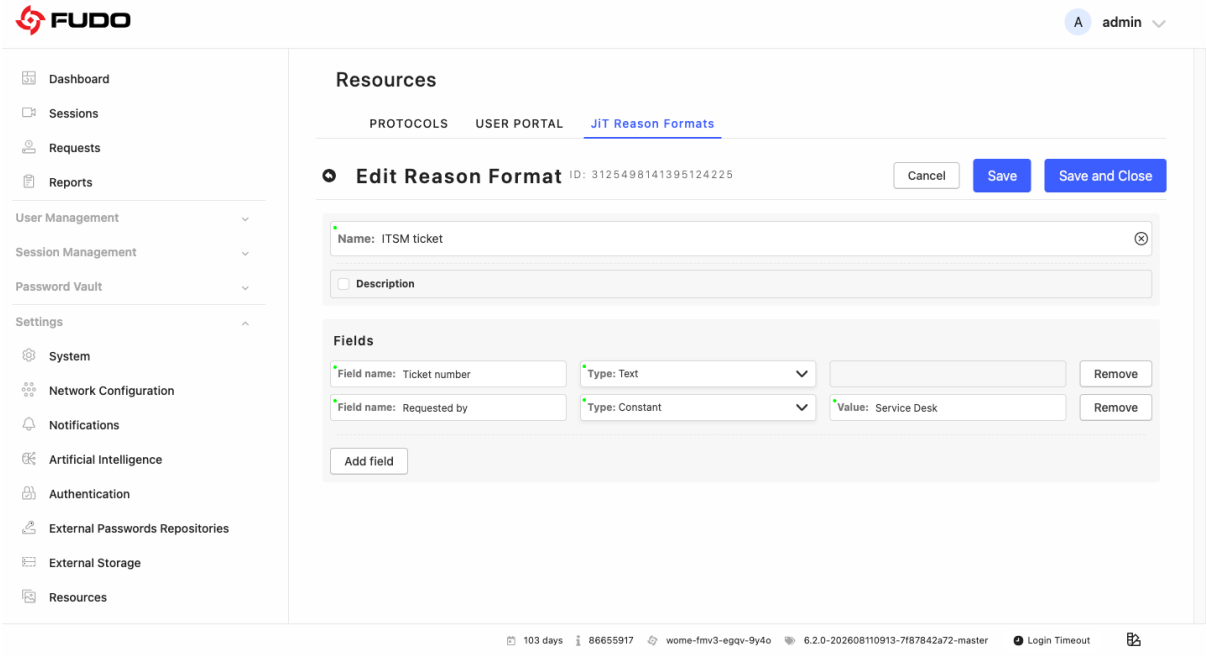
Defining formats does not change the existing behaviour. Free-form text remains available and is the default option, and as long as no format is defined, access requests work exactly as before.

12.8.3.1 Creating a Reason Format

1. Select *Settings* > *Resources* and go to the *JiT Reason Formats* tab.



2. Click *Add Reason Format*.
3. Enter the *Name* of the format. This is the name the user selects when sending a request.
4. Optionally select the *Description* option and describe the format. The description is displayed to the user after they select the format.
5. In the *Fields* section, enter the *Field name* and select the *Type* of the field:
   - *Text* - the user enters any text,
   - *Number* - the user enters a number,
   - *Constant* - a fixed value that you enter yourself in the *Value* field. The user does not fill it in and cannot change it.
6. Click *Add field* to add further fields, or *Remove* to delete a field.



7. Click *Save*.

Note

- **Every field of a format is required.** The user cannot send a request until all of them are filled in, so a composed reason never contains an empty value.
- **Fields appear in the order in which they were added.** The order cannot be changed later - to move a field, remove it and add it again.
- Field names, values of *Constant* fields and text entered by the user **cannot contain line breaks**, because line breaks separate the composed lines.

12.8.3.2 Scope and Limitations

Note

- Defined formats are available for **all** requests for access to accounts and resources. They cannot be limited to a selected safe.
- Formats are not available for requests for access to secrets in the Password Vault, nor for requests coming from another Fudo Enterprise connected through *Fudo ShareAccess*. Those requests keep a free-form reason.
- A free-form reason may be up to 250 characters long; a reason composed from a format may be up to 1024 characters.
- The stored reason is ordinary text. It does not record which format was used, so it cannot be proven from the reason alone that a format was applied.

Warning

Managing reason formats requires the `access-request-modify` privilege. Viewing them requires `access-request-read`.

Related topics:

- *Access Requests*
- *Resources*

12.9 Backup and Retention

12.9.1 Session Data Backup

Warning

Session data backup contains confidential information.

Fudo Enterprise allows configuring multiple backup target destinations, where data can be stored. Each backup target can have Backblaze, FTP, S3, or SFTP as a destination place.

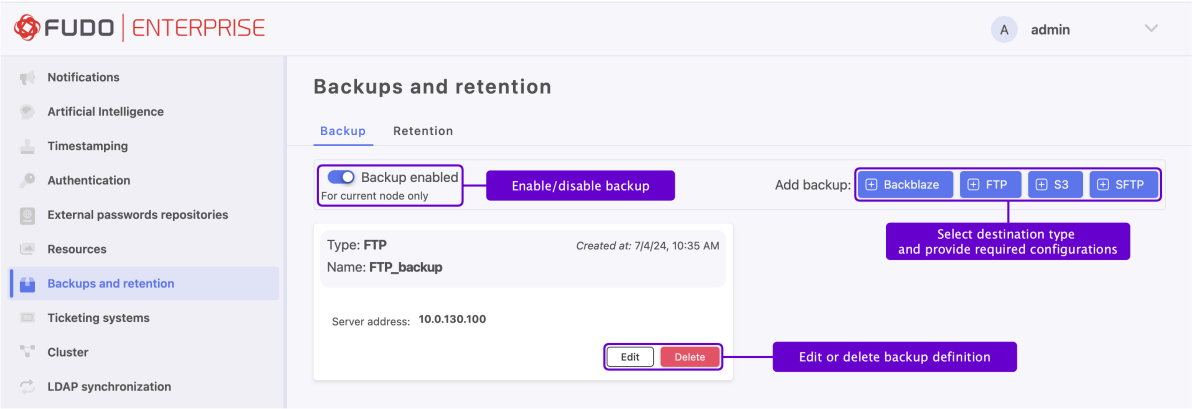
To enable automated backups service, proceed as follows.

1. Select *Settings* > *Backup and retention*.
2. Select *Backup enabled* option. Please note that in case of the configured cluster, this option enables backup for the current node only.
3. In the *Add backup* field click desired backup type button in order to configure your future backup target place: *+Backblaze, +S3, +FTP* or *+SFTP*.
4. Set a name for your backup target.
5. Provide additional data depending on the selected connection type:

- Configuring a **Backblaze** backup target, provide: *Bucket, Directory,* and credentials, such as *Account* and *Key*.
- For **FTP** type backup target provide: *Server address (IP address or host address), Directory,* and credentials, such as *Username* and *Password*.
- With **S3** type chosen, provide additionally: *Bucket, Directory, Access key, Secret Access key, Region* and *Endpoint*.

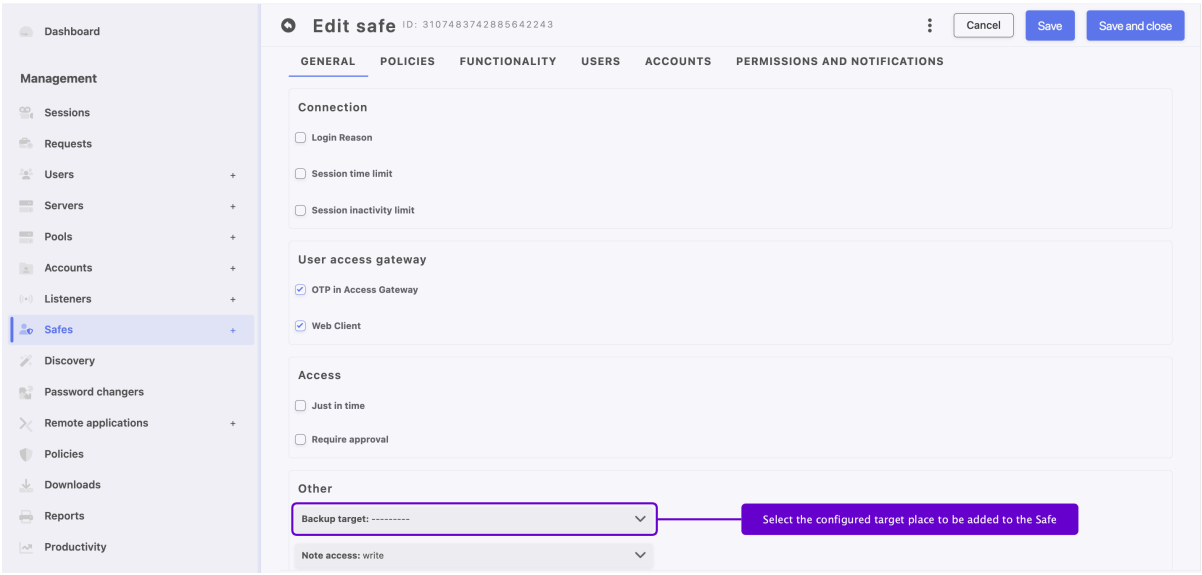
> **Note**
>
> The bucket must already exist in your S3 provider - Fudo Enterprise does not create it. If the bucket given in *Bucket* is missing, or its name is mistyped, archiving to this target fails with `NoSuchBucket`. The account whose credentials you provide does not need the `s3:CreateBucket` permission.

- For **SFTP** type backup target provide: *Server address (IP address or host address), Username, Directory, User private key, Server public key,* and *Port* number.

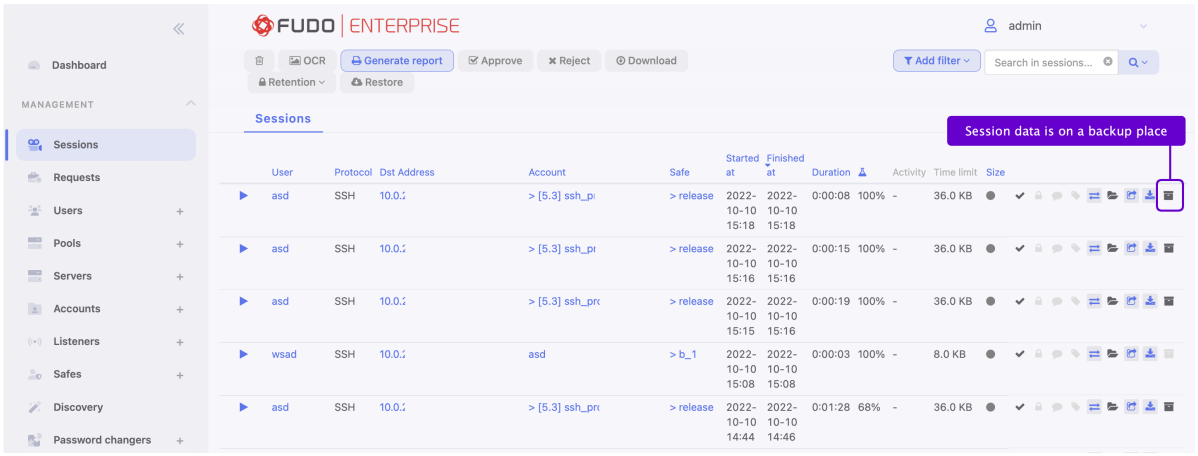


7. Click *Save*.

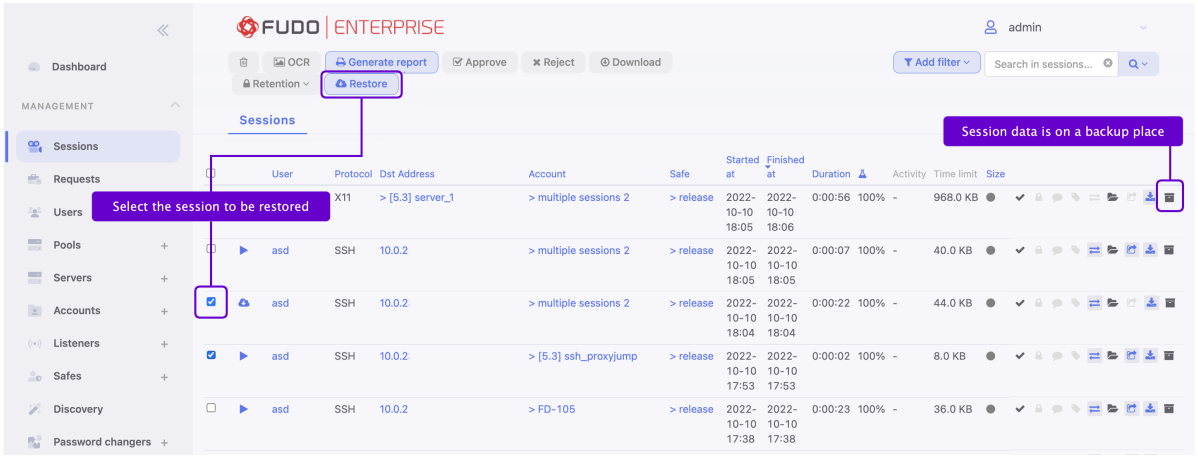
Now, the configured *Backup target* can be added to the Safe settings to enable automatic storing the sessions and safe data in the defined target place.



Sessions data that was sent to the backup target place is assigned with the respective icon on the Sessions list.



If the session has its backup version stored outside of Fudo Enterprise, it can be downloaded from the backup place to the Fudo Enterprise local instance with the *Restore* option.



Restoring system from backup

System restore service is provided by the technical support department on terms agreed in the

SLA.

Related topics:

- *Exporting/Importing System Configuration*
- *Security measures*
- *Creating a new safe*

12.9.2 Data Retention

Fudo Enterprise supports two data retention scenarios depending on the availability of external storage:

- **Two-steps retention:** Initially, data is transferred from the internal storage to external storage connected via a fiber channel interface. After defined time period session data is automatically deleted.
- **One-step retention:** If external storage is not used, sessions will be immediately deleted from Fudo Enterprise.

For more information on configuring the external storage, see the *External Storage* chapter.

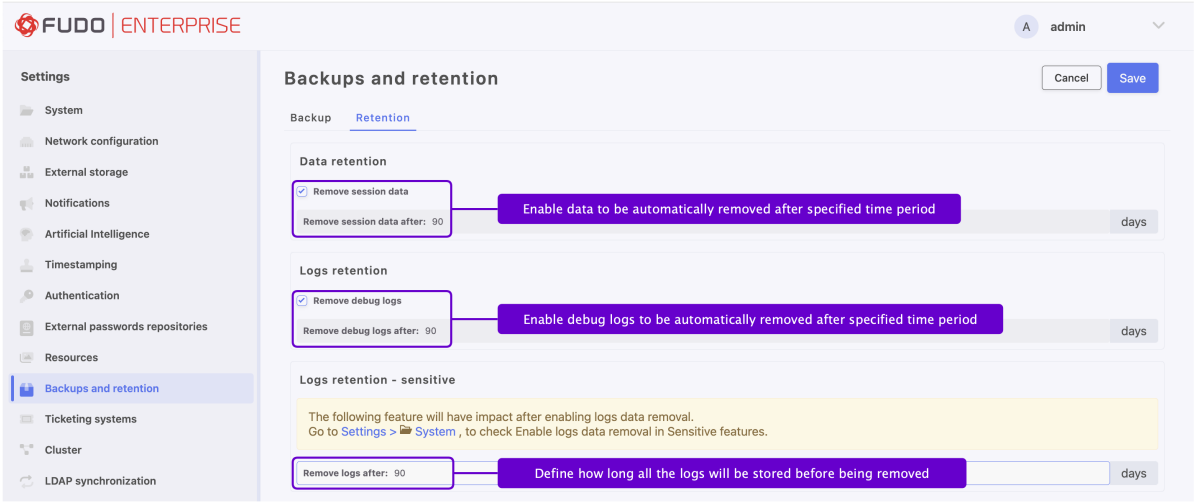
> **Note**
>
> Sessions which have been exported and the content is still available for download, will not be deleted automatically. These sessions must be either *deleted manually* or you must delete the exported material in the *Downloads* section for the retention mechanism to delete those session.

Enabling data retention

To enable data retention service, proceed as follows.

1. Select *Settings* > *Backup and retention* > *Retention*.
2. Select *Remove session data* option in the *Data retention* section to have the data automatically removed after specified time period.
3. Define how long data will be stored before being removed.
4. Select *Remove debug logs* option in the *Logs retention* section to have the debug logs automatically removed after specified time period.
5. Define how long debug logs will be stored before being removed. Default value is 90 days.
6. In the *Logs retention - sensitive* section define how long all the logs will be stored before being removed.

> **Warning**
>
> The following feature will have impact after enabling logs data removal. Go to *Settings* > *System* to check *Enable logs data removal* option in the *Sensitive features and system security* section.

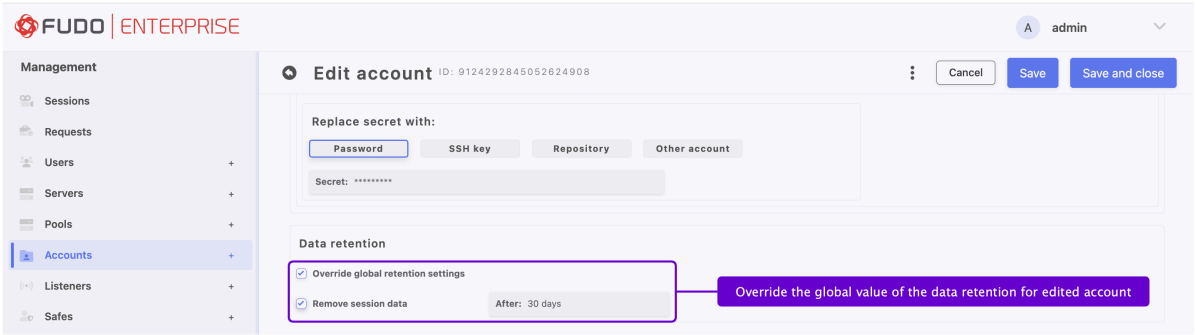


7. Click *Save*.

Overwriting the global value of the data retention for accounts

It is possible to overwrite the value of the data retention parameter for the selected account. To specify the value of the data retention parameter in the account settings, proceed as follows.

1. Select *Management* > *Accounts*.
2. Find and click desired object's name to open its configuration page.
3. In the *Data retention* section, define automatic data removal settings.
   - Select *Override global retention settings* option to set other than global retention values for connections established using this account.
   - Check the *Delete session data* option to exclude sessions from retention mechanism.
   - Next to the *Delete session data* field, define the number of days after which the session data will moved to external storage device. Default value when the option is checked, is 30 days.



4. Click *Save*.

Note

- Defining the retention parameter value in the account settings will not activate data retention itself. Data retention has to be enabled globally (from the menu *Settings* > *Backup and retention* > *Retention*).

- Global retention parameter values have lower priority than the values set in the *accounts*.
- Global retention settings are replicated within the *cluster configuration*. Please note that *Remove session data after* variable is not replicated within the cluster but is set per node.

Sessions' retention lockdown

Fudo Enterprise allows for excluding selected sessions from the retention mechanism. Session exclusion procedure is described in chapter *Sessions' retention lockdown*.

Related topics:

- *Security measures*
- *Exporting/Importing System Configuration*
- *Creating a new safe*

12.10 Cluster Configuration

12.10.1 Session Data Replication and Behavior in the Event of a Node Failure

Fudo Enterprise cluster ensures uninterrupted access to servers in case of cluster node failure as well as enables implementing static load balancing scenarios.

Warning

- Cluster configuration does not facilitate data backup. If session data is deleted on one of the cluster nodes, it is also deleted from other nodes.
- Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances **must not** be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

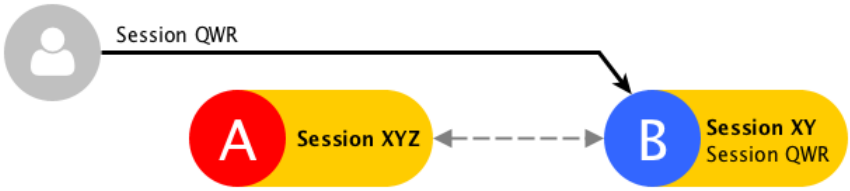
Data replication between cluster nodes is highly customizable. The administrator can choose the node that the data will be replicated to as well as which data (data model objects/session data) is replicated.

In case of a node failure, user access requests will be picked up by another cluster node, determined by the *redundancy group priority*.

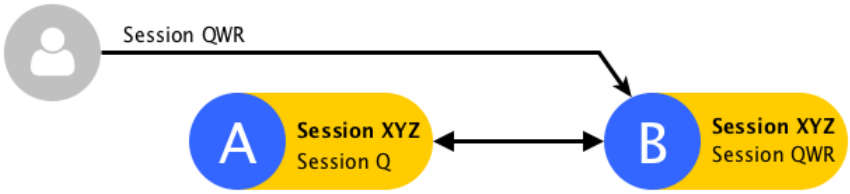
Current session data is replicated to other nodes while the connection is still ongoing.

If the node that fails was recording sessions, those sessions will be terminated...

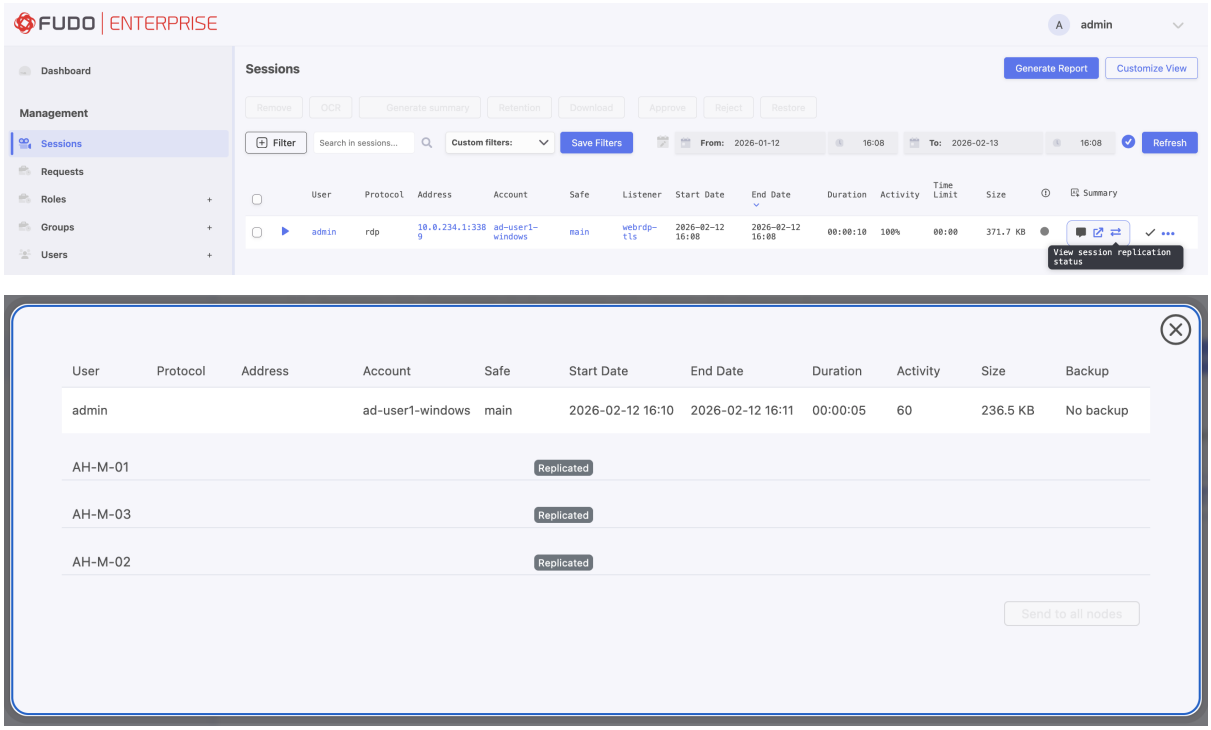
. . . and users will have to reconnect.



A part of the session data from the node that malfunctioned, which has synchronized, can be accessed on the other nodes, but the session will be fully accessible once the node becomes operational and session data is synchronized between cluster nodes.



Session replication status can be verified by clicking the ⇄ icon on the sessions list.



Related topics:

- *Cluster Initialization*
- *Editing Cluster Nodes*

- *Removing Cluster Nodes*
- *Redundancy Groups*

12.10.2 Cluster Initialization

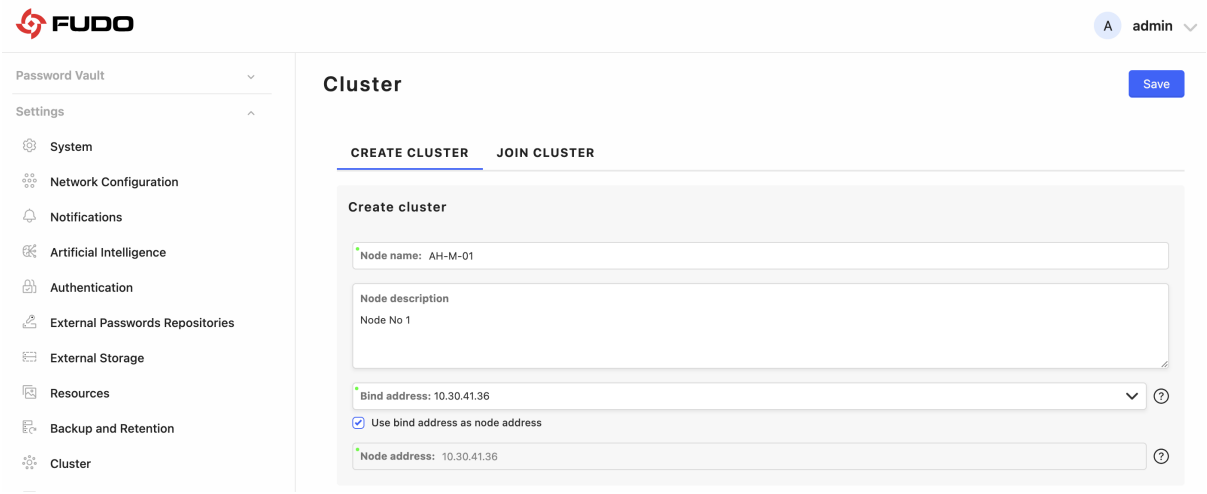
The cluster is created on the first node (Fudo Enterprise instance). Data from this node will be copied to the remaining nodes that belong to the cluster.

Warning

- Proper cluster operation requires configuring the *NTP time server* on all cluster nodes. It is recommended to configure **the same NTP servers** on all nodes.
- Make sure that the **license allows cluster creation**. If not, upload the appropriate license (the cluster node limit must be greater than or equal to the number of nodes after cluster expansion).
- Ensure that port `65522` is open between the node addresses dedicated to cluster communication.

To initialize a Fudo Enterprise cluster, follow the instructions below.

1. From the left menu, select *Settings* > *Cluster*.
2. Go to the *CREATE CLUSTER* tab.

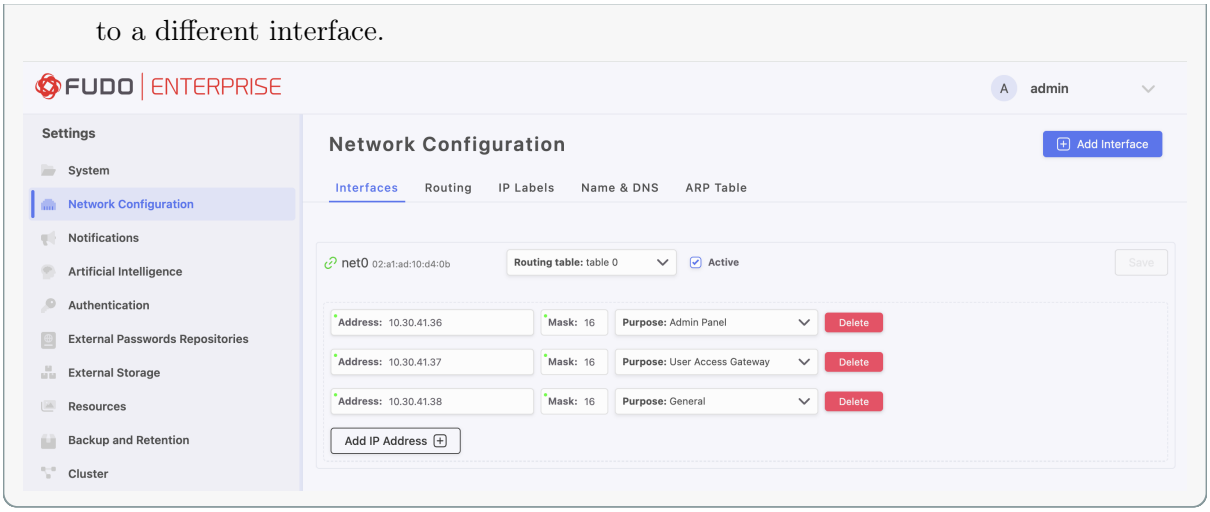


3. Enter a name for the node being created and a description to help identify it.
4. From the *Bind address* drop-down list, select the local IP address that this node will use for outbound cluster traffic (replication). Select *Any* to let the node choose the outbound address automatically.

Note

- The bind address must be configured on one of this node's network interfaces and have the *General* function assigned in the *network settings*.
- In the example below, the same IP address is used as for the Admin Panel. However, the cluster communication address may belong to a different subnet and be assigned

to a different interface.



5. Specify the address that the other cluster nodes will use to reach this node:
   - Leave the *Use bind address as node address* option selected (default) when the bind address is directly reachable by the other nodes. The *Node address* field is then filled in automatically and cannot be edited.
   - Clear the *Use bind address as node address* option when the other nodes reach this node through a different address - for example when there is NAT in front of Fudo Enterprise. Then enter that address (e.g. the public or NAT-translated address) in the *Node address* field.

Note

Separating the node address from the bind address prevents replication failures in NAT environments, where the address that other nodes use to reach this node does not exist on the node's local interfaces and therefore cannot be used as the outbound (bind) address.

6. Click *Save* to initialize the cluster.

Note

The next step in configuring the cluster environment is to add additional node(s) to the cluster. Proceed to the *Adding Cluster Nodes* section.

Related topics:

- *Adding Cluster Nodes*
- *Editing Cluster Nodes*
- *Removing Cluster Nodes*
- *Redundancy Groups*
- *Cluster Configuration*

12.10.3 Adding Cluster Nodes

Adding a new node to an existing cluster results in its full synchronization with the initial node. This process includes clearing local data and restoring configuration and data based on information replicated from the cluster.

Warning

- Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances **must not** be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.
- Session data and configuration parameters (*servers*, *users*, *accounts*, *safes*, *listeners*, *external authentication servers*) of the node being joined to the cluster **are deleted**. After joining, the node is initialized with data replicated from the cluster.
- In environments containing a large amount of data, the initialization and data copying process to the joining node **may take several hours**.

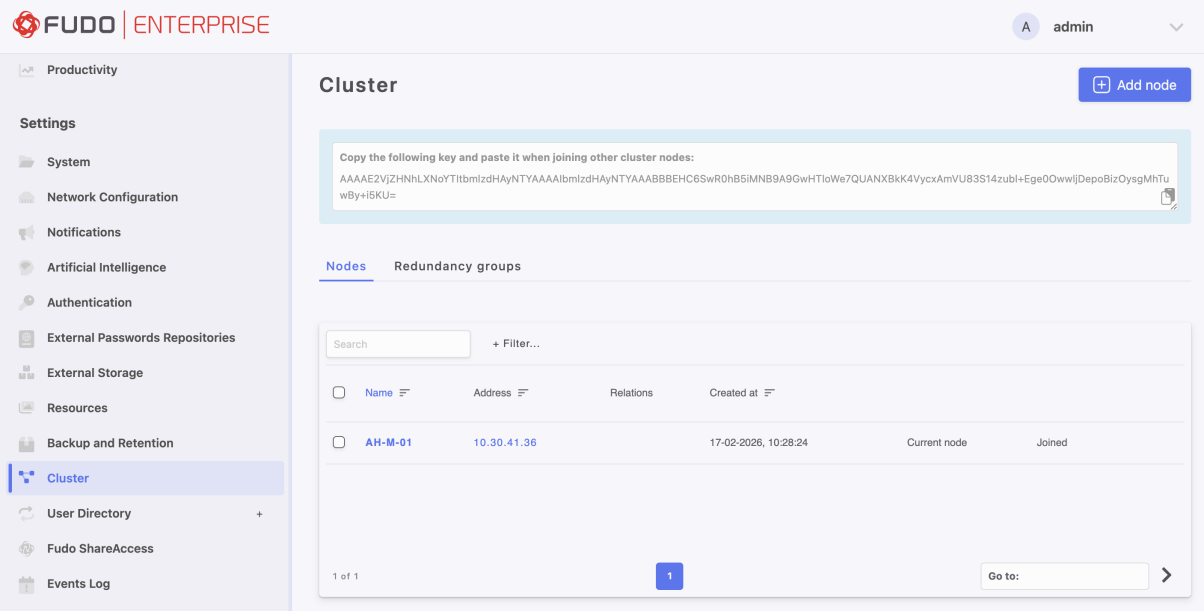
Danger

- The mechanism of joining a node to the cluster **relies on completely wiping its data** and copying data from the node on which the cluster was initialized.
- Incorrect configuration of relationships between nodes or skipping any step of the procedure may lead to irreversible damage to the joining node. In such a case, the synchronization process will not be completed.
- Some configuration elements (e.g., SMTP) are not replicated between cluster nodes and must be configured manually on each node.

12.10.3.1 Cluster Initialization and Adding Nodes

To add a node to the Fudo Enterprise cluster, follow the instructions below.

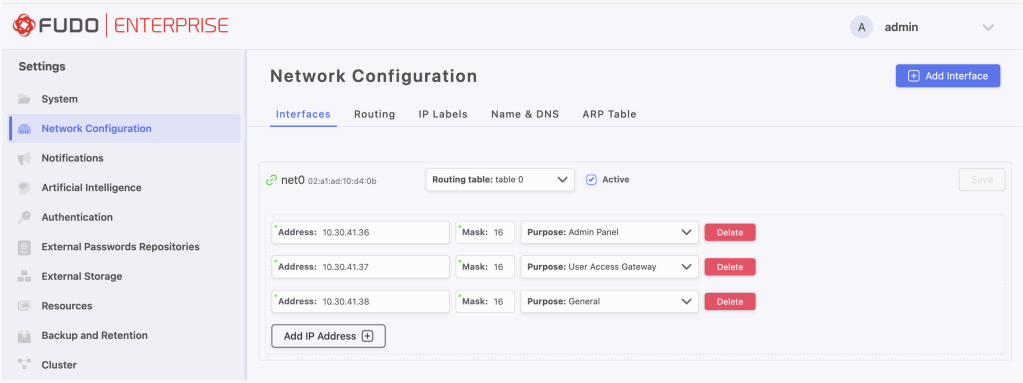
1. Log in to the Fudo Enterprise Administration Panel where the cluster was *initialized* — the **initial node**.
2. From the left menu, select *Settings* > *Cluster*.
3. Click *Add node*.

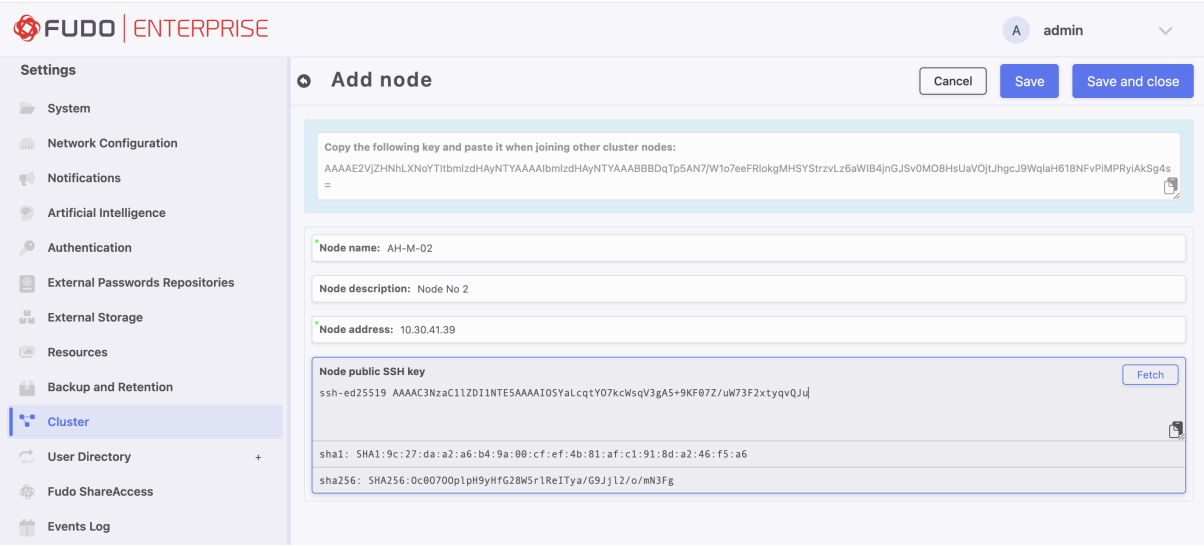


4. Enter the node name and a description to help identify the node.
5. Provide the IP address of the node being added (that is, the Fudo Enterprise instance to which data from the initial node will be replicated).

Note

The address of the joining node must have the *General* role set in the network settings. For more information about configuring network settings, see *Network Interfaces Configuration*.





6. Click *Fetch* to download the node's SSH public key.
7. Click *Save and close*.
8. Repeat steps 3–7 if you want to add additional nodes.

Note

In scenarios where secret changers are used, at least two active cluster nodes are required for them to operate. In a two-node environment, the failure of a single node causes secret changers to stop working; therefore, a **three-node configuration** is recommended.

12.10.3.2 Setting Relationships Between Nodes

Note

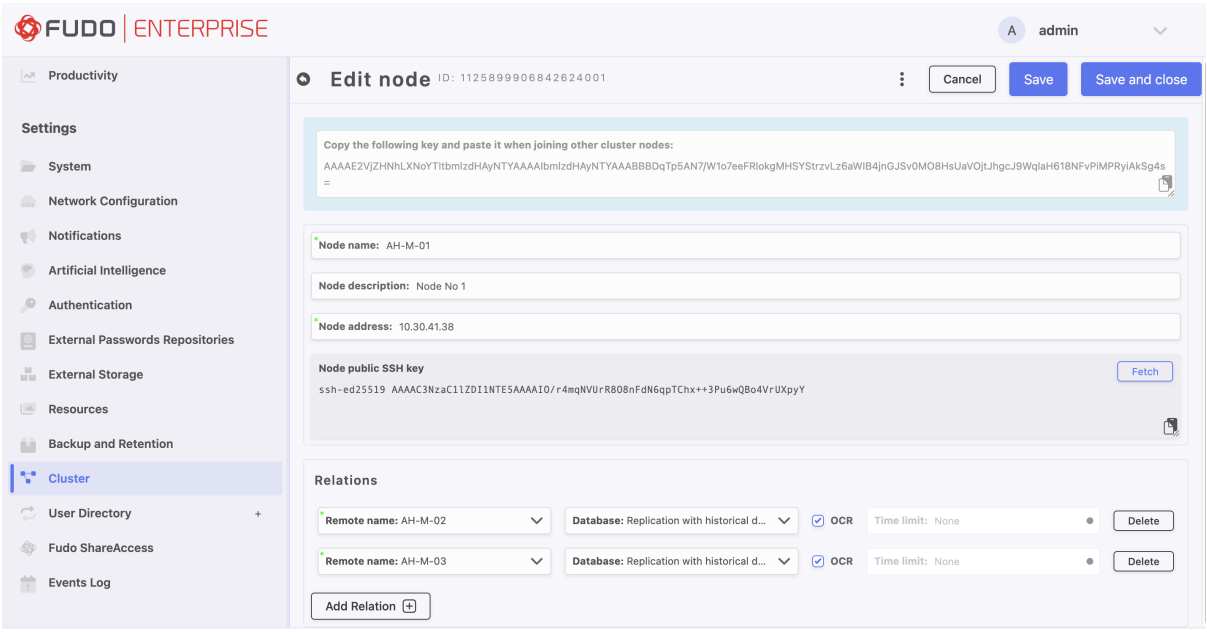
- The recommended cluster configuration is to define bidirectional relationships between nodes. It is not required to configure relationships between every pair of nodes; however, no node may remain without at least one defined relationship.
- In a topology where nodes are not connected in a "full mesh" (each node connected to every other node), be aware of the limitations regarding session data replication. In such configurations, session data is replicated only between nodes that have a defined relationship.

Warning

Creating relationships is essential to ensure that data is replicated between nodes.

1. Click the name of the first node to edit it.
2. In the *Relations* section of the edited node, click the *Add Relation* + button.
3. From the *Remote name* list, select the node to which data from the node you are currently logged in to (in this case, the primary node) will be replicated.

4. From the *Database* list, select which data should be replicated to the selected cluster node.
5. Select the *OCR* option to allow the selected node to process excess graphical sessions.
6. Click *Save and close*.
7. Edit the remaining nodes and Add Relations to the other nodes in the cluster as described above.



Important

The option selected from the **Database** list determines the scope of replicated data:

- **Replication** — only configuration data (users, servers, accounts, safes, listeners, external authentication servers) and session metadata are replicated. **Session material, logs and reports are not transferred to the remote node.**
- **Replication with new session data** — logs, material of sessions recorded after the relation was created and **reports** are replicated as well.
- **Replication with historical data** — as above, and additionally sessions recorded locally before the relation was created are transferred retroactively to the remote node.

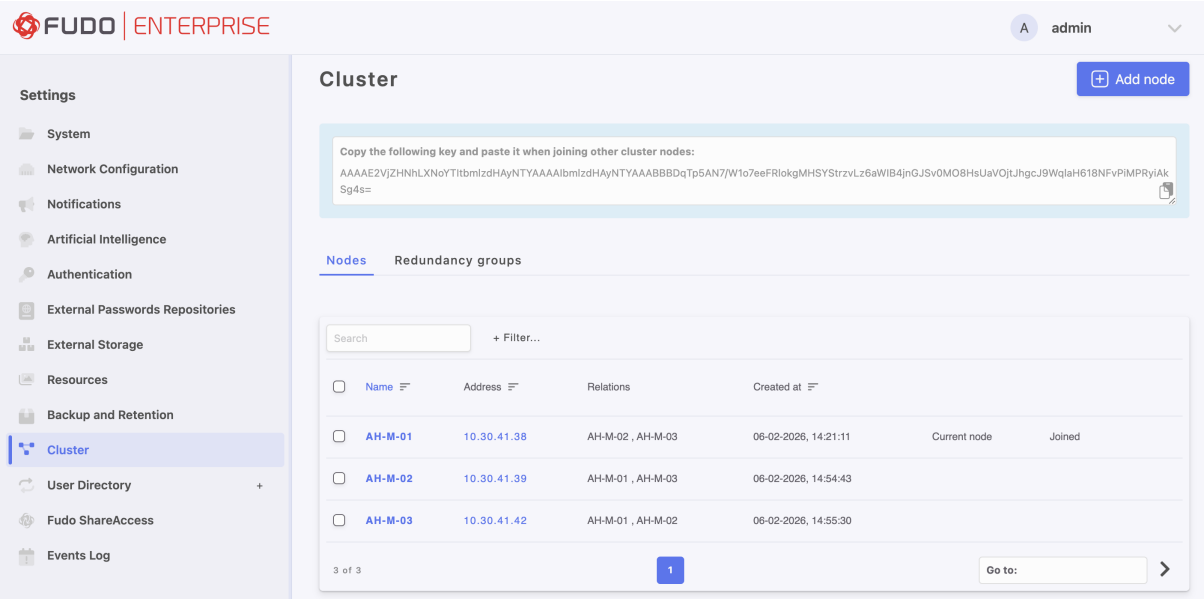
If reports generated on one node are not visible on the other nodes, check whether the relation between the nodes has been set to **Replication** only.

Note

Each Fudo Enterprise instance has a license-defined limit on the number of OCR processes used to process graphical sessions. The *OCR* option allows delegating the processing of excess sessions to the selected node when the number of connections exceeds the number of local processes responsible for processing and indexing content.

12.10.3.3 Linking Nodes with the Initial Node

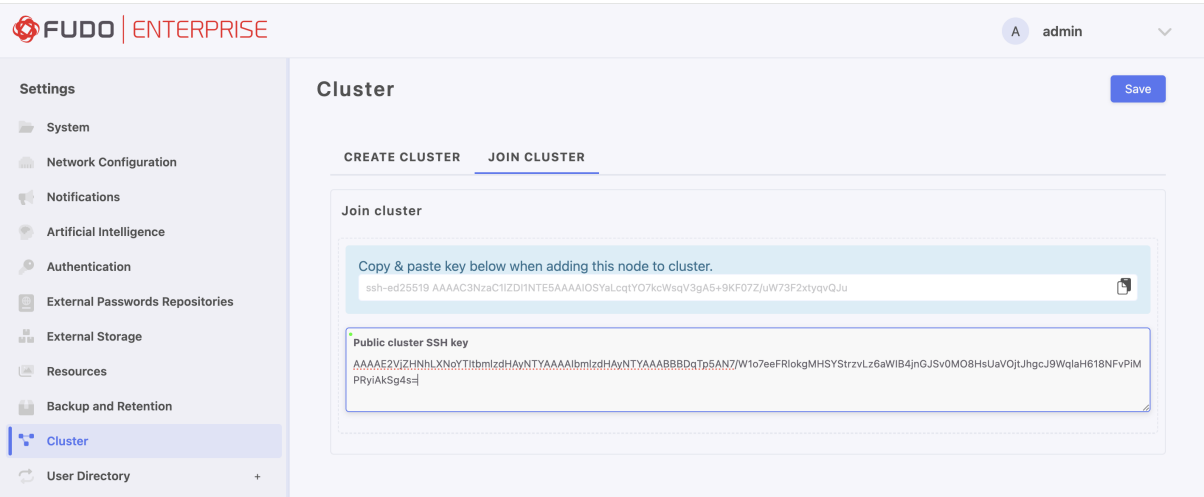
1. Make sure you are in the Fudo Enterprise Administration Panel where the cluster was initialized.
2. Go to the main view of the *Cluster* tab.
3. Copy the cluster SSH public key.



4. Log in to the Administration Panel of the joining node.

> **Note**
>
> You can use the shortcut by clicking the address of the selected node in the list of added nodes in the cluster view.

5. From the left menu, select *Settings* > *Cluster*.
6. Go to the *JOIN CLUSTER* tab.



7. Paste the copied key into the *Cluster SSH public key* field.
8. Click *Save*.

Warning

After accepting the data wipe warning, all data on this node will be deleted.

9. Read the data wipe message and click *I understand the consequences. Proceed.*
10. Wait until the cluster is initialized and the objects are copied between cluster nodes.

Note

The added node will be restarted. If disk encryption is used (USB key or password), connect the key or provide the password in the hypervisor terminal.

12.10.3.4 Cluster Initialization Completion Verification

The cluster initialization time depends on the amount of data on the initial node. For a new, unused instance, the process may take several minutes. In environments containing large amounts of data (e.g., logs, session recordings), initialization may take from several hours to several days.

After replication is complete, log in to the newly added node and verify synchronization by:

- checking the cluster node status on the Dashboard,
- analyzing the event log,
- verifying cluster settings.

Additionally, it is recommended to confirm replication of configuration data (e.g., users, servers) by reviewing the appropriate tabs in the administrative interface.

Completion of the initial replication is confirmed by log entries on the initial node (the one where the cluster was created):

- `Initial objects replication to cluster node <name> completed.`
- `Initial logs replication to cluster node <name> completed.`

Related topics:

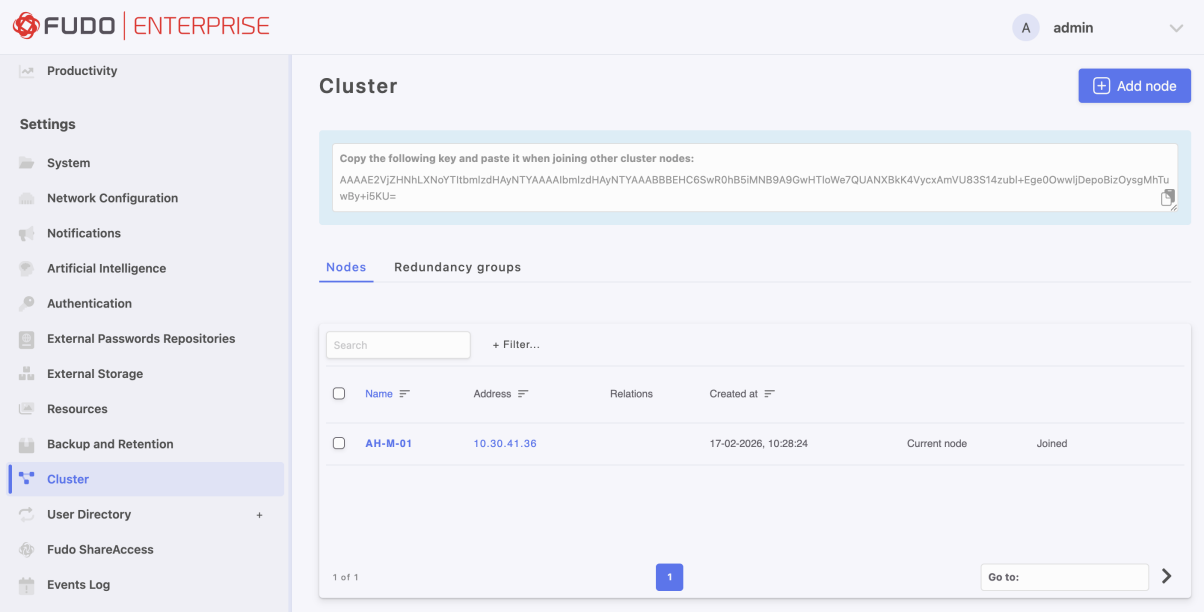
- *Editing Cluster Nodes*
- *Removing Cluster Nodes*
- *Cluster Security Configuration*

12.10.4 Cluster Expansion with New Nodes

Note

Cluster expansion requires following the procedure strictly according to the steps below.

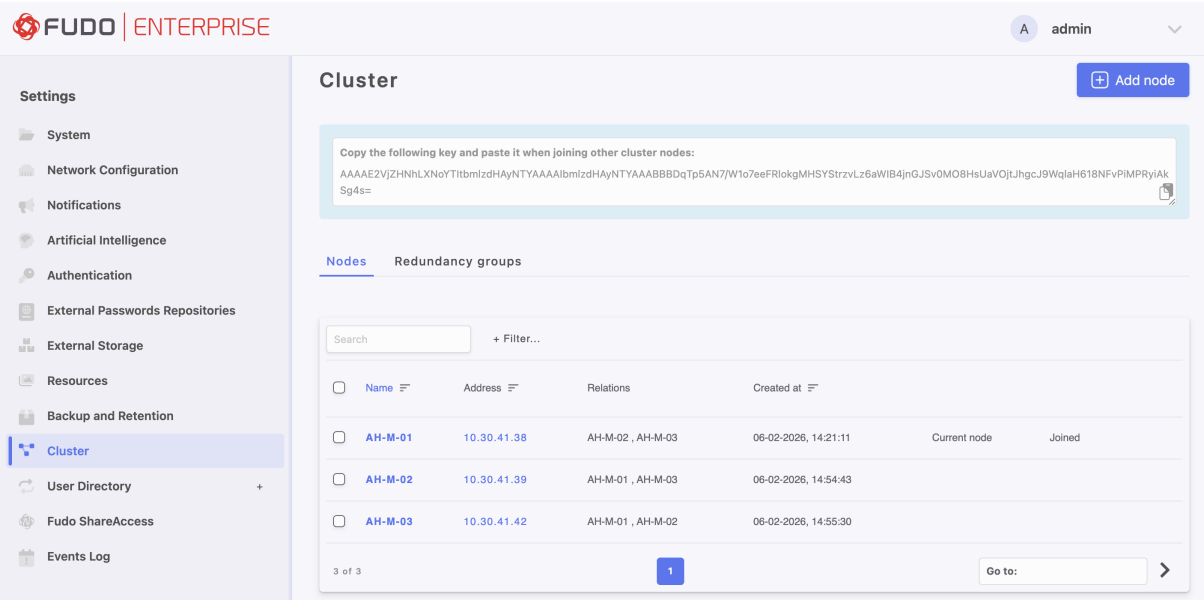
1. Log in to the Fudo Enterprise Administration Panel where the cluster was *initialized* — that is, the **primary node**.
2. From the left menu, select *Settings* > *Cluster*.
3. Click *Add node*.



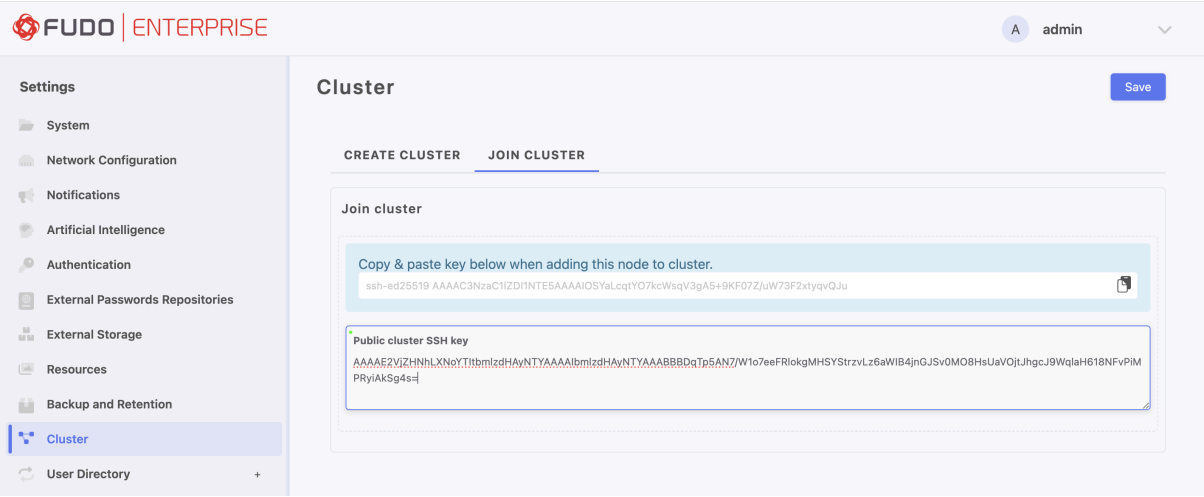
4. Enter the node name and a description to help identify the joining node.
5. Provide the IP address of the node being added.

> **Note**
>
> The address of the joining node must have the *General* role set in the *network settings*. For more information about configuring network settings, see *Network Settings: Network Interface Configuration*.

6. Click *Download* to download the node's SSH public key.
7. Click *Save*.
8. Add relationships between the remaining nodes (it is recommended to add relationships with all nodes).
9. Edit each of the remaining cluster nodes and add a relationship with the newly added node (a "full mesh" configuration is recommended).
10. Click *Save and close*.
11. Go to the main view of the *Cluster* tab.
12. Copy the cluster SSH public key.



13. Log in to the Administration Panel of the joining node.
14. From the left menu, select *Settings* > *Cluster*.
15. Go to the *JOIN CLUSTER* tab.



16. Paste the copied key into the *Cluster SSH public key* field.
17. Click *Save*.

Warning

After accepting the data wipe warning, all data on this node will be deleted.

18. Read the data wipe message and click *I understand the consequences. Proceed.*
19. Wait until the cluster is initialized and the objects are copied between cluster nodes.

Note

The added node will be restarted. If disk encryption is used (USB key or password), connect

the key or provide the password via the hypervisor terminal.

Related topics:

- *Cluster Initialization*
- *Editing Cluster Nodes*
- *Removing Cluster Nodes*
- *Cluster Security Configuration*

12.10.5 Editing Cluster Nodes

To modify the configuration of a Fudo Enterprise cluster node, follow the instructions below.

1. From the left menu, select *Settings* > *Cluster*.
2. In the list of nodes, find the node you want to edit and click its name.
3. Modify the node data as needed.
4. Click *Save*.

Related topics:

- *Adding Cluster Nodes*
- *Removing Cluster Nodes*
- *Security: Cluster configuration*

12.10.6 Removing Cluster Nodes

Warning

- Removing a node and re-adding it to a cluster may result in data loss.
- After removing a node, you will no longer be able to delete session data recorded by this node and replicated to other nodes.
- Such a disconnected node **MUST NOT** be added/reconnected to the cluster again.

Danger

If it is necessary to remove a node, we recommend contacting the **Fudo Technical Support Team** before starting any actions.

12.10.6.1 Removing a Node from the Cluster

To remove a node from the Fudo Enterprise cluster, follow the instructions below.

1. Log in to the Fudo Enterprise Administration Panel.
2. From the left menu, select *Settings* > *Cluster*.

3. In the node list, locate the node you intend to remove.
4. Select the *Delete* option next to the chosen cluster node.
5. Click *Save*.

12.10.6.2 Rejoining a Removed Node

> **Warning**
>
> If it is necessary to reconnect a removed node to the cluster, the node must be **reset to factory settings** from the terminal in accordance with the procedure described in *Resetting Configuration to Default Settings*, and only then rejoined to the cluster according to the instructions in *Adding Cluster Nodes*.

Related topics:

- *Adding Cluster Nodes*
- *Editing Cluster Nodes*
- *Security: Cluster configuration*

12.10.7 Redundancy Groups

Redundancy groups enable high-availability scenarios. In the event of a failure of the node acting as the master for a given redundancy group, the IP addresses assigned to that group are taken over by another node with the highest priority within that group. Assigning different priorities to redundancy groups on individual cluster nodes allows for static load balancing while maintaining high-availability functionality.

> **Note**
>
> The redundancy group configuration options are available after the cluster has been initialized.

Adding Redundancy Groups

To add a redundancy group, follow the instructions below.

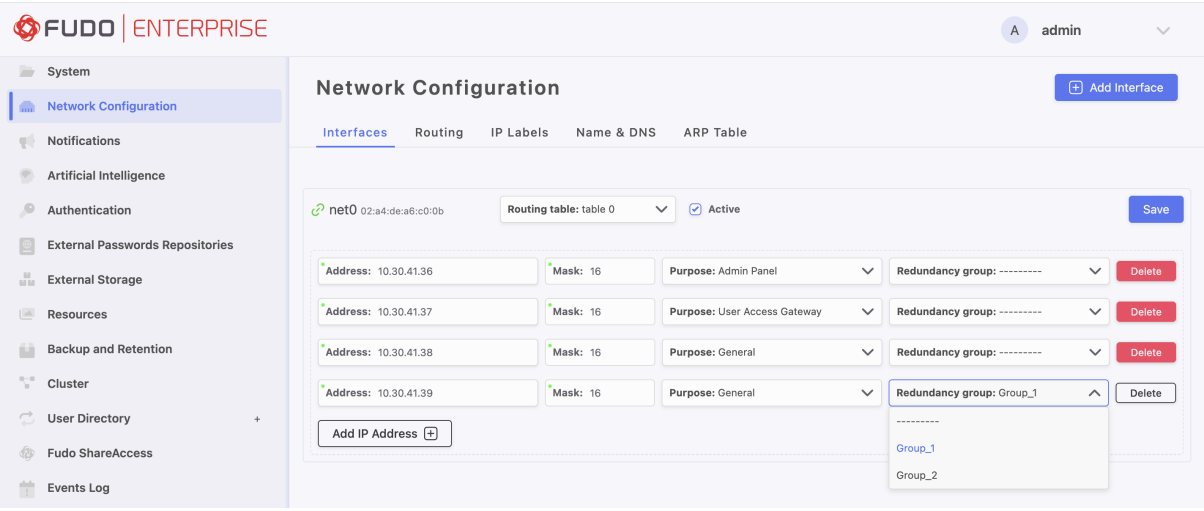
1. From the left menu, select *Settings* > *Cluster*.
2. Go to the *Redundancy Groups* tab.
3. Click *+ Add group*.
4. Define the group parameters:
   - **Name** – the name of the redundancy group.
   - **ID** – the redundancy group identifier (allowed range: 1–255).
   - **Priority** – the redundancy group priority (allowed range: 0–254). A lower parameter value indicates a higher priority.

- **Network interface** – the network interface used by the redundancy group to communicate with other cluster nodes.

Note

- Redundancy group with higher priority assumes the **master** role and handles all requests to monitored servers accessed through IP addresses assigned to this group. In case given cluster node crashes, user requests are directed to on of the remaining nodes with the highest priority defined for given redundancy group.
- The **network interface** (interlink interface) is used to monitor the state of a given redundancy group. The master node broadcasts keep-alive packets over the Layer 2 network to inform other nodes that it is active and operational. The remaining cluster nodes use the interlink interface to listen for these packets.
- All cluster nodes must have their interlink interfaces connected to the same broadcast domain (VLAN). Additionally, in VMware-based environments, the vSwitch security settings must be adjusted to allow MAC address changes and forged transmits.
- By default, once a node takes the *master* role, it will continue on indefinitely as the *master* node.

5. Click *Save and exit*.
6. From the left menu, select *Settings* > *Network configuration*.
7. Click *Add IP address* + to add an IP address.
8. Enter the IP address and select the *General* function to assign the cluster attribute.
9. From the drop-down list, select the previously defined redundancy group.
10. Click *Save*.



Note

The cluster IP address must be defined on each cluster node.

Editing Redundancy Groups

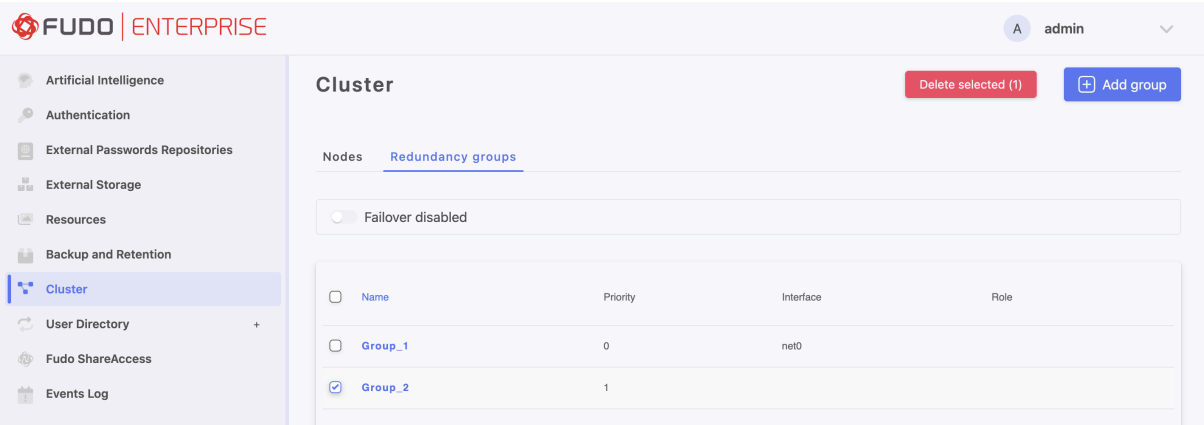
To modify a redundancy group, follow the instructions below.

1. From the left menu, select *Settings* > *Cluster*.
2. Go to the *Redundancy Groups* tab.
3. Modify the parameters of the selected redundancy group.
4. Click *Save and exit*.

Removing Redundancy Groups

To remove a redundancy group, follow the instructions below.

1. From the left menu, select *Settings* > *Cluster*.
2. Go to the *Redundancy Groups* tab.
3. Select *Remove selected* for the chosen redundancy group.
4. Click *Confirm*.



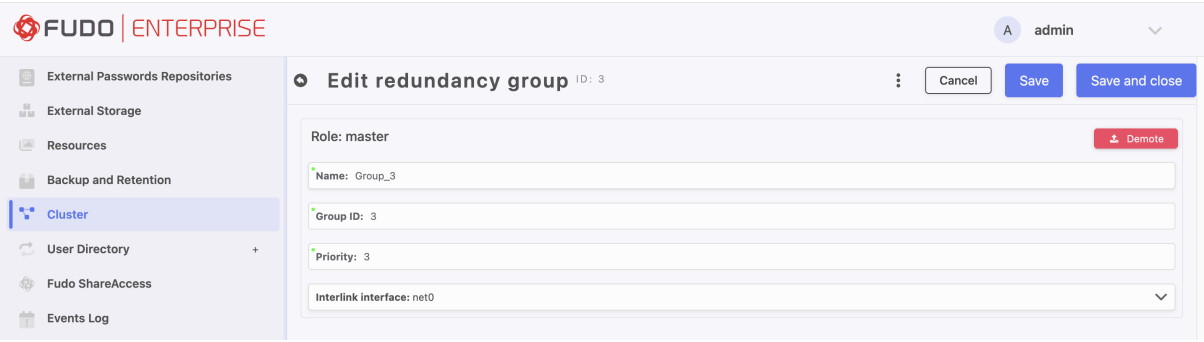
Demoting a Redundancy Group

Note

Demoting a group switches the master role for the given redundancy group to another cluster node. The node on which the selected redundancy group has the highest priority will assume the master role.

To demote a redundancy group, follow the instructions below.

1. From the left menu, select *Settings* > *Cluster*.
2. Go to the *Redundancy Groups* tab.
3. Edit the group you want to demote.
4. Click *Demote* for the selected redundancy group.
5. Click *Save and exit*.



Note

If, after demoting the group, none of the remaining nodes assumes the master role, it will be restored to the redundancy group on the edited node.

Forcing the Slave Role

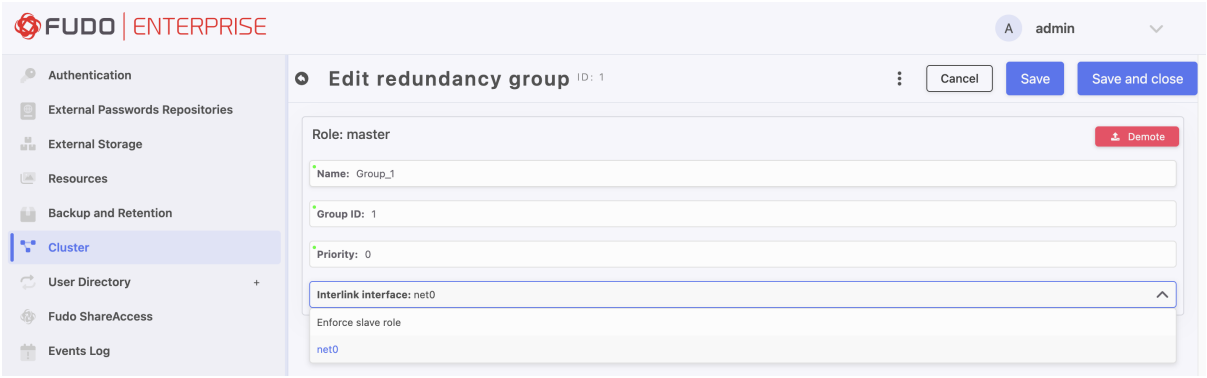
Note

- Forcing the slave role ensures that the redundancy group will never switch to master mode, regardless of the state of the other cluster nodes.
- Forcing the slave role is recommended before performing maintenance work to ensure that network traffic is redirected to the remaining cluster nodes. Another use case is a cluster node deployed in a separate location without Layer 2 connectivity to the other cluster nodes.

To force the slave role for a selected redundancy group, follow the instructions below.

1. From the left menu, select *Settings* > *Cluster*.
2. Go to the *Redundancy Groups* tab.
3. Locate the redundancy group and click its name to edit it.
4. From the *Cluster communication interface* drop-down list, select `Force slave mode`.

5. Click *Save and exit*.

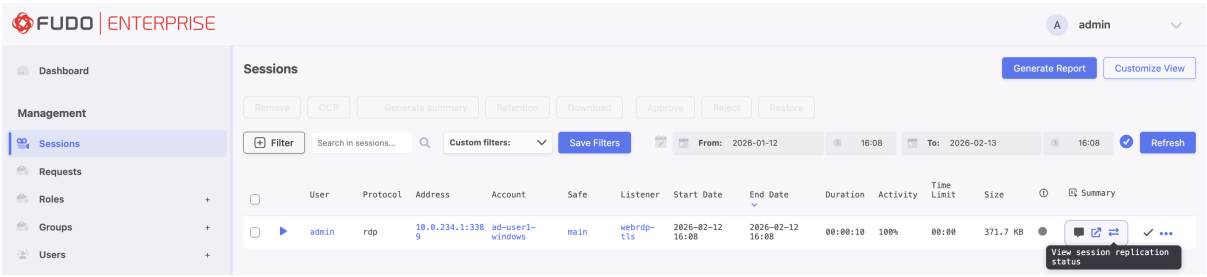


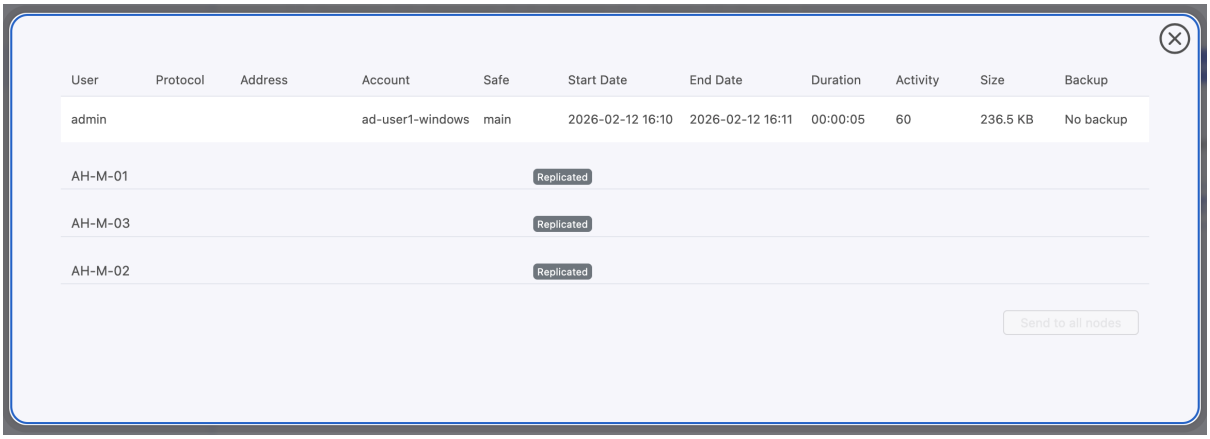
Related topics:

- *Security: Cluster configuration*
- *Cluster Initialization*
- *Cluster Configuration*

12.10.8 Checking Session Replication Status

To check the session replication status, locate the connection in the session list and click the ⇄ icon.





Related topics:

- *Editing Cluster Nodes*
- *Removing Cluster Nodes*
- *Cluster Security Configuration*

12.11 Users Synchronization - User Directory

User is one of the fundamental *data model* entity. Only defined users are allowed to connect to monitored servers. Fudo Enterprise features automatic users synchronization service which enables importing users information from *Active Directory* servers or other servers compatible with the *LDAP* protocol.

Warning

It is required that LDAP server supports a `memberOf` parameter - an attribute that specifies the distinguished names of the groups to which this object belongs.

New users definitions and changes in existing objects are imported from the directory service periodically every 5 minutes. Deleting a user object from an *AD* or an *LDAP* server requires performing the full synchronization to reflect those changes on Fudo Enterprise. The full synchronization process is triggered automatically once a day at 00:00, or can be triggered manually.

12.11.1 Configuring Users Synchronization Service

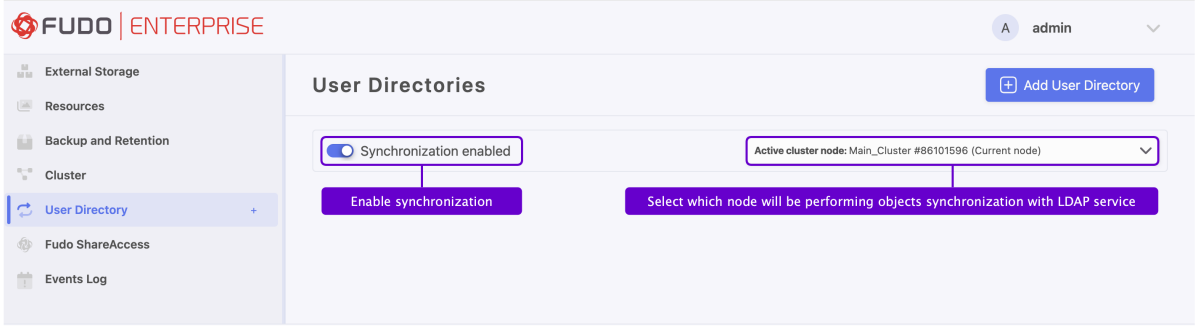
Note

When Kerberos is enabled in Fudo Enterprise, synchronization with Active Directory uses the Kerberos protocol by default. This setup requires proper configuration of domain services and accurate system time synchronization. For more information, refer to the *Kerberos Support for Active Directory* section.

If you do not plan to use Kerberos, deselect the *Enable Kerberos for LDAP synchronization* option in the **Settings** > **Authentication** > **Global** tab to continue using *simple bind* for synchronization. For more information, refer to the *Kerberos Authentication Settings* section.

To enable users synchronization feature, proceed as follows.

1. Select *Settings* > *User Directory*.
2. Select *Synchronization enabled*.
3. In case of *cluster configuration*, from the *Active cluster node* drop-down list, select which node will be performing objects synchronization with LDAP service.
4. Click *+ Add User Directory*.



5. Enter a unique name for this configuration.

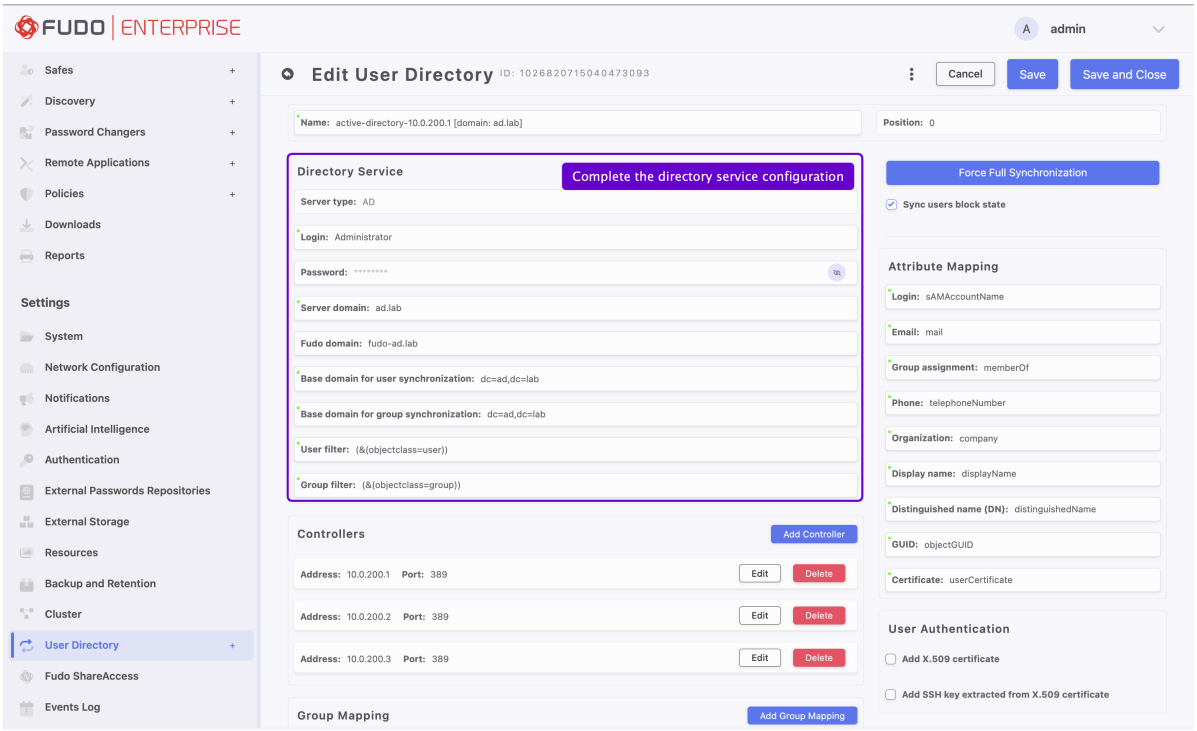
6. In the **Position** field, define the priority that determines the order in which the domains are queried.

> **Note**
>
> A lower number indicates a higher priority.

7. In the *Directory Service* section, select data source type from the *Server type* drop-down list.
8. Provide the user authentication information (login and password) to access user data on given server.
9. Enter domain name, to which imported users are assigned to.
10. Provide base DN parameter for users' objects (eg. `DC=devel,DC=whl`).
11. Provide base DN for parameter groups' objects (eg. `DC=tech,DC=whl`).

> **Note**
>
> Do not include any whitespace characters in the DN parameter.

12. Define filter (or leave the default value) for user records, which are subject to synchronization.
13. Define filter (or leave the default value) for user groups, which are subject to synchronization.



Defining Directory Service Server

14. In the *Controllers* section, click *Add Controller* to define directory service server.

15. Provide IP address and port number.

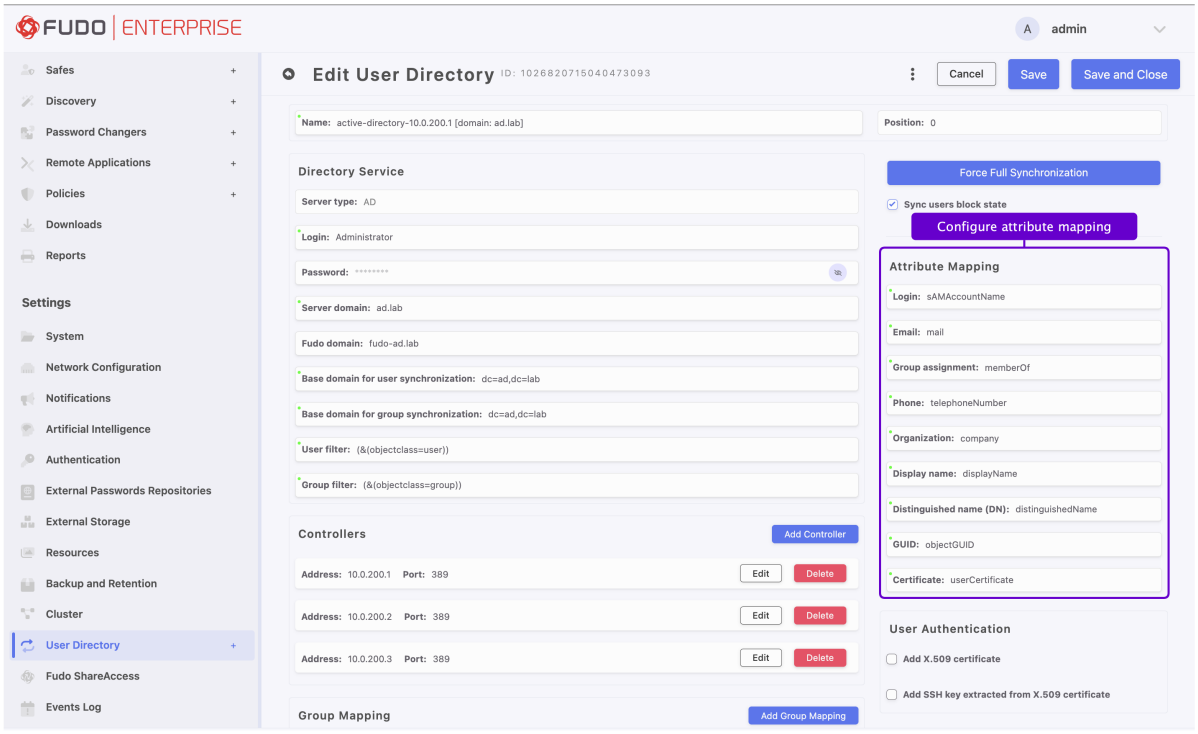
> **Note**
>
> In case of TLS-encrypted connection, define LDAP server's address using its full domain name (e.g. `tech.ldap.com`) instead of an IP address, to ensure the certificate is verified properly. Make sure that the given server name is included in certificate's *Common Name* field.

16. Select the *Page LDAP results* option to enable paging.
17. Select the *Encrypted connection* option to enable encryption and upload the CA certificate.
18. Click *Save*

> **Note**
>
> To add multiple controllers, repeat the steps described above.

Defining User Information Mapping

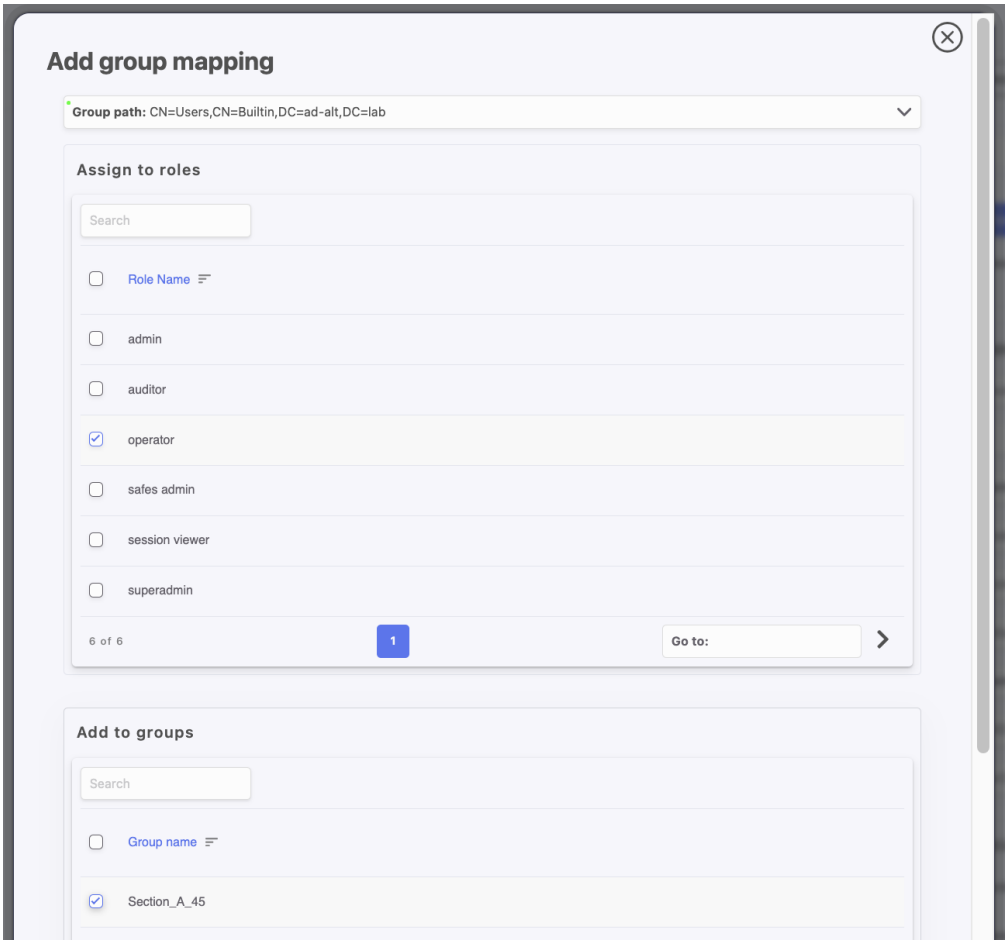
> **Note**
>
> Fields mapping enables importing users information from nonstandard attributes, e.g. telephone number defined in an attribute named *mobile* instead of the standard *telephoneNumber*.



19. Select *Sync users block state* to automatically block local users' accounts blocked in the directory.

Mapping External Groups to User Roles

20. In the *Group Mapping* section, click *Add Group Mapping* to assign user groups to Fudo roles, Fudo groups, and external authentication methods.
21. In the *Group path* field, select the distinguished name (DN) of the group.
22. In the *Assign to roles* section, select the Fudo Enterprise roles to assign to users from this group.
23. In the *Add to groups* section, select the Fudo Enterprise groups to assign to users from this group.
24. In the *Authentications* section, select external authentication source to assign to users from this group.
25. Click *Save*.



Note

External authentication sources are assigned to users in the exact sequence they are defined in groups mapping. Thus if the same user is present in more than one group, Fudo Enterprise will be authenticating him against external authentication sources starting from those defined in the first group mapping defined.

For example:

A user is assigned to groups A and B. Group B is mapped to `Safe RDP` and has `CERB` and `Radius` authentication sources assigned. Group A is second in order and it is mapped to `Safe SSH` and has `AD` authentication source assigned.

Authenticating a user, Fudo Enterprise will send requests to external authentication sources in the following order:

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

26. In the *User Authentication* section, select the *Add X.509 certificate* option to retrieve user's certificate and assign it as one of user's authentication methods.
27. Select the *Add SSH key extracted from X.509 certificate* option to retrieve user SSH key from certificate and assign it as one of user's authentication methods.

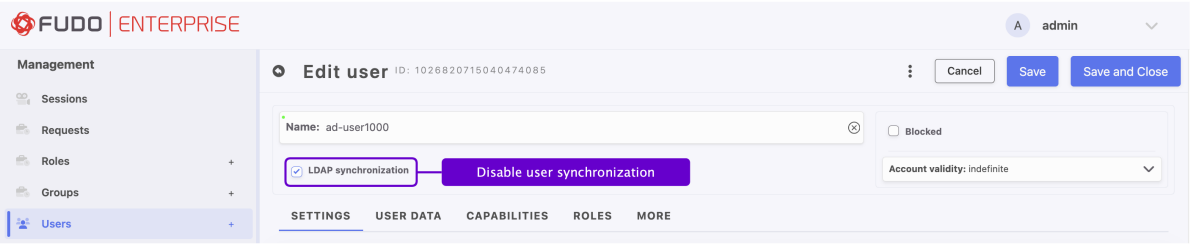
28. To save the configuration, click *Save and Close* in the upper-right corner of the screen.

Note

- The *Force Full Synchronization* option enables processing changes in directory structures which cannot be processed during periodical synchronization, eg. deleting a defined group or deleting a user.
- The full synchronization process is triggered automatically once a day at 00:00, or can be triggered manually.
- Use *diagnostics tools* to troubleshoot problems with LDAP configuration.
- Fudo Enterprise supports nested LDAP groups.

12.11.2 Disabling Data Synchronization for User

Fudo Enterprise allows synchronizing the user's data with the LDAP service source. The **Synchronize with LDAP** option is responsible for this process. When this option is checked for the given user, an administrator can't edit the user's data manually but can add or edit their authentication methods. If the **Synchronize with LDAP** option is unchecked, the user is no longer synchronized with LDAP source, and can be edited by an administrator. The administrator can still check the option and reinstate synchronization with LDAP, but any change made manually will disappear with the next synchronization attempt. Only the added authentication methods won't change.



Note

Because authentication methods are excluded from the synchronization, a synchronized user can be invited to Fudo ShareAccess and granted the *Trusted* status. The Fudo ShareAccess identity of a user is stored as the *ShareAccess Key* authentication method, so it is not overwritten by the next synchronization pass. For more information, refer to the *ShareAccess Key Authentication Method* section.

12.11.3 Kerberos Support for Active Directory

When the *Enable Kerberos for LDAP synchronization* option is selected in the **Settings** > **Authentication** > **Global** tab and the User Directory server type is set to **AD (Active Directory)**, synchronization uses the Kerberos protocol.

Note

If you do not plan to use Kerberos, deselect the *Enable Kerberos for LDAP synchronization* option in the **Settings** > **Authentication** > **Global** tab to continue using *simple bind* for synchronization. For more information, refer to the *Kerberos Authentication Settings* section.

If you plan to use **Kerberos** authentication for User Directory synchronization, ensure the following:

- Port **88 (Kerberos)** is open on the firewall — otherwise, synchronization will fail.
- The **DNS server** from the same domain is properly configured.

Note

The Fudo hostname no longer needs to include a domain suffix (eg. `fudo.qa.kerberos`) for Kerberos synchronization to work correctly. This also allows synchronization across multiple domains.

- The **controller address** matches the **SPN (Service Principal Name)** of the LDAP server defined in the domain.
- If your current configuration uses an IP address instead of a hostname, update it to use the correct hostname.

Note

Fudo Enterprise supports **LDAP channel binding**, so User Directory synchronization works even when Windows domain controllers enforce channel binding (the *Domain controller: LDAP server channel binding token requirements* policy, registry setting *LdapEnforceChannelBinding*, set to **value 2**). On LDAPS connections, session integrity is provided by the TLS protocol.

Channel binding is likewise handled for LDAP-based Discovery and LDAP secret changers. It does not apply to external authentication because external authentication uses either Kerberos-only or LDAP-only authentication.

Related topics:

- *External Authentication Server Definition*
- *Users management*
- *Diagnostics*

12.12 SCIM 2.0 Provisioning

Fudo Enterprise can act as a SCIM 2.0 **Service Provider**. It exposes a SCIM endpoint that an external identity provider (IdP) uses to provision and manage user identities and group membership in Fudo Enterprise. Fudo Enterprise only **receives** provisioning requests from the IdP - it never initiates them.

SCIM automates the user identity lifecycle (creating, updating, disabling, and re-enabling users) and group membership. It does **not** manage other Fudo Enterprise objects, such as servers, ac-

counts, safes, password vaults, session policies, or authentication flows. Those remain configured locally in Fudo Enterprise.

Note

When *OpenID Connect (OIDC)* login is also used for SCIM-provisioned users, configure SCIM and OIDC on the **same IdP application** so that both integrations refer to the same set of users and identities are used consistently.

12.12.1 Managing Access to the SCIM Configuration

SCIM provisioning of users and groups is performed internally by the built-in `scim_manager` system user, which Fudo Enterprise creates automatically and which already has the privileges required to create, update, block, and re-enable SCIM-managed users and groups. You do not need to create a user or assign any privileges for provisioning itself to work.

You only need to configure a role if you want to allow a user other than the `superadmin` to **manage the SCIM configuration** - that is, to view its state, enable or disable provisioning, and rotate the API key. Grant such a user a role with the SCIM privileges from the `User Sources` group:

- `scim-read` - view the SCIM configuration state;
- `scim-modify` - configure SCIM provisioning, including enabling or disabling it and rotating the API key.

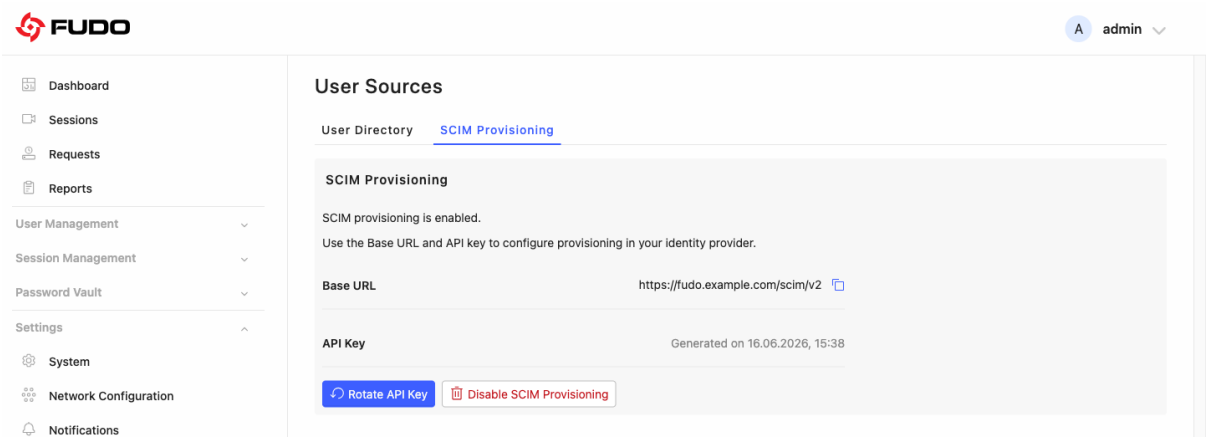
Note

This role grants access to the SCIM **configuration** only (`scim-modify` is required to configure SCIM provisioning). It does not affect how users and groups are provisioned - that is always handled internally by the `scim_manager` system user.

12.12.2 Configuring SCIM Provisioning

To connect an identity provider to Fudo Enterprise, provide the IdP with the Fudo Enterprise SCIM **Base URL** and the **API key** that serves as the SCIM bearer token.

1. Select *Settings* > *User Sources*.
2. Go to the *SCIM Provisioning* tab.
3. Click *Generate API key*. Fudo Enterprise generates the *Base URL* and the *API key*.



4. Copy the *Base URL* - it is the SCIM endpoint address of this Fudo Enterprise instance (for example, `https://<fudo-address>/scim/v2`).
5. Copy the *API key*.

Warning

The *API key* is shown only once, at the moment it is generated. Copy it immediately and store it securely. If the key is lost, rotate it to generate a new one.

6. Configure your identity provider with these values, as described in *Configuring the identity provider*. No separate OAuth flow is required.

12.12.3 Configuring the Identity Provider

Note

The exact steps depend on the identity provider. The following procedure provides general guidance typical for SCIM 2.0-compliant identity providers.

1. In the identity provider, add or create an application that supports **SCIM 2.0** provisioning.
2. In the application's provisioning settings, set the SCIM endpoint (named **SCIM connector base URL**, **Tenant URL**, or similar) to the Fudo Enterprise *Base URL*.
3. Set the authentication method to a **bearer token** (HTTP header) and paste the Fudo Enterprise *API key* as the token (also called the *Secret Token*). Use the provider's *Test connection* function to verify the setup.
4. Review the attribute mappings so that the provider sends at least `userName`, `name`, `displayName`, the primary `emails` and `phoneNumbers` values, `active`, and `externalId`. The `externalId` is the correlation key (see *Attribute mapping*).
5. Set the provisioning scope to the assigned users and groups, and enable provisioning.
6. Assign users and groups to the application to provision them in Fudo Enterprise. Some providers require an explicit step to provision groups (for example, the Okta *Push Groups* feature).

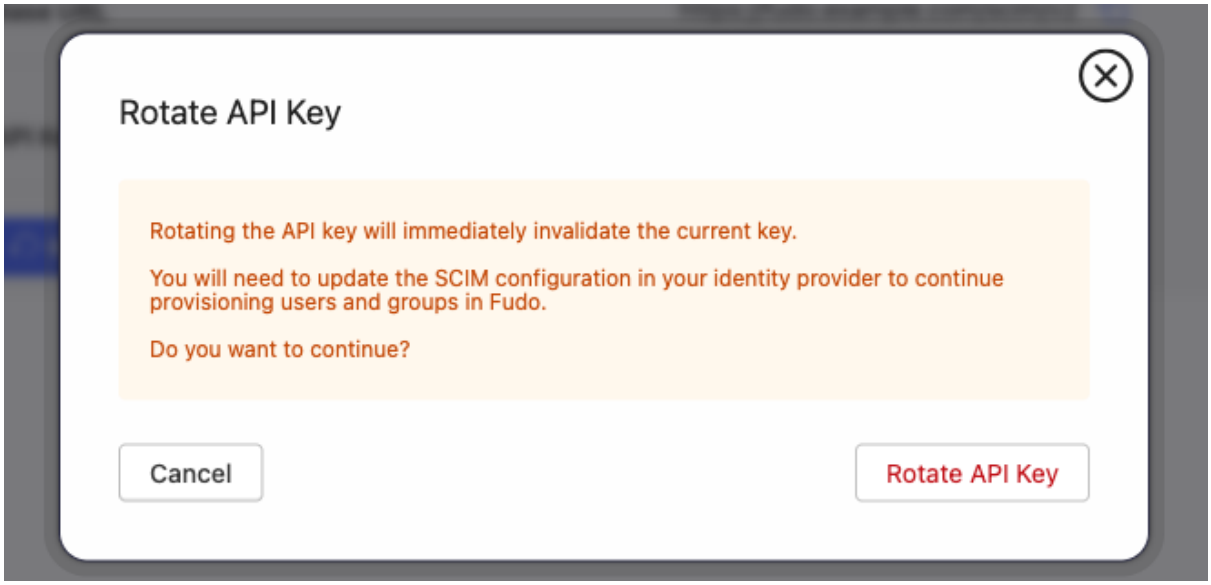
Note

- In **Okta**, assigned users are provisioned automatically, while groups must be pushed explicitly with *Push Groups*.
- **Microsoft Entra ID** requires an **Entra ID P1 (or higher)** license. Changes are applied with *Provision on demand* or on the automatic (approximately 40-minute) cycle; deletions are applied only on the automatic cycle.
- Field names and navigation differ between providers and may change over time. Always follow the current SCIM 2.0 setup documentation of your identity provider (Okta or Microsoft Entra ID).

12.12.4 Rotating the API Key

You can rotate the API key at any time, for example as part of credential hygiene or if the key may have been exposed.

1. Select *Settings* > *User Sources* > *SCIM Provisioning*.
2. Click *Rotate API Key* and confirm.



Warning

Rotating the API key **immediately invalidates the current key**. Update the SCIM configuration in your identity provider with the new key to continue provisioning users and groups in Fudo Enterprise.

12.12.5 Disabling SCIM Provisioning

To stop accepting SCIM requests, click Disable SCIM Provisioning on the *SCIM Provisioning* tab. After disabling:

- the API key stops working and the IdP can no longer provision changes;

- existing SCIM-managed users and groups **remain in** Fudo Enterprise but become **locally managed** and can be edited by an administrator.

12.12.6 SCIM-Managed Account Behavior

After SCIM provisioning is enabled, the identity provider manages selected user accounts in Fudo Enterprise. Users assigned to the application on the IdP side are automatically created in Fudo Enterprise and marked as managed by SCIM.

During synchronization, Fudo Enterprise updates mapped user attributes, such as the login, email address, or display name. Fields managed by SCIM are treated as data coming from the IdP and cannot be edited locally in Fudo Enterprise - the system enforces this.

If a user is deactivated in the IdP or removed from the provisioning scope, Fudo Enterprise blocks the user account. Any active user sessions are terminated, while session history, audit data, and previous associations are preserved.

Note

- Fudo Enterprise identifies records by `externalId`. Both `externalId` and `userName` are unique: a `POST` request that reuses the `externalId` or `userName` of an existing user is rejected with `409 Conflict` (`scimType: uniqueness`). Accounts are created with `POST`; existing accounts are updated, and deactivated accounts re-enabled, with `PATCH`.
- Identity providers query Fudo Enterprise before writing and determine on that basis whether to create or update a record. Fudo Enterprise performs no de-duplication of its own; matching an incoming identity to an existing record is handled by the identity provider.

12.12.7 Attribute Mapping

The identity provider is authoritative for all mapped identity attributes. In Fudo Enterprise, these fields are **read-only** for SCIM-managed users and are updated only through SCIM.

SCIM attribute (from IdP)	Fudo Enterprise user field	Notes
`externalId`	Internal correlation key	Primary correlation key. Not displayed and not editable. Used to match the same identity across creation, update, blocking, and re-enabling.
`userName`	Login / username	Required and unique. Read-only. If the `userName` contains an `@` (for example `jdoe@fudosecurity.com`), only the local part before the `@` is used as the Fudo Enterprise login (`jdoe`); the full value is retained internally for correlation, filtering, and sorting.
`name.givenName`, `name.familyName`	Name components	Read-only.
`displayName`	Full name	Read-only. The sole source of the full name.
`emails` (primary)	Email	Only the entry marked `primary: true` is stored, together with its `type`. If no entry is marked as primary, the email address remains empty. Read-only.
`phoneNumbers` (primary)	Phone	Only the entry marked `primary: true` is stored, together with its `type`. If no entry is marked as primary, the phone number remains empty. Read-only.
`active`	Account state	Drives blocking and unblocking (see *Blocking model*).
`groups`	Group membership	Read-only on the user resource. Membership is managed through the `/Groups` endpoint (see *Example payloads*); values sent in `groups` on the user resource are not applied.

12.12.8 Attributes That Are Not Supported

Fudo Enterprise implements the SCIM 2.0 core `User` and `Group` schemas only. Attributes outside the mapping table above are accepted and ignored: the request succeeds, no error is returned, and the values are not stored in Fudo Enterprise.

Ignored attributes include:

- `organization`, `title`, `roles`, and `entitlements`;
- `name.formatted`, `name.middleName`, `name.honorificPrefix`, and `name.honorificSuffix`;
- the whole **Enterprise User** extension (`urn:ietf:params:scim:schemas:extension:enterprise:2.`

`0:User`), including `department`, `employeeNumber`, and `manager`.

> **Note**
>
> Once SCIM provisioning is enabled, the instance publishes the definitions of the supported schemas at `<Base URL>/Schemas` - for example `https://<fudo-address>/scim/v2/Schemas`.
>
> The endpoint requires no bearer token and returns the list of attributes of the `User` and `Group` resources supported by that Fudo Enterprise version.

12.12.9 Example Payloads

The requests below use the *Base URL* and *API key* from the *SCIM Provisioning* tab; the API key is sent as a bearer token (`Authorization: Bearer <API key>`) and the content type is `application/scim+json`.

Creating a user with every supported attribute - `POST <Base URL>/Users`:

```
{
  "schemas": ["urn:ietf:params:scim:schemas:core:2.0:User"],
  "externalId": "12345-abcde",
  "userName": "john.doe@example.com",
  "name": {
    "givenName": "John",
    "familyName": "Doe"
  },
  "displayName": "John Doe",
  "emails": [
    { "value": "john.doe@example.com", "type": "work", "primary": true }
  ],
  "phoneNumbers": [
    { "value": "+49-555-0100", "type": "work", "primary": true }
  ],
  "active": true
}
```

This creates an active Fudo Enterprise user whose login is `john.doe` (the part before the `@`) and whose full name is `John Doe`. The response returns the assigned Fudo Enterprise user `id`, which is the value used to manage group membership.

Adding that user to an existing group - `PATCH <Base URL>/Groups/<group id>`:

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations": [
    {
      "op": "add",
      "path": "members",
```

(continues on next page)

(continued from previous page)

```
      "value": [ { "value": "<user id>" } ]
    }
  ]
}
```

Removing that user from the group - `PATCH <Base URL>/Groups/<group id>`:

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations": [
    {
      "op": "remove",
      "path": "members[value eq \"<user id>\"]"
    }
  ]
}
```

Deactivating a user - `PATCH <Base URL>/Users/<user id>`. The same request with `"value": true` re-enables the user:

```
{
  "schemas": ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
  "Operations": [
    {
      "op": "replace",
      "path": "active",
      "value": false
    }
  ]
}
```

Note

These requests are issued by the identity provider during normal operation. The examples show the payload structure and can be used to verify connectivity while the integration is being set up.

12.12.10 Restrictions On Scim-Managed Objects

Once a user or group is managed by SCIM, the identity provider is its source of truth. In Fudo Enterprise you therefore **cannot**:

- edit the identity data of a SCIM-managed user or group (name, email, phone, or the group name);
- change a SCIM-managed group's membership - the assign/remove user controls are disabled, and local Fudo Enterprise users cannot be added to it;

- create or delete SCIM-managed users and groups manually.

You **can** still configure the following locally, because SCIM does not touch it:

- safe access, account access, and object rights for the SCIM-managed user or group;
- roles, the *Fudo domain*, and authentication methods of a SCIM-managed user.

These local settings are preserved when the identity provider updates a group, for example after a rename or a membership change. Roles are assigned to users **directly** in Fudo Enterprise; unlike User Directory groups, Fudo Enterprise groups (including SCIM-managed groups) do not grant roles through a group-to-role mapping.

The separation applies in both directions. The identity provider manages identity attributes and group membership; the following are set in Fudo Enterprise only and have no SCIM representation:

- roles (see *Attributes that are not supported* for the ignored `roles` attribute);
- the *Fudo domain*;
- safe access, account access, and object rights;
- authentication methods.

Provisioning is also confined to SCIM-managed objects. The identity provider manages the users and groups that SCIM created, and SCIM-managed users belong to SCIM-managed groups only. Accounts and groups created locally in Fudo Enterprise remain outside its scope.

Note

When a group is deleted in the identity provider, Fudo Enterprise removes the group and its members lose the access that the group granted. Access granted by other means is not affected.

12.12.11 Blocking Model

Fudo Enterprise tracks two **independent** block states for a SCIM-managed user; clearing one does not clear the other:

- `Blocked by SCIM` - applied when the identity provider deactivates the user (`active=false`).
- `Blocked locally` - applied when an administrator blocks the user manually in Fudo Enterprise. A local block requires a reason and is audited; an emergency local block of a SCIM-managed user is allowed.

The `Blocked by SCIM` state takes precedence: while it is in effect, the user stays blocked even if the local block is removed. The user is unblocked only when the identity provider reactivates them (`active=true`).

Note

If the identity provider sends a delete request instead of a deactivation, Fudo Enterprise removes the user rather than blocking them. In practice, Okta and Microsoft Entra ID

always deactivate users (`active=false`) rather than delete them.

The *Managed by* column shows the source of each object: `SCIM`, `Fudo (local)`, or `User directory`. A SCIM-managed user also displays a *Managed externally (SCIM)* indicator on its details view.

12.12.12 Authentication with OIDC

SCIM-provisioned users typically sign in through OIDC, while SCIM remains **authoritative for identity data**. OIDC only authenticates the user and does not overwrite SCIM-managed attributes. SCIM-provisioned users can also be assigned other Fudo Enterprise authentication methods, such as a password or an API key.

OIDC authentication and SCIM provisioning are **independent mechanisms**: Fudo Enterprise does not require a user to be SCIM-provisioned in order to sign in through OIDC. Any Fudo Enterprise user whose identity matches the OIDC login - whether created by SCIM or added manually - can sign in. For SCIM-managed users, SCIM remains authoritative for their identity attributes regardless of the login method.

12.12.13 Auditing

Fudo Enterprise records every SCIM operation in the *events log*, capturing **who** performed it, **what** changed, and **when**. Provisioning changes received from the identity provider are recorded under the built-in `scim_manager` system user, which keeps SCIM activity clearly distinguishable from local administrator actions. The events log can be exported to a SIEM over syslog.

Related topics:

- *Users Synchronization - User Directory*
- *OpenID Connect Authentication Definition*
- *Users management*

12.13 Certificate-based Authentication Scheme

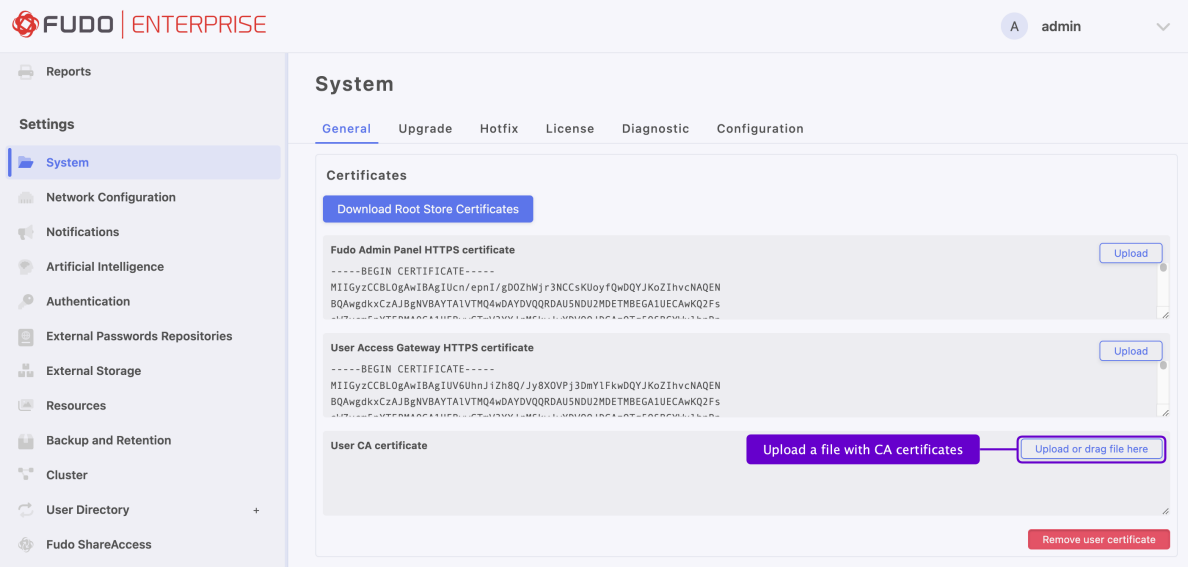
Fudo Enterprise allows authenticating with certificate, complied with PIV standards.

In order to configure authentication method *Certificate*, proceed as follows:

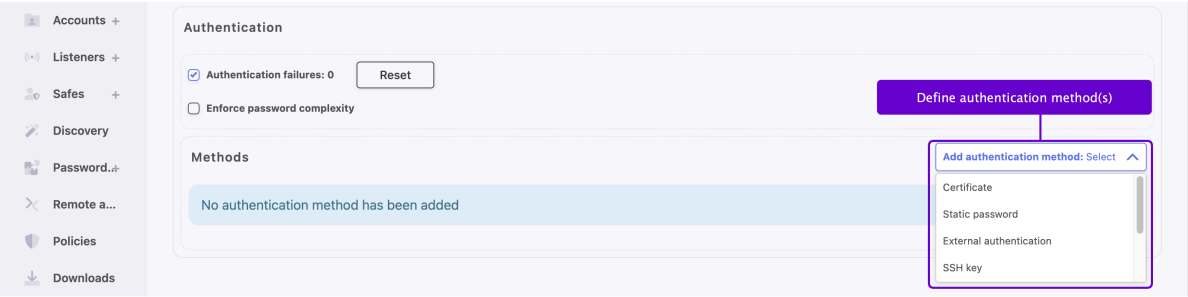
1. Select *Settings* > *System*
2. In the *General* tab, under the *User CA certificates* section upload a file with CA certificate(s) in PEM format.

Note

Fudo Enterprise supports a multiple-domain configuration. For such configuration, the administrator has to upload a PEM file that consists of root/intermediate certificates from all the CAs. The *Subject* field should be unique for each user.



3. Click *Save*.
4. Go to *User Management* > *Users* and edit the user, for whom you want to set authentication method *Certificate*, or create a new user by selecting *User Management* > *Users* and then clicking *+ Add user*.
5. In the *Authentication* section select *Certificate* type from the *Add authentication method* drop-down list.



6. Provide *Subject* and click *Save*.

Note

The subject must comply with the RFC 2253 or RFC 4514 requirements.

7. Click *Save* to save changes in the user definition.

Related Topics:

- *Creating a User*

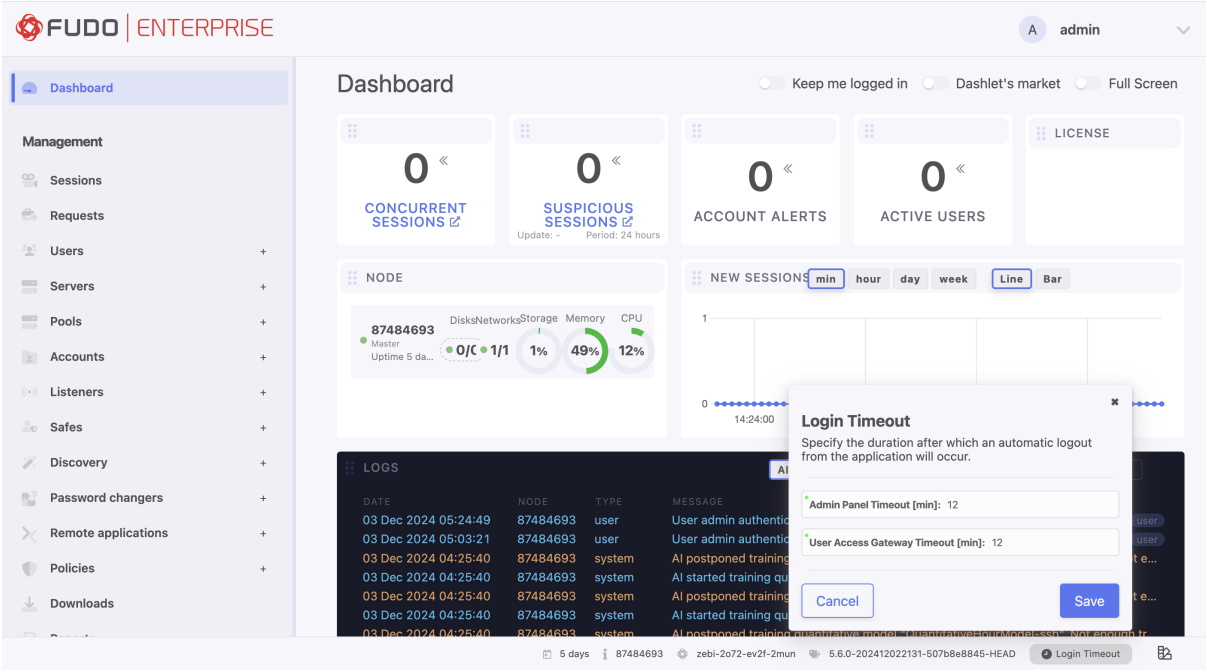
12.14 Login Timeout

The **Login Timeout** feature allows administrators to set inactivity timeout limits for both the Admin Panel and User Access Gateway. This feature ensures that users are automatically logged out after a specified period of inactivity, enhancing system security.

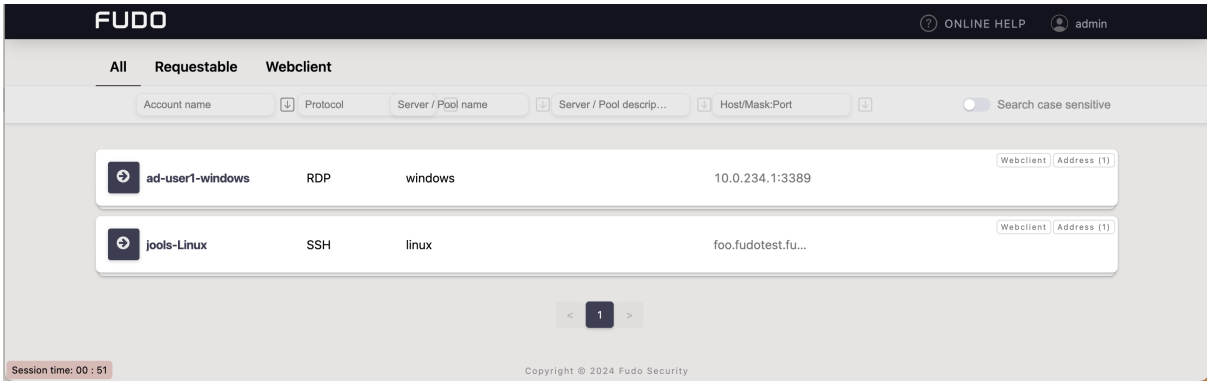
> **Note**
>
> Only users with the **superadmin** or **admin** role can manage Login Timeout settings.

Users with operator role should not see 'Login timeout' section on the footer

3. Click *Save* to apply the settings.



Once the timeout settings are configured, a countdown timer will automatically appear in the Admin Panel and User Access Gateway to indicate the remaining time before automatic logout due to inactivity.



Related Topics:

- *Dashboard: Keep me logged in*

12.15 System Version Restore

In the case there is a problem with the current system revision, it is possible to restore the system to its previous version.

Warning

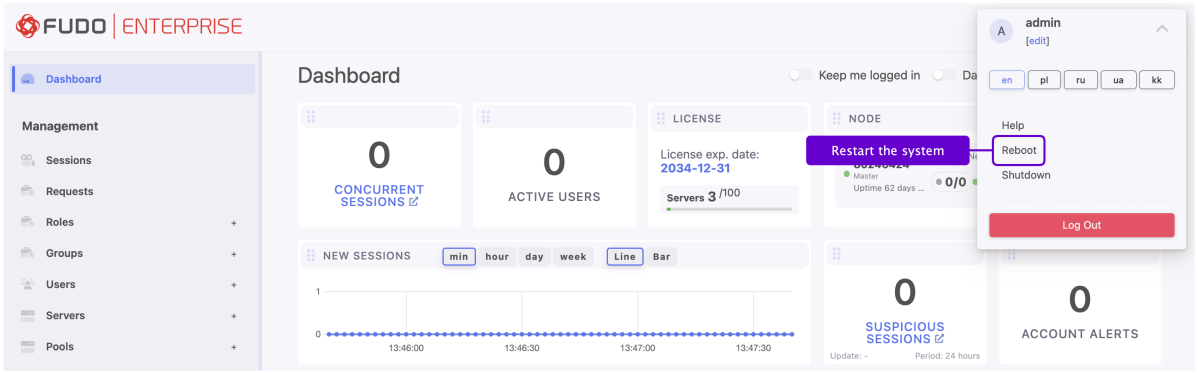
Restoring the system to the previous version will bring back the system's state prior the update. **Session data** and **configuration changes** in the current system revision will be lost. This includes the **secret changers** activity. If any passwords were changed during the newer version's usage, restarting Fudo will lead to lost access to corresponding systems.

Note

- System restore requires USB flash drive with the encryption key connected to the device.
- Restoring the system will terminate all current users' connections.
- Use the *Deny new connections* option in *Settings* > *Authentication* > *Global* tab to prevent new connections from being established and to limit the number of active users before restarting the system. For more information, see *Deny New Connections*.

To restore the system to the previous revision, proceed as follows.

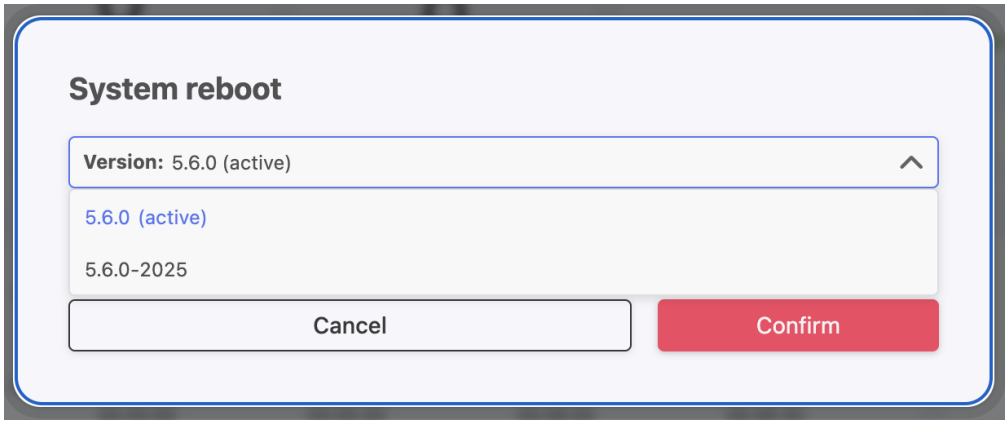
1. Connect one of the USB flash drives containing the encryption key.
2. Select *Reboot* from user options menu.



3. Select system revision to be loaded after restarting the system.

Note

Current system version is selected by default.



4. Click *Confirm* to proceed with restarting the system to the selected revision.

Warning

Restarting the system will terminate all current users' connections.

Related topics:

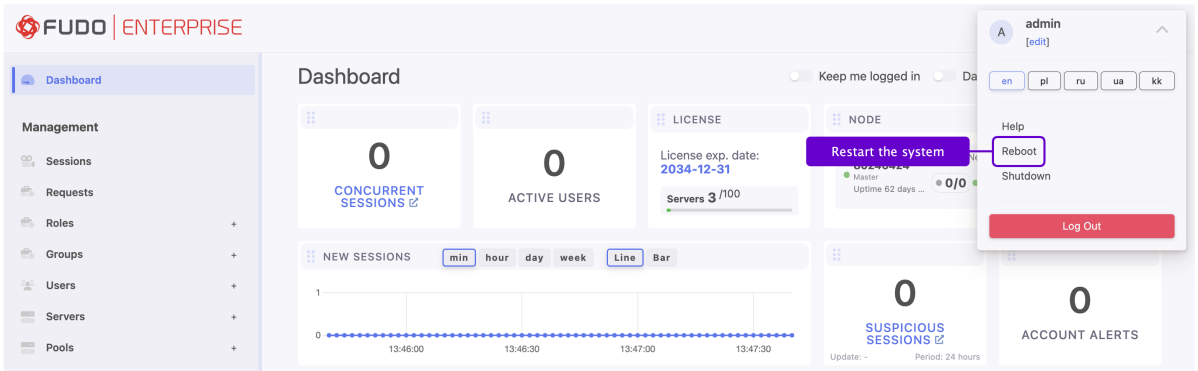
- *System initiation*
- *System update*

12.16 System Reboot

Note

- System reboot requires USB flash drive with the encryption key connected to the device.
- Restarting the system will terminate all current users' connections.
- Use the *Deny new connections* option in *Settings* > *Authentication* > *Global* tab to prevent new connections from being established and to limit the number of active users before restarting the system. For more information, see *Deny New Connections*.

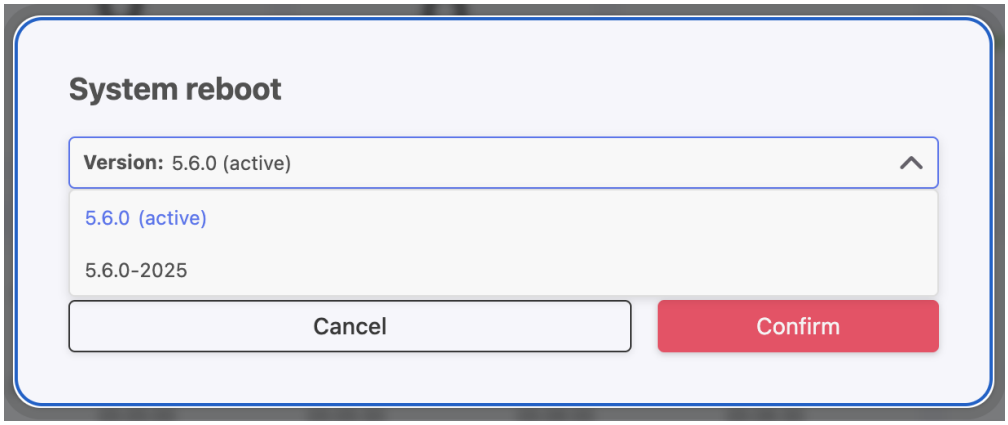
1. Connect one of the USB flash drives containing the encryption key.
2. Select *Reboot* from user options menu.



3. Select the previous system revision to be loaded after restarting the system.

Note

Current system version is selected by default.



Warning

Restoring the system to the previous version will bring back the system's state prior the update. **Session data** and **configuration changes** in the current system revision will be lost. This includes the **secret changers** activity. If any passwords were changed during the newer version's usage, restarting Fudo will lead to lost access to corresponding systems.

4. Click *Confirm* to proceed with restarting the system to the selected revision.

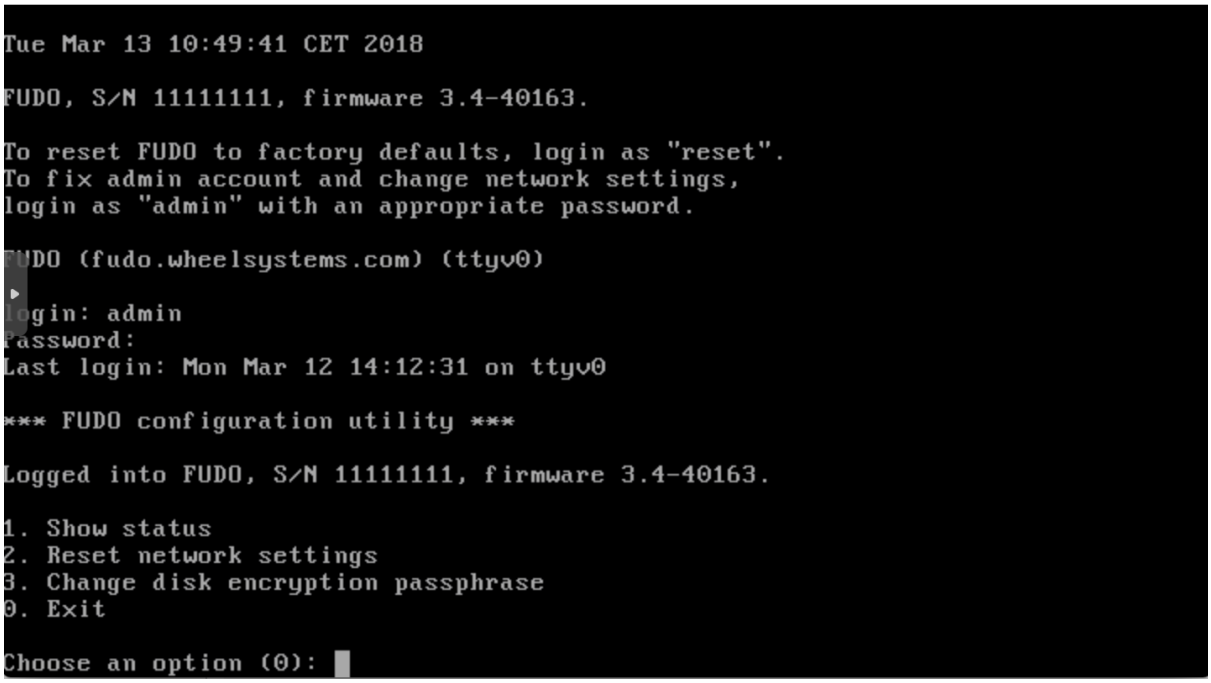
Related topics:

- *System initiation*
- *System version restore*

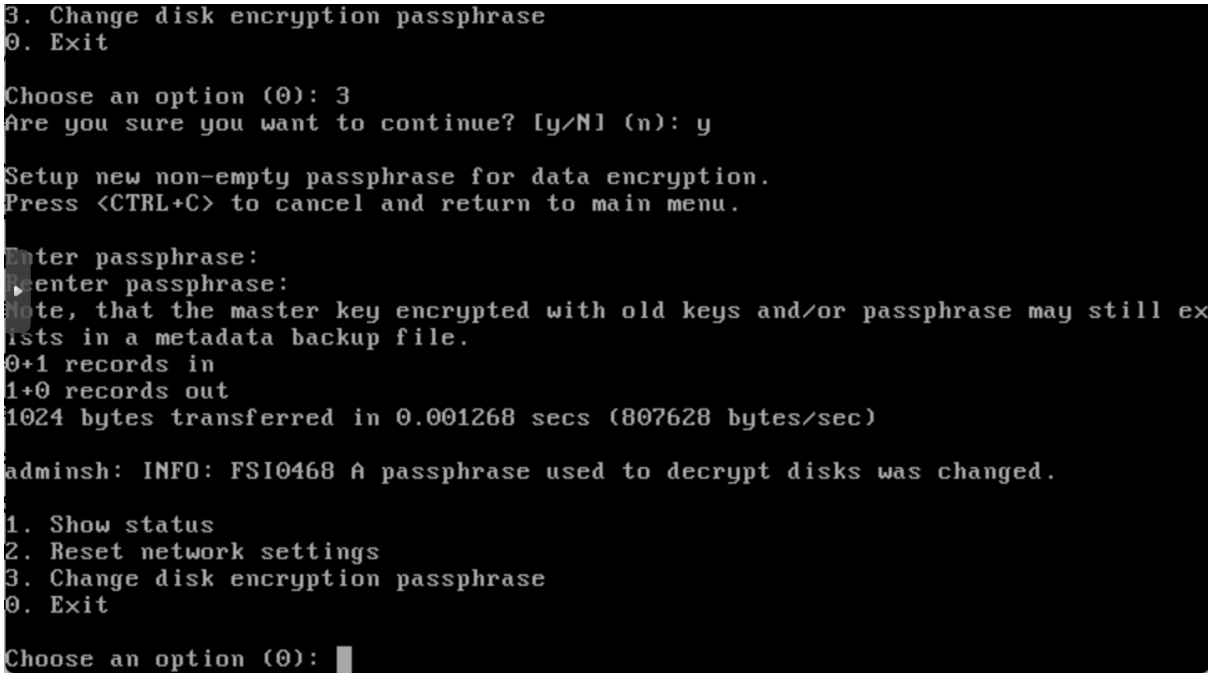
12.17 Changing Encryption Passphrase

In case of Fudo Enterprise deployed in a virtual environment, data is encrypted using a passphrase. To change current passphrase, proceed as follow.

1. Log in to system console on an account with **superadmin** privileges.
2. Type in `3` and confirm by pressing the *Enter* key.



3. Type in `y` and press the *Enter* key, to proceed with changing encryption passphrase.
4. Enter the new passphrase and press the *Enter* key.
5. Enter the passphrase once again and press the *Enter* key.



6. Restart the system to apply changes.

Related topics:

- *System Update*
- *Session Data Backup*

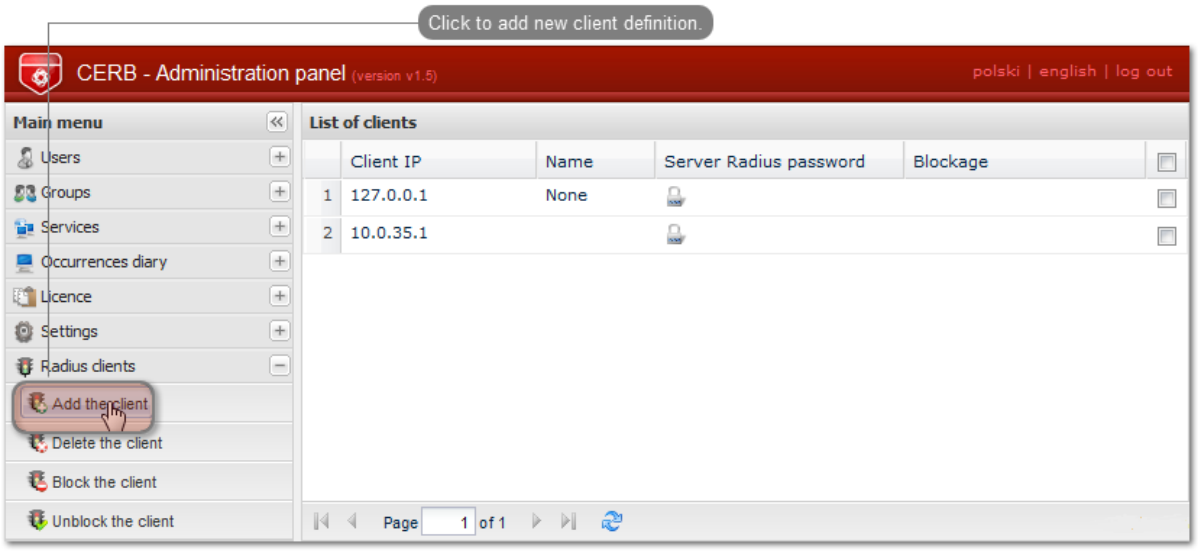
12.18 Integration with CERB Server

CERB is complete user authorization solution which supports a number of authorization mechanisms (i.e. mobile token, onetime passwords, etc.). The following procedure describes configuration steps required to enable Fudo Enterprise to verify users credentials using CERB server.

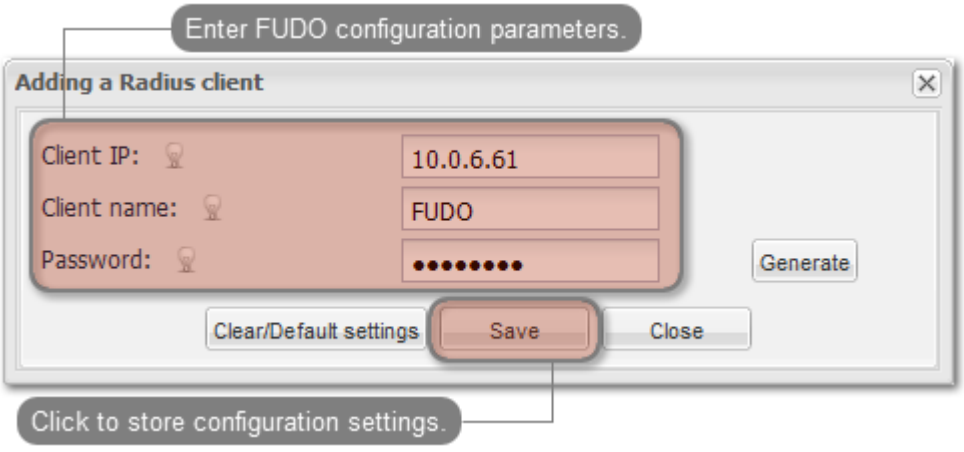
CERB server configuration

1. Adding RADIUS client.

- Select *RADIUS clients* > *Add client* to add Fudo Enterprise as a RADIUS client.



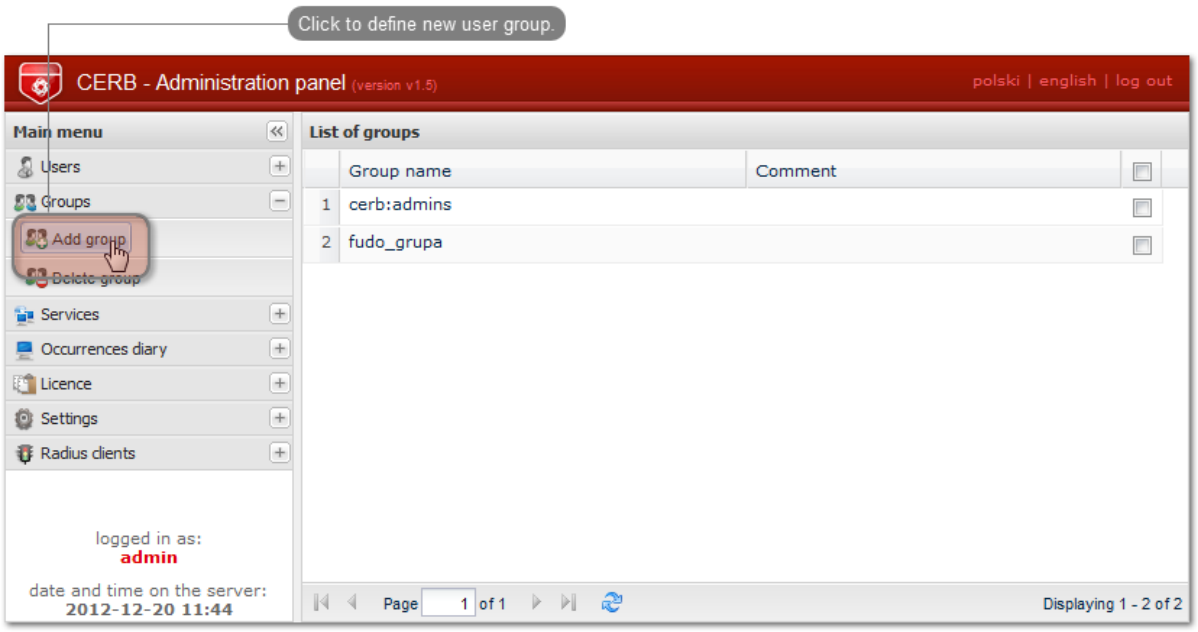
- Provide Fudo Enterprise IP address, client's name and password and click *Save*.



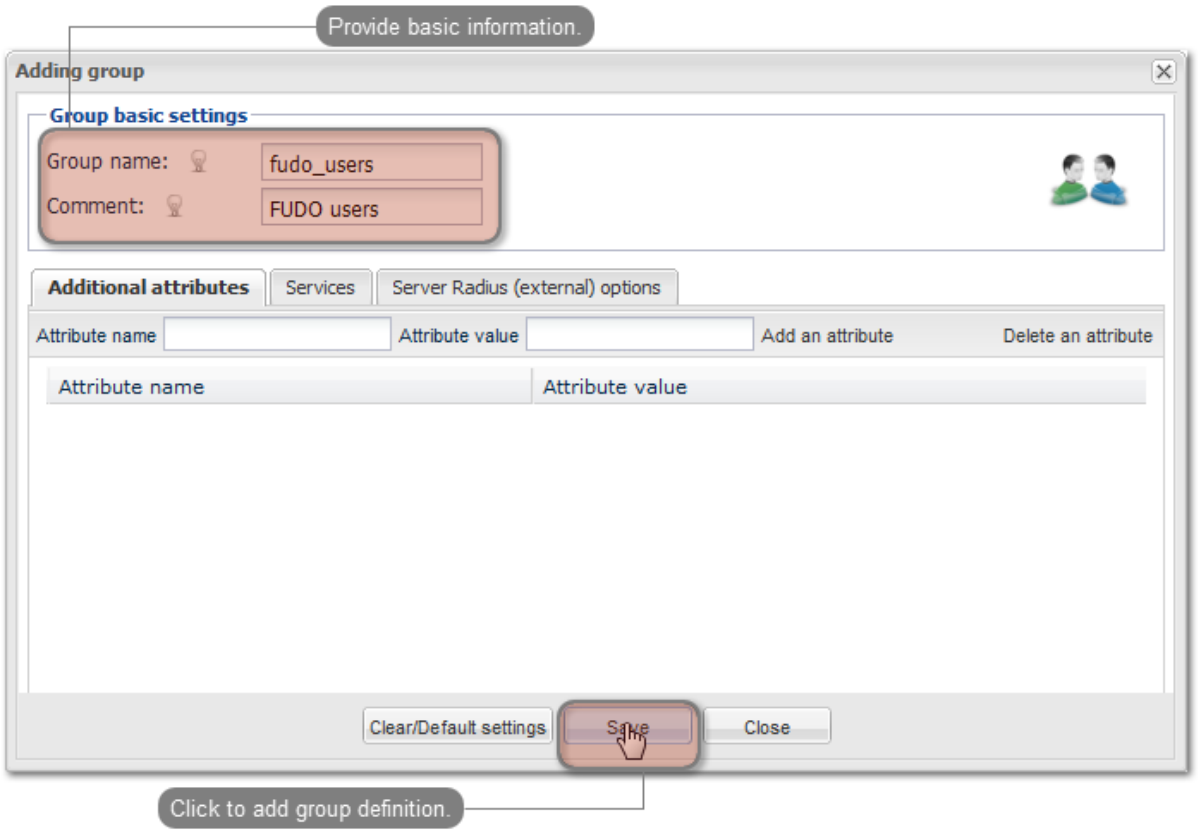
> **Note**
>
> Password will be required to define external authorization server in Fudo Enterprise administration panel.

2. Adding user group.

- Select *Groups* > *Add group* to define Fudo Enterprise users who will be authorized by the CERB server.

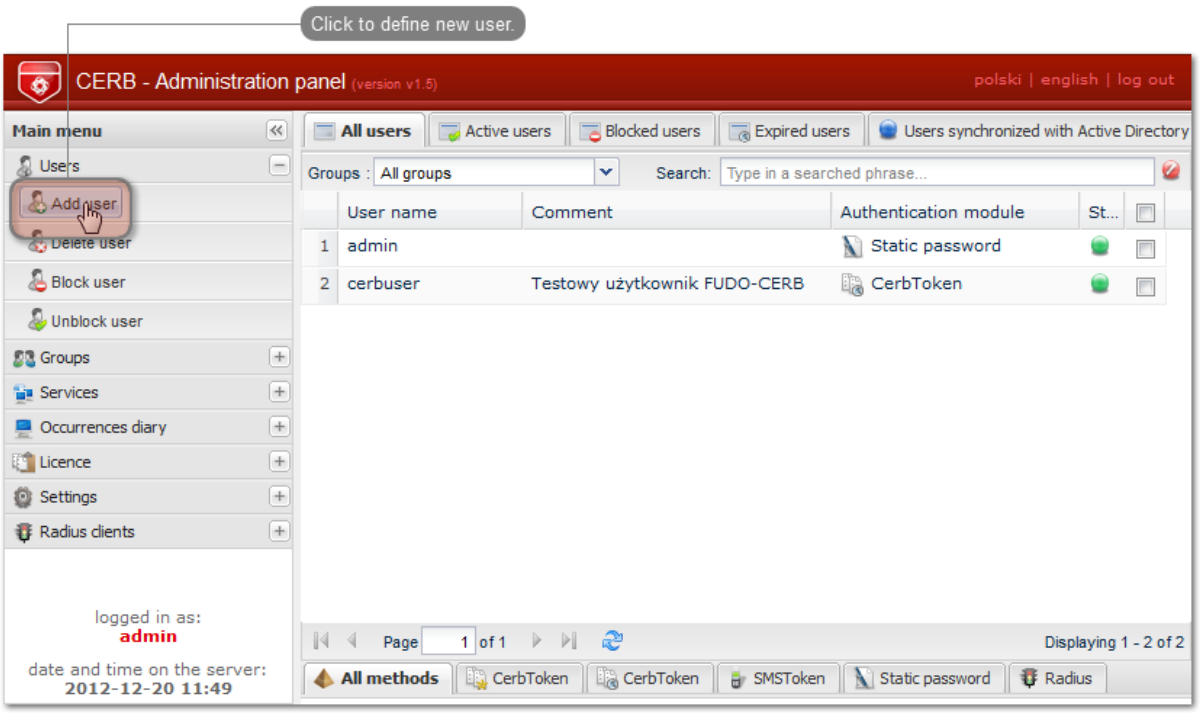


- Enter group's name (`fudo_users`) and click *Save*.

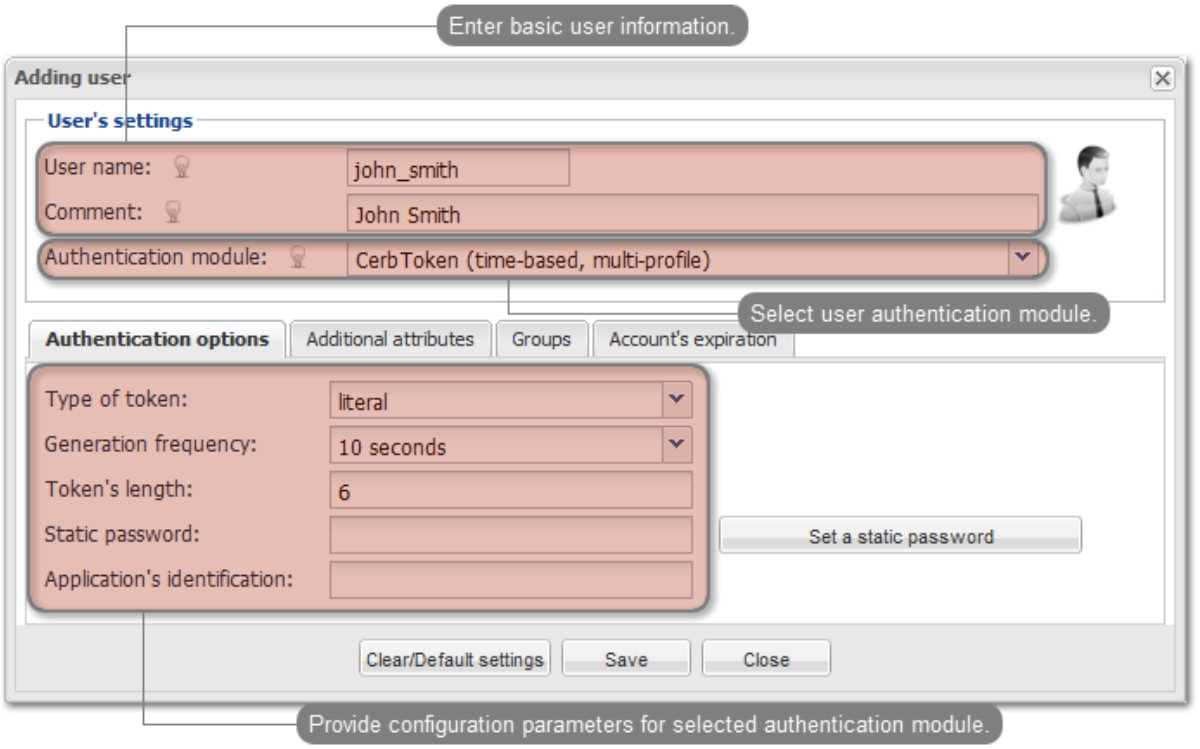


3. Adding user.

- Select *Users* > *Add user* to open new user definition window.



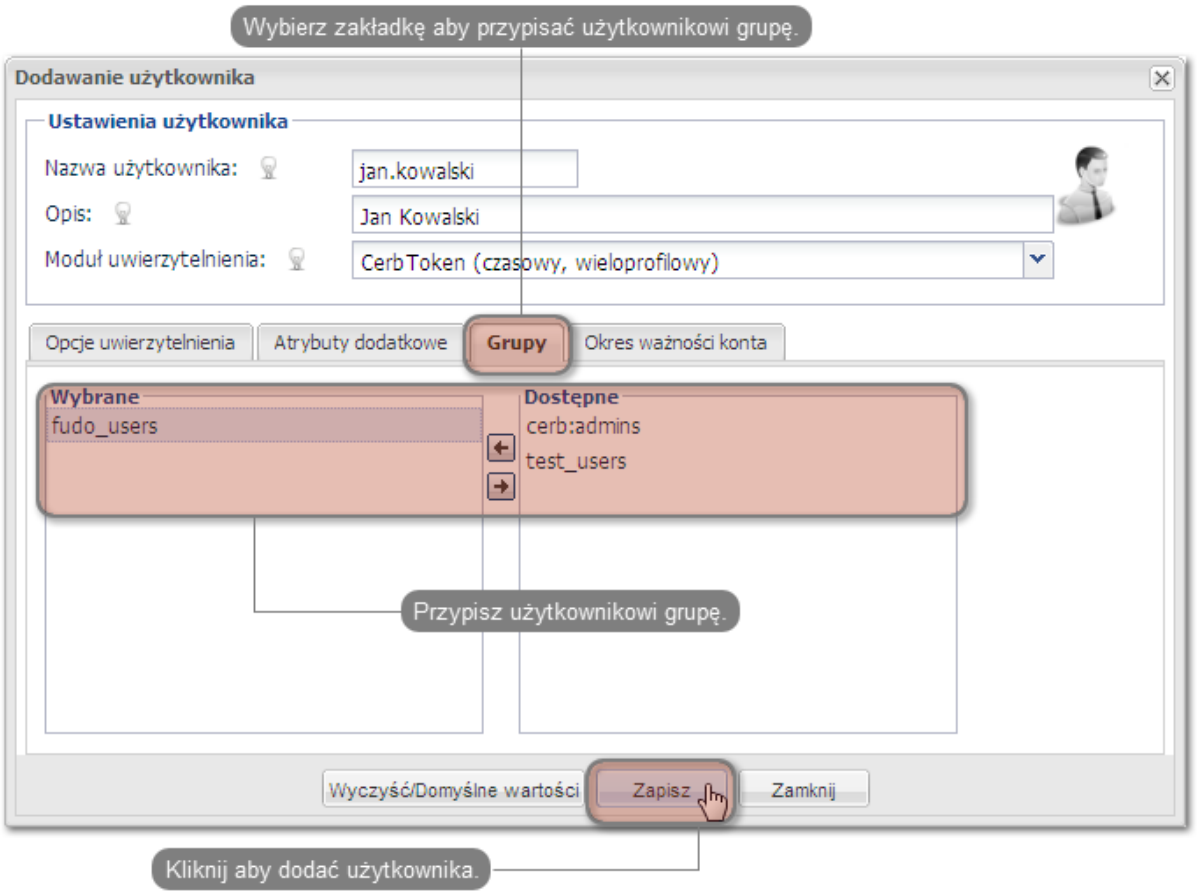
- Provide user name, description and select desired authorization module (refer to CERB server documentation form more information on authorization modules).



Note

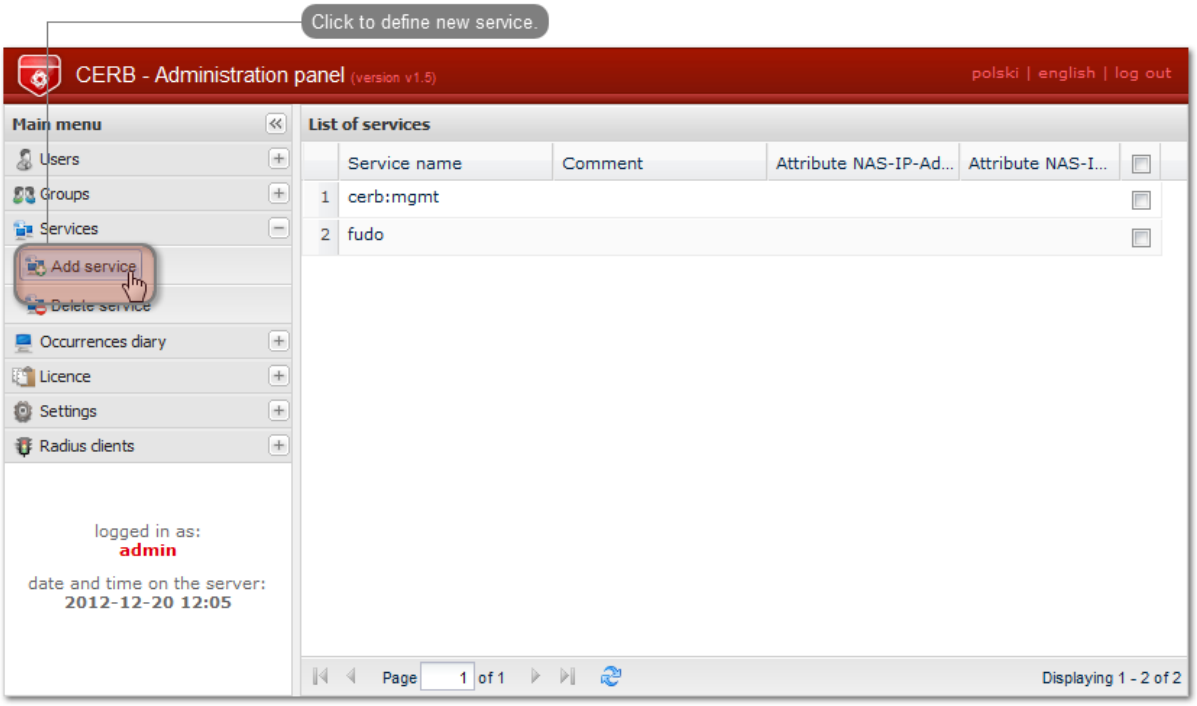
Username is used to authenticate users on Fudo Enterprise.

- Assign user to previously created `fudo_users` group and click *Save*.



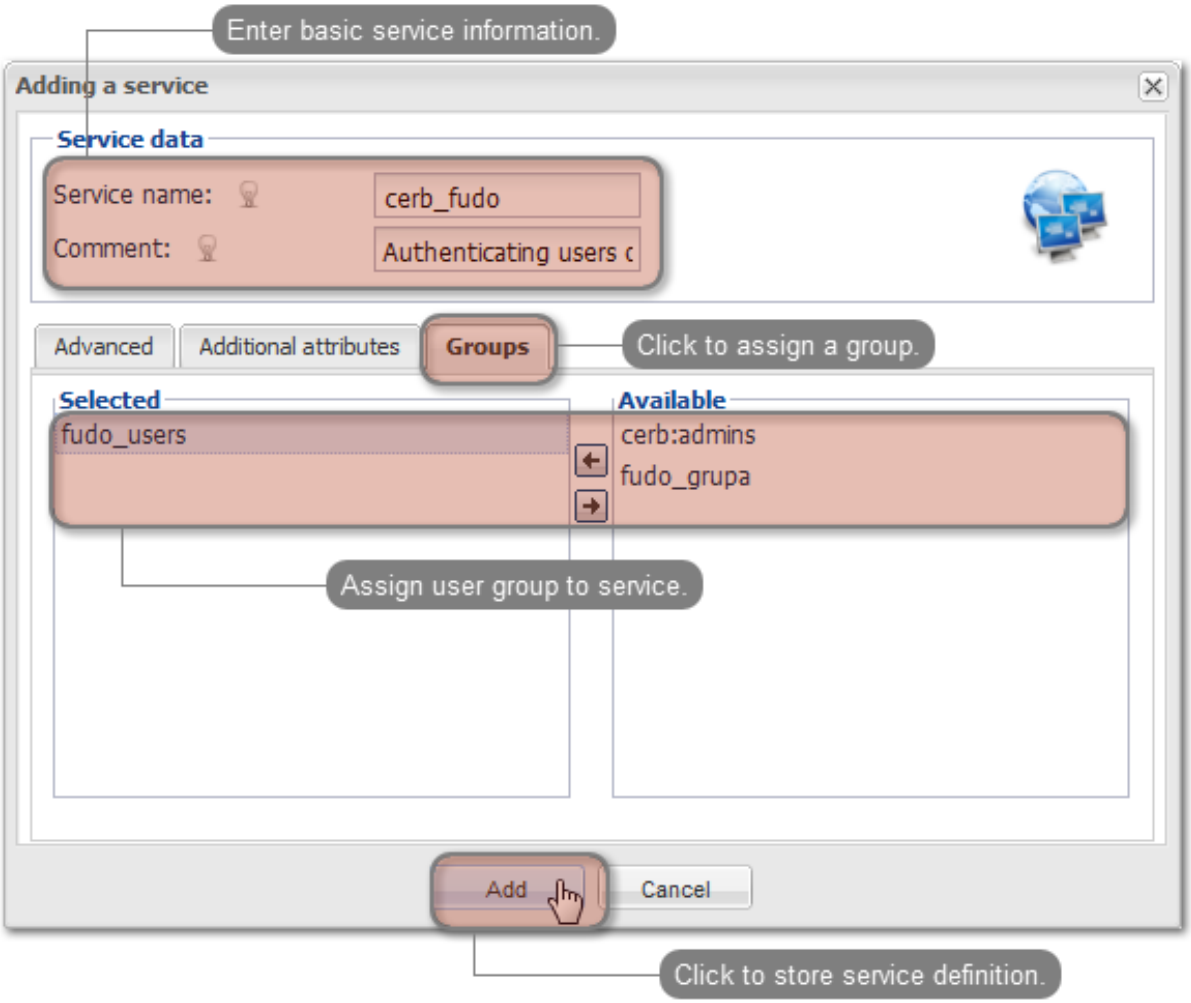
4. Configuring service.

- Select *Services* > *Add service* to open new service definition window.



- Provide name identifying authorization service (`cerb_fudo`) and service description.

- Add `fudo_users` group to service and click *Add*.

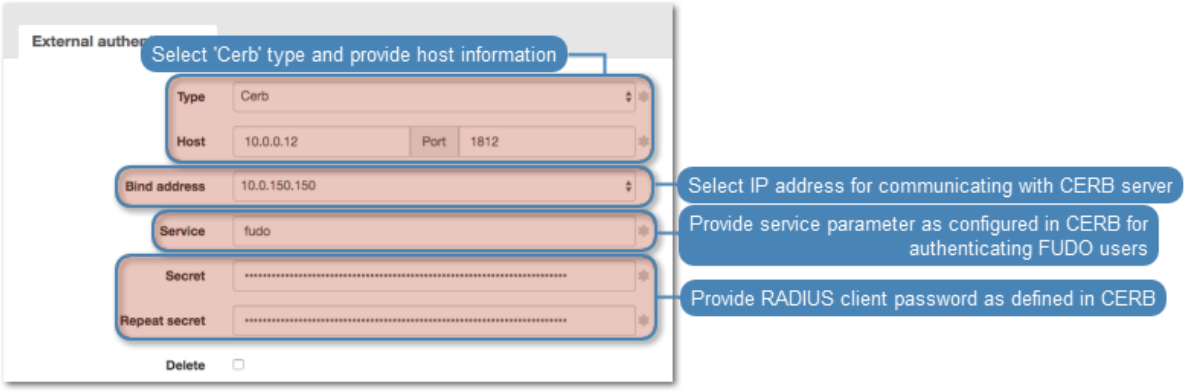


Fudo Enterprise server configuration

1. Adding CERB external authorization server.

- Select *Settings* > *External authentication*.
- Click *Add external authentication source* to add CERB server definition.
- Provide CERB server IP address, *secret* and service name identifying authorization service.

> **Note**
>
> Secret must match the RADIUS client password on CERB server. Service name must match the service name on CERB



- Click *Save*.

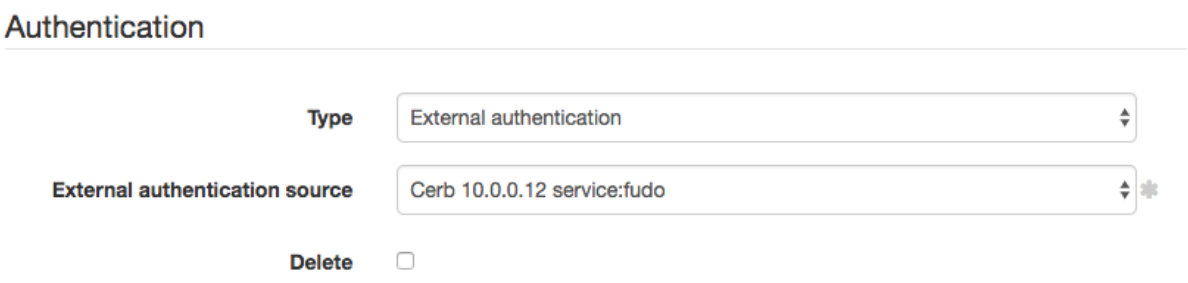
2. Adding user.

- Select *Management* > *Users*.
- Click *Add*.
- Provide basic user information.

Note

Username must match the user name defined on CERB server.

- Add safes that the user will be able to access.
- In the *Authentication* section, select *External authentication* from the *Type* drop-down list and select previously created Cerb server from the *External authentication source* drop-down list.



- Click *Save*.

Related topics:

- *Users*
- *Authentication*
- *User Authentication Methods and Modes*

12.19 System Maintenance

The following section contains descriptions of maintenance procedures.

Fudo Enterprise allows resizing internal system storage by applying the Virtual Hardware storage settings. Once respective VM changes are made, restart your Fudo instance, as described at the *Restart* page so that the current VM settings are taken by Fudo Enterprise.

12.19.1 Backing up Encryption Keys

Encryption keys stored on USB flash drives are necessary to initialize the file system, which stores session data. If the USB flash drive is lost or damaged, it will be impossible to boot the system and access session data.

Microsoft Windows

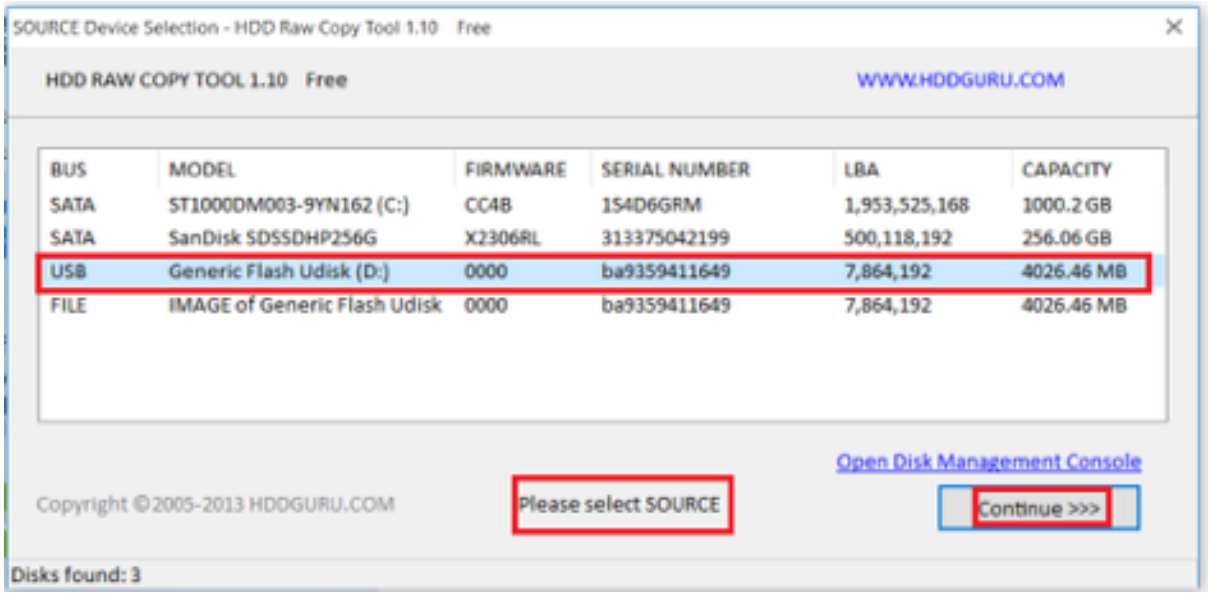
> **Warning**
>
> After connecting the flash drive to your computer, do not initiate or format it. Ignore the system message about it not being able to read data and proceed with the backup procedure.

1. Download and install *HDD Raw Copy Tool*.

   `http://hddguru.com/software/HDD-Raw-Copy-Tool/` (portable version is also available)

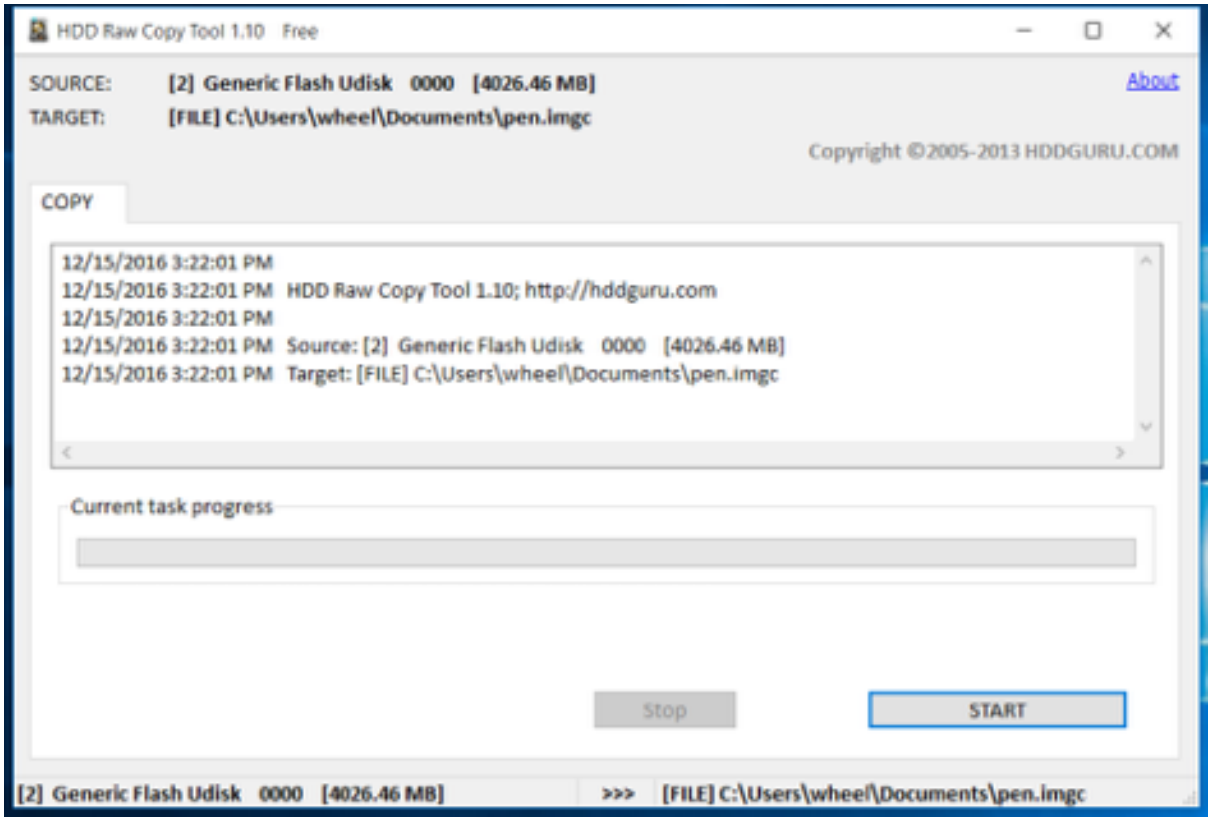
2. Start the program.

3. On the source drive selection window, choose the USB drive with the encription key and click *Continue*.



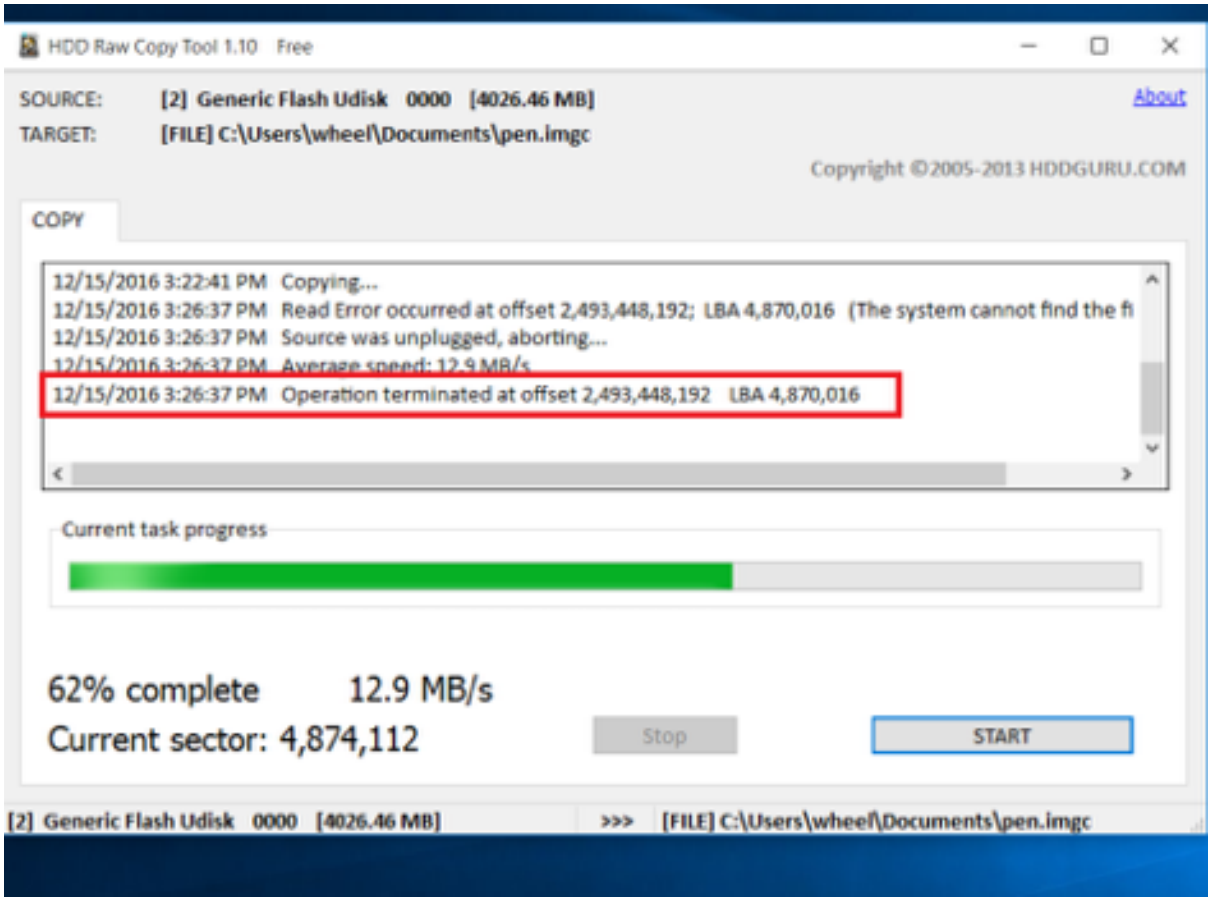
4. Click *FILE* twice, select the target image file and click *Continue*.

5. Click *START* to proceed with copying data.

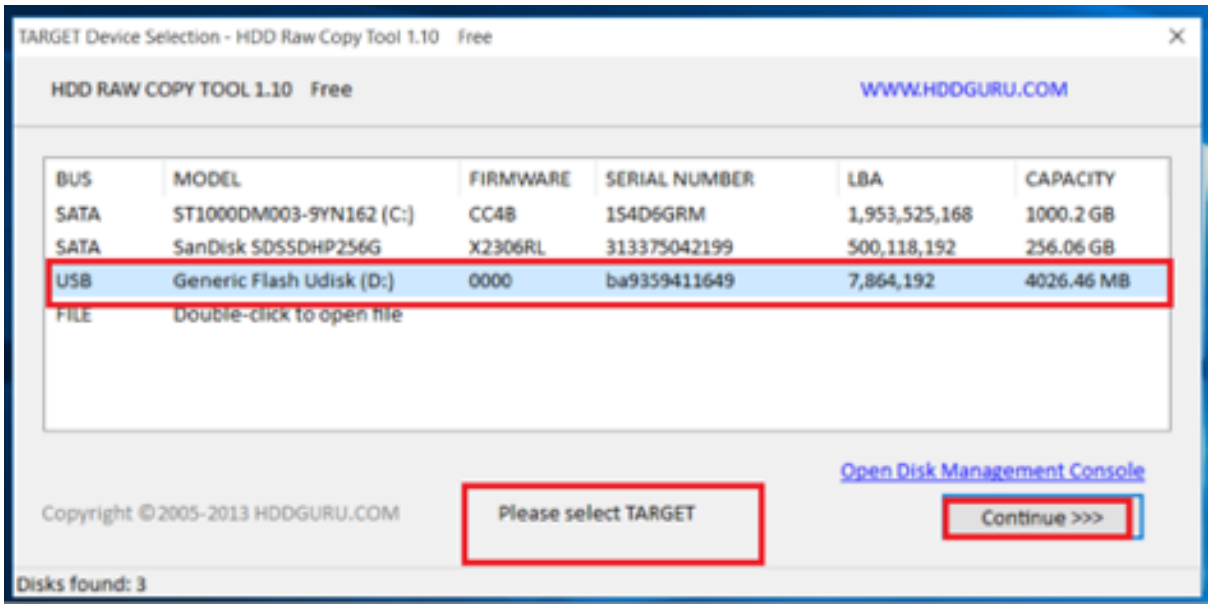


6. Once the following message occurs

   `Operation terminated at offset...` close the application and disconnect the USB drive.



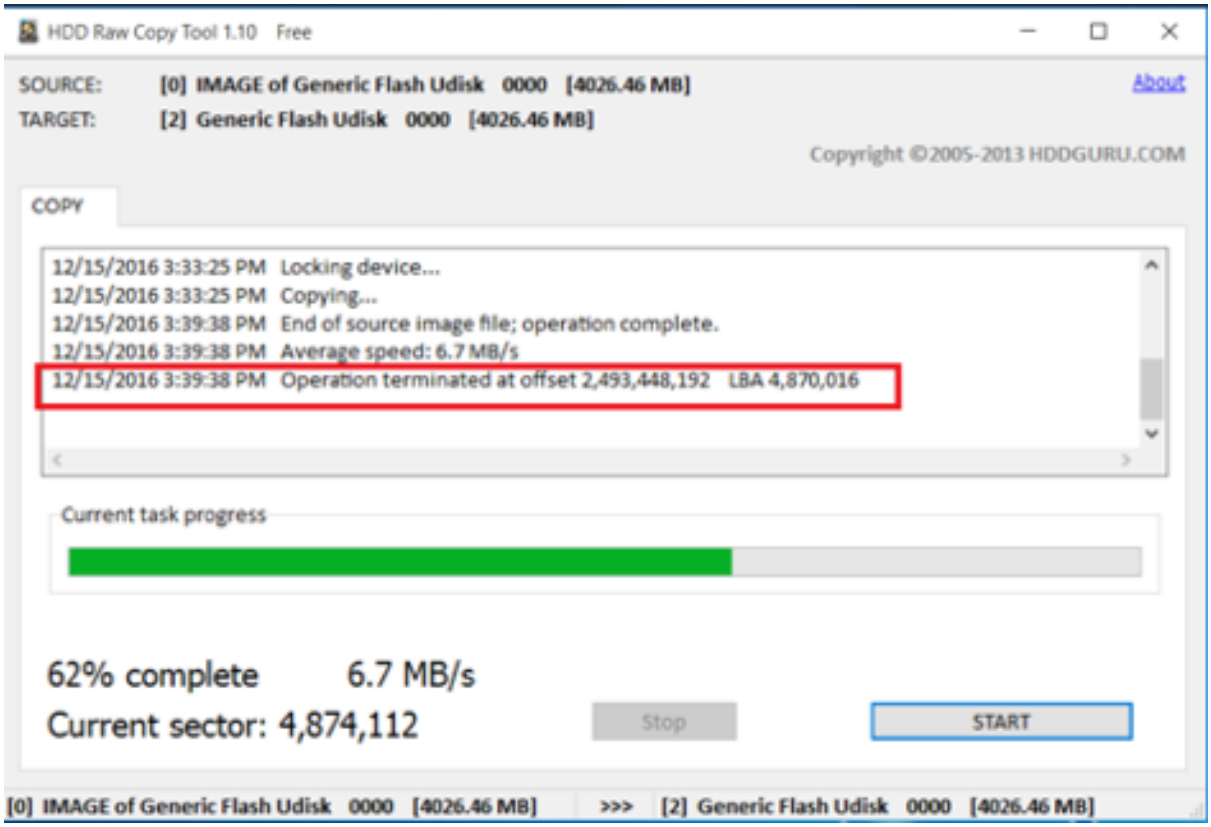
7. Connect another USB drive and start *HDD Raw Copy Tool*.
8. On the source drive selection screen select *FILE* and browse the file system to find the encryption keys image file.
9. Select the newly connected USB flash drive as a target device and click *Continue*.



10. Click *Continue*.
11. Click *START*.

12. The copying will end once the following message occurs:

```
Operation terminated at offset....
```



13. Close the application and disconnect the USB drive.

Mac OS X

1. Start the terminal.
2. Execute the `sudo -s` command and enter password.
3. Execute the `diskutil list` to list connected drives.
4. Find the drive with the following partitions layout:

```
/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. Execute the `dd if=/dev/disk2 of=fudo_pen.img bs=1m` command, where `if` points to the USB drive.
6. Disconnect the flash drive and connect the new one.
7. Execut the `dd if=fudo_pen.img of=/dev/disk2 bs=1m` command.
8. Execute the `sync` command.
9. Disconnect the USB flash drive from your computer.

Linux

1. Start the terminal.
2. Execute the `sudo -s` command and enter password.
3. Execute the `dmesg | less` command to determine the USB flash drive identifier.
4. Execute the `dd if=/dev/disk2 of=fudo_pen.img bs=1m` command, where `if` points to the USB drive.
5. Disconnect the flash drive and connect the new one.
6. Execut the `dd if=fudo_pen.img of=/dev/disk2 bs=1m` command.
7. Execute the `sync` command.
8. Disconnect the USB flash drive from your computer.

Related topics:

- *Events Log*
- *Frequently Asked Questions*

12.19.2 Monitoring System Condition

Monitoring system condition allows preventing system failures and overloads, ensuring Fudo Enterprise Fudo Enterprise remains operational.

Monitoring active sessions

1. Login to Fudo Enterprise administration panel.
2. Select *Dashboard*.
3. Check the number of currently running user sessions.

> **Note**
>
> Fudo Enterprise supports up to 300 RDP connections.

Monitoring network bandwidth

1. Login to Fudo Enterprise administration panel.
2. Select *Dashboard*.
3. Check current network transfer rate.

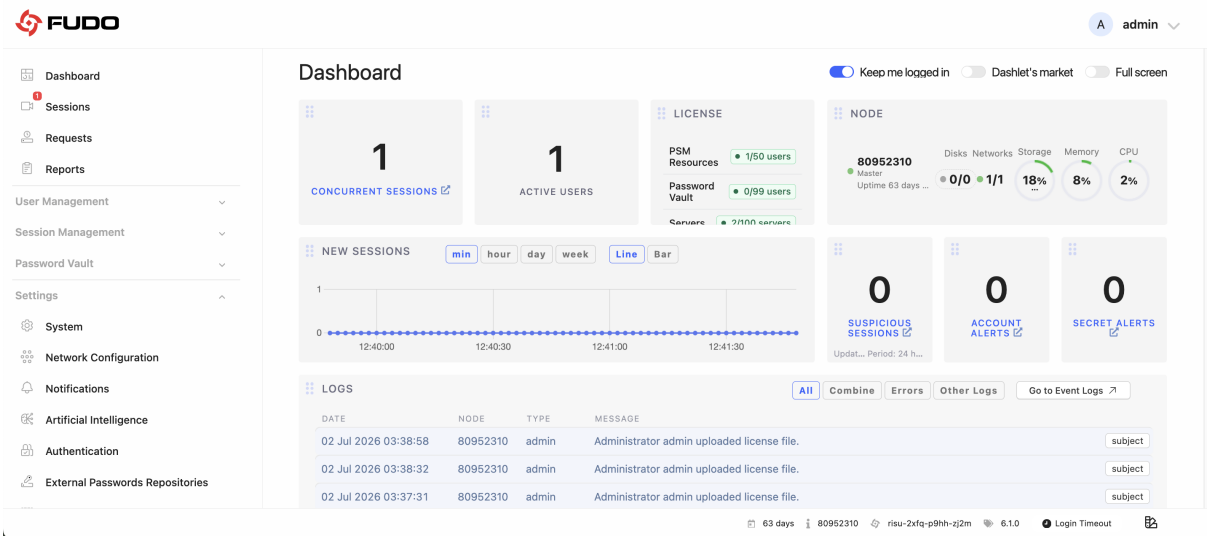
> **Note**
>
> Fudo Enterprise features 1Gbps network interface cards. In case the current network bandwidth usage exceeds 500Mbps, users may notice a decrease in system communication performance.

Monitoring storage

Warning

Fudo Enterprise will not allow new connections when storage usage reaches 90%.

1. Login to Fudo Enterprise administration panel.
2. Select *Dashboard*.
3. Check the storage usage percentage, review and delete archived sessions to free up space if need be.



Related topics:

- *System log*
- *Frequently asked questions*

12.19.3 Health Check

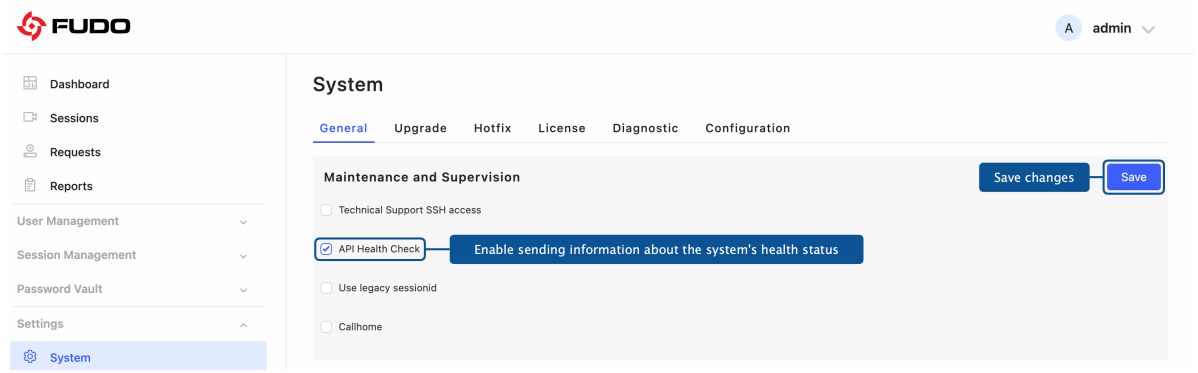
Fudo Enterprise regularly checks its "health" status. There are multiple tests that check the status of both hardware and software components. These tests are called "health checks".

The results of the health checks can be accessed by an administrator in two ways:

1. Using *SNMP*, which provides all *health check* results.
2. Using the *API health check* endpoint, which provides a summary of all *health checks*.

12.19.3.1 API Health Check

The *Health Check API* option is available under the *Maintenance and supervision* section of the *Settings* > *System* tab, in the *General* subtab.



Enabling this option activates an API endpoint that provides quick information about Fudo Enterprise's health status. This endpoint can be used by external systems to periodically monitor the state of Fudo Enterprise.

The information is returned as a JSON object:

```
{
   "status": "${value}"
}
```

The `${value}` may be set to:

- `ok`: if Fudo Enterprise works properly
- `error`: if Fudo Enterprise doesn't work properly and some of it functions may not be available.

Note

The health check status is designed to be simple and easy to interpret, therefore it doesn't contain detailed information about the problems that caused the error status. The detailed information about health check results can be obtained using *SNMP*.

Once the health check option is enabled, the following endpoint will be exposed at the URL path:

```
/api/v2/healthcheck
```

Warning

The API endpoint is accessible without authentication. It means that anyone having TCP access to Fudo Enterprise will be able to get information about its health status.

12.19.4 Callhome

Callhome service is a valuable tool designed to collect statistics on feature usage, offering insights into how often specific functions are utilized and identifying areas for improvement. This service also helps to enhance customer support by allowing certain tasks to be performed remotely and automatically. It simplifies the process of product maintenance and diagnostics, enabling the Fudo Support Team to gather essential data without direct user intervention.

Note

Callhome is intended solely for collecting diagnostic data and monitoring system status. For remote support, a separate function—*SSH Access*—must be enabled through the system settings to ensure secure and direct assistance when needed.

12.19.4.1 Data Collected by Callhome Service

The *Callhome* service automatically collects essential diagnostic data to ensure the Fudo Enterprise system remains optimized and secure. The following metrics are monitored:

- **Disk Status:** Keeps track of disk health to prevent failures.
- **Storage Utilization:** Monitors how storage resources are being used.
- **Sensor Temperatures:** Checks the temperature of various system sensors to avoid overheating.
- **Session Data Replication Status:** Monitors the replication status to ensure data integrity.
- **Critical Errors:** Logs any critical errors that could impact system performance.
- **System Crashes:** Records crashes to help identify and resolve issues quickly.
- **Version Deployment:** Gathers data on Fudo Enterprise version usage, including hours in operation and reported issues.

The *Callhome* service is designed with strict security measures in mind:

- Fudo Security **cannot make any changes** to the Fudo Enterprise system.
- Fudo Security **does not collect any data related to the client's configuration.**
- Fudo Security **does not collect or process any personal data** stored in Fudo Enterprise.

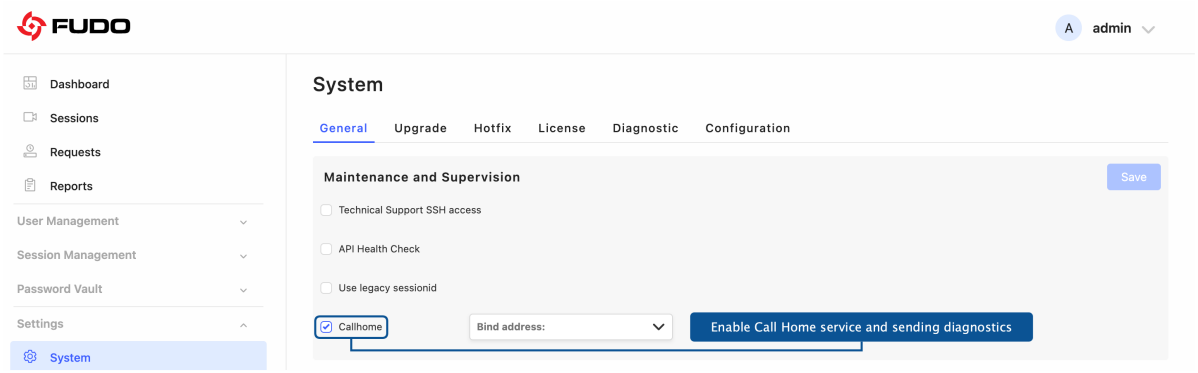
12.19.4.2 The Benefits of Using Callhome

- **Insight into Feature Usage:** Fudo Security gains visibility into which features are actively utilized by clients, enabling the prioritization and enhancement of the most valuable functionalities based on actual user preferences.
- **Priority Client Engagement:** Proactive users play a pivotal role in the development process. Their usage data directly informs future enhancements of Fudo Security products.
- **Version Tracking:** Provides immediate insight into which clients have upgraded and their current version, ensuring all users are operating on the most secure and efficient release.
- **Faster Issue Resolution:** Enables swifter problem resolution by reducing the need for extensive communication. Immediate access to diagnostics allows for quicker interventions.
- **Remote Management:** License updates, upgrades, and hotfixes can be deployed remotely, minimizing the need for client involvement.
- **Rapid Security Response:** In the event of a vulnerability, Fudo Security can implement hotfixes immediately, reducing exposure to threats and bypassing time-consuming communications.

12.19.4.3 Enable/Disable Callhome

In order to configure the Callhome service, proceed as follows:

1. Go to *Settings* > *System*.
2. Open the *General* tab, and go to the *Maintenance and Supervision* section.
3. Check the *Callhome* option.
4. Choose the IP address of your Fudo Enterprise instance or `Any` address.



Note

- The Callhome functionality requires an account created on Fudo Security servers. To create an account, contact your partner and provide your machine Fudo Unique Identifier (FUID). Check at the *Footer Information* page where you can see your FUID.
- The Fudo appliance initiate an outbound SSH connection to `home.fudosecurity.com` (IP:`178.33.6.1`, Port: `22`).
- Note: In previous versions, this feature was referred to as **Call Home**.

Related topics:

- *SSH Access*

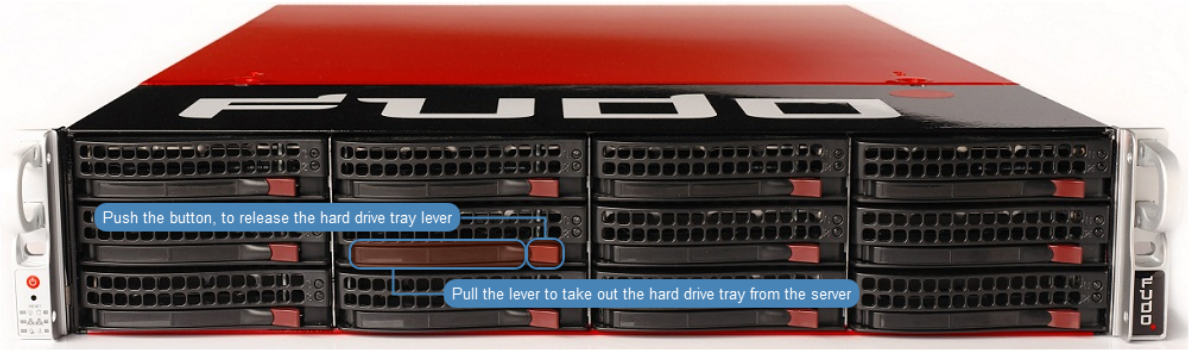
12.19.5 Hard Drive Replacement

In default configuration, Fudo Enterprise's storage array comprises 12 hard drives in RAIDZ2 configuration running ZFS file system allowing the system to remain fully operational in case of a failure of two hard drives.

Replacing a hard drive

1. Move the front bezel release latch to the left and take the front bezel off.

2. Push the hard drive tray lever release button and pull the lever to take out the tray from the chassis.



3. Unscrew the screws securing the hard drive and take out the hard drive from the tray.
4. Install replacement hard drive in the tray and secure it with the screws.
5. Install the hard drive tray back in the server.

Note

Fudo Enterprise will automatically detect the change in the storage array state and will start rebuilding the data structure. The duration of the array rebuilding process depends on the volume of data stored on the server.

Related topics:

- *Hardware Overview*
- *Frequently Asked Questions*

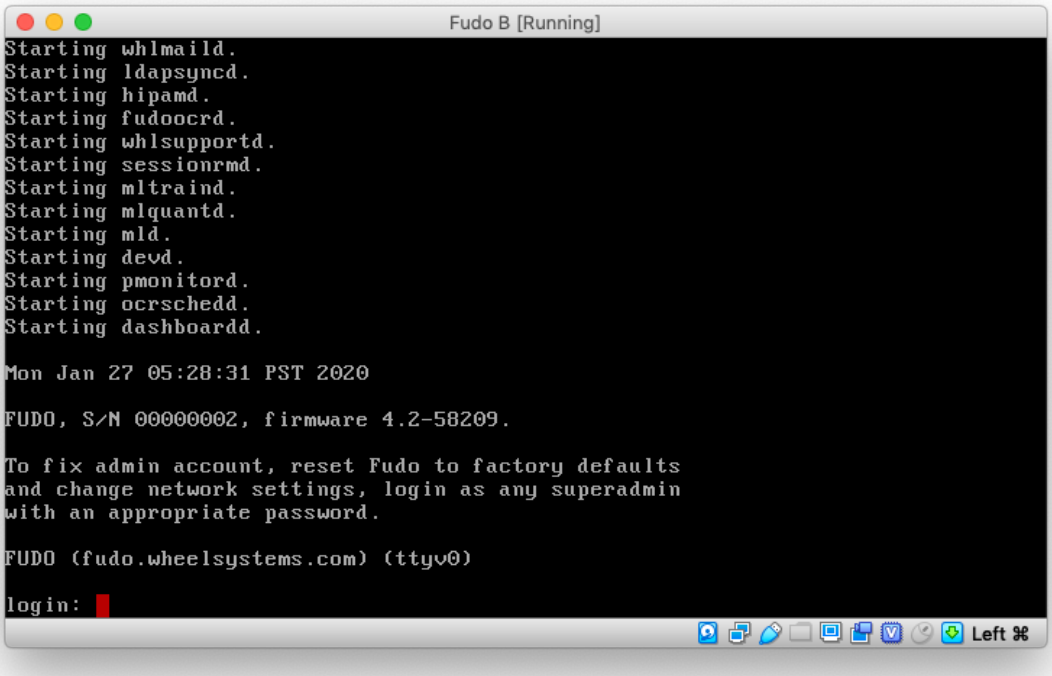
12.19.6 Resetting Configuration to Default Settings

Warning

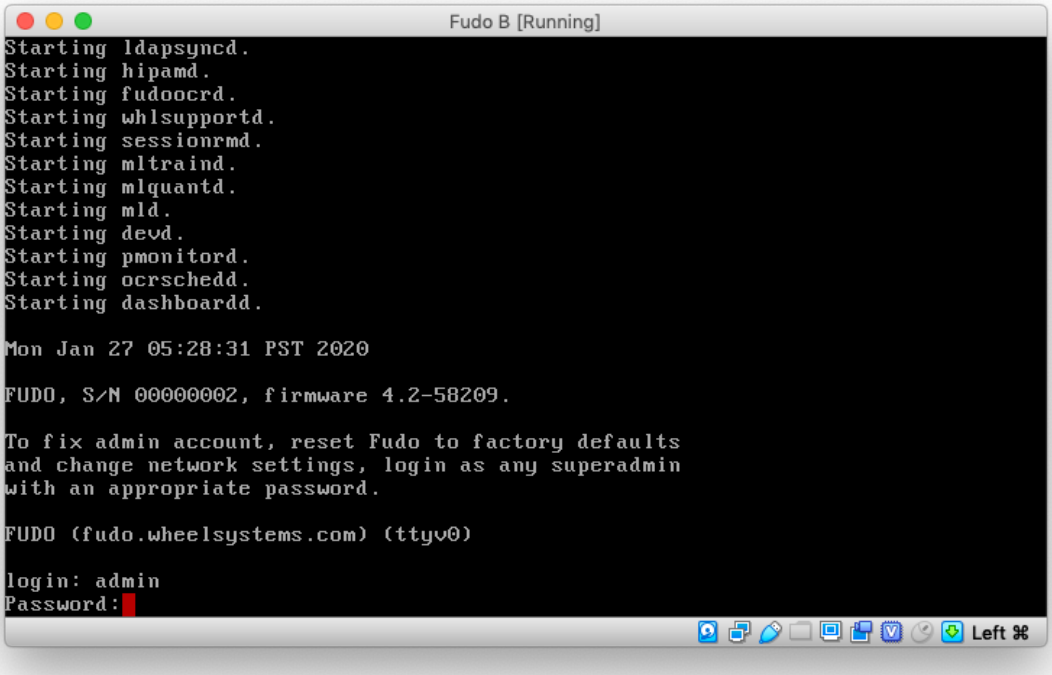
Configuration reset procedure is irreversible and it results in deleting all recorded sessions, system settings and defined objects. The device needs 2 pendrives plugged in to be properly executed.

1. Access system terminal.

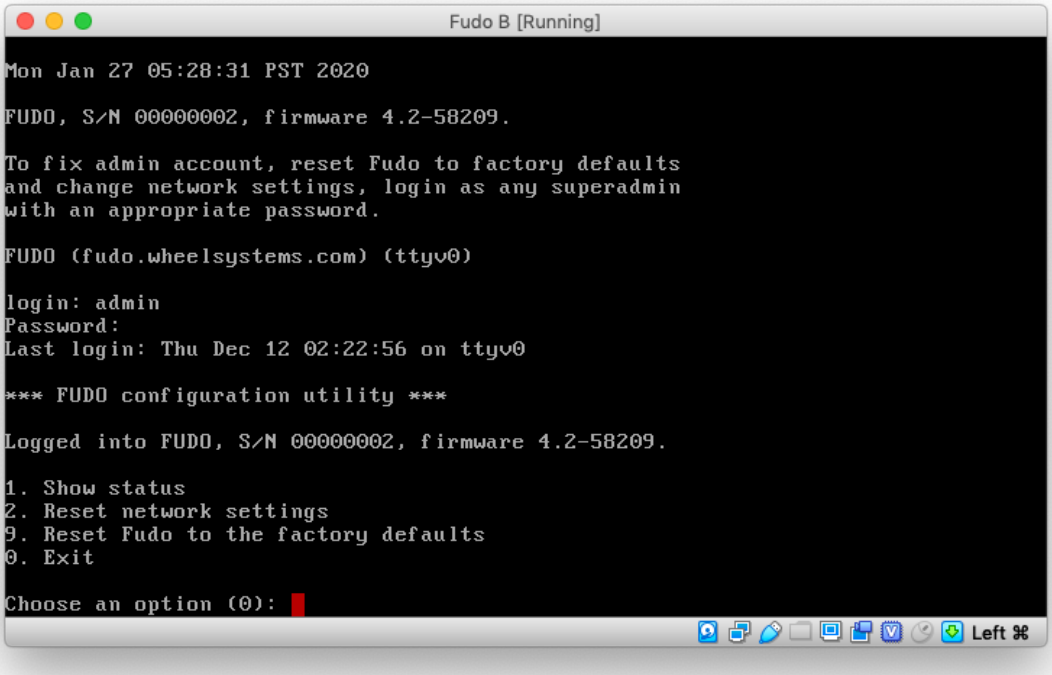
2. Enter administrator account login and press *Enter*.



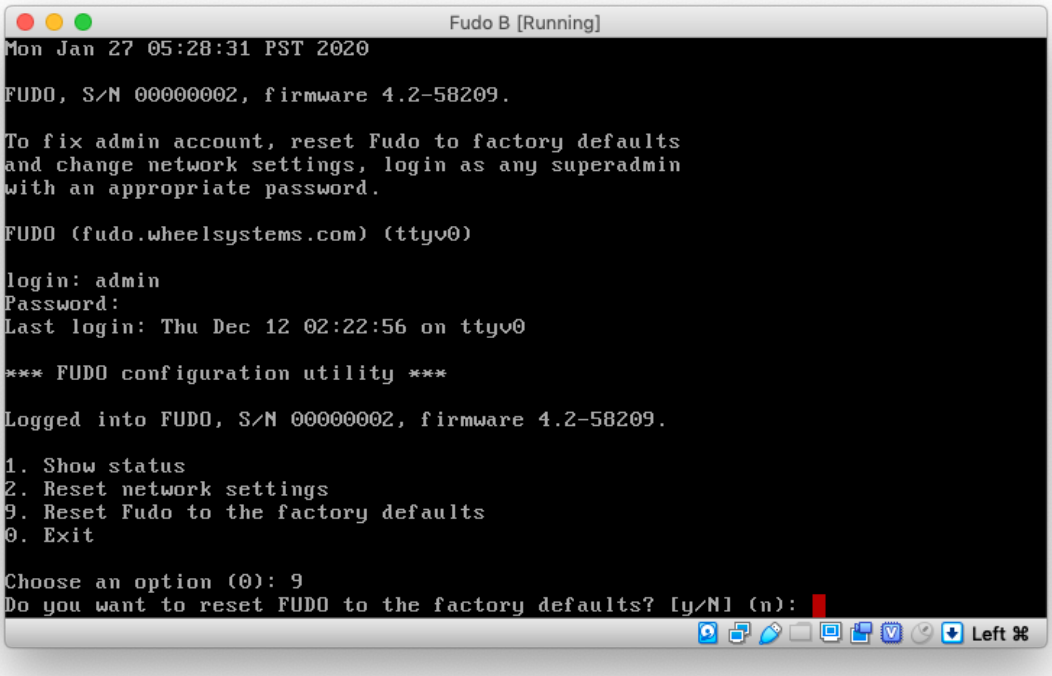
3. Enter administrator account password and press *Enter*.



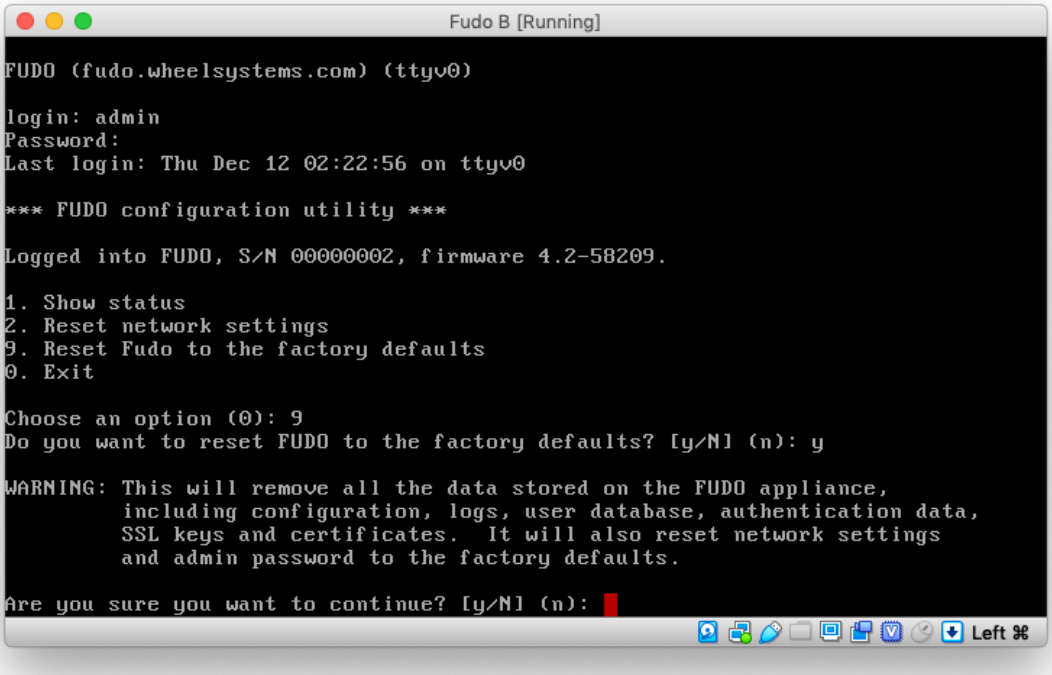
4. Enter 9 and press *Enter*.



5. Enter `y` and press *Enter*.



6. Enter `y` and press *Enter* to proceed with factory reset.



Note

In case you are returning a demonstration unit, remember to also erase the USB flash drive containing the encryption key.

Related topics:

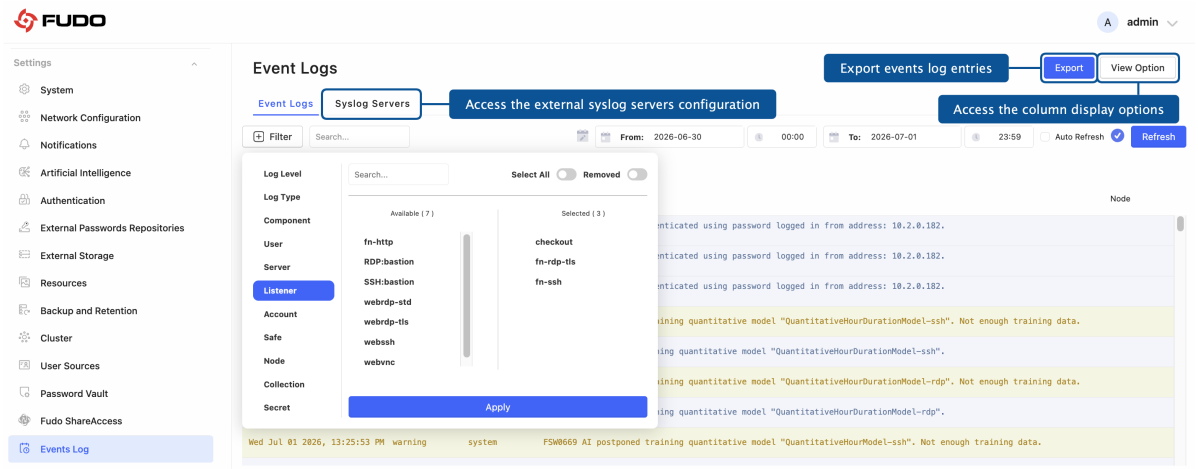
- *Network Interfaces Configuration*
- *System Maintenance*

CHAPTER 13

Events Log

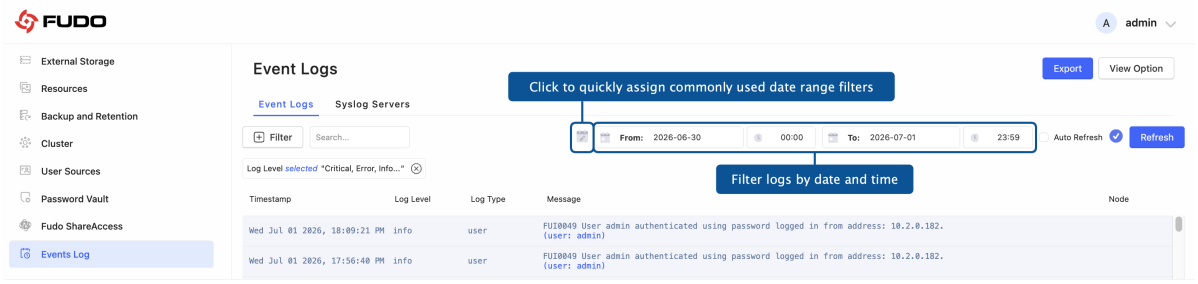
System log is an internal registry of users activities which influence system state (login information, administrative actions, etc.). Please refer to the *Log Messages* section for a list of key log messages.

To display system log contents, select *Settings* > *Events log*.



13.1 Filtering Logs by Date and Time

Logs can be filtered by date and time directly from the *date bar* located above the log list. Additionally, there is a set of commonly used date range filters, such as *Today*, *Last 24 Hours*, *This Week*, *Last 1 Hour*, *Last 1 Year*, etc., accessible through the calendar icon.

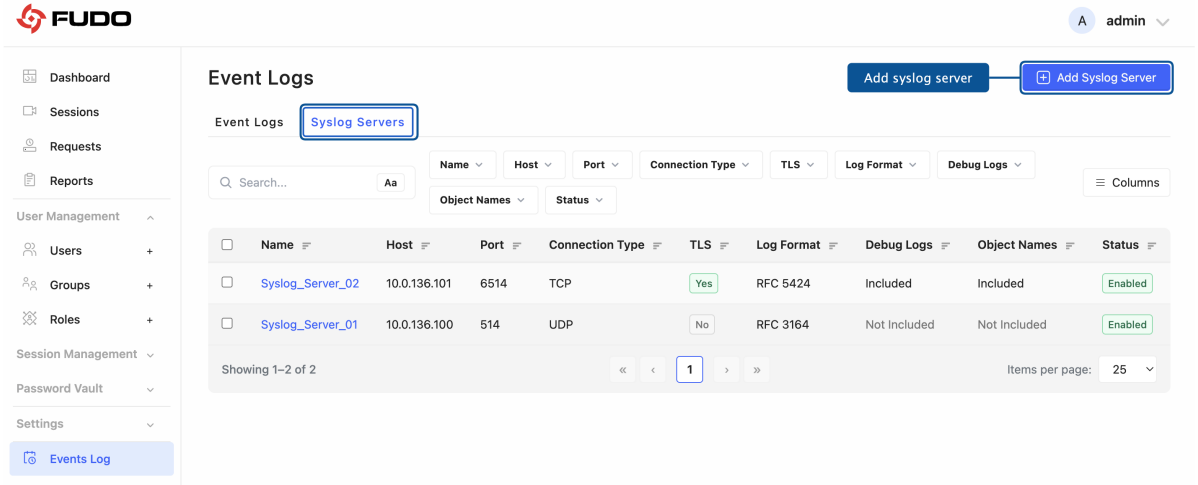


13.2 External Syslog Servers

Fudo Enterprise can forward event log entries to external *Syslog* servers. Configured servers are managed in the dedicated *Syslog Servers* view, available under Settings > Events log. The view lists each configured server together with its name, host, port, connection type, TLS status, log format, whether debug logs and object names are included, and whether the server is enabled.

Note

- Fudo Enterprise can communicate with syslog servers over the **UDP** or **TCP** transport. TLS encryption is available for connections that use the **TCP** transport.
- Event log entries can be forwarded in the **RFC 3164** (BSD, default) or the **RFC 5424** format. The log format is selected individually for each server.
- Messages are sent to the syslog server through the network interface that has the **Admin Panel** purpose selected in the network configuration. The IP address used must either be able to reach the target host's network directly or use the default gateway. For more information, refer to the *Network Interfaces Configuration* section.
- During an upgrade from version 6.0 or earlier, an existing syslog configuration is automatically migrated to the new syslog server model as **UDP** syslog servers using the **RFC 3164** log format.

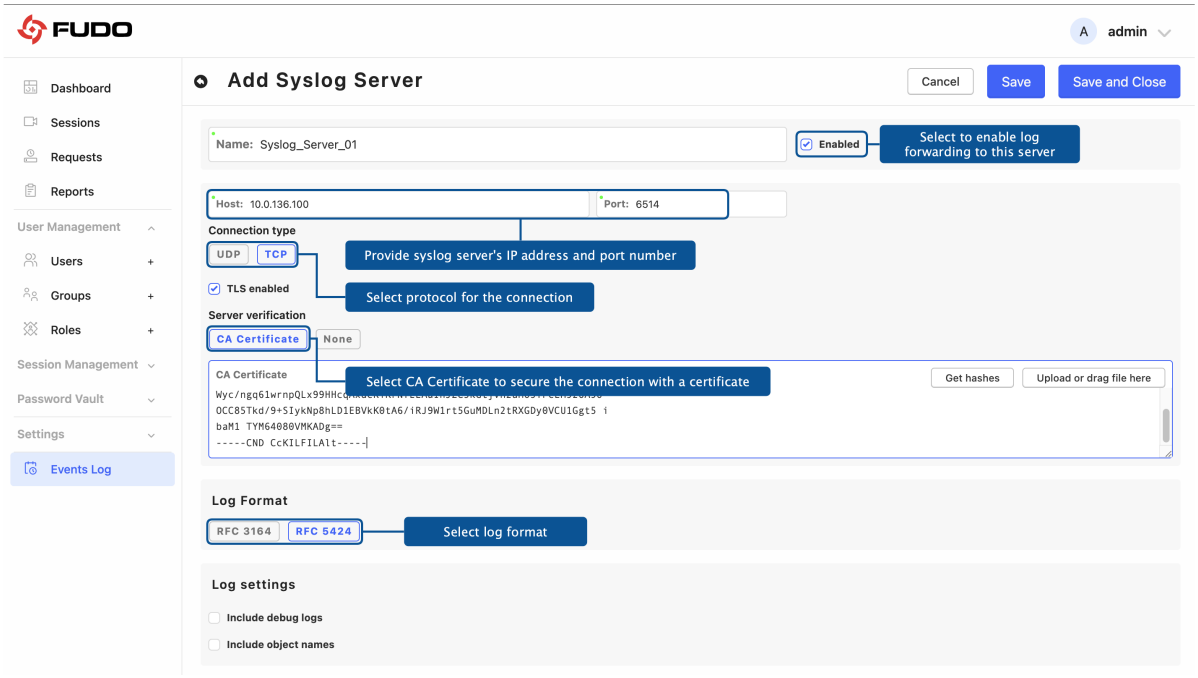


Adding a Syslog Server

To add a *Syslog* server, proceed as follows.

1. Select *Settings* > *Events log*.

2. Open the *Syslog Servers* tab and click *Add Syslog Server*.
3. In the *Name* field, enter a unique name for the server.
4. Provide the server's *Host* and *Port* (the default port is *514* for *UDP* and *6514* for *TCP* connections).
5. Set *Connection type* to *UDP* or *TCP*.
6. For a *TCP* connection, select *TLS enabled* to encrypt the transmission. Under *Server verification*, select *CA Certificate* and paste or upload the CA certificate used to verify the syslog server, or select *None* to connect without verifying it.
7. Under *Log Format*, select *RFC 3164* to send messages in the BSD format, or *RFC 5424* to send them in the RFC 5424 format.
8. Optionally, under *Log settings*, select *Include debug logs* and *Include object names*.
9. Make sure the *Enabled* option is selected to activate log forwarding to this server.
10. Click *Save*.



Note

- Log entries sent to syslog servers that use the *RFC 3164* log format are formatted as follows:

  `[level] TIMESTAMP TAG[PID]: MESSAGE`

  where:

  - `level` – log level (optional),
  - `TIMESTAMP` – time of the log entry,
  - `TAG` – application name, always `fudo`,
  - `PID` – process ID,

  - `MESSAGE` – the actual log message, preceded by the component or module name.

- Example:

```
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.
```

- For servers that use the *RFC 5424* log format, the message header is built according to RFC 5424:

  `<PRI>VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID SD MESSAGE`

  where:

  - `PRI` – priority value derived from the `local7` facility and the log level,
  - `VERSION` – format version, always `1`,
  - `TIMESTAMP` – time of the log entry in UTC, in the RFC 3339 format with microsecond precision,
  - `HOSTNAME` – Fudo Enterprise host name,
  - `APP-NAME` – application name, always `fudo`,
  - `PROCID` – process ID,
  - `MSGID` – message identifier, always `-`,
  - `SD` – structured data field, always empty (`-`),
  - `MESSAGE` – the actual log message, preceded by the component or module name.

- The message content is identical for both log formats. In the *RFC 5424* format, Fudo Enterprise context data (object IDs and names) stays in the message content and is not moved to the structured data field.
- For detailed list of log messages, refer to the *Log Messages* topic.

Editing Syslog Server Definition

To edit a *Syslog* server definition, proceed as follows.

1. Select *Settings* > *Events log*.
2. Open the *Syslog Servers* tab and click the name of the server you want to edit.
3. Modify the server definition as needed.
4. Click *Save*.

Deleting Syslog Server Definition

To delete a *Syslog* server definition, proceed as follows.

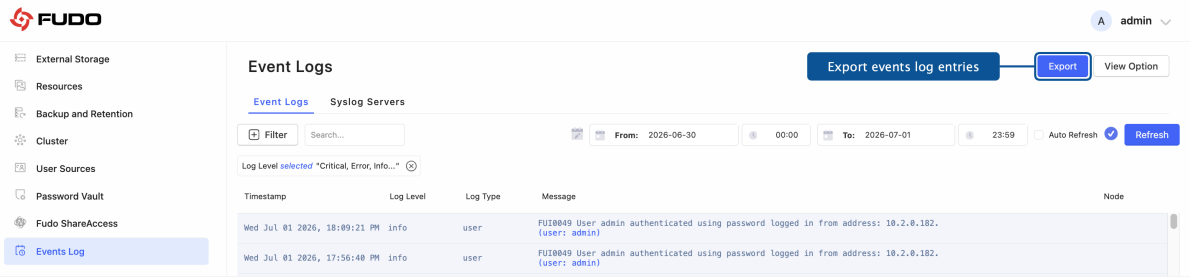
1. Select *Settings* > *Events log*.
2. Open the *Syslog Servers* tab.

3. Select the checkbox next to the server you want to remove.
4. Click *Delete selected* and confirm the deletion.

13.3 Exporting Events Log

To export events log entries, proceed as follows.

1. Select *Settings* > *Events log*.
2. Click *Export* and select where to save exported log entries.



Related topics:

- *Log Messages*
- *Security*
- *Managing servers*

CHAPTER 14

Account Activity in the User Access Gateway (UAG)

Fudo Enterprise allows configuring an option to be informed about existing connection.

The **Resource in use** feature works while establishing connection to the target server, to which another user is already connected via the same account. If the user continues establishing connection, the session is terminated.

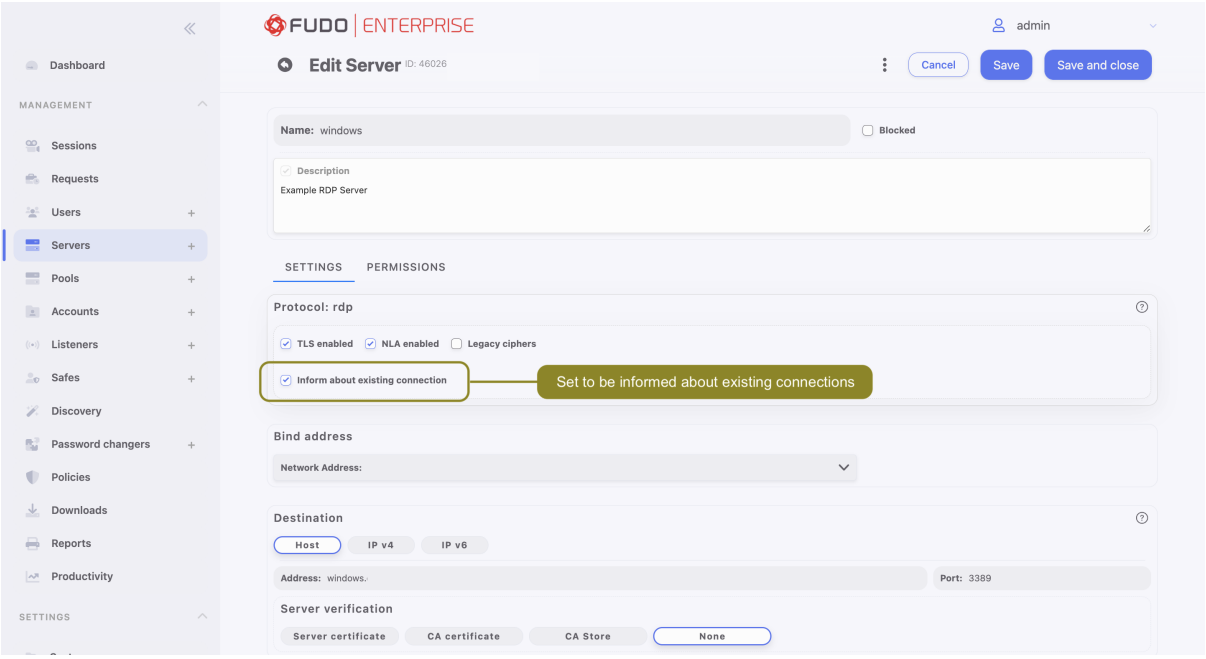
Warning

This option is available for RDP connections only.

In order enable the *Resource in use* option for the RDP connections, follow the instruction:

1. Select *Management* > *Servers*.

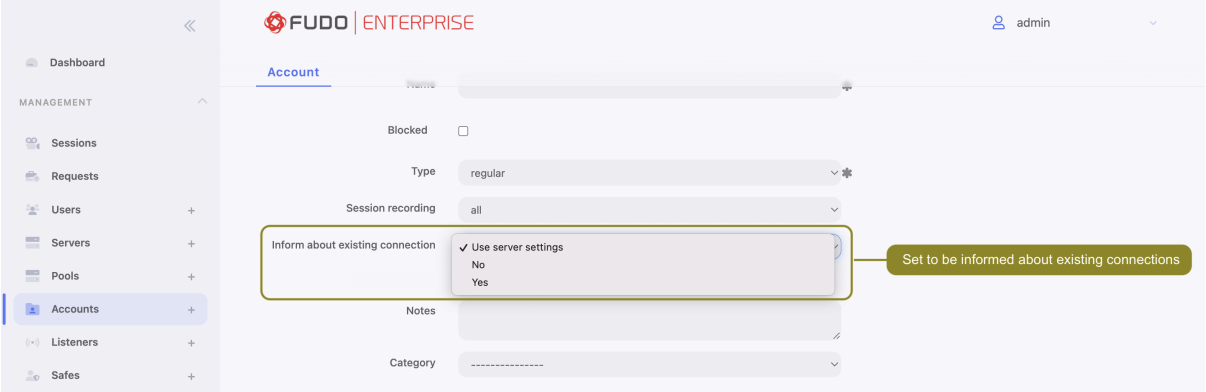
- Define filters to limit the number of objects displayed on the list, or select an RDP server that needs to be edited right from the list.
- Check the *Inform about existing connection* option in the *Settings* section.



- Click *Save* or *Save and close*.

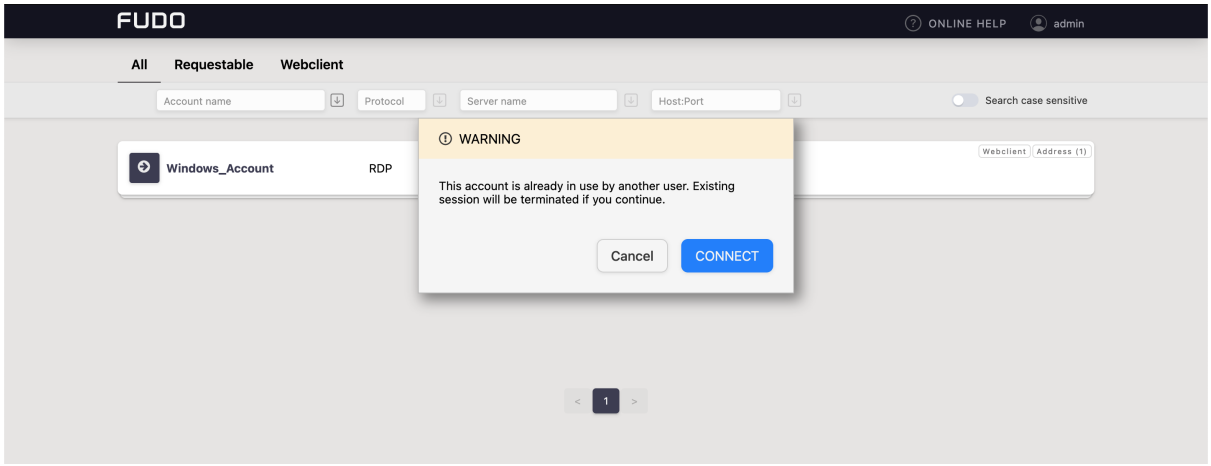
2. Select *Management* > *Accounts*.

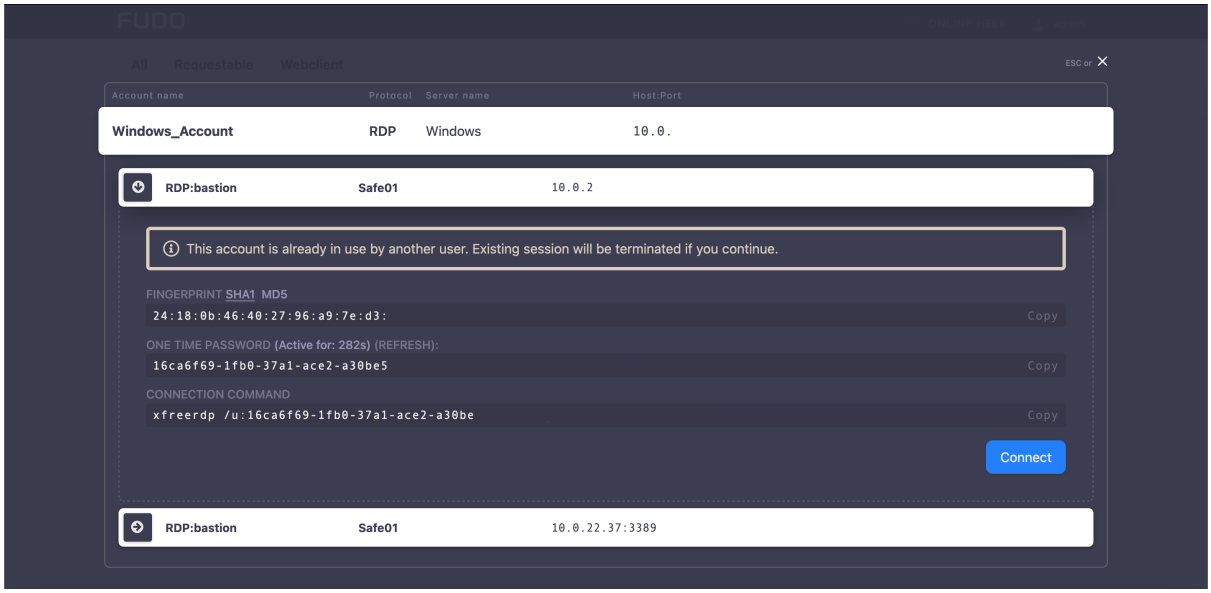
- Define filters to limit the number of objects displayed on the list, or select an account with access to an RDP server that needs to be edited right from the list.
- In the *Inform about existing connection* field select:
  - `Use server settings` to inherit the settings of the server, which was added to the account in the *Server* section,
  - `Yes` to enable functionality (independently from the server settings),
  - `No` to disable functionality.



- Click *Save*.

Information about existing connection will be presented to the user in the User Access Gateway. Here is the default message:

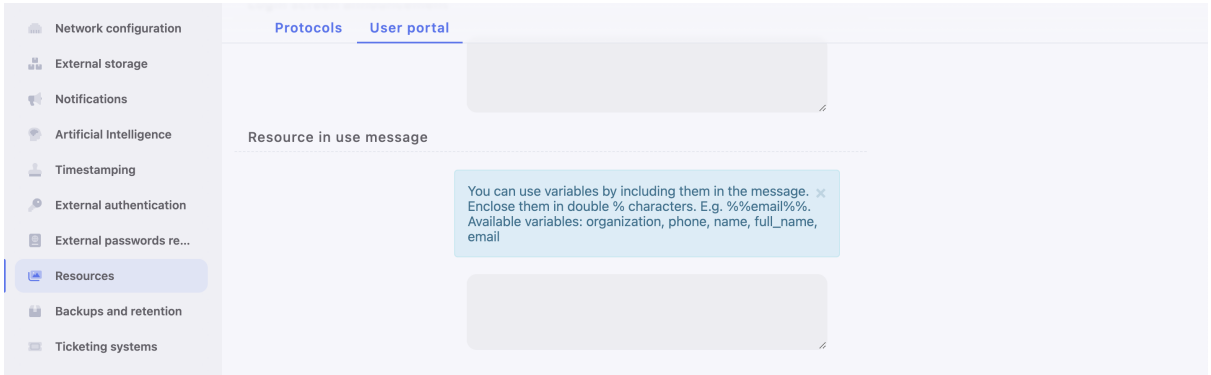




You can customize that message by including variables (`organization`, `phone`, `name`, `full_name`, or `email`), enclosed in double %% symbols. E.g., `%%email%%`.

In order to do that:

1. Select *Settings* > *Resources* > *User portal* tab.
2. Provide a new message in the *Resource in use message* field.
3. Click *Save*.



Related Topics:

- *Creating an RDP Server*
- *User Portal Configuration*

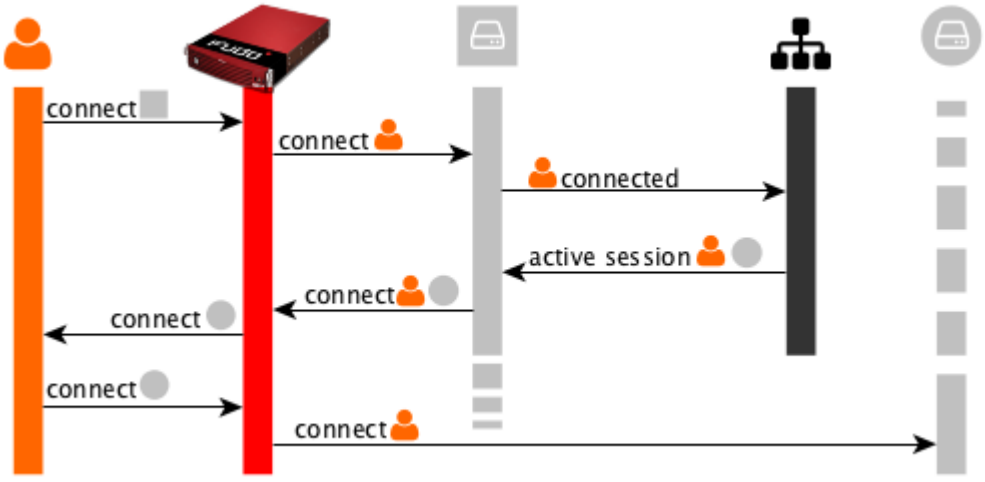
CHAPTER 15

Reference Information

15.1 RDP Connections Broker

Connections broker enables users to reconnect to their existing sessions on a specific server within a pool of load-balanced resources.

If the broker identifies an existing user session on another server, the connection will be redirected to it and the user will be prompted to login again.



Note

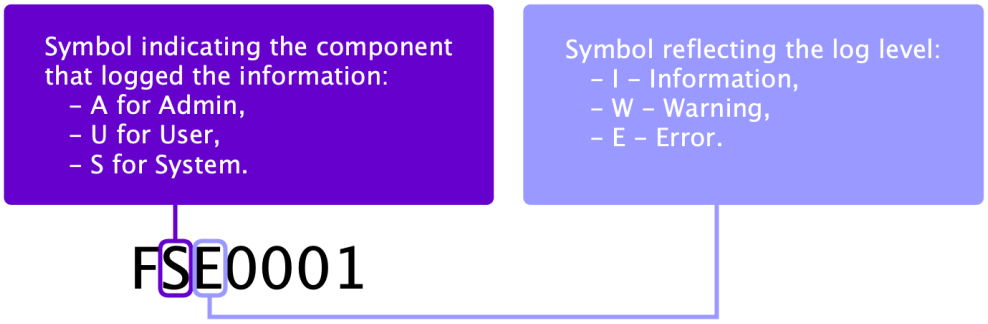
To successfuly redirect a connection, the server identified by the broker must be defined on Fudo Enterprise, it must listen on default RDP port (3389) and user must be allowed to connect to given server.

Related topics:

- *Data Model*
- *RDP*
- *Servers*
- *Accounts*

15.2 Log Messages

The message code provides information about the type of log message and the component that generated it.



The second symbol of the code indicates the component associated with the log:

- A for Admin,
- U for User,
- S for System.

The third symbol reflects the log level*:

- I for Information,
- W for Warning,
- E for Error.

Note

*There are also Critical and Debug log levels, which are intended for internal use. These logs may change without notice and should not be relied upon by users.

Message code	Log level	Component type	Message
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.
FSE0005	ERROR	SYSTEM	Unable to initialize %s.
FSE0006	ERROR	SYSTEM	Invalid license.
FSE0007	ERROR	SYSTEM	Unable to find license file.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSE0008	ERROR	SYSTEM	Unable to attach disk %s.
FSE0009	ERROR	SYSTEM	Upgrade failed.
FSE0010	ERROR	SYSTEM	License expired.
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.
FSI0019	INFO	SYSTEM	Disk %s replaced. Data synchronization may take a while.
FSI0021	INFO	SYSTEM	Disk %s attached.
FSI0023	INFO	SYSTEM	Manual encryption does not support disk hot-swap: %s.
FSE0024	ERROR	SYSTEM	Disk belongs to another Fudo: %s.
FSI0025	INFO	SYSTEM	Cluster node %s (%s) host key set to '%s'.
FSE0026	ERROR	SYSTEM	Cluster communication error.
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).
FSI0041	INFO	SYSTEM	Initial connection from master cluster node.
FSI0042	INFO	SYSTEM	Cluster node %s (%s) connected from address %s.
FSI0044	INFO	SYSTEM	Connected to cluster node %s (%s) on address %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/%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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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.
FUW0059	WARNING	USER	User %s, logging in from address %s, has more than one 'password' method, using the first password.
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.
FSI0071	INFO	SYSTEM	Established gateway connection from %s to %s (%s:%u).
FSI0072	INFO	SYSTEM	Established transparent connection from %s to %s (%s:%u).
FSI0073	INFO	SYSTEM	Bastion connection from %s to %s (%s:%u).
FSW0074	WARNING	SYSTEM	Connection terminated because license has expired or was not set.
FSW0075	WARNING	SYSTEM	Connection terminated because number of nodes in cluster exceeded license limit.
FSE0076	ERROR	SYSTEM	Unable to establish connection, could not find specified transparent server (tcp://%s:%u).
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.
FUW0088	WARNING	USER	Session has been terminated due to exceeding the time window defined in the connection %s time policy.
FUE0089	ERROR	USER	Authentication timeout.
FSE0090	ERROR	SYSTEM	Unable to connect to the passwords repository server %s.
FSE0091	ERROR	SYSTEM	Unable to add server %s.
FSE0092	ERROR	SYSTEM	Passwords repository server %s communication error.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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.
FUI0100	INFO	USER	HTTP connection beetwen client and server initiated.
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.
FUE0114	ERROR	USER	TLS Security configured, but missing TLS certificate.
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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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.
FSE0148	ERROR	SYSTEM	Listening on %s:%u failed while adding bastion %s.
FAI0149	INFO	ADMIN	User %s deleted previous system version.
FAI0150	INFO	ADMIN	User %s changed backup and retention settings.
FAI0151	INFO	ADMIN	User %s %s bastion %s.
FAI0152	INFO	ADMIN	User %s deleted bastion %s.
FSE0153	ERROR	SYSTEM	Session indexing failure.
FSE0154	ERROR	SYSTEM	Session conversion failure for session %s.
FSI0155	INFO	SYSTEM	Starting encoding session video %s.
FSI0156	INFO	SYSTEM	Completed session video %s encoding.
FAI0157	INFO	ADMIN	User %s %s failover configuration.
FAI0158	INFO	ADMIN	User %s added node %s.
FAI0159	INFO	ADMIN	User %s changed %s in node %s.
FAI0160	INFO	ADMIN	User %s deleted node %s.
FAI0161	INFO	ADMIN	User %s disconnected node from the cluster.
FAI0162	INFO	ADMIN	Cluster has no active nodes. Cluster will be disabled.
FAI0163	INFO	ADMIN	User %s created new cluster - %s.
FAI0164	INFO	ADMIN	User %s attached current node to cluster.
FAE0165	ERROR	ADMIN	Error authenticating user %s.
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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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.
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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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 shared session with share %s.
FAI0229	INFO	ADMIN	User %s from IP address %s joined session.
FAI0230	INFO	ADMIN	User %s (%s) suspended session.
FAI0231	INFO	ADMIN	User %s (%s) resumed session.
FAE0232	ERROR	ADMIN	MySQL session playback error.
FAI0233	INFO	ADMIN	Anonymous user from IP address %s accessed shared session %s with share %s on the %s address.
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.
FAI0240	INFO	ADMIN	User %s blocked connection %s.
FAI0241	INFO	ADMIN	User %s unblocked connection %s.
FAI0242	INFO	ADMIN	User %s addedd new time policy to connection %s for %s from %s to %s.
FAI0243	INFO	ADMIN	User %s changed connection %s %s time policy %s from %s to %s.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0244	INFO	ADMIN	User %s deleted time policy for %s %s - %s from connection %s.
FAI0247	INFO	ADMIN	User %s deleted server %s.
FAI0248	INFO	ADMIN	User %s %s server %s.
FAI0251	INFO	ADMIN	User %s deleted connection %s.
FAI0252	INFO	ADMIN	User %s %s connection %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.
FAI0264	INFO	ADMIN	User %s modified policies settings.
FAI0265	INFO	ADMIN	User %s modified regular expressions settings.
FSW0266	WARNING	SYSTEM	Failed to send email.
FSE0267	ERROR	SYSTEM	Error generating report %d: %s.
FAI0268	INFO	ADMIN	User %s deleted report “%s”.
FAW0269	WARNING	ADMIN	User %s cannot delete report “%s”.
FAI0270	INFO	ADMIN	Report {} created by user {}.
FAW0271	WARNING	ADMIN	User %(username)s is blocked.
FAW0272	WARNING	ADMIN	User %(username)s is not allowed to log in to the management.
FAW0273	WARNING	ADMIN	User %(username)s logging from IP %(ip)s not found.
FAI0276	INFO	ADMIN	User %s unblocked user %s.
FAI0277	INFO	ADMIN	User %s deleted user %s.
FAI0278	INFO	ADMIN	User %s added user %s to connection %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.
FSW0287	WARNING	SYSTEM	No server key configured, skipping verification.
FSI0288	INFO	SYSTEM	Server key verification failed.
FUI0289	INFO	USER	MSSQL connection terminated.
FSI0290	INFO	SYSTEM	User %s (%d) was removed. Reason: user wasn”t in any of synchronized groups.
FAI0295	INFO	ADMIN	User %s blocked bastion %s.
FAI0296	INFO	ADMIN	User %s unblocked bastion %s.
FAI0297	INFO	ADMIN	User %s created bastion %s.
FAI0298	INFO	ADMIN	User %s changed bastion %s.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0299	INFO	ADMIN	User %s created server %s.
FAI0300	INFO	ADMIN	User %s changed server %s.
FAI0301	INFO	ADMIN	User %s changed connection %s.
FAI0302	INFO	ADMIN	User %s created connection %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.
FSE0307	ERROR	SYSTEM	Error fetching password from HiPAM server %s: unable to get sessid for user %s.
FSE0308	ERROR	SYSTEM	HiPAM server internal error.
FSE0309	ERROR	SYSTEM	Error fetching password from HiPAM server %s: unable to get sessdat for user %s.
FSE0310	ERROR	SYSTEM	Incorrect server configuration: HiPAM name is empty.
FSE0311	ERROR	SYSTEM	Unable to fetch password from HiPAM.
FSE0312	ERROR	SYSTEM	Error connecting to HiPAM server %s: incorrect URL in configuration.
FSE0313	ERROR	SYSTEM	Error connecting to HiPAM server %s: incorrect protocol specified.
FSE0330	ERROR	SYSTEM	Bad login field configured on LDAP server %s.
FSE0331	ERROR	SYSTEM	Error while processing userAccountControl value of user %s.
FSI0332	INFO	SYSTEM	User %s will be blocked.
FSI0333	INFO	SYSTEM	User %s will be unblocked.
FSW0334	WARNING	SYSTEM	User %s has incorrect principal name.
FSI0335	INFO	SYSTEM	User %s synchronized from LDAP server %s.
FSI0336	INFO	SYSTEM	Remove pair connection %s user %s.
FSI0337	INFO	SYSTEM	Add conection %s to user %s.
FSW0338	WARNING	SYSTEM	User %s paired with connection %s, server conflict.
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.
FSI0341	INFO	SYSTEM	User %s connections cleared.
FSI0342	INFO	SYSTEM	User %s will be resynchronized from server %s.
FSI0343	INFO	SYSTEM	Resynchronized user %s will be removed.
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 shared session with share %s.
FAI0350	INFO	ADMIN	User %s from IP address %s left session.
FUE0351	ERROR	USER	Client sent unsupported NTLM v1 response.
FSE0352	ERROR	SYSTEM	Bastion requires login and server delimited with one of '%s' (%s).
FAI0353	INFO	ADMIN	User %(username)s is deleting upgrade snapshost.
FAI0354	INFO	ADMIN	User %(username)s deleted upgrade snapshot.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSE0355	ERROR	SYSTEM	Inconsistent data, starting recovery replication to cluster node %s (%s).
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.
FUE0365	ERROR	USER	RDP server %s:%u has to listen on the default RDP port in order to redirect sessions.
FSE0366	ERROR	SYSTEM	Error connecting to CyberArk server %s: incorrect URL in configuration.
FSE0367	ERROR	SYSTEM	Error connecting to CyberArk server %s: incorrect protocol specified.
FSE0368	ERROR	SYSTEM	Error fetching password from CyberArk server %s.
FSE0369	ERROR	SYSTEM	Error fetching password from CyberArk server %s: unable to get password for user %s for server %s.
FUI0370	INFO	USER	User %s authenticated using OTP logged in from address: %s.
FSE0372	ERROR	SYSTEM	Unable to invalidate OTP password %jd.
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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0399	INFO	ADMIN	User %s changed safe %s.
FAI0400	INFO	ADMIN	User %s created safe %s.
FAI0401	INFO	ADMIN	User %s blocked account %s.
FAI0402	INFO	ADMIN	User %s unblocked account %s.
FAI0403	INFO	ADMIN	User %s deleted account %s.
FAI0404	INFO	ADMIN	User %s changed account %s.
FAI0405	INFO	ADMIN	User %s created 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.
FAI0409	INFO	ADMIN	User %s changed listener %s.
FAI0410	INFO	ADMIN	User %s created 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.
FAI0421	INFO	ADMIN	User %s assigned listener %s to safe %s.
FAI0422	INFO	ADMIN	User %s unassigned listener %s from safe %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.
FUI0436	INFO	USER	User %s authenticated using token logged in from address: %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.
FAI0440	INFO	ADMIN	User %s granted access for account %s to user %s.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0441	INFO	ADMIN	User %s revoked access for account %s from user %s.
FAI0442	INFO	ADMIN	User %s granted access for listener %s to user %s.
FAI0443	INFO	ADMIN	User %s revoked access for listener %s from user %s.
FAI0444	INFO	ADMIN	User %s created policy %s.
FAI0445	INFO	ADMIN	User %s deleted policy %s.
FAI0446	INFO	ADMIN	User %s changed policy %s.
FAI0447	INFO	ADMIN	User %s assigned regexp %s to policy %s .
FAI0448	INFO	ADMIN	User %s unassigned regexp %s from 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.
FAI0452	INFO	ADMIN	User %s granted access for safe %s to user %s.
FAI0453	INFO	ADMIN	User %s revoked access for safe %s from user %s.
FAI0454	INFO	ADMIN	User %s granted access for server %s to user %s.
FAI0455	INFO	ADMIN	User %s revoked access for server %s from user %s.
FAI0456	INFO	ADMIN	User %s granted access for user %s to user %s.
FAI0457	INFO	ADMIN	User %s revoked access for user %s from user %s.
FAI0458	INFO	ADMIN	User %s displayed password history for account %s. Reason: %s.
FAI0459	INFO	ADMIN	User %s displayed historical password for account %s changed at %s. Reason: %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 {}.
FAE0464	ERROR	ADMIN	User %s is not allowed to login from address %s.
FUW0465	WARNING	USER	Establishing new connections has been disabled.
FSE0466	ERROR	SYSTEM	Fudo versions do not conform.
FUE0467	ERROR	USER	Client tried to authenticate using an invalid UTF-8 login.
FSI0468	INFO	SYSTEM	A passphrase used to decrypt disks was changed.
FSE0469	ERROR	SYSTEM	Unexpected number of bastions (%s).
FSE0470	ERROR	SYSTEM	Unexpected number of servers (%s).
FSE0471	ERROR	SYSTEM	Unexpected number of users (%s).
FSE0472	ERROR	SYSTEM	RDP servers %s must all use TLS (NLA) or Standard RDP Security.
FSE0473	ERROR	SYSTEM	Fudo cannot be upgraded to PAM.
FSI0474	INFO	SYSTEM	Fudo can be upgraded to PAM.
FSE0475	ERROR	SYSTEM	Connection %s replaces a login and forwards a secret for servers %s which is not allowed.
FSE0476	ERROR	SYSTEM	ZVOL with encryption key does not exist.
FSE0477	ERROR	SYSTEM	Replication of encryption key to cluster node %s (%s) failed.
FSE0478	ERROR	SYSTEM	Unable to join cluster's node ${name}. Fudo versions do not conform (local: ${VERSION}, remote: ${rversion}).

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSE0479	ERROR	SYSTEM	Servers %s must all use the same %s settings.
FSE0480	ERROR	SYSTEM	Servers %s must all use the same protocol.
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.
FSE0495	ERROR	SYSTEM	Communication error with cluster node %s (%s): connection failure.
FSE0496	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to replicate a batch with object %jd to table %s.
FSE0497	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to replicate a batch with object %jd (name: %s) to table %s.
FSE0498	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to store object %jd in table %s.
FSE0499	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to store object %jd (name: %s) in table %s.
FSE0500	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to connect to database.
FSE0501	ERROR	SYSTEM	Communication error with cluster node %s (%s): failure during handshake.
FSE0502	ERROR	SYSTEM	Database error.
FSE0503	ERROR	SYSTEM	Communication error with a cluster node: Fudo version mismatch (local: %s, remote: %s).
FSE0504	ERROR	SYSTEM	Communication error with cluster node %s (%s): %s.
FSE0505	ERROR	SYSTEM	Communication error with a cluster node: failure during handshake.
FSE0506	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to receive data.
FSE0507	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to send data.
FSI0508	INFO	SYSTEM	Successfully replicated encryption key to node %s (%s).
FSE0509	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to replicate session data.
FSE0510	ERROR	SYSTEM	Communication error with cluster node %s (%s): initial replication failed.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAW0514	WARNING	ADMIN	User %s of role %s tried to view %s, but has insufficient privileges for this action.
FSE0515	ERROR	SYSTEM	Unable to upload backup #${currno} at ${datetime}.
FSI0516	INFO	SYSTEM	Backup #${currno} at ${datetime} successfully uploaded.
FSE0517	ERROR	SYSTEM	Backup configuration error: %s.
FSE0518	ERROR	SYSTEM	Backup internal error.
FSI0519	INFO	SYSTEM	${type} backup snapshot ${snapname} successfully taken.
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.
FSE0533	ERROR	SYSTEM	Unable to attach external storage.
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.
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.
FSE0544	ERROR	SYSTEM	Failed to list bookmarks.
FSW0545	WARNING	SYSTEM	Unable to change password for account %s.
FAE0547	ERROR	ADMIN	User %s could not create a ticket requesting an access to safe %s.
FAI0548	INFO	ADMIN	User %s created ticket %s requesting an access to safe %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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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.
FAI0555	INFO	ADMIN	User %s added address %s to server %s.
FAI0556	INFO	ADMIN	User %s removed address %s from server %s.
FAI0557	INFO	ADMIN	User %s changed address %s assigned to server %s.
FSI0558	INFO	SYSTEM	Starting encoding file for session %s.
FSI0559	INFO	SYSTEM	Completed encoding file for session %s.
FSE0560	ERROR	SYSTEM	Session has not been approved nor rejected.
FSE0561	ERROR	SYSTEM	Unexpected number of connections (%s).
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	INFO	ADMIN	User {} changed 4 Eyes proxy API certificate settings.
FAI0577	INFO	ADMIN	User {} changed 4 Eyes proxy settings.
FSI0578	INFO	SYSTEM	User %s (%s) was removed. Reason: user's user directory doesn't exists any more.
FAI0579	INFO	ADMIN	User {} changed 4 Eyes Fudo Mobile settings.
FSE0580	ERROR	SYSTEM	Cluster %s has an invalid token: %s.
FAI0581	INFO	ADMIN	User %s changed domain search path from %s to %s.
FSW0582	WARNING	SYSTEM	Disk %s detached.
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
FAW0587	WARNING	ADMIN	Couldn't find handler for %s.
FSE0588	ERROR	SYSTEM	Failed to replicate an object to node %s (%s): %s.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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.
FSE0593	ERROR	SYSTEM	Inconsistent data, starting recovery replication of %s filesystem to cluster node %s (%s).
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.
FSE0600	ERROR	SYSTEM	Could not re-encrypt Fudo using key %s.
FUI0601	INFO	USER	VNC connection terminated.
FSW0602	WARNING	SYSTEM	Retention module was unable to fetch the current time.
FSI0603	INFO	SYSTEM	Finished full synchronization from LDAP server %s.
FAI0604	INFO	ADMIN	User %s created IP label %s.
FAI0605	INFO	ADMIN	User %s changed IP label %s.
FAI0606	INFO	ADMIN	User %s deleted IP label %s.
FAI0607	INFO	ADMIN	User %s restored original logo for portal.
FAI0608	INFO	ADMIN	User %s changed logo for portal.
FSI0609	INFO	SYSTEM	Successfully generated new master key: %s.
FAI0610	INFO	ADMIN	User %s invalidated master key.
FSE0611	ERROR	SYSTEM	Fudo cannot be upgraded: %s.
FSI0612	INFO	SYSTEM	Cancelled encoding file for session %s.
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.
FSE0625	ERROR	SYSTEM	Upgrade cannot be performed due to inconsistency: %s.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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.
FSW0648	WARNING	SYSTEM	No server found %s.
FSW0649	WARNING	SYSTEM	More than one server address %s.
FSE0652	ERROR	SYSTEM	Browser could not be started.
FAI0653	INFO	ADMIN	User %s loaded new plugin %s.
FUE0654	ERROR	USER	Client sent an unexpected URL: %s.
FAI0655	INFO	ADMIN	User %s created account password changer %s.
FAI0656	INFO	ADMIN	User %s deleted account password changer %s.
FAI0657	INFO	ADMIN	User %s changed account password changer %s.
FSI0658	INFO	SYSTEM	AI started training quantitative model "%s-%s".
FSE0659	ERROR	SYSTEM	AI training quantitative model "%s-%s" failed: "%s".
FSI0660	INFO	SYSTEM	AI finished training quantitative model "%s-%s".
FSE0661	ERROR	SYSTEM	AI training failed for "%s-%s".
FSI0662	INFO	SYSTEM	AI started training corpus "%s".
FSE0663	ERROR	SYSTEM	AI training corpus "%s" failed: "%s".
FSI0664	INFO	SYSTEM	AI finished training corpus "%s".
FSI0665	INFO	SYSTEM	AI started training model "%s".
FSE0666	ERROR	SYSTEM	AI training model "%s" failed: "%s".
FSI0667	INFO	SYSTEM	AI finished training model "%s". Model weight: %s
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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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.
FSI0687	INFO	SYSTEM	Successfully established callhome tunnel to %s.
FSI0688	INFO	SYSTEM	Disconnected callhome tunnel.
FSW0689	WARNING	SYSTEM	Upgrade or rollback to ${oldversion} failed.
FSW0690	WARNING	SYSTEM	Upgrade or rollback to ${version} succeded.
FSE0691	ERROR	SYSTEM	Failed to expand external storage.
FAI0692	INFO	ADMIN	User %s changed node name from %s to %s.
FUW0694	WARNING	USER	Session has been terminated: time limit exceeded (user %s, safe %s).
FUW0695	WARNING	USER	Session has been terminated: inactivity limit exceeded (user %s, safe %s).
FUI0698	INFO	USER	User %s authenticated using SMS token logged in from address: %s.
FUE0700	ERROR	USER	Unable to send one-time password to user %s: %s.
FUI0703	INFO	USER	User %s authenticated using DUO/Push logged in from address: %s.
FUE0705	ERROR	USER	Unable to send DUO/%s to user %s: %s.
FAI0706	INFO	ADMIN	User %s enabled send diagnostics setting.
FAI0707	INFO	ADMIN	User %s disabled send diagnostics setting.
FSW0708	WARNING	SYSTEM	AI Identified suspicious activity in session %s.
FSI0709	INFO	SYSTEM	AI Assessed activity in session %s with threat level %s.
FUE0710	ERROR	USER	Unable to change Active Directory password for user %s (domain %s): %s.
FUE0711	ERROR	USER	User %s OTP authentication failed: %s.
FSI0712	INFO	SYSTEM	Azure backup snapshot started.
FSI0713	INFO	SYSTEM	Azure backup snapshot finished.
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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0718	INFO	ADMIN	User %s created account remote application %s.
FAI0719	INFO	ADMIN	User %s deleted account remote application %s.
FAI0720	INFO	ADMIN	User %s changed account remote application %s.
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.
FSI0725	INFO	SYSTEM	Prepare updated progress to %s.
FAE0726	ERROR	ADMIN	Hotfix%s installation by user %s failed: %s
FAI0727	INFO	ADMIN	Hotfix %s installation by user %s succeeded.
FAI0729	INFO	ADMIN	User %s changed management SSO settings.
FAI0730	INFO	ADMIN	User %s successfully changed password.
FAI0731	INFO	ADMIN	User %s %s API health check setting.
FSI0732	INFO	SYSTEM	Successfully archived session: %s
FSI0733	INFO	SYSTEM	Successfully restored session: %s
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.
FSI0736	INFO	SYSTEM	Immediate access from request (%s) started at %s and expires at %s.
FSI0737	INFO	SYSTEM	User %s (%s) accepted access request (%s).
FSI0738	INFO	SYSTEM	Access request (%s) has been granted because the required number of votes was reached.
FSI0739	INFO	SYSTEM	Access request (%s) was rejected with vote (%s) from user %s (%s). Reason: %s.
FSI0740	INFO	SYSTEM	User %s (%s) sent access request (%s) requiring %s vote(s).
FSW0741	WARNING	SYSTEM	Resolved conflicts: deleted duplicate vote (%s) of user %s (%s) for access request (%s).
FSW0742	WARNING	SYSTEM	Resolved conflicts: accepting vote (%s) of user %s (%s) for access request (%s) has been revoked after receiving rejecting vote.
FSE0743	ERROR	SYSTEM	Unable to archive session %s: %s.
FSE0744	ERROR	SYSTEM	Unable to restore session %s: %s.
FSI0745	INFO	SYSTEM	%zu accounts onboarded.
FSI0746	INFO	SYSTEM	%zu accounts quarantined.
FSI0747	INFO	SYSTEM	Scanner %jd/%s removed account %s.
FSI0748	INFO	SYSTEM	Scanner %jd/%s created account %s.
FSE0749	ERROR	SYSTEM	%s %s (pid %d) failed with status %d.
FSE0750	ERROR	SYSTEM	%s %s (pid %d) was terminated by signal %d.
FAI0751	INFO	ADMIN	User {} downloaded {}.
FSE0752	ERROR	SYSTEM	Client sent an invalid request.
FSI0753	INFO	SYSTEM	User %s is waiting for session approval.
FAI0754	INFO	ADMIN	User %s enabled Call Home.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0755	INFO	ADMIN	User %s disabled Call Home.
FAI0756	INFO	ADMIN	User %s requested session %s from archive.
FAW0757	WARNING	ADMIN	Malformed upgrade package: %s
FSE0758	ERROR	SYSTEM	Max number of retries exceeded. Could not remove sessions %s.
FSW0759	WARNING	SYSTEM	Could not remove sessions %s.
FSI0760	INFO	SYSTEM	%s until removal retry for sessions %s.
FAE0761	ERROR	ADMIN	Failed authentication attempt from address %s.
FUI0762	INFO	USER	User %s authenticated using SSO token logged in from address: %s.
FUI0763	INFO	USER	User %s authenticated using X509 certificate logged in from address: %s.
FUE0764	ERROR	USER	User failed to authenticate using SSO token and logging in from address: %s.
FUE0765	ERROR	USER	User failed to authenticate using X509 certificate and logging in from address: %s.
FAE0766	ERROR	ADMIN	Error parsing %s file at position %s.
FAI0767	INFO	ADMIN	User %s changed password complexity settings.
FAI0768	INFO	ADMIN	User %s changed User CA certificates.
FAI0769	INFO	ADMIN	User %s changed retention configuration.
FAI0770	INFO	ADMIN	User %s disabled backup configuration.
FAI0771	INFO	ADMIN	User %s enabled backup configuration.
FAI0772	INFO	ADMIN	User %s created backup target %s.
FAI0773	INFO	ADMIN	User %s changed backup target %s.
FAI0774	INFO	ADMIN	User %s deleted backup target %s.
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.
FSE0778	ERROR	SYSTEM	Unknown configuration variable: %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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSE0792	ERROR	SYSTEM	Unable to establish connection: server not found, user not found or user has no access to the server (listener: %s, username: %s%s%s, targetname: %s).
FSW0793	WARNING	SYSTEM	DNS is slow. It took %jums to resolve %s.
FSE0794	ERROR	SYSTEM	System error:
FSI0795	INFO	SYSTEM	System information:
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
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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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,secret=account.secret_id,collection=account.co
FAI0840	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the account {old.name} to: {attribute.value}. {account=old.id,secret=account.secret_id,collection=account.collecti
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}
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}

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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
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}

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}
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_list
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,li
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_list

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}
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

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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_safe_time_pol
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}.
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}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}.
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}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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 {}.
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}.
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.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}.
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	Rejected an unparsable client request: {err}
FSE0964	ERROR	SYSTEM	Failed to execute client command {description}: {err}
FSE0965	ERROR	SYSTEM	Failed to get scheduled job, error: {err}
FSE0966	ERROR	SYSTEM	Failed to queue scheduled job, error: {err}

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}
FSE0972	ERROR	SYSTEM	Job ({id}) {name} failed with error: {err}
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}.
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}).

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}).
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_

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}.
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}).

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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 (share_id={session_share.id}, authenticated={session_share.authenticated}, readonly={session_share.readonly}, valid_since={session_share.valid_since}, valid_to={session_share.valid_to}, vhost={session_share.created_vhost}). {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	User {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.
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}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}
FAI1059	INFO	ADMIN	Administrator {subject.name} removed user {group_user.user_name} from the group {group_user.group_name}. {user=group_user.user_id}

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}, share_id={share_id}, {settings}).
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}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}
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}).

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}).
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}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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.
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 Fudo ShareAccess service: {service_name}.
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}

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}
FAI1133	INFO	ADMIN	Administrator {subject.name} added group {group_collection.group_name} to the collection {group_collection.collection_name}. {collection=group_collection.collection_id,group=group_collection.grou
FAI1134	INFO	ADMIN	Administrator {subject.name} removed group {group_collection.group_name} from the collection {group_collection.collection_name}. {collection=group_collection.collection_id,group=group_collection.grou
FAI1137	INFO	ADMIN	Administrator {subject.name} added user {user_collection.user_name} to the collection {user_collection.collection_name}. {collection=user_collection.collection_id,user=user_collection.user_id}
FAI1138	INFO	ADMIN	Administrator {subject.name} removed user {user_collection.user_name} from the collection {user_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_collection.user_name}'s access to collection {user_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_collection.group_name}'s access to collection {group_collection.collection_name}. {collection=group_collection.collection_id,group=group_collection.grou

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}
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}
FSW1156	WARNING	SYSTEM	License verification failed. This may result in limited functionality.
FUI1157	INFO	USER	Sudo command '{command}' as system user {runas_user} (group {runas_group}) approved for fudo user {user_name} per policy {policy_name}, matched regexp {regexp_name} ({regexp_pattern}).
FUW1158	WARNING	USER	Sudo command '{command}' as system user {runas_user} (group {runas_group}) denied for fudo user {user_name}.
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}).
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 {} ({}).

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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 {}:{}.
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: {}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}).
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}.
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}

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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	INFO	ADMIN	Administrator {subject.name} saved secret {secret_name} with policy violations: {violations}. {collection=collection_id,secret=secret_id}
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 {secret_password_changer.password_changer_name} to the secret {secret_password_changer.secret_name}. {secret=secret_password_changer.secret_id,collection=secret_pa
FAI1234	INFO	ADMIN	Administrator {subject.name} set attribute {attribute.name} to {attribute.value} for password_changer {secret_password_changer.password_changer_name}'s assignment to secret {secret_password_changer.secret_name}. {secret=secret_password_changer.secret_id,collection=secret_passv
FAI1235	INFO	ADMIN	Administrator {subject.name} removed password_changer {secret_password_changer.password_changer_name} from the secret {secret_password_changer.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_i
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.
FSE1240	ERROR	SYSTEM	FIDO2 registration failed for user %s: %s.
FUI1241	INFO	USER	User {subject.name} registered FIDO2 credentials.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSE1242	ERROR	SYSTEM	FIDO2 authentication failed from address %s: %s.
FSE1243	ERROR	SYSTEM	FIDO2 authentication failed for user %s from address %s: %s.
FSI1244	INFO	SYSTEM	User %s presence confirmed during FIDO2 authentication.
FSI1245	INFO	SYSTEM	User %s verified during FIDO2 authentication.
FSI1246	INFO	SYSTEM	User %s authenticated using FIDO2 (%s) logged in from address: %s.
FSE1247	ERROR	SYSTEM	FIDO2 discovery failed: %s.
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.
FSE1252	ERROR	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	Password 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 {}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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 {}.
FAI1275	INFO	ADMIN	Administrator {subject.name} updated SMTP CA certificate.
FSE1276	ERROR	SYSTEM	Invalid JWT: %s.
FSW1280	WARNING	SYSTEM	Failed to notify remote mld about model update on %s.
FAI1281	INFO	ADMIN	Administrator {subject.name} saved DNS configuration: hostname={hostname}, search={search}, bind_to={bind_to}.
FUI1282	INFO	USER	File upload from user to session storage completed: %s (%zu bytes).
FUI1284	INFO	USER	File download from session storage to user completed: %s (%zu bytes).
FUE1285	ERROR	USER	%s failed: unable to register events.
FUW1286	WARNING	USER	File upload blocked: not enabled in safe configuration.
FUW1287	WARNING	USER	File download blocked: not enabled in safe configuration.
FUW1288	WARNING	USER	File transfer blocked: unrecognized request type.
FUW1289	WARNING	USER	File transfer service temporarily unavailable.
FUE1290	ERROR	USER	%s failed: unable to prepare request.
FUE1291	ERROR	USER	%s failed: unable to send request headers.
FUE1292	ERROR	USER	%s failed: unable to receive data from client.
FUE1293	ERROR	USER	%s failed: unable to forward data to file transfer service.
FUE1294	ERROR	USER	%s failed: unable to receive response from file transfer service.
FUE1295	ERROR	USER	%s failed: unable to send data to client.
FUI1296	INFO	USER	File upload from user to session storage canceled.
FUE1297	ERROR	USER	File upload from user to session storage failed.
FUI1298	INFO	USER	File download from session storage to user canceled: %s.
FUE1299	ERROR	USER	File download from session storage to user failed: %s.
FUI1300	INFO	USER	File download from session storage to user started: %s.
FUI1301	INFO	USER	File upload from user to session storage started (%zu bytes).
FSI1302	INFO	SYSTEM	File selected for upload to server: %s (%d bytes).
FSI1303	INFO	SYSTEM	File download from server to session storage started: %s.
FSW1304	WARNING	SYSTEM	File download from server to session storage failed: %s (%d bytes, quota exceeded).

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSI1305	INFO	SYSTEM	File download from server to session storage completed: %s (%d bytes).
FSI1306	INFO	SYSTEM	File download from server to session storage canceled: %s (%d bytes).
FSE1307	ERROR	SYSTEM	Batch response missing lookup result.
FSE1308	ERROR	SYSTEM	Lookup failed with status %d: %s.
FSE1309	ERROR	SYSTEM	Lookup response missing secret field.
FSW1310	WARNING	SYSTEM	Checkin failed with status %d: %s. Checkout session may remain open.
FSW1311	WARNING	SYSTEM	No TLS certificate provided, accepting any certificate.
FSE1312	ERROR	SYSTEM	Failed to execute whldiskreprobe: {e}
FSE1313	ERROR	SYSTEM	Support license notification failed.
FSI1314	INFO	SYSTEM	Created {event_name} notification for parrotd.
FSE1324	ERROR	SYSTEM	Server's certificate does not match configured CA certificate.
FSE1325	ERROR	SYSTEM	Server's certificate does not match server address %s.
FSE1327	ERROR	SYSTEM	Listener "%s" conflicts with listener "%s" on resolved IP+port pair.
FSE1328	ERROR	SYSTEM	Changing label "%s" IP causes conflict between listeners "%s" and "%s".
FSE1329	ERROR	SYSTEM	Changing portal IPs causes conflict between UAG listener "%s" and listener "%s".
FAI1330	INFO	ADMIN	User {subject.name} added {authentication_method.type} authentication method at position {authentication_method.position}. {user=subject.id}
FAI1331	INFO	ADMIN	User {subject.name} set the attribute {attribute.name} on {old.type} authentication method at position {old.position} to: {attribute.value}. {user=subject.id}
FAI1332	INFO	ADMIN	User {subject.name} removed {authentication_method.type} authentication method at position {authentication_method.position}. {user=subject.id}
FSE1333	ERROR	SYSTEM	Failed to acquire database connection for secret password change scheduling.
FSE1334	ERROR	SYSTEM	Unable to change password for secret {}, no change scripts configured.
FSE1335	ERROR	SYSTEM	Unable to change password for secret {}, multiple verifiers found.
FSE1336	ERROR	SYSTEM	Unable to change secret {}, SSH key changer has no key type configured.
FSE1337	ERROR	SYSTEM	Error fetching password from Azure Key Vault. Details: %s.
FSW1340	WARNING	SYSTEM	Failed to mark session as finished: %s; row may stay with pid set and finished_at NULL.
FSW1341	WARNING	SYSTEM	Session cleanup done but database row not updated.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSW1342	WARNING	SYSTEM	Session-finished UPDATE affected 0 rows; row may not exist or may have been replaced out from under us.
FAI1343	INFO	ADMIN	Administrator {subject.name} created syslog server {syslog_server.name} ({syslog_server.host}:{syslog_server.port} {syslog_server.transport} {syslog_server.protocol}).
FAI1344	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the syslog server {old.name} ({old.host}:{old.port} {old.transport} {old.protocol}) to: {attribute.value}.
FAI1345	INFO	ADMIN	Administrator {subject.name} removed syslog server {syslog_server.name} ({syslog_server.host}:{syslog_server.port} {syslog_server.transport} {syslog_server.protocol}).
FSE1346	ERROR	SYSTEM	Failed to generate syslog forwarding configuration: {e:#}
FSE1347	ERROR	SYSTEM	Failed to receive NOTIFY: {e}.
FSE1348	ERROR	SYSTEM	Failed to refresh debug flag from fudo_syslog_server: {e}.
FSE1349	ERROR	SYSTEM	Failed to fetch fudo_log_entry id={entry_id}: {e}.
FSE1350	ERROR	SYSTEM	whlsyslogd terminated: {e}
FSW1351	WARNING	SYSTEM	'%s' doesn't look like a valid CSS selector. Ensure that a valid CSS selector has been configured.
FSE1352	ERROR	SYSTEM	HTTP rendered browser setup failed: %s
FAI1353	INFO	ADMIN	Administrator {subject.name} added DNS server entry: address={dns_server.address} domain={dns_server.domain}.
FAI1354	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for DNS server {old.address} to: {attribute.value}.
FAI1355	INFO	ADMIN	Administrator {subject.name} deleted DNS server entry id={dns_server.id}.
FAI1356	INFO	ADMIN	Administrator {subject.name} configured SCIM authentication.
FAI1357	INFO	ADMIN	Administrator {subject.name} rotated SCIM apikey.
FAI1358	INFO	ADMIN	Administrator {subject.name} cleared SCIM configuration and released SCIM-managed users and groups to manual control.
FSE1359	ERROR	SYSTEM	fudo-secret-audit-cli failed to connect to database.
FSE1360	ERROR	SYSTEM	fudo-secret-audit-cli could not open an active hashdb.
FSE1361	ERROR	SYSTEM	fudo-secret-audit-cli failed.
FSE1362	ERROR	SYSTEM	fudo-secret-audit-cli could not inspect the cluster hashdbs.
FSE1363	ERROR	SYSTEM	fudo-secret-audit-cli failed to remove the stale local hashdb.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSI1364	INFO	SYSTEM	fudo-secret-audit-cli on node {serial} removed its stale local hashdb; the newest is on node {newest_serial}.
FSE1365	ERROR	SYSTEM	H.264 decode error on the OCR surface.
FSE1366	ERROR	SYSTEM	Passthrough aborted: reason=%u codec=%u text=%.*s.
FSE1367	ERROR	SYSTEM	Passthrough FBS frame too large (%u bytes).
FUW1368	WARNING	USER	Passthrough recording aborted (%s): %s [reason %u]: %s.
FUE1369	ERROR	USER	Session rejected: %s.
FSE1370	ERROR	SYSTEM	Unable to create %s dump for session %jd: %s.
FUE1371	ERROR	USER	Unable to open the RAW dump; continuing without RAW recording.
FUE1372	ERROR	USER	Unable to open the FBS dump; continuing without FBS recording.
FAI1373	INFO	ADMIN	User {subject.name} has changed their password.
FSW1375	WARNING	SYSTEM	Failed to rollback configuration session {}: {:#}.
FUW1376	WARNING	USER	Stored server TLS certificate is unparsable as PEM.
FUW1377	WARNING	USER	Received outbound chain leaf is unparsable as PEM.
FUW1378	WARNING	USER	Stored CA TLS certificate is unparsable as PEM.
FUW1379	WARNING	USER	Received outbound chain has no parsable leaf cert.
FUW1380	WARNING	USER	Outbound chain verify failed: %s.
FUW1381	WARNING	USER	Outbound cert IP mismatch for %s.
FUW1382	WARNING	USER	Outbound cert hostname mismatch for %s.
FUW1383	WARNING	USER	Outbound chain does NOT verify against CA TLS certificate (host=%s).
FUW1384	WARNING	USER	Outbound cert does NOT match pinned server TLS certificate (host=%s).
FSW1385	WARNING	SYSTEM	Unable to synchronously replicate checkout session %jd to the active node; it will be replicated asynchronously.
FAI1386	INFO	ADMIN	User {subject.name} generated database key for mobile device.
FSE1388	ERROR	SYSTEM	Skipping unparsable job '{}': {}.
FSE1389	ERROR	SYSTEM	Quarantined unparsable scheduled job '{}'.
FSE1390	ERROR	SYSTEM	Quarantined unparsable job '{}' from the queue.
FSE1391	ERROR	SYSTEM	Quarantined unparsable job '{}' during queue recovery.
FSE1392	ERROR	SYSTEM	Failed to quarantine unparsable scheduled job '{}', discarding it: {}.
FSE1393	ERROR	SYSTEM	Failed to quarantine unparsable job '{}' from the queue, discarding it: {}.
FSE1394	ERROR	SYSTEM	Failed to quarantine unparsable job '{}' during queue recovery, discarding it: {}.
FSE1395	ERROR	SYSTEM	Job '{}' failed to parse: {}.
FSE1396	ERROR	SYSTEM	Failed to remove bad job entry '{}' from the processing queue; it stays there until the next restart: {}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSE1397	ERROR	SYSTEM	Failed to remove bad job entry '{}' from the pending queue; it stays there until the next queue recovery: {}.
FSE1398	ERROR	SYSTEM	Failed to remove job entry '{}' from the schedule; it is retried on the next poll: {}.
FSE1401	ERROR	SYSTEM	Syslog queue full; dropped {total} oldest entries.
FSW1402	WARNING	SYSTEM	Exiting with {} unforwarded log entries.
FSE1403	ERROR	SYSTEM	Local syslog socket still unavailable; log forwarding is stalled.
FSI1405	INFO	SYSTEM	Restored syslog socket connection; {still_queued} log entries queued.
FUI1412	INFO	USER	Oracle connection terminated by client.
FUE1413	ERROR	USER	Oracle connection receive error: %s.
FUE1414	ERROR	USER	Invalid Oracle packet: %s.
FUE1415	ERROR	USER	Oracle session refused: %s.
FUE1416	ERROR	USER	Oracle session failed: %s.
FSW1421	WARNING	SYSTEM	Unable to replicate the secret for account %s: no other cluster node is reachable. Secret changers require at least two active cluster nodes to operate.
FUE1422	ERROR	USER	Server's certificate does not match configured CA certificate.
FUE1423	ERROR	USER	Server's certificate does not match server address %s.
FSE1424	ERROR	SYSTEM	{error}.
FSI1425	INFO	SYSTEM	HSM descriptor in {} is healthy.
FSE1426	ERROR	SYSTEM	HSM descriptor in {} is not usable: {}.
FSE1427	ERROR	SYSTEM	HSM broker stopped accepting connections: {error}.
FSE1428	ERROR	SYSTEM	Failed to reveal a master key from the HSM: {error}.
FSW1429	WARNING	SYSTEM	Refused reveal peer uid {uid} (only {reveal_uid} is authorized).
FSW1430	WARNING	SYSTEM	Refused a reveal peer whose uid could not be read: {error}.
FSI1431	INFO	SYSTEM	Loaded config from {}: socket '{}', reveal uid {}, descriptor '{}'.
FSI1432	INFO	SYSTEM	HSM broker ready on {}; token '{}' ({}).
FSE1433	ERROR	SYSTEM	Cannot read HSM descriptor in {}: {error}.
FSE1434	ERROR	SYSTEM	HSM master key present but %s is not accessible.
FSE1435	ERROR	SYSTEM	Unable to connect to hsmproxyd.
FSE1436	ERROR	SYSTEM	Unable to create the hsmproxyd client.
FSE1437	ERROR	SYSTEM	Unable to reveal an HSM master key: %s.
FSE1438	ERROR	SYSTEM	hsmproxyd revealed an empty key.
FSE1439	ERROR	SYSTEM	Unable to open master key file %s.
FSE1440	ERROR	SYSTEM	Master key file %s is not %d bytes long.
FSE1441	ERROR	SYSTEM	Unable to open HSM master key file %s.
FSE1442	ERROR	SYSTEM	HSM master key file %s has invalid size.
FSE1443	ERROR	SYSTEM	Unable to read HSM master key file %s.
FSE1444	ERROR	SYSTEM	HSM master key %s is not %d bytes long.
FSW1445	WARNING	SYSTEM	Ignoring unexpected file %s in the master key
FSE1446	ERROR	SYSTEM	Unable to stat master key file %s.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSE1447	ERROR	SYSTEM	Duplicate master key id %s.
FSE1448	ERROR	SYSTEM	Master key reload failed; keeping the previous key set.
FSE1449	ERROR	SYSTEM	Unable to protect the key: {error}.
FSE1450	ERROR	SYSTEM	Cannot list HSM bundle: {error}.
FSE1451	ERROR	SYSTEM	Cannot read bundle from stdin: {error}.
FSE1452	ERROR	SYSTEM	Cannot extract HSM bundle: {error}.
FSE1453	ERROR	SYSTEM	Cannot read staged descriptor from stdin: {error}.
FSE1454	ERROR	SYSTEM	Cannot stage HSM descriptor in {}: {error}.
FAI1455	INFO	ADMIN	Administrator {subject.name} tested an HSM configuration.
FAI1456	INFO	ADMIN	Administrator {subject.name} uploaded an HSM bundle.
FAI1457	INFO	ADMIN	Administrator {subject.name} set a group-safe access policy for user {user_group_safe_policy.user_name} on safe {user_group_safe_policy.safe_name}. {safe=user_group_safe_policy.safe_id}
FAI1458	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} of the group-safe access policy for user {user_group_safe_policy.user_name} on safe {user_group_safe_policy.safe_name} to: {attribute.value}. {safe=user_group_safe_policy.safe_id}
FAI1459	INFO	ADMIN	Administrator {subject.name} removed the group-safe access policy for user {user_group_safe_policy.user_name} on safe {user_group_safe_policy.safe_name}. {safe=user_group_safe_policy.safe_id}
FAI1460	INFO	ADMIN	Administrator {subject.name} created a time policy on the group-safe access policy for user {user_group_safe_policy_time_policy.user_name} on safe {user_group_safe_policy_time_policy.safe_name}. {safe=user_group_safe_policy_time_policy.safe_id}
FAI1461	INFO	ADMIN	Administrator {subject.name} set attribute {attribute.name} of a time policy on the group-safe access policy for user {user_group_safe_policy_time_policy.user_name} on safe {user_group_safe_policy_time_policy.safe_name} to: {attribute.value}. {safe=user_group_safe_policy_time_policy.safe_id}
FAI1462	INFO	ADMIN	Administrator {subject.name} removed a time policy from the group-safe access policy for user {user_group_safe_policy_time_policy.user_name} on safe {user_group_safe_policy_time_policy.safe_name}. {safe=user_group_safe_policy_time_policy.safe_id}
FSI1463	INFO	SYSTEM	Disabled HSM; master keys are stored locally.
FSI1464	INFO	SYSTEM	Enrolled HSM master key %s.
FSI1465	INFO	SYSTEM	Updated HSM configuration.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSE1466	ERROR	SYSTEM	Cannot read active HSM descriptor: {error}.
FSE1467	ERROR	SYSTEM	Cannot write blob: {error}.
FSE1468	ERROR	SYSTEM	HSM enrollment failed: {error}.
FSE1469	ERROR	SYSTEM	Cannot read blob from stdin: {error}.
FSE1470	ERROR	SYSTEM	Unwrap failed: {error}.
FSE1471	ERROR	SYSTEM	Revealed key does not match keyid {keyid}.
FSE1472	ERROR	SYSTEM	Cannot write cleartext: {error}.
FSE1473	ERROR	SYSTEM	Cannot read key from stdin: {error}.
FSE1474	ERROR	SYSTEM	Wrap failed: {error}.
FSE1475	ERROR	SYSTEM	Cannot stage HSM descriptor: {error}.
FSE1476	ERROR	SYSTEM	Cannot read staged descriptor: {error}.
FSE1477	ERROR	SYSTEM	Cannot set aside the current descriptor: {error}.
FSE1478	ERROR	SYSTEM	Cannot activate staged descriptor: {error}.
FAI1479	INFO	ADMIN	Administrator {subject.name} updated the HSM configuration.
FAI1480	INFO	ADMIN	Administrator {subject.name} enabled HSM master-key mode.
FAI1481	INFO	ADMIN	Administrator {subject.name} disabled HSM master-key mode.
FSE1482	ERROR	SYSTEM	Staged HSM descriptor is not usable: {}.
FUI1483	INFO	USER	Rejecting duplicate WebSocket connection %u (tab duplication is not supported).
FSE1486	ERROR	SYSTEM	Upload payload is missing the filename separator.
FSI1487	INFO	SYSTEM	Rejecting connection: %s.
FUW1488	WARNING	USER	User %s location policy check for address %s fell back to allow: GeoIP status %s.
FUE1489	ERROR	USER	User %s denied by location policy: source address %s is invalid while an enforcing location policy is configured for the user.
FUE1490	ERROR	USER	User %s blocked from %s: policy "%s" (%s) denied - source not in the allow-list (country %s, location %s, geoip status %s).
FUE1491	ERROR	USER	User %s blocked from %s (%s): policy "%s" (%s) matched %s entry %s (geoip status %s).
FUW1492	WARNING	USER	API request from %s by user %s allowed because the source location could not be determined (GeoIP status %s).
FUE1493	ERROR	USER	API request by user %s: location policy check failed unexpectedly (source %s); request rejected with 503.
FUE1494	ERROR	USER	API request from %s by user %s blocked: policy "%s" (%s) - source not in allow-list (country %s, location %s, geoip status %s).
FUE1495	ERROR	USER	API request from %s by user %s blocked from %s: policy "%s" (%s) matched %s entry %s (geoip status %s).
FSW1496	WARNING	SYSTEM	location-policy change rejected: would lock out caller {caller} from {source_ip} (policy {policy_name}).

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI1497	INFO	ADMIN	Administrator {subject.name} created location policy {location_policy.name}.
FAI1498	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the location policy {old.name} to: {attribute.value}.
FAI1499	INFO	ADMIN	Administrator {subject.name} deleted location policy {location_policy.name}.
FAI1500	INFO	ADMIN	Administrator {subject.name} added an entry to the location policy {location_policy_entry.policy_name}.
FAI1501	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the entry in the location policy {old.policy_name} to: {attribute.value}.
FAI1502	INFO	ADMIN	Administrator {subject.name} removed an entry from the location policy {location_policy_entry.policy_name}.
FAI1503	INFO	ADMIN	Administrator {subject.name} assigned the location policy {group_location_policy.policy_name} to the group {group_location_policy.group_name}. {group=group_location_policy.group_id}
FAI1504	INFO	ADMIN	Administrator {subject.name} unassigned the location policy {group_location_policy.policy_name} from the group {group_location_policy.group_name}. {group=group_location_policy.group_id}
FSE1505	ERROR	SYSTEM	Failed to scan cluster for HSM configuration: {e}. Falling back to local.
FSE1506	ERROR	SYSTEM	Failed to restart remote hsmproxyd after HSM config update on %s.
FSE1507	ERROR	SYSTEM	Failed to merge and promote remote masterkeys after update on %s.
FSI1508	INFO	SYSTEM	Supervisor %s (access %jd) disconnected from %s's supervised session.
FSI1509	INFO	SYSTEM	Supervisor %s (access %jd) connected to %s's supervised session.
FSE1510	ERROR	SYSTEM	Supervision quorum missing on the parked session; requiring one supervisor.
FSI1511	INFO	SYSTEM	User %s is waiting for session supervisors (%jd required).
FSE1512	ERROR	SYSTEM	Session has not gathered the required supervisors.
FSW1513	WARNING	SYSTEM	Safe %s requires live supervision but listener %s (protocol %s) does not support live supervision; refusing the session.
FSW1514	WARNING	SYSTEM	Safe %s requires live supervision but account %s records no live stream (dump mode %s); refusing the session.
FSE1515	ERROR	SYSTEM	Nested session requested for a supervised leader; terminating.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSI1516	INFO	SYSTEM	User %s gathered the required session supervisors (%jd); starting the session.
FSI1517	INFO	SYSTEM	Session terminated: session supervisors did not return within the allowed time (operator %s).
FSI1518	INFO	SYSTEM	Session terminated: session supervisors dropped below the required %jd (operator %s).
FSI1519	INFO	SYSTEM	Session paused: session supervisors dropped below the required %jd (operator %s, supervisors present: %s).
FSI1520	INFO	SYSTEM	Session resumed: the required %jd session supervisors are present again (operator %s, supervisors present: %s).
FSI1521	INFO	SYSTEM	Supervised session ended (operator %s).
FUI1522	INFO	USER	Session terminated: live supervision was lost.
FUW1523	WARNING	USER	Supervision latched after the graphics policy was decided; disabling the peer GFX channel late.
FUI1524	INFO	USER	Supervised session: unrecorded SSH file transfer rejected.
FUI1525	INFO	USER	Supervised session: SSH channel data before recording start rejected.
FUI1526	INFO	USER	Supervised session: non-terminal SSH channel rejected; only a watchable terminal is allowed.
FUI1527	INFO	USER	Supervised session: additional SSH channel (%s) rejected.
FUI1528	INFO	USER	Supervised session: SSH global request (%s) rejected.
FUI1529	INFO	USER	Supervised session: non-terminal SSH request (%s) rejected.
FUI1530	INFO	USER	Supervised session: unrecordable SSH file transfer rejected.
FAW1531	WARNING	ADMIN	Failed to terminate session %s: %s
FAI1532	INFO	ADMIN	User %s from IP address %s accessed shared session %s with share %s on the %s address.
FAW1533	WARNING	ADMIN	Rejected player websocket from %s: Origin %s does not match host %s.
FAW1534	WARNING	ADMIN	Rejected player websocket from %s: authenticated request has no Origin header (host %s).
FAI1535	INFO	ADMIN	Supervisor %s from IP address %s terminated supervised session via share %s.
FAW1536	WARNING	ADMIN	Supervisor %s from IP address %s could not terminate supervised session via share %s.
FAI1537	INFO	ADMIN	User %s from IP address %s joined shared session with share %s.
FAI1538	INFO	ADMIN	User %s from IP address %s left shared session with share %s.
FAI1539	INFO	ADMIN	User {subject.name} added a comment to session {session_comment.session_id}. {session=session_comment.session_id}

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI1540	INFO	ADMIN	User {subject.name} set the attribute {attribute.name} for comment {old.id} in session {old.session_id} to: {attribute.value}. {session=old.session_id}
FAI1541	INFO	ADMIN	User {subject.name} removed comment {session_comment.id} from session {session_comment.session_id}. {session=session_comment.session_id}
FAI1542	INFO	ADMIN	User {subject.name} shared their session (session_id={session_id}, share_id={share_id}, authenticated=true, readonly=false, valid_to=until the session ends, vhost=uag).
FAI1543	INFO	ADMIN	User {subject.name} revoked their session share (session_id={session_id}, share_id={share_id}, {settings}).
FSE1544	ERROR	SYSTEM	Failed to initialize transcriptd: {err}.
FSE1545	ERROR	SYSTEM	Live session analysis service was interrupted: {res:?}.
FSE1546	ERROR	SYSTEM	Unable to start live analysis of the session: {err:#}.
FSE1547	ERROR	SYSTEM	Unable to list active sessions for live analysis: {err:#}.
FSW1548	WARNING	SYSTEM	Unable to load analysis checkpoints; analyzing the session from the start: {err:#}.
FSW1549	WARNING	SYSTEM	Unable to load session context; analyzing without it: {err:#}.
FSE1550	ERROR	SYSTEM	Analysis agent {agent_id} has an unusable LLM provider and will not run: {err:#}.
FSE1551	ERROR	SYSTEM	Unable to persist a verdict of analysis agent {agent_id}: {err:#}.
FSE1552	ERROR	SYSTEM	Unable to mark the analysis of agent {agent_id} as finished: {err:#}.
FSE1553	ERROR	SYSTEM	Unable to open the session recording {dump_fbs} for live analysis: {err}.
FSE1554	ERROR	SYSTEM	Live analysis stopped: error reading the session recording: {err}.
FSW1555	WARNING	SYSTEM	Ignored a lifecycle notification on {channel} with an unparsable session id {payload:?}: {err}.
FSW1556	WARNING	SYSTEM	Unable to load prior operator feedback; analyzing without it: {err:#}.
FAI1557	INFO	ADMIN	Administrator {subject.name} created analysis agent {analysis_agent.name}.
FAI1558	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the analysis agent {old.name} to: {attribute.value}.
FAI1559	INFO	ADMIN	Administrator {subject.name} removed analysis agent {analysis_agent.name}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI1560	INFO	ADMIN	Administrator {subject.name} enabled analysis agent {safe_analysis_agent.agent_name} in the safe {safe_analysis_agent.safe_name}. {safe=safe_analysis_agent.safe_id}
FAI1561	INFO	ADMIN	Administrator {subject.name} disabled analysis agent {safe_analysis_agent.agent_name} in the safe {safe_analysis_agent.safe_name}. {safe=safe_analysis_agent.safe_id}
FAI1562	INFO	ADMIN	Administrator {subject.name} set live session analysis {attribute.name} to: {attribute.value}.
FAI1563	INFO	ADMIN	Administrator {subject.name} created LLM provider {llm_provider.name}.
FAI1564	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the LLM provider {old.name} to: {attribute.value}.
FAI1565	INFO	ADMIN	Administrator {subject.name} removed LLM provider {llm_provider.name}.
FAI1566	INFO	ADMIN	Operator {subject.name} recorded judgment on analysis verdict {session_analysis_verdict_feedback.verdict_id}.
FAI1567	INFO	ADMIN	Operator {subject.name} updated judgment on analysis verdict {session_analysis_verdict_feedback.verdict_id}.
FAI1568	INFO	ADMIN	Operator {subject.name} retracted judgment on analysis verdict {session_analysis_verdict_feedback.verdict_id}.
FSE1569	ERROR	SYSTEM	Destroying KEK failed: {error}.
FSE1570	ERROR	SYSTEM	Old KEK %s left on the token (stage failed).
FSE1571	ERROR	SYSTEM	Old KEK %s left on the token (destroy failed).
FSI1572	INFO	SYSTEM	Rotated HSM KEK.
FSI1573	INFO	SYSTEM	Resuming interrupted HSM KEK rotation (post-swap).
FSI1574	INFO	SYSTEM	Discarding interrupted HSM KEK rotation (pre-swap).
FAI1575	INFO	ADMIN	Administrator {subject.name} rotated the HSM KEK.
FAI1576	INFO	ADMIN	User %s from IP address %s disconnected from shared session %s with share %s on the %s address.
FAI1577	INFO	ADMIN	Anonymous user from IP address %s disconnected from shared session %s with share %s on the %s address.
FAI1578	INFO	ADMIN	Administrator {subject.name} created access request reason format {reason_format_name}.
FAI1579	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for access request reason format {reason_format_name} to: {attribute.value}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI1580	INFO	ADMIN	Administrator {subject.name} deleted access request reason format {access_request_reason_format.name}.
FAW1581	WARNING	ADMIN	User %s (%s) could not terminate session.
FSE1582	ERROR	SYSTEM	Master key operation failed: %s
FSE1587	ERROR	SYSTEM	Unable to give cluster node %s the HSM master key.
FSE1588	ERROR	SYSTEM	HSM delete failed: {error:#}
FSI1589	INFO	SYSTEM	Disabled HSM across {} nodes.
FSI1590	INFO	SYSTEM	Disabled HSM on this node.
FSE1591	ERROR	SYSTEM	HSM enrollment failed: {error:#}
FSE1592	ERROR	SYSTEM	HSM master key generation failed: {error:#}
FSI1593	INFO	SYSTEM	Generated master key {keyid} across the cluster.
FSI1594	INFO	SYSTEM	Gave cluster node {node} HSM master key {keyid}.
FSI1595	INFO	SYSTEM	Adopted master key {keyid}.
FSI1596	INFO	SYSTEM	Created the new HSM KEK.
FSI1597	INFO	SYSTEM	New HSM KEK already present.
FSI1598	INFO	SYSTEM	HSM KEK rotation already applied on this node.
FSE1599	ERROR	SYSTEM	HSM KEK rotation failed: {error:#}
FSI1600	INFO	SYSTEM	Moved this node onto the new HSM KEK.
FSW1601	WARNING	SYSTEM	HSM delete incomplete: {} nodes disabled.
FSW1602	WARNING	SYSTEM	HSM enrollment incomplete: {} nodes enrolled.
FSI1603	INFO	SYSTEM	Enrolled HSM master key {} across {} nodes.
FSI1604	INFO	SYSTEM	Resuming HSM KEK rotation {} onto {}.
FSW1605	WARNING	SYSTEM	HSM KEK rotation incomplete: {} of {} nodes moved.
FSI1606	INFO	SYSTEM	Rotated the HSM KEK across {} nodes.
FSI1607	INFO	SYSTEM	Enrolled HSM master key {keyid} on this node.
FSE1621	ERROR	SYSTEM	Session %jd OCR failed: %s.
FUE1622	ERROR	USER	Unreachable WIRE entry; failing recording closed.
FUE1623	ERROR	USER	Server %s is incompatible with this RDP listener. Enable "Use legacy RDP implementation" in the listener configuration.
FSE1624	ERROR	SYSTEM	Error authenticating user %s over TACACS+.
FUI1625	INFO	USER	User %s authenticated through %s/%s (Host: %s, Port: %d) logged in from address: %s.
FSE1626	ERROR	SYSTEM	Unable to parse the client certificate.
FSE1627	ERROR	SYSTEM	Unable to use the client certificate.
FSE1628	ERROR	SYSTEM	Unable to add a certificate to the client chain.
FSE1629	ERROR	SYSTEM	Unable to parse the client certificate chain.
FSE1630	ERROR	SYSTEM	Unable to parse the client private key.
FSE1631	ERROR	SYSTEM	Unable to use the client private key with the client certificate.
FSE1645	ERROR	SYSTEM	Failed to mark legacy sessionid change as needing a restart.
FAI1646	INFO	ADMIN	Administrator {subject.name} changed the legacy session cookie setting from {old} to {new}.
FSE1647	ERROR	SYSTEM	Raw file {filename} is corrupted: {error}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FUI1656	INFO	USER	Session paused due to policy violation (user %s, safe %s).
FUI1657	INFO	USER	Session paused due to regexp match (user %s, safe %s).
FSW1658	WARNING	SYSTEM	User %s not synchronized from LDAP server %s, reason: %s.
FSE1659	ERROR	SYSTEM	Unable to enable reverse proxy connections for listener %s. Direct connections to this listener are not affected. Contact Fudo support.
FSI1660	INFO	SYSTEM	Tunnel for reverse proxy {name} ({id}) uses routing table {running_fib} instead of {configured_fib}. Terminating and recreating it.
FSE1661	ERROR	SYSTEM	OIDC back-channel logout: unable to scan {dir}: {err}.
FSE1662	ERROR	SYSTEM	OIDC back-channel logout: unable to remove session {name}: {err}.
FSI1663	INFO	SYSTEM	OIDC back-channel logout removed session for user {} (oidc_id={oidc_id}).
FSE1664	ERROR	SYSTEM	Server disconnected during SSH key exchange: %s (%.200s).
FSE1665	ERROR	SYSTEM	Server closed the connection during SSH key exchange.
FSE1666	ERROR	SYSTEM	SSH key exchange error.
FSE1667	ERROR	SYSTEM	OIDC back-channel logout was not propagated to cluster node {node}.
FUW1668	WARNING	USER	File upload from user to session storage blocked [%s]: '%s' (%zu bytes), %s.
FUW1669	WARNING	USER	File upload from user to session storage: unparsable response (%zu bytes buffered).
FUW1670	WARNING	USER	File upload from user to session storage rejected [%s]: %s
FUW1671	WARNING	USER	File upload from user to session storage: unrecognized response (%zu bytes buffered).
FSW1672	WARNING	SYSTEM	File download from server to session storage blocked: %s (%d bytes), %s.
FSI1673	INFO	SYSTEM	The file transfer service started.
FSI1674	INFO	SYSTEM	The file transfer service stopped.
FSE1675	ERROR	SYSTEM	Unable to look up session {session_id}, refusing its start: {e}.
FSE1676	ERROR	SYSTEM	Unable to read the scanning switch for session {session_id}, refusing its {direction} {filename:?}: {e}.
FSW1677	WARNING	SYSTEM	Hashing a transfer of session {session_id} did not finish within {secs} s of its end, its digests are not recorded.
FSE1678	ERROR	SYSTEM	Unable to record the {direction} {filename:?} of session {session_id}, refusing it: {e}.
FSW1679	WARNING	SYSTEM	Transfer {id} of session {session_id} did not report its delivery within {secs} s, its status stays unknown.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSW1680	WARNING	SYSTEM	Transfer {id} of session {session_id} reported a malformed delivery result, its status stays unknown: {reject}.
FSE1681	ERROR	SYSTEM	Unable to record the delivery of transfer {id}: {e}.
FSI1682	INFO	SYSTEM	The scanning engine at {url} echoed a clean object back instead of answering 204, doubling the scanning traffic.
FSE1683	ERROR	SYSTEM	Unable to read the AV scanning configuration: {e}.
FSI1684	INFO	SYSTEM	The scan of a transfer of session {session_id} failed over to engine {name}.
FSE1685	ERROR	SYSTEM	Scanning engine {name} failed a scan of session {session_id}: {why}.
FSW1686	WARNING	SYSTEM	Scanning engine {name} is unreachable: {why}.
FSE1687	ERROR	SYSTEM	Unable to start the file transfer service: {e}.
FSE1688	ERROR	SYSTEM	The file transfer service stopped: {e:#}.
FSI1689	INFO	SYSTEM	Transfer {id} of session {session_id}: {direction} {filename:?}, size {size}, outcome clean, engine {engine}, ISTag {istag}, sha256 {sha256}, sha1 {sha1}, md5 {md5}.
FSW1690	WARNING	SYSTEM	Transfer {id} of session {session_id}: {direction} {filename:?}, size {size}, outcome infected, threat {threat}, engine {engine}, ISTag {istag}, sha256 {sha256}, sha1 {sha1}, md5 {md5}.
FSI1691	INFO	SYSTEM	Transfer {id} of session {session_id}: {direction} {filename:?}, size {size}, outcome not_scanned, scanning off, sha256 {sha256}, sha1 {sha1}, md5 {md5}.
FSW1692	WARNING	SYSTEM	Transfer {id} of session {session_id}: {direction} {filename:?}, size {size}, outcome unscannable, reason {reason}, engine {engine}, waited {queued:.1} s for a slot, {with_engine:.1} s scanning, sha256 {sha256}, sha1 {sha1}, md5 {md5}.
FSI1693	INFO	SYSTEM	Transfer {id} of session {session_id}: {direction} {filename:?}, size {size}, outcome unscannable, reason {reason}, engine {engine}, sha256 {sha256}, sha1 {sha1}, md5 {md5}.
FSI1694	INFO	SYSTEM	Transfer {id} of session {session_id}: {direction} {filename:?}, status completed, location {location}.
FSW1695	WARNING	SYSTEM	Transfer {id} of session {session_id}: {direction} {filename:?}, status failed.
FSE1696	ERROR	SYSTEM	Unable to start charon: {err:#}.
FAI1697	INFO	ADMIN	Administrator {subject.name} created antivirus engine {avscan_engine.name} (address {avscan_engine.address}, port {avscan_engine.port}, service {avscan_engine.service_path}).
FAI1698	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the antivirus engine {old.name} to: {attribute.value}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI1699	INFO	ADMIN	Administrator {subject.name} removed antivirus engine {avscan_engine.name} (address {avscan_engine.address}, port {avscan_engine.port}, service {avscan_engine.service_path}).
FSE1700	ERROR	SYSTEM	Cannot open raw files of session {session_id}: {error}.
FSE1701	ERROR	SYSTEM	Cannot open raw file {file}: {error}.
FSE1702	ERROR	SYSTEM	Cannot build raw HTTP preview response: {e}.
FSE1703	ERROR	SYSTEM	Failed to mark job ({}) {} as in progress; leaving it in the processing queue for the next recovery: {err}
FSE1704	ERROR	SYSTEM	Failed to schedule retry for job ({}) {}; leaving it in the processing queue for the next recovery: {err}
FSE1705	ERROR	SYSTEM	Failed to take a dedicated Redis connection for the queue consumer: {err}
FUE1706	ERROR	USER	Unable to reconnect the outbound RDP transport to the target.
FAI1707	INFO	ADMIN	Administrator {subject.name} initiated mobile application pairing for user {user_authentication_method.user_name}. {user=user_authentication_method.user_id}
FAI1708	INFO	ADMIN	User {subject.name} removed mobile application access for user {old.user_name}. {user=old.user_id}
FSW1709	WARNING	SYSTEM	Failed to query listener TLS credentials: {e}
FSW1710	WARNING	SYSTEM	Listener {listener_id} cert not used to sign .rdp: {reason}
FSW1711	WARNING	SYSTEM	Failed to sign RDP config: {e:#}
FSE1712	ERROR	SYSTEM	HTTP rendered browser crashed on %s: %s
FUW1714	WARNING	USER	Session refused for user %s to safe %s: the user already has an active session %jd to safe %s on node %s, and safe %s does not allow concurrent sessions through other safes.
FUW1715	WARNING	USER	Session %jd of user %s to safe %s has been terminated: the user has an earlier active session %jd to safe %s on node %s, and safe %s does not allow concurrent sessions through other safes.
FUW1716	WARNING	USER	Session allowed for user %s to safe %s, although safe %s does not allow concurrent sessions through other safes: the user may still have an active session %jd to safe %s on node %s, but this cannot be verified because there is no working replication path from that node to this node. Check cluster replication.
FSE1717	ERROR	SYSTEM	Failed to accept client connection: {err}.
FSE1718	ERROR	SYSTEM	Failed to read client request from Unix Socket: {err}.
FSW1719	WARNING	SYSTEM	Listener {listener_id}: .rdp unsigned, {host:?} not allowed.
FAI1720	INFO	ADMIN	Administrator {subject.name} set the Access Gateway allowed {attribute.name} to: {attribute.value}.

continues on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI1727	INFO	ADMIN	Administrator {subject.name} enabled protocol {analysis_agent_protocol.protocol} for analysis agent {analysis_agent_protocol.agent_name}.
FAI1728	INFO	ADMIN	Administrator {subject.name} disabled protocol {analysis_agent_protocol.protocol} for analysis agent {analysis_agent_protocol.agent_name}.

CHAPTER 16

Fudo Officer

Fudo Officer is a mobile app that allows Fudo Enterprise administrators to manage the users' requests to the target servers. The requests are accepted or rejected by the administrators via the Fudo Officer app, or on Admin Panel in the *Sessions* tab.

Fudo Officer also gives users access to the Fudo Enterprise Password Vault: they can browse, request access to and add secrets on their phone, and fill in saved logins in other apps. For more information, refer to the *Password Vault in Fudo Officer* section.

Note

Refer to the *Access Requests* section for more information about the Just In Time feature and maintaining users' requests on the Admin Panel.

Fudo Officer is available for Android and iOS. Download our mobile application from your respective app store.

Warning

Fudo Enterprise works exclusively with the **latest currently available version** of Fudo Officer. Older versions are not supported and may not provide full functionality or compatibility with the system. It is recommended to regularly update the mobile application to ensure security, compliance with current authentication mechanisms, and access to the latest Fudo Enterprise features.

16.1 Configuration

Note

- To bind mobile device, the *Callhome* feature must be enabled. Please navigate to *Settings* > *System*, and enable it on the *General* tab, under the *Maintenance and supervision* section.
- You need to request access to the **Callhome** feature from your Fudo Enterprise distributor.

Note

For the Fudo Officer mobile application to connect to the service, the network used by the mobile device must allow outbound TCP traffic to `officer.fudosecurity.com`:

- on port **443 (HTTPS)** — the app sends the initial request here (with the cluster id) and receives a random, one-time high port in response;
- on ports from the **dynamic range 49152–65535** — the app opens a second HTTPS connection on the assigned port to fetch the requested resource (e.g. `officer.fudosecurity.com:<port>/api/v2/requests`). The TCP connection stays open until the app closes it.

On the Fudo Enterprise side, the ports required by the *Callhome* feature must be open.

To configure Fudo Officer, please download the application from the respective app store for Android or iOS, and follow the instruction:

Warning

During the configuration process, ensure that you grant Fudo Officer permission to access the camera and send notifications.

1. Set up Fudo Enterprise:

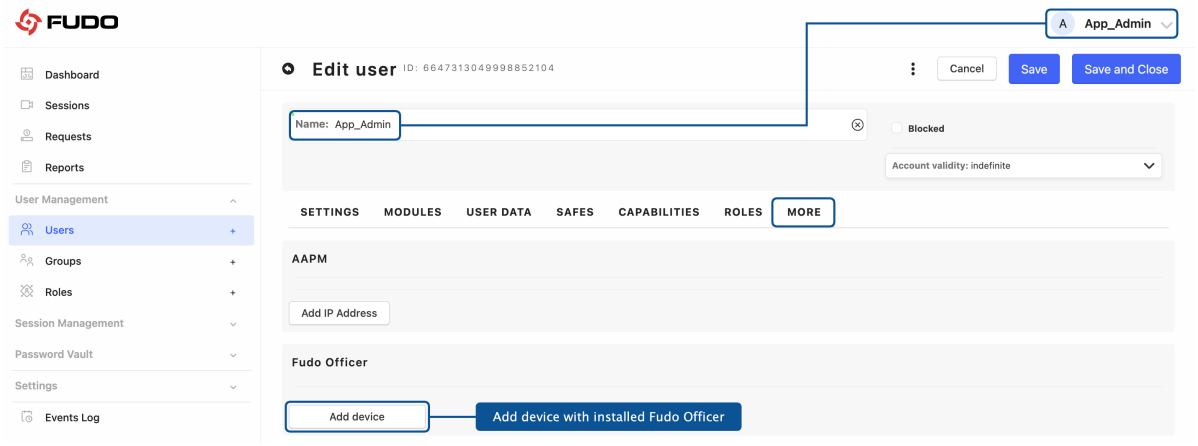
   1.1. Open Fudo Enterprise Admin Panel and go to *User Management* > *Users*.

   1.2 Find and edit the user for whom you want to create a profile in the Fudo Officer.

   1.3. Go to the *MORE* tab and click the *Add device* button in the *Fudo Officer* field to generate the QR code.

Note

- In the Admin Panel, the QR code can be generated only for the user currently logged in. For other users, initiate pairing as described in *Pairing initiated by an administrator* below.
- For the permissions required to pair and use the Fudo Officer mobile app, see *Fudo Officer permissions*.



2. Open Fudo Officer app on your mobile device and tap *Get started*:

   2.1. Allow Fudo Officer to access the camera, which is required for scanning QR codes.

   2.2. Tap *Scan QR code* and scan the QR code displayed in the Admin Panel with your mobile device.

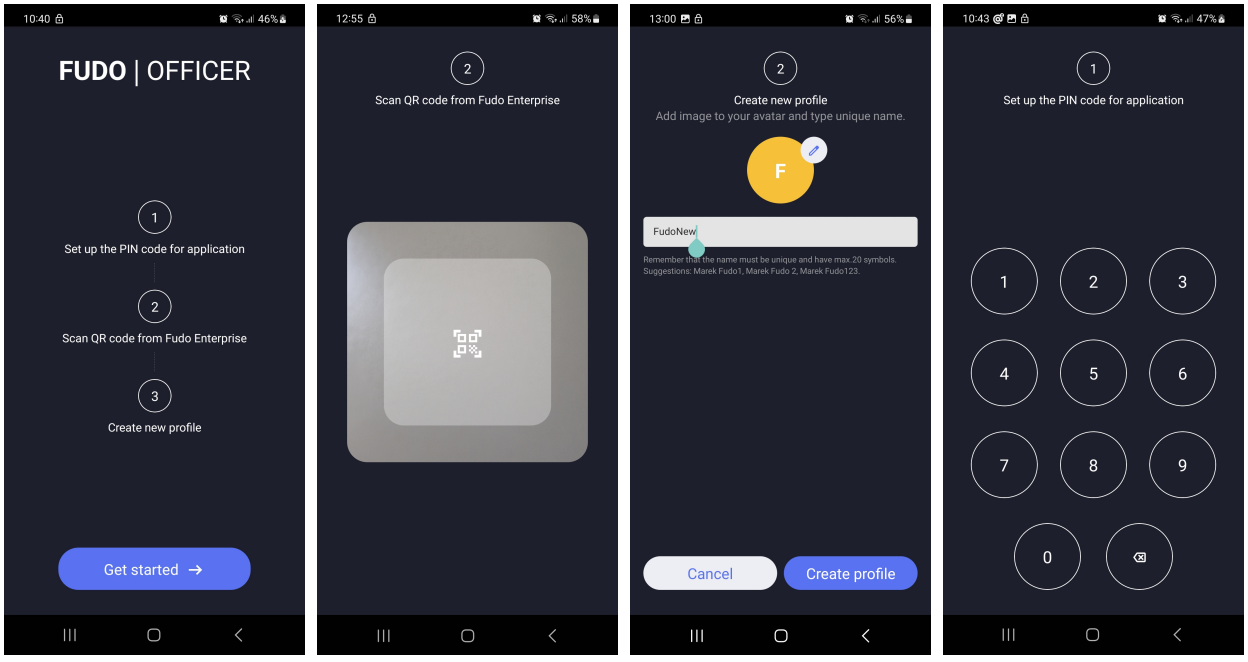
   2.3. Set a profile name and tap the *Create profile* button.

   2.4. Set a 6-digit PIN that will be used to protect access to the application.

   2.5. Repeat the provided PIN to confirm it.

   2.6. Choose whether to enable biometric sign-in. You can change this later in the application settings.

   2.7. Allow Fudo Officer to send notifications.



Note

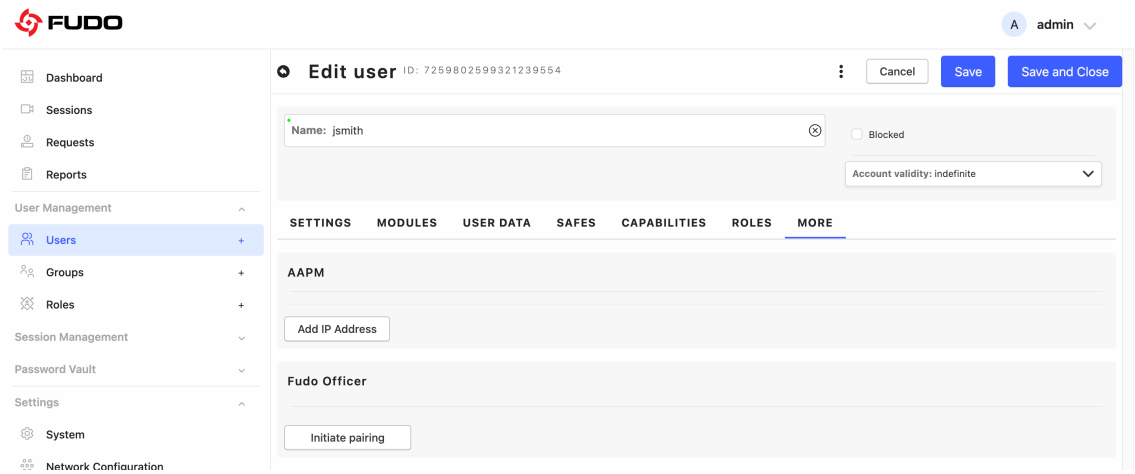
The profile name is editable.

3. Go back to the Fudo Enterprise Admin Panel and click *Close* in the QR code window. The *Fudo Officer* section now has the *Platform* field filled with the binding device name and the *Push ID* with the respective string.
4. Click the Save button to save changes in the user configuration.
5. Now, you can manage the users' requests via the created profile.

Pairing initiated by an administrator

Users who sign in only to the User Access Gateway can pair Fudo Officer there, after an administrator initiates the pairing for them:

1. In the Admin Panel, go to *User Management* > *Users* and edit the user.
2. Go to the *MORE* tab and click *Initiate pairing* in the *Fudo Officer* field.



3. Ask the user to sign in to the User Access Gateway, select *Fudo Officer app* from the user menu and scan the displayed QR code with the Fudo Officer mobile app.

Note

- *Initiate pairing* is available to administrators who can modify the user, as long as the user has no paired device.
- Until the user completes the pairing, you can cancel it with *Disconnect device*.
- To remove the pairing, click *Remove binding* in the *Fudo Officer* field. To pair the app again, initiate pairing again.

Related topics:

- *Managing Profiles*
- *Managing Session Requests*
- *Fudo Officer Settings*

16.2 Managing Profiles

A Profile corresponds to the User object in the Fudo Enterprise. You can manage multiple Profiles from a single application.

16.2.1 Add New Profile

Note

The first Profile is created during the *initial configuration of the application*.

Note

- You can configure the device association only for the user currently logged into the Fudo Enterprise's Admin Panel.
- Only user with the *superadmin* or *admin* role can use the Fudo Officer mobile app.

To add new profile, follow below steps:

1. Set up Fudo Enterprise:

   1.1. Open Fudo Enterprise Admin Panel and go to *User Management* > *Users*.

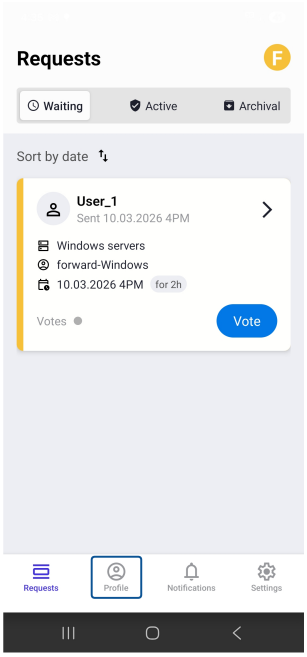
   1.2 Find and edit the user for whom you want to create a profile in the Fudo Officer.

   1.3. Go to the *MORE* tab and click the *Add device* button in the *Fudo Officer* field to generate the QR code.

Note

- To add mobile device *Callhome* feature has to be enabled. Please navigate to Settings > System, and enable it on the *General* tab, under the *Maintenance and supervision* section.
- You need to request access to the **Callhome** feature from your Fudo Enterprise distributor.

2. Open Fudo Officer app, tap the *Profile* icon at the bottom of the screen, and click the *+ Add new profile* button.



3. Scan the QR code displayed in the Admin Panel with your mobile device.
4. Set a Profile name and click the *Create profile* button.

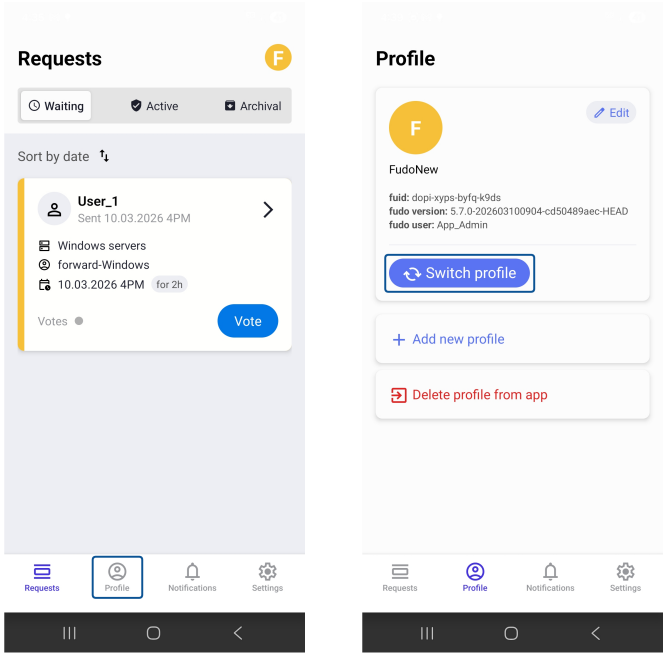
> **Note**
>
> The profile name is editable.

5. Go back to the Fudo Enterprise Admin Panel and click *Close* in the QR code window. The *Fudo Officer* section now has the *Platform* field filled with the binding device name and the *Push ID* with the respective string.
6. Click the *Save* button to save changes in the user configuration.

16.2.2 Switch Profiles

You can easily switch profiles to manage requests from different assignments. To switch between available profiles, follow below steps:

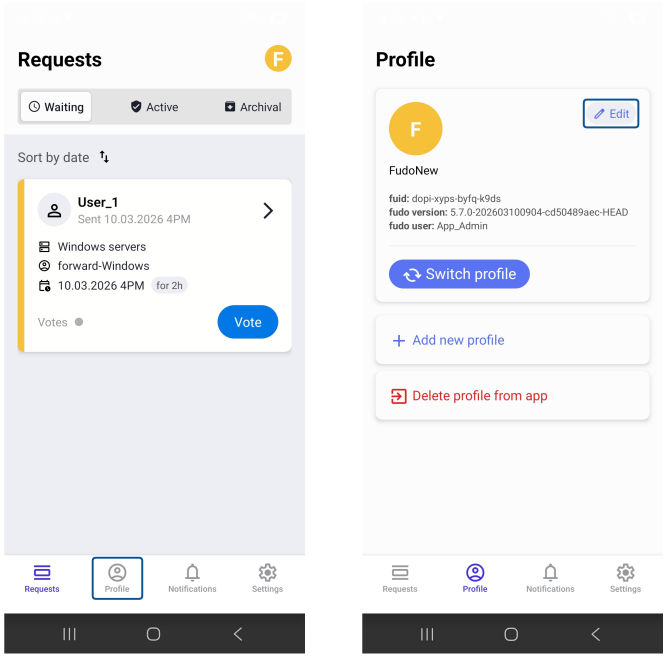
1. Tap the *Profile* icon at the bottom of the screen.
2. Chose *Switch profile* to access the list of available profiles.
3. Tap the desired profile name from the list to select it.
4. You will be automatically redirected to the *Requests* view to manage requests addressed for this profile.



16.2.3 Edit Profile

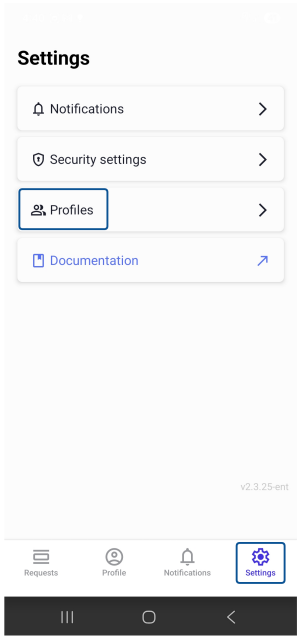
You can edit the name and the profile picture of an active profile:

1. Choose the *Profile* icon at the bottom of the screen.
2. Tap *Edit* icon next to the Profile's name.
3. Provide new Profile's name.
4. Edit the avatar by taping the pencil icon next to it and uploading desired image from your mobile storage.
5. Click 'Save' to save the changes.



Note

You can also switch profiles in the application settings. Just click on the gear icon in the bottom right corner of the screen, and tap *Profiles*.



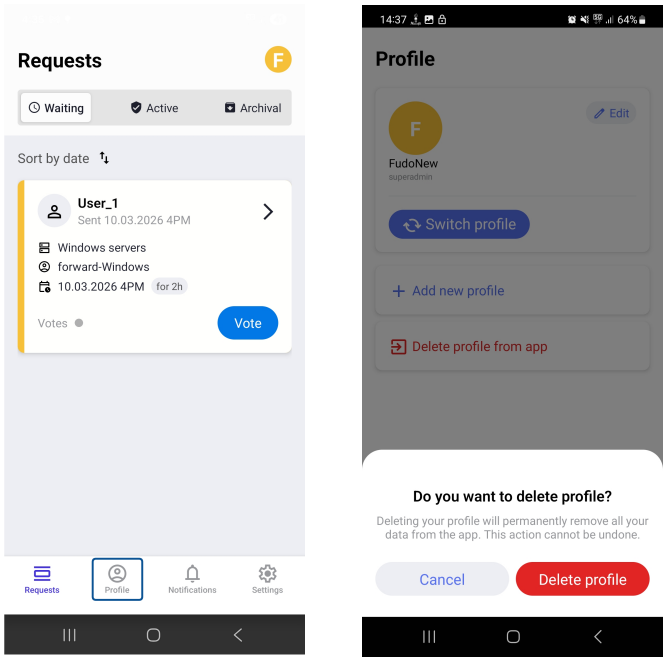
Note

To change PIN, please follow the *Change PIN Code* section.

16.2.4 Delete Profile

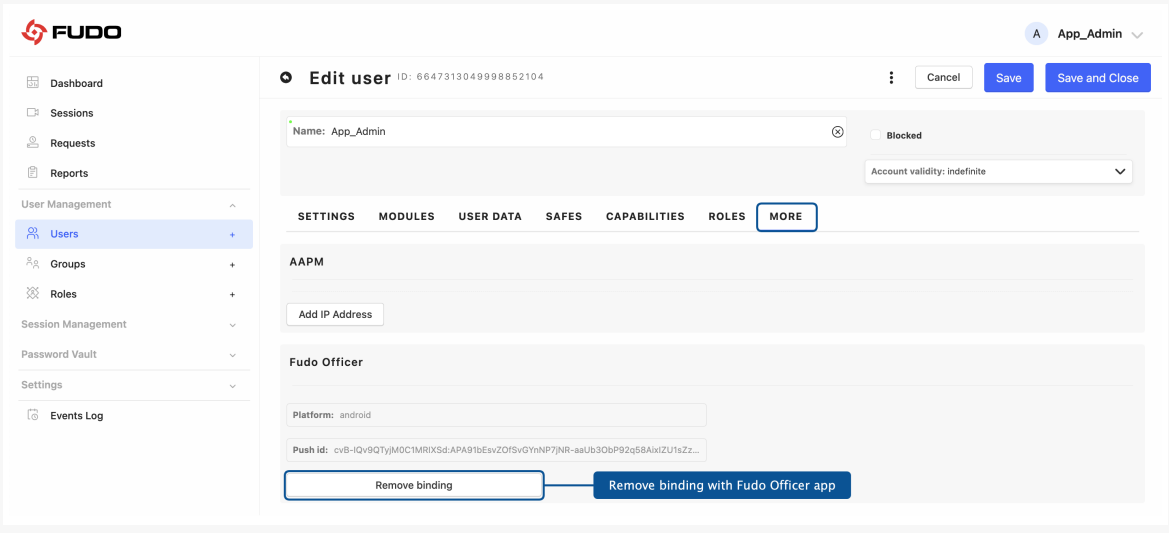
To delete profile from the Fudo Officer, first you have to switch to this profile:

1. Tap the *Profile* icon at the bottom of the screen.
2. Chose *Switch profile* to access the list of available profiles.
3. Tap the desired profile name from the list to select it.
4. Once more tap the *Profile* icon at the bottom of the screen.
5. Tap *Delete profile from app.*
6. Tap 'Delete profile' to confirm.



Note

Ensure that you disconnect the device in the user configuration in the Fudo Enterprise Admin Panel.



Related topics:

- *Managing Session Requests*
- *Fudo Officer Settings*

16.3 Managing Session Requests

There are three types of requests: awaiting, active, and archival.

Note

To be able to manage requests, ensure the *Just In Time* option is selected within the assigned safe Safe, and enable the *Access request sent (push)* option for push notifications for the user. To learn more about this topic, refer to the **GENERAL TAB**, and **PERMISSIONS AND NOTIFICATIONS TAB** subsections in the *Creating a Safe* section.

16.3.1 Awaiting Requests

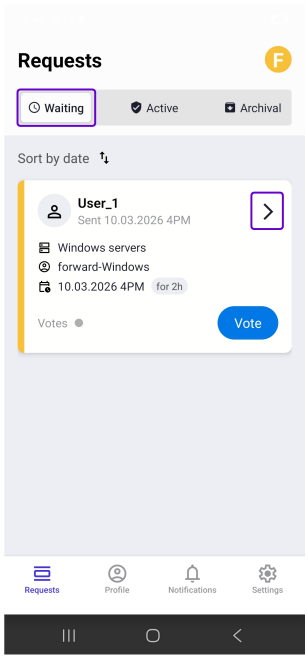
The **Waiting tab** shows a list of the requests that are waiting for a decision of the current user profile.

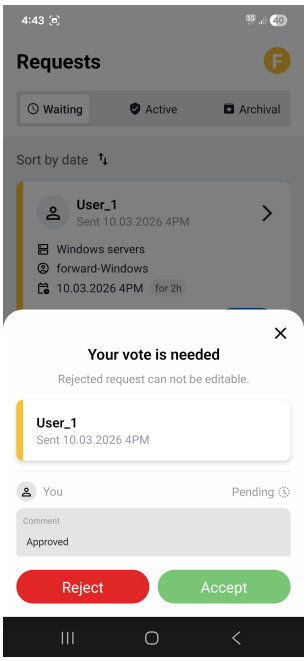
Note

- Two types of requests are available for the user who sends an access request: *immediate* and *scheduled*. For detailed information, refer to the *Access Requests* section.
- To learn how users can send requests, refer to the Connecting via access request section of the Access Gateway documentation.
- Requests can also concern Password Vault secrets. For such requests, the request details show the secret and its collection instead of the server and account.
- The access period is shown as the start date and time, followed by the duration. For scheduled requests, the end date is also shown. Dates and times are displayed in the time zone of the mobile device.

In order to vote for approval or rejection of the request, follow the steps:

1. Open Fudo Officer and provide PIN code. You will be automatically redirected to the **Waiting tab.**
2. Tap the arrow next to the username to expand the request details.
3. Alternatively, tap *Vote* button to accept or reject the request directly from this tab.
4. In case of rejection a comment for the decision is required.
5. Tap *Accept* or *Reject* button.





Note

- Accepted requests can be found under the **Active tab**.
- Rejected requests can be found under the **Archival tab**.

Note

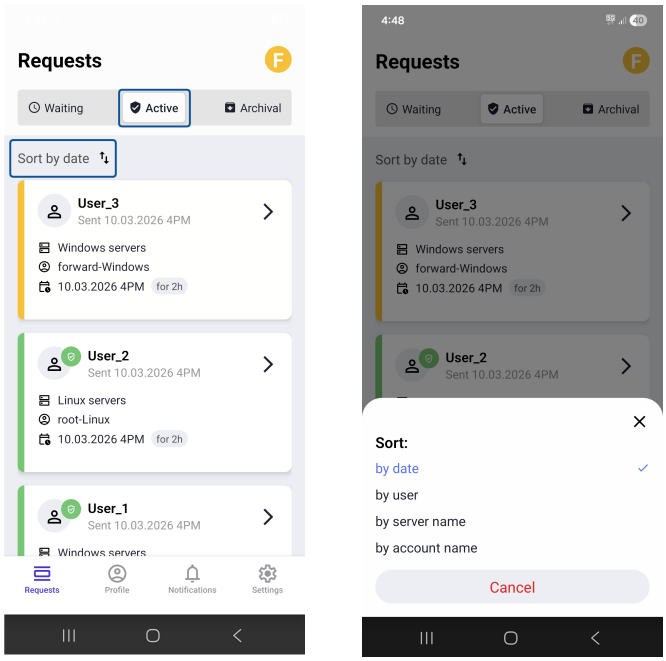
- Users who sent the request via the User Access Gateway and have their e-mail address configured on the Admin Panel, receive notifications when their request was accepted or rejected.

16.3.2 Active Requests

The **Active tab** displays a list of two types of requests:

- Requests that have been accepted by the required number of voters (marked in green).
- Requests that are waiting for other voters (marked in yellow).

Requests can be sorted by *date, user, server name, or account name.*



16.3.3 Revoking Request

Given vote for accepted and active requests can be revoked, for example, for preventing a possible misuse. This option is useful when the user finished their work earlier than expected, but their request is still valid.

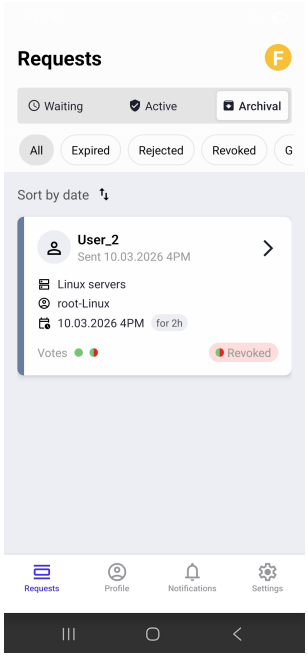
In order to revoke accepted and active requests, follow the steps:

1. Open Fudo Officer and provide PIN code.
2. Tap **Active tab.**
3. Tap the arrow next to the username to expand the request details.
4. Tap the *Edit Vote* button at the bottom of the request screen.
5. In the **Comment** field, provide the reason for the revocation (required).
6. Tap the *Reject* button to revoke the request.

> **Note**
>
> If you have accepted a request that is still awaiting votes from other administrators, the *Reject* button will be available directly on the request screen.

16.3.4 Archived Requests

History of the processed requests is available under the **Archival tab.** Archived requests can be sorted by *expired, rejected, revoked,* and *granted* status.



Related topics:

- *Fudo Officer Settings*

16.4 Password Vault in Fudo Officer

The *Vault* tab gives you access to the Fudo Enterprise Password Vault on your phone. It shows the organization collections assigned to you and your personal vault, with the same secrets you see in the User Access Gateway.

Note

- The *Vault* tab is not available with the Basic license.
- What you can do with a secret depends on the access level assigned to its collection: *View on request*, *View* or *Full edit*. For more information, refer to the *Assigning Users and Groups to Collections* section.

16.4.1 Browsing Secrets

To browse secrets, tap *Vault* at the bottom of the screen. The *Secrets* screen opens.

The *Secrets* screen offers the following options:

- The filter buttons show *All* secrets, only *Organization* secrets (building icon) or only *Personal* secrets (person icon).
- The buttons on the right switch between the collection view (folder icon) and a flat list of secrets.
- In the collection view, tap a collection to open it. Nested collections are shown before the secrets of the collection. Tap the arrow next to the collection name to go back.
- The *Search secrets* field searches secret names in the whole vault.

Personal collections and secrets are marked with a person icon, so you can tell them apart from organization ones.

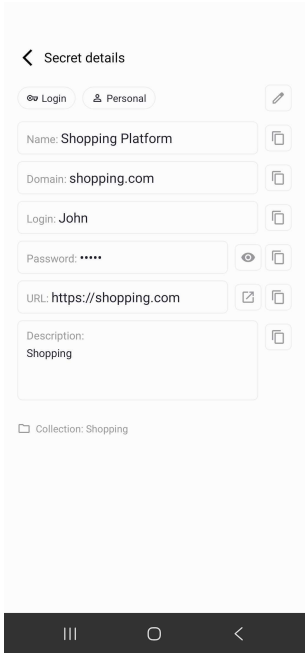
16.4.2 Secret Details

Tap a secret to open the *Secret details* screen. The tags at the top show the secret type and the vault it belongs to.

The screen shows the following information:

- Each field has a copy button. The password, key or note is masked; tap the eye icon to reveal it.
- The *URL* field shows the first URL saved for the secret. Tap the arrow icon to open it in the browser.
- *Collection* shows the collection that holds the secret.
- *Last use* shows when the secret details were last opened on this device. It is not shown the first time you open a secret.

The pencil icon is available only when you can edit the secret. See *Editing a Secret* below.



16.4.3 Requesting Access to a Secret

In a collection with the *View on request* access level, the secret value is replaced by the *Access request* button. To view the value, send an access request and wait for an administrator to approve it.

1. Open the secret and tap *Access request*.
2. Select the request type:
    - *Immediate* - access is granted as soon as the request is approved. Use the *Time* slider to set how long you need access, from 1 to 24 hours.
    - *Scheduled* - access is granted for the selected period. Set *Start* and *End*. The start cannot be in the past, and the period must be at least one hour long.

3. Enter the reason in the *Reason (required)* field, up to 250 characters.
4. Tap *Send request*.

Until the request is approved, the secret shows the message that the access request is pending. After approval, you can reveal and copy the secret value.

16.4.4 Checking Out Secrets

For secrets with managed checkout, the value is available only after checkout:

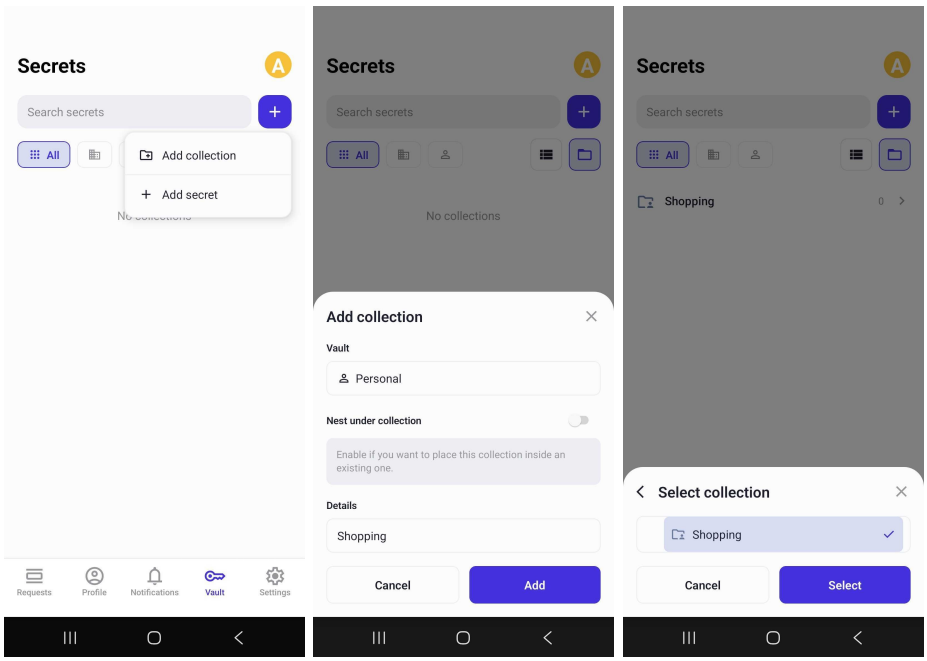
- Tap *Checkout* to check the secret out. You can then reveal and copy its value.
- Tap *Checkin* to return the secret when you no longer need it.
- With exclusive checkout, the *Checkin* button shows the remaining time. A secret checked out exclusively by another user cannot be checked out until it is returned.

For other secrets, the app checks the secret out and back in automatically when you reveal or copy its value.

16.4.5 Adding a Collection

The app creates collections in your personal vault.

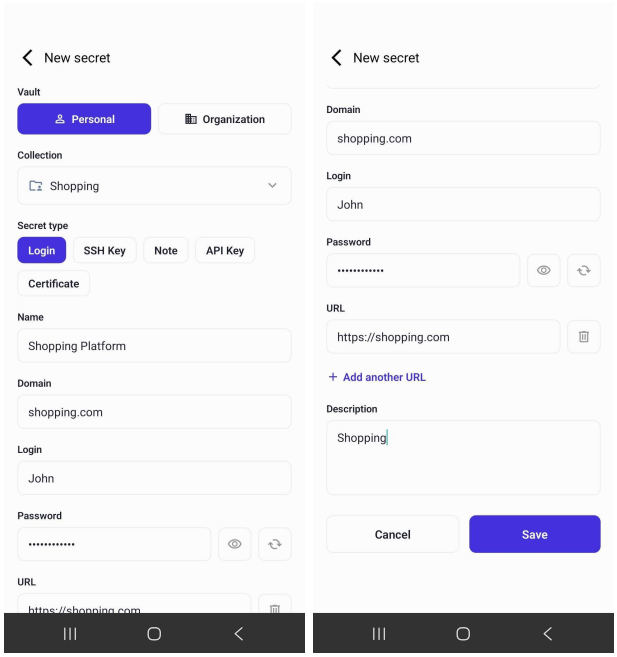
1. On the *Secrets* screen, tap the + button and select *Add collection*.
2. To place the new collection inside an existing one, enable *Nest under collection*, select the parent collection and tap *Select*.
3. Enter the collection name in the *Details* field.
4. Tap *Add*.



16.4.6 Adding a Secret

You can add secrets to your personal collections and to organization collections where you have the *Full edit* access level.

1. On the *Secrets* screen, tap the + button and select *Add secret*.
2. In the *Vault* field, select *Personal* or *Organization*.
3. In the *Collection* field, select the target collection. Only collections where you can add secrets are listed.
4. Select the *Secret type* and fill in the fields. See the table below.
5. Optionally, enter one or more URLs and a description. Tap *Add another URL* to add more URLs.
6. Tap *Save*.



Note

- The secret value can be up to 64 KiB.
- Private keys and certificates are validated while you type. The certificate must match the private key.
- If the password does not meet the password policy, the app shows a warning, but the secret is still saved.

Generating Passwords and Keys

The app can generate the secret value for you:

- For a *Login* secret, tap the generate icon next to the *Password* field. Set the *Length* and the character groups to include, optionally enter characters to exclude, and tap *Use*. When the password policy defines complexity requirements, *Use default settings* applies them.

- For an *SSH Key* secret, tap the generate icon next to the *Private key* field, select the *Key Algorithm* and tap *Generate*. The default algorithm is Ed25519.
- For a *Certificate* secret, tap the generate icon next to the *Private key* field, select the *Key Algorithm*, enter the Common Name and tap *Generate*. The app generates a private key and a self-signed certificate.

16.4.7 Editing a Secret

To edit a secret, open it and tap the pencil icon. The icon is available in collections where you have the *Full edit* access level.

The following rules apply when you edit a secret:

- The secret type, vault and collection cannot be changed.
- The password, key and note fields are empty. Leave a field empty to keep its current value.
- A secret cannot be edited while it is checked out.

16.4.8 Limitations

Some Password Vault operations are not available in the app:

- Deleting secrets and collections.
- Renaming collections.
- Creating organization collections.
- Moving secrets to another collection.

Use the User Access Gateway or the Admin Panel for these operations.

16.4.9 Autofill

Fudo Officer can fill in logins and passwords from the Password Vault in other apps and on websites, on Android and iOS.

Enabling Autofill

1. Choose the gear icon in the bottom right corner of the screen.
2. Choose *Security settings*.
3. Switch on *Enable system autofill service*.

The next steps depend on the system:

- On Android, select Fudo Officer as the autofill service in the system window that opens. To use autofill in Chrome, also tap *Use autofill in Chrome*.
- On iOS, biometric authentication must be enabled in the app first. The switch opens the iOS settings, where you enable Fudo Officer under *Settings* > *Passwords* > *AutoFill*.

Note

On Xiaomi, Redmi and POCO devices, autofill also requires the *Display pop-up windows while running in the background* and *Autostart* permissions for Fudo Officer. Use the buttons shown in *Security settings* to open the respective system settings.

Filling In a Login Form

1. In another app or on a website, tap the login field and select Fudo Officer from the autofill suggestions.
2. Unlock the vault: enter your PIN on Android, or use biometric authentication on iOS.
3. Select the secret to fill in. The login and the secret value are entered in the form.

By default, the list shows only secrets with a URL that matches the host of the app or website (*Only secrets for <host>*). The host must match exactly; subdomains do not match. For Android apps without a web address, the app package name is used as the host. To search the whole vault, switch the filter off; the search returns up to 30 secrets.

Tip

Add the URL of the website to a secret, so that the secret is suggested on that website.

Secrets that require an access request, and secrets checked out exclusively by another user, are greyed out and cannot be filled in.

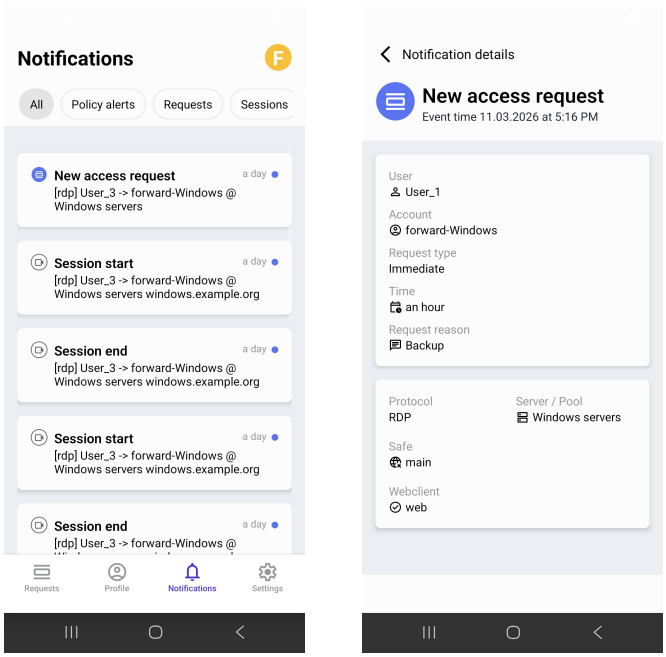
Related topics:

- *Assigning Users and Groups to Collections*
- *Fudo Officer Settings*

16.5 Notifications

The **Notifications** tab allows you to review the history of notifications configured for the current profile.

1. At the bottom of the screen, choose the bell icon labeled *Notifications*.
2. Review the history of notifications assigned to this user.
3. Use the available filters to narrow the list of notifications by category:
   - *Policy alerts*
   - *Requests*
   - *Sessions*
   - *Events*
4. Click selected notification to review the details.



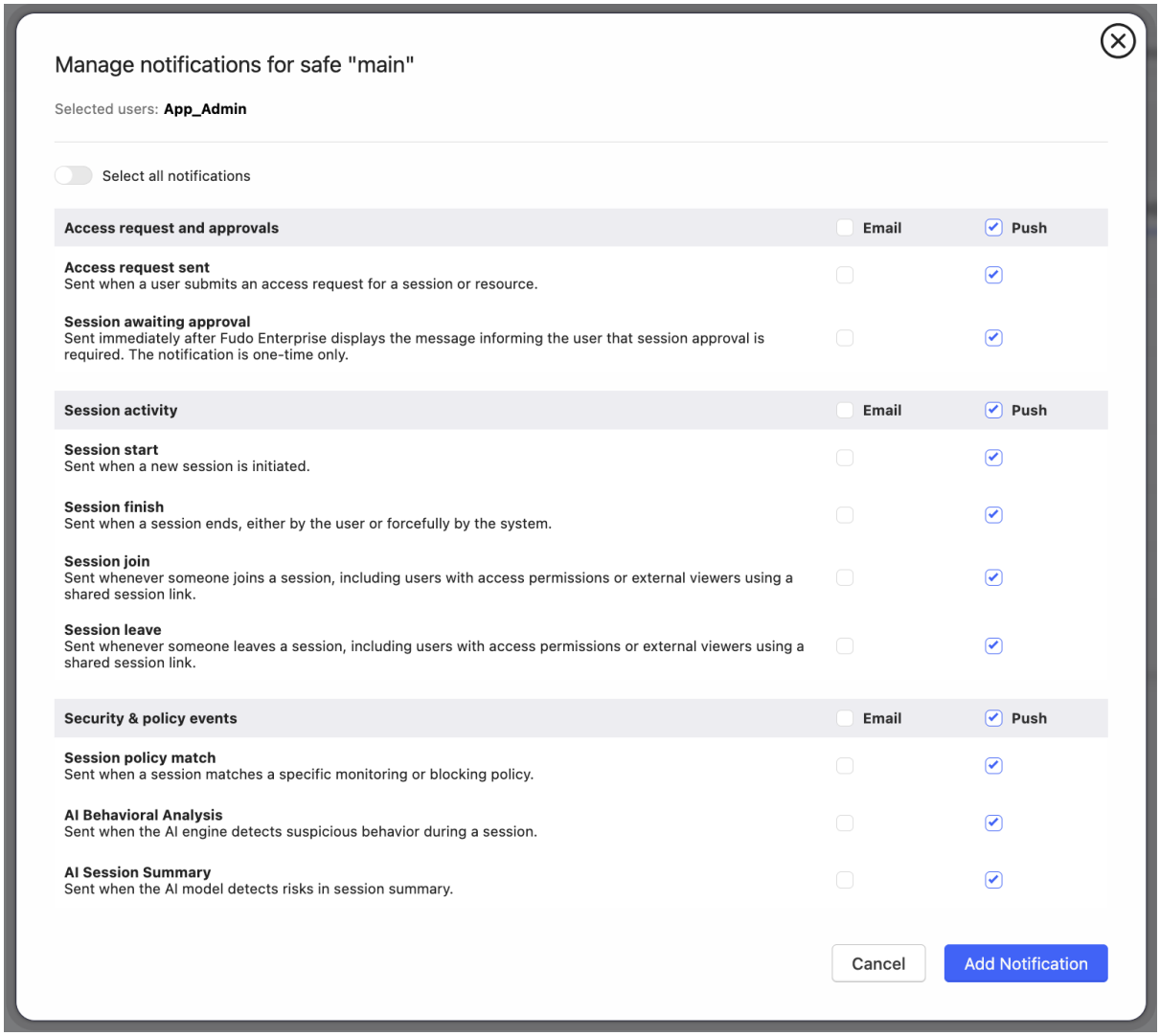
Note

- The event time is displayed in the time zone of the mobile device.
- The *Requests* category also includes notifications about your accepted and rejected access requests.

16.5.1 Configuring Application Notifications

Application notifications are configured in Fudo Enterprise, in the safe settings, in the *Notifications* tab. Selected notifications are then delivered to the application for the user associated with the profile.

1. Log in to Fudo Enterprise Admin Panel.
2. Select *Session Management* > *Safes* and open the safe for which you want to configure notifications.
3. Go to the *NOTIFICATIONS* tab.
4. To define notification types for a user, select the checkbox in front of the desired user's name and click *Manage Notifications*.



5. In the list of notification types, select the notifications that should be available for the user in the application.
6. Mark the appropriate entries in the *Push* column.
7. Click *Add Notification* to save the settings and close the modal window.
8. Click *Save* or *Save and close* to save the safe configuration.

Related topics:

- *Managing Session Requests*
- *Fudo Officer Settings*

16.6 Settings

To access the application settings, click on the gear icon in the bottom right corner of the screen.

16.6.1 Biometric Authentication

To enable Biometric Authentication option:

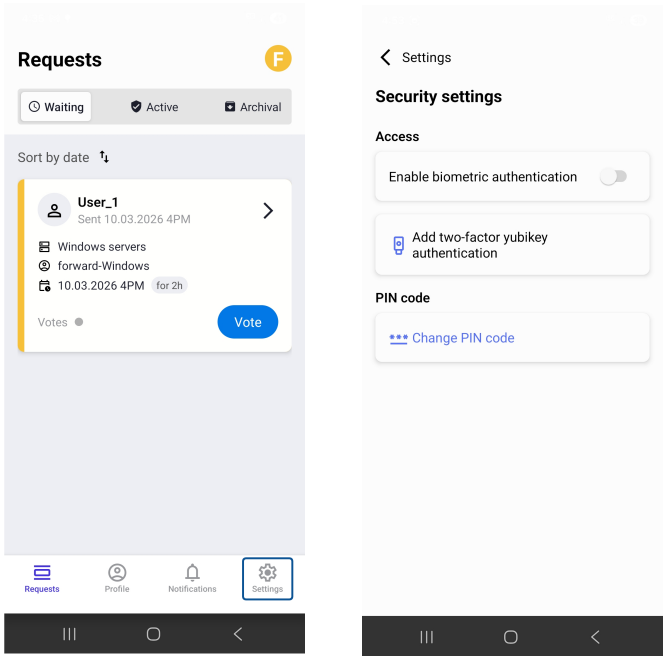
1. Choose the gear icon in the bottom right corner of the screen.
2. Choose *Security settings*.
3. Switch on the *Enable Biometric Authentication* option.
4. Scan your fingerprint to complete the procedure.

Note

- Once the option is enabled, biometric authentication will be set as the default method when launching the application.
- After updating the application to version 2.4, biometric authentication is switched off. Enable it again to continue using it.
- On iOS, biometric authentication is required for *autofill*. Switching it off also stops autofill.

16.6.2 Change PIN Code

1. Choose the gear icon in the bottom right corner of the screen.
2. Choose *Security settings*.
3. Choose *Change PIN code*.



4. Provide a new 6 digits PIN code.
5. Repeat provided 6 digits PIN code to confirm the change.

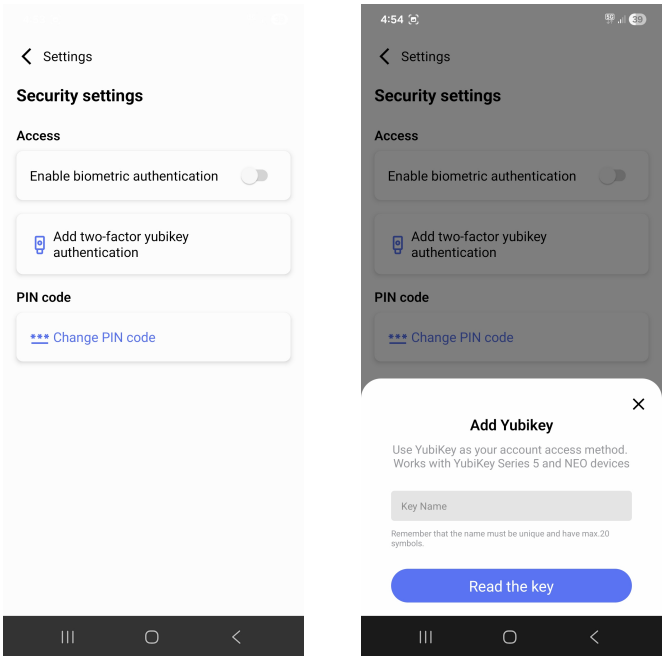
Note

- The current PIN is not required. The new PIN protects all profiles in the application.
- *Change PIN code* is not available when you signed in with biometric authentication. Sign in with your PIN to change it.

16.6.3 Two-Factor YubiKey Authentication

To use YubiKey as your profile access method:

1. Choose the gear icon in the bottom right corner of the screen.
2. Choose *Security settings*.
3. Tap the *Add Two-Factor YubiKey Authentication* option.
4. Enter the Key Name and tap *Read the key* button.
5. Touch the YubiKey to your mobile device to complete the procedure.



Note

Fudo Officer supports NFC connection with *YubiKey 5 Series, YubiKey 5 FIPS Series and YubiKey NEO* devices.

16.6.4 Autofill

The *Security settings* screen also contains the *Enable system autofill service* option, which lets Fudo Officer fill in logins and passwords from the Password Vault in other apps. For more information, refer to the *Autofill* section.

16.6.5 Application Lock

Fudo Officer protects access to the application in the following ways:

- When the application stays in the background for more than 30 seconds, you need to enter your PIN or use biometric authentication again.
- After three incorrect PIN attempts, signing in with the PIN is blocked for 5 minutes. You can still sign in with biometric authentication. The lock remains in place when you restart the application.
- The PIN is verified by Fudo Enterprise, so the device must be able to connect to Fudo Enterprise to unlock the application.

Note

If an administrator has deactivated your profiles, each sign-in attempt is treated as an incorrect PIN, and repeated attempts block signing in with the PIN.

16.6.6 Clearing App Data

Clearing app data removes all profiles, keys and databases from the device. Use it, for example, when you no longer remember your PIN.

1. On the PIN screen, tap the three-dot icon in the top right corner, or tap *Clear app data* in the window shown when signing in with the PIN is blocked.
2. Tap *Clear app data* to confirm.

Warning

This operation cannot be undone. To use the application again, you need to pair it with Fudo Enterprise again, as described in the *Configuration* section.

Updating from earlier versions

After updating from an earlier version, the application migrates the profiles to the new storage the first time you enter your PIN. The migration requires a connection to the Fudo Enterprise instance of each profile.

If a profile is not available, the application offers the following options:

- *Retry migration* - try again, for example after restoring the connection.
- *Delete profile "<name>" and retry* - remove the unavailable profile and migrate the remaining ones.
- *Clear app data* - remove all profiles from the device.

16.6.7 Language

The application language is set according to the phone's language settings.

Related topics:

- *Managing Session Requests*

CHAPTER 17

Fudo ShareAccess

Fudo ShareAccess is a revolutionary platform that enables instant collaboration between enterprises and third parties. It allows you to provide fast and secure vendor access while simplifying resource sharing across diverse environments.

Fudo ShareAccess integrates privileged access management, streamlines connection and credential setup, and provides third parties with instant, seamless access to resources directly through their web browsers, ensuring security and simplicity.

Fudo Enterprise serves Fudo ShareAccess as a **Gateway** providing both an access point to resources and a platform for configuring access to those resources.

> **Note**
>
> This chapter provides a description of the configuration process from within Fudo Enterprise. For more information about Fudo ShareAccess, please refer to the dedicated ShareAccess documentation.

17.1 Data Model

Fudo ShareAccess defines following object types:

Organization - Object representing company that is using Fudo ShareAccess. It is required that every user of Fudo ShareAccess is assigned to organization as member.

User - An object representing the account of an individual using Fudo ShareAccess. It is created during the sign up process and is utilized for authenticating and authorizing the user to access the shared data.

Gateway - An object representing Fudo Enterprise in Fudo ShareAccess, assigned to an Organization. The Gateway serves as the access point to resources and the central configuration hub for managing access to those resources.

Resource - A representation of a resource that can be connected to, received from Fudo Enterprise. A resource can be shared with a user through Fudo ShareAccess by configuring the

settings in the Fudo Enterprise Admin Panel. Fudo ShareAccess does not store any information about the resources; it presents the configuration retrieved from the Fudo Enterprise Admin Panel.

Related topics:

- *Pairing Fudo Enterprise with Fudo Shareaccess*
- *Manage Fudo ShareAccess Members*
- *Manage Access to Resources*

17.2 Pairing Fudo Enterprise with Fudo Shareaccess

Note

There are few requirements that must be met before pairing Fudo Enterprise with Fudo ShareAccess can be finished:

- A user with a role that has permissions to manage Fudo ShareAccess and an email identical to that of the **Organization** owner must exist in the Fudo Enterprise configuration.
- NTP configuration is required. Please go to *Settings* > *System* configuration and set up NTP server (refer to *Date and Time* section).
- DNS configuration is required. Please go to *Settings* > *Network configuration* configuration and set up NTP server (refer to *DNS Configuration* section).
- To establish a tunnel between Fudo Enterprise and Fudo ShareAccess, outbound traffic on port 65522 must be allowed to any destination.

Note

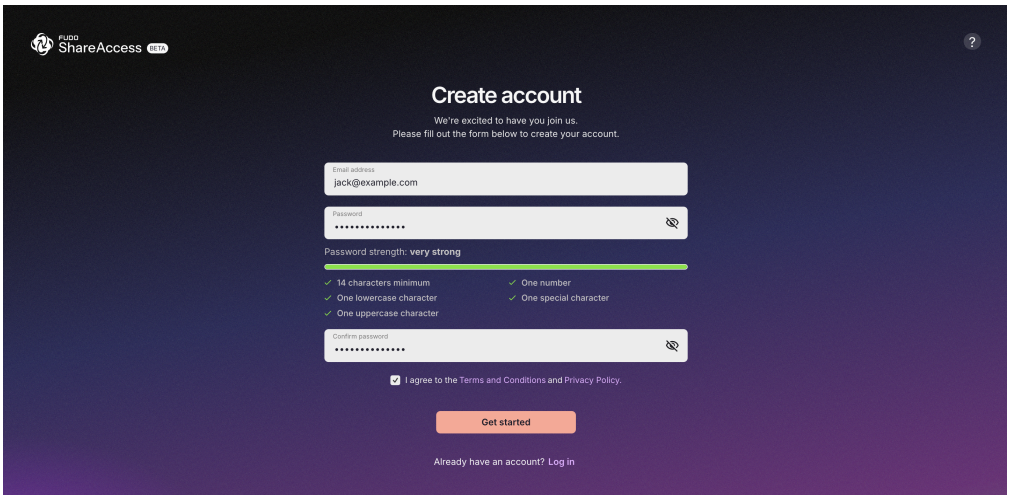
To enable Fudo Enterprise communication with the Fudo ShareAccess platform, make sure the following outbound connections are allowed:

- `api.shareaccess.com` on port `443` – required for API communication over HTTPS.
- `connect.shareaccess.com` on port `65522` – required to establish a tunnel between Fudo ShareAccess and Fudo Enterprise.
- `acme-v02.api.letsencrypt.org` on port `443` - required for certificate issuance and renewal.

1. Log in to Fudo Enterprise instance Admin Panel.
2. Create user:
    - Select *User Management* > *Users* and then click + *Add user*.
    - Enter user name.
    - Click *Save*.
    - In the *Role* tab, click *Assign Role* and select a role that has permissions to manage Fudo ShareAccess.

- In the *User Data* tab, in the *User info* field enter:
  - user's full name,
  - user's email address (provide the same email address as for your Fudo ShareAccess account),
  - user's organizational unit,
  - user's phone number.
- Click *Save*.
- Go back to the *Settings* tab, and in the *Authentication* section select desired authentication type from the *Add authentication method* drop-down list. This will be used to authenticate user against Fudo Enterprise User Access Gateway.
- Click *Save and close*.

3. Create an account in Fudo ShareAccess:
   - Go to the Fudo ShareAccess website.
   - Click *Sign In*.
   - Provide the same email address as the user created in Fudo Enterprise.
   - Provide password for created account.

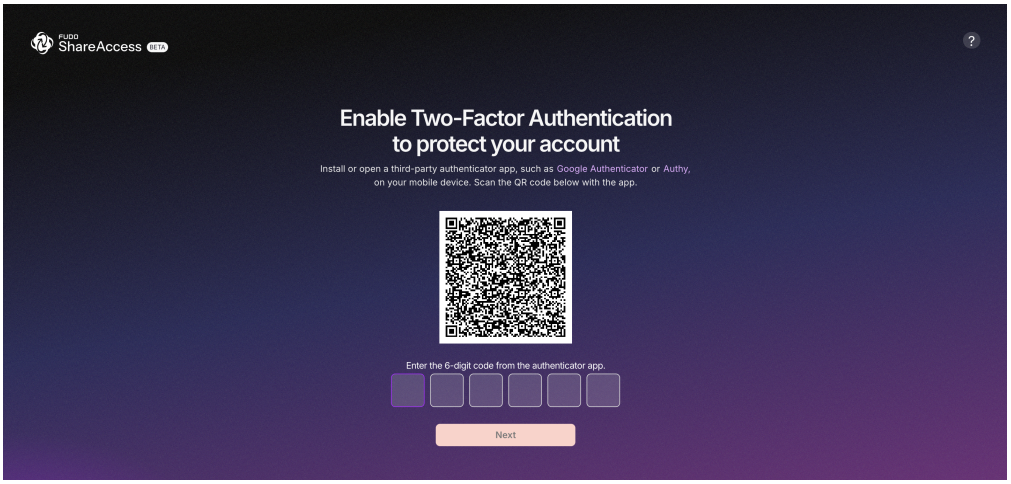


Note

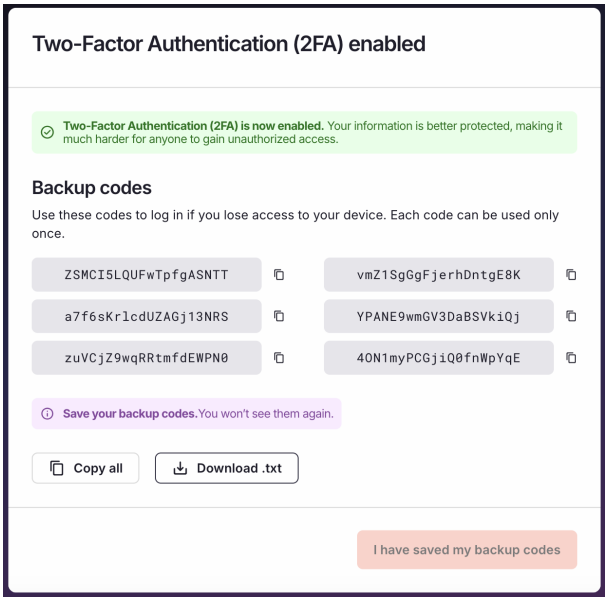
To create an account you have to agree to our Terms and Conditions and Privacy Policy.

- Click Get started.
- Please check your email for a confirmation message and follow the provided link to verify your account.
- After verifying your email, log in using the email and password you provided during registration to proceed with account setup.

- Open a third-party authenticator app, such as *Google Authenticator* or *Authy*, on your mobile device and scan the QR code displayed on the screen.
- Enter the 6-digit code from the authenticator app.



- Click Next.
- Secure your backup codes displayed in the modal window. Use the Copy all button to copy the codes and save them in a secure location, or click Download to download the codes as a `.txt` file. Please note that these codes will not be displayed again.



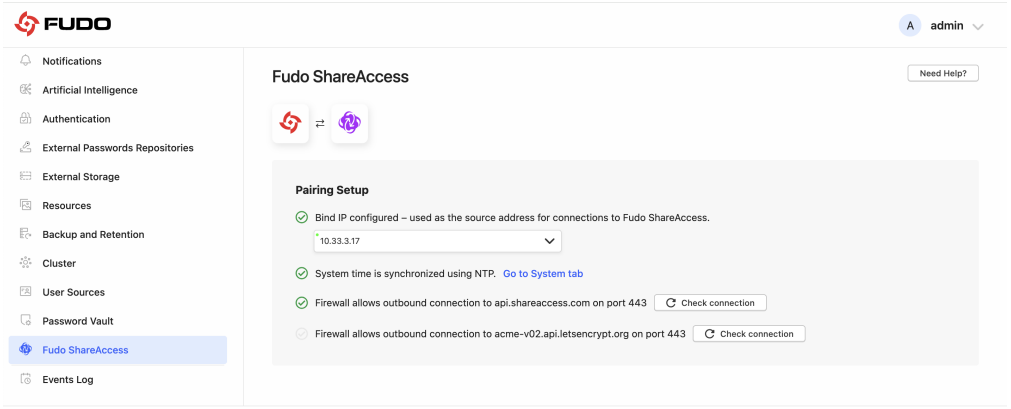
Warning

- If you lose your backup codes, you will no longer be able to access your account. In such cases, please contact Fudo Support immediately for assistance.

- Click I have saved my backup codes to confirm the backup and complete the configuration process.

4. In the Fudo Enterprise Admin Panel, start the pairing setup:

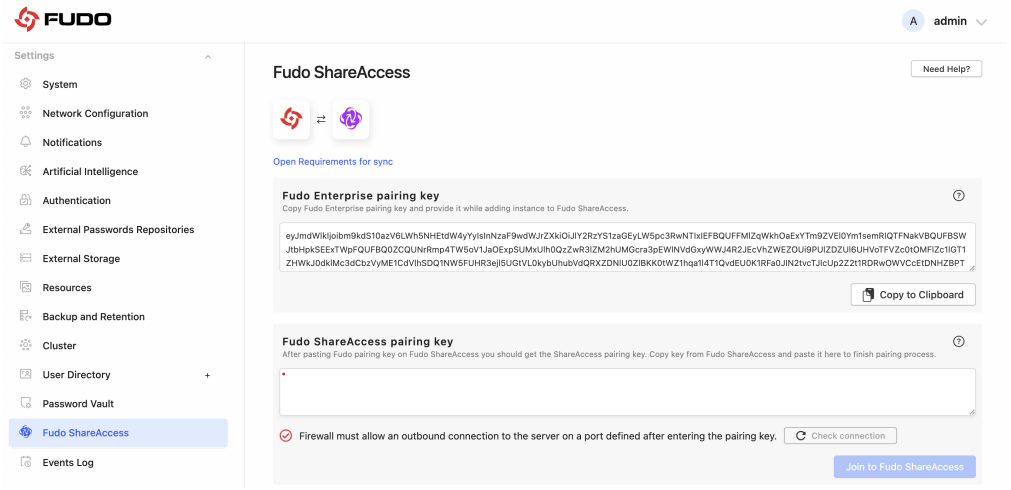
- Select *Settings* > *Fudo ShareAccess*.
- In the drop-down list, select the Bind IP address. This address is used as the source address for connections to Fudo ShareAccess.
- Verify that the NTP server status is OK. System time must be synchronized using NTP.
- Verify that the firewall allows outbound connections to `api.shareaccess.com` on port `443` by clicking *Check connection*.
- Verify that the firewall allows outbound connections to `acme-v02.api.letsencrypt.org` on port `443` by clicking *Check connection*.



Note

When all requirements are met and both outbound connections are verified, the pairing key fields will be displayed and you can continue with the pairing process.

5. Copy the *Pairing Key* from Fudo Enterprise:
   - Click *Copy to Clipboard* to copy the *Fudo Enterprise pairing key*.

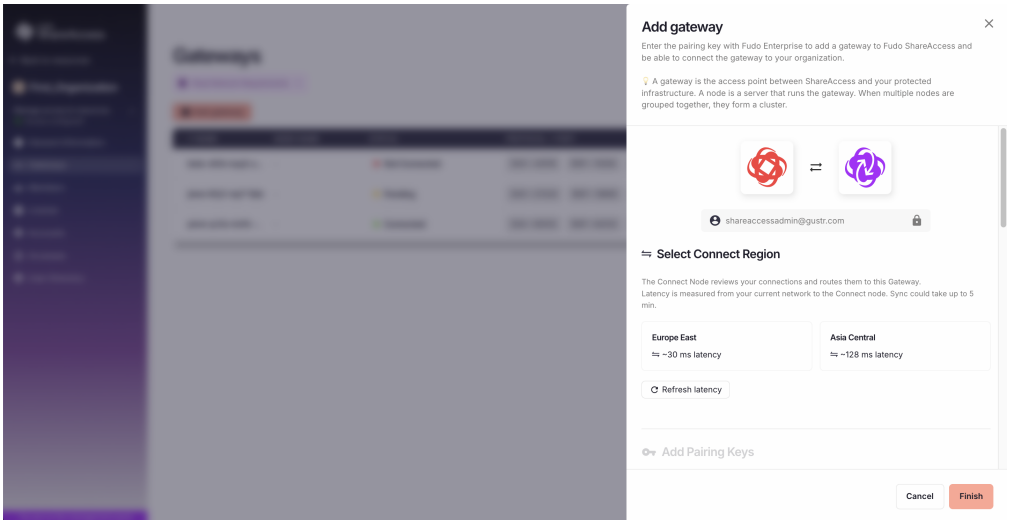


Note

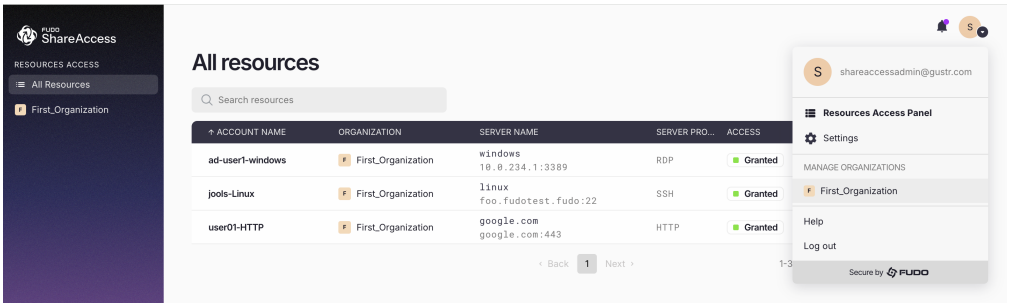
> After your first login and selecting the **Give Access** workflow and the Fudo Security **product** used by your company, you will be automatically redirected to the *Add Gateway* window.

6. Add **Gateway** in Fudo ShareAccess:

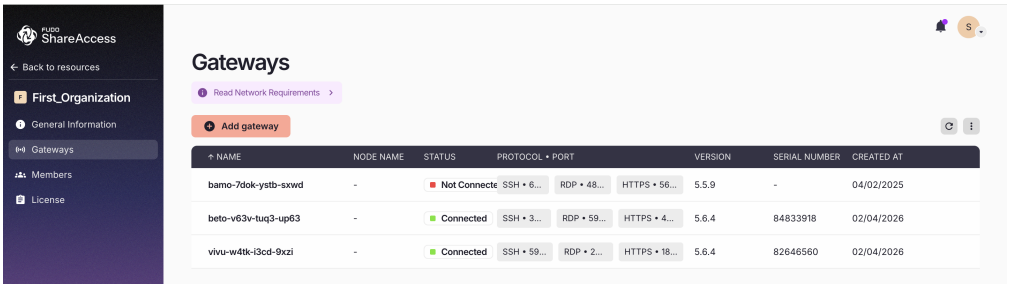
   - Select *Connect Region*. The Connect Node reviews your connections and routes them to this Gateway. Latency is measured from your current network to the Connect node. Sync could take up to 5 min.
     - *Europe East* – ~30 ms latency,
     - *Asia Central* – ~128 ms latency.
   - Click *Refresh latency* to update the measured latency values.



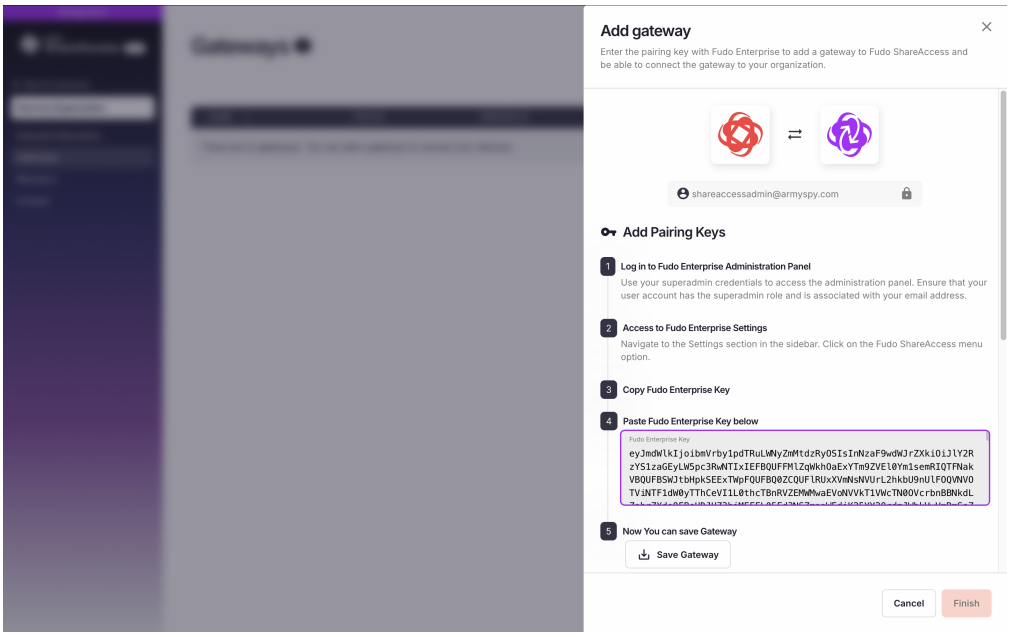
   - Log in to Fudo ShareAccess, expand the **User Drop-down** menu in the upper-right corner and select *Manage organizations* > *Your Organization Name* to access the organization settings.



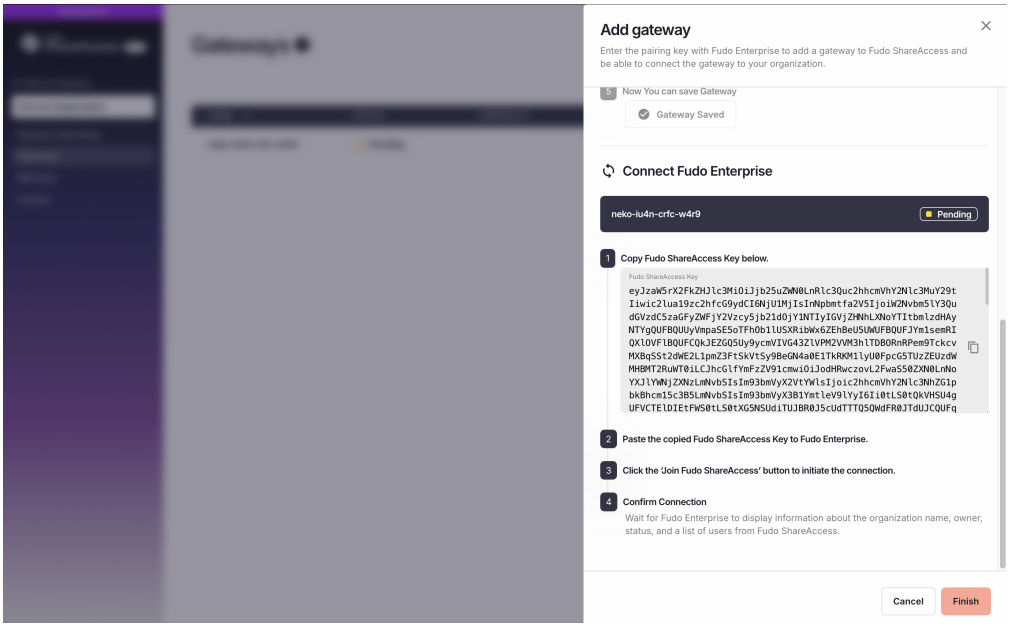
   - In the left-hand menu, select *Gateways*.
   - Click *+ Add Gateway*.



- Paste the *Fudo Enterprise pairing key* that was copied earlier in the manual.
- Click *Save Gateway*.



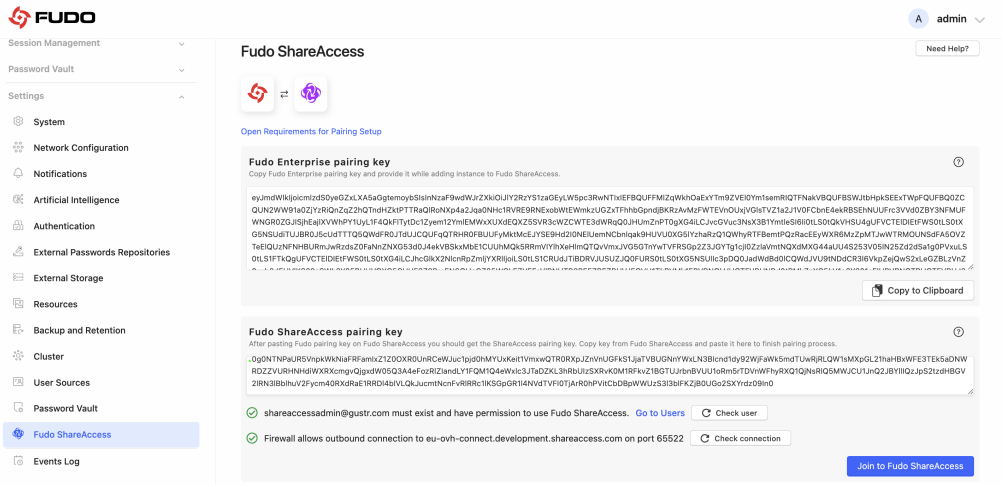
- Next, copy the *Fudo Pairing Key* displayed below.



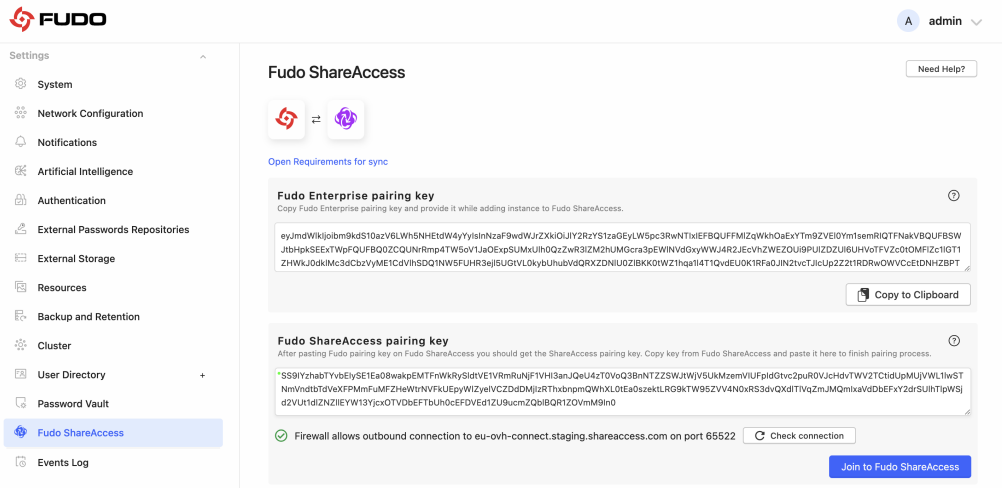
7. Go back to Fudo Enterprise Admin Panel and paste the *Fudo Pairing Key* in the *ShareAccess pairing key* field.

8. Click *Check user* to verify that the user with Fudo ShareAccess privileges, created in the previous steps, exists and has permission to use Fudo ShareAccess.

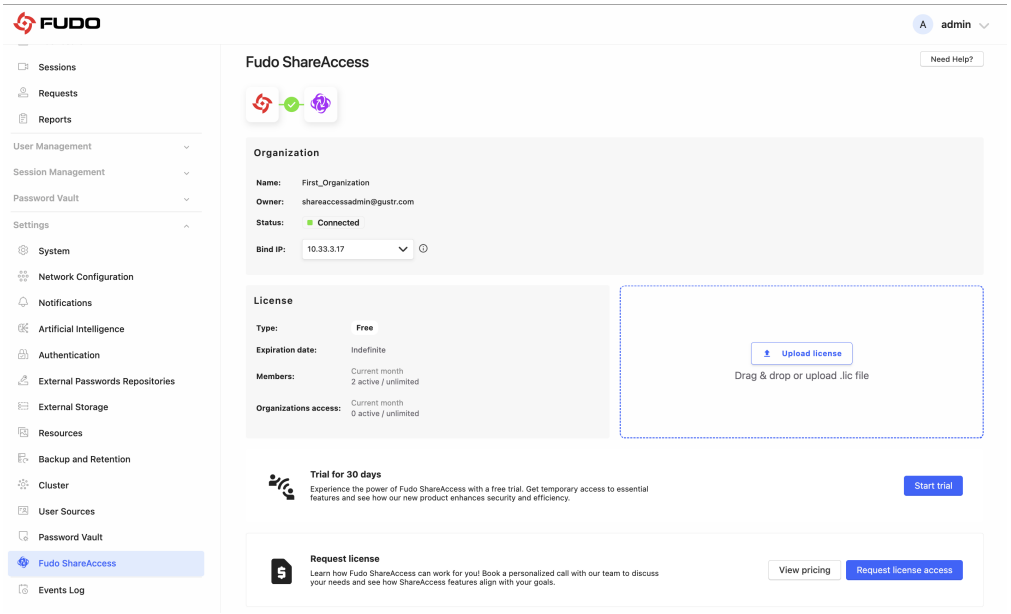
9. Check if firewall allows outbound connection to `eu-ovh-connect.shareaccess.com` on port `65522` by clicking *Check connection*.



10. Click *Join to Fudo shareaccess*.



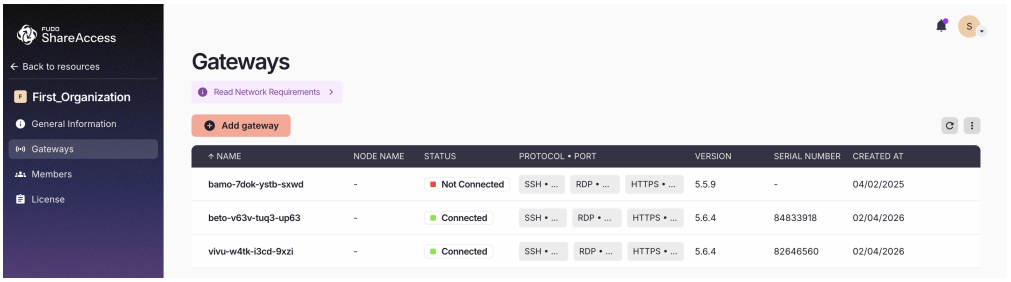
11. Wait until the Fudo Enterprise instance displays information about the organization name, owner, status of the connection, license, and a list of users from Fudo ShareAccess.



Note

This process may take up to a minute. If the information does not appear, please contact support at support@shareaccess.com.

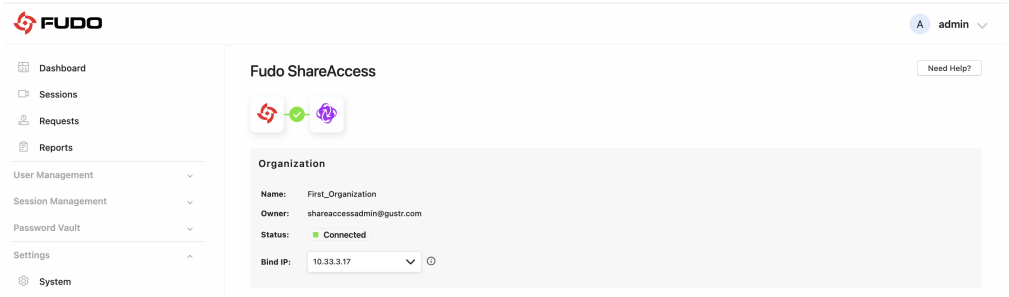
12. Go back to Fudo ShareAccess and click Finish.
13. After successful pairing, the Fudo Unique Identifier will be displayed on the Gateways list.



17.2.1 Troubleshooting the connection

If the connection between Fudo Enterprise and Fudo ShareAccess is not working as expected, you can diagnose and resolve the most common issues directly from the Fudo Enterprise Admin Panel, without contacting support.

1. Select Settings > Fudo ShareAccess.
2. In the upper-right corner, click Need Help?.



The *Need Help?* panel offers the following actions:

- **Restart Tunnels** – restarts the SSH tunnel used to establish connections. This action does not affect the configuration or stored data and is recommended as the first troubleshooting step. Outbound firewall access to `eu-ovh-connect.shareaccess.com` must be allowed. The panel displays the current tunnel status and a *Go to Logs* link. Click Restart tunnels to restart the tunnel.

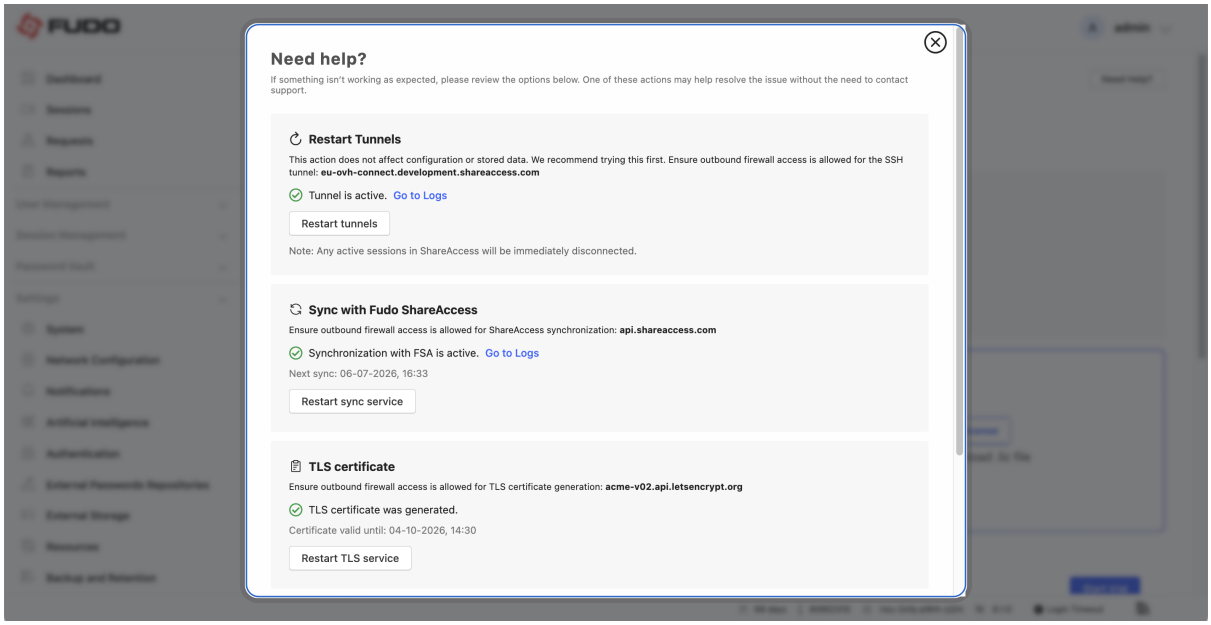
Note

Any active sessions in Fudo ShareAccess will be immediately disconnected.

- **Sync with Fudo ShareAccess** – restarts synchronization with Fudo ShareAccess. Outbound firewall access to `api.shareaccess.com` must be allowed. The panel displays the synchronization status, the time of the next synchronization, and a *Go to Logs* link. Click Restart sync service to restart synchronization.
- **TLS certificate** – restarts TLS certificate generation and renewal. Outbound firewall access to `acme-v02.api.letsencrypt.org` must be allowed. The panel displays the certificate status and its validity date. Click Restart TLS service to restart the service.
- **Contact Fudo Support** – if you need further assistance, click Open support portal to reach out to the support team.
- **Force Unpair** – click the expand arrow to reveal the Unpair Fudo ShareAccess button. This action removes the entire configuration and requires you to set everything up again from scratch. Your license and account remain intact.

Warning

Use *Force Unpair* only as a last resort. It removes the complete pairing configuration between Fudo Enterprise and Fudo ShareAccess.



Related topics:

- *Manage Fudo ShareAccess Members*
- *Manage Access to Resources*

17.3 ShareAccess License

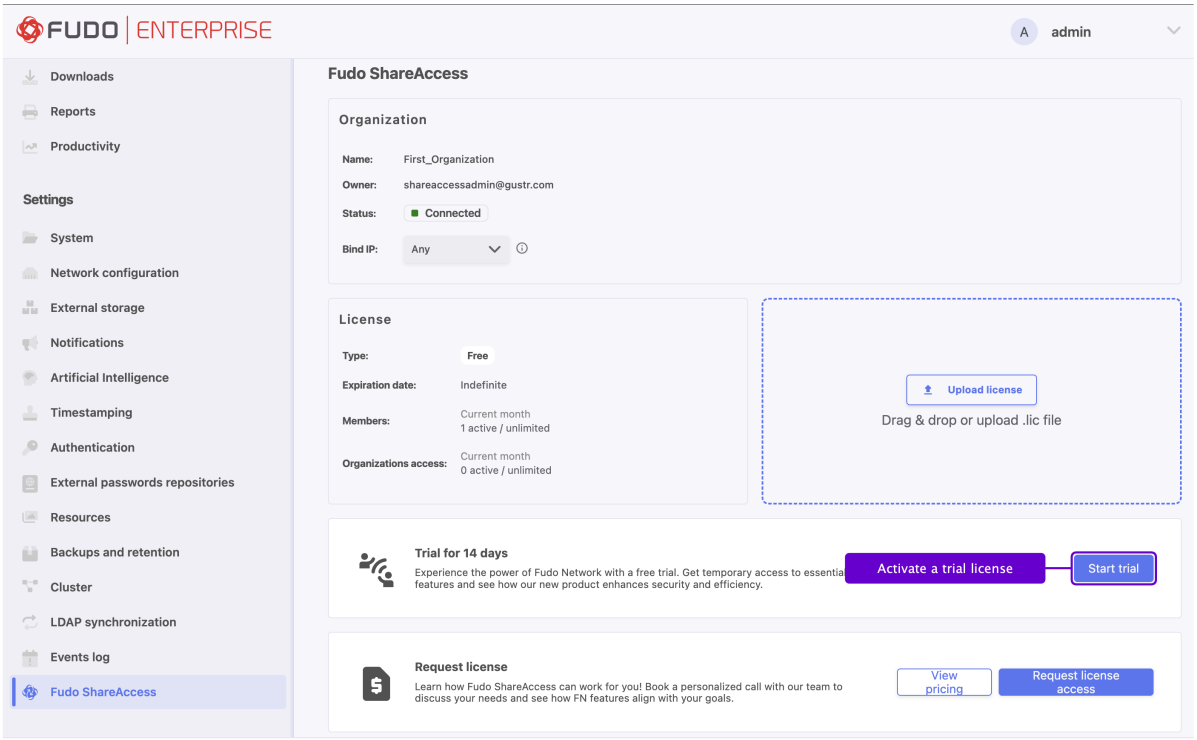
License management is streamlined and accessible exclusively within the Fudo Enterprise platform, to users with a role that has permissions to manage Fudo ShareAccess.

17.3.1 Trial License Activation

The trial license is available only once per organization. This type of license operates under the same rules as a standard license, offering a realistic experience of the system's capabilities.

To enable the trial version of the Fudo ShareAccess:

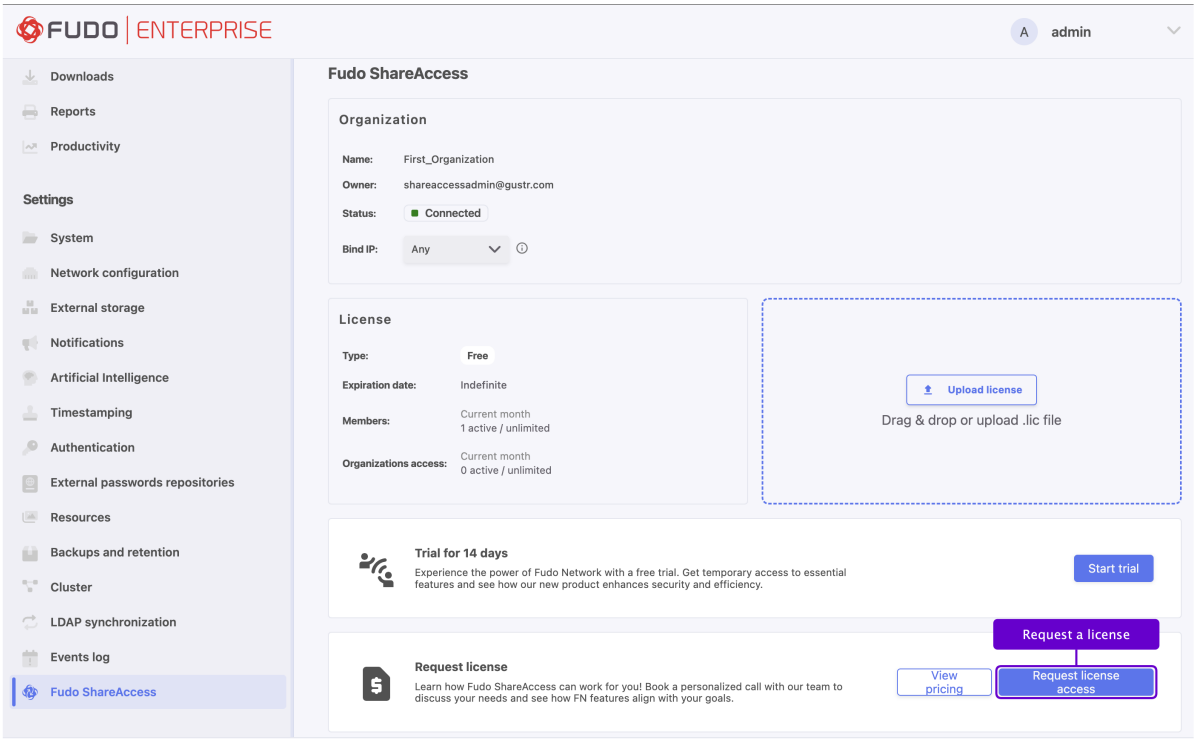
1. Log in to the Admin Panel of the Fudo Enterprise instance.
2. Select Settings > Fudo ShareAccess.
3. In the *License* section click the Start trial button.



17.3.2 Requesting a License

To request a license for the Fudo ShareAccess:

1. Log in to the Admin Panel of the Fudo Enterprise instance.
2. Select Settings > Fudo ShareAccess.
3. In the *License* section click the Request license access button.
4. Fill out the quote form to get in touch with Fudo Security.



17.3.3 Uploading License File

After receiving the license file you need to upload it in the Fudo Enterprise instance:

1. Log in to the Admin Panel of the Fudo Enterprise instance.
2. Select Settings > Fudo ShareAccess.
3. In the *License* section, click the Upload license button or drag the license file directly into the *Drag and Drop* field.
4. The license file will be automatically processed, and the license will be loaded accordingly.

Related topics:

- *Pairing Fudo Enterprise with Fudo Shareaccess*
- *Manage Fudo ShareAccess Members*
- *Manage Access to Resources*

17.4 Manage Fudo ShareAccess Members

17.4.1 Inviting Members

You can invite users to access organization resources via Fudo ShareAccess or to become an organization members.

Inviting a user establishes a connection between Fudo Enterprise user and Fudo ShareAccess user, which is necessary to grant access to resources.

Note

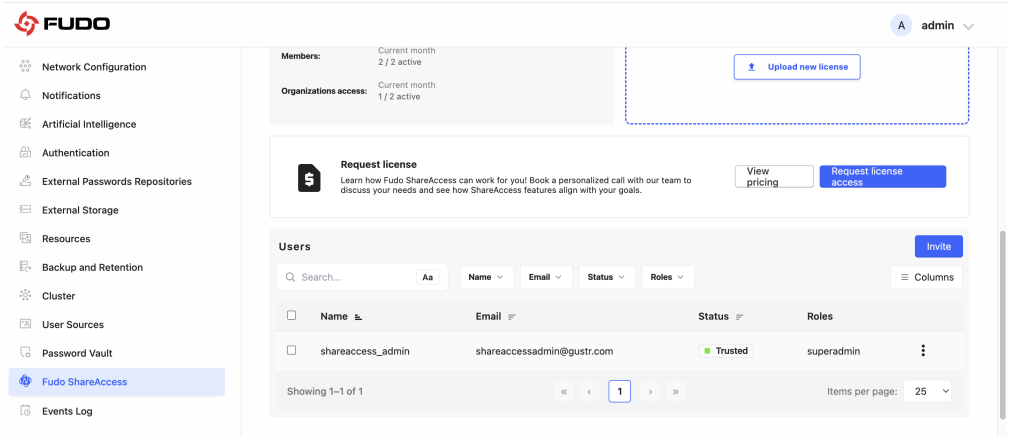
- You can manage Fudo ShareAccess users directly from within the Fudo ShareAccess or the Fudo Enterprise.
- If you are using Fudo Enterprise, inviting users through it is more convenient for management purposes. Users invited directly via Fudo ShareAccess 1.0 will not be created in Fudo Enterprise.

Note

Starting with version 6.1.2, users imported from an *Active Directory* or *LDAP* service can also be invited to Fudo ShareAccess and granted the *Trusted* status. The Fudo ShareAccess identity is stored as a separate *ShareAccess Key* authentication method, so it is no longer overwritten by directory synchronization and no longer conflicts with the *Synchronize with LDAP* option. For more information, refer to the *Users Synchronization - User Directory* section.

To add users from Fudo Enterprise and connect them with Fudo ShareAccess follow below steps:

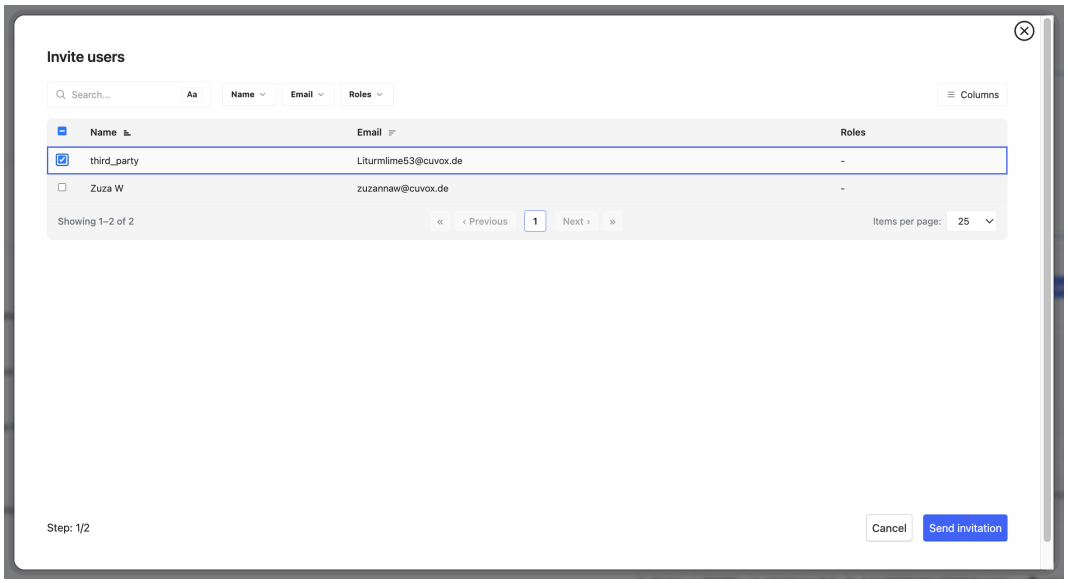
1. Create user with email that will be used as email for Fudo ShareAccess access:
    - Select *User Management* > *Users* and then click *+ Add user*.
    - Enter user name.
    - From the *Role* drop-down list select desired role.
    - In the *User Data* tab, in the *User info* field enter:
        - user's full name (required),
        - user's email address that will be used as email for Fudo ShareAccess access (required),
        - user's organizational unit,
        - user's phone number.
    - Click *Save*.
    - Go back to the *Settings* tab, and in the *Authentication* section select desired authentication type from the *Add authentication method* drop-down list. This will be used to authenticate user against Fudo Enterprise Access Gateway.
    - Click *Save and close*.
2. Select *Settings* > *Fudo ShareAccess* and click the *Invite* button.



3. In the modal window select users you want to invite from the list of available users.

Note

- Only users with a configured email address can be invited to Fudo ShareAccess.
- The email address is recorded at the moment of invitation as the user's Fudo ShareAccess user name and is not changed afterwards. Editing the user's email address in Fudo Enterprise (manually or through directory synchronization) does not affect the existing Fudo ShareAccess membership. This is why the *Email* column on the *Fudo ShareAccess* list can differ from the email address shown on the user's form.
- A given Fudo ShareAccess user name can be assigned to only one Fudo Enterprise user.



4. Click the *Send invitation* button.
5. Fudo ShareAccess requires a user to be *Trusted* in order to access assigned resources. In the next step, decide when to trust the invited user:
   - Click Grant access to trust the user immediately, without verifying their identity, or
   - Click I want to verify them first to verify the user after they accept the invitation.

Note

Granting access immediately means trusting the user without verifying their identity. If the invitation is intercepted, someone else could gain access. Choosing *I want to verify them first* lets you withhold access until you have compared the user's fingerprint, which confirms that the right person is joining.

6. Sending an invitation will add entries to the users list, with their status marked as *Invitation Pending* until the user clicks the email link to join the organization.

Note

Sending an invitation means the user will receive an email containing a link that allows them to either create an account and accept the invitation or simply accept the invitation if they already have an account on Fudo ShareAccess.

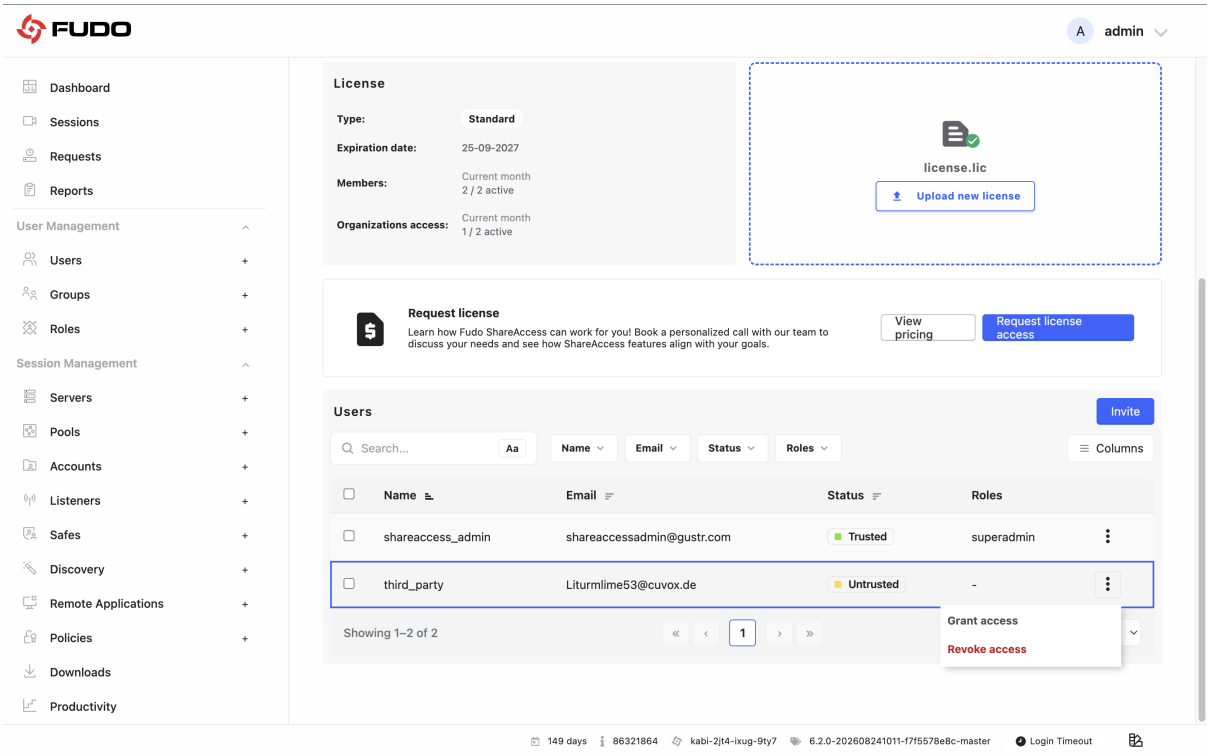
17.4.2 Verifying Members Status

User that is paired with Fudo ShareAccess can have *Trusted* or *Untrusted* status. This status defines if user can see resources in Fudo ShareAccess.

Note

The Fudo Enterprise user with a role that has permissions to manage Fudo ShareAccess can perform verification (change *Untrusted* status) only after the user has created an account in Fudo ShareAccess and accepted the invitation to join organization.

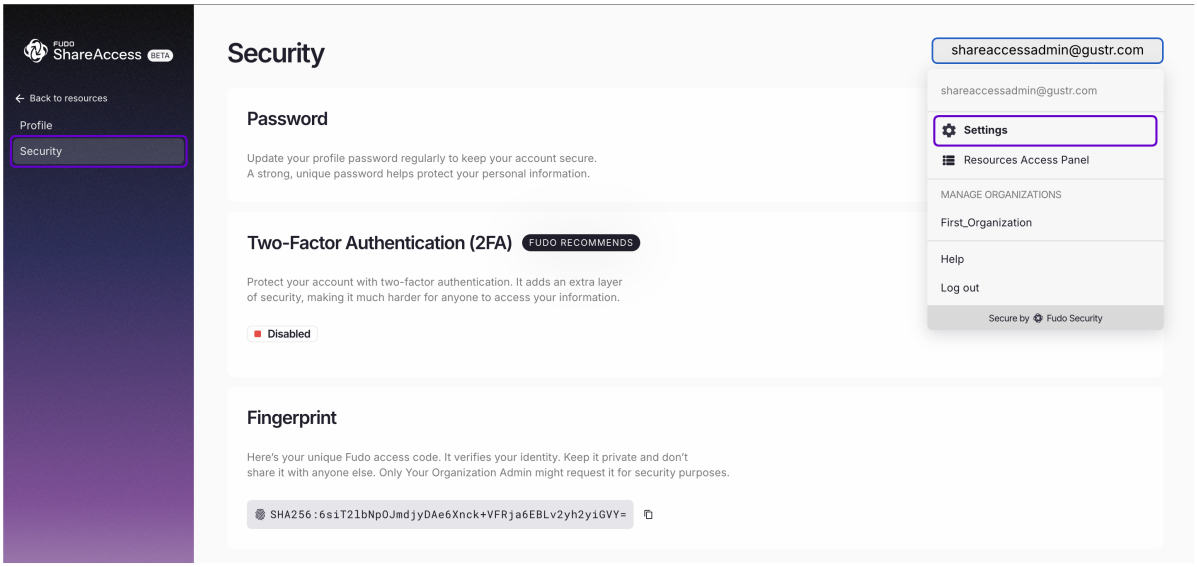
1. Select *Settings* > *Fudo ShareAccess*.
2. On the users list, find the user with the *Untrusted* status, click the three-dots icon at the end of their row and select *Grant access*.



3. In the *Establish trust* window, ask the user for the *Fingerprint Key* from their Fudo ShareAccess account and compare it with the fingerprint displayed in the window.

Note

The *Fingerprint Key* can be viewed after logging into the Fudo ShareAccess user account, selecting *Settings* from the drop-down menu in the upper-right corner and then *Security* in the left-hand menu.



4. Click *Trust user now*. The status of the user changes to *Trusted*.

Note

- There is no requirement to complete that process. It is at the Administrator's discretion whether to trust users without verification.
- Blocking the user in Fudo Enterprise will automatically disable their access to resources shared with Fudo ShareAccess.
- An administrator can also revoke a previously granted trust without disconnecting the user from Fudo ShareAccess. The *Untrust* action is available on the user's form, in the *ShareAccess Key* authentication method. For more information, refer to the *ShareAccess Key Authentication Method* section.

17.4.3 ShareAccess Key Authentication Method

The Fudo ShareAccess identity of a user is presented on the user's form as a separate authentication method named *ShareAccess Key*. This lets the administrator inspect the Fudo ShareAccess membership and manage it without leaving the *Users* tab.

Note

- The *ShareAccess Key* method appears automatically after the user has been invited to Fudo ShareAccess and disappears when their access is revoked. It cannot be added manually and is therefore not available on the *Add authentication method* drop-down list.
- The *ShareAccess Key* method is not used to log in to Fudo Enterprise and is not taken into account in the order of authentication methods. Fudo ShareAccess uses it to verify the signature of the requests sent by the user.

To review a user's Fudo ShareAccess identity, proceed as follows.

1. Select *User Management* > *Users* and select the user from the list.

2. Go to the *Settings* tab and find the *ShareAccess Key* entry in the *Authentication* section, in the *Methods* field.

The entry displays the following information:

- *Username* - the user's Fudo ShareAccess user name, recorded at the moment of invitation.
- *Fingerprint* - the SHA256 fingerprint of the user's Fudo ShareAccess key pair. The fingerprint is displayed only after the user has accepted the invitation and their keys have been transferred to Fudo Enterprise.

The following actions are available, depending on the state of the Fudo ShareAccess membership:

Action	Availability	Result
Trust	the user has accepted the invitation and is not trusted yet	Opens the fingerprint comparison window and grants the *Trusted* status. The user gains access to the resources shared with them.
Untrust	the user has the *Trusted* status	Revokes the *Trusted* status. The user remains a member of the organization but loses access to the shared resources until trust is granted again.
Delete	always	Ends the Fudo ShareAccess membership of the user. It is the equivalent of the *Revoke access* action available on the *Fudo ShareAccess* list.

Note

Before the user accepts the invitation, only the *Delete* action is available - there are no keys to verify yet, so trust cannot be granted.

17.4.4 Creating an Account Without an Invitation

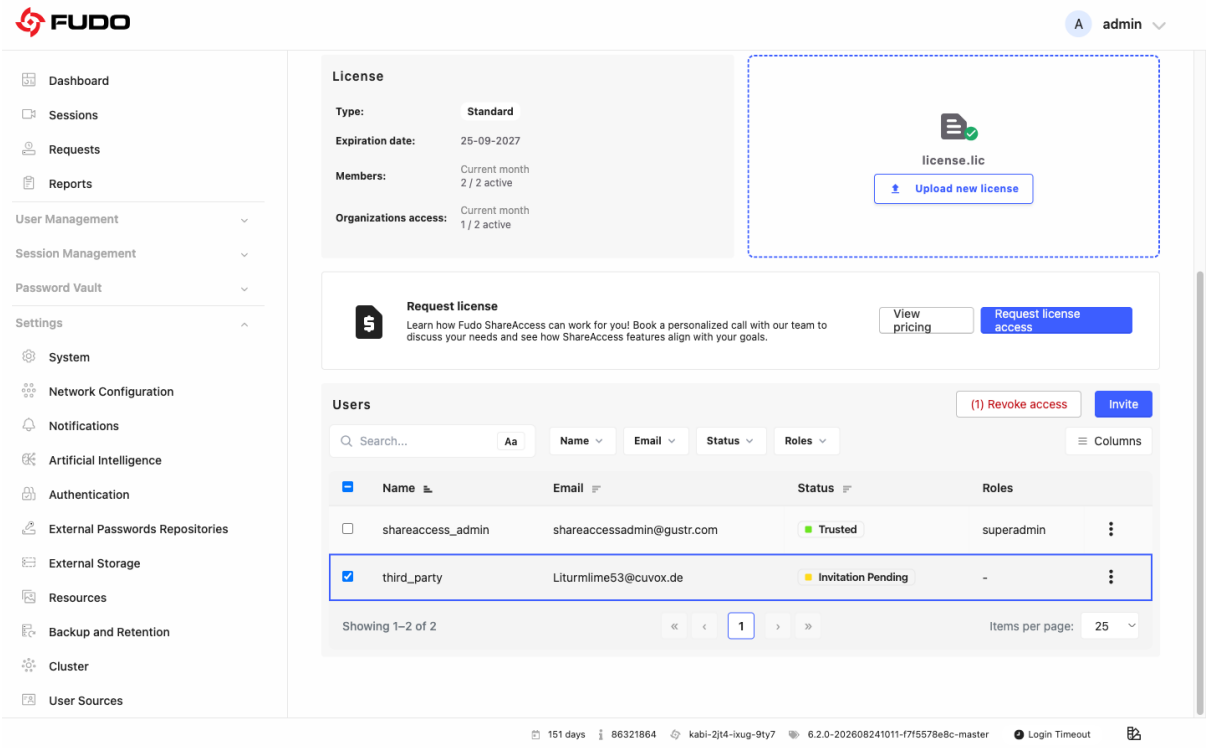
It is possible for user to create an account without an invitation. If the user's email domain matches an existing organization's domain in Fudo ShareAccess, they will automatically be assigned to that organization. By default, the account will be inactive, and the user will not have access to Fudo ShareAccess. The organization owner will receive an email notification about the new user, including a link to activate the user's account.

For more information please follow the ShareAccess documentation.

17.4.5 Revoking Members Status

The administrator has the ability to revoke access to Fudo ShareAccess. This means the user will be disconnected from their Fudo ShareAccess account and will no longer be able to work with Fudo ShareAccess. To carry out this procedure:

1. Select *Settings* > *Fudo ShareAccess*.
2. Revoke the access in one of the following ways:
   - on the users list, click the three-dots icon at the end of the user's row and select *Revoke access*, or
   - select the check boxes of the users you want to disconnect and click the *Revoke access* button above the list. The button shows the number of the selected users.
3. Once the access is revoked, these users are removed from the list.



Note

Access can also be revoked from the user's form by deleting the *ShareAccess Key* authentication method. The result is the same as using the *Revoke access* action. For more information, refer to the *ShareAccess Key Authentication Method* section.

17.4.6 Deleting Members

There is no possibility to remove user from Organization or Fudo ShareAccess. The only possibility is to set account as *Inactive*. For more information please follow the ShareAccess documentation.

Related topics:

- *Data Model*
- *Pairing Fudo Enterprise with Fudo Shareaccess*
- *Manage Access to Resources*

17.5 Manage Access to Resources

Resource access via Fudo ShareAccess is administered in Fudo Enterprise through its objects, including Users, Servers, Accounts, and Safes. This section explains the fundamental workflow for resource management.

Note

In Fudo ShareAccess, visibility of configurations depends on specific conditions. Below is a summary of the prerequisites and conditions that must be met for configurations to be visible:

- **User Requirements:** The user must be paired with or invited to Fudo ShareAccess.
- **Supported Protocols:** The following protocols are available for use within Fudo ShareAccess:
  - RDP
  - SSH
  - VNC
- **Account Types:** Only the following account types are supported:
  - Regular accounts with properly configured credentials
  - Forward accounts
- **Safe:** The server must have the following options enabled:
  - Fudo ShareAccess enabled
  - OTP enabled
  - Webclient enabled

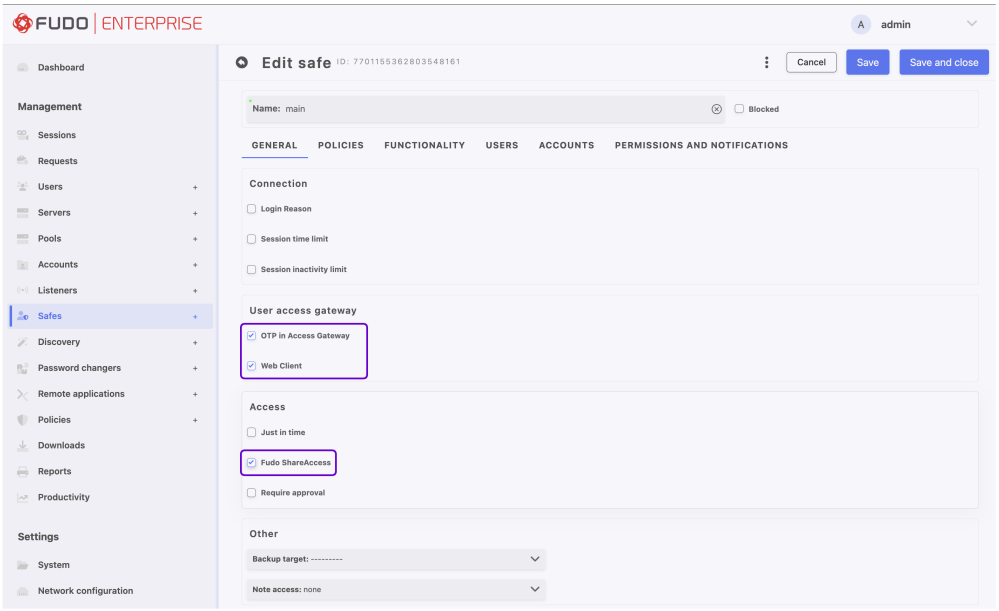
*Listener is not required object for giving access to resources to Fudo ShareAccess.

To grant a user access to a specific server via Fudo ShareAccess, follow the steps below:

1. Create user and invite them to join Fudo ShareAccess. Refer to the *Manage Fudo ShareAccess Members* section for detailed instructions.
2. Create the server you want to grant access to via Fudo ShareAccess.
   - Select *Management* > *Servers* and then click *+ Add server*.
   - Enter server's unique name.
   - In the *Settings* section on the list of available protocols select `RDP` or `SSH`.
   - From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.
   - In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.
   - Click *Save and close*.
3. Create account which points to that server:

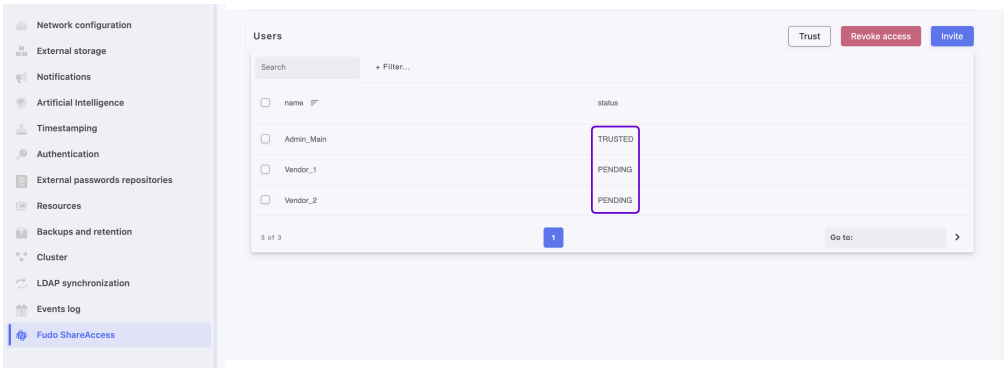
- Select *Management* > *Accounts* and then click + *Add account*.
- Define object's name.
- In the *Settings* tab, in the *Type* field, press the *REGULAR* button.
- In the *Target* section, click the *Server* button to assign the account to a specific server, then choose the server created in the previous step from the *Server* drop-down list.
- In the *Credentials* section, enter the login for the account on the server.
- In the *Replace secret with* section, click the button for the desired option, such as *Password*, and enter the account password in the *Secret* field.
- Click *Save and close*.

4. Create safe:
   - Select *Management* > *Safes* and then click + *Add safe*.
   - Enter object's name.
   - Click *Save* to save the object and proceed with further configuration.
   - In the *General* tab:
     - The *OTP in Access Gateway* option is enabled by default and is responsible for generating OTP in the User Access Gateway (required).
     - Select *Web Client* option to allow connecting to the session using the built-in browser client (required).
     - Select *Fudo ShareAccess* option to enable the Safe for use with Fudo ShareAccess (required).
     - Select *Just in time* option and provide a number of the voters. This feature allows defining and scheduling the time when a user is allowed to access specific resources for a set period of time. The user sends requests via the Access Gateway, and the voters accept or reject them on in the Admin Panel. Read more about the Just-In-Time feature in a *Access Requests* section (optional).



- Click *Save*.

5. Add created user and account to safe:
    - Go to the *Users* tab to assign users allowed to access accounts assigned to this safe.
    - Click *Manage users*.
    - Mark the checkbox in front of the users' names to enable their server access through the monitored safe.
    - Click *Save* to close the modal window.
    - Select *Accounts* tab to add *accounts* accessible through this safe.
    - Click *Manage accounts*.
    - Mark the checkbox in front of the accounts' names to add it.
    - Click *Save* to close the modal window.
    - Click *Save* to close the modal window.
6. Ensure the user is trusted:
    - Select *Settings* > *Fudo ShareAccess*.
    - Find the desired user in the members list and verify that their status is *TRUSTED*.



7. After completing this guide, the user assigned to the safe can now log in to Fudo ShareAccess and access the server linked to the safe. For more information please follow the ShareAccess documentation.

Related topics:

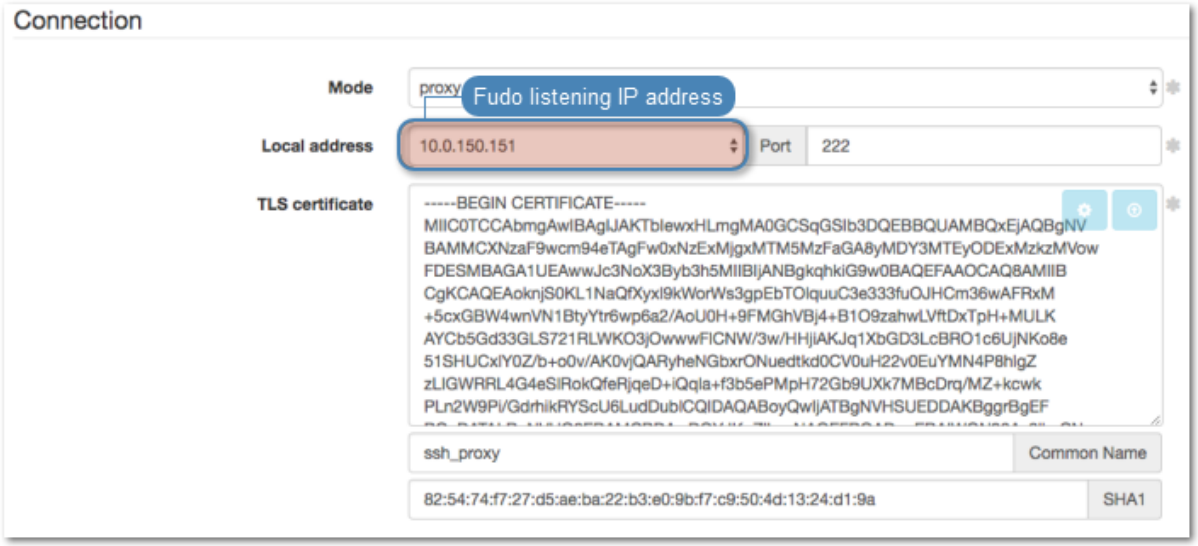
- *Manage Fudo ShareAccess Members*
- *Require Approval for Access*
- *Access Requests*

CHAPTER 18

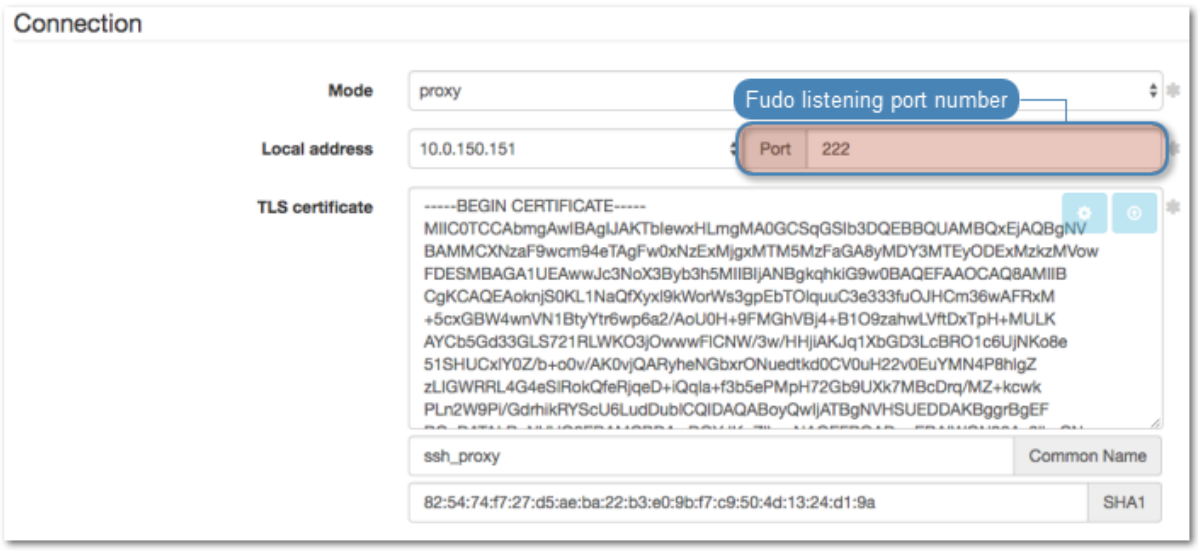
Client Applications

18.1 PuTTY

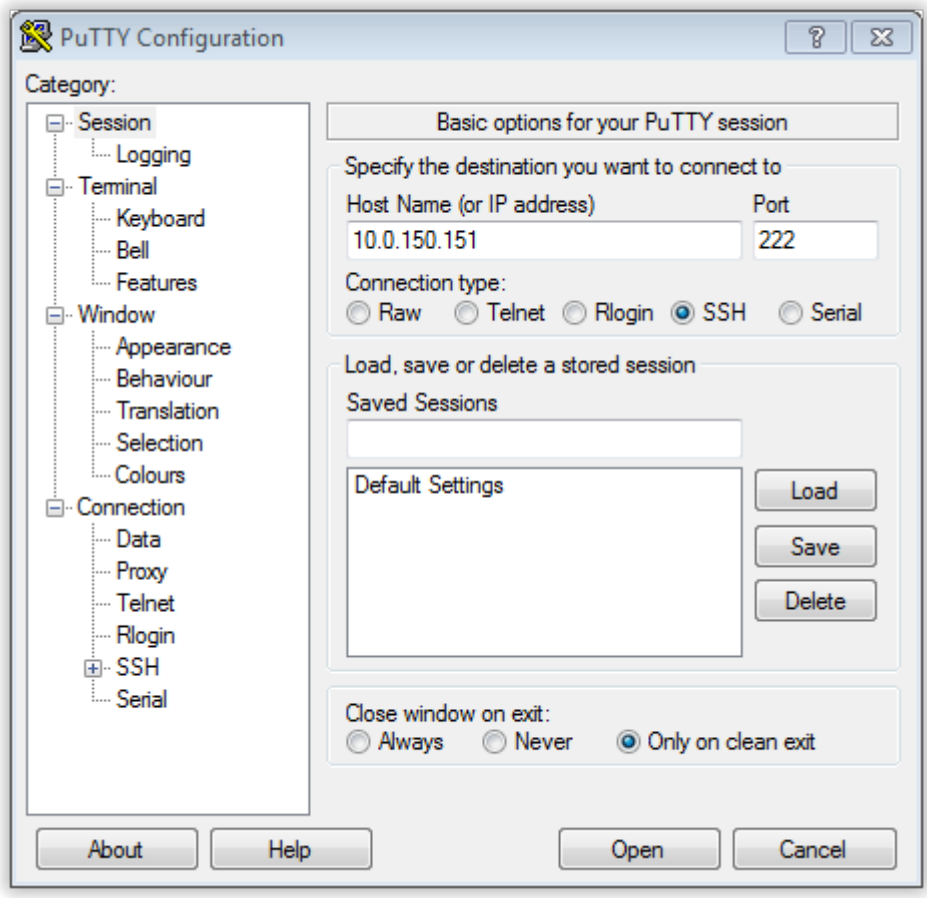
1. Download and launch PuTTY.
2. In the *Host Name (or IP address)* field, enter IP address defined in the listener.



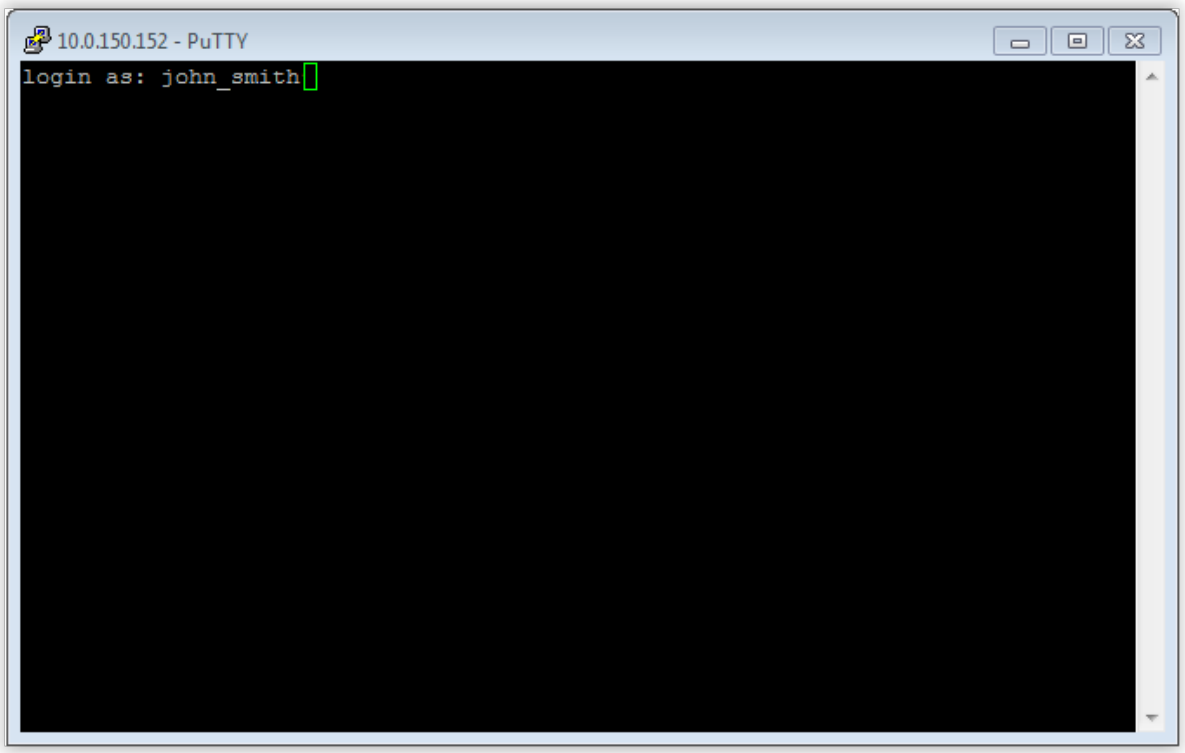
3. In the *Port number* field, enter port number defined in the listener.



4. Select the `SSH` connection type.



5. Click *Open*.
6. Enter username.



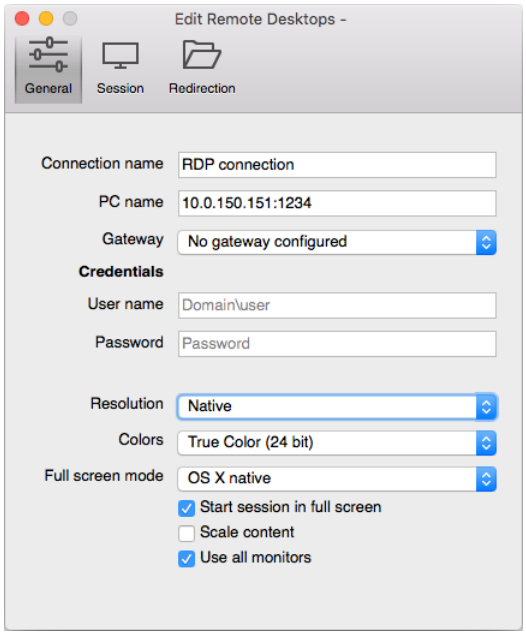
7. Enter password.

Related topics:

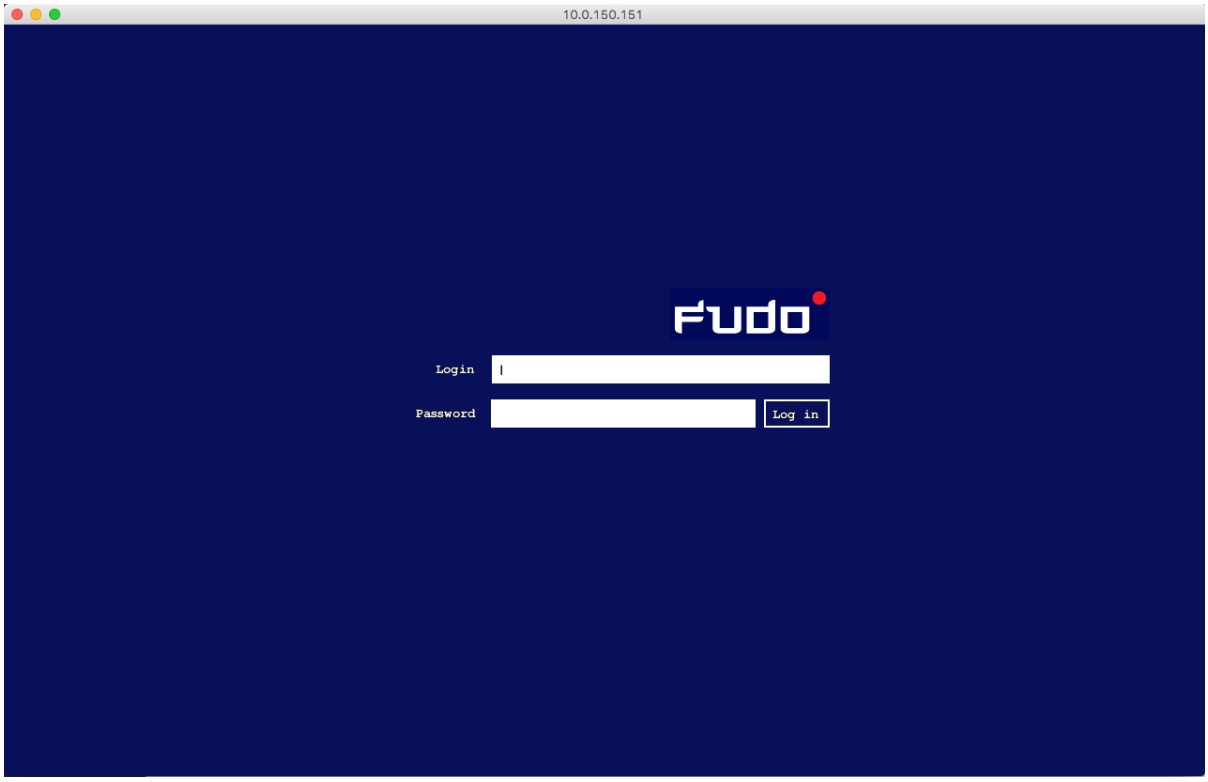
- *SSH*
- *Creating an SSH Server*
- *Setting up the SSH Listener*

18.2 Microsoft Remote Desktop

1. Launch *Microsoft Remote Desktop*.
2. Enter connection name.
3. Provide destination host IP address and RDP service port number in the *PC name* field as defined in the listener object.

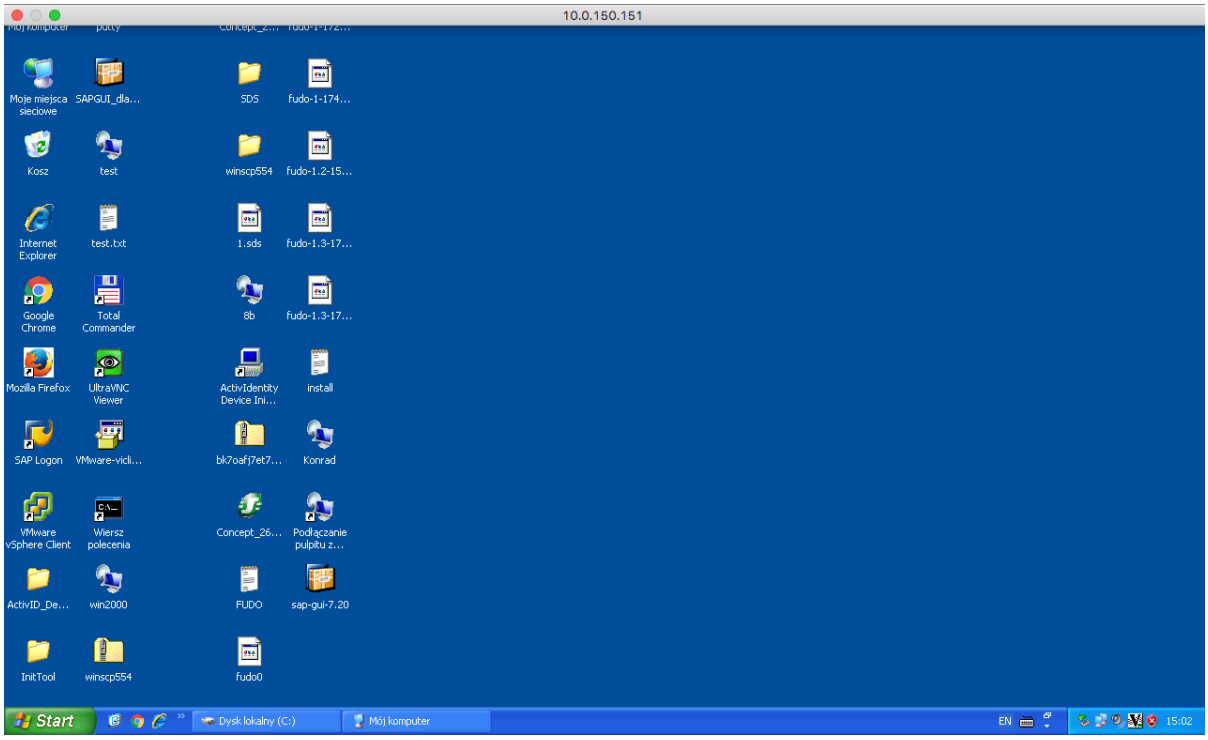


3. Enter user login and password and press the [Enter] keyboard key.



Note

Fudo Enterprise enables using custom login, no access and session termination screens for RDP and VNC connections. For more information on user defined images for graphical remote sessions, refer to the *Resources* topic.

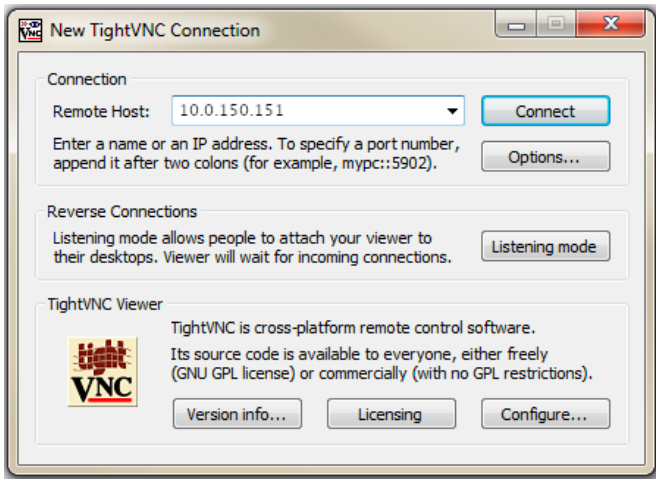


Related topics:

- *RDP*
- *Creating an RDP Server*
- *Setting up the RDP Listener*

18.3 TightVNC Viewer

1. Launch *TightVNC Viewer*.
2. Enter IP address in the server address field as defined in the created VNC listener object (for more information refer to the *Quick start - VNC* topic).



3. Enter username and password and press the enter key.

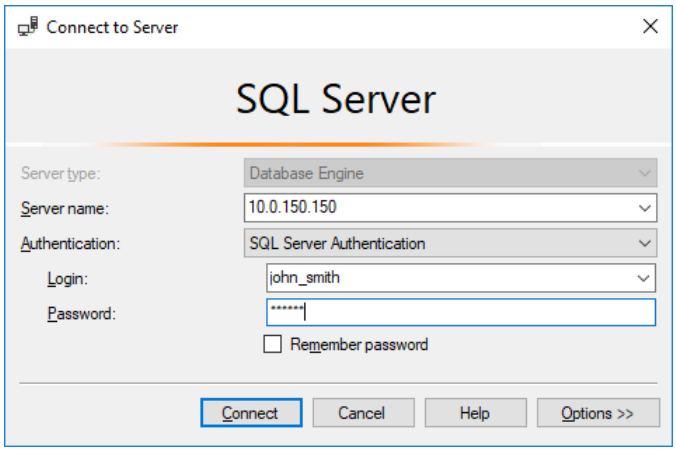
Related topics:

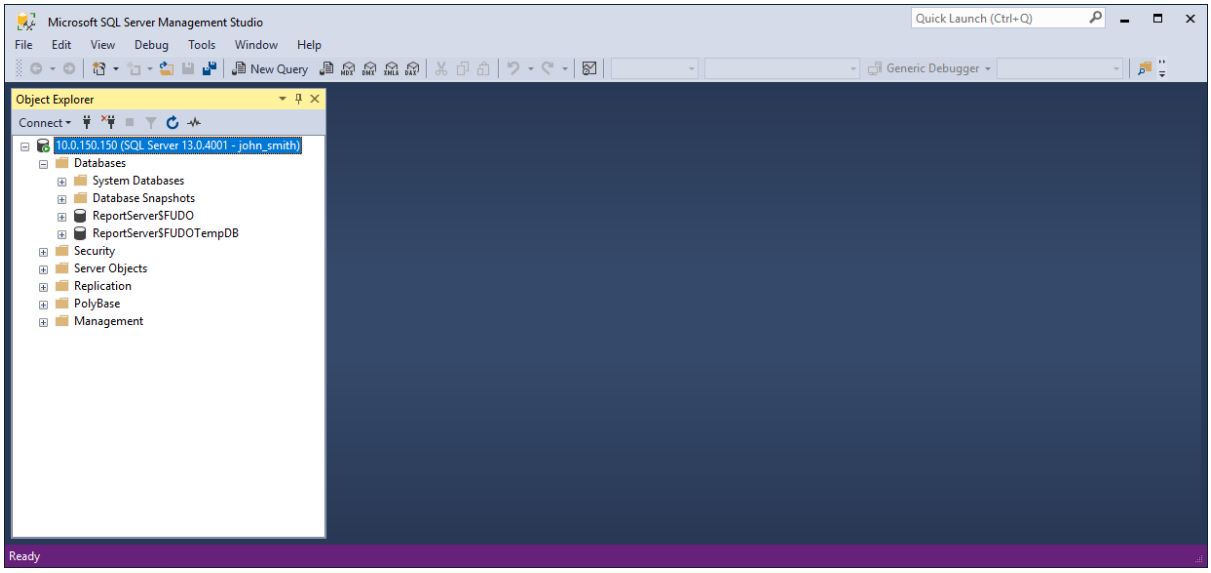
- *VNC*

- *Creating a VNC Server*
- *Setting up the VNC Listener*

18.4 SQL Server Management Studio

1. Start *SQL Server Management Studio*.
2. Enter IP address as defined in the listener object.
3. From the *Authentication* drop-down list, select *SQL Server Authentication*.
4. Enter user login and password.
5. Click *Connect*.





Related topics:

- *MS SQL*
- *Creating a MS SQL Server*
- *Setting up the MS SQL Listener*

CHAPTER 19

Troubleshooting

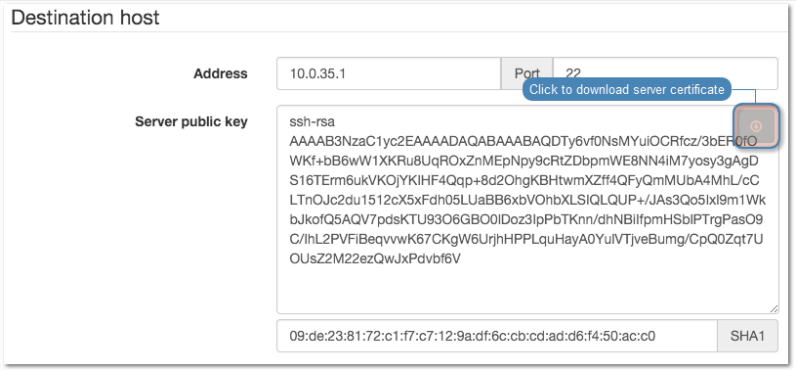
19.1 Booting Up

Problem	Symptoms and solution
Fudo Enterprise does not boot up	• Make sure that both power supplies are connected to power outlets. Not connecting both power supplies will result in sound alarm. • Make sure that encryption key is properly connected. • In case the problem is a result of unsuccessful system update, wait a few minutes. During that time, Fudo Enterprise will detect the problem and will restore previous system revision.

19.2 Connecting to Servers

Problem	Symptoms and solution
Cannot connect to server	**Symptoms:** • User cannot log in. • Events log entry: *Authentication failed: Invalid username kowalski or password.*
	Solution: • Verify that user definition exists in Fudo Enterprise database. • Make the login credentials are correct. • Make sure that the client software does not have outdated credentials stored. • Check if the user has a domain defined and make sure it is provided when attempting to log in. • If there are two users with the same login, one of which has the domain configured the same as the *default domain*, and the other does not have the domain defined, Fudo Enterprise will report authentication problem as it cannot determine which user is trying to connect.
	Symptoms: events log entry: *Unable to establish connection to server zbigniew (10.0.35.53:3399).*
	Cause: incorrect server configuration.
	Solution: • Verify that the server in question is properly configured (IP address, port number). • Check if the server is reachable from Fudo Enterprise: 1. Log in to Fudo Enterprise administration panel. 2. Select *Settings* > *System*, *Diagnostics* tab. 3. Enter server address in the *Ping* section and execute command and test host's availability. • Check if the server is reachable on given port number: 1. Log in to Fudo Enterprise administration panel. 2. Select *Settings* > *System*, *Diagnostics* tab. 3. Enter server address along with the port number in the *Netcat* section and execute command.
	Symptoms: Message in client software: *Cannot establish new connection because the capacity of the filesystem has been reached.*
	Cause: Storage usage has reached 90%.
	Solution: *Delete sessions* to free up storage space.

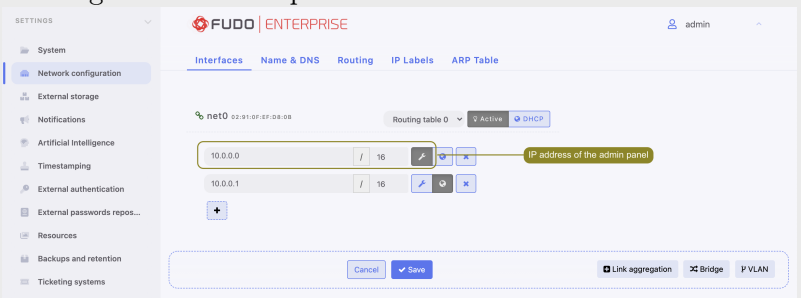
Problem	Symptoms and solution
When logging in not all of the users see the Fudo Enterprise logon screen.	**Cause:** • Credentials stored in RDP client result in users being automatically logged in to remote host. • Credentials stored in RDP client, user is successfully authenticated against credentials stored so the Fudo Enterprise logon screen is not displayed. Next, Fudo Enterprise forwards user credentials to target server but they are no longer valid which results in Windows gina being displayed.
	Symptoms: • Client software message: *Connection closed by remote host.* • Events log entry: *Failed to authenticate against the server as user root using password.*
	Cause: incorrect login credentials.
	Solution: provide correct login credentials in server configuration.
	Symptoms: • RDP client message: *Connection refused.* • SSH client message: *ssh: connect to host 10.0.1.111 port 10011: Connection refused*
	Cause: server has been blocked.
	Solution: log in to Fudo Enterprise administration panel and unblock the server.

Problem	Symptoms and solution
Connection is terminated	**Symptoms:** • User tries to log in to server monitored by Fudo Enterprise, after entering username and password session is immediately terminated. • Events log entry: *TLS certificate verification failed.*
	Solution:
	Download new target host certificate in the *Target host* section.
	
	Symptoms: • After entering username and password the connection is terminated. • Events log entry: *RDP connection error.*
	Solution: check if in the *General* tab in TCP-Rdp properties, the *Encryption level* option is not set to `FIPS Compliant`.
Cannot connect to server	**Symptoms:** • Cannot log in to server with error message *User user0 not allowed to connect to server.* • Events log entry: *Authentication failed: User user0 not allowed to connect to server.*
	Cause: user is not assigned to proper connection.
	Solution: add user to appropriate connection object.

Problem	Symptoms and solution
	Symptoms: • After entering username and password, the screen freezes. • Events log entry *Terminating session: User user0 (id=8483885321111147010) is blocked.*
	Cause: user is blocked.
	Solution: log in to Fudo Enterprise administration panel and unblock the user in question.
User has to provide login credentials twice	**Symptoms:** user connecting over RDP protocol enters login credentials and immediately afterwards is asked again for the same login information.
	Cause: server is a part of an infrastructure managed by connections broker which has detected an active user's session on another server.
	Symptoms: user connecting over SSH protocol enters login credentials and immediately afterwards is asked again for login information.
	Cause: in *connection* object options for login and password substitution are enabled but the input fields are left blank which results in two fold authentication - first time against Fudo Enterprise and second time against the target host.
Cannot connect to server over RDP protocol	**Symptoms:** • User connecting over RDP is disconnected a moment after establishing connection. • Events log entry: *RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.*
	Cause: connection is redirected to a host which does not listen on port number 3389.
	Solution: configure server in question so it accepts user connections on port number 3389.
	Symptoms: • Events log entry: *User user0 has no access to host 192.168.0.1:3389*
	Cause: connections broker determines an existing user session on another server and redirects user to that host but it is not configured on Fudo Enterprise or the user does not have sufficient access rights to connect to given server.
	Solution: • Make sure that the server object exists. • Add user to proper *safe* object.

Problem	Symptoms and solution
Cannot connect to Telnet5250 server using PC5250 client revision 20091005 S/20111019 S	**Symptoms:** cannot establish connection to target host.
	Cause: in case of aforementioned client applications, Fudo Enterprise requires setting up additional objects to enable TCP traffic on ports number 449, 8470 and 8476.
	Soluiton: • Add Telnet TN5250 server with default port number. • Add three server objects with `TCP` protocol and following port numbers 449, 8470 and 8476. • Add `TN5250` listener, in `Proxy` mode with default port number. • Add three `TCP` listener objects, in `Proxy` mode, with port numbers 449, 8470 and 8476. • Add `regular` account, define authentication parameters and assign it to the main TN5250 server definition. • Add three `anonymous` accounts and assign each to one of supporting servers. • Add safe and assign account with corresponding listeners.

19.3 Logging to Administration Panel

Problem	Symptoms and solution
Cannot log in to administration panel	• Make sure that Fudo Enterprise IP address is correct. • Set Fudo Enterprise IP address from the console as described in the *Fudo Enterprise System documentation* in the *Network interfaces configuration* topic. • Make sure that the IP address in question has the management access option enabled. 

19.4 Session Playback

Problem	Symptoms and solution
Cannot playback exported video	**Cause:** required video codecs are missing.
	Solution: install correct video codecs.
Administrator user does not see sessions	**Symptoms:** session list does not contain expected entries.
	Cause: insufficient access rights.
	Solution: grant access rights to specific user, server and connection objects.
Cannot playback session in session player	**Symptoms:** message: `Could not find session data.`
	Cause: recording has been disabled in connection properties when given session transpired.
	Solution: enable session recording to be able to playback session material in future.

19.5 Cluster Configuration

Problem	Symptoms and solution
Data model objects are not replicated to other nodes	**Symptoms:** Objects created on a node are not copied to other cluster nodes. **Solution:** Contact technical support department.
	Symptoms: A report generated on one cluster node is not visible in the Administration Panel of the other nodes.
	Cause: The relation between the nodes has been set to **Replication** only, which covers configuration data and session metadata exclusively. Reports, logs and session material require full replication.
	Solution: Edit the node on which the reports are generated and, in the **Relations** section, change the **Database** list to **Replication with new session data** or **Replication with historical data**. To make reports visible on both nodes, define the relation in both directions. For more information, refer to the *Adding Cluster Nodes* chapter.
	Symptoms: A session recorded on one node cannot be played back on another cluster node.
	Cause: There is no relation between those nodes, or the relation is set to **Replication** only.
	Solution: Session data is replicated only between nodes with a defined relation, and only from the node where the session was recorded. Define a relation with the **Replication with new session data** option. To transfer sessions recorded before the relation was created, select **Replication with historical data**.

19.6 Trusted Timestamping

Problem	Symptoms and solution
Session are not timestamped	**Symptoms:** • System log entry: *Timestamping service communication error.*
	Reason: Timestamping host is not reachable by Fudo.
	Solution: Make sure that firewall settings allow traffic to the timestamping service server. • PWPW timestamping service IP address: `193.178.164.5` • KIR timestamping service IP address: `http://www.ts.kir.com.pl/HttpTspServer`
	Symptoms: • System log entry: *Unable to timestamp session.* • No session timestamp icon on sessions list.
	Reason: Timestamping service misconfiguration.
	Solution: Make sure that timestamping service has been *configured properly*.

19.7 File Scanning

Problem	Symptoms and solution
File transfers are refused in all safes	**Symptoms:** In rendered HTTP sessions, every upload and download is refused with the message `Transfer blocked: the scanning service is unavailable. The file was not transferred.`, also in safes where file scanning is turned off.
	Cause: The internal Fudo service that records file transfers is unavailable. A transfer that cannot be recorded is refused, whether scanning is turned on or not.
	Solution: Fudo restarts the service automatically. Ask the user to close the session and start a new one. If the message also appears in new sessions, contact technical support.
Files are blocked in safes with file scanning enabled	**Symptoms:** Transfers are blocked and the *Files* tab of the session shows *File could not be scanned* with the *Engine unreachable* reason.
	Cause: Fudo cannot connect to any of the configured providers.
	Solution: In *Settings* > *System* > *General* > *File scanning*, check the status of the providers and use *Test connection*. Make sure that the firewall allows traffic from Fudo to the ICAP port of the provider (`1344` by default). For details, refer to the *File Scanning in Rendered HTTP Sessions* topic.
The provider connection test fails	**Symptoms:** *Test connection* shows *Provider reached, but it does not advertise RESPMOD and cannot scan transfers.*
	Cause: The ICAP service at the given *Service path* does not support the `RESPMOD` method used for scanning.
	Solution: Check the *Service path* in the provider settings with the antivirus vendor's documentation, for example `avscan`, `respmod` or `virus_scan`.

19.8 Sudo Plugin Issues

Problem	Symptoms and solution
Plugin denies every command	**Symptoms:** • All sudo commands are denied regardless of policy configuration. • No commands are authorized even when matching whitelist patterns.
	Solution: • Check `/etc/fudo/approval.key` ownership and permissions: – Must be owned by `root:root` – Permissions must be `0600` (read/write for owner only) – Run: `chown root:root /etc/fudo/approval.key && chmod 0600 /etc/fudo/approval.key` • Verify that the Fudo CA certificate is trusted on the target system. • Check if the API user has all required privileges (see *Typical Role Scenarios and Required Privileges*).
Command unexpectedly denied	**Symptoms:** • Sudo command is denied despite having a valid Fudo session. • Command appears to match configured regular expressions.
	Solution: • Check the audit trail via API: `GET /api/v2/session/<id>/command` • Review Fudo Enterprise event logs for entries: – **FUI1157** - Command approved (includes matched policy and regex) – **FUW1158** - Command denied (includes denial reason) • Verify the regular expression pattern matches the full binary path. • Ensure the policy is attached to the correct safe. • Check if the policy type is set to **Whitelist**.
No notifications for matched policy	**Symptoms:** • Sudo commands are being evaluated by policy. • No email, push, or SNMP notifications are received.
	Solution: • Verify the policy has the corresponding notification flags enabled: – Email notification flag – Push notification flag (Fudo Officer) – SNMP trap flag • Check notification service configuration in Fudo Enterprise settings. • Verify SMTP server settings for email notifications. • Ensure Fudo Officer is properly configured for push notifications.

Related topics:

- *Sudo Command Control Policy*
- *Typical Role Scenarios and Required Privileges*

19.9 Support Mode

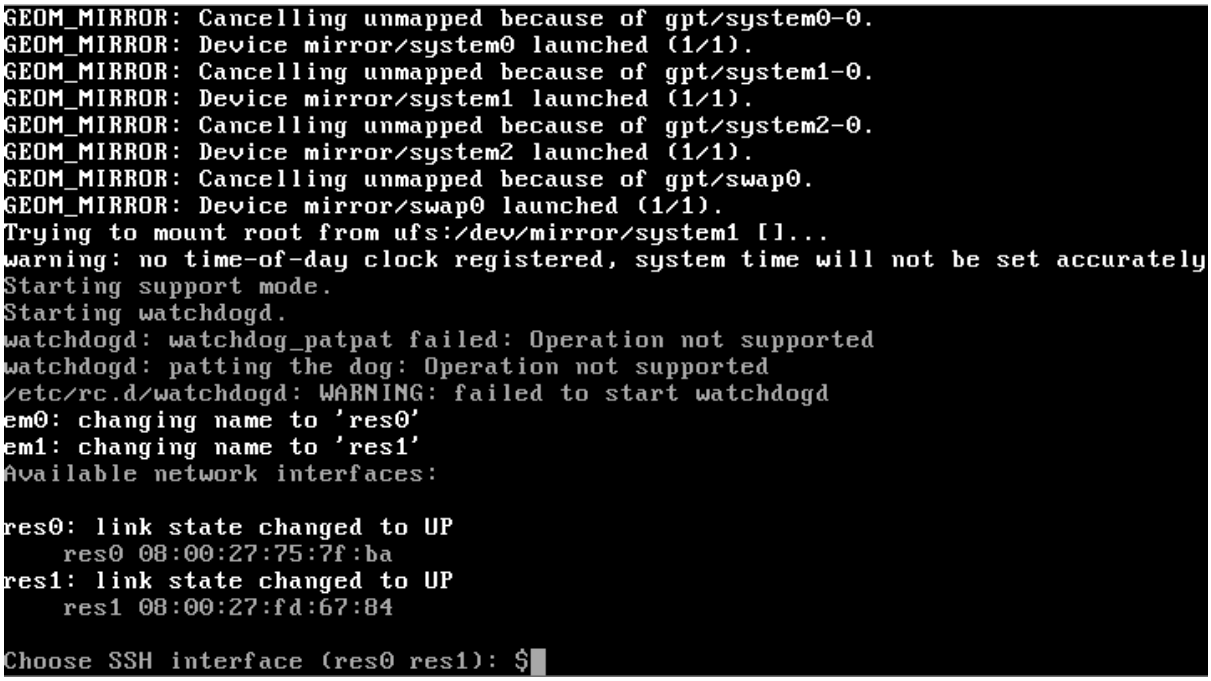
Support mode enables remote access to Fudo Enterprise in case it cannot boot up properly.

Enabling support mode

1. Access the system terminal.
2. During the boot up, enter `1` and press the *Enter* key to confirm.

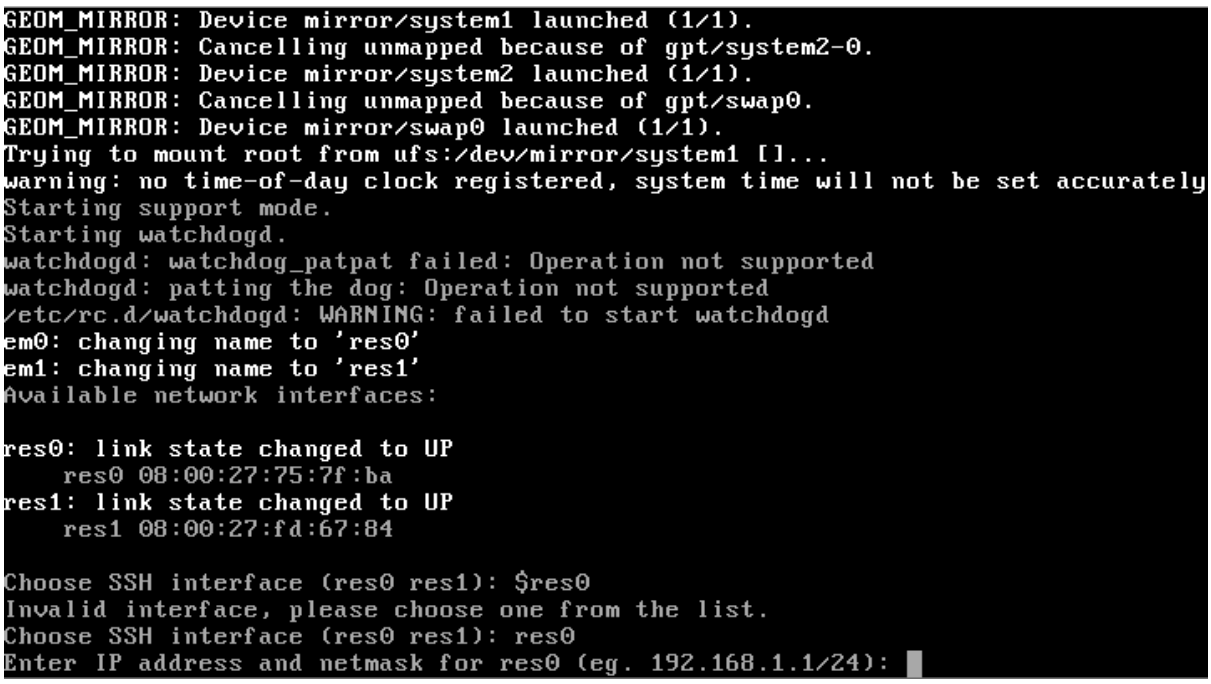
3. Select network interface.

> **Note**
>
> In support mode, network interfaces are named `res*` instead of `net*`.



4. Enter the IP address along with network mask, eg. `10.0.0.8/16`.

> **Note**
>
> The IP address is used for establishing remote SSH connection, thus it must be reachable by the technical support specialist. If possible, the IP address should be the same as before the system's malfunction.



5. Enter the gateway's IP address and press enter to enable connection to your Fudo Enterprise.

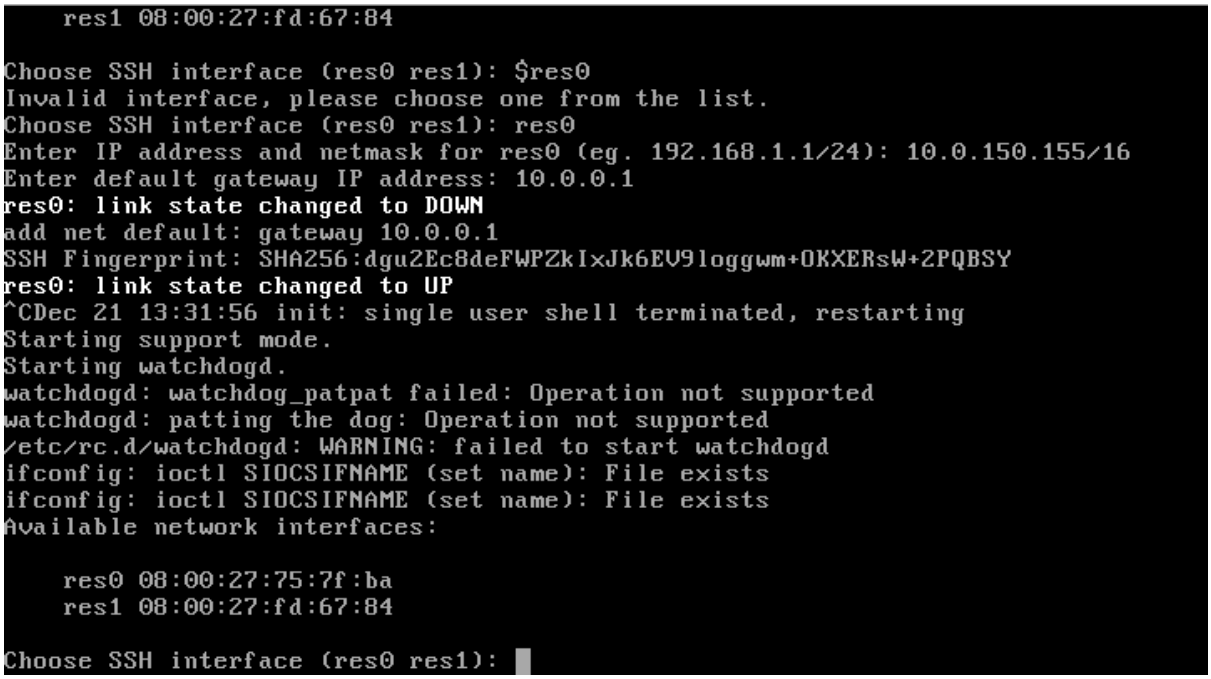
```
GEOM_MIRROR: Cancelling unmapped because of gpt/system2-0.
GEOM_MIRROR: Device mirror/system2 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/swap0.
GEOM_MIRROR: Device mirror/swap0 launched (1/1).
Trying to mount root from ufs:/dev/mirror/system1 []...
warning: no time-of-day clock 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:
```

Note

- Fingerprint allows for verifying that the connection has been established with the correct remote host.

```
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. Once the work is done and the connection is no longer needed, press `[Ctrl]` + `C` keys to close it and reset the network settings.



Related topics:

- *Network Interfaces Configuration*
- *System Maintenance*

CHAPTER 20

Use Cases

20.1 Two-Factor OATH Authentication with Google Authenticator

Google Authenticator generates verification code as a dynamic component to a static password to increase account security.

Fudo Enterprise allows configuring default settings for the OATH authentication so they are automatically added to the user definition, when administrator selects `OATH` as an active authentication method.

Note

When configuring two-factor OATH authentication in Fudo Enterprise you can also consider using alternative applications such as Microsoft Authenticator.

20.1.1 Protocols Supporting OATH Authentication Method

When logging in, OATH authentication can be performed either in *Challenge-Response* mode or by concatenating the dynamic code generated by Google Authenticator to the end of the static password defined in the authentication method, such as `password481418.` Please note that not all protocols support this authentication method.

Table 1: `OATH Availability Across Protocols`

Platform or Protocol	Challenge-Response Mode	Password + Dynamic Code
Logging into Access Gateway	available	available
Logging into Admin Panel	available	available

continues on next page

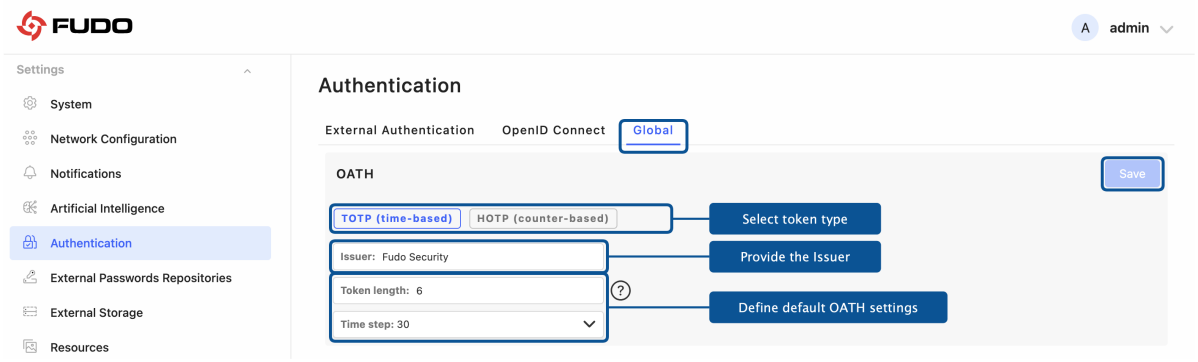
Table 1 – continued from previous page

Platform or Protocol	Challenge-Response Mode	Password + Dynamic Code
VNC	available	available
SSH	available	available
RDP	available	available
Telnet 3270	not available	available
Telnet 5250	not available	available
Telnet	not available	available
MySQL	not available	available
MS SQL(TDS)	not available	not available
HTTP/S	not available	not available
TCP	not available	not available
X11	not available	not available
Modbus	not available	not available

20.1.2 Configuring the OATH Authentication Method

In order to configure default settings for the OATH authentication method, follow the instruction:

1. Select *Settings* > *Authentication* > *Global* tab.
2. Go to *OATH* section and select token type: `TOTP (time-base)` or `HOTP (counter-base)`.
3. Fill out the *Issuer* field.
4. Fill out the *Token length* field.
5. Input *Time step* if selected *Token type* was `TOTP (time-base)`.
6. Click *Save* next to the *OATH* section name.



In order to configure OATH as an active authentication method for a user, follow the steps:

1. Select *User Management* > *Users*.
2. Find and click the user for whom you want to add the OATH authentication method.
3. Scroll down to the *Authentication* section.
4. Choose `OATH` type from the *Add authentication method* drop-down list.

5. Choose the `Static password` or `External authentication` as a first factor.

If `Password` is chosen:

- Enter password's static part.
- Fields *Token type*, *Token length* and *Time step* will be filled out automatically as default settings claim. Their value is editable.
- Enter a secret that will be used by *Google Authenticator*. Note, that the secret must be a `Base32` encoded value. Alternatively, click *Generate* to generate it automatically or *QRCode* to show the *QR code*.

If `External authentication` is chosen:

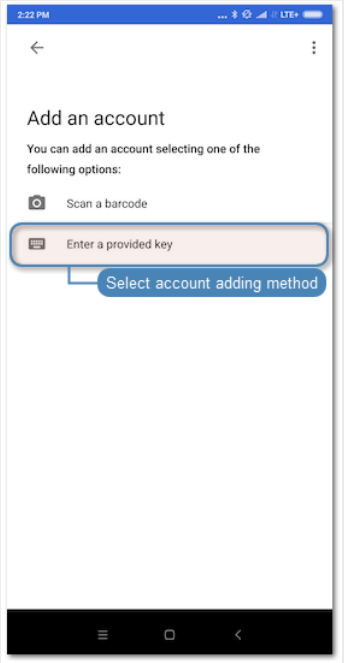
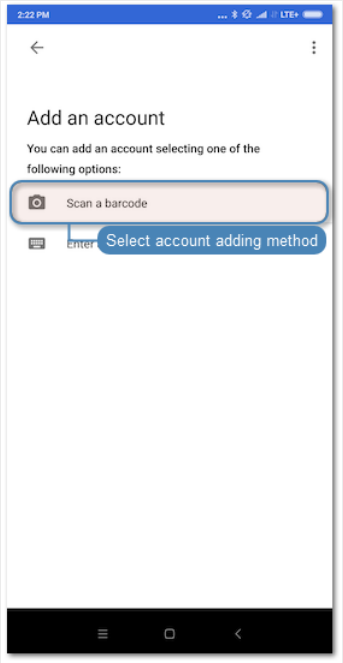
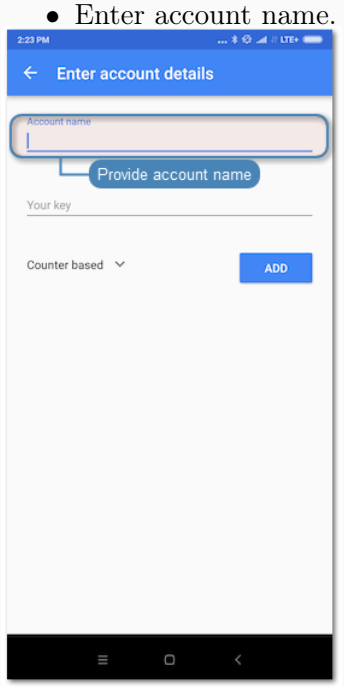
- Select External authentication source.
- Fields *Token type*, *Token length* and *Time step* will be filled out automatically as default settings claim. Their value is editable.
- Enter a secret that will be used by *Google Authenticator*. Note, that the secret must be a `Base32` encoded value. Alternatively, click *Generate* to generate it automatically or *QRCode* to show the *QR code*.

Note

Optional:

- Enable **Allow reuse** option to permit the same valid TOTP code to be accepted more than once within its current time window. This is useful for parallel access scenarios such as automated SSH access, CI/CD operations, or bulk file transfers.
- The *Initialized* option serves for the user's initialization via the QR code. When their *static password* as a *First factor* setting is filled or *External authentication* source if configured, the QR code is displayed during their first connection. After successful first authentication the *Initialized* option becomes checked and takes uneditable state.

6. Click *Save*.
7. Launch *Google Authenticator*.

Manual entry	QR Code
• Select *Enter a provided key.* 	• Click on user configuration form, next to the *Secret* field in the *Authentication* section. • Select *Scan a barcode* in *Google Authenticator* and scan the code. 
• Enter account name. 	

continues on next page

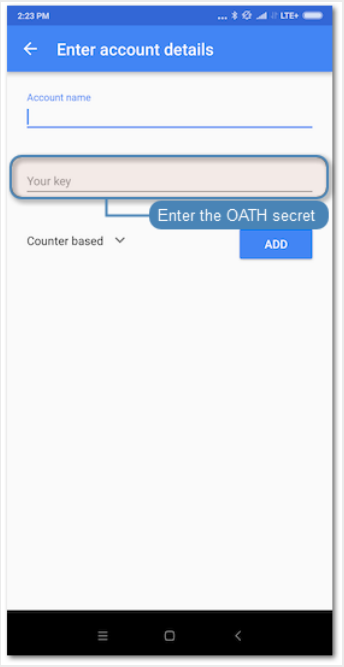
Table 2 – continued from previous page

Manual entry	QR Code

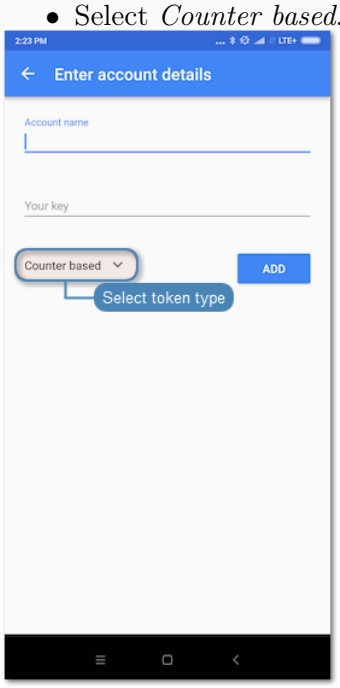
- Enter the secret defined in OATH authentication method.

Note

Click on the user configuration form in the *Authentication* section to reveal the secret.

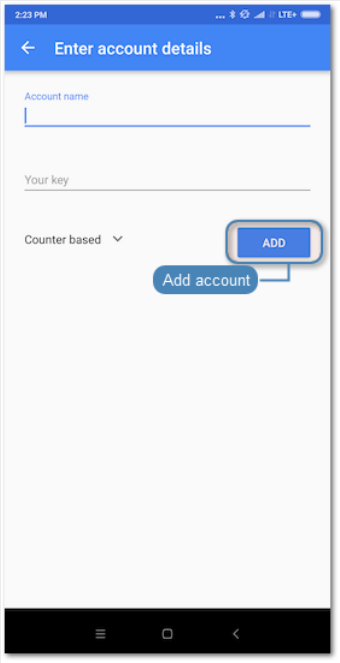


- Select *Counter based*.

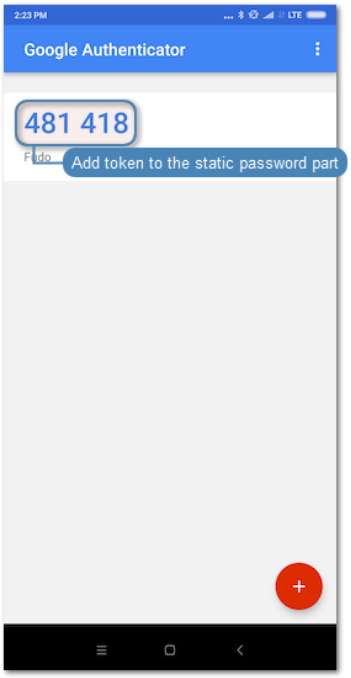


continues on next page

Table 2 – continued from previous page

Manual entry	QR Code
• Select ADD. 	

8. When logging in, the password string consists of a static password defined in the authentication method and dynamic part generated by the *Google Authenticator*, e.g. `password481418`.



20.1.3 TOTP Code Reuse for Parallel Access

The **Allow reuse** option enables the same valid TOTP code to be accepted more than once within its current time window. This feature is designed for scenarios where parallel access is required and protected with two-factor authentication.

20.1.3.1 Use Cases

This feature is particularly useful for:

- Scripted SSH access
- Ansible playbooks
- Parallel scp or rsync operations
- CI runners connecting to multiple systems
- Access through multiple bastion hosts
- Bulk RDP gateway hand-offs

20.1.3.2 Default Behavior

By default, the **Allow reuse** option is disabled. Each TOTP code can be used only once. After successful verification, another attempt using the same code will be rejected. This ensures the highest security level for standard use cases.

20.1.3.3 Behavior When Enabled

When **Allow reuse** is enabled for an OATH/TOTP authentication method:

- The same TOTP code can be accepted multiple times within its current time window
- An operator can use the same TOTP code for multiple parallel connections within one timestep
- Once the timestep expires, the previous code becomes invalid and a new code is required
- This allows supporting automation and bulk access scenarios without changing the standard TOTP expiration model

Note

The **Allow reuse** option is available only for TOTP (time-based) tokens. HOTP (counter-based) and other authentication methods do not support code reuse.

Warning

Enable this option only when necessary for specific use cases. Allowing TOTP code reuse reduces the security level compared to single-use codes. Always evaluate the security implications for your specific environment before enabling this feature.

Related topics:

- *User Authentication Methods and Modes*

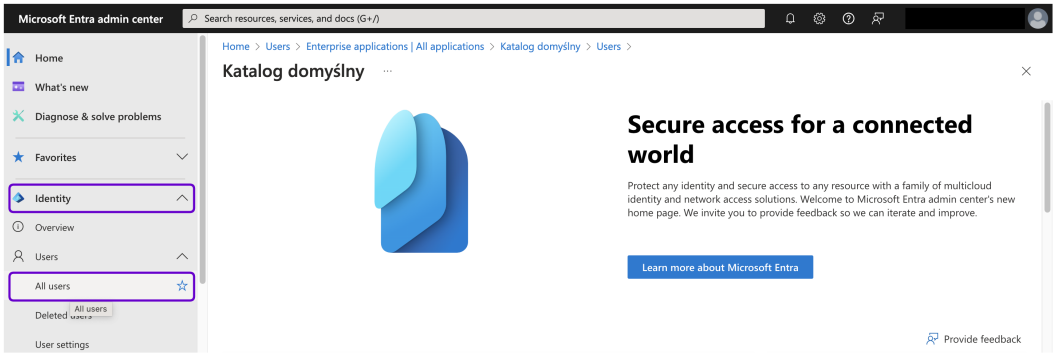
20.2 OpenID Connect Authentication Definition with Microsoft Entra (Azure)

To configure the OpenID Connect authentication method with Microsoft Entra, please follow below steps.

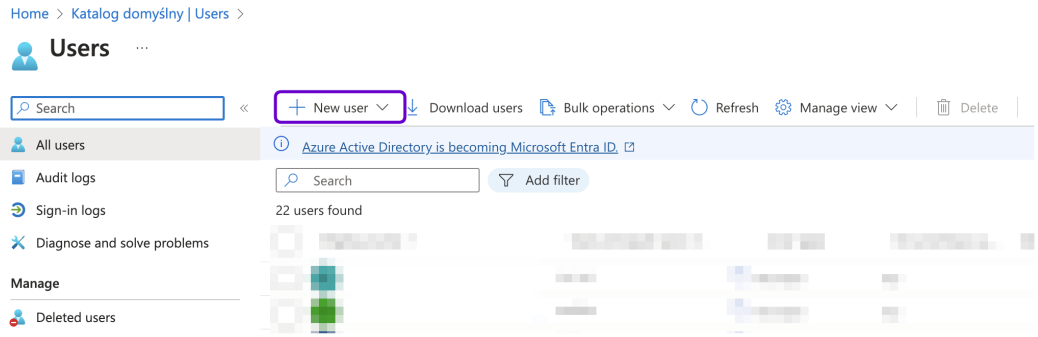
> **Note**
>
> Please note that this is a general guide, and specific details may vary depending on your Microsoft Entra setup. Refer to Microsoft Entra documentation for precise configuration steps.

Create user in Microsoft Entra ID

1. Go to the Microsoft Entra Admin Center and log in with your Microsoft Entra credentials.
2. In the left-hand menu, select *Entra ID* > *Users* > *All users*.



4. Click the *+ New user* and select *Create new user* from the drop-down list.



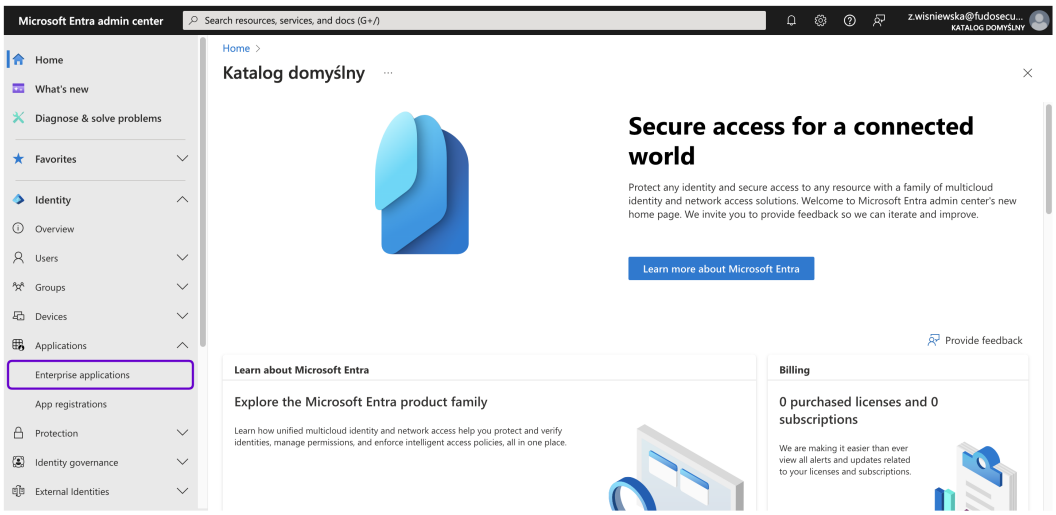
5. In the *User principal name* field, enter the username of the user account. For example, `user1@fudosecurity.com`.
6. In the *Display name* field, provide the name of the user of the account.
7. Provide the password phrase in the *Password* field or click the *Auto-generate password* option to generate the password.
8. Select the *Account enabled* option.
9. In the *Properties* tab, under the *Contact Information*, in the *Email* field provide the email address. For example, `user1@fudosecurity.com`.

10. Enter the details required for the user under the *Properties* and *Assignments* tabs.

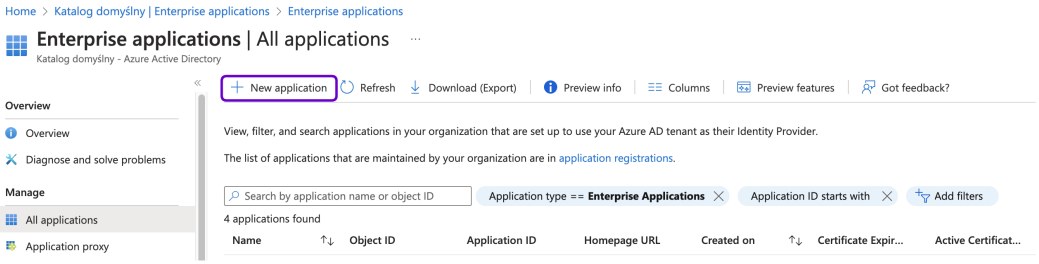
11. Click *Create*.

Register Fudo in Microsoft Entra ID

1. In the left-hand menu, select *Entra ID* > *Enterprise apps*.



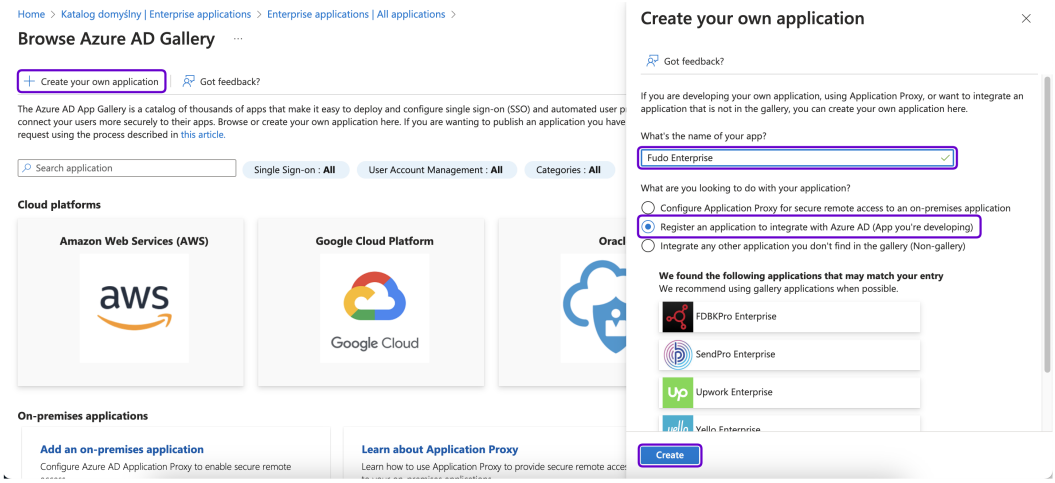
2. Click the + *New application* button to create a new application.



3. Click the + *Create your own application* button.

4. In the right-hand dialog box provide the name of your app and chose *Register an application to integrate with Microsoft Entra ID (App you're developing)* option.

5. Click *Create*.

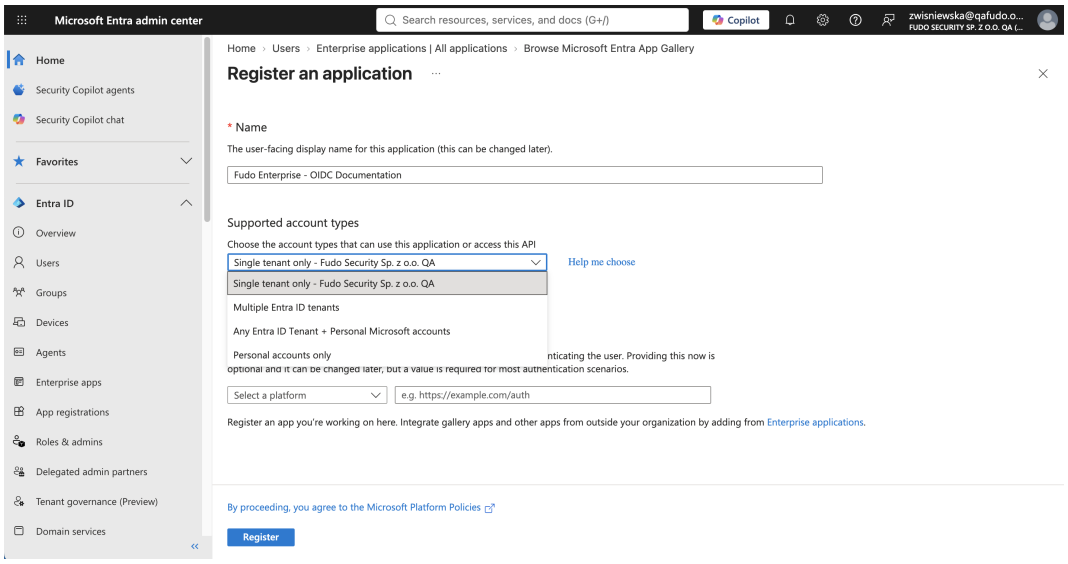


6. In the next page, under the *Supported account types* select the *Single tenant only* option.

7. Under the *Redirect URI* section select *Web* from the *Select a platform* drop-down list and provide the address of the Fudo Enterprise Access Gateway with the `/oidc` suffix. For example, `https://10.0.58.239/oidc` or `https://fudo.example.com/oidc`.

Note

You can find the User Access Gateway address under the Settings > Network configuration menu in the Fudo Enterprise. For more information, please follow the *Network Settings* section.

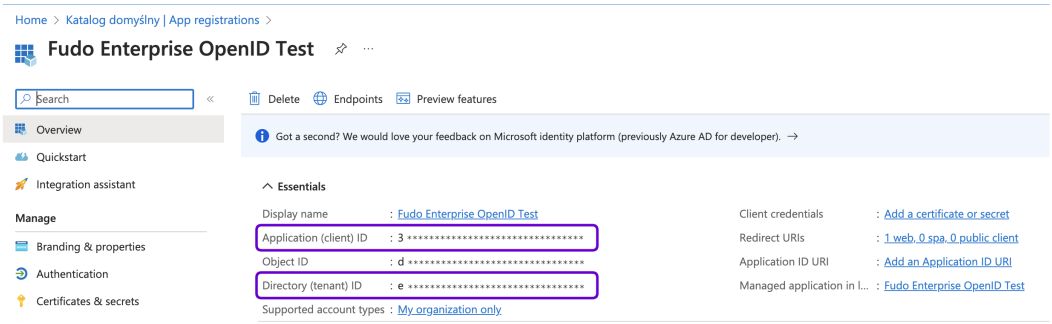


8. Click *Register* to create the application.

9. In the left-hand menu, select *Entra ID* > *App registrations.*

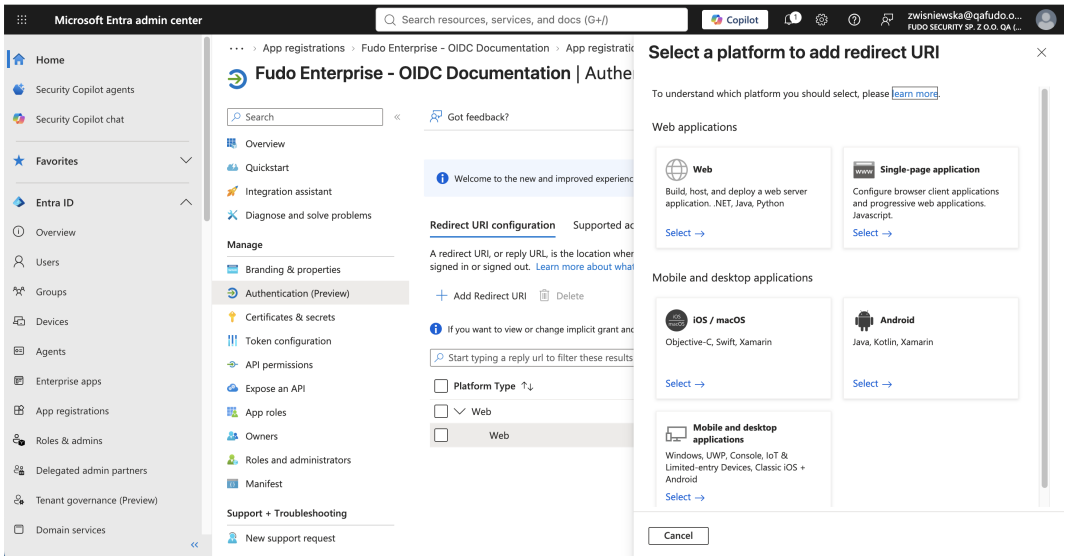
10. Change to *All applications* tab and find created application on the applications list.

11. Click on it's name to edit the parameters. Note down the *Application (client) ID* and *Directory (tenant) ID* as you will need these later.

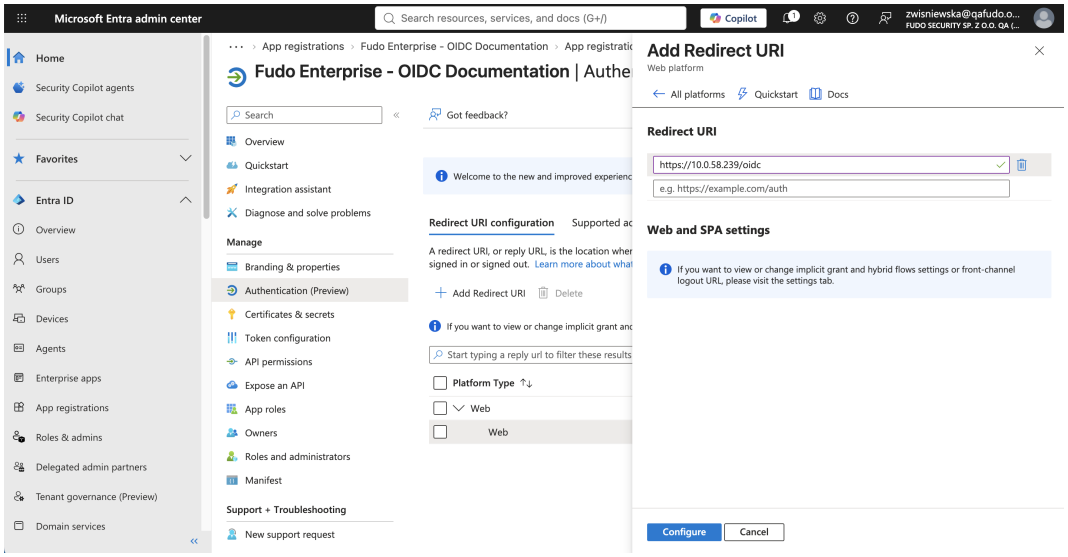


Configure Authentication Setting

1. In the left-hand menu, select *Entra ID* > *App registrations*.
2. Find created application on the applications list and click on it's name to edit the parameters.
3. Under the *Manage* section, click on *Authentication*.
4. In the *Redirect URI configuration* tab click *Add Redirect URI(s)*.
5. Select *Web*.

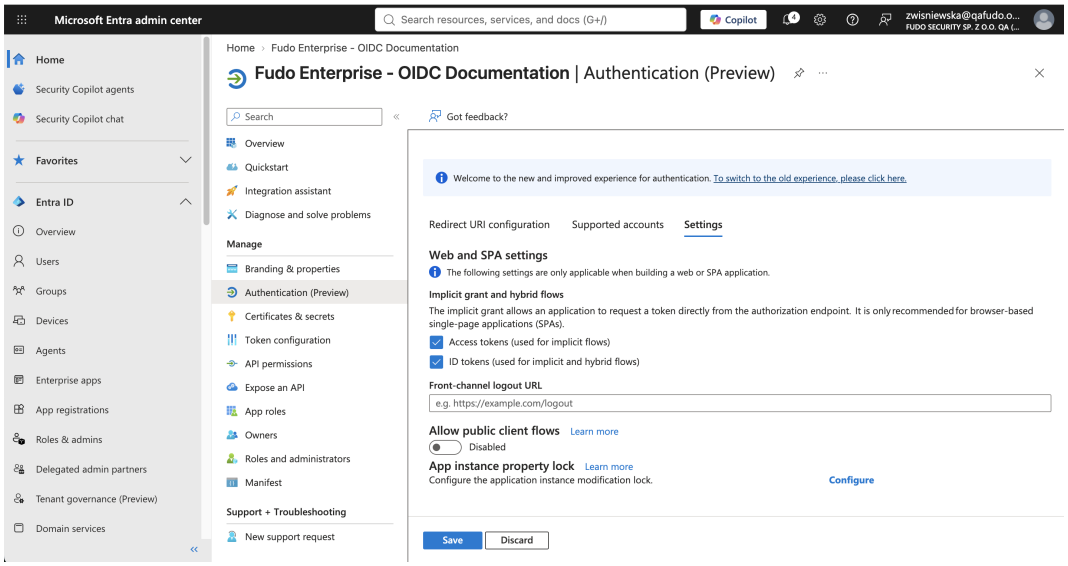


6. Provide the address following to the Fudo Enterprise Admin Panel with the `/oidc` suffix. For example, `https://10.0.58.238/oidc` or `https://fudo.example.com/oidc`.
7. Click *Configure*.

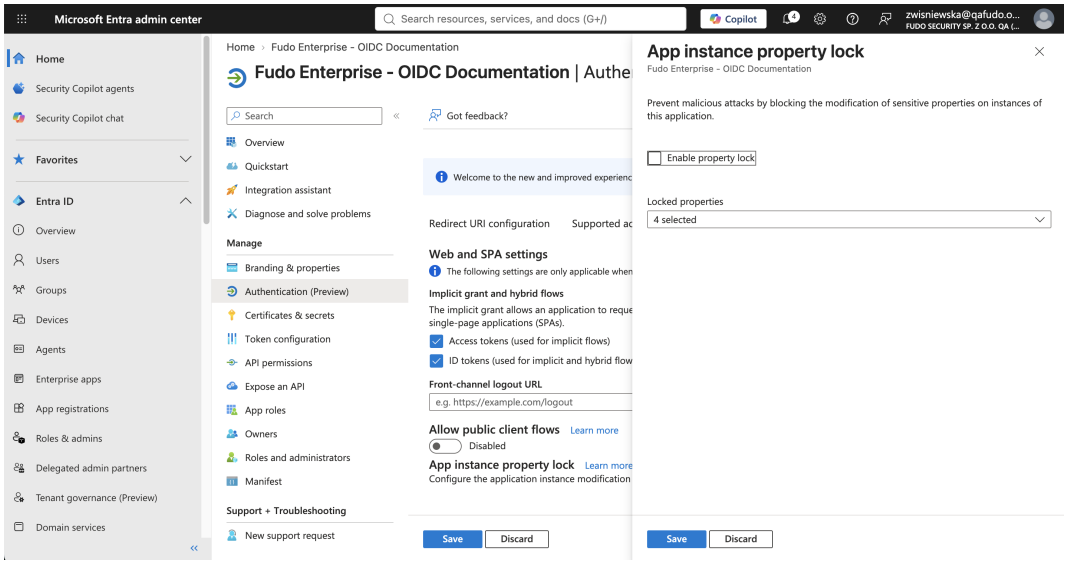


8. Go to *Settings* tab.

9. In the *Implicit grant and hybrid flows* section, check *Access tokens* and *ID tokens* options.



10. In the *App instance property lock* section, click *Configure* and uncheck the *Enable property lock* option in the right-hand dialog box. Click *Save* to close the dialog box.

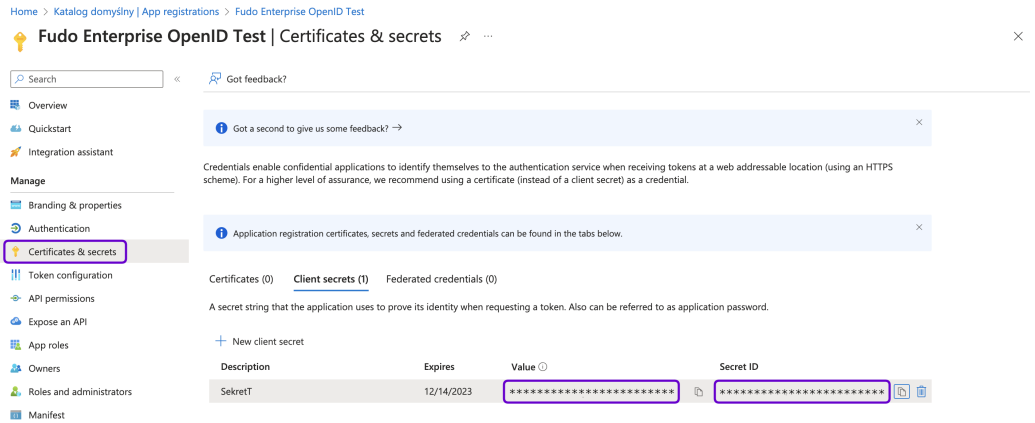


11. Click *Save* to save your authentication settings.

Generate Client Secret

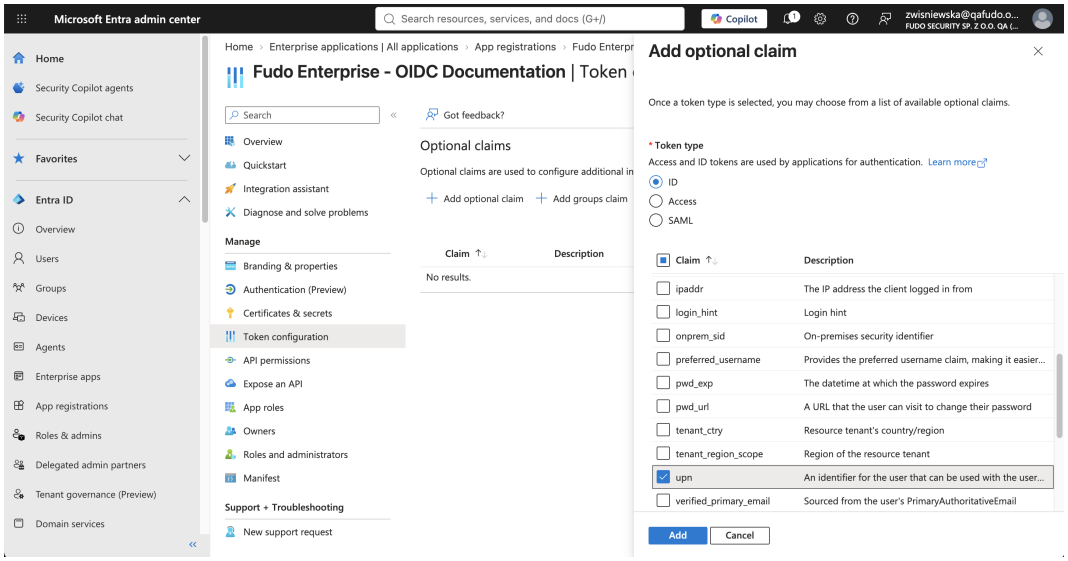
1. In your application's settings, navigate to the *Certificates & secrets* section.
2. Go to *Client secrets* tab and click *+ New client secret.*
3. Provide a description, select the desired expiration period, and click *Add.*

> **Warning**
>
> Note down the generated *Secret ID* and *Value* as you will need it for Fudo Enterprise configuration. Once saved, the secret value will no longer be visible.



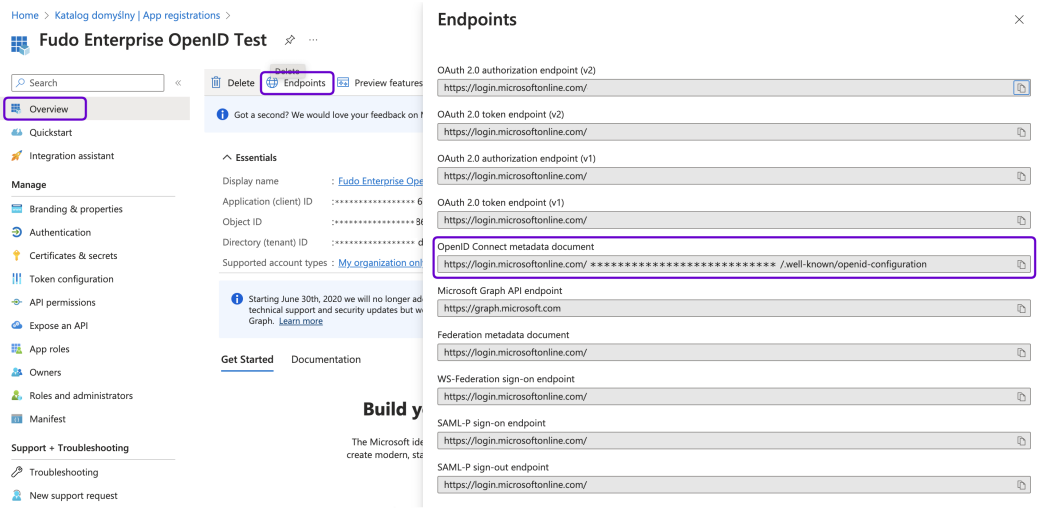
Token Configuration

1. In your application's settings, navigate to the *Token Configuration* section.
2. Click *+ Add optional claim.*
3. In the *Token type* select *ID.*
4. In the *Claim* list select *upn.*
5. Click *Add.*



Get OpenID Connect Configuration URL

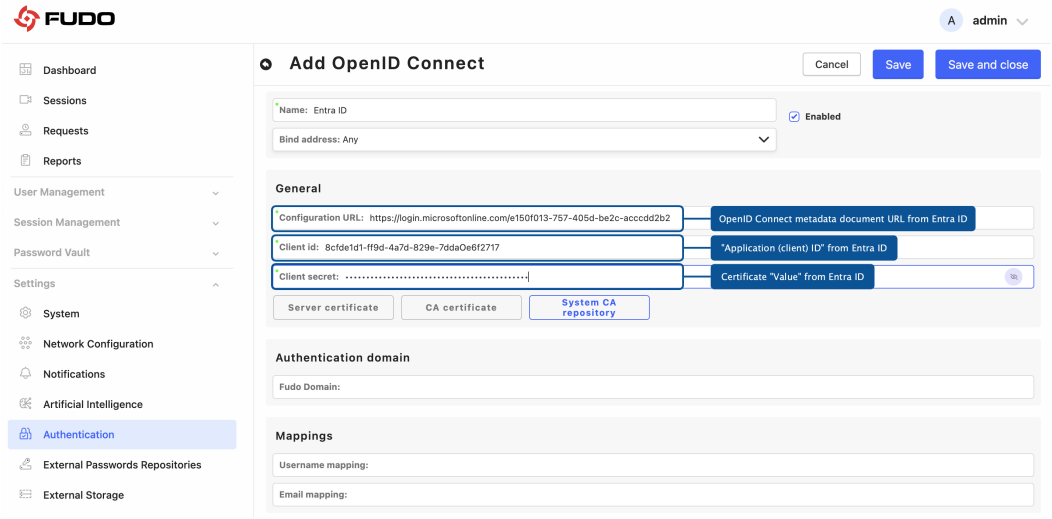
1. In your application's settings, navigate to the *Overview* section.
2. Open the *Endpoints* tab, and look for the *OpenID Connect metadata document* URL. This is your OpenID Connect Configuration URL. Copy it as you'll need it for Fudo Enterprise configuration.



Configure OpenID Connect authentication method in Fudo

1. Go to your Fudo Enterprise Admin Panel.
2. Select *Settings* > *Authentication*.
3. Choose **OpenID Connect** tab.
4. Click *Add OpenID Connect*.
5. Check the *Enabled* option to globally enable OpenID Connect authentication.
6. Provide Name (for example, *Entra ID*).
7. Set the *Bind address* to *Any*.
8. Input the *Configuration URL* (the *OpenID Connect metadata document URL* from Microsoft Entra).

9. Provide the *Client ID* (the *Application (client) ID* from Microsoft Entra).
10. Provide the *Client secret* (the certificate *Value* from Microsoft Entra).



11. Add *Username mapping* and *Email mapping* (optional). Those fields are useful when user's name has different naming convention.
12. Click *Save*.

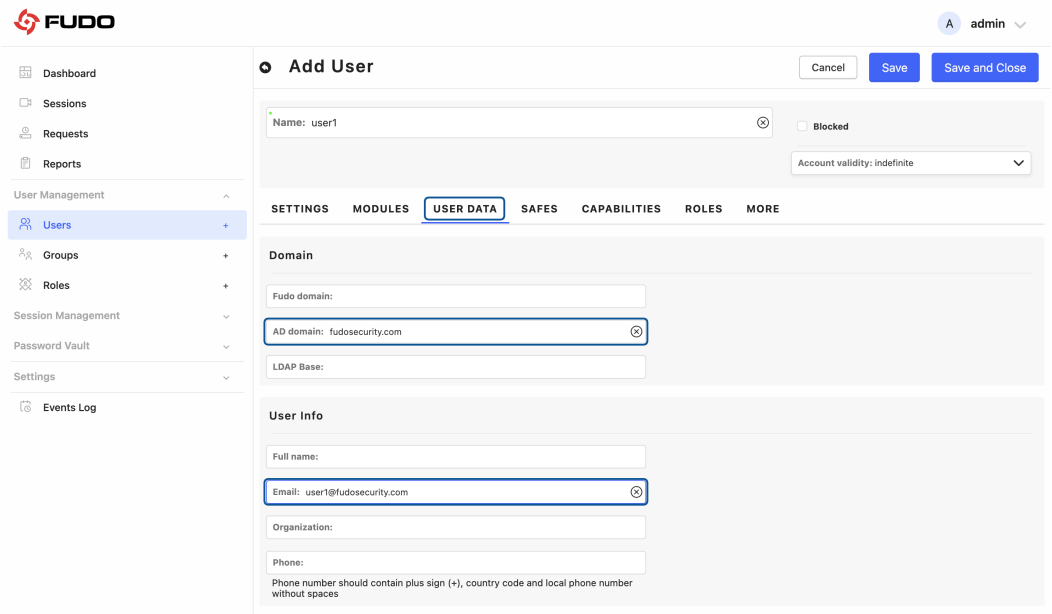
> **Note**
>
> To learn more about the algorithm used to determine the user's identity, visit *OpenID Connect Authentication Definition* section.

Create new user in Fudo

1. Select *User Management* > *Users* and then click + *Add user*.
2. Enter user name (`user1`).
3. In the *User Data* tab, in the *AD domain* field, enter the domain part of the user's *User principal name* - in this case `fudosecurity.com`.

> **Note**
>
> Fill in this field when users are identified by their *User principal name* (the `upn` claim). Fudo Enterprise matches the user name combined with the *AD domain* against the UPN received from Microsoft Entra, so the user name has to be the part of the UPN before the `@` sign - in this case `user1` - and the *AD domain* the part after it. A user whose *AD domain* is empty, or holds a value other than the UPN suffix, cannot be identified, and their first sign-in fails.

4. In the *User Data* tab, under the *User info* section, in the *Email* field enter the email address used during user creation in Microsoft Entra - in this case `user1@fudosecurity.com`.

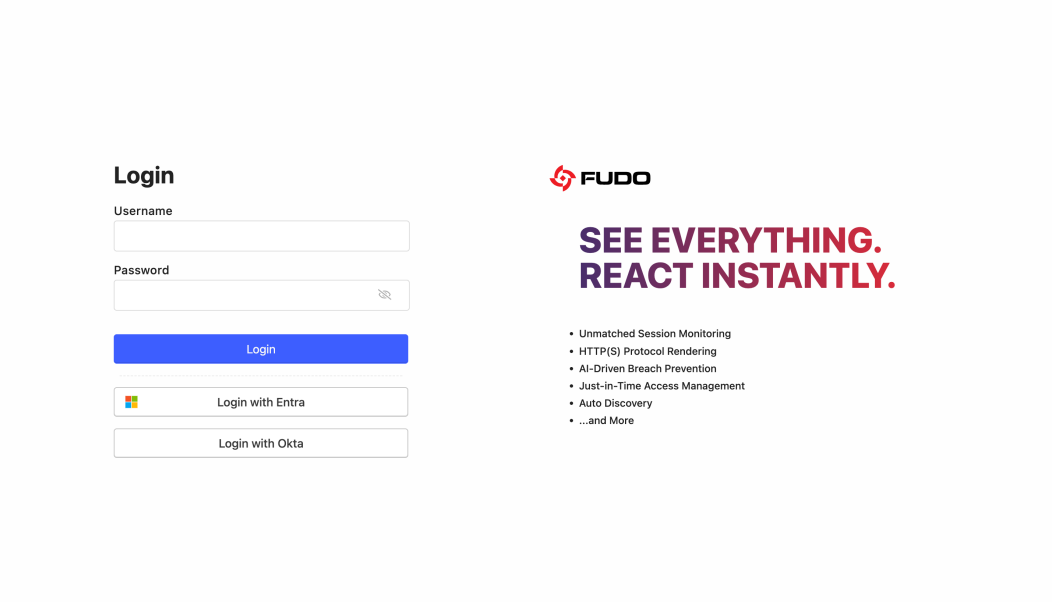


5. Fill in the rest of the parameters according to your needs.
6. Click *Save*.

> **Note**
>
> This address is utilized to associate Fudo Enterprise users with their corresponding accounts created in Microsoft Entra. Ensure that there is no duplication of email addresses among users.

Testing

You can now test the *OpenID Connect* authentication by attempting to log in to Fudo Enterprise. Click on created Microsoft Entra authentication method button under the default *Login* button.



Related topics:

- *User authentication methods and modes*
- *Authentication*
- *Integration with CERB server*

20.3 Remote Desktop Services Configuration on Windows Server for Fudo Enterprise

Before you start the procedure, check the following requirements:

- All servers with Windows Server 2019 or 2022 environment are connected in a domain;
- Domain Controller with AD user group is configured on Windows Server;
- All Windows servers have the security patch `CredSSP CVE-2018-0886` installed;
- You have the access to the Fudo Admin Panel to set up an RDP connection.

Warning

Support for the **anonymous** account in RDS has been removed.

20.3.1 Setup Remote Desktop Services (RDS) on Windows

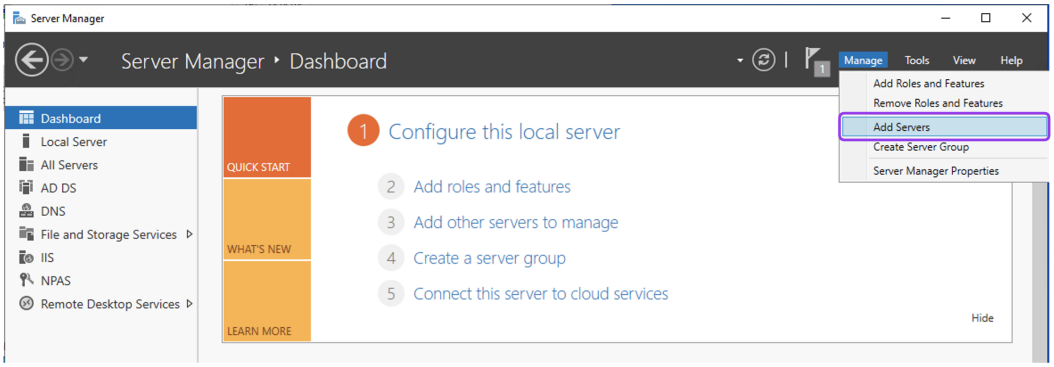
To configure and use the Remote Desktop Services (RDS) with Fudo Enterprise, please follow below steps.

Note

Please note that this is a general guide, and specific details may vary depending on your Windows Server setup. Refer to the Windows Server documentation for precise configuration steps.

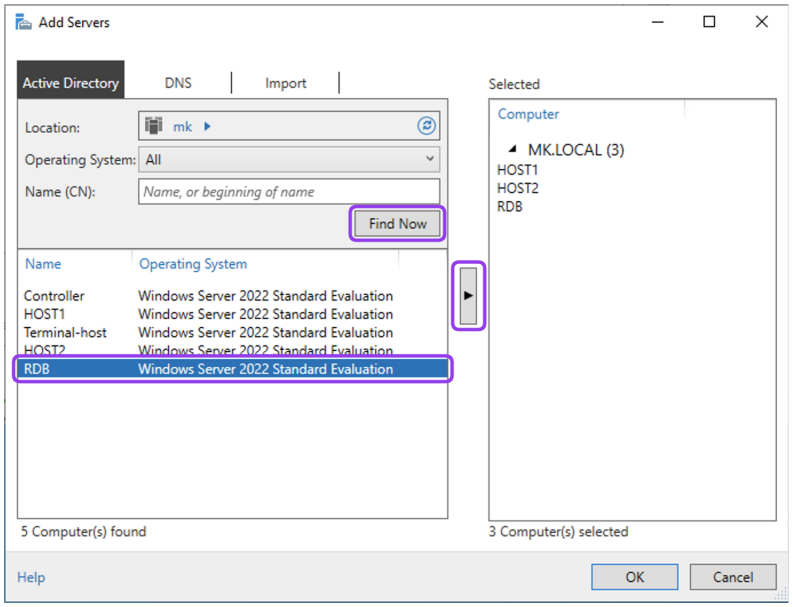
Add Servers:

1. Log in to the server on which you want to setup the Remote Desktop Services.
2. Open the *Server Manager* application.
3. Click *Manage* button on the upper right corner of the window to expand the menu list and select *Add Servers*.



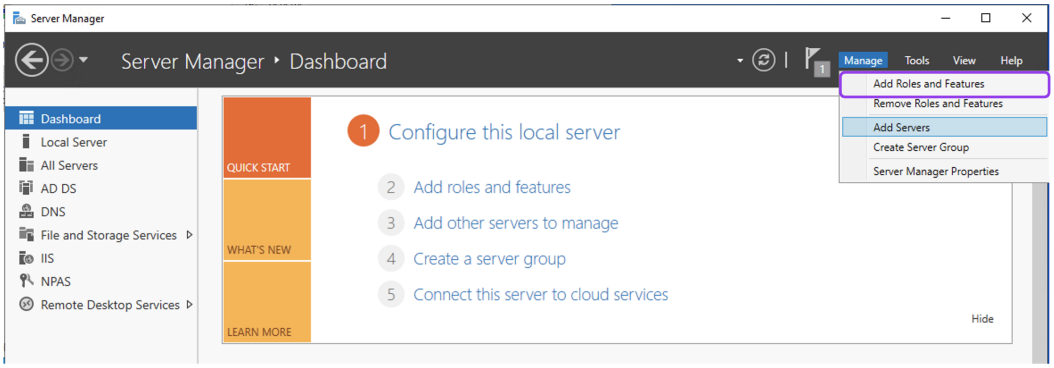
4. Click *Find Now*.

5. Add all the servers you're going to use for RDS by clicking on each server in the deployment. Click *OK*. In this use case we add 3 servers: `HOST1`, `HOST2`, and `RDB` which will play the Broker role.

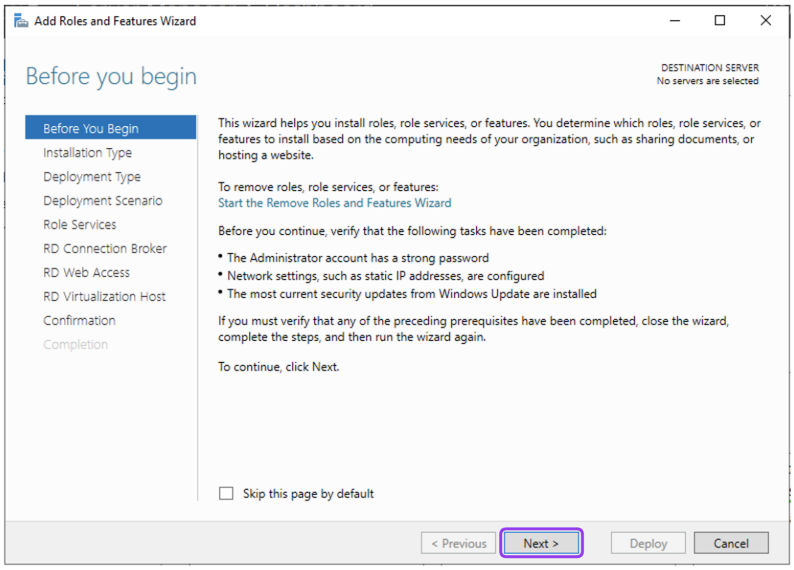


Deploy the Remote Desktop Services Components:

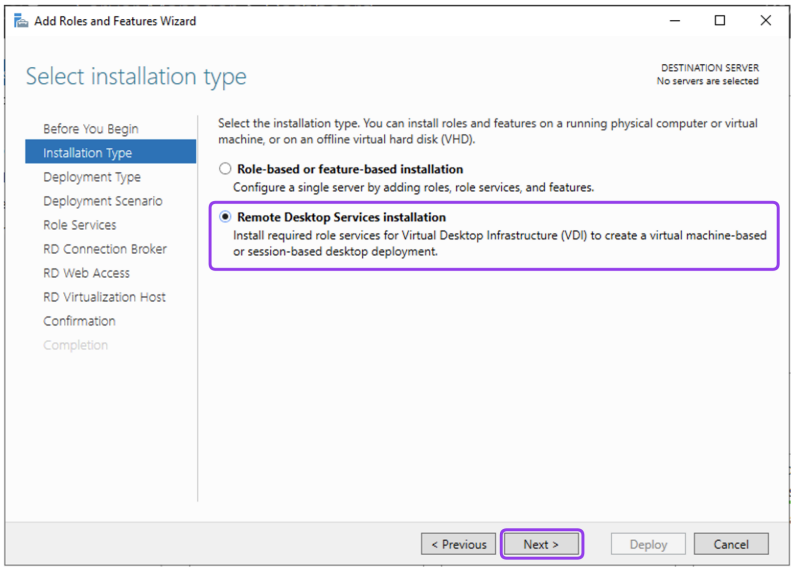
1. Click *Manage* button on the upper right corner of the window to expand the menu list and select *Add Roleas and Features*.



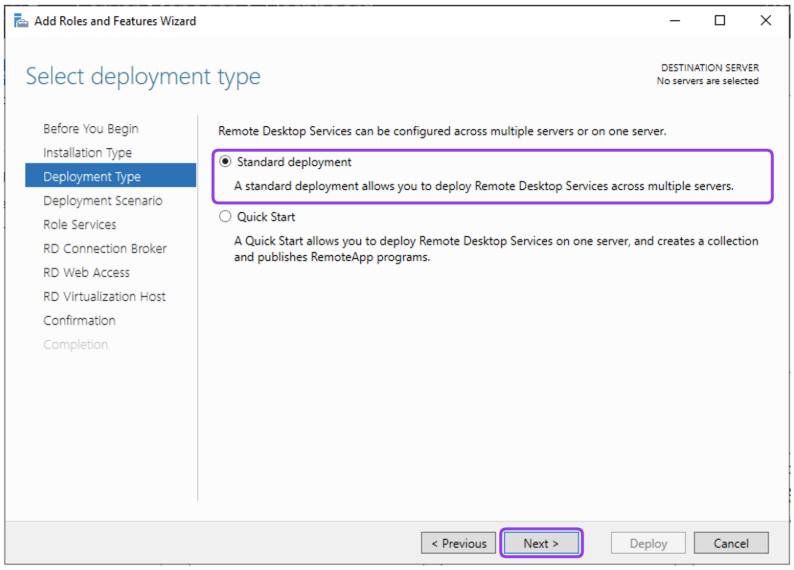
2. On the *Before You Begin* tab, click *Next* to proceed.



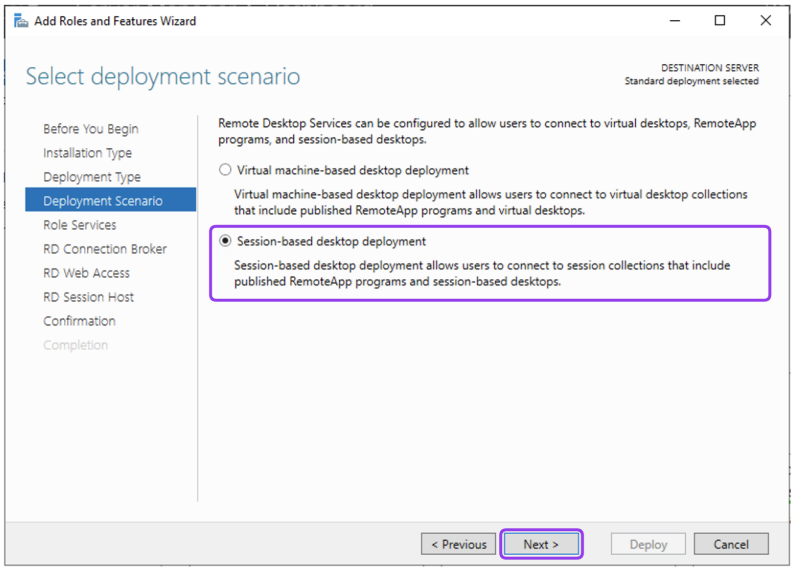
3. On the *Installation Type* tab, select *Remote Desktop Services installation*, and click *Next* to proceed.



4. On the *Deployment Type* tab, select *Standard Deployment* to access more detailed instructions for installing Remote Desktop Services. Click *Next* to proceed.

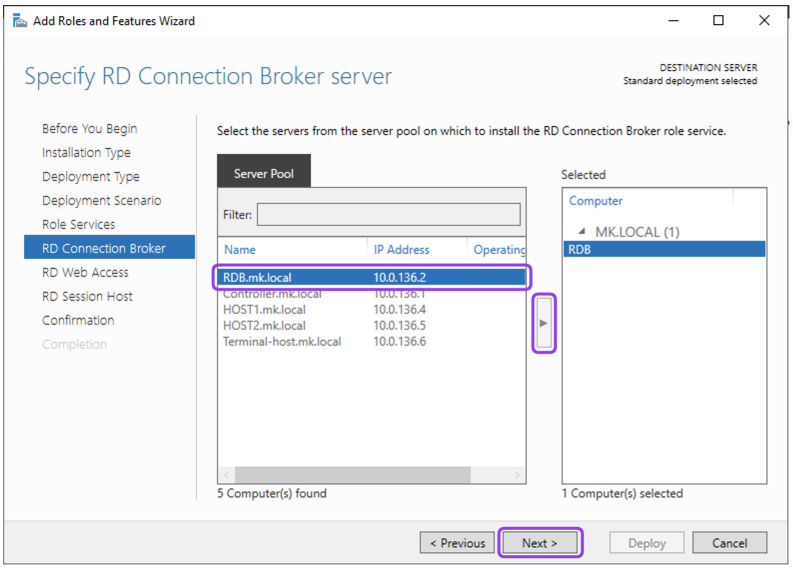


5. On the *Deployment Scenario* tab, select *Session-based desktop deployment*. Click *Next* to proceed.

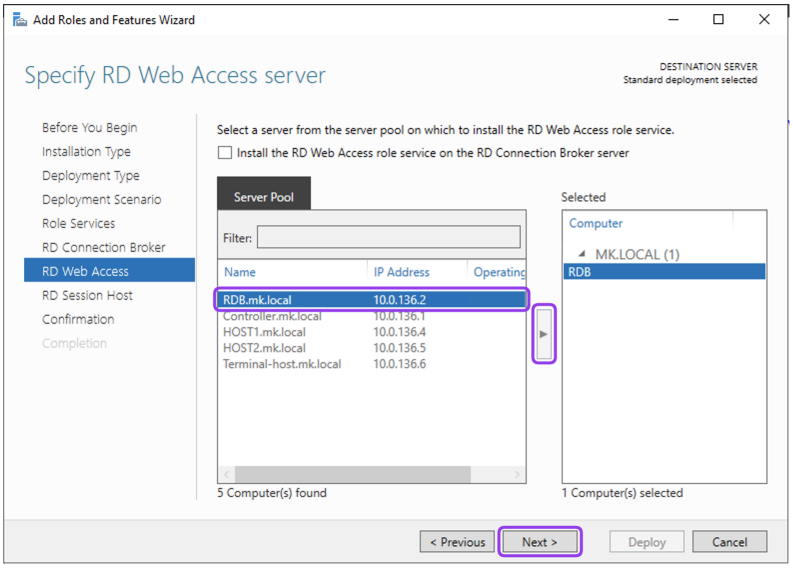


6. On the *Role Services* tab, review the services that will be installed. Click *Next* to proceed.

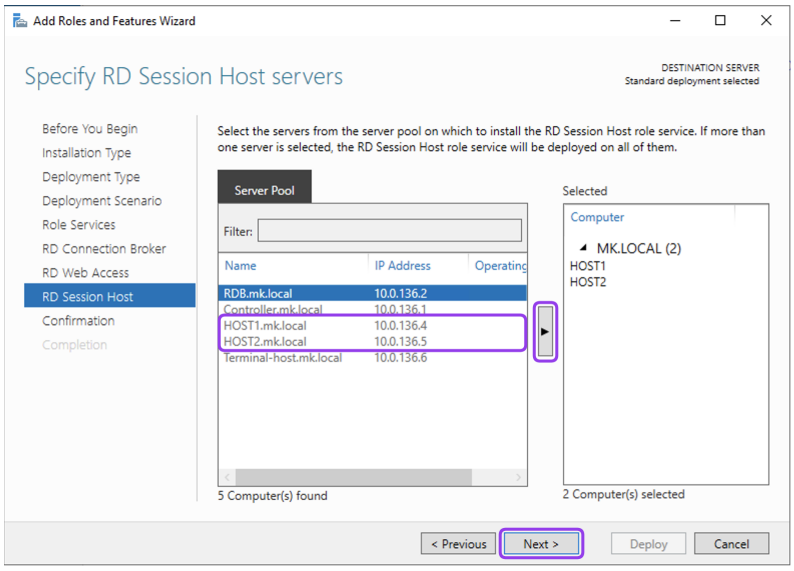
7. On the *RD Connection Broker* tab, select the appropriate server on which to install the RD Connection Broker role service. In this example `RDB` server was selected. Click *Next* to proceed.



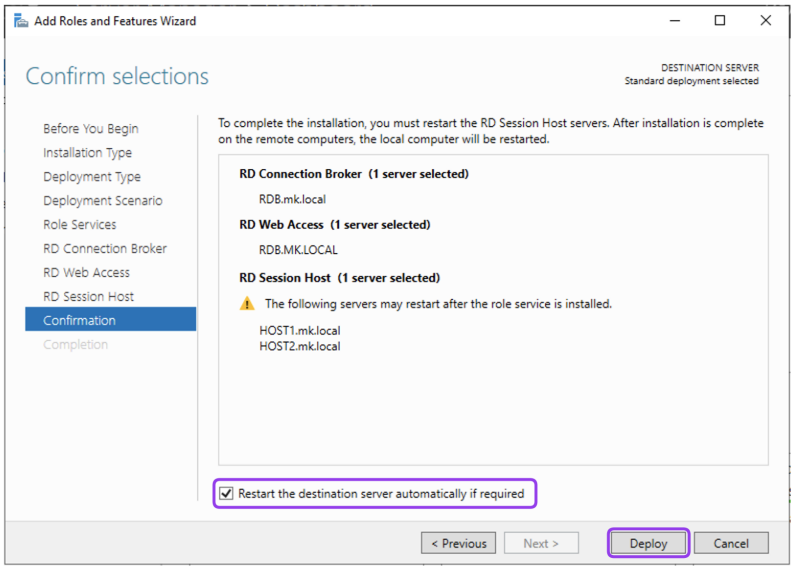
8. On the *RD Web Access* tab, select the appropriate server on which to install the RD Web Access role service. In this example, the `RDB` server was also selected. Click *Next* to proceed.



9. On the *RD Session Host* tab, select the appropriate servers on which to install the RD Session Host role service. In this example, the `HOST1` and `HOST2` servers were selected. Click *Next* to proceed.



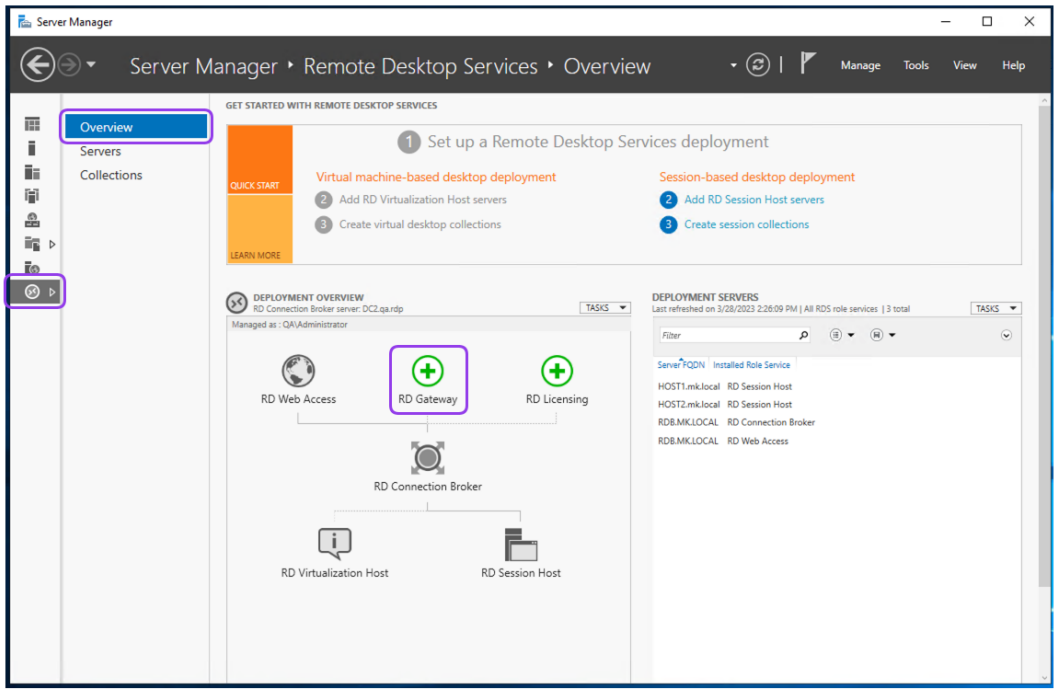
10. On the *Confirmation* tab, select *Restart the destination server automatically if required*, and then click *Deploy*.



11. Wait for the deployment to complete successfully and click *Close*.

Add the RD Gateway server and certificate name:

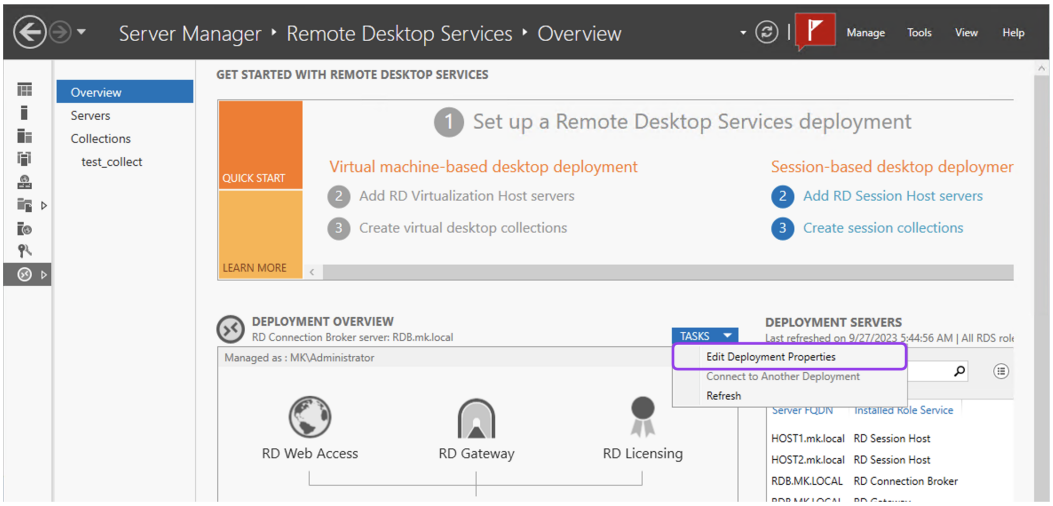
1. Select the *Remote Desktop Services* section from the left-hand menu and go to *Overview* tab.
2. Click the *+ RD Gateway* button and in the *Add RD Gateway Servers wizard*, select the virtual machine where you want to install the RD Gateway server. In this example `RDB` server was selected.



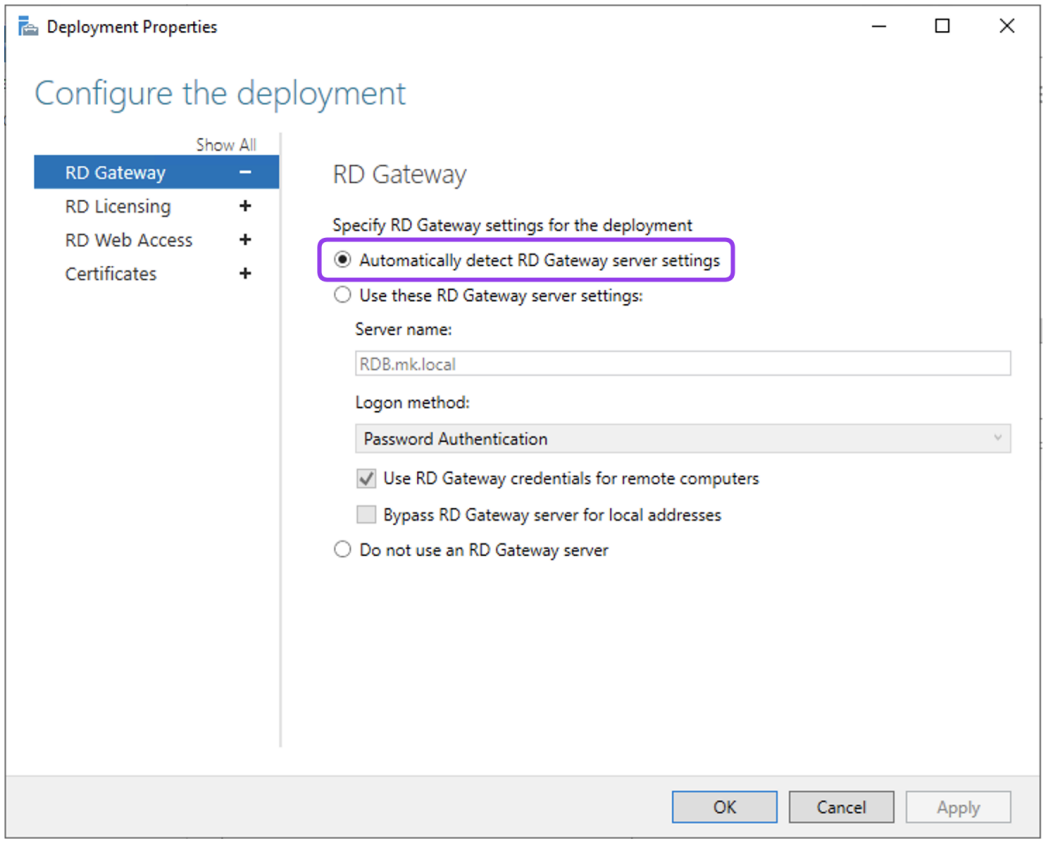
3. Click *Next*.
4. Enter the SSL certificate name for the RD Gateway server using the external fully qualified DNS Name (FQDN) of the RD Gateway server. Example, `cert.mk.local`.
5. Click Next, and then click *Add*.
6. Wait until the role service is deployed and click *Close*.

Configure the RD Gateway and RD Licensing deployment properties:

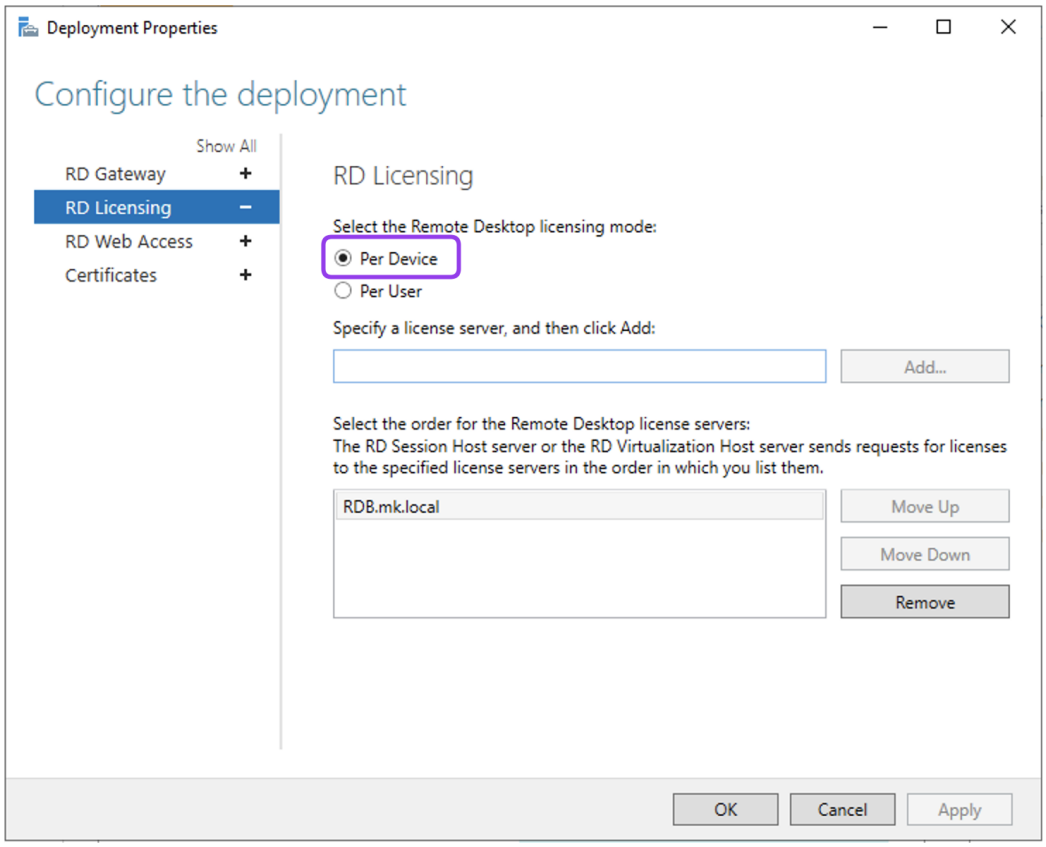
1. Go back to the *Overview* tab, click *Tasks* and select *Edit Deployment Properties* from the drop down list.



2. On the *RD Gateway* tab, select *Automatically detect RD Gateway server settings* option and click *Apply*.

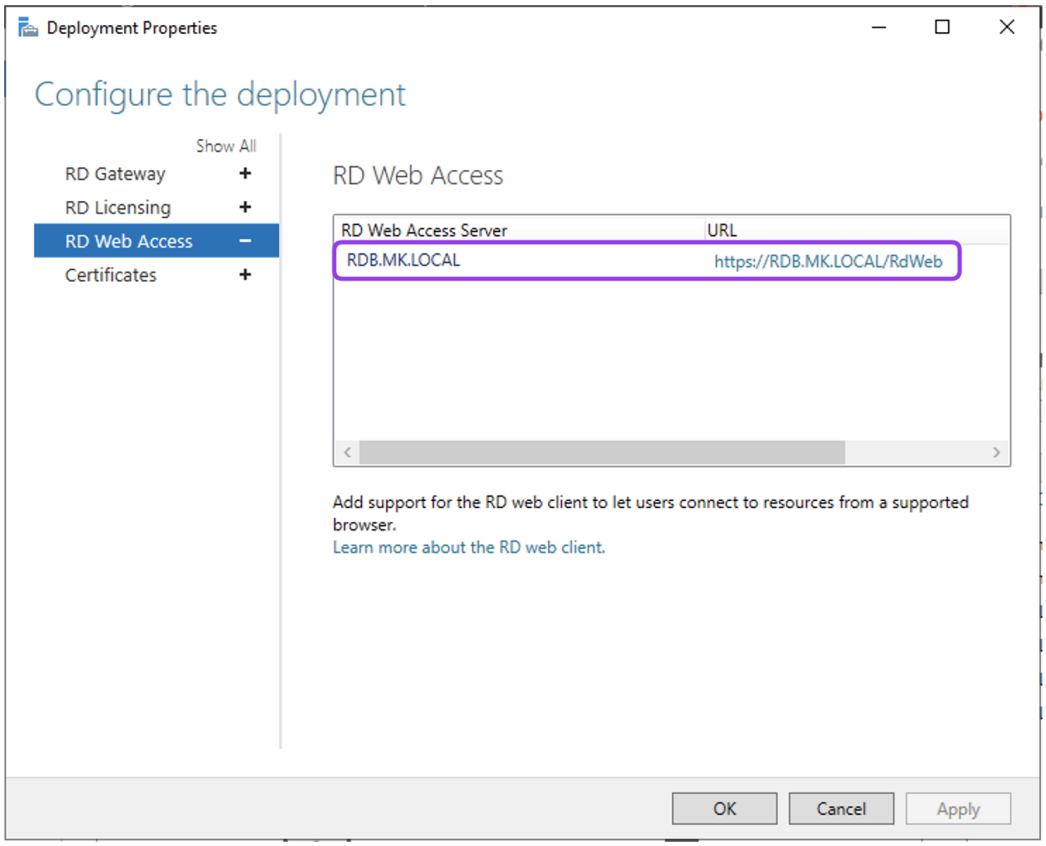


3. Expand the *RD Licensing* tab and select *Per Device*. Click *Apply*.



4. Expand the 'RD Web Access' tab, to check the RD Web Access IIS application

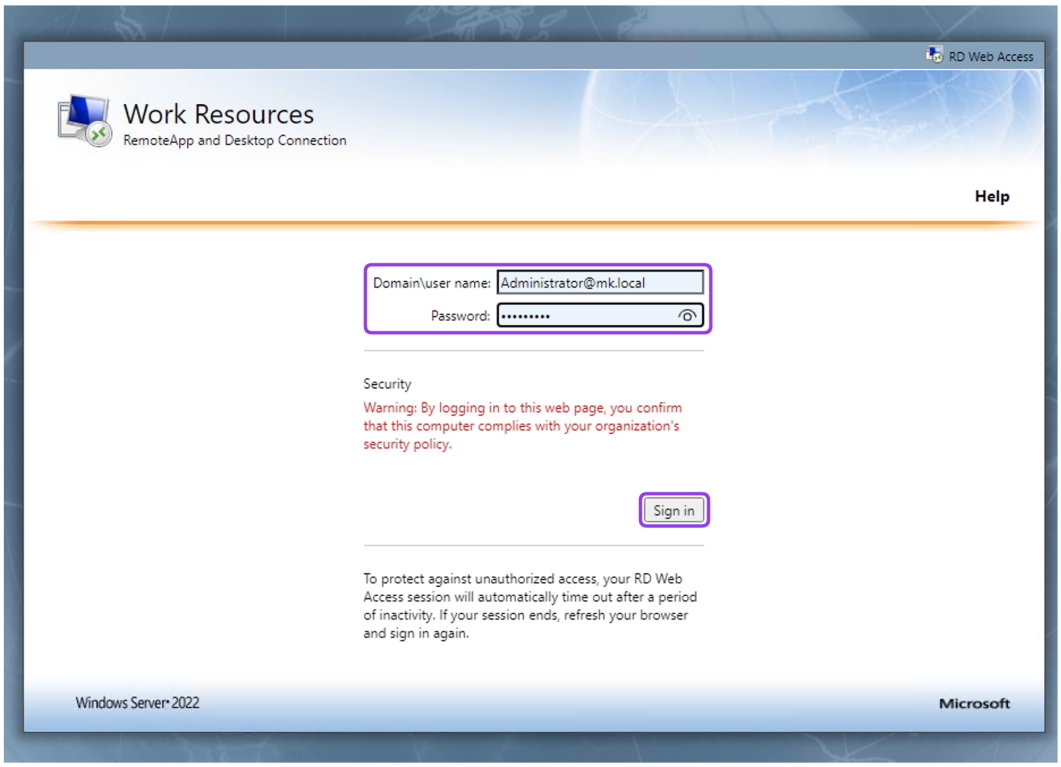
URL. It is installed by default under the `/RdWeb`.



5. Click on the displayed URL to verify the RD Web Access login using the administrator account.

Note

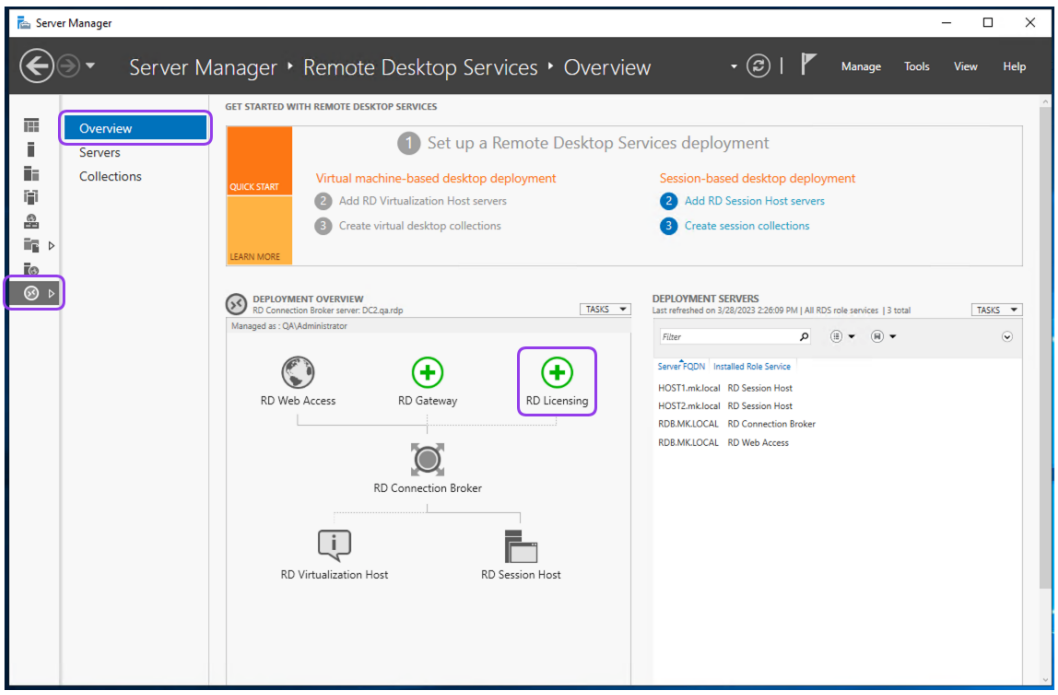
While login, please use the domain in the *user name* field. For example, `Administrator@mk.local`.



6. Save this address for the subsequent configuration steps.
7. Click *OK* in the *Deployment Properties* window to go back to the *Overview* tab of the *Remote Desktop Services* section.

Add the RD License Server:

1. Click the *+ RD Licensing* button in the *Overview* tab of the *Remote Desktop Services* section.



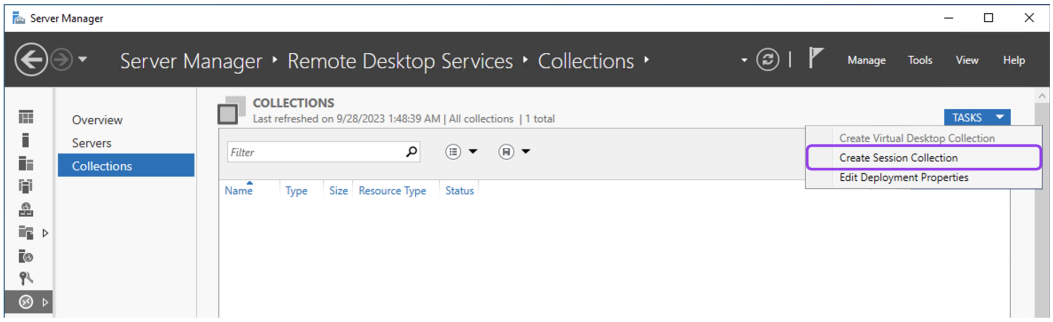
2. Select the virtual machine where the RD license server will be installed. In this

example `RDB` server was selected. Click *Next*, and then click *Add*.

3. Wait until the role service is deployed and click *Close*.

Create a session collection:

1. Go to the *Collections* tab of the *Remote Desktop Services* section, click *Tasks* and select *Create Session Collection* from the drop down list.



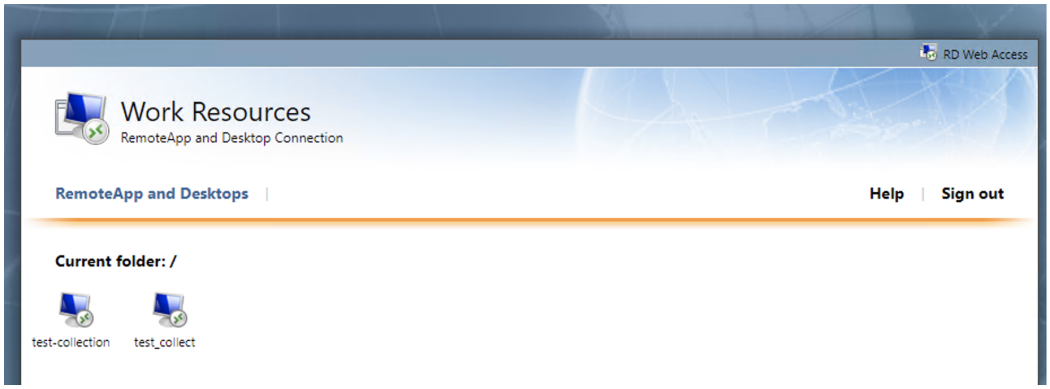
2. On the *Before You Begin* tab, click *Next* to proceed.
3. On the *Collection Name* tab, provide a descriptive name of the collection. In this example we used `test-collection` name. Click *Next* to proceed.

> **Note**
>
> This name will be displayed under its icon in the Web Access interface.

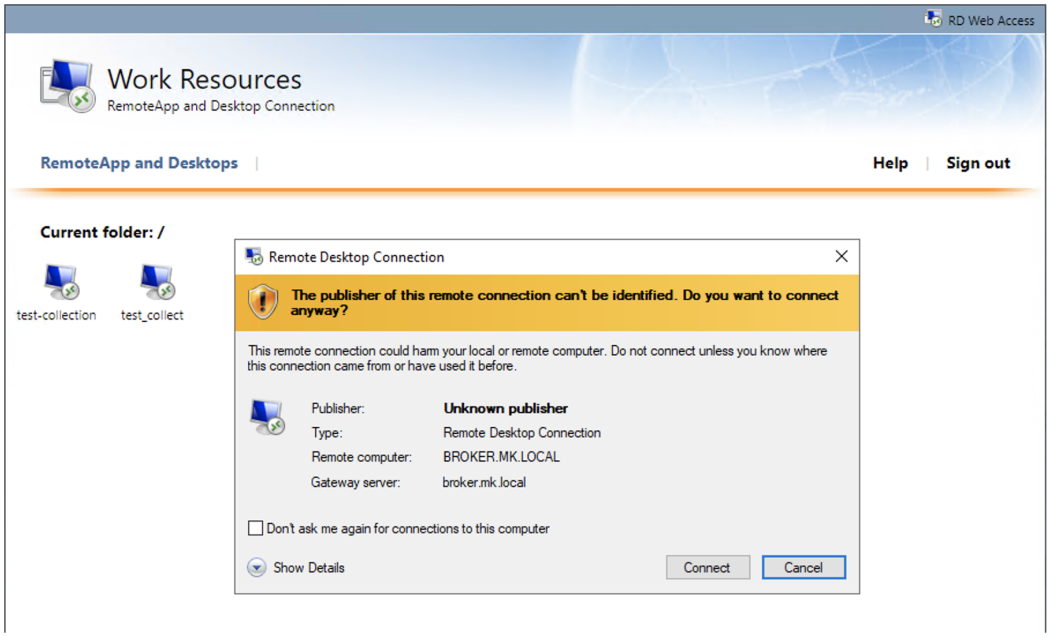
4. On the *RD Session Host* tab, select the RD Session Host Servers to add to this collection. In this example, the `HOST1` and `HOST2` servers were selected.
5. On the *User Groups* tab, define user groups. You can either accept the default user groups or add one or more groups of users permitted to connect using RDP to the Session Host server(s).
6. On the *User Profile Disks* tab, select *Enable User Profile Disks* option and specify the settings if needed. You can also leave this option disabled.
7. On the *Confirmation* tab, please review all the information and then click 'Create'.
8. Wait until the collection is created. Click *Close*.

Test the connection:

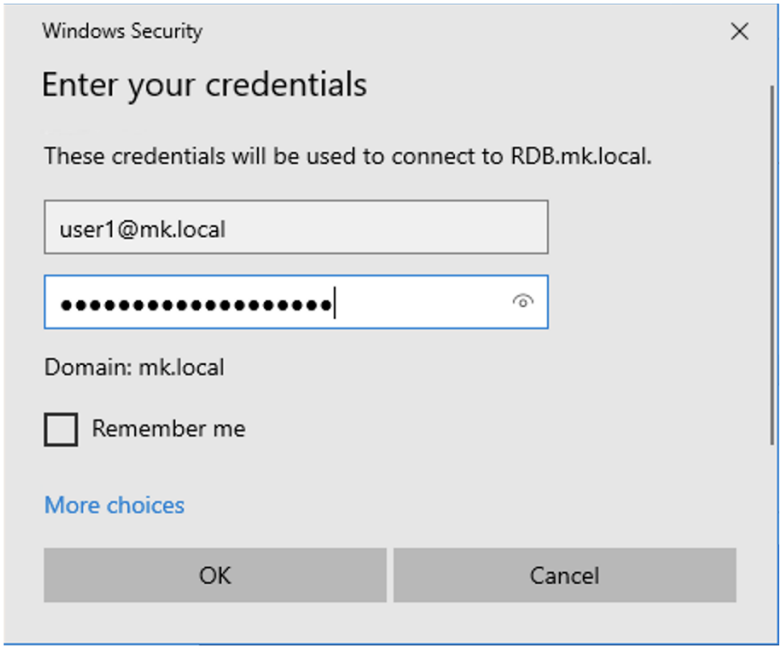
1. Open the RD Web Access URL saved in previous steps (e.g., `https://rdb.mk.local/RDWeb/`).
2. Enter a valid username and password and click *Sign in*. You can use the domain admin account to login, for example, `Administrator@mk.local`.
3. After logging in, the full collection of created desktop sessions is presented.



4. Click on the created `test-collection` icon to download the RDP connection file or immediately establish a connection.



5. Provide login credentials of one of the users specified in the domain.



Note

In this part of the manual, a general process for configuring Remote Desktop Services has been presented. To utilize Fudo Enterprise's functionality during connections, please follow the steps outlined in the subsequent part of the instruction.

Related topics:

- *RDP in Bastion Mode*
- *Authentication*
- *Integration with CERB server*

20.3.2 Setup Fudo Enterprise - Bastion Scenario (Recommended)

The Bastion scenario is the recommended setup for the RDS feature, as it requires minimal manual configuration on Fudo. In this scenario, you need to:

- create users via the RDS functionality to correspond with Active Directory users,
- add all servers included in the RDS Collection,
- configure an account for server authentication,
- set up a single listener in bastion mode paired with this account.

Note

This use case describes how to configure Fudo Enterprise using the Active Directory external authentication method. Please keep in mind that you can customize user authentication using any other method supported by Fudo Enterprise to align with your specific requirements, the methods typically used in your environment, and your work scenarios.

Configure external authentication method:

1. Login into your Fudo Enterprise Admin Panel.
2. Select *Settings* > *Authentication*.
3. In the **External authentication** tab click *Add external authentication*.
4. Enter unique name (e.g., `ActiveDirectory01`).
5. Set the *Bind address* to *Any*.
6. In the *General* section select *Active Directory*.
7. In the *Host* field provide the Domain Controller IP address (e.g., `10.0.136.1`).
8. Leave default port number: `389`.
9. Provide the name of the domain which will be used for authenticating users in Active Directory (e.g., `mk.local`).
10. In the *Credentials* fields provide the privileged account's login credentials used to access the Domain Controller.
11. Click *Save*.

Create User in Fudo:

1. Select *User Management* > *Users* and then click + *Add user*.
2. Enter the user name that matches the chosen user account in Active Directory (e.g., 'user1').
3. In the *Settings* tab, under the *Safes* section, select *portal*.
4. Click *Save*.
5. Go to the *Authentication* section and from the *Add authentication method* drop down list select *External authentication*.
6. Chose created in previous steps Active Directory method and click *Save*.
7. If necessary, please fill in the remaining parameters as needed for your specific configuration. For more details, please refer to the *Creating a User* section.
8. Click *Save and close*.

Configure Server with the role of Connection Broker:

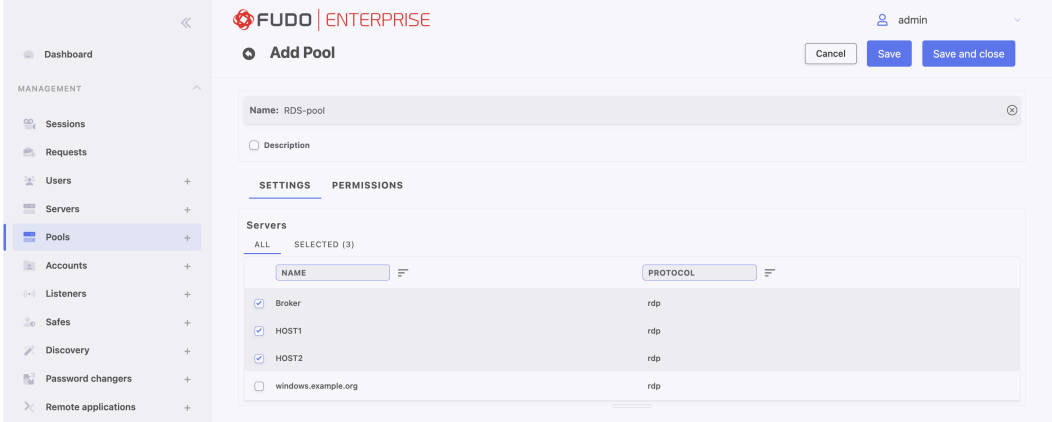
1. Select *Management* > *Servers* and then click + *Add server*.
2. Enter server's unique name (e.g., `Broker`).
3. In the *Permissions* section, add users allowed to manage this object.
4. In the *Settings* section on the list of available protocols select `RDP`.
5. Select the *TLS enabled* and the *NLA enabled* options.
6. In the *Destination* section select `IPv4` and enter IP address of the server selected during RDS setup for the RD Broker role (in our example, `RDB` server with IP `10.0.136.2`).
7. Click *Save and close*.

Configure Servers with the role of Session Hosts:

1. Select *Management* > *Servers* and then click *+ Add server*.
2. Enter server's unique name (e.g., `HOST1`).
3. In the *Permissions* section, add users allowed to manage this object.
4. In the *Settings* section on the list of available protocols select `RDP`.
5. Select the *TLS enabled* and the *NLA enabled* options.
6. In the *Destination* section select `IPv4` and enter server's IP address (in our example, `10.0.136.4`).
7. Click *Save and close*.
8. Repeat all the above steps to create second server with name `HOST2` and IP address `10.0.136.5`.

Configure Pool:

1. Select *Management* > *Pools* and then click *+ Add pool*.
2. Enter pool's unique name (e.g., `RDS-pool`).
3. In the *SETTINGS* tab select servers to be added to the pool including the broker (e.g., `HOST1, HOST2, BROKER`).
4. In the *PERMISSIONS* section, add users allowed to manage this object (e.g., `user1`).



6. Click *Save and close*.

Configure Account:

1. Select *Management* > *Accounts* and then click *+ Add account*.
2. Define object's name (e.g., `user1`).
3. In the *Type* section select *FORWARD*.
4. In the *Target* section select *Pool* button, and from the drop down list select Pool created in previous step (e.g., `RDS-pool`) to assign created account to this server pool.
5. Select *Forward domain* option to have the domain name included in the string identifying the user.
6. In the *Credentials* section provide domain's name (e.g., `ml.local`).

7. Click *Save*.

Configure Listener

1. Select *Management* > *Listeners* and then click *+ Add listener*.
2. Enter listener's unique name (e.g.,``rdp-broker-bastion``).
3. Go to *PERMISSIONS* tab and add users allowed to manage this listener (e.g., `user1`).
4. Go to *SETTINGS* tab and press the `RDP` button in the *Protocol* field.
5. Select the *TLS enabled* option to enable encryption.
6. Check the *NLA enabled* option for additional security.
7. In the *Connection mode* section, select `bastion`.
8. Set the local address to `10.0.58.238` or `Any`, and port `3389.`
9. In the *CA certificate* field, click *Generate certificate* to generate TLS certificate, or click *Upload* to upload server certificate file with private key pasted at the end of the file.
10. Click *Save and close*.

Configure Safe:

1. Select *Management* > *Safes* and then click *+ Add safe*.
2. Enter safe's unique name (e.g.,``rdp-safe``).
3. Click *Save* to save the object and proceed with further configuration.
4. Go to the *Users* tab to assign users allowed to access accounts assigned to this safe.
   - Click *Manage users*.
   - Mark the checkbox in front of the users' names to enable their server access through the monitored safe (e.g., `user1`).
   - Click *Save* to close the modal window.
5. Select *Accounts* tab to add *accounts* accessible through this safe.
   - Click *Manage accounts.*
   - Mark the checkbox in front of the accounts' names to add it (e.g., `user1`).
   - Click *Save* to close the modal window.
   - Select desired account and click *Manage listeners* to assign listener to account (e.g.,``rdp-broker-bastion``).
   - Click *Save* to close the modal window.
6. Click *Save and close* to save the safe configuration.

Establish a connection through the User Access Gateway:

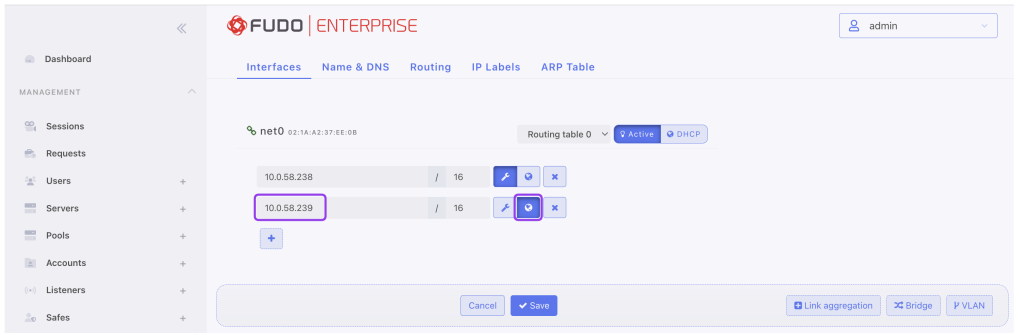
Warning

When establishing connections using the Remote Desktop Services, please use the *Native client* option. *Web client* feature is not functional for this type of scenario.

1. Log in to the Fudo Enterprise Access Gateway using `user1` as the username and password corresponding to the one configured in the Active Directory.

Note

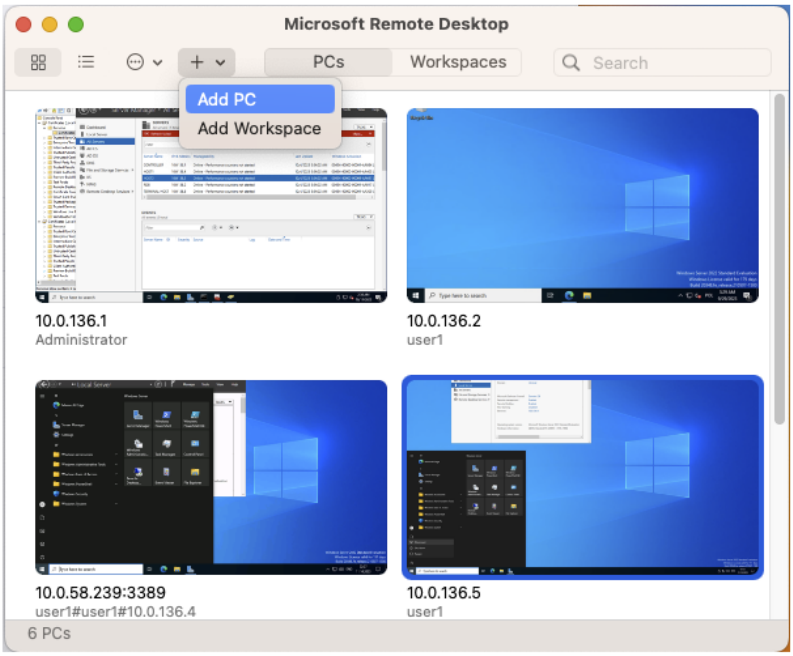
You can find the User Access Gateway address in the *Settings* > *Network configuration* menu tab.



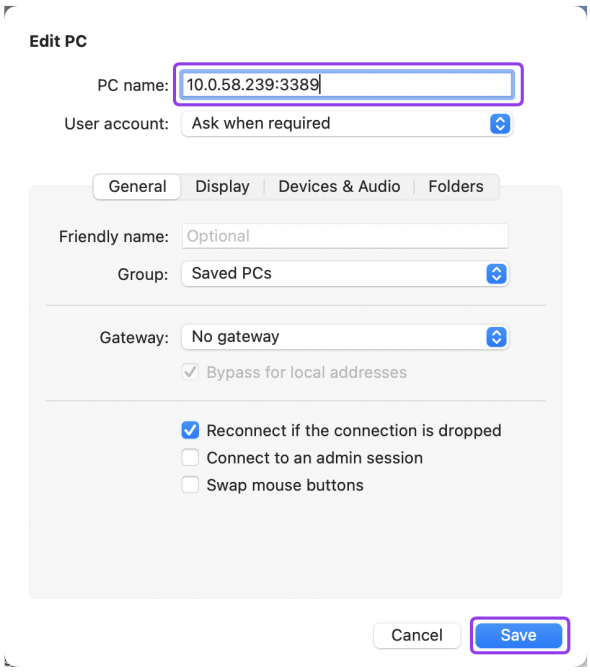
2. Hover the cursor over the `user1` account name, select *Native client* and click the *Connect* button to download the `.rdp` configuration file.
3. Open the downloaded file to establish a connection.
4. Enter the password for the `user1` account to log in to the server.

Redirect the connection through Fudo using RDP native client:

1. In order to redirect the connection through Fudo Enterprise, we need to use the Fudo Access Gateway address in the RDP client configuration.
2. Choose your favorite remote desktop client, such as Microsoft Remote Desktop, and follow its workflow to add a new PC for connection.
3. Following the example of Microsoft Remote Desktop, click the plus icon in the upper part of the window and select *Add PC*.

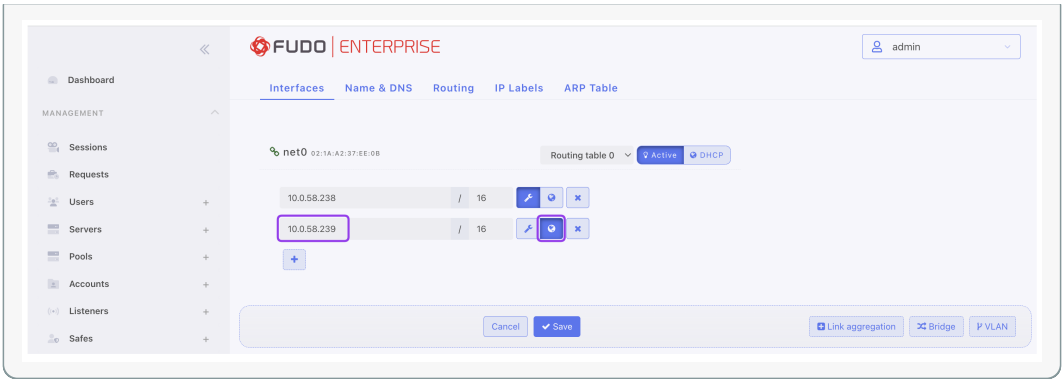


4. In the *PC Name* field, enter the address of the Fudo Enterprise Access Gateway followed by the port number and click *Add*.



Note

You can find the User Access Gateway address in the *Settings* > *Network configuration* menu tab.



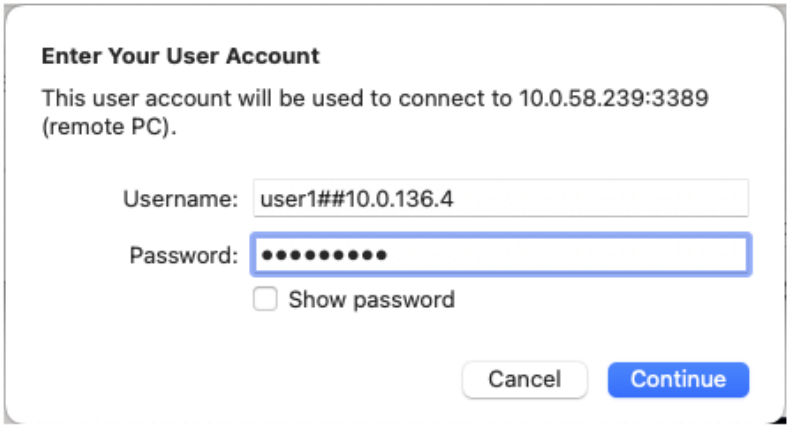
5. Connect to the added PC by providing the bastion login string in *Username* field and password in the *Password* field.

Note

- Please use the following pattern for the bastion login string: user name # account login on the target server # target server address (e.g., `user1#user1#10.0.136.4`).

You may specify the IP address of any server within the RDS collection as the `target server address` in the login string, and the broker will handle the connection redirection in accordance with RDS rules.

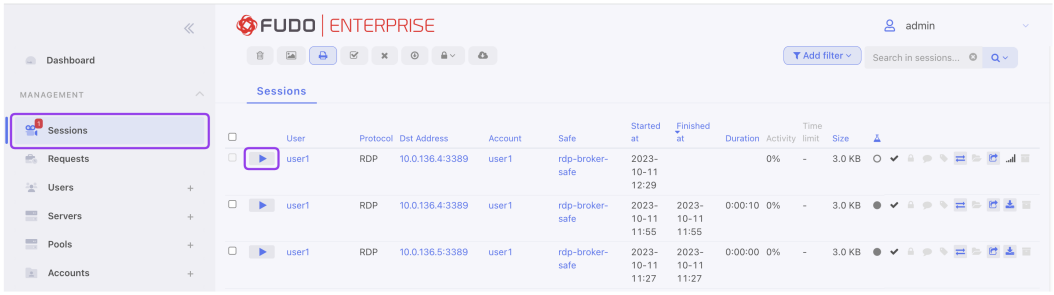
- You can skip the account login if it's the same as the user name, e.g, `user1##10.0.136.4`

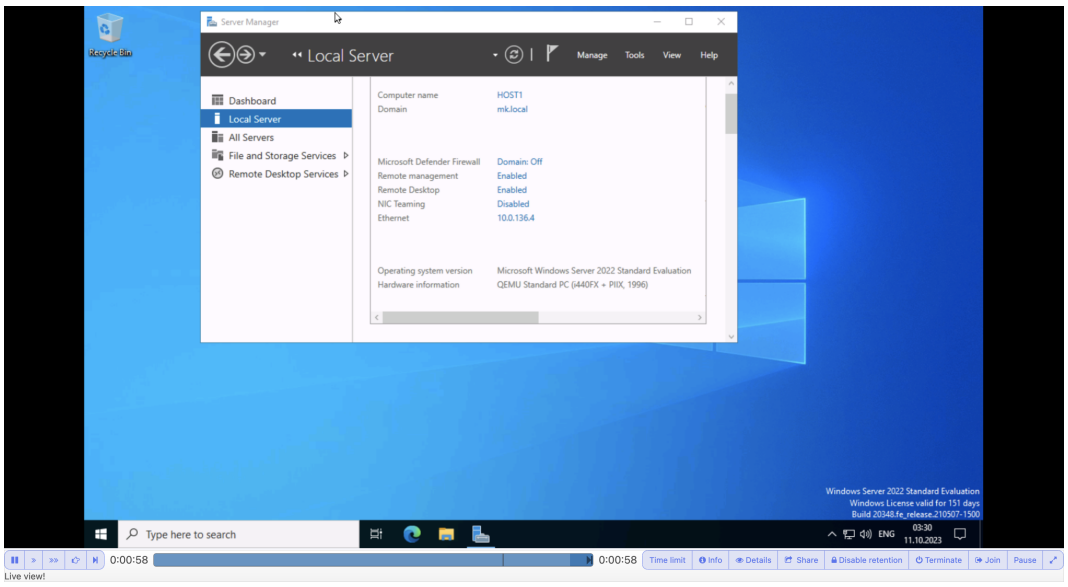


6. Remote Desktop client will establish connection with one of the servers from the RDS collection.

View the established session in the Fudo Enterprise Admin Panel:

1. Login into your Fudo Enterprise Admin Panel.
2. Select *Sessions* and run the session preview.
3. Find desired session and click the play icon next to it.





Related topics:

- *Setup Fudo Enterprise - Bastion Scenario (Recommended)*
- *RDP in Bastion Mode*
- *Authentication*
- *Network Interfaces Configuration*

20.3.3 Setup Fudo Enterprise - Proxy Scenario

The proxy scenario for RDS requires more manual configuration in Fudo Enterprise compared to the bastion scenario but offers simplified connection method. Each server in the RDS Collection must have its own proxy listener on Fudo Enterprise, assigned a dedicated IP address with port 3389.

In this setup, you need to:

- create users through the RDS functionality to align with Active Directory users,
- add all servers in the RDS Collection,
- configure an account for each server,
- create a listener in proxy mode for each server.

Note

This use case describes how to configure Fudo Enterprise using the Active Directory external authentication method. Please keep in mind that you can customize user authentication using any other method supported by Fudo Enterprise to align with your specific requirements, the methods typically used in your environment, and your work scenarios.

Configure external authentication method:

1. Login into your Fudo Enterprise Admin Panel.
2. Select *Settings* > *Authentication*.
3. In the **External authentication** tab click *Add external authentication*.
4. Enter unique name (e.g., `ActiveDirectory01`).
5. Set the *Bind address* to *Any*.
6. In the *General* section select *Active Directory*.
7. In the *Host* field provide the Domain Controller IP address (e.g., `10.0.136.1`).
8. Leave default port number: `389`.
9. Provide the name of the domain which will be used for authenticating users in Active Directory (e.g., `mk.local`).
10. In the *Credentials* fields provide the privileged account's login credentials used to access the Domain Controller.
11. Click *Save*.

Create User in Fudo:

1. Select *User Management* > *Users* and then click + *Add user*.
2. Enter the user name that matches the chosen user account in Active Directory (e.g., `user1`).
3. In the *Settings* tab, under the *Safes* section, select *portal*.
4. Click *Save*.
5. Go to the *Authentication* section and from the *Add authentication method* drop down list select *External authentication*.
6. Chose created in previous steps Active Directory method and click *Save*.
7. If necessary, please fill in the remaining parameters as needed for your specific configuration. For more details, please refer to the *Creating a User* section.
8. Click *Save and close*.

Configure Server with the role of Connection Broker:

1. Select *Management* > *Servers* and then click + *Add server*.
2. Enter server's unique name (e.g., `Broker`).
3. In the *Permissions* section, add users allowed to manage this object.
4. In the *Settings* section on the list of available protocols select `RDP`.
5. Select the *TLS enabled* and the *NLA enabled* options.

6. In the *Destination* section select `IPv4` and enter IP address of the server selected during RDS setup for the RD Broker role (in our example, `RDB` server with IP `10.0.136.2`).
7. Click *Save and close*.

Configure Servers with the role of Session Hosts:

1. Select *Management* > *Servers* and then click + *Add server*.
2. Enter server's unique name (e.g., `HOST1`).
3. In the *Permissions* section, add users allowed to manage this object.
4. In the *Settings* section on the list of available protocols select `RDP.`
5. Select the *TLS enabled* and the *NLA enabled* options.
6. In the *Destination* section select `IPv4` and enter server's IP address (in our example, `10.0.136.4`).
7. Click *Save and close*.
8. Repeat all the above steps to create second server with name `HOST2` and IP address `10.0.136.5`.

Configure Accounts:

1. Select *Management* > *Accounts* and then click + *Add account*.
2. Define object's name (e.g., `rds-host1-forward`).
3. In the *Type* section select *FORWARD*.
4. In the *Target* section select *Server* button, and from the drop down list select Server created in previous step (e.g., `HOST1`) to assign created account to this server.
5. Click *Save*.
6. Repeat all the above steps to create accounts for `HOST2` and `BROKER` servers (e.g., `rds-host2-forward, rds-broker-forward`).

Configure Listeners

1. Select *Management* > *Listeners* and then click + *Add listener*.
2. Enter listener's unique name (e.g.,``rdp-proxy-01``).
3. Go to *PERMISSIONS* tab and add users allowed to manage this listener (e.g., `user1`).
4. Go to *SETTINGS* tab and press the `RDP` button in the *Protocol* field.
5. Select the *TLS enabled* option to enable encryption.
6. Check the *NLA enabled* option for additional security.
7. In the *Connection mode* section, select *proxy*.
8. Set the local address to dedicated IP address (e.g., `10.0.58.238`), and port `3389.`

> **Note**
>
> To learn how to manage additional IP addresses, please refer to the *Network Interfaces Configuration* section.

9. In the *CA certificate* field, click *Generate certificate* to generate TLS certificate, or click *Upload* to upload server certificate file with private key pasted at the end of the file.
10. Click *Save and close*.
11. Repeat all the above steps to create additional listeners with a dedicated IP address and port 3389 for `HOST2` and `BROKER` servers.

Configure Safe:

1. Select *Management* > *Safes* and then click *+ Add safe*.
2. Enter safe's unique name (e.g.,``rdp-safe``).
3. Click *Save* to save the object and proceed with further configuration.
4. Go to the *Users* tab to assign users allowed to access accounts assigned to this safe.
   - Click *Manage users*.
   - Mark the checkbox in front of the users' names to enable their server access through the monitored safe (e.g., `user1`).
   - Click *Save* to close the modal window.
5. Select *Accounts* tab to add *accounts* accessible through this safe.
   - Click *Manage accounts*.
   - Mark the checkboxes next to each account name created in the previous steps to add it (e.g., `rds-host1-forward`, `rds-host2-forward`, `rds-broker-forward`).
   - Click *Save* to close the modal window.
   - Select each account in turn and click *Manage listeners* to assign a listener to it (e.g.,``rdp-proxy-01, rdp-proxy-02, rdp-proxy-03``).
   - Click *Save* to close the modal window.
6. Click *Save and close* to save the safe configuration.

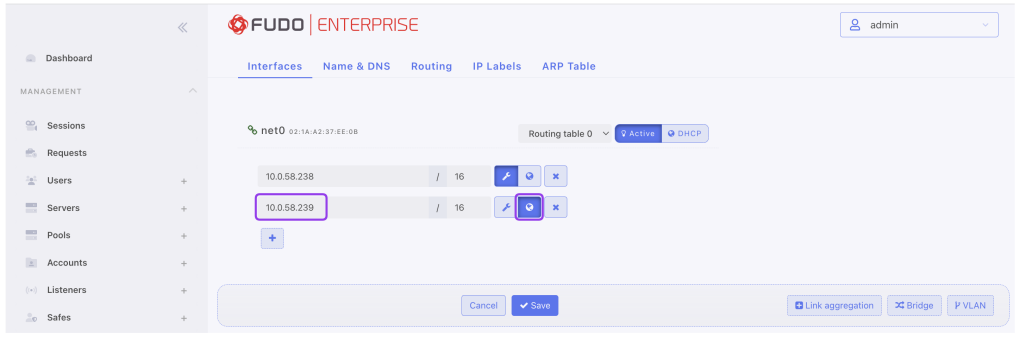
Establish a connection through the User Access Gateway:

> **Warning**
>
> When establishing connections using the Remote Desktop Services, please use the *Native client* option. *Web client* feature is not functional for this type of scenario.

1. Log in to the Fudo Enterprise Access Gateway using `user1` as the username and password corresponding to the one configured in the Active Directory.

Note

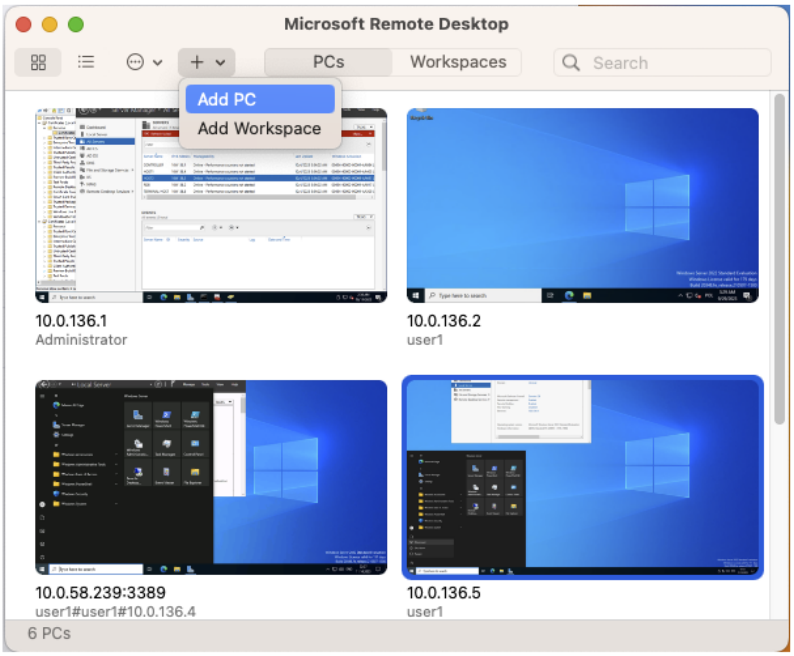
You can find the User Access Gateway address in the *Settings* > *Network configuration* menu tab.



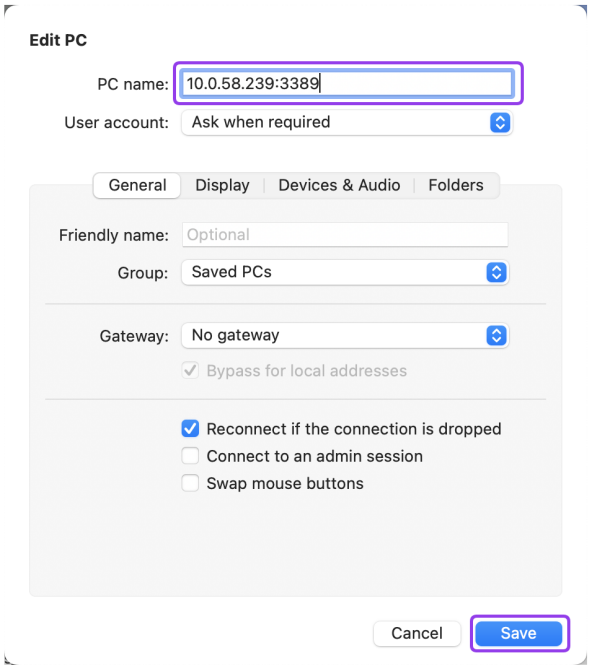
2. Hover the cursor over the `user1` account name, select *Native client* and click the *Connect* button to download the `.rdp` configuration file.
3. Open the downloaded file to establish a connection.
4. Enter the password for the `user1` account to log in to the server.

Redirect the connection through Fudo using RDP native client:

1. In order to redirect the connection through Fudo Enterprise, we need to use the Fudo Access Gateway address in the RDP client configuration.
2. Choose your favorite remote desktop client, such as Microsoft Remote Desktop, and follow its workflow to add a new PC for connection.
3. Following the example of Microsoft Remote Desktop, click the plus icon in the upper part of the window and select *Add PC*.

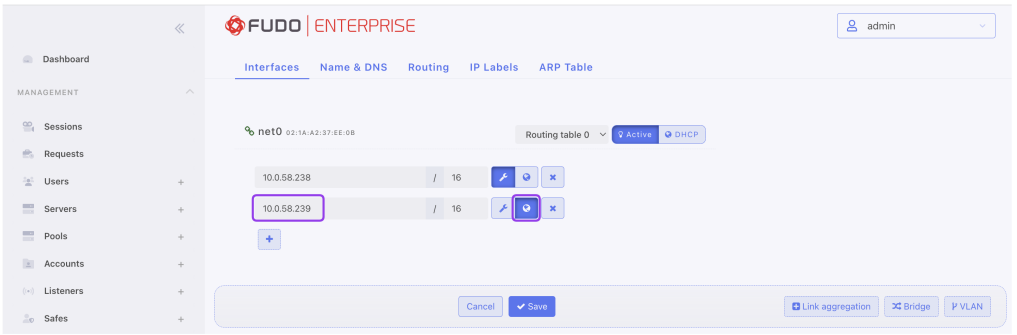


4. In the *PC Name* field, enter the address of the Fudo Enterprise Access Gateway followed by the port number and click *Add*.



Note

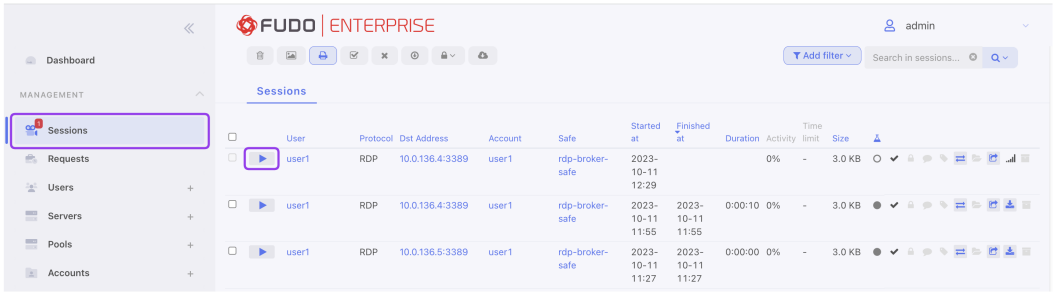
You can find the User Access Gateway address in the *Settings* > *Network configuration* menu tab.

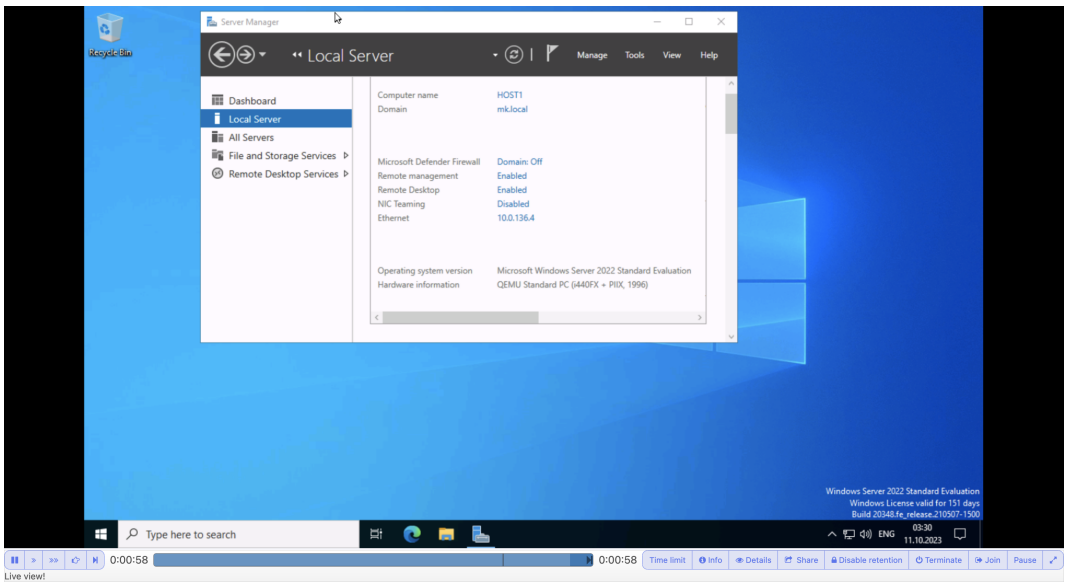


5. Connect to the added PC by providing the login and password of the `user1` set in the Active Directory environment (according to method selected while creating user in Fudo Enterprise).
6. Remote Desktop client will establish connection with one of the servers from the RDS collection.

View the established session in the Fudo Enterprise Admin Panel:

1. Login into your Fudo Enterprise Admin Panel.
2. Select *Sessions* and run the session preview.
3. Find desired session and click the play icon next to it.





Related topics:

- *Setup Fudo Enterprise - Bastion Scenario (Recommended)*
- *Authentication*
- *Network Interfaces Configuration*

20.4 Custom RDP Hostname in the Session Title

> **Note**
>
> Please note that this is a general guide, and specific details may vary depending on your Windows Server setup. Refer to the Windows Server documentation for precise configuration steps.

This use case describes how to configure a custom hostname displayed in the RDP client title bar for sessions started from the User Access Gateway using the *Native client* option.

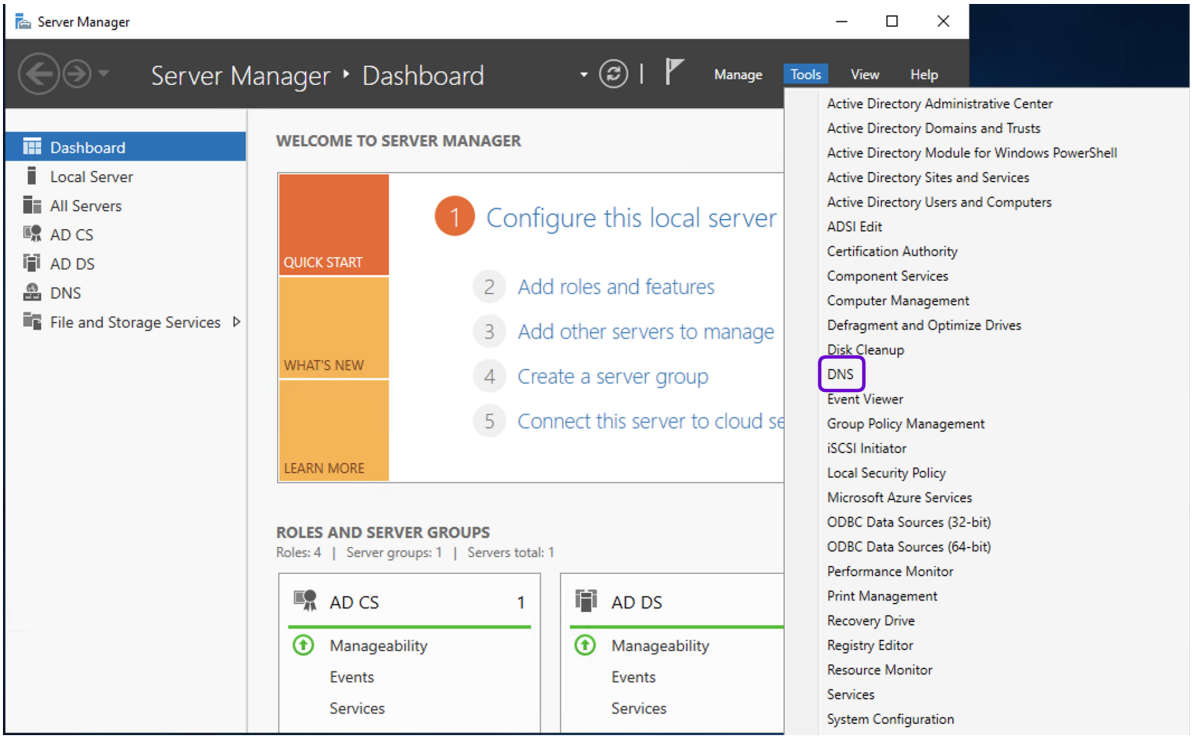
This configuration enables clear, user-friendly RDP session identification by preserving custom hostnames through Fudo Enterprise.

> **Warning**
>
> Wildcard must be created on DNS side. Fudo Enterprise does NOT generate DNS records.

20.4.1 DNS Configuration in Windows DNS Manager

Create Subdomain for Wildcard Usage:

1. Open the *Server Manager* application.
2. Click *Tools* button on the upper right corner of the window to expand the menu list and select *DNS*.



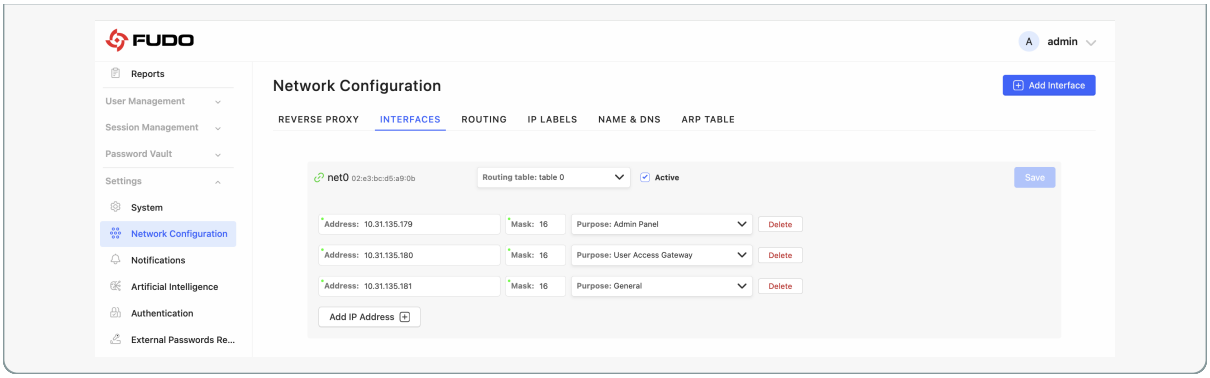
3. Go to *Forward Lookup Zones*, right click on the domain name (e.g., `main.lab`) and select *New Domain*.
4. Provide the *New DNS domain name* (e.g., `dev`).
5. Click *OK*.

Create Wildcard A Record:

1. Right click on the added zone name (`dev`) and select *New Host (A or AAAA)*.
2. In the *Name* field, type an asterisk (`*`).
3. In the *IP address* field, type the Fudo Enterprise User Access Gateway address (e.g., `10.31.135.180`).
4. Optionally, you can select the *Create associated pointer (PTR) record* option.
5. Click *Add Host*.

Note

You can check the address assigned for User Access Gateway in the *Settings* > *Network Configuration* > *Interfaces*. Ensure that the interface is *Active*.



20.4.2 Fudo Enterprise Configuration

1. Select *Management* > *Listeners* and click the selected *RDP listener's* name to edit it.
2. In the listener configuration, locate the *RDP config domain* field.
3. Enter the domain that should be appended to the generated hostname (e.g., `jdoe.dev.main.lab`).
4. Click *Save*.

Note

- When the *RDP config domain* field is configured, the listener uses hostnames from the specified domain. Leave this field empty if you do not want to use custom hostnames for listener.
- Each RDP listener can use a different custom domain.

20.4.3 Start RDP Connection

1. Sign in to the User Access Gateway.
2. Navigate to *Resources*.
3. Find desired RDP account and server, hover your mouse over to show more options.
4. Select the *Native client* button.
5. Choose the listener, via which you want to connect.
6. Click *Connect*.
7. *Google Chrome* will automatically download generated `.rdp` file.
8. Open the downloaded `.rdp` file using your native RDP client (e.g., Remote Desktop Connection for Windows, Windows App for macOS.

20.4.4 Result

When *RDP config domain* is configured, the generated `.rdp` file contains a hostname built with that domain in the `full address` entry. As a result, the RDP client title bar shows a custom hostname that is easier for the user to identify. Session title shows configured hostname (e.g., `server-name - 10.0.242.25.jdoe.dev.main.lab:2222`).

Note

If the *RDP config domain* field is left empty, the generated RDP configuration uses the default connection address, as in previous versions.

RDP File Example

```
full address:s:10.0.234.1.jdoe.dev.main.lab:2222
username:s:<generated_username>
prompt for credentials:i:1
```

Where:

- `10.0.234.1` – target server IP
- `jdoe.dev.main.lab` – custom hostname
- `2222` – listener port
- `generated_username` – temporary / OTP username from Fudo Enterprise

Note

The custom RDP hostname is a DNS label pointing to the Fudo Enterprise listener, not to the target server itself.

Related topics:

- *Setting up the RDP Listener*
- *Microsoft Remote Desktop*
- *Remote Desktop Services Configuration on Windows Server for Fudo Enterprise*

20.5 Managing RDP Server Certificates in Windows Server

While *creating RDP Server* in Fudo Enterprise, you can specify the server verification method by getting the server certificate or importing the CA certificate. You can follow below manual to manage mentioned certificates in the Windows Server environment.

20.5.1 Locating the Server Certificate in Windows Server

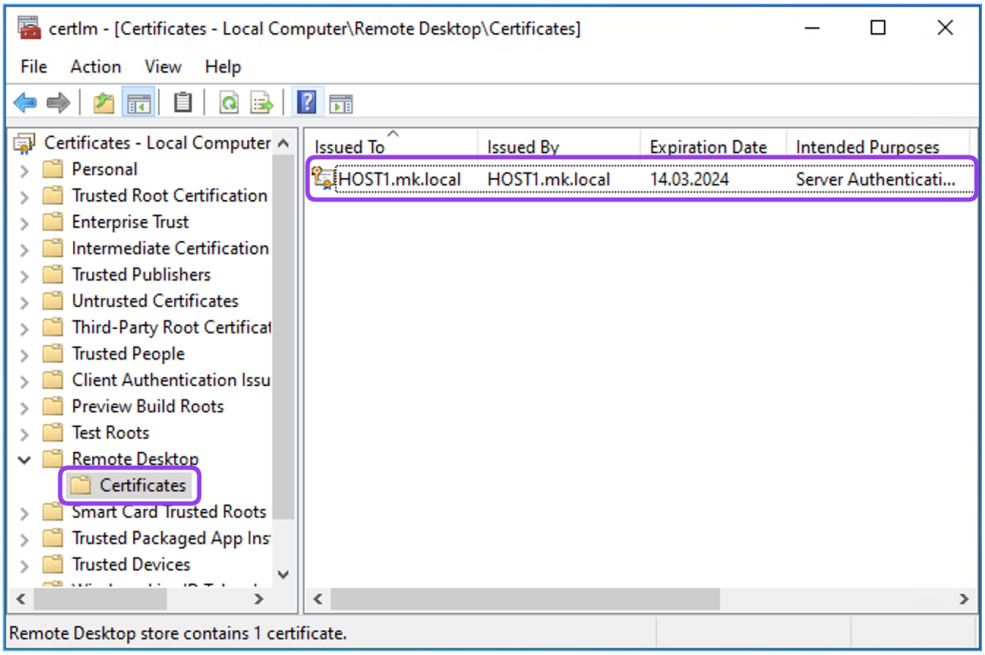
Please follow one of below scenarios to localize the certificate retrieved by Fudo Enterprise from the Widnows Server during the RDP server creation.

Locating the Server Certificate in Certificate Manager Tool:

You can localize the certificate retrieved by Fudo Enterprise from the Widnows Server in the Certificate Manager tool. To view the certificate, please follow below steps:

1. Select *Run* from the *Start menu* in Widnows Server, and then enter `certlm.msc`.
2. The Certificate Manager tool for the local device appears.

3. To view your certificate, expand the *Remote Desktop* > *Certificates* directory under the *Certificates - Local Computer* in the left pane of the Certificate Manager tool window.



Locating the Server Certificate by the Serial Number:

You can also localize certificate used by Fudo Enterprise by extracting certificate's serial number.

1. After clicking the 'Get certificate' button, Fudo Enterprise connects to the specified address and port to retrieve the certificate. A similar action can be performed from the command line by invoking below command:

```
openssl s_client -connect adres:port
```

Example:

```
openssl s_client -connect 10.0.133.4:3389
```

2. In the response you will receive the certificate that you can use to extract the certificate serial number by typing below command and providing the obtained certificate content:

```
c x509 -noout -serial

-----BEGIN CERTIFICATE-----
MIIChbdygdu656sdf65ac55mpn1PmpBK/
↪7OWFeh+xjANBgkqhkiG9w0BAQsFADAZ
MRcwFQYDVQQDEw5IT1NUMS5tay5sb2NhbDAeFw0yMzA5MTMxNzA2NTRaFw0yNDAz
MTQxNzA2NTRaMBkxFzAVcas7c6c6sh83uydtLm1rLmxvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2ngYkoMa4dgLgGl1+G+m2UEAIH/
↪6ttyQep5u
tUYkxKeuqpn9AWnYP8To1fornJN387ddhcy76d7jchc8Q093RWVb2cMKKjgOAW9w
```

(continues on next page)

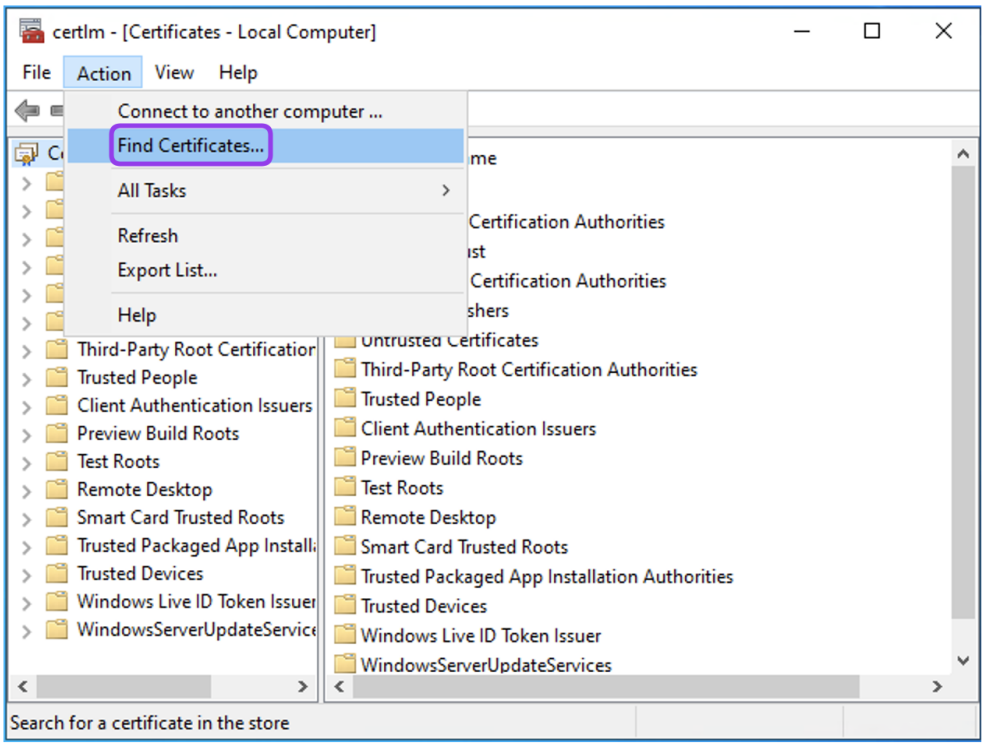
(continued from previous page)

```
qLFW+WrLEUPY8hYvsCFYgFH3HOHhKLEoWBN5qHH7vjIiW3RbOY7xeGb9xOFWItQX
mbF6sucGdlH+OsjepxMLPVh3Qpb2WQ18kSQGyS1ocbJxOWST9sH4MQkRVFL3rkxN
f7/
 ↪qdJcdM6sFxEJTdp3OCITRfbORXacl84bStjW2MJzvJRqr94xDHonRdIM9tUka
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-----
```

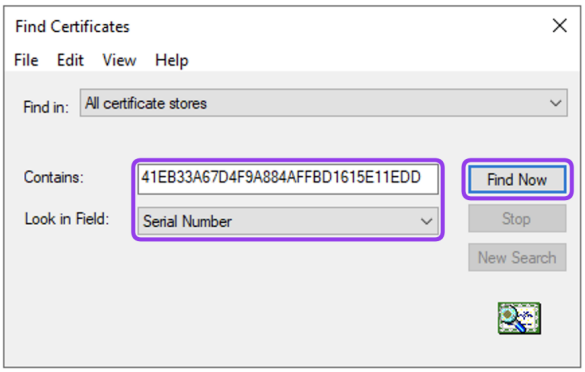
3. This will result in extracting the certificate's serial number that you can use to search the exact certificate in the Certificate Manager tool.

   ```
   serial=41EB33A67D4F9A884AFFBD1615E11EDD
   ```

4. Copy extracted serial number and go to the Windows Server.
5. Select *Run* from the *Start menu*, and then enter `certlm.msc` to open the Certificate Manager tool.
6. Go to *Action* > *Find Certificates...*



7. Provide copied serial number in the *Contains* field and select *Serial Number* from the *Look in Field* drop down list.



8. Click *Find Now*.

20.5.2 Providing the CA Certificate

Note

- This is a conceptual guide that outlines the fundamental setup of a CA for the RDP protocol. The necessary steps may vary depending on the initial settings of the environment in which you are working.
- To prepare CA certificate to be used in Fudo Enterprise it is needed to deploy internal Certificate Authority on the network with an RDP certificate template to issue RDP certificates.

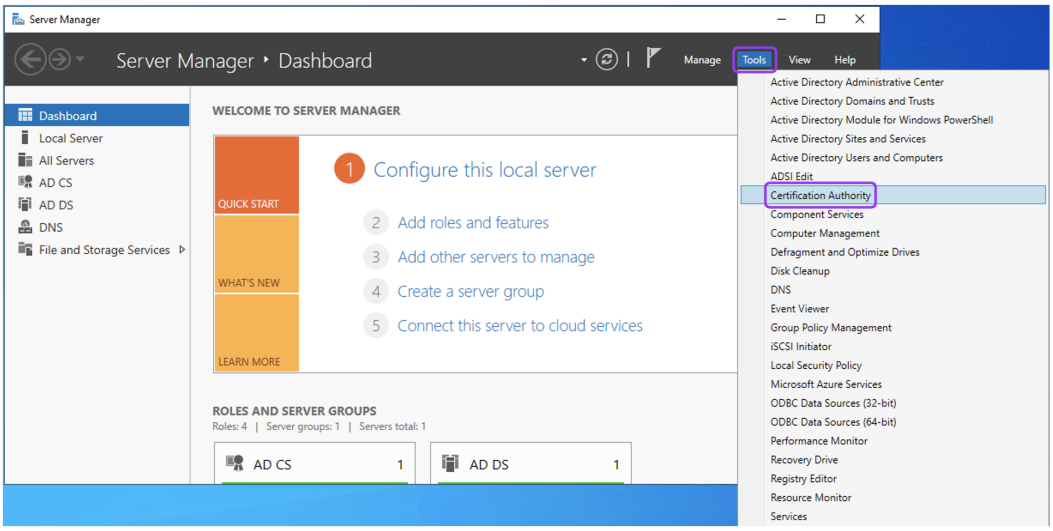
Install the Certificate Authority on Windows Server:

To install the Certificate Authority on Windows Server, follow the default configuration as specified in the manufacturer's manual.

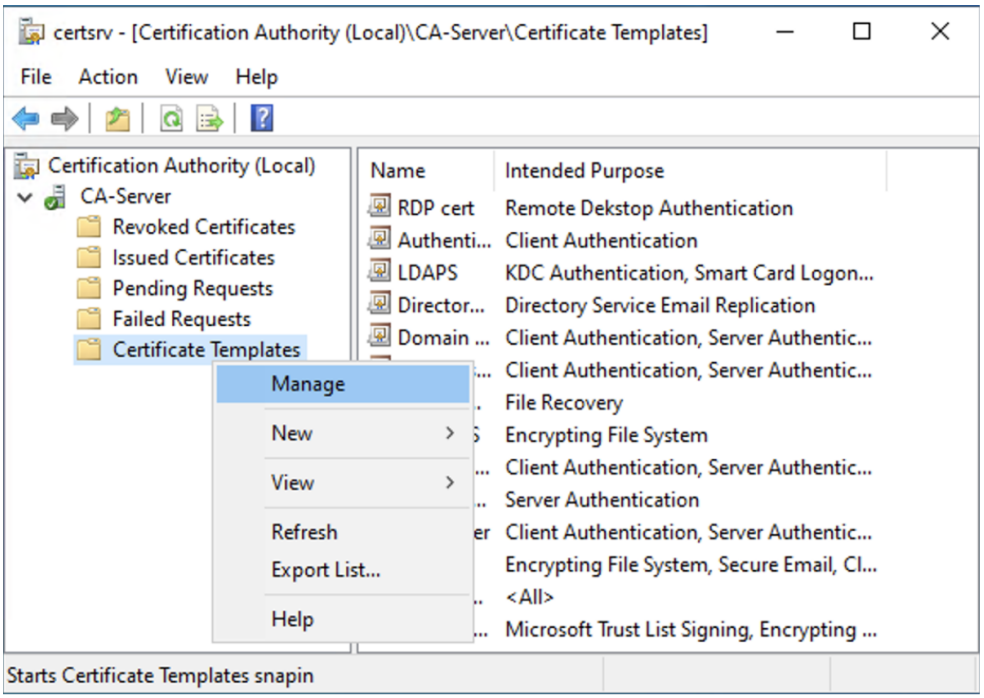
> **Note**
>
> For the procedure outlined in the manual below, the *Enterprise CA* option was selected.

Create a Template for RDP Certificate:

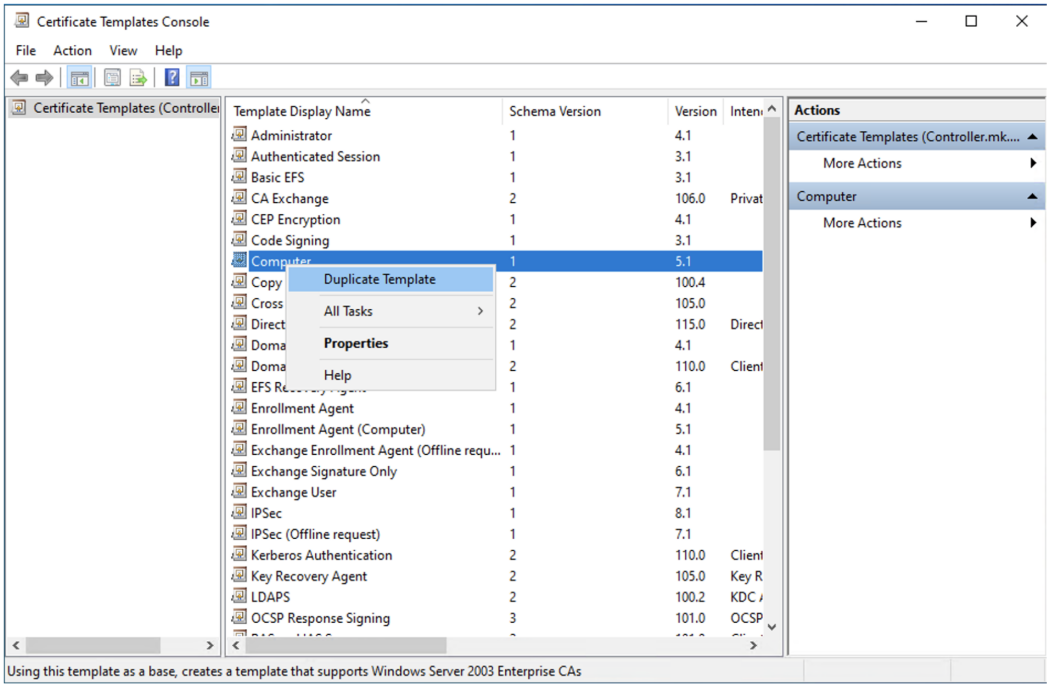
1. Open the Certificate Authority from the *Server Manager* by clicking *Tools* > *Certification Authority* in the upper right corner of the window.



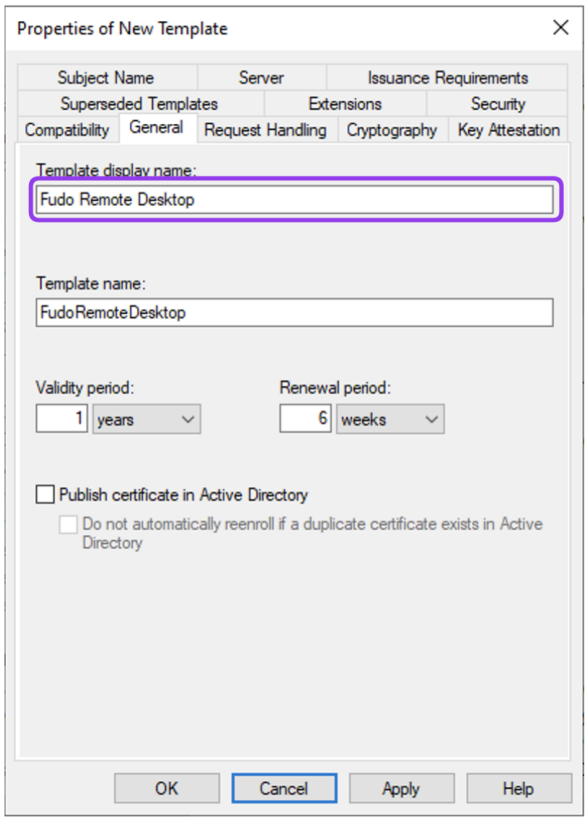
2. Right click on the *Certificate Template* and choose *Manage*.



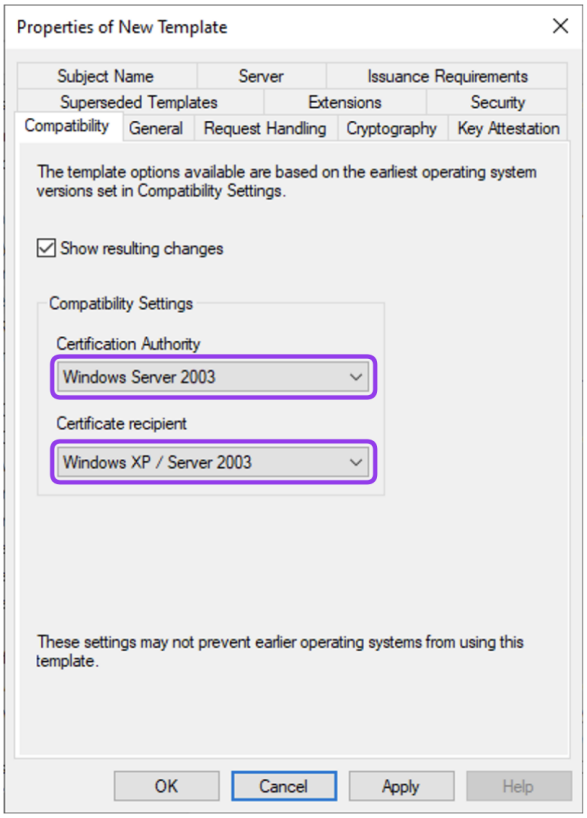
3. Find the *Computer* template, right click on it and choose *Duplicate Template*.



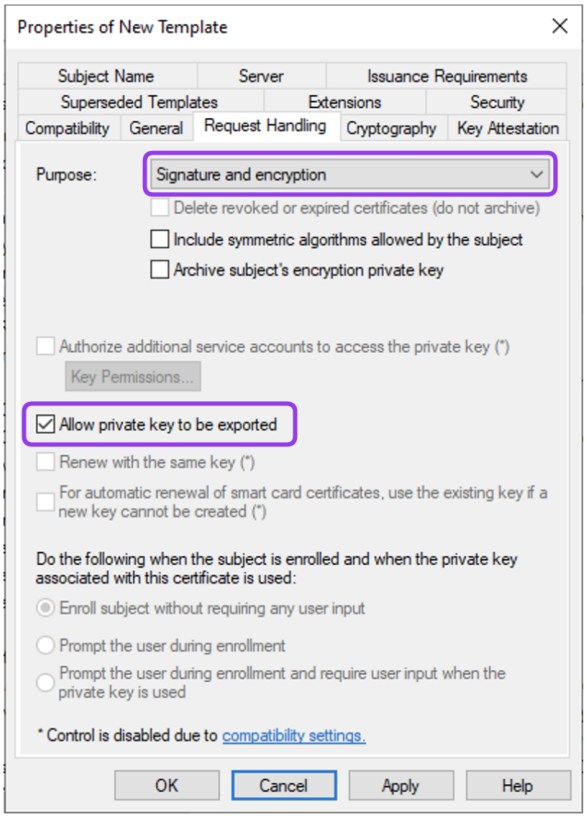
4. In the *General* tab, enter the name for new template and specify the validity and renewal period according to your needs.



5. In the *Compatibility* tab, choose *Windows Server 2003* from the `Certification Authority` drop-down list and `Windows XP/ Server 2003` from the *Certificate recipient* drop-down list.

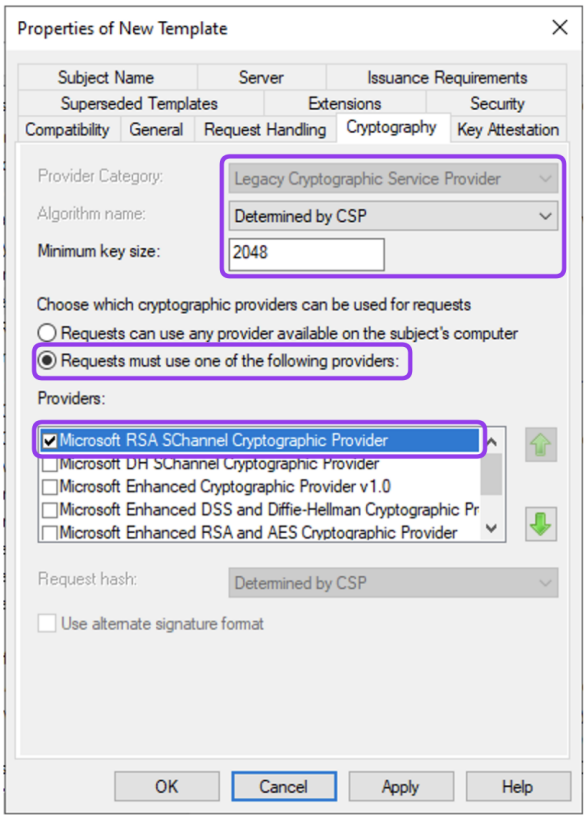


6. In the *Request Handling* tab, set the *Purpose* to the *Signature and encryption* and check the *Allow private key to be exported*.

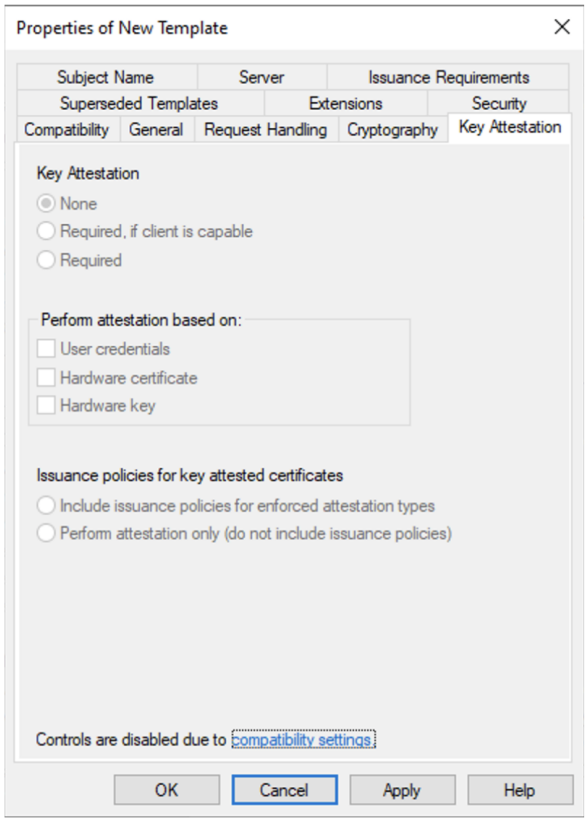


7. In the *Cryptography* tab, choose:

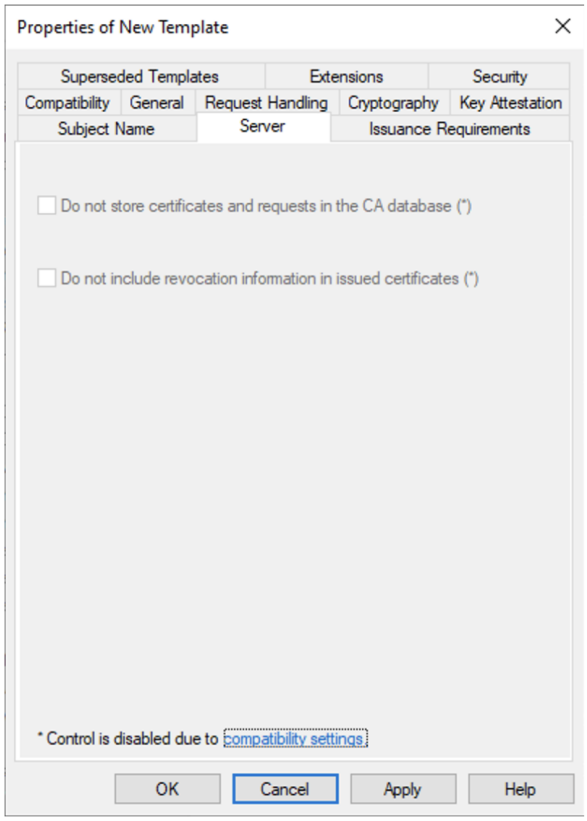
- set the *Provider Category* to *Legacy Cryptography Service Provider*,
- set the *Algorithm name* to *Determined by CSP*,
- set the *Minimum Key Size* according to organisation security requirement (e.g., 1024).
- choose the *Request must use one of the following providers* option and select the *Microsoft RSA SChannel Cryptographic Provider*.



8. In the *Key Attestation* tab, leave default settings.



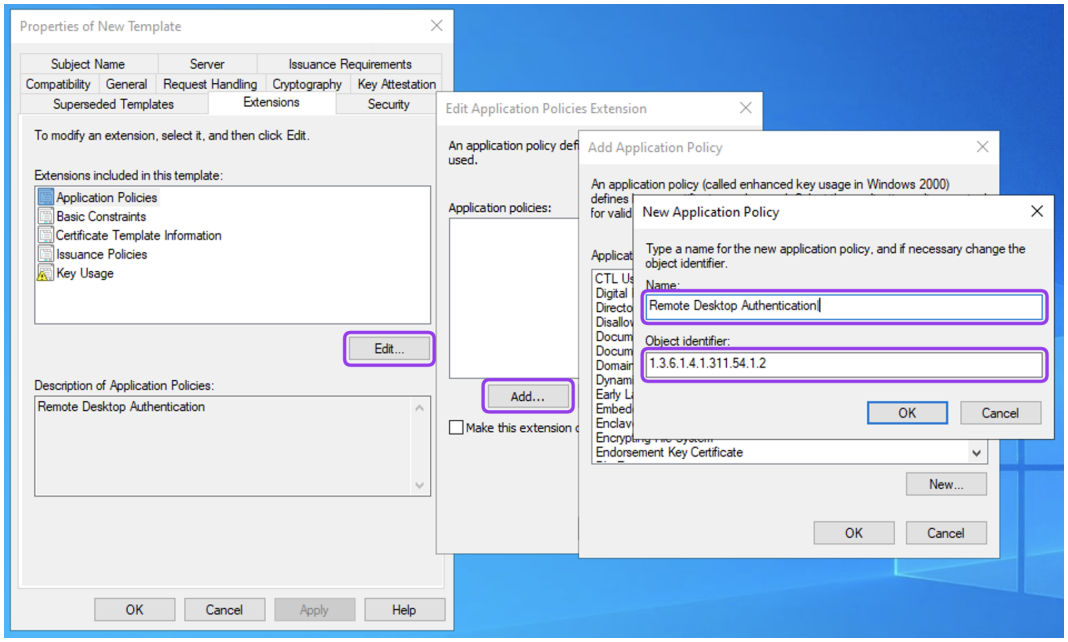
9. In the *Server* tab, leave default settings.



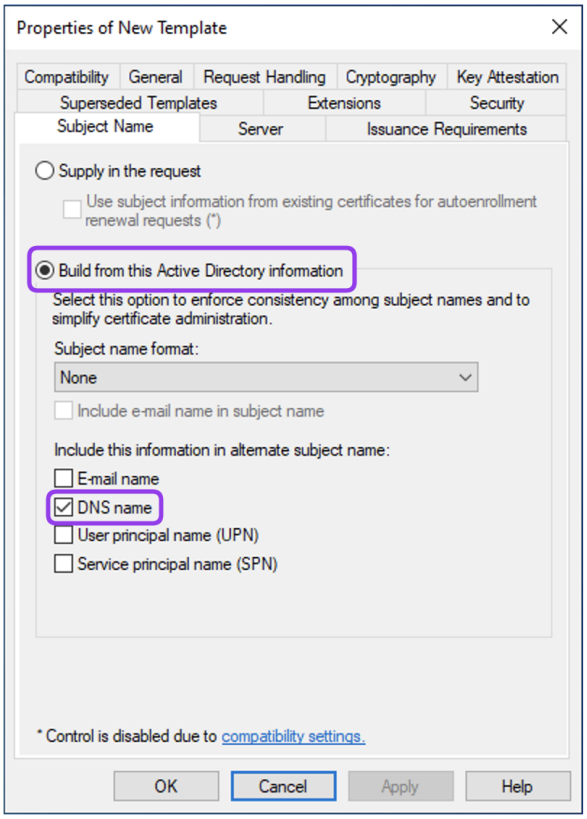
10. In the 'Security' tab, add the computers and groups you want to be able to enroll for this template. Check if group or user you are using has the *Read,*

Write, and *Enroll* permissions enabled. It is needed to request the certificate using this template in the next steps.

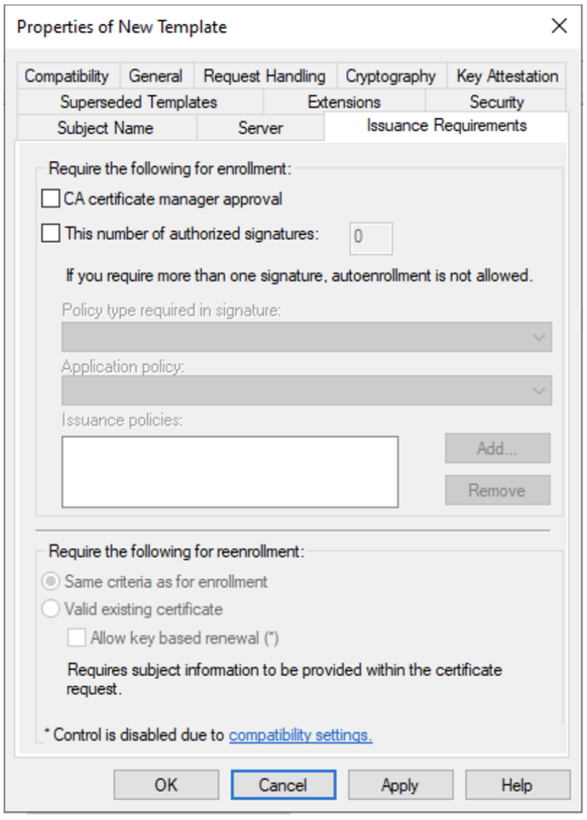
11. In the *Extensions* tab, edit the *Application Policies*.
12. Remove the *Server Authentication* and *Client Authentication* policies.
13. Add new policy by clicking *Add*, and *New* in the next window.
14. In the Name field enter `Remote Desktop Authentication` and in the *Object identifier* field type `1.3.6.1.4.1.311.54.1.2`.



15. Click three times *OK* to return to the *Properties of New Template* window.
16. In the *Subject Name* tab, select *Build from this Active Directory information* option and next the *DNS name*.

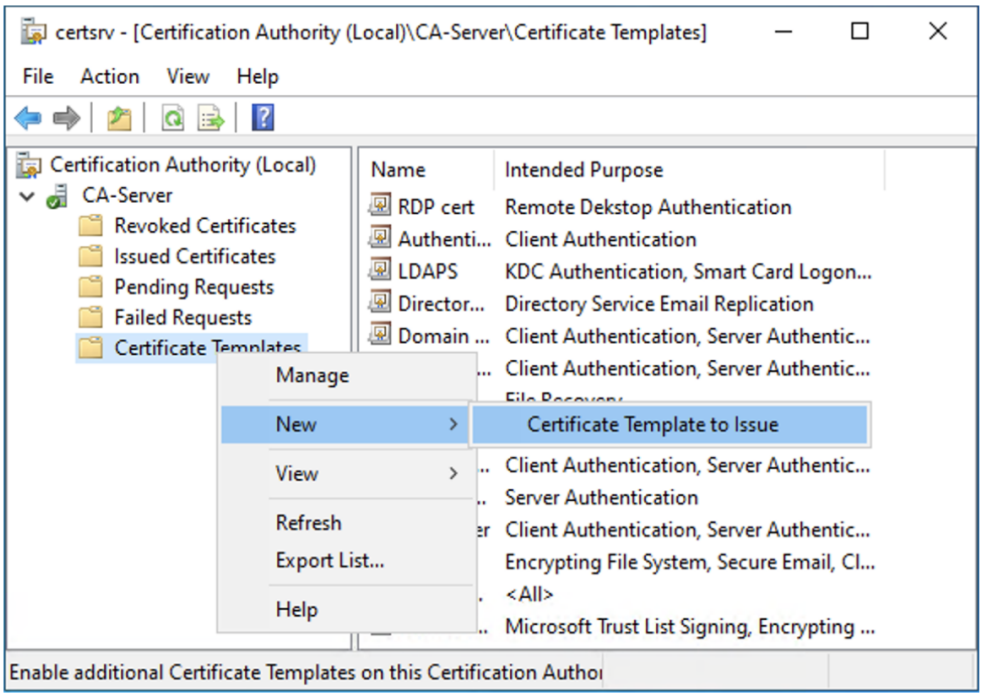


17. In the *Issuance Requirements* tab, leave default settings.

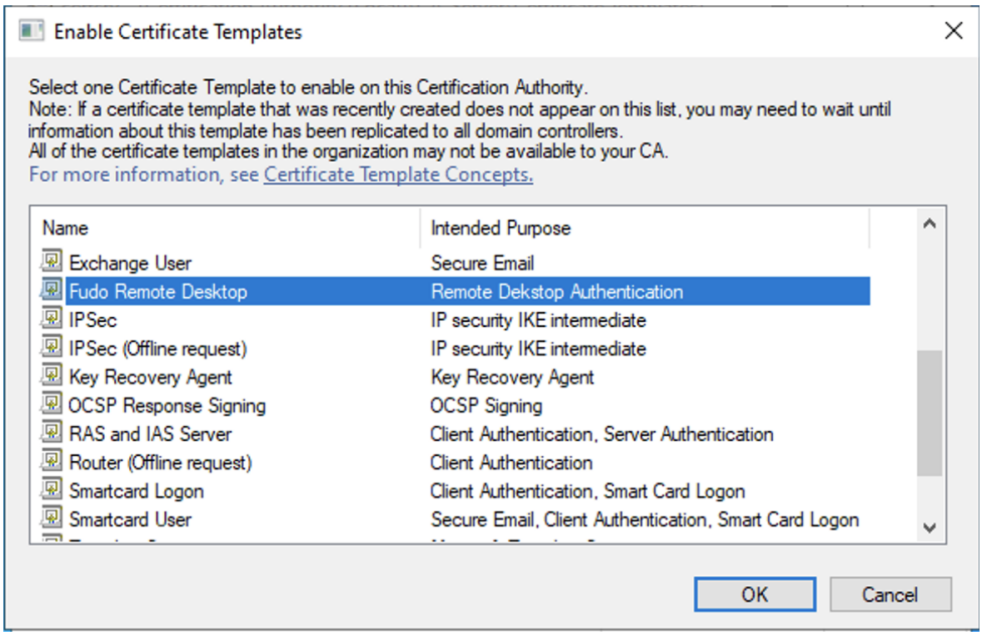


18. Click *OK* to save created template. Close the *Certificate Templates Console*.

19. Go back to the *Certification Authority* window. Right click on the *Certificate Template* and choose *New* > *Certificate Template to Issue*.



20. Select created template and click *OK*.

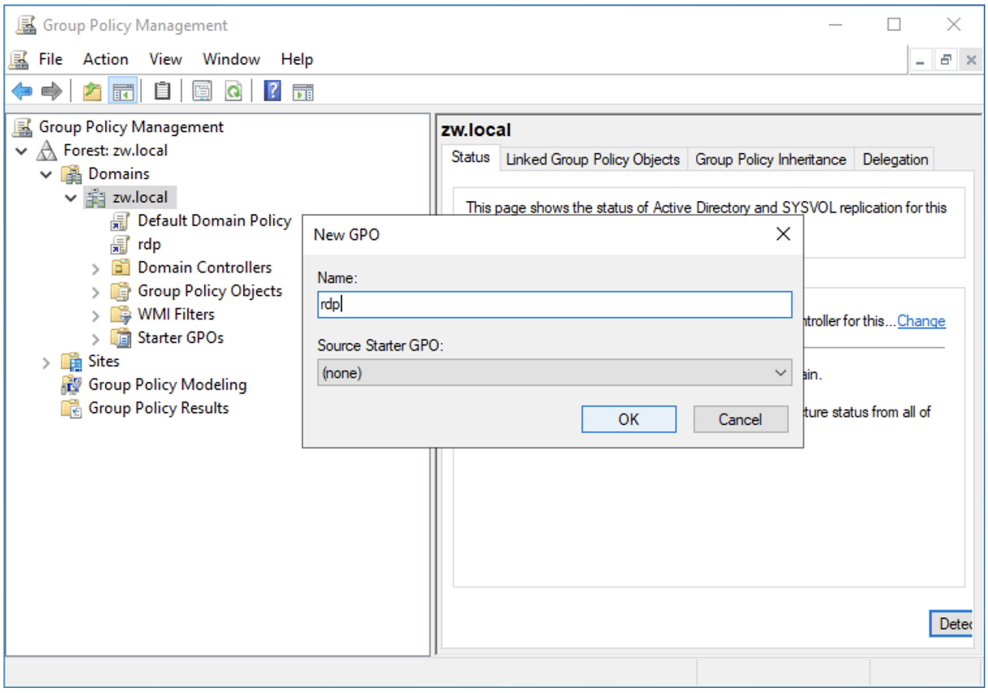


Configure a GPO to Deploy the Template

1. Press `Win + R`, type `gpmc.msc`, and press *Enter* to open the *Group Policy Management* on the server.
2. Create new Group Policy Object (GPO), or navigate to the GPO, you are going to edit. In this example we will create new one.
3. Right click on the domain name and choose *Create a GPO in this domain, and*

Link it here...

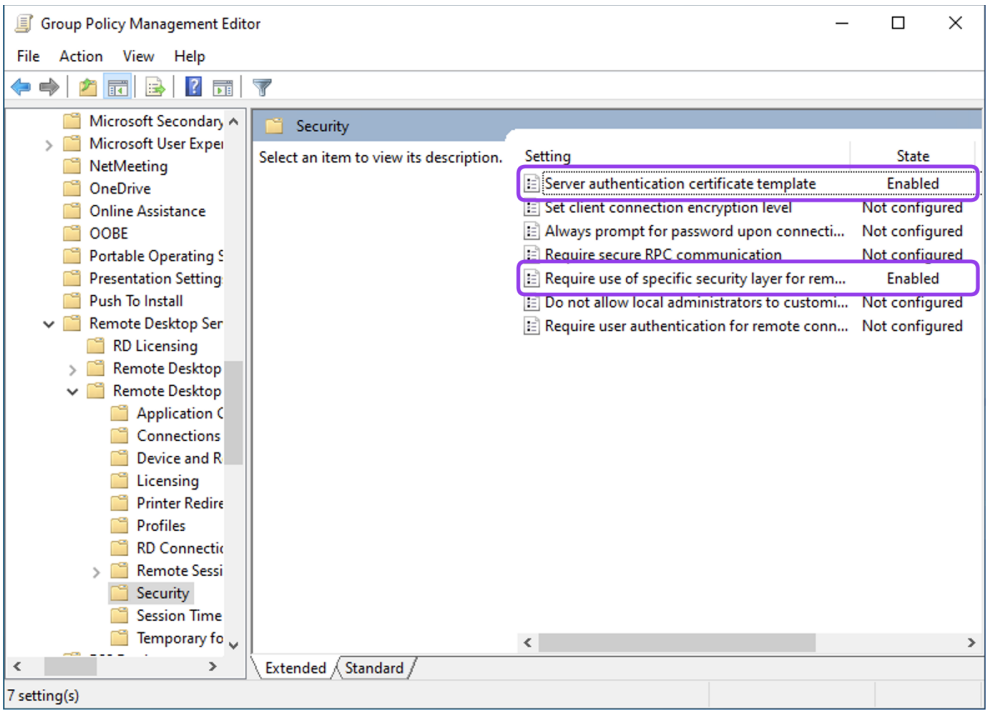
4. Provide a name for new GPO (e.g., *rdp*) and click *OK*.



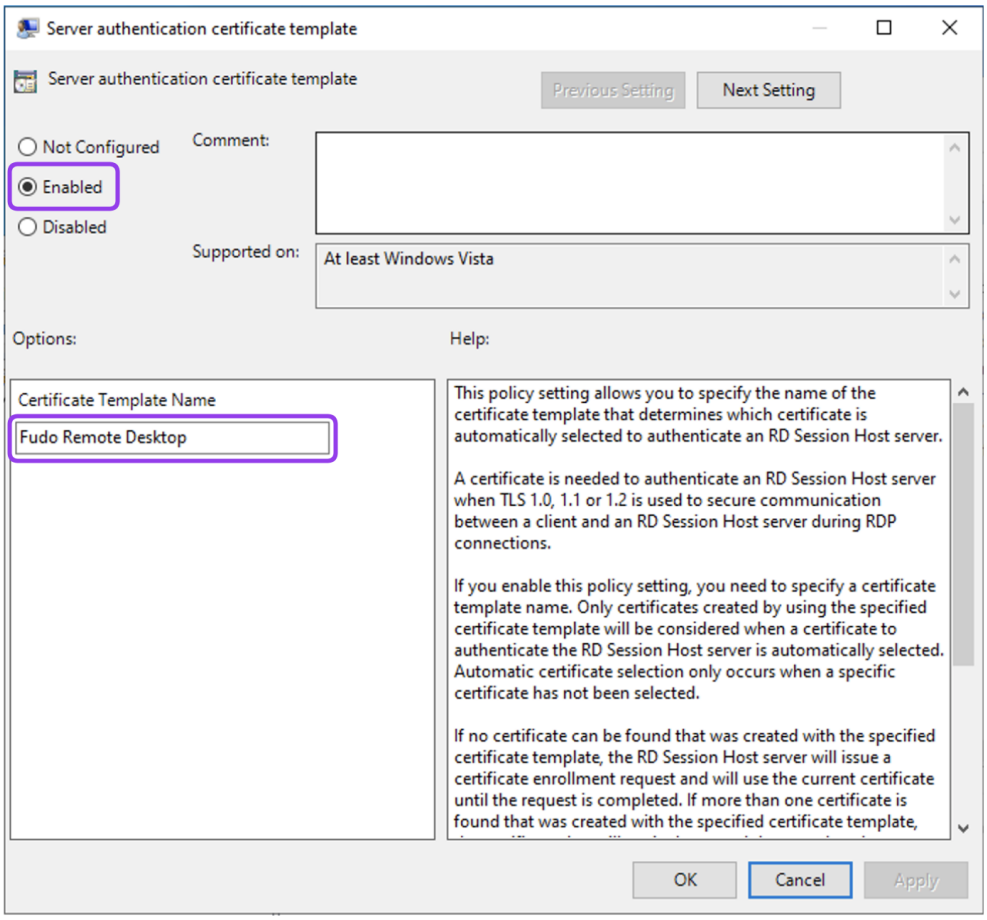
5. Right click on the name of created GPO and select *Edit...*.

6. In the *Group Policy Management Editor* navigate to *Computer Configuration* > *Policies* > *Administrative Templates* > *Windows Components* > *Remote Desktop Services* > *Remote Desktop Session Host* > *Security*.

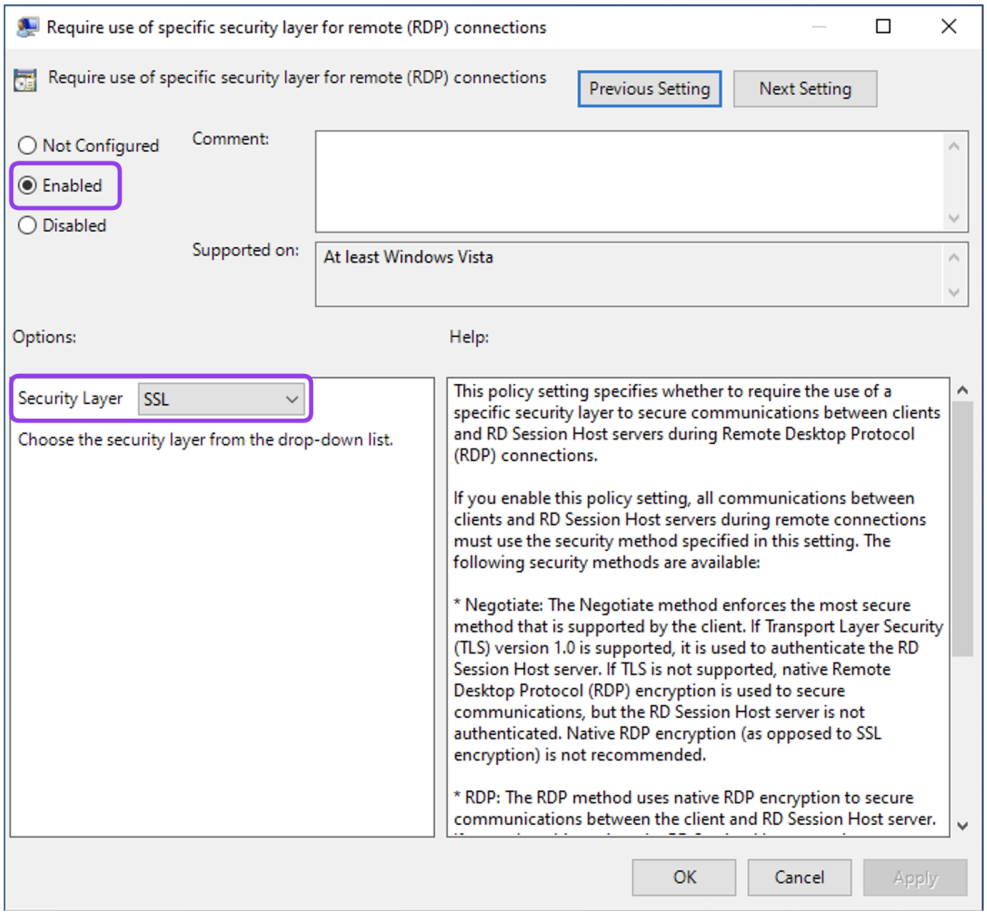
7. Double-click on the *Server authentication certificate template* to edit this setting.



8. Select *Enabled* option and enter the name of the template created in the previous steps into the *Certificate Template Name* field.



9. Click *OK*.
10. Double click on the *Require use of specific security layer for remote (RDP) connections* to edit this setting.
11. Select *Enabled* option and choose `SSL` from the *Security Layer* drop-down menu.



12. Click *OK*.
13. Link the GPO to the OU containing your servers / desktops that need RDP certificates if needed. They will auto enroll when Group Policy is updated.

Enroll the RDP Certificate

1. Press `Win + R`, type `certlm.msc`, and press *Enter* to open the *Certificate Manager* tool for the local device.
2. Navigate to *Personal* > *Certificates*.
3. Right-click in the manager window and select *All Tasks* > *Request New Certificate...*.
4. Click *Next* on the *Before You Begin* and on the *Select Certificate Enrollment Policy* tabs.
5. On the *Request Certificate* tab, select the template created in previous steps and click *Enroll*.
6. Copy the enrolled certificate to the *Trusted Root Certification Authorities* > *Certificates* directory.

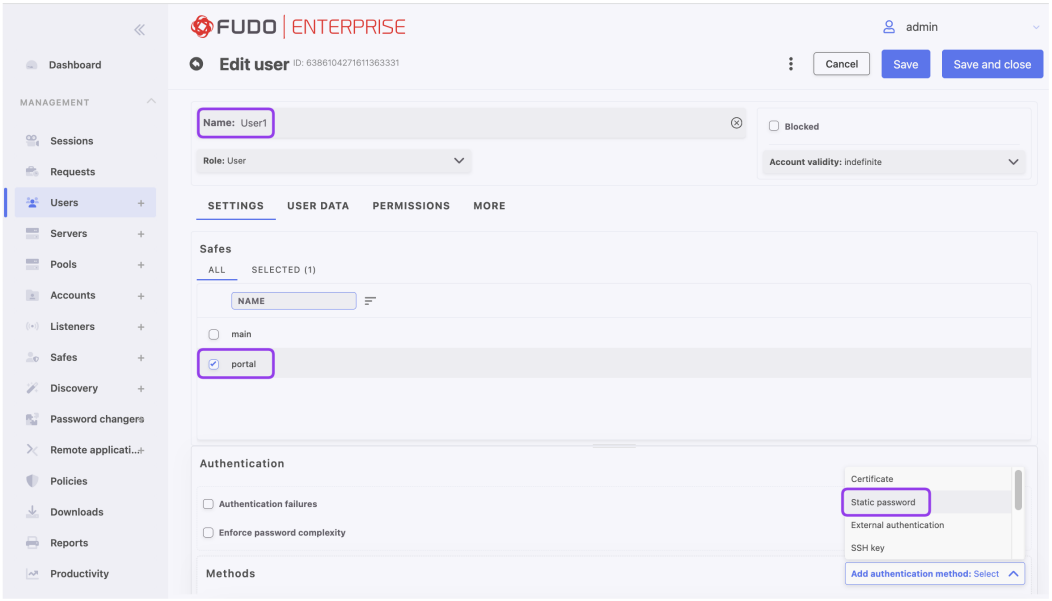
Export the CA Certificate

1. Press `Win + R`, type `certlm.msc`, and press *Enter* to open the *Certificate Manager* tool for the local device.
2. Navigate to *Trusted Root Certification Authorities* > *Certificates*.

3. Right-click on your Root Certification Authority certificate and select *All Tasks* > *Export...*.
4. Click *Next*.
5. Select *Base-64 encoded X. 509 (.CER)* format and click *Next*.
6. Specify the name and localisation for the exported certificate.
7. Click *Next* and *Finish* to save the file.

Create User in Fudo:

1. Select *User Management* > *Users* and then click + *Add user*.
2. Enter the user name (e.g., 'User1').
3. In the *Settings* tab, under the *Safes* section, select *portal*.
4. Click *Save*.
5. Go to the *Authentication* section and from the *Add authentication method* drop down list select *Static password*.

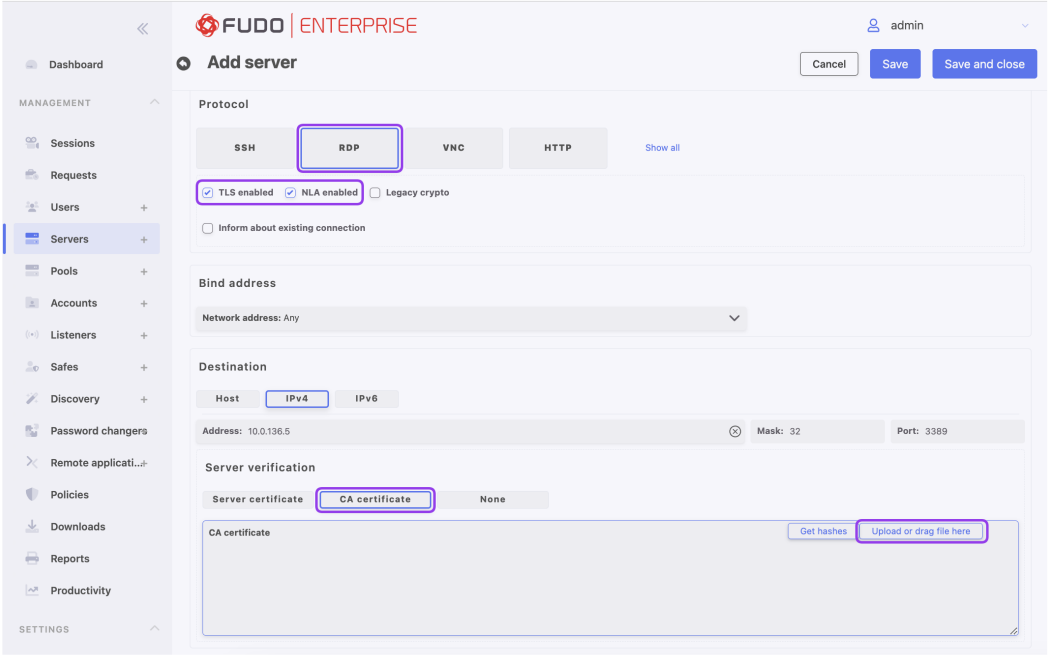


6. Provide password and click *Save*.
7. If necessary, please fill in the remaining parameters as needed for your specific configuration. For more details, please refer to the *Creating a User* section.
8. Click *Save and close*.

Configure RDP Server:

1. Select *Management* > *Servers* and then click + *Add server*.
2. Enter server's unique name (e.g., `ServerRDP`).
3. In the *Permissions* section, add users allowed to manage this object.
4. In the *Settings* section on the list of available protocols select `RDP`.
5. Select the *TLS enabled* and the *NLA enabled* options.

6. In the *Destination* section select `IPv4` and enter IP address of the server for which you wish to set up an RDP connection.
7. In the *Server verification* section select *CA certificate* and upload exported CA certificate file.



8. Click *Save and close*.

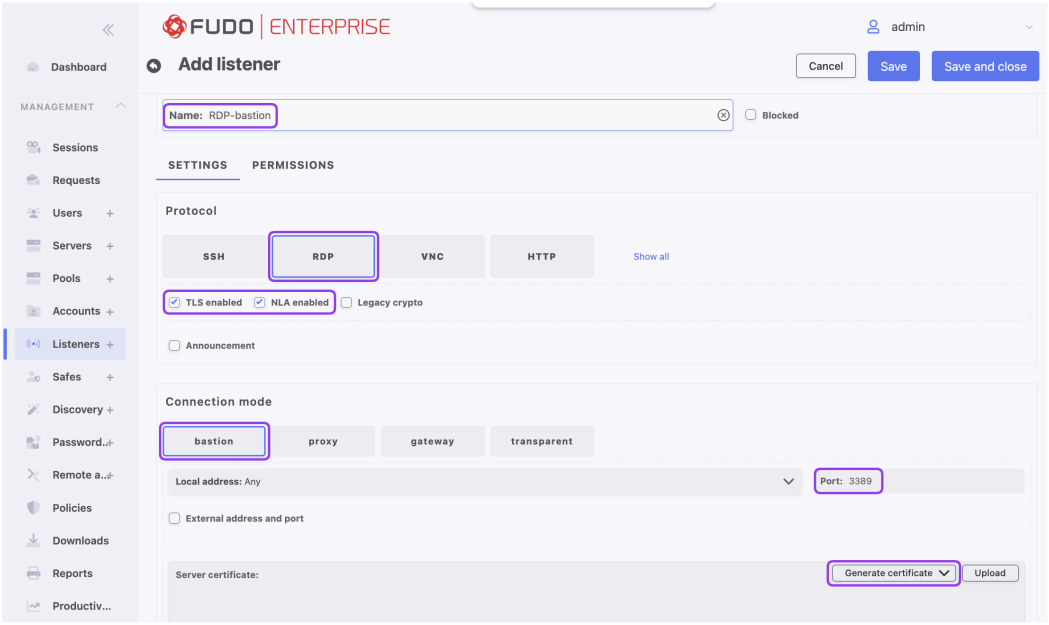
Configure Account:

1. Select *Management* > *Accounts* and then click *+ Add*.
2. Define object's name (e.g., `CA-account`).
3. Select `regular` from the *Type* drop-down list.
4. Go to the *Server / Pool* section and from the drop down list select the server created in previous step (e.g., `ServerRDP`) to assign created account to this server.
5. In the *Credentials* section provide the *Domain* and *Login* used to authenticate on the server.
6. From the *Replace secret with* drop down list select password, and provide password used to authenticate on the server.
7. Click *Save*.

Configure Listener:

1. Select *Management* > *Listeners* and then click *+ Add listener*.
2. Enter listener's unique name (e.g., `RDP-bastion`).
3. Go to *Permissions* tab and add users allowed to manage this listener (e.g., `User1`).
4. Go to *Settings* tab and press the `RDP` button in the *Protocol* field.
5. Select the *TLS enabled* option to enable encryption.

6. Check the *NLA enabled* option for additional security.
7. In the *Connection mode* section, select *bastion*.
8. Set the local address to `any` and port `3389`.
9. In the *Server certificate* field, click *Generate certificate* to generate TLS certificate by choosing key algorithm and providing Common Name (server name where the certificate is installed).



10. Click *Save and close*.

Configure Safe:

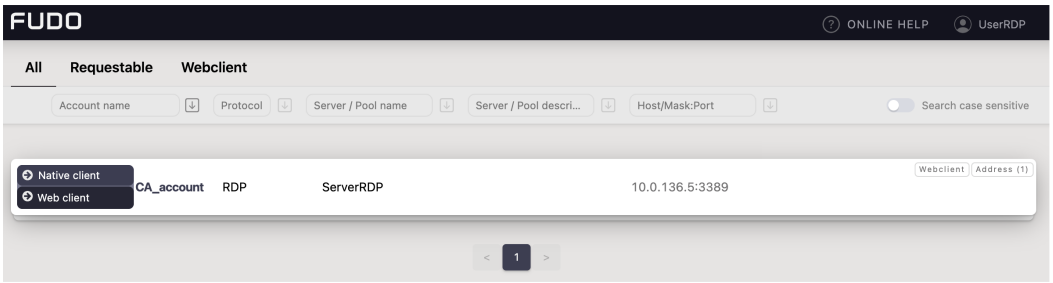
1. Select *Management* > *Safes* and then click *+ Add*.
2. Enter object's name (e.g., `SafeRDP`).
3. Select *Web Client* option to allow connecting to the session in browser.
4. Select **Users** tab to assign users allowed to access accounts assigned to this safe.

- Click *+ Add user*, and then click the + button next to `User1,` which was created in previous steps, to enable server access over monitored safe.
- Click *ok* to close the modal window.

5. Select **Accounts** tab to add accounts accessible through this safe.
   - Click *+ Add account*, and then click the + next to `CA-account,` which was created in previous steps.
   - Click *ok* to close the modal window.
   - Click ✎ to assign listener to accounts.
   - Click + to add listener `RDP-bastion` created in previous steps.
   - Click *ok* to close the modal window.
6. Click *Save*.

Establish a session:

1. Log in to the Fudo Enterprise Access Gateway using `User1` as the username and password provided during the creation of this user.
2. Hover the cursor over the `CA_account` name and select *Web client* to start the session.



Related topics:

- *Creating an RDP Server*
- *Creating a User*

20.6 Configuring the Single Sign On (SSO)

Before you start the procedure, check the following requirements:

- All servers with Windows Server 2019 or 2022 environment are connected in a domain;
- Domain Controller with AD user group is configured on Windows Server.

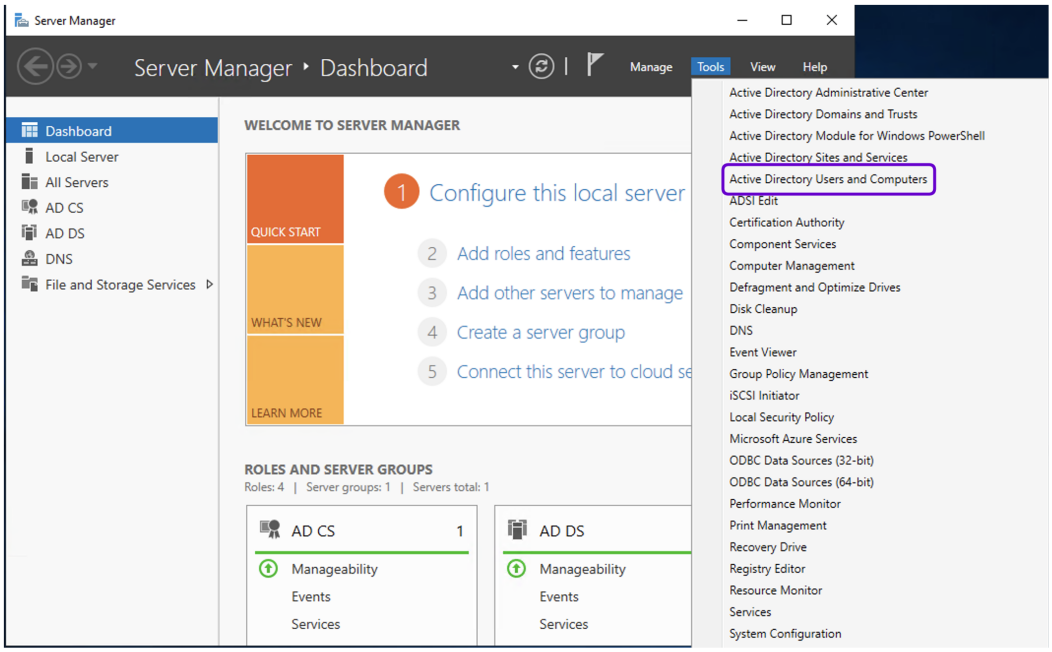
To configure and use the Single Sign On (SSO) with Fudo Enterprise, please follow below steps.

> **Note**
>
> Please note that this is a general guide, and specific details may vary depending on your Windows Server setup. Refer to the Windows Server documentation for precise configuration steps.

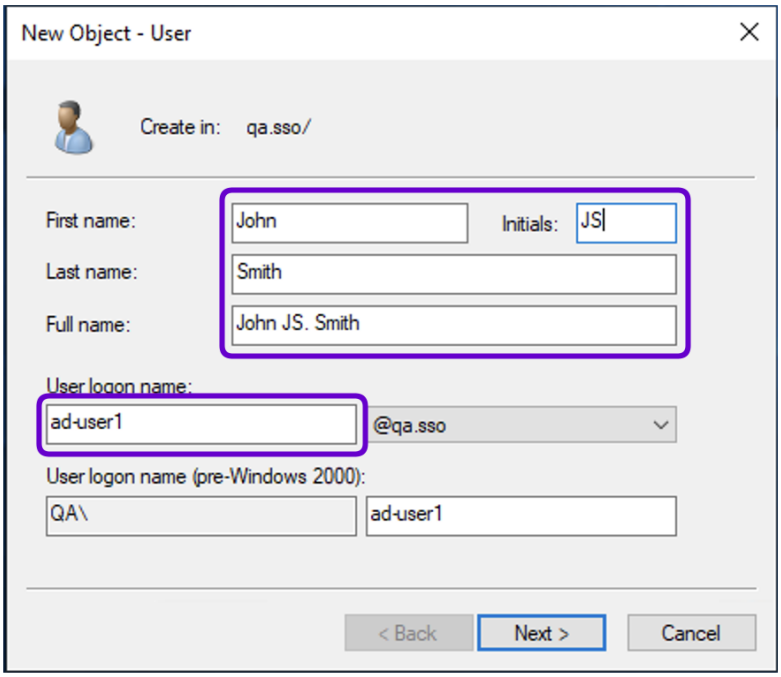
20.6.1 SSO Configuration on Windows Server 2019

Add User:

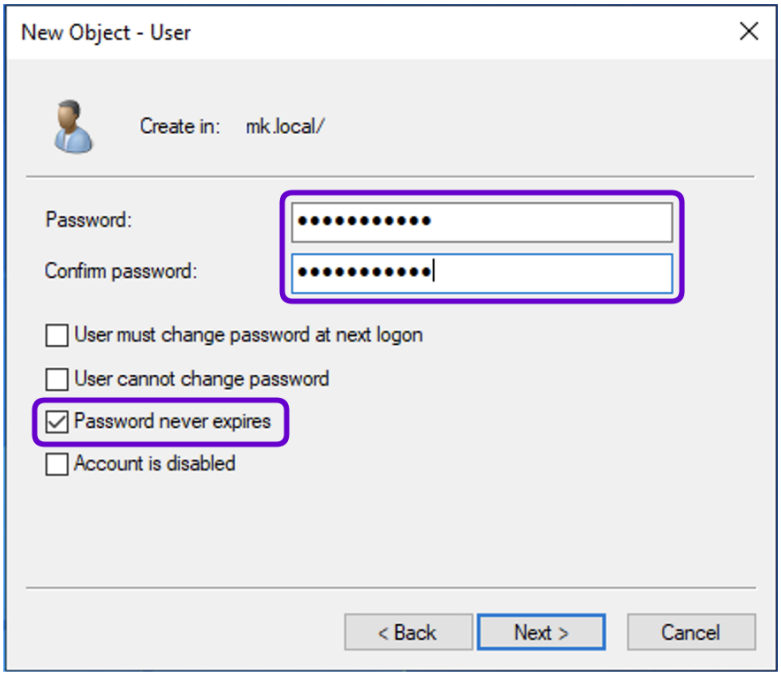
1. Log in to the server on which you want to setup the SSO using the administrator account.
2. Open the *Server Manager* application.
3. Click *Tools* button on the upper right corner of the window to expand the menu list and select *Active Directory Users and Computers.*



4. In the Manager window, navigate to the domain name, or a specific user group, and right-click on the *Users* catalog.
5. Select *New* > *User*.
6. Create a user who will use SSO to log in to Fudo Enterprise (e.g., `User logon name: ad-user1`).

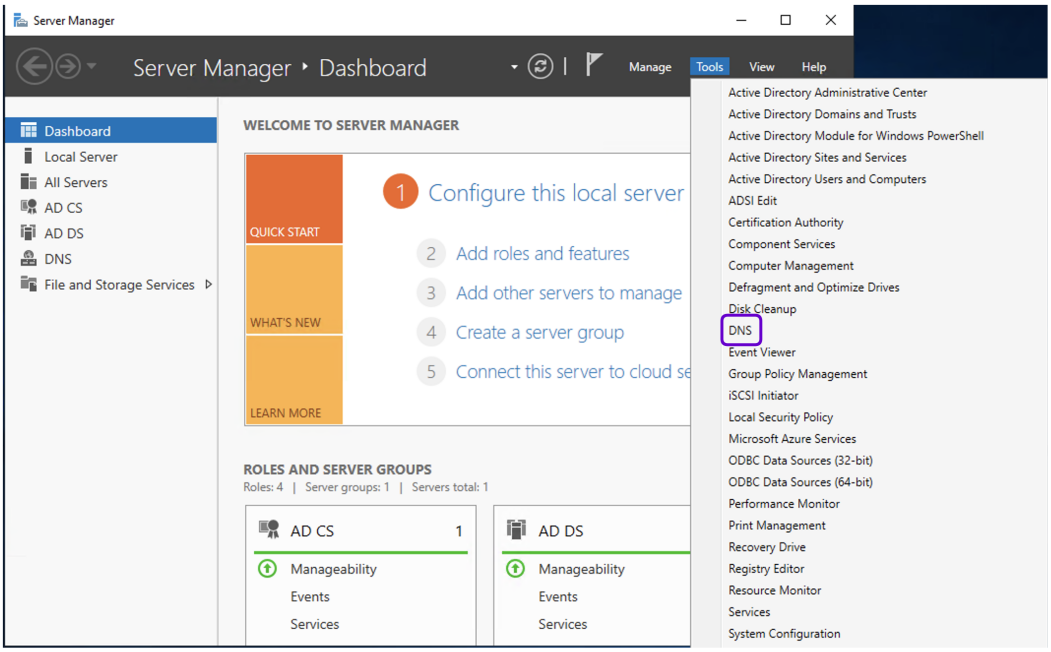


7. Click *Next*.
8. Provide the password for created user (e.g., `PaSSwOrD`) and select *Password never expires* option.
9. Click *Next* and *Finish*.

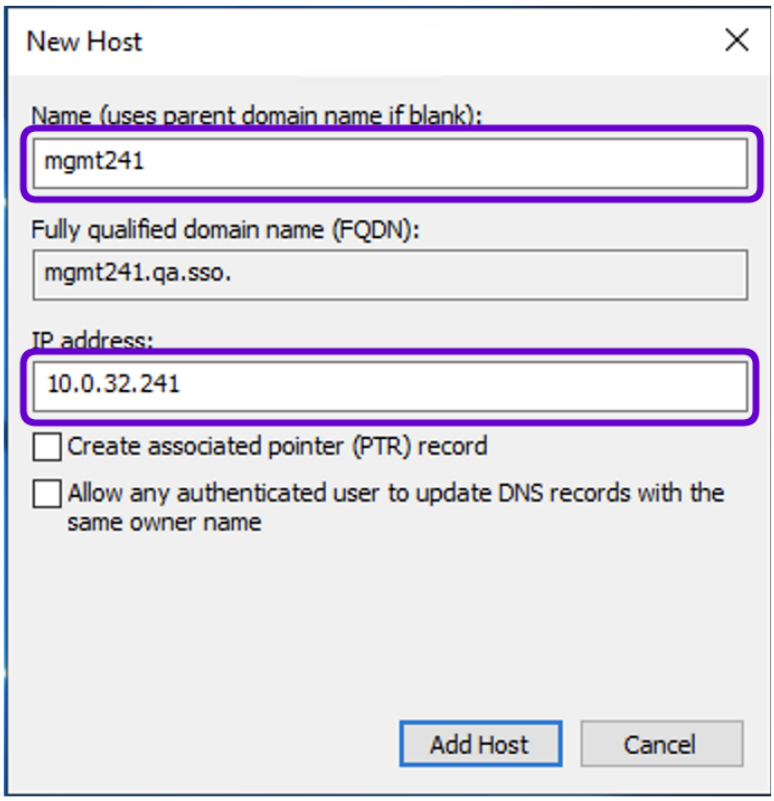


Configure DNS entries:

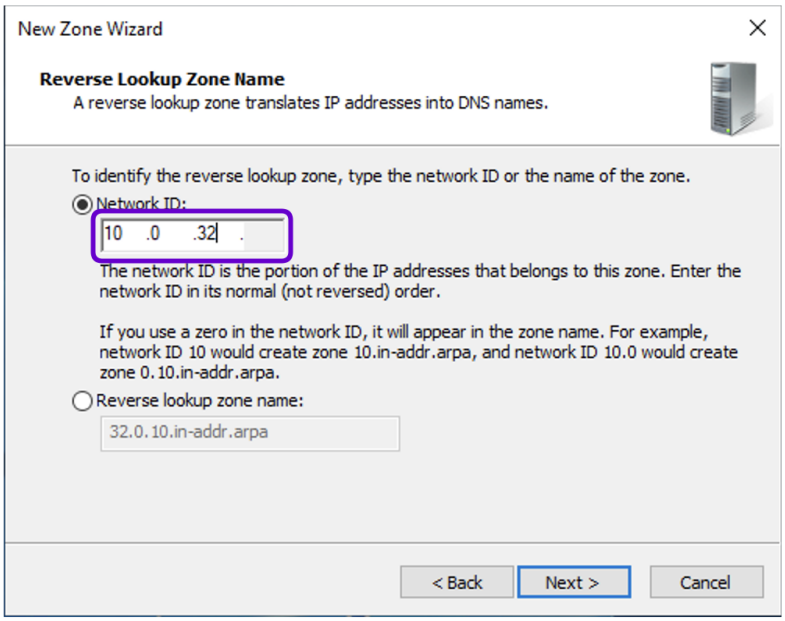
1. Open the *Server Manager* application.
2. Click *Tools* button on the upper right corner of the window to expand the menu list and select *DNS*.



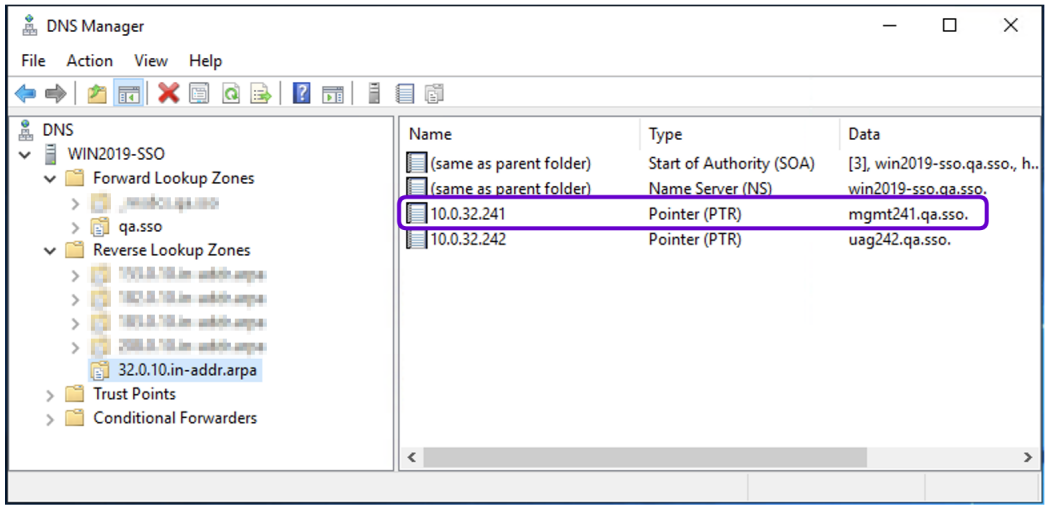
3. Go to *Forward Lookup Zones*, right click on the domain name and select *New Host*.
4. Provide the *Name* and *IP address* of the Fudo Enterprise Admin Panel (e.g., `mgmt241.qa.sso, 10.0.32.241`).
5. Click *Add Host*.



6. Right click on *Reverse Lookup Zone* and select *New Zone.*
7. Click *Next.*
8. Select *Primary zone* option and click *Next.*
9. Select *To all DNS servers running on domain controllers in this domain:* option and click *Next.*
10. Select *IPV4 Reverse Lookup Zone* option and click *Next.*
11. In the *Network ID* field, type in the start of the subnet range of your network (e.g., `10.0.32`) and click *Next.*



12. Choose the dynamic update option (e.g., *Allow only secure dynamic updates*) and click *Next.*
13. Click *Finish.*
14. Right click on created zone `32.0.10.in-addr.arpa` and select *New Pointer (PTR).*
15. Provide the *Host IP Address* and *Host name* of the Admin Panel (e.g., `10.0.32.241` and `mgmt241.qa.sso`).



Create Kerberos ticket:

1. Run the following command in the Powershell or CMD console:

   ```
   ktpass -princ HTTP/hostname.yourdomain.local@yourdomain.local
   -mapuser netbios_domain_name\username -pass password -ptype
   KRB5_NT_PRINCIPAL -out hostname.yourdomain.local.keytab
   ```

   - Example for this use case:

```
ktpass -princ HTTP/mgmt241.qa.sso@QA.SSO -mapuser QA\ad-user1 -pass
PaSSwOrD -ptype KRB5_NT_PRINCIPAL -out mgmt241.qa.sso.keytab
```

2. Copy the generated keytab file to the workstation where you will be configuring Fudo.

20.6.2 Setup Fudo Enterprise

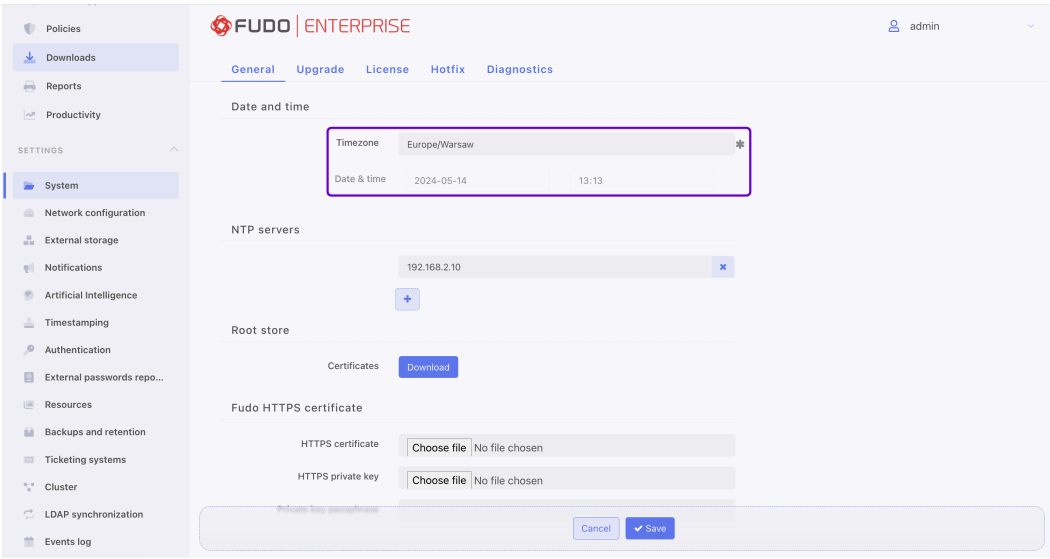
> **Note**
>
> This use case describes how to configure Fudo Enterprise using the Active Directory external authentication method. Please keep in mind that you can customize user authentication using other method supported by Fudo Enterprise to align with your specific requirements, the methods typically used in your environment, and your work scenarios.

Configure SSO:

In order to define SSO service parameters in Fudo Enterprise, follow the steps:

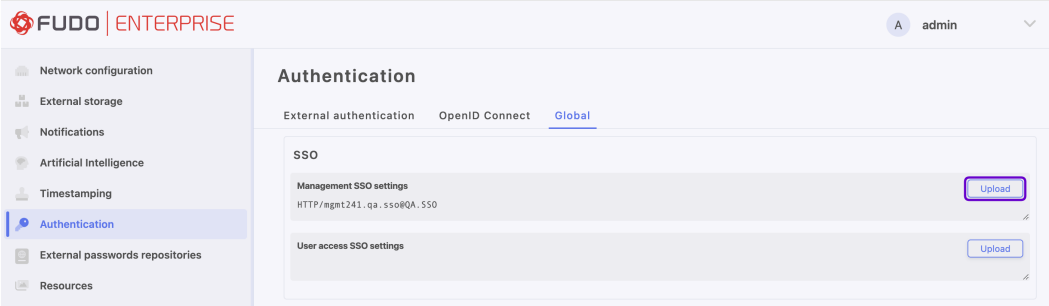
1. Login into your Fudo Enterprise Admin Panel using the credentials for user with `superadmin` role.
2. Select *Settings* > *System*.
3. In the *Timezone* section, check if the selected timezone is consistent with the Windows client timezone configuration.

> **Warning**
>
> Fudo Enterprise Timezone must match the Windows client timezone configuration.

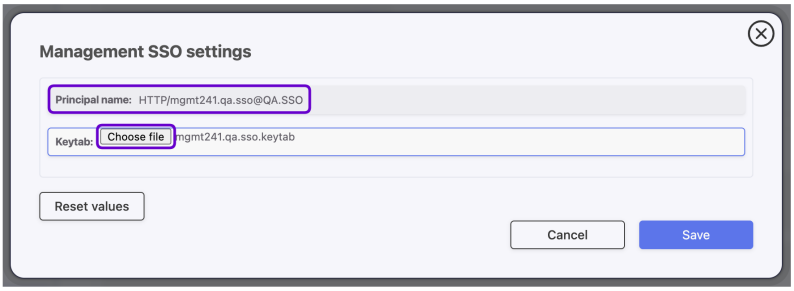


4. Select *Settings* > *Authentication*.
5. Go to *Global* tab.

6. In the *SSO* section, click the *Upload* button next to the *Management SSO settings* field.



7. In the *Principal name* field, provide service identifier that will match the user account with the service instance (e.g., `HTTP/mgmt241.qa.sso@QA.SSO`).
8. In the *Keytab* field, upload the keytab file containing user's ID and encryption keys for encrypting and decrypting Kerberos tickets (generated in previous steps `mgmt241.qa.sso.keytab` file).



9. Click *Save*.

> **Note**
>
> You can also configure SSO for the *User Access Gateway* by uploading the appropriately configured keytab file in the *User Access SSO settings* field. Remember to use the User Access Gateway IP address when configuring the Windows environment.

Configure DNS:

1. Go to *Settings* > *Network configuration*.
2. Switch to the *Name & DNS* tab.
3. Enter `hostname.yourdomain.local` in the *Hostname* field (e.g., `mgmt241.qa.sso`).
4. Configure DNS server to point to a DNS server in the *yourdomain.local* domain (in this example we will use a domain controller IP address):
    - Click *Add DNS server* to define new DNS server.
    - Enter DNS server IP address (e.g., `10.0.242.100`).
    - Click *Save*.

Configure external authentication method:

1. Login into your Fudo Enterprise Admin Panel.
2. Select *Settings* > *Authentication*.
3. In the **External authentication** tab click *Add an external authentication source*.
4. In the *Name* field, provide a name for this configuration.
5. Set the *Bind address* to *Any*.
6. In the *General* field select *Active Directory*.
7. In the *Host* field provide the Domain Controller IP address (e.g., `10.0.242.100`).
8. Leave default port number: `389`.
9. Provide the name of the domain which will be used for authenticating users in Active Directory (e.g., `qa.sso`).
10. In the *Login* and *Secret* fields provide the privileged account's login credentials used to access the Domain Controller.
10. Click *Save*.

Create User in Fudo:

> **Warning**
>
> **Single Sign On setup** is available only for users with the `superadmin` role, and can be used by users with the `operator`, `admin`, and `superadmin` roles.

1. Select *User Management* > *Users* and then click + *Add user*.
2. Enter the user name that matches created in previous steps user account in Active Directory (e.g., `ad-user1`).
3. Select the `Admin` role.
4. In the *Settings* tab, under the *Safes* section, select *main* to grant access rights to the Admin Panel.
5. Click *Save*.
6. Go to the *Authentication* section and from the *Add authentication method* drop down list select *External authentication*.
7. Chose created in previous steps Active Directory method and click *Save*.
8. In the *User Data* tab, fill in the *Fudo domain* and *AD domain* (e.g., `qa.sso`).

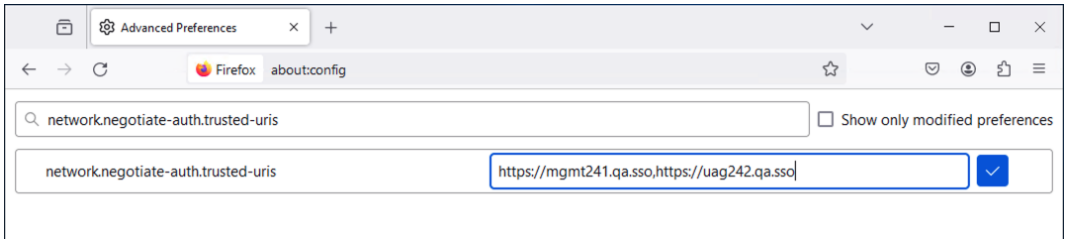
> **Note**
>
> Both the *Fudo domain* and *AD domain* should match the domain name specified in the Kerberos ticket.

9. If necessary, please fill in the remaining parameters as needed for your specific configuration. For more details, please refer to the *Creating a User* section.
10. Click *Save and close*.

20.6.3 Setup and Check User Workstation - Windows2010 Client

Firefox browser configuration:

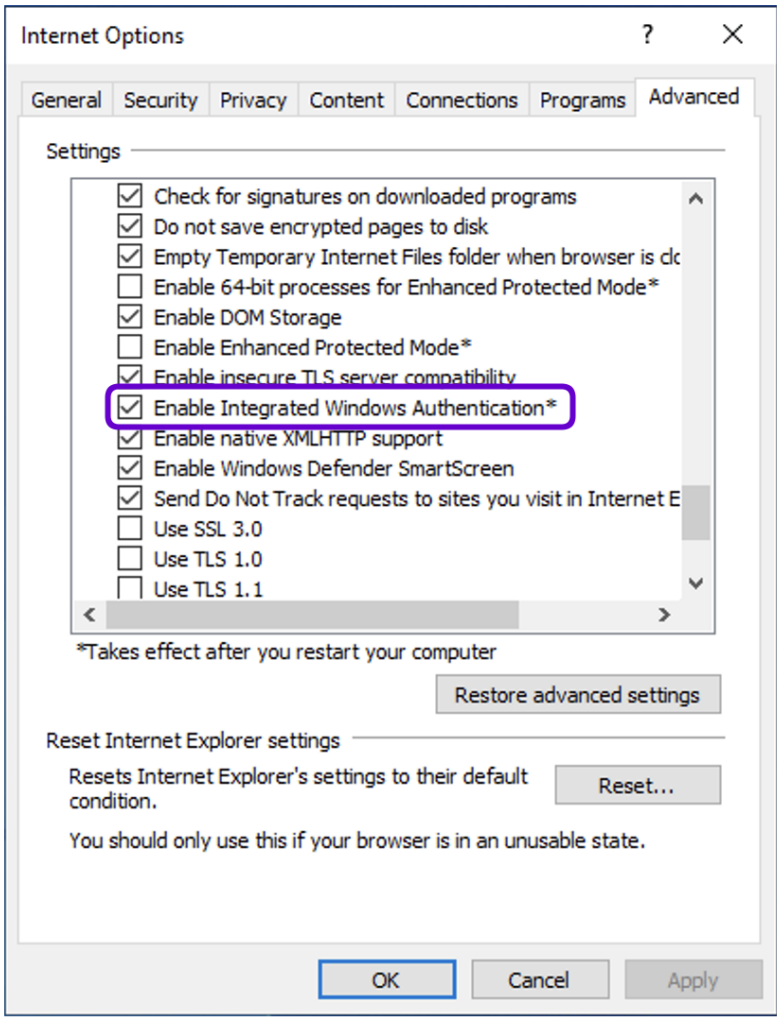
1. Log in to Windows Client using the `ad-user1` account.
2. Open *Firefox,* type `about:config` in the address bar, and press *Enter.*
3. A warning message will appear. Click on *Accept the Risk and Continue* option to proceed.
4. In the search bar at the top, type `network.negotiate-auth.trusted-uris.`
5. Double-click on the `network.negotiate-auth.trusted-uris` and enter the desired FQDN (Fully Qualified Domain Name) with a protocol, separating entries with a comma (e.g., `https://mgmt241.qa.sso,https://uag242.qa.sso).`
6. Press *Enter* to save the changes.



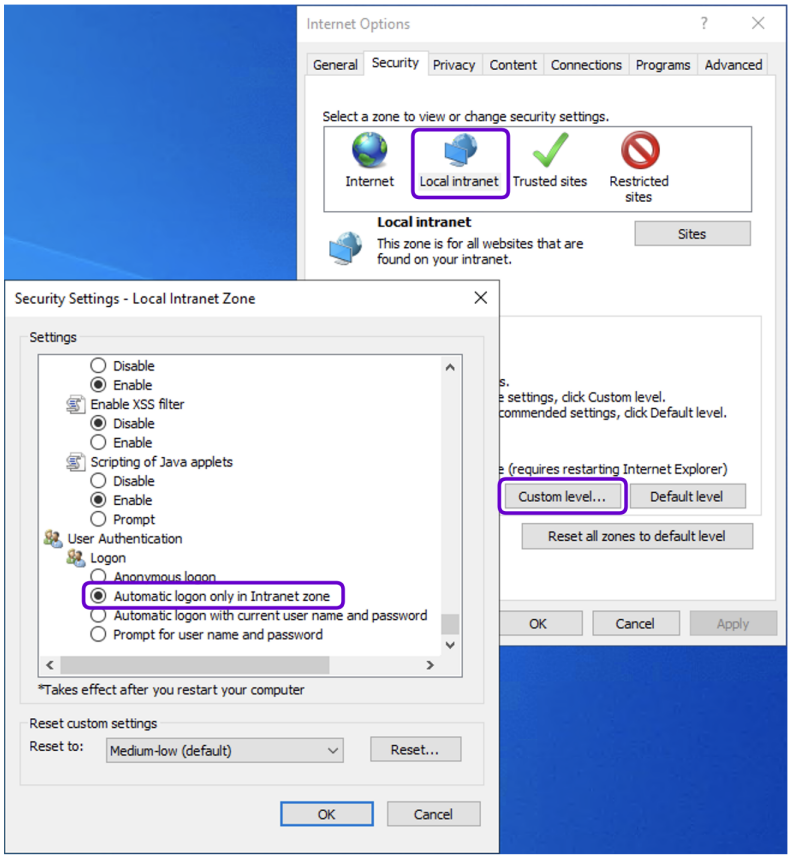
7. Next, type in `network.automatic-ntlm-auth.trusted-uris` in the search bar.
8. Double-click on the `network.automatic-ntlm-auth.trusted-uris` and enter the desired FQDN (Fully Qualified Domain Name) with a protocol, separating entries with a comma (e.g., `https://mgmt241.qa.sso,https://uag242.qa.sso).`
9. Press *Enter* to save the changes.
10. Restart the browser.

Internet Explorer browser configuration:

1. Navigate to *Tools* > *Internet Options* > *Advanced.*
2. On the *Advanced* tab and in the *Security* section, select *Enable Integrated Windows Authentication.*



3. On the *Security* tab, select *Local Intranet.*
4. Click *Custom Level.*
5. In the *User Authentication/Logon* section, select *Automatic logon only in Intranet zone.*



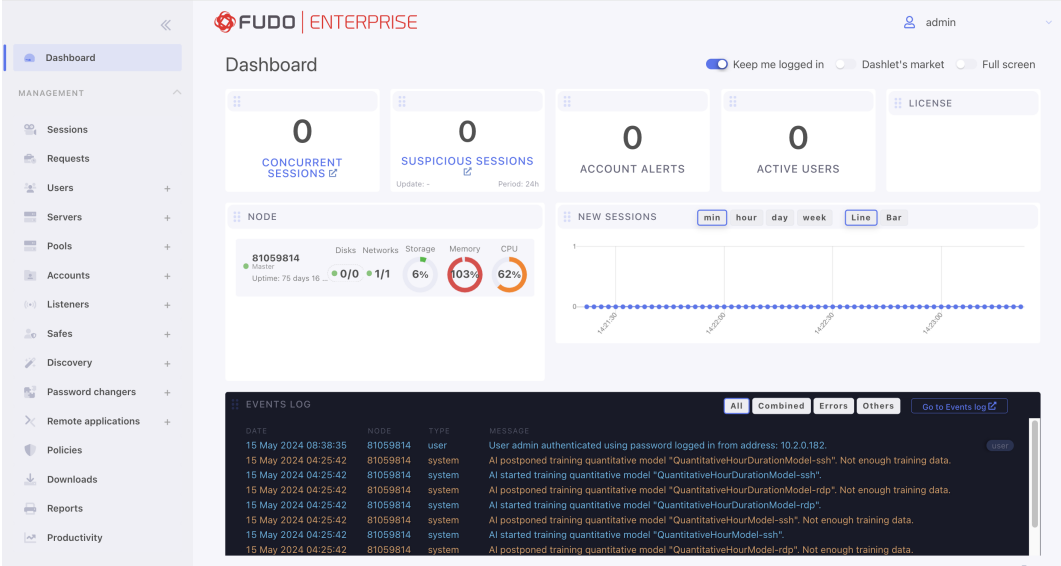
6. Click *OK*.
7. Click *Sites* and select all check boxes.
8. Click *Advanced* and add Remedy SSO service website to the local zone (in our example, it's `https://mgmt241.qa.sso`).
9. Click *Add*.
10. Click *OK* for all pop-ups.
11. Uruchom ponownie przeglądarkę.

Chrome browser configuration:

Google Chrome supports Kerberos authentication. Once Internet Explorer is configured, no additional settings are needed for Google Chrome, as it relies on Internet Explorer's configuration.

Log into the Admin Panel using SSO:

1. Open the *Firefox* browser and enter the previously defined FQDN in the address bar (in our example, it's `https://mgmt241.qa.sso`).
2. The Fudo Enterprise Admin Panel Dashboard will appear without the need to use login credentials.



Related topics:

- *Single Sign On*
- *Authentication*

20.7 Handling Local Account Password Changes Using a Domain Account with WinRM Secret Changer

The following guide describes the basic configuration of Fudo Enterprise required to enable local account password changes on domain-joined workstations using a domain account.

To ensure proper operation of the secret changer in Fudo Enterprise, the following configurations must be added:

- Hostname and DNS server configuration.
- KDC server configuration.
- Configuration of the server where the local account is located.
- Configuration of a privileged account used to perform the password change.
- Configuration of the local or domain account for which the password will be changed.

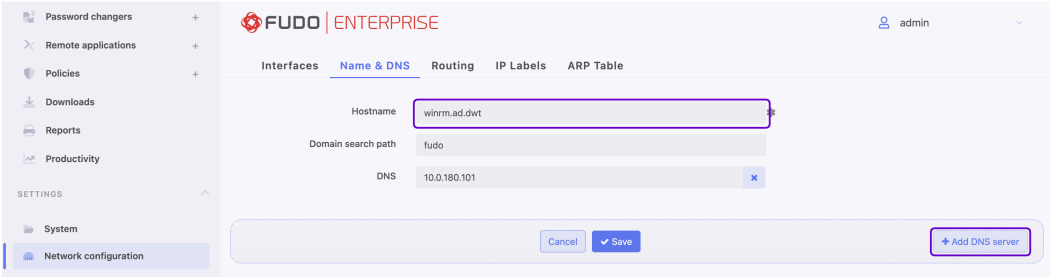
Note

- Fudo Enterprise must be configured with the same time zone as the domain.
- A privileged domain account can be used to change passwords for both local and domain accounts. This should be considered when configuring privileged users responsible for password changes and those whose passwords will be changed.

20.7.1 Hostname and DNS Server Configuration

Set the hostname by following these steps:

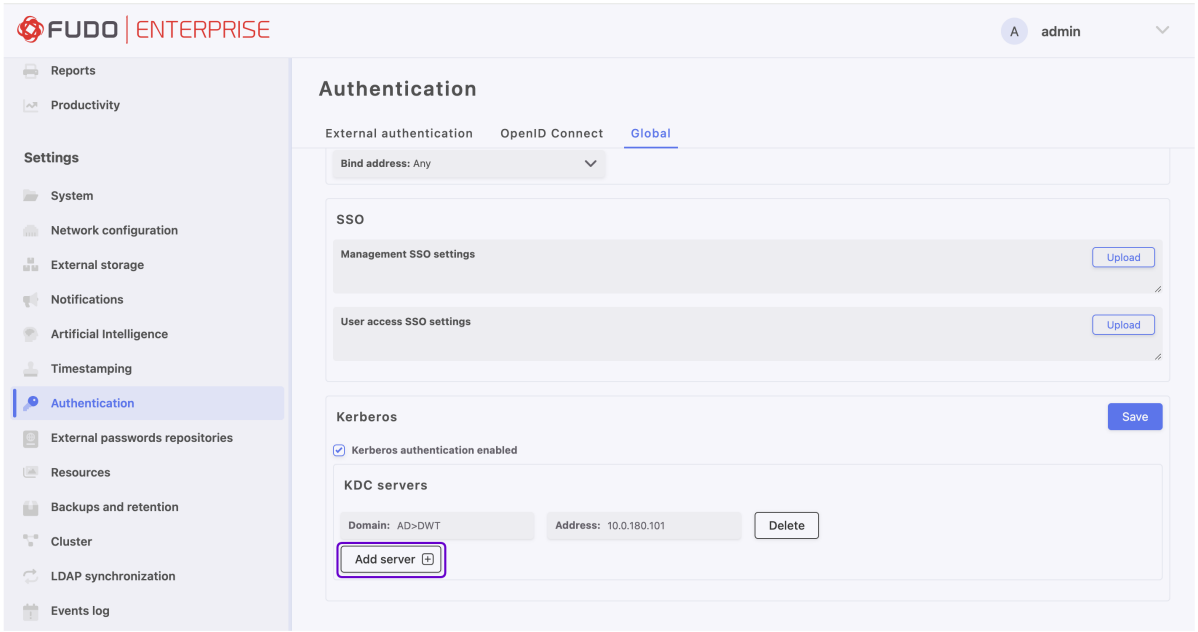
1. Go to *Settings* > *Network Configuration*.
2. Navigate to the *Name and DNS* tab.
1. In the *Hostname* field, enter the hostname along with the domain in the following format: `hostname.yourdomain.local` (e.g., `winrm.ad.dwt`).
2. Configure the DNS server:
    - Click *Add Server* + to define a new DNS server.
    - Enter the IP address of the DNS server (e.g., `10.0.180.101`).
    - Click *Save*.



20.7.2 Adding a KDC Server

Add the KDC server configuration by following these steps:

1. Select *Settings* > *Authentication* > *Global* tab.
2. In the *Kerberos* section, ensure the *Use Kerberos authentication* option is enabled.
3. Click *Add Server* +.



4. In the *Domain* and *Address* fields, enter the domain and IP address of the server responsible for authentication and key distribution in the Kerberos protocol (e.g., `AD.DWT` and `10.0.180.101`).

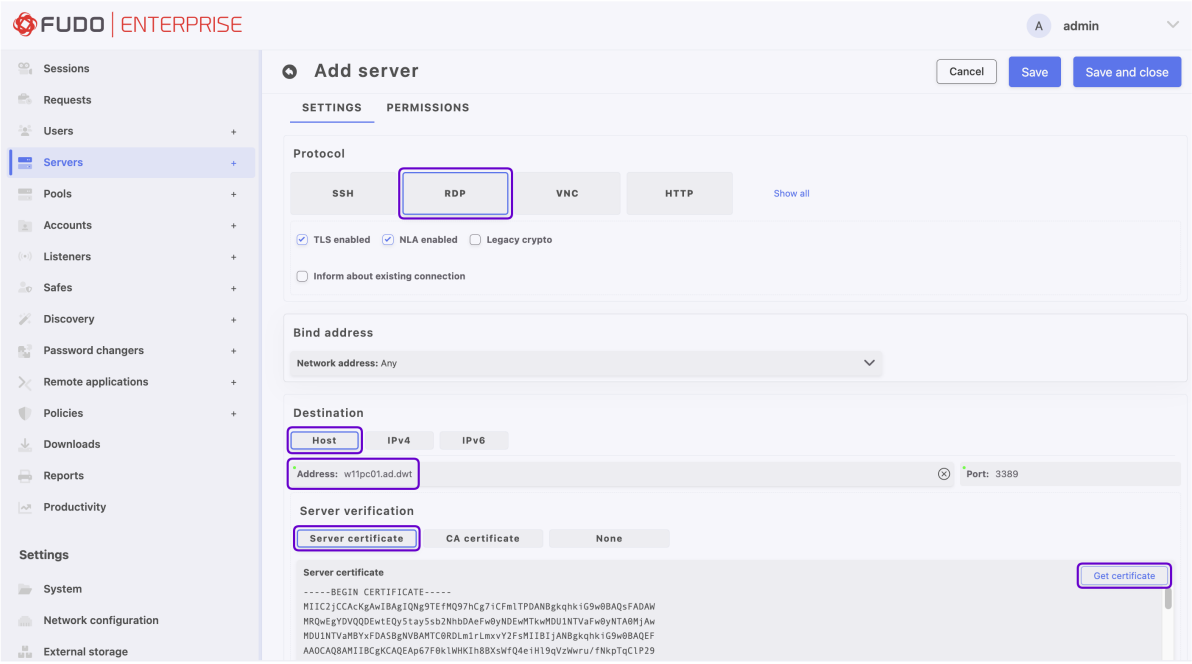
20.7.3 Server Configuration

Create a configuration for the server where the local account is located:

1. Select *Management* > *Servers* from the left menu and click *+ Add Server*.
2. Enter a unique name for the created object (e.g., `RDP_Server`).
3. Navigate to the *Settings* section.
4. In the *Protocol* field, select `RDP`.
5. Define the destination server:

- Select `Host`.
- In the *Address* field, enter the hostname along with the domain (e.g., `w11pc01.ad.dwt`).
- Enter the *Port* number.

6. In the *Server Verification* section, select *Server Certificate* and click *Download Certificate*.
1. Click *Save and Exit*.



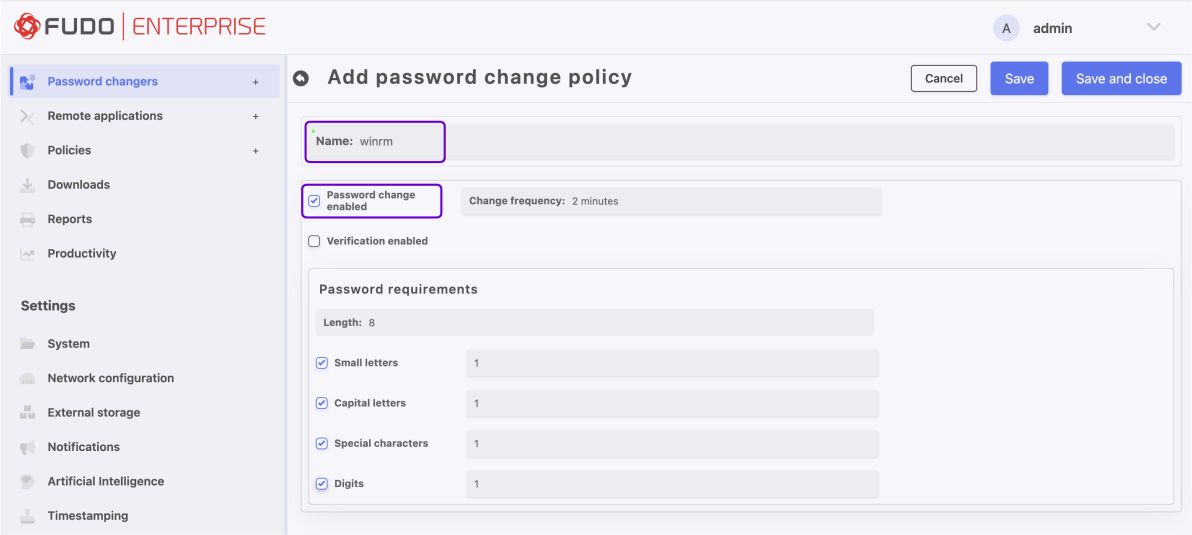
Note

In this scenario, the hostname along with the domain must be provided. This name will be used in the `transport_host` variable of the secret changer. Defining the server by IPv4/IPv6 address is not supported.

20.7.4 Adding a Secret Change Policy

Create a password policy:

1. Select *Management* > *Secret Changers*.
2. Go to the *Secret Change Policies* tab and click *+ Add Secret Change Policy*.
3. Enter a unique name for the policy being created (e.g., `winrm`).
4. Select the *Secret change* option and define the interval between each password change.
5. Define password complexity.



Note

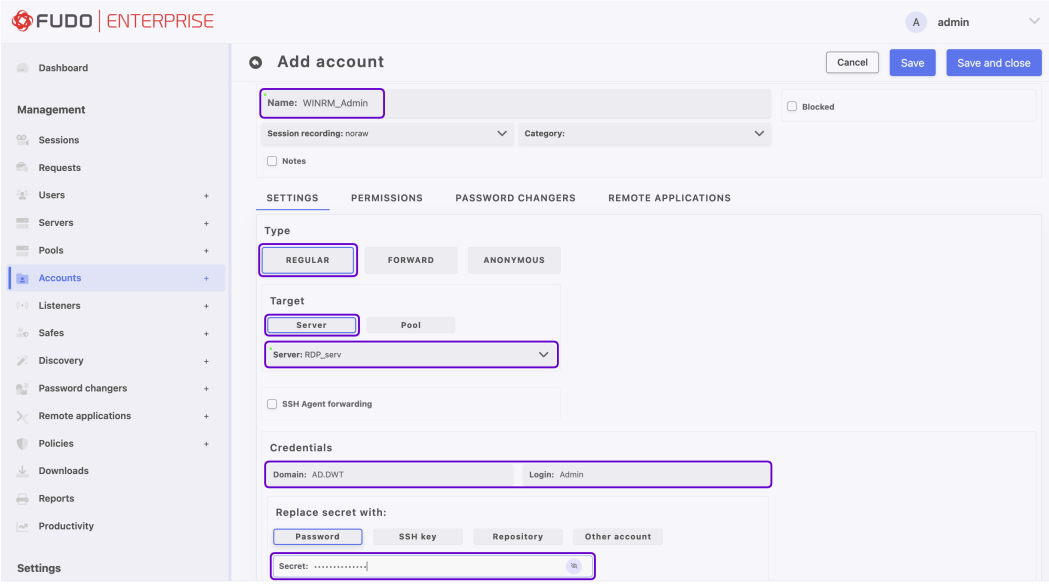
- Password verification in the scenario of changing a domain account password using another domain account is not supported in the current version of Fudo Enterprise.
- Password verification works in the scenario of changing a password for an account outside the domain.

20.7.5 Administrator Account

Add an account that will be used when changing passwords for local accounts. The following example is based on a regular domain account with privileges to change passwords.

1. Select *Management* > *Accounts*, then click *+ Add account*.
2. Enter a unique name for the object being created (e.g., `WINRM_Admin`).
3. In the *Settings* tab, in the *Type* field, click the *REGULAR* button.
4. In the *Target* section, select the *Server* button, then from the list choose the previously created RDP server where the local account is located (`RDP_Server`).
5. In the *Credentials* section:
   - Enter the domain name (e.g., `AD.DWT`).
   - Enter the *Login* of the account that will be used to change local account passwords (e.g., `Admin`).

- In the *Override secret* section, click the button corresponding to one of the desired authentication options (e.g., *Password*) and in the *Secret* field enter the password for the mentioned account.
- Click *Save* to close the dialog.



6. Click *Save and exit*.

20.7.6 Account for Which the Password Will Be Changed

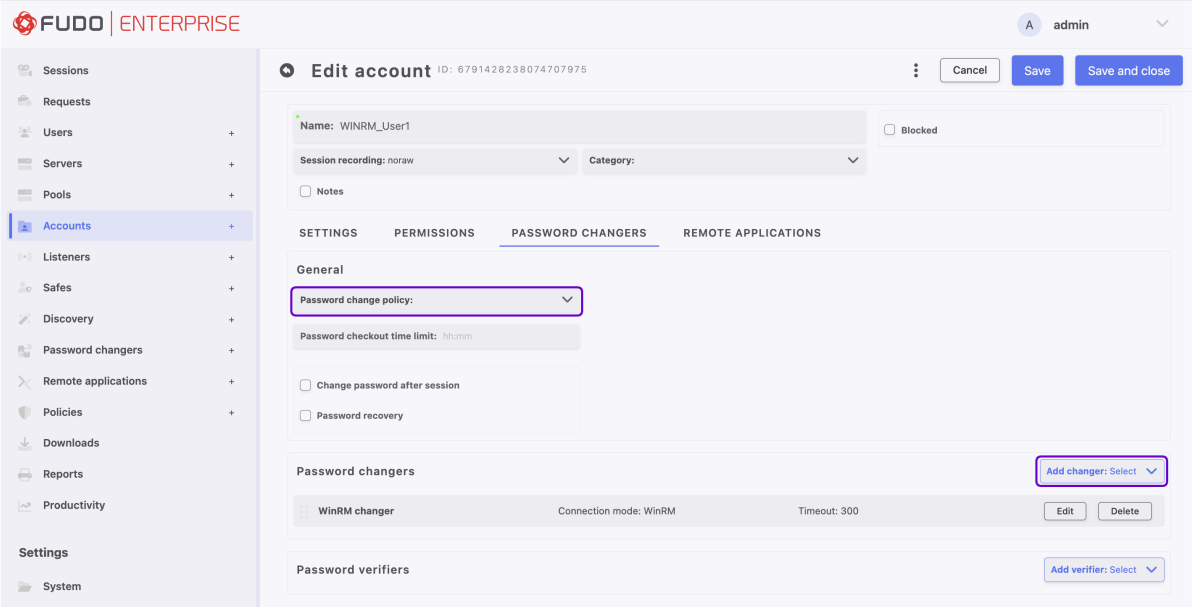
Add a local user account for which the password will be changed. The following example is based on a regular local user account.

1. Select *Management* > *Accounts*, then click *+ Add account*.
2. Enter a unique name for the object being created (e.g., `WINRM_User1`).
3. In the *Settings* tab, in the *Type* field, click the *REGULAR* button.
4. In the *Target* section, select the *Server* button, then from the list choose the previously created RDP server where the local account is located (`RDP_Server`).
5. In the *Credentials* section:
   - Enter the domain name (e.g., `AD.DWT`) – if this is a domain account.
   - Enter the *Login* of the local account (e.g., `User1`).
   - In the *Override secret* section, click the button corresponding to one of the desired authentication options (e.g., *Password*) and in the *Secret* field enter the password for the local account.
   - Click *Save* to close the dialog.

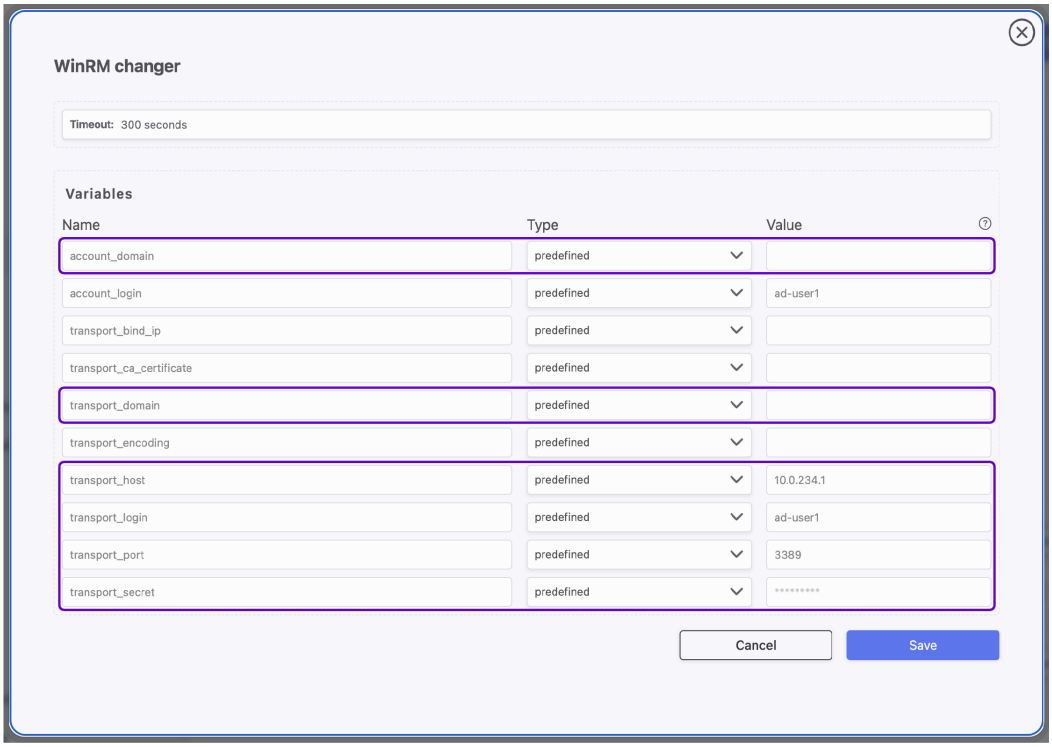
> **Note**
>
> Providing the domain in this case is optional and depends on whether the account is in the domain or outside of it.

6. Go to the *SECRET CHANGERS* tab.

7. In the *General* section, in the *Secret changers policy* field, select the previously created policy (`winrm`).
8. In the *Secret Changers* section, from the *Add changer* drop-down list, select *WinRM changer*.



9. For the changer to work correctly, the following fields must be configured:
   - `transport_domain` – used when authenticating with the account used to change local or domain account passwords. By default, it is set to *predefined*, which means the domain name entered for the currently configured account is used. Other available options are:
     - *constant* – allows entering a fixed value for the domain name.
     - *account* – allows selecting an account from which the domain name value will be taken.
   - `transport_login` – field specifying the login of the privileged account that will be used to change the password. In the *Type* column select *account*, then in the *Value* column select the account that will be used when changing passwords for local accounts. In this scenario, this will be the `WINRM_Admin` account.
   - `transport_port` – port 5986 used to log in to the server where the password will be changed (required port: `5986`).
   - `transport_secret` – field specifying the secret of the privileged account that will be used to change the password. In the *Type* column select *account*, then in the *Value* column select the account that will be used when changing passwords for local accounts. In this scenario, this will be the `WINRM_Admin` account.
   - `account_domain` – this field must be filled in if you want to configure a secret changer for a domain account. If the account for which you want to change the password is a local account, this field can be left empty. By default, this field is set to *predefined*, which means the domain name entered for the currently configured account is used.



10. Click *Save* to close the dialog.
11. Click *Save and exit*.

Related Topics:

- *Creating a Regular Account*
- *Authentication*

20.8 Configuring SSH Key Rotation for an Account

This guide describes how to configure automatic SSH key rotation for an account in Fudo Enterprise.

Important

The complete workflow is:

1. Create a secret change policy that generates the SSH key.
2. Create an *SSH key* secret changer.
3. Store the SSH key as an *SSH Key* secret in the Password Vault.
4. Assign the changer (and, optionally, a verifier) to that secret.
5. Point the account at the Password Vault secret.

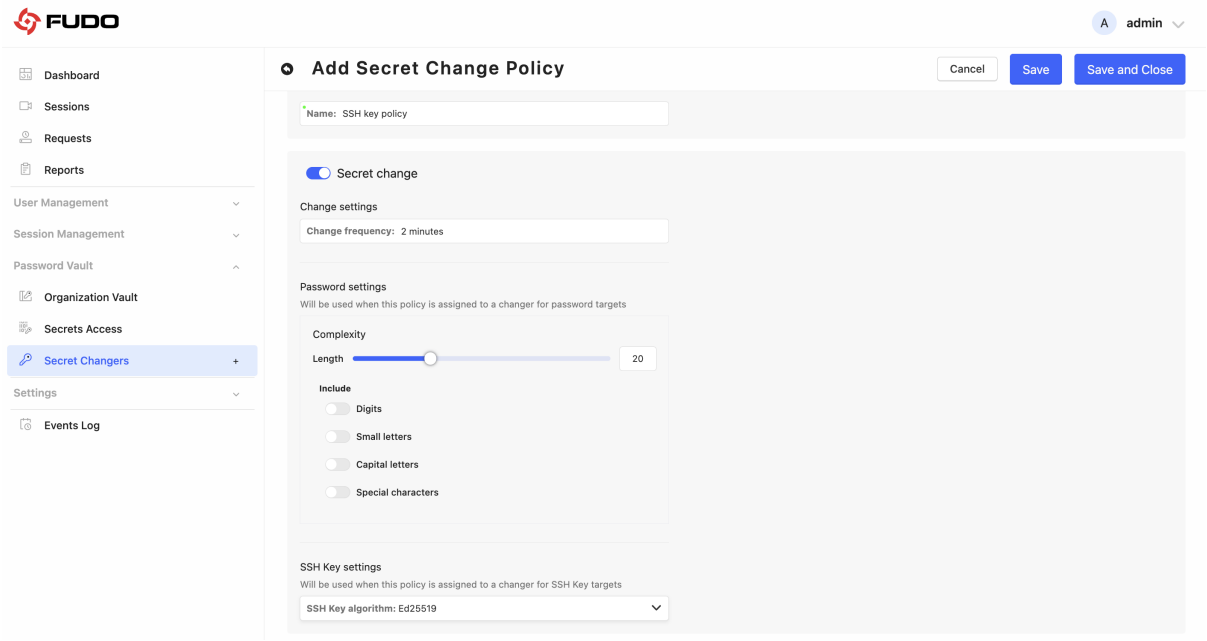
20.8.1 Creating a Secret Change Policy

A secret change policy defines how often the key is rotated and which key algorithm is generated. Create it before the changer so that it can be selected in the changer's *Settings* section.

1. Select *Password Vault* > *Secret Changers* and go to the *Secret Change Policies* tab.
2. Click *+ Add Secret Change Policy*.
3. In the *Name* field, enter a unique name (e.g., `SSH key policy`).
4. Enable *Secret change* and, in the *Change frequency* field, define how often the key is rotated.
5. In the *SSH Key settings* section, from the *SSH Key algorithm* drop-down list, select the algorithm to generate (e.g., `Ed25519`).
6. Click *Save*.

Note

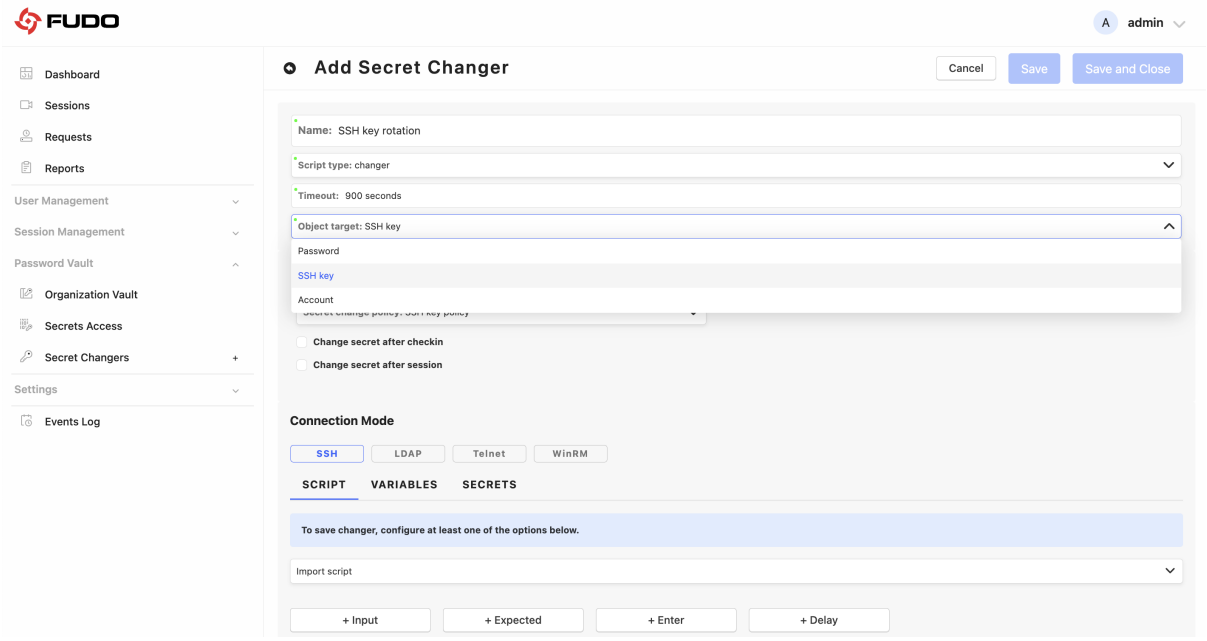
The *SSH Key settings* apply only when the policy is assigned to a changer whose *Object target* is *SSH key*.



20.8.2 Creating an SSH Key Secret Changer

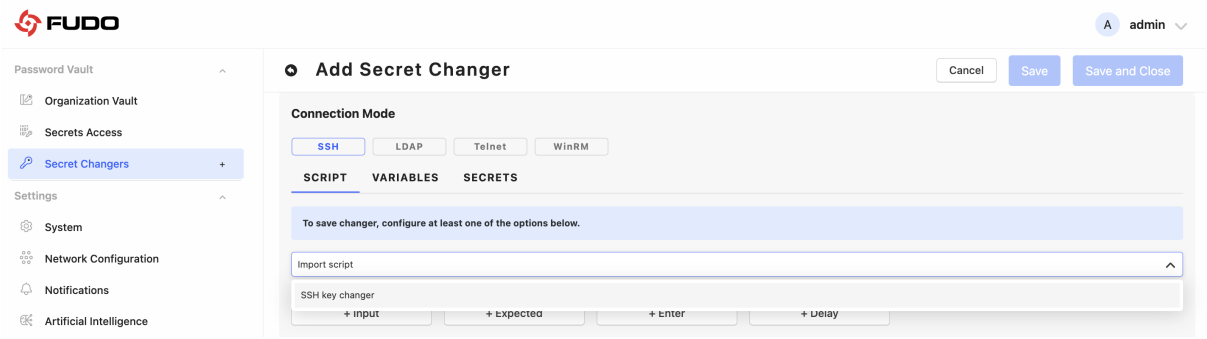
1. Select *Password Vault* > *Secret Changers* and click *+ Add Secret Changer*.
2. In the *Name* field, enter a unique name (e.g., `SSH key rotation`).
3. From the *Script type* drop-down list, select `changer`.
4. In the *Timeout* field, define the script's execution time limit.
5. From the *Object target* drop-down list, select **SSH key**.

> **Note**
>
> After you select **SSH key**, a *Settings* section appears where you can select a *Secret change policy* and, optionally, enable *Change secret after checkin* and *Change secret after session*.



6. In the *Settings* section, from the *Secret change policy* drop-down list, select the policy created above (`SSH key policy`). Use `Static, without restrictions` instead when the key should not be regenerated on a schedule.
7. In the *Connection Mode* section, select the transport layer (typically *SSH*).
8. In the *SCRIPT* tab, add the commands that deploy the new key on the target host.

> **Note**
>
> Instead of entering the commands manually, you can load the built-in `SSH key changer` script from the *Import script* drop-down list and adjust it as needed.



The example below (for a Linux host) writes the newly generated public key to the user's `authorized_keys` file:

	Action	Command
1	EXPECTED	`Last login:`
2	INPUT	`mkdir -p /home/%%secret_login%%/.ssh`
3	INPUT	`echo %%new_ssh_public_key%% > /home/%%secret_login%%/.ssh/authorized_keys`
4	INPUT	`chown -R %%secret_login%%:%%secret_login%% /home/%%secret_login%%/.ssh`
5	INPUT	`chmod 700 /home/%%secret_login%%/.ssh`
6	INPUT	`chmod 600 /home/%%secret_login%%/.ssh/authorized_keys`
7	INPUT	`logout`
8	EXPECTED	`closed`

Note

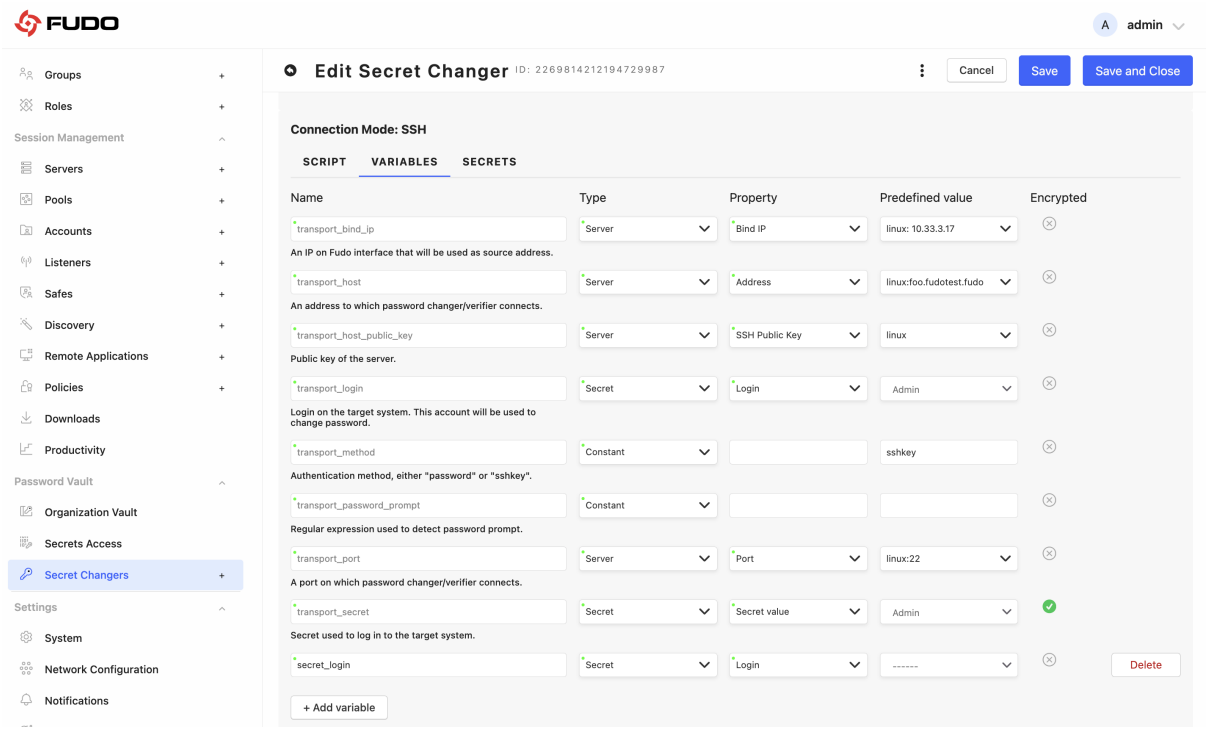
For an *SSH key* target, the `%%secret_login%%` variable is the login stored in the rotated secret, and `%%new_ssh_public_key%%` is the public part of the key that Fudo Enterprise generates according to the assigned policy.

9. In the *VARIABLES* tab, fill in every required field (marked with a red dot). Initialize the transport variables (`transport_bind_ip`, `transport_host`, `transport_port`, `transport_host_public_key`) from the target server object — in this example, the `linux` server. Then set the following:

   - `transport_method` – change the *Predefined value* from `password` to `sshkey`.
   - `transport_login` – set *Type* to `secret` and *Property* to `login`, then select the privileged secret used to connect (e.g., `Admin_314`) as the *Predefined value*.
   - `transport_secret` – set *Type* to `secret` and *Property* to `secret value`, then select the same privileged secret (e.g., `Admin_314`) as the *Predefined value*.
   - `secret_login` – the login of the regular user, stored in the secret whose key will be changed. Leave it set to `------` so that the changer can operate on any secret it is run against (self).

Important

The `transport_method` variable defaults to `password`. For SSH key rotation you must change its *Predefined value* to `sshkey` manually; otherwise the changer will not authenticate to the target host with the key.



10. Click *Save*.

> **Note**
>
> Create a matching *SSH key* verifier the same way (set *Script type* to `verifier`) if you also want Fudo Enterprise to verify the key stored on the target host.

20.8.3 Storing the SSH Key in the Password Vault

The SSH key that will be rotated must be stored as an *SSH Key* secret in the Password Vault.

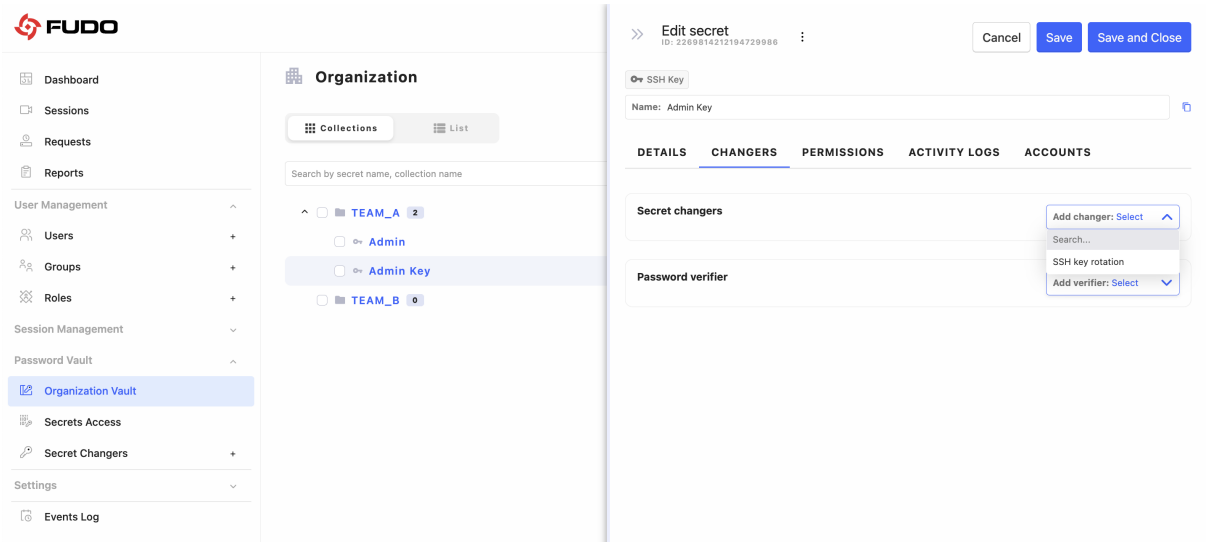
1. Select *Password Vault* > *Organization Vault*.
2. Click *Add secret*, select the **SSH Key** type, and define the secret.

> **Note**
>
> If the secret already exists (for example, it was created together with the account), you can skip this step.

20.8.4 Assigning the Changer to the Secret

1. Select *Password Vault* > *Organization Vault* and open the *SSH Key* secret.
2. Go to the *CHANGERS* tab.
3. In the *Secret changers* field, select your SSH key changer from the *Add changer* drop-down list.
4. Optionally, in the verifier field, select an SSH key verifier from the *Add verifier* drop-down list.

5. Click *Save*.



Note

The *Add changer* and *Add verifier* drop-down lists show only secret changers whose *Object target* matches the secret type — for an *SSH Key* secret, only *SSH key* changers appear.

20.8.5 Pointing the Account at the Secret

Finally, make the account use the Password Vault secret so that it always presents the current key.

1. Select *Session Management* > *Accounts* and open (or create) the account.
2. In the *SETTINGS* tab, in the *Credentials* section, set *Replace secret with* to *Password Vault*.
3. From the *Secret name* drop-down list, select the *SSH Key* secret configured above.
4. Click *Save*.

Note

Because the key is managed through the Password Vault, the account's SECRET CHANGERS tab stays inactive — this is expected. Rotation is driven by the changer assigned to the secret, not by the account.

Related Topics:

- *Secret Changers*
- *Custom Secret Changers*
- *Accessing Secret Editing*
- *Creating a Regular Account*

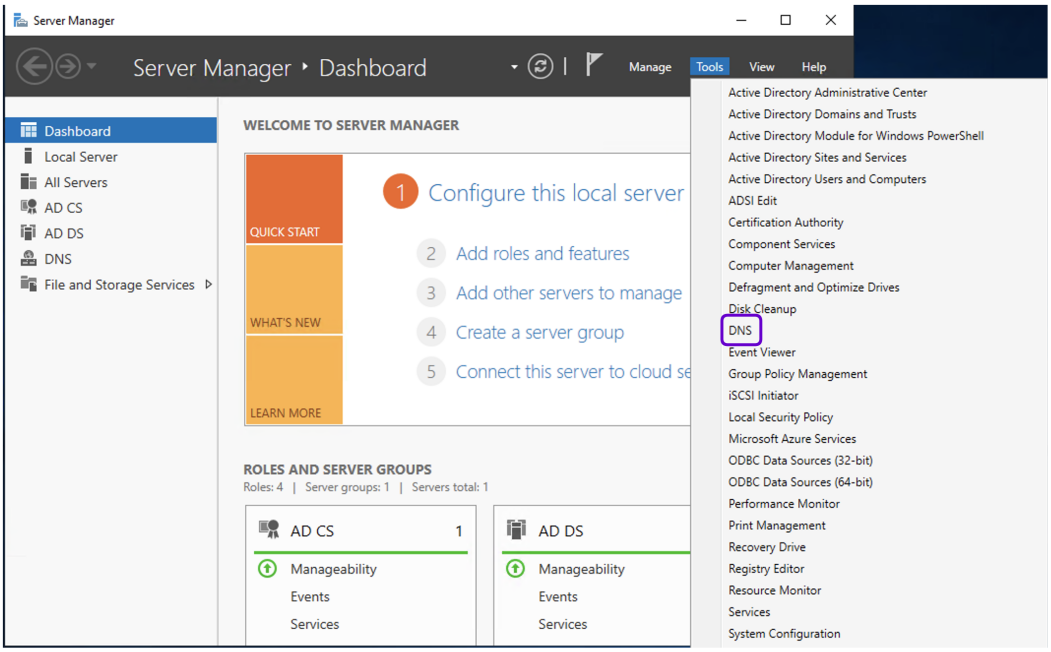
20.9 Configuring Kerberos Constrained Delegation for MSSQL(TDS) Server

> **Note**
>
> Please note that this is a general guide, and specific details may vary depending on your Windows Server setup. Refer to the Windows Server documentation for precise configuration steps.

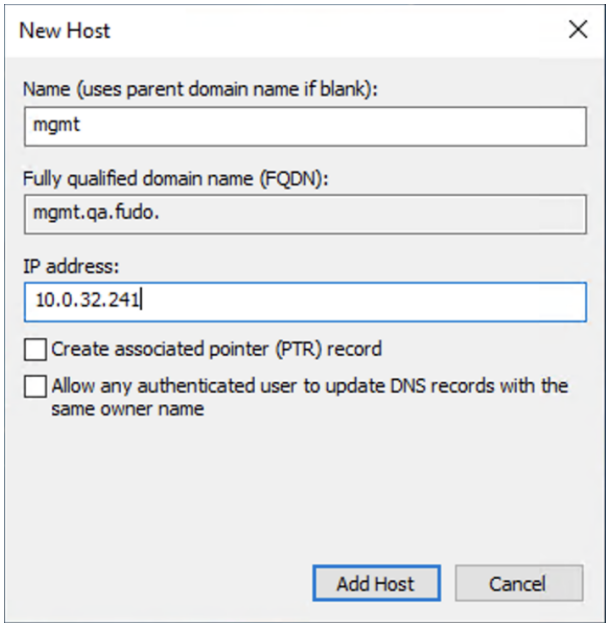
20.9.1 Kerberos Authentication Configuration on Windows Server

Configure DNS Entry:

1. Open the *Server Manager* application.
2. Click *Tools* button on the upper right corner of the window to expand the menu list and select *DNS*.



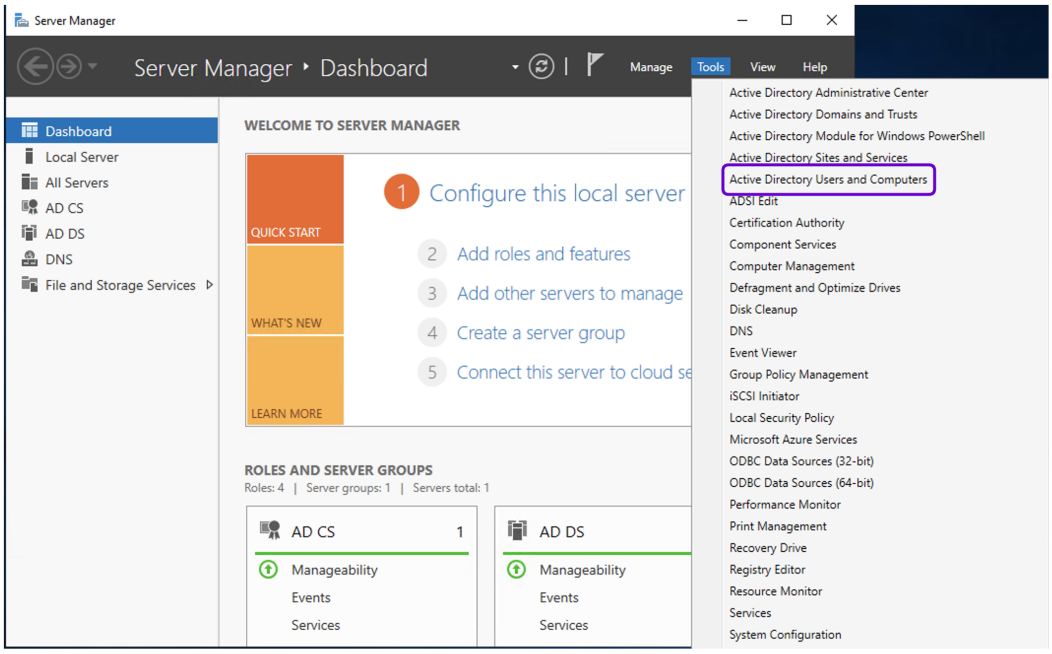
3. Go to *Forward Lookup Zones*.
4. Add an A record: right click on the selected domain name and click *New Host (A or AAAA)*.
5. Provide the *Name* and *IP address* of the Fudo Enterprise Admin Panel (e.g., `mgmt.qa.fudo, 10.0.32.241`).
6. Click *Add Host*.



Create Service User Account:

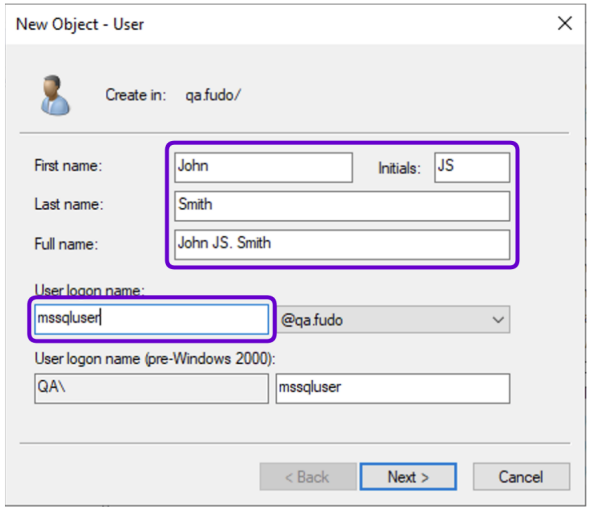
In this section we add the service user `mssqluser`, which will represent the MSSQL service in the domain.

1. Log in to the server on which you want to setup the Kerberos using the administrator account.
2. Open the *Server Manager* application.
3. Click *Tools* button on the upper right corner of the window to expand the menu list and select *Active Directory Users and Computers*.

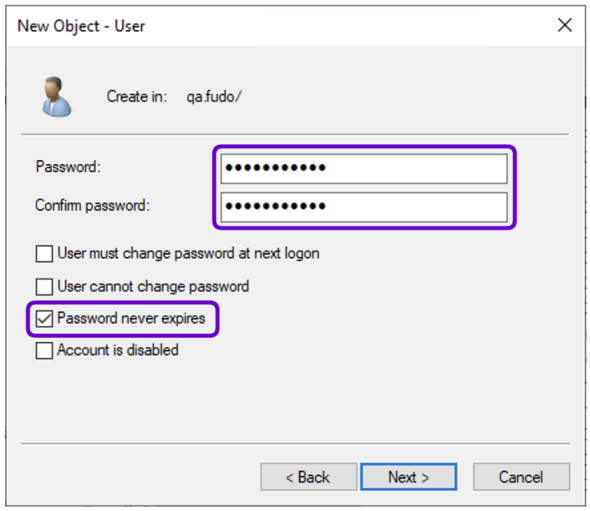


4. In the Manager window, navigate to the domain name, or a specific user group, and right-click on the *Users* catalog.
5. Select *New* > *User*.

6. Create a user (e.g., User logon name: `mssqluser`).



7. Click *Next.*
8. Provide the password for created user (e.g., `PaSSwOrD`) and select *Password never expires* option.
9. Click *Next* and *Finish.*



10. Add an SPN (Service Principal Name) by running the following command in the PowerShell or CMD console:

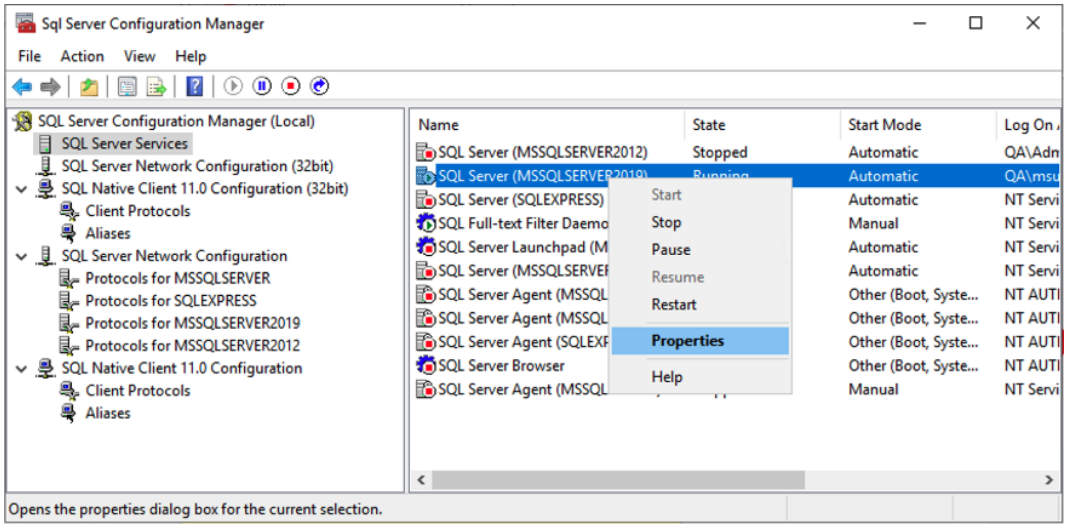
    ```
    setspn -S <service class>/<server name>.<domain>:<port>
    <service account>
    ```

    Example:

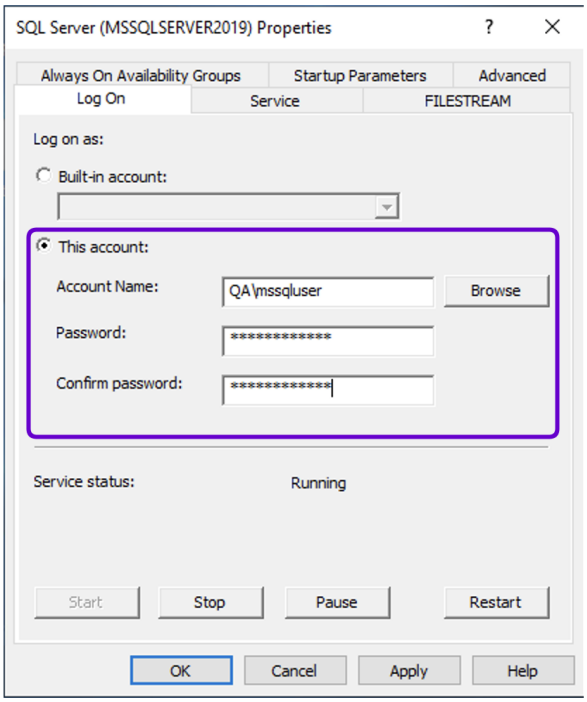
    ```
    setspn -S MSSQLSvc/WIN2019-DC1.qa.fudo:1433 mssqluser
    ```

SQL Server Configuration Manager:

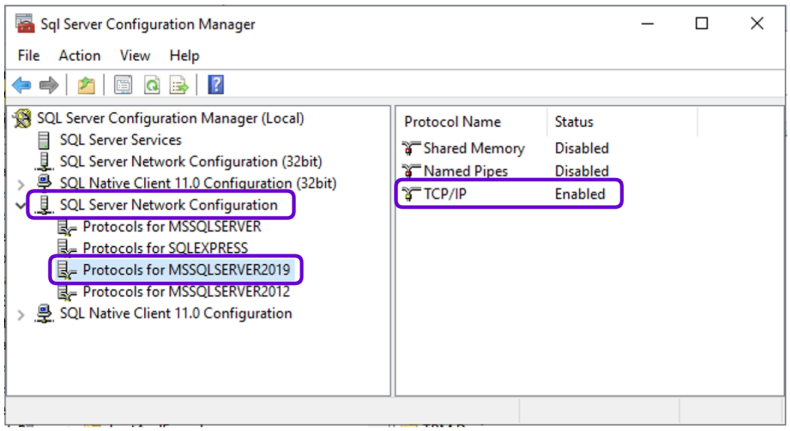
1. Launch SQL Server Configuration Manager.
2. Expand SQL Server Services, select the server, and open the Properties.



3. In the Log On tab, enter the authentication credentials for the `mssqluser` account.



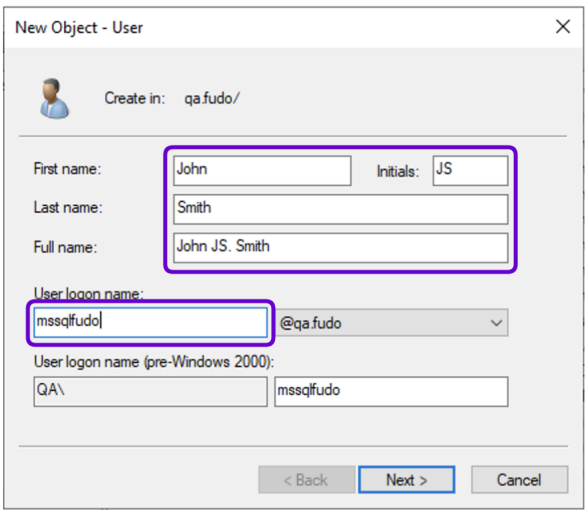
4. Expand SQL Server Network Configuration, select the server, and ensure that the TCP/IP connection is enabled.



Create Service User representing MSSQL on Fudo:

In this section add the service user account `mssqlfudo`, which will represent the MSSQL service in Fudo Enterprise.

1. Open the *Server Manager* application.
2. Click *Tools* button on the upper right corner of the window to expand the menu list and select *Active Directory Users and Computers.*
3. In the Manager window, navigate to the domain name, or a specific user group, and right-click on the *Users* catalog.
4. Select *New* > *User.*
5. Create a user who will use the Kerberos delegation to log in to MSSQL(TDS) server (e.g., User logon name: `mssqlfudo`).



6. Click *Next.*
7. Provide the password for created user (e.g., `PaSSwOrD`) and select *Password never expires* option.
8. Click *Next* and *Finish.*
9. Add an SPN (Service Principal Name) by running the following command in the PowerShell or CMD console:

```
setspn -S <service class>/<fudo admin panel name>:<port>
<service account>
```

Example:

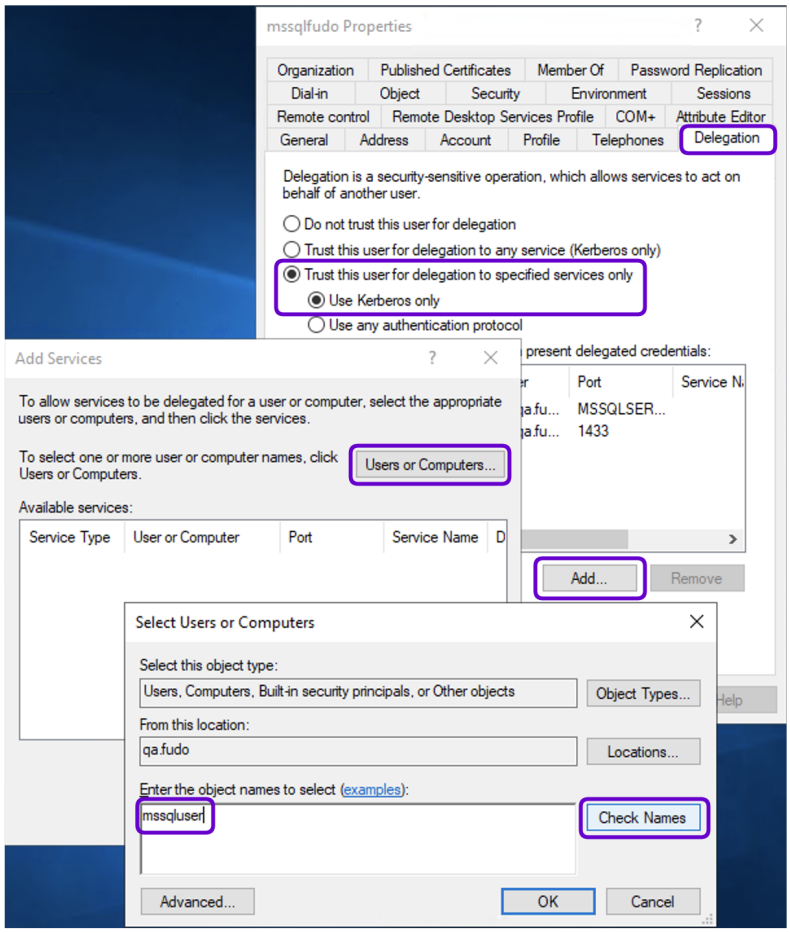
```
setspn -S MSSQLSvc/mgmt.qa.fudo:1433 mssqlfudo
```

Kerberos Delegation

Note

- When the SPN is set for user `mssqlfudo`, a new tab called *Delegation* appears in the user modification window.
- If the *Delegation* tab is not visible, you may need to refresh the *Active Directory Users and Computers* management console.

1. Right-click on the `mssqlfudo` account (created in the previous steps) in the Active Directory Users and Computers window, and select Properties.
2. Go to the Delegation tab.
3. Select *Trust this user for delegation to specified services only.*
4. Choose *Use Kerberos only.*
5. Add the Services:
   - Click the *Add* button.
   - In the *Select Users or Computers* window, type `mssqluser` and click *Check Names* to ensure accuracy.
   - Click *OK* to proceed.



6. Select Services for Delegation:
   - In the *Add Services* window, you will see a list of SPNs associated with the `mssqluser` account.
   - Select all available services, or choose specific SPNs if needed.
   - Click *OK* to confirm the selection.
7. Click *Apply* and then *OK* to save the settings.
8. If changes are not immediately visible, refresh the *Active Directory Users and Computers* console by pressing F5 or right-clicking on the Users container and selecting *Refresh*.

Generate Keytab:

1. Run the following command in the Powershell or CMD console:

```
ktpass -princ HTTP/hostname.yourdomain.local@yourdomain.
local  -mapuser netbios_domain_name\username -pass password
-ptype KRB5_NT_PRINCIPAL -crypto AES256-SHA1 -out hostname.
yourdomain.local.keytab
```

   - Example for this use case:

```
ktpass -princ MSSQLSvc/mgmt.qa.fudo:1433@QA.FUDO -mapuser
QA\mssqlfudo        -pass PaSSwOrD -pType KRB5_NT_PRINCIPAL
-crypto AES256-SHA1 -out mssqlfudo.keytab
```

> **Note**
>
> By default, the `ktpass` command creates a keytab file that uses the RC4 encryption algorithm. Starting with Windows Server 2025 (the April 2025 update), RC4 is disabled by default, so such a keytab will not work. The `-crypto AES256-SHA1` parameter forces generating an AES-based keytab (without RC4).

2. Copy the generated keytab file to the workstation where you will be configuring Fudo.

> **Note**
>
> It is an alternative authentication method to using a password. The password must match the one specified when creating the user. If the user's password is changed, their keytab will be invalidated.

20.9.2 Setup Fudo Enterprise

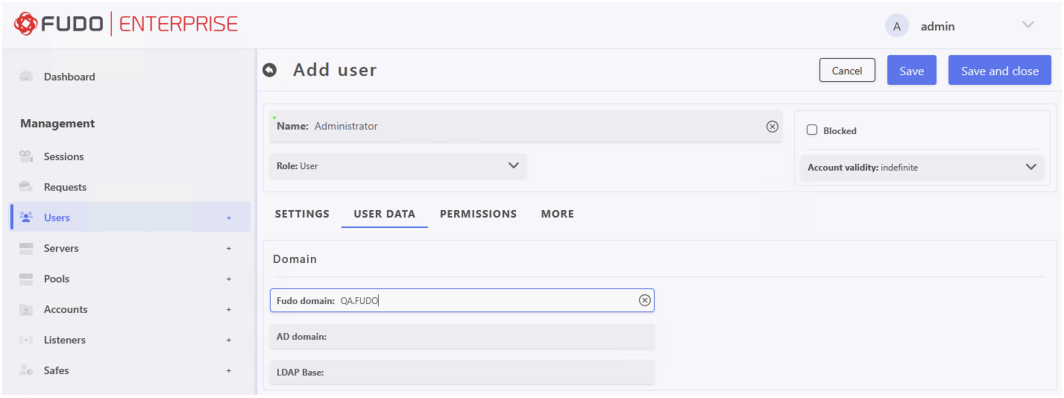
Configure DNS:

1. Go to *Settings* > *Network configuration*.
2. Switch to the *Name & DNS* tab.
3. Configure DNS server to point to a DNS server in the *yourdomain.local* domain (in this example we will use a domain controller IP address):
   - Click *Add DNS server* to define new DNS server.
   - Enter DNS server IP address (e.g., `10.0.242.100`).
   - Click *Save*.

Create User in Fudo:

1. Select *User Management* > *Users* and then click + *Add user*.
2. Enter the user name that matches created in previous steps user account in Active Directory (e.g., `Administrator`).
3. Select the `user` role.
4. In the *Settings* tab, under the *Safes* section, select *main* to grant access rights to the Admin Panel.
5. Click *Save*.
6. Go to the *User Data* tab, and fill in the *Fudo domain* (e.g., `QA.FUDO`).

> **Note**
>
> The *Fudo domain* should match the domain name specified in the Kerberos ticket.



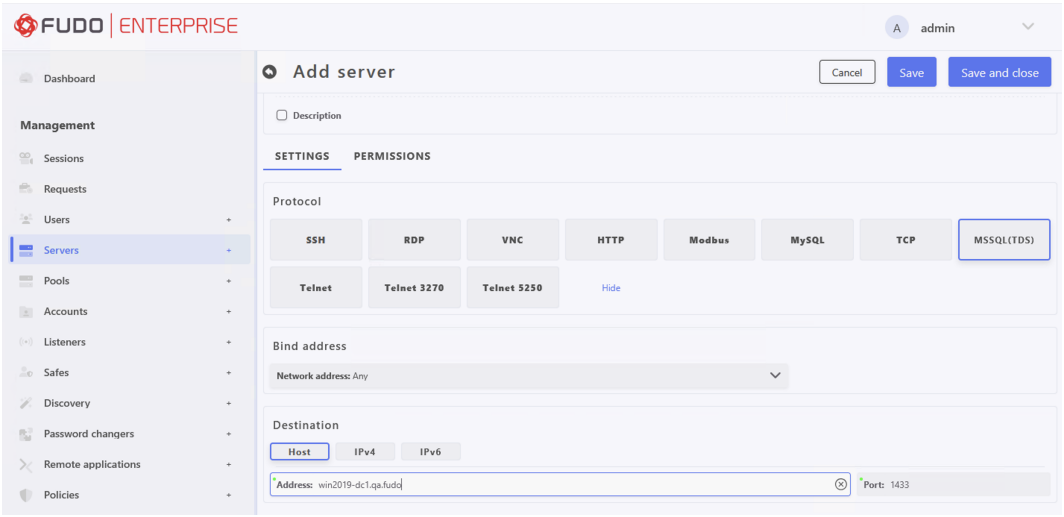
7. If necessary, please fill in the remaining parameters as needed for your specific configuration. For more details, please refer to the *Creating a User* section.
8. Click *Save and close*.

Configure MSSQL(TDS) Server:

1. Select *Management* > *Servers* and then click *+ Add server*.
2. Enter server's unique name (e.g., `tds`).
3. In the *Settings* section on the list of available protocols select `MSSQL(TDS)`.
4. In the *Destination* section select `Host` and enter server's host name (in our example, `win2019-dc1.qa.fudo`).

> **Note**
>
> For Kerberos authentication to target systems to work correctly, the **Destination** field in the server configuration must be set to `Host` (hostname). Kerberos relies on hostname-based SPN (Service Principal Name) resolution. Configuring the destination using an IP address will result in authentication failure.

5. Enter port: `1433`.



6. Click *Save and close*.

Configure Account:

1. Select *Management* > *Accounts* and then click + *Add account*.
2. Define object's name (e.g., `tds:forward`).
3. In the *Type* section select *FORWARD*.
4. In the *Target* section select *Server* button, and from the drop down list select server created in previous step (e.g., `tds`) to assign created account to this server.
5. In the *Replace secret with* section select *None*.
6. Click *Save*.

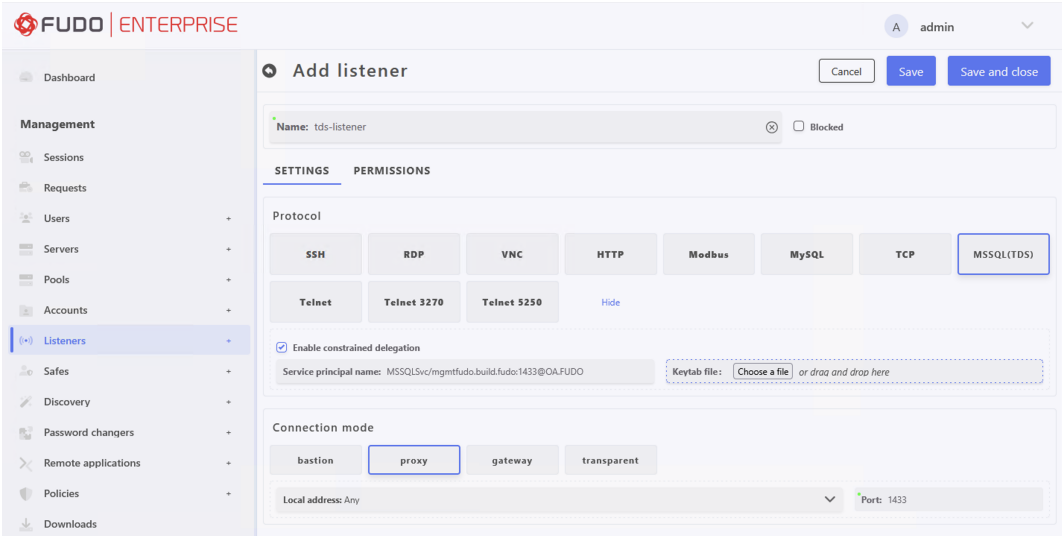
> **Note**
>
> The *forward* account type is recommended in this scenario because *S4U2Proxy* delegation requires using the existing user ticket to authenticate against the TDS server. Therefore, the username of the user who logged in to Fudo Enterprise is always used, and the credentials entered for the account will not be utilized.

Configure Listener

1. Select *Management* > *Listeners* and then click + *Add listener*.
2. Enter listener's unique name (e.g., `tds-listener`).
3. Go to *SETTINGS* tab and press the `MSSQL(TDS)` button in the *Protocol* field.
4. Select *Enable constrained delegation* option.
5. In the *Service principal name* field, enter the following: `MSSQLSvc/mgmt.qa.fudo:1433@QA.FUDO`.
6. Upload Keytab file.
7. In the *Connection mode* section, select `proxy`.

> **Note**
>
> It is possible to use `bastion` mode, but it will not be possible to use bastion login strings.

8. Set the local address (e.g., `Any`), and port `1433`.



9. Click *Save and close*.

Configure Safe:

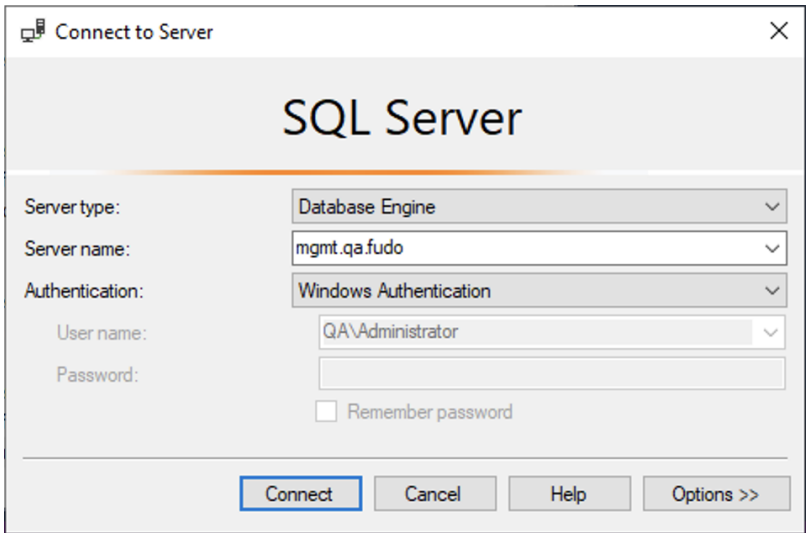
1. Select *Management* > *Safes* and then click + *Add safe*.
2. Enter safe's unique name (e.g., `tds-safe`).
3. Click *Save* to save the object and proceed with further configuration.
4. Go to the *Users* tab to assign users allowed to access accounts assigned to this safe.
   - Click *Manage users*.
   - Mark the checkbox in front of the users' names to enable their server access through the monitored safe (e.g., `Administrator`).
   - Click *Save* to close the modal window.
5. Select *Accounts* tab to add *accounts* accessible through this safe.
   - Click *Manage accounts*.
   - Mark the checkbox in front of the accounts' names to add it (e.g., `tds:forward`).
   - Click *Save* to close the modal window.
   - Select desired account and click *Manage listeners* to assign listener to account (e.g., `tds-listener`).
   - Click *Save* to close the modal window.
6. Click *Save and close* to save the safe configuration.

20.9.3 Establish a Connection

To establish a connection:

1. Run the SQL client application.
2. Select *File* > *Connect object explorer...*.

3. In the *Server name* field provide the Fudo Enterprise Admin Panel name set in the DNS entry: *mgmt.qa.fudo*.
4. From the *Authentication* list select *Windows Authentication*.
5. Click *Connect*.



Note

Logging in using typical *SQL Server Authentication* is also possible when using a listener with constrained delegation enabled.

Related topics:

- *Creating a MS SQL Server*
- *Setting up the MS SQL Listener*
- *Authentication*

20.10 Establishing Connections to Servers via SSH Tunnel in Fudo Enterprise

This chapter describes how to establish connections to various types of servers (SSH, Oracle, HTTP) via an SSH tunnel in Fudo Enterprise. The step-by-step guide presents the configuration of required objects (user, listener, server, account, safe), PuTTY client setup, and methods for initiating connections from a terminal, web browser, or a dedicated client—depending on the type of resource.

20.10.1 General Requirements

To establish a connection via SSH tunnel in Fudo Enterprise, the following objects must be created:

- A **user** authorized to initiate connections,
- A **listener** of type `Tunnel`,
- A **target server** (SSH, TCP, or HTTP),

- An **account** used to authenticate to the target server,
- A **safe** containing the above objects.

20.10.1.1 Establishing an SSH Connection

User Configuration

1. Go to *User Management* > *Users* and click + *Add user*.
2. Enter a name (e.g., `Tunnel_User`) and click *Save*.
3. Select the user authentication method:
   - Choose e.g. *Static password* from the *Add authentication method* dropdown.
   - Enter the password for the created user (e.g., `TestPassw0rd`).
   - Click *Save* to close the dialog.
4. Click *Save and exit*.

Creating a Listener

1. From the left menu, select **Management** > **Listeners** and click + **Add listener**.
2. Enter a unique name (e.g., `SSH_Tunnel`).
3. Go to the **Settings** tab and press the **SSH** button in the **Protocol** field.
4. In the **Connection mode** section, select **Tunnel**.
5. From the **Local address** list, select an IP address and port (e.g., `3455`).
6. Click **Save**.

> **Note**
>
> The **Keys** field displays generated SSH, TLS, and Standard RDP Security keys as well as a TLS certificate required for proper operation of a "Tunnel"-type listener.

SSH Server Configuration

1. From the left menu, select **Management** > **Servers** and click + **Add server**.
2. Enter a name (e.g., `SSH_Tunnel_Server`).
3. In the **Settings** section, choose **SSH** as the protocol.
4. In the **Destination** section: - Choose **Host, IPv4** or **IPv6**. - Enter the address and port (e.g., `192.168.0.100`, port: `22`).
5. Click **Save and exit**.

Account Configuration

1. Select **Management** > **Accounts**, click + **Add account**.
2. Enter a name (e.g., `Tunnel_Account`).

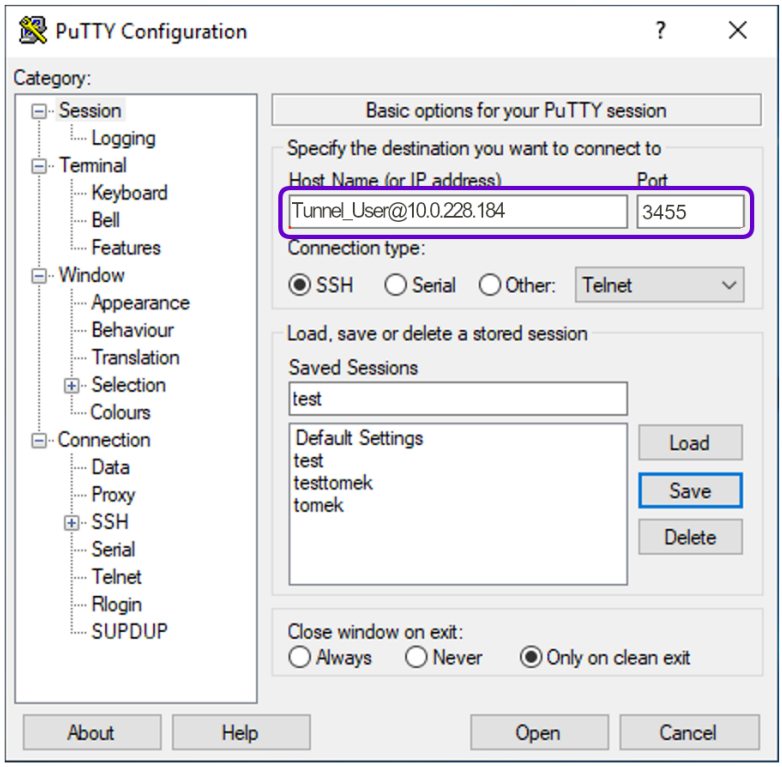
3. In the **Settings** tab, under **Type**, select **REGULAR**.
4. In the **Target** section, select the `SSH_Tunnel_Server`.
5. In the **Credentials** section: - Enter the login (e.g., `admin`). - Click the button in the **Replace secret** section, choose e.g. **Password**, and enter the password.
6. Click **Save**, then **Save and exit**.

Safe Configuration

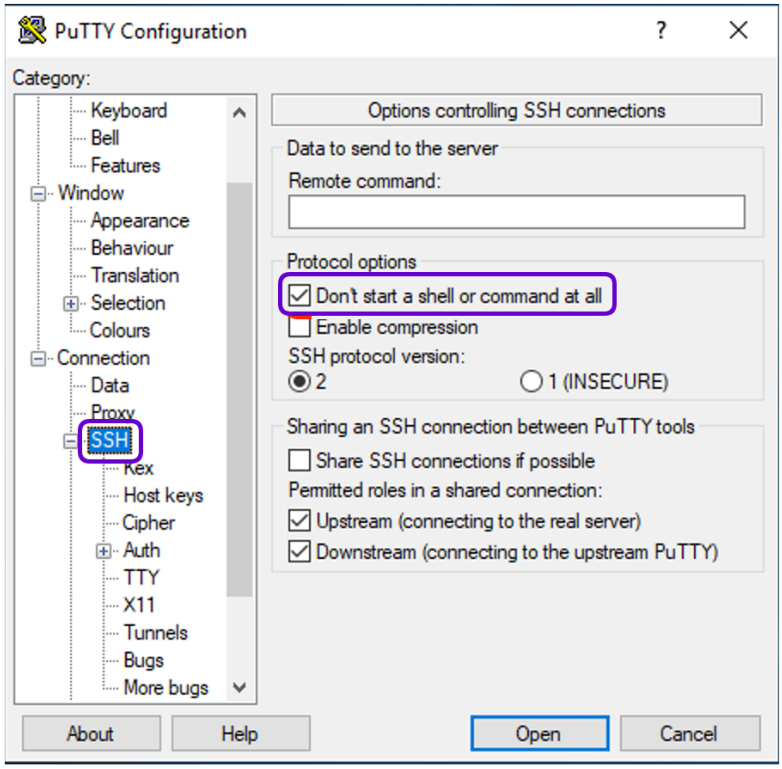
1. Select **Management** > **Safes** and click + **Add safe**.
2. Enter a name (e.g., `Tunnel_Safe`), click **Save**.
3. In the **Users** tab, click **Manage users** and select the `Tunnel_User`.
4. Click **Save**.
5. In the **Accounts** tab, click **Manage accounts** and select `Tunnel_Account`.
6. Click **Save**.
7. Select `Tunnel_Account`, click **Manage listeners**, and select `SSH_Tunnel`.
8. Click **Save**, then **Save and close**.

PuTTY Configuration

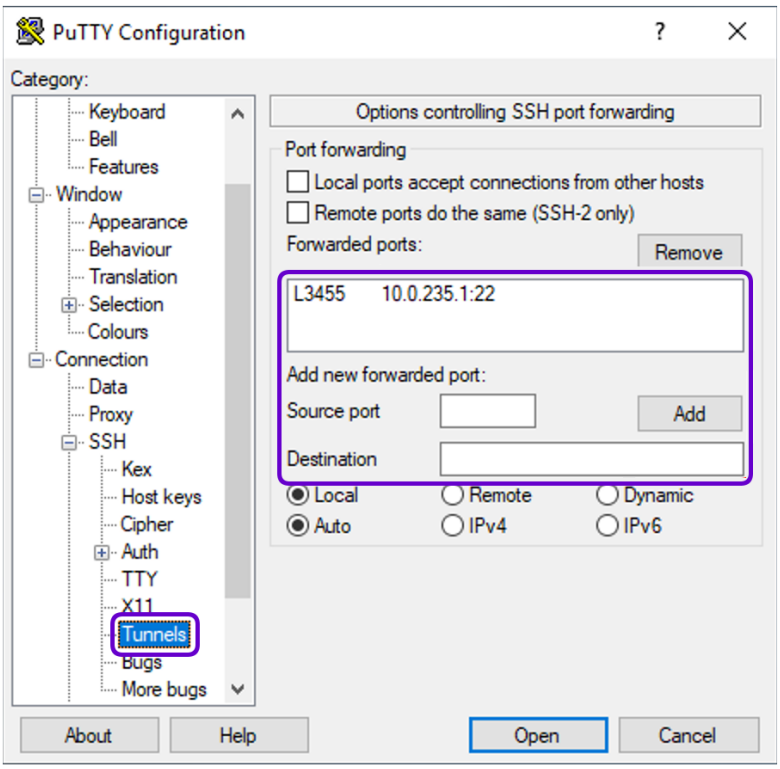
1. Launch PuTTY.
2. In the **Host Name** field, enter `<Fudo_user>@<Fudo_IP_address>`, e.g., `Tunnel_User@10.0.228.184`.
3. In the **Port** field, enter the port of the previously created *Tunnel*-type listener (e.g., `3455`).



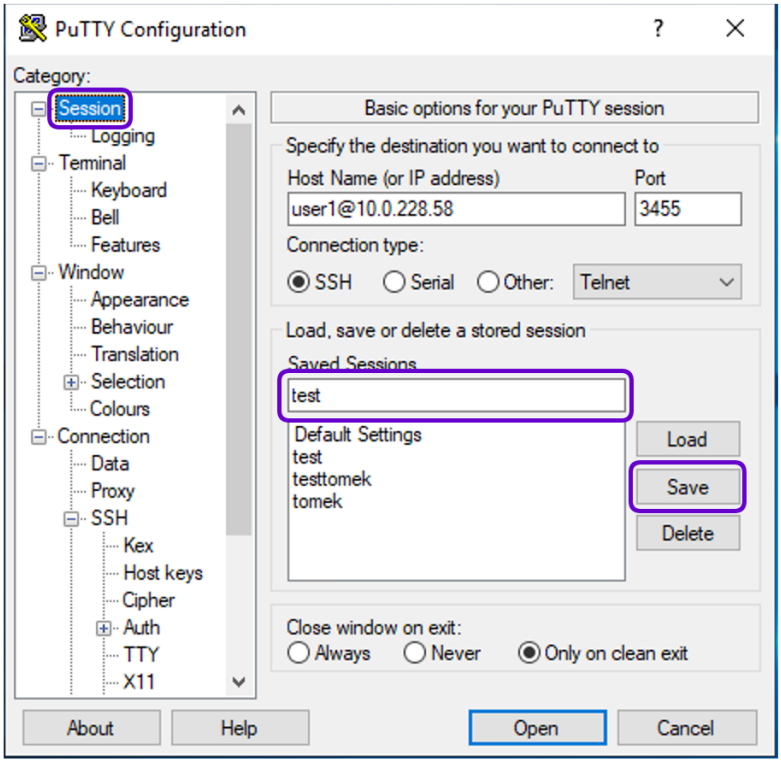
4. Go to the **SSH** tab and check **Don't start a shell or command at all**.



5. Go to the **Tunnels** tab and add a forwarded port:
   - **Source port**: enter the port to be forwarded (e.g., `3455`).
   - **Destination**: enter the destination server address and port in the format `<destination_server_address>:<port>` (e.g., `192.168.0.100:22`).
   - Click **Add**.



6. Return to the **Sessions** tab and save the configuration.



7. Click **Open**.
8. In the displayed terminal, enter the password for the Fudo user created earlier (`TestPassw0rd`).
9. The tunnel has been established.

10. Open a new terminal window and enter the following command to connect to the server `192.168.0.100` through the tunnel:

```
ssh -l "<Fudo_user>#<Server_user>#<Server_address>" localhost -p <Tunnel_
↪listener_port>
```

Example:

```
ssh -l "Tunnel_User#admin#192.168.0.100" localhost -p 3455
```

Connection Without PuTTY

The tunnel can also be established directly from the terminal without using PuTTY by executing the following commands:

- Establish the SSH tunnel:

```
ssh -N -l <Fudo_user> <Fudo_IP> -p <Listener_port_tunnel> -L <Listener_port_
↪tunnel>:<Server_address>:<server_port>
```

- Connect via the established SSH tunnel:

```
ssh -l '<Fudo_user>#<server_user>#<server_address>' localhost -p <Listener_port_
↪tunnel>
```

Option explanation:

- `-N`: establish the SSH connection without executing remote commands or opening a shell.
- `-l`: specifies the username to connect with.
- `-p`: specifies the port the SSH server listens on.

You may also consider using:

- `-f`: runs the SSH connection in the background, often used with `-N` for tunneling.
- `-n`: redirects standard input (stdin) to `/dev/null`, useful for background tasks.

Example:

```
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
```

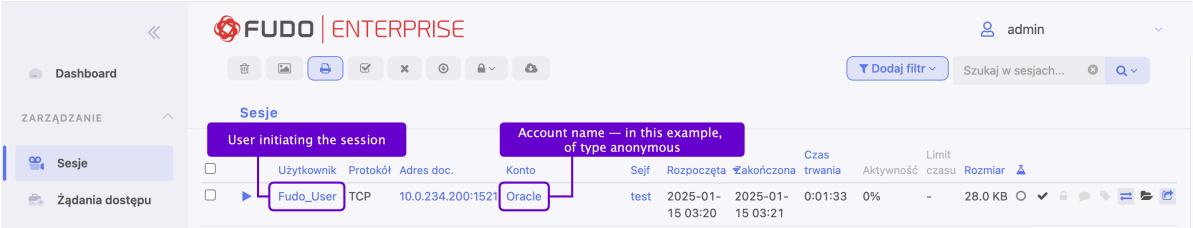
Note

If the target server is configured to use an SSH reverse tunnel (the **Use SSH tunnel** option in the server configuration), see *Connection to a Server with Reverse Tunnel via Tunnel-type Listener*.

Session List View

After the connection is established, an entry for the tunnel session will appear in the **Management** > **Sessions** tab with the following details:

- Fudo username (also for anonymous accounts),
- Session protocol,
- Destination server address,
- Account name used for the connection,
- Safe name,
- Session start and end time,
- Session duration.



20.10.1.2 Establishing an HTTP Connection

User Configuration

1. Go to *User Management* > *Users* and click + *Add user*.
2. Enter a name (e.g., `Tunnel_User`) and click *Save*.
3. Choose the user authentication method:
   - Select e.g. *Static password* from the *Add authentication method* dropdown.
   - Enter the password for the new user (e.g., `TestPassw0rd`).
   - Click *Save* to close the dialog.
4. Click *Save and exit*.

Creating a Listener

1. From the left menu, select **Management** > **Listeners** and click + **Add listener**.
2. Enter a unique name (e.g., `HTTP_Tunnel`).
3. Go to the **Settings** tab and in the **Protocol** field, press **SSH**.
4. In the **Connection mode** section, select **Tunnel**.
5. From the **Local address** list, select an IP address and port (e.g., `3455`).
6. Click **Save**.

> **Note**
>
> The **Keys** field displays generated SSH, TLS, and Standard RDP Security keys and the TLS certificate required for proper operation of a "Tunnel"-type listener.

HTTP Server Configuration

Create a TCP server configuration:

1. From the left menu, select **Management** > **Servers** and click + **Add server**.
2. Enter a name (e.g., `HTTP_Tunnel_Server`).
3. In the **Settings** section, select **HTTP** as the protocol.
4. In the **Destination** section: - Select **Host**. - Enter the address and port (e.g., `twitter.com`, port: `443`).
5. Click **Save and exit**.

Account Configuration

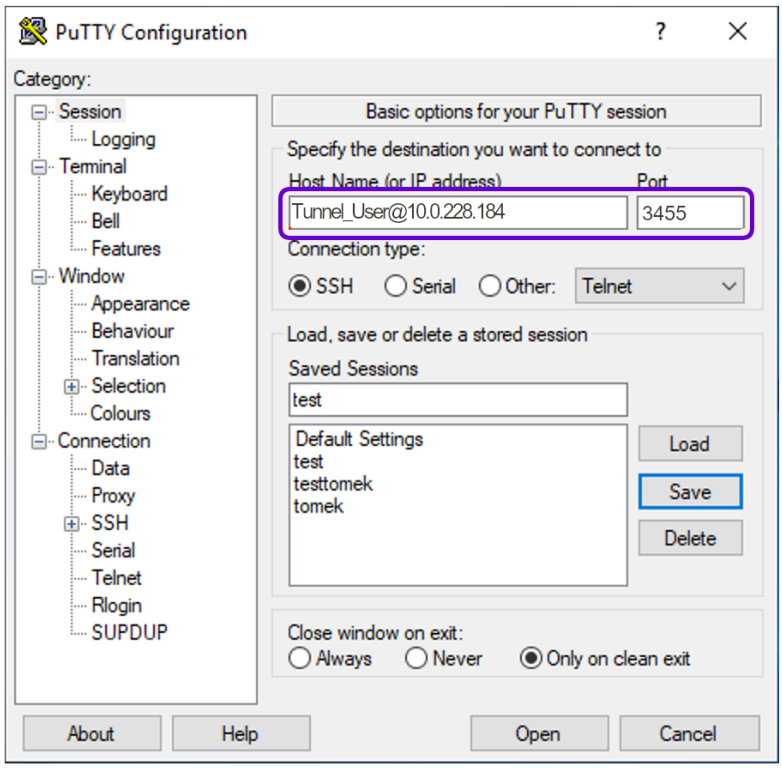
1. Select **Management** > **Accounts**, click + **Add account**.
2. Enter a name (e.g., `HTTP_Tunnel_Account`).
3. Set **Session recording** to **noraw**.
4. In the **Settings** tab, under **Type**, select **FORWARD**.
5. In the **Target** section, select the server `HTTP_Tunnel_Server`.
6. In the **Replace secret** section, select **none**.
7. Click **Save**, then **Save and exit**.

Safe Configuration

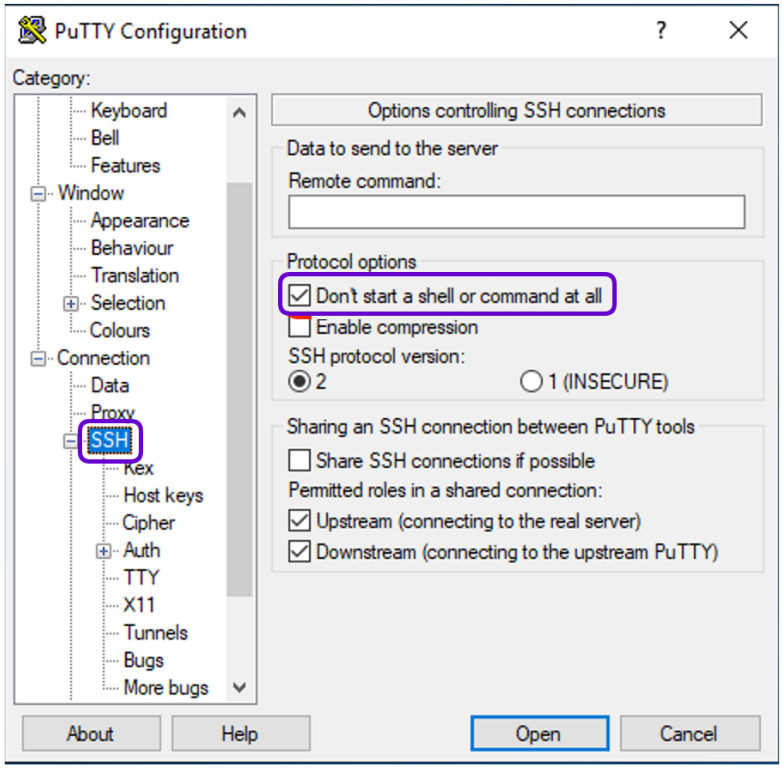
1. Select **Management** > **Safes** and click + **Add safe**.
2. Enter a name (e.g., `Tunnel_Safe`), click **Save**.
3. In the **Users** tab, click **Manage users** and select `Tunnel_User`.
4. Click **Save**.
5. In the **Accounts** tab, click **Manage accounts** and select `HTTP_Tunnel_Account`.
6. Click **Save**.
7. Select `HTTP_Tunnel_Account`, click **Manage listeners**, and select `HTTP_Tunnel`.
8. Click **Save**, then **Save and close**.

PuTTY Configuration

1. Launch **PuTTY**.
2. In the **Host Name** field, enter `<Fudo_user>@<Fudo_IP_address>`, e.g., `Tunnel_User@10.0.228.184`.
3. In the **Port** field, enter the port of the *Tunnel*-type listener created earlier (e.g., `3455`).

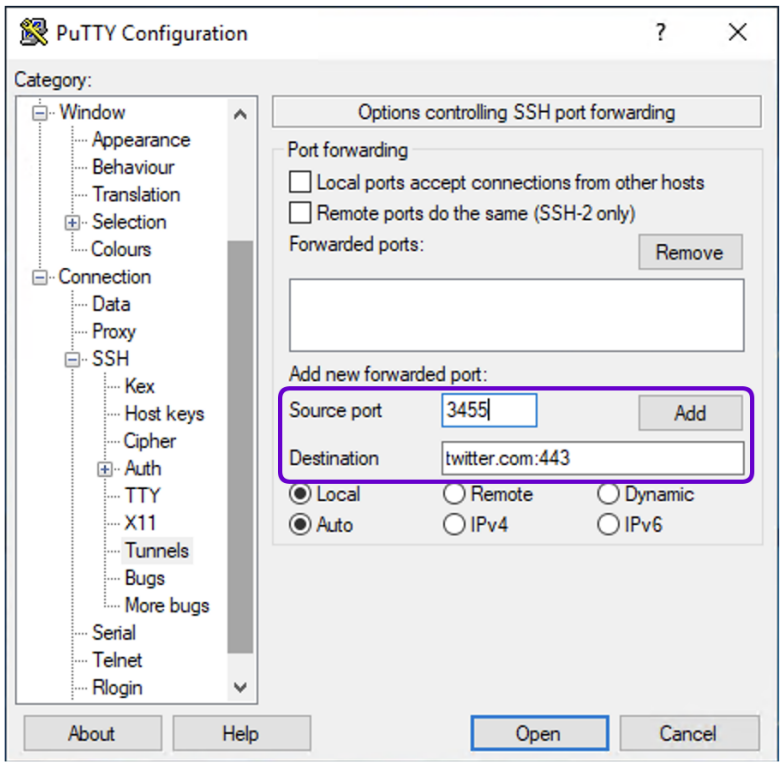


4. Go to the **SSH** tab and check **Don't start a shell or command at all**.

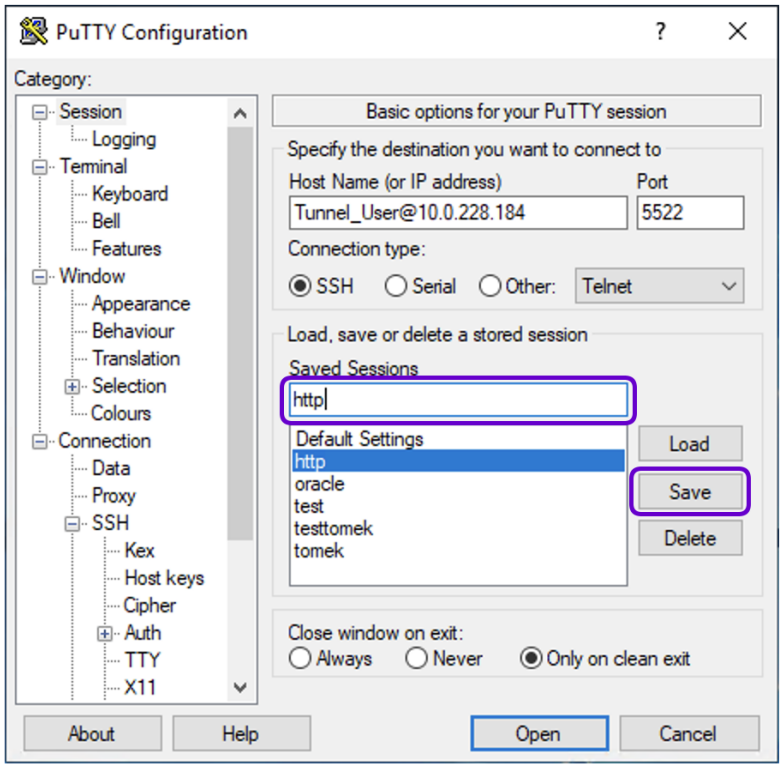


5. Go to the **Tunnels** tab and add a forwarded port:
   - **Source port**: enter the port you want to forward (e.g., 3455).
   - **Destination**: enter the target server address and port in the format `<destination_server_address>:<port>` (e.g., `twitter.com:443`).

- Click **Add**.



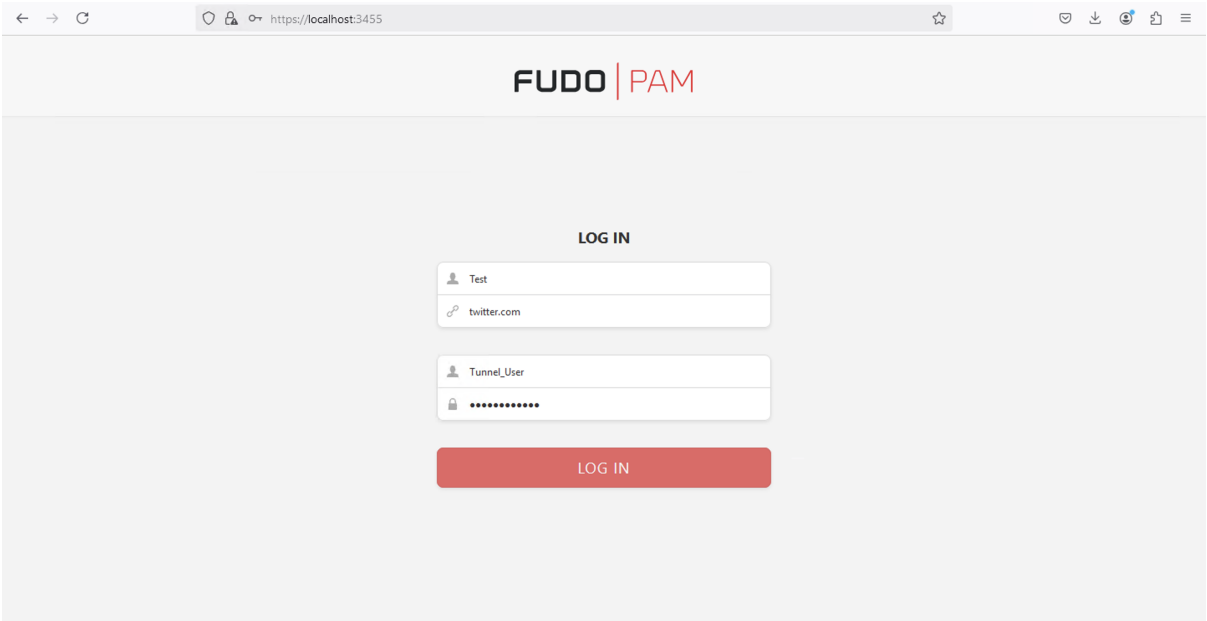
6. Return to the **Sessions** tab, save the configuration, and click **Open**.



7. Enter the password for `Tunnel_User` (e.g., `TestPassw0rd`) and press **Enter**.
8. The tunnel is established.

Connecting via Browser

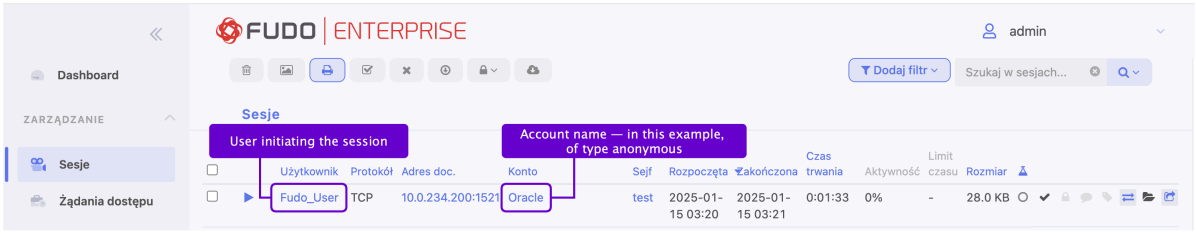
1. Open a web browser.
2. In the address bar, enter the address with the port configured for the listener: `https://localhost:3455`.
3. In the Fudo login screen:
   - **Server login** – enter any name (not used in this scenario),
   - **Server address** – enter the target server address (e.g., `twitter.com`),
   - **Username** – enter the Fudo username (e.g., `Tunnel_User`),
   - **Password** – enter the password for the Fudo user (e.g., `TestPassw0rd`).
4. Click **LOG IN**.



Session List View

After the connection is established, an entry for the session established through the tunnel will appear under **Management** > **Sessions**. The following details will be visible:

- Fudo username (also if an anonymous account was used),
- Session protocol,
- Destination server address,
- Name of the account used for the connection,
- Safe name,
- Session start and end time,
- Session duration.



20.10.1.3 Connecting to an Oracle Database

User Configuration

1. Go to *User Management* > *Users* and click + *Add user*.
2. Enter a name (e.g., `Tunnel_User`) and click *Save*.
3. Choose the user authentication method:
   - Select e.g. *Static password* from the *Add authentication method* dropdown.
   - Enter a password for the new user (e.g., `TestPassw0rd`).
   - Click *Save* to close the dialog.
4. Click *Save and exit*.

Creating a Listener

1. From the left menu, select **Management** > **Listeners** and click + **Add listener**.
2. Enter a unique name (e.g., `Oracle_Tunnel`).
3. Go to the **Settings** tab and in the **Protocol** field, press **SSH**.
4. In the **Connection mode** section, select **Tunnel**.
5. From the **Local address** list, choose an IP and enter the port that will be used for the SSH tunnel (e.g., `5522`).
6. Click **Save**.

> **Note**
>
> The **Keys** field shows generated SSH, TLS, and Standard RDP Security keys and the TLS certificate required for correct operation of a "Tunnel"-type listener.

TCP Server Configuration

1. From the left menu, select **Management** > **Servers** and click + **Add server**.
2. Enter a name (e.g., `Oracle_Tunnel_Server`).
3. In the **Settings** section, select **TCP** as the protocol.
4. In the **Destination** section: - Select **Host, IPv4** or **IPv6**. - Enter the **Address, Mask**, and **Port** (e.g., `192.168.0.100`, mask: `32`, port: `1521`).
5. Click **Save and exit**.

Account Configuration

Note

To configure the connection, an **anonymous** account type and **raw** session recording type are required.

Warning

If an *anonymous* account is used in a session established through an *SSH tunnel*, the name of the user who created the tunnel is displayed in the Sessions list.

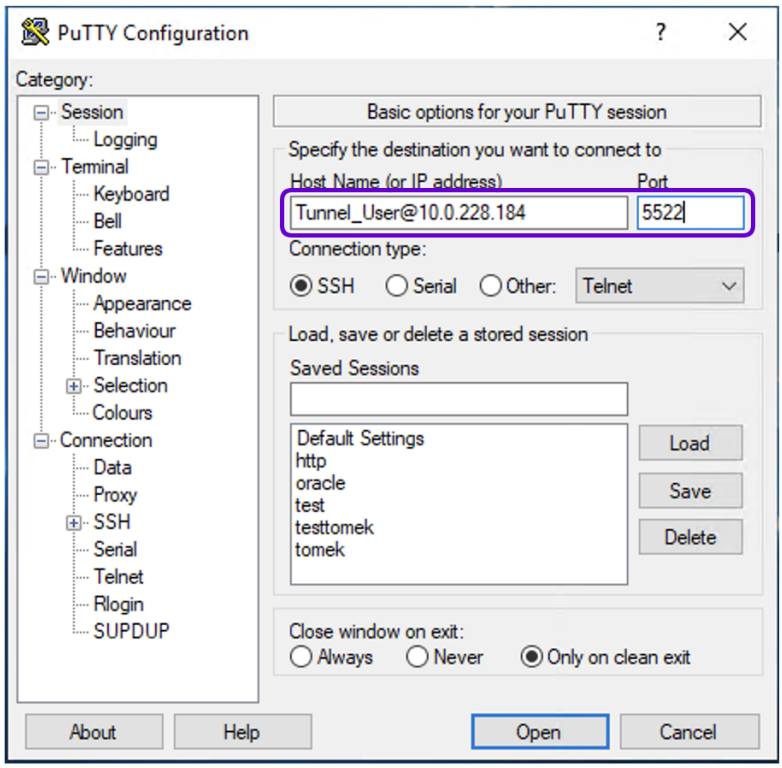
1. Select **Management** > **Accounts**, click + **Add account**.
2. Enter a name (e.g., `Oracle_Tunnel_Account`).
3. Set the **Session recording** option to **raw**.
4. In the **Settings** tab, under **Type**, select **ANONYMOUS**.
5. In the **Target** section, select the `Oracle_Tunnel_Server`.
6. Click **Save and exit**.

Safe Configuration

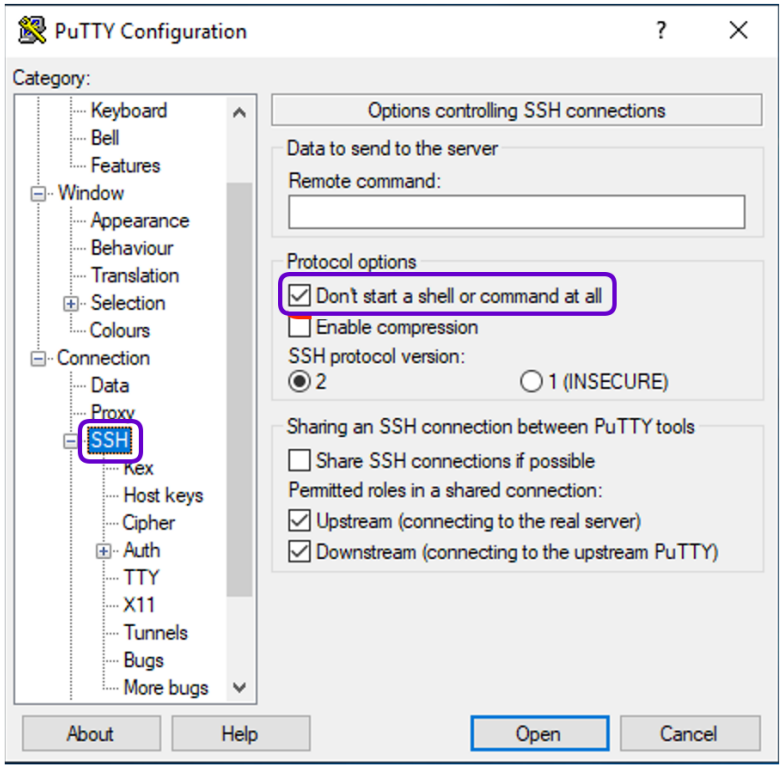
1. Select **Management** > **Safes** and click + **Add safe**.
2. Enter a name (e.g., `Tunnel_Safe`), click **Save**.
3. In the **Users** tab, click **Manage users** and select `Tunnel_User`.
4. Click **Save**.
5. In the **Accounts** tab, click **Manage accounts** and select `Oracle_Tunnel_Account`.
6. Click **Save**.
7. Select the `Oracle_Tunnel_Account`, click **Manage listeners**, and choose `Oracle_Tunnel`.
8. Click **Save**, then **Save and close**.

PuTTY Configuration

1. Launch **PuTTY**.
2. In the **Host Name** field, enter `<Fudo_user>@<Fudo_IP_address>`, e.g., `Tunnel_User@10.0.228.184`.
3. In the **Port** field, enter the port of the *Tunnel*-type listener created earlier (e.g., `5522`).

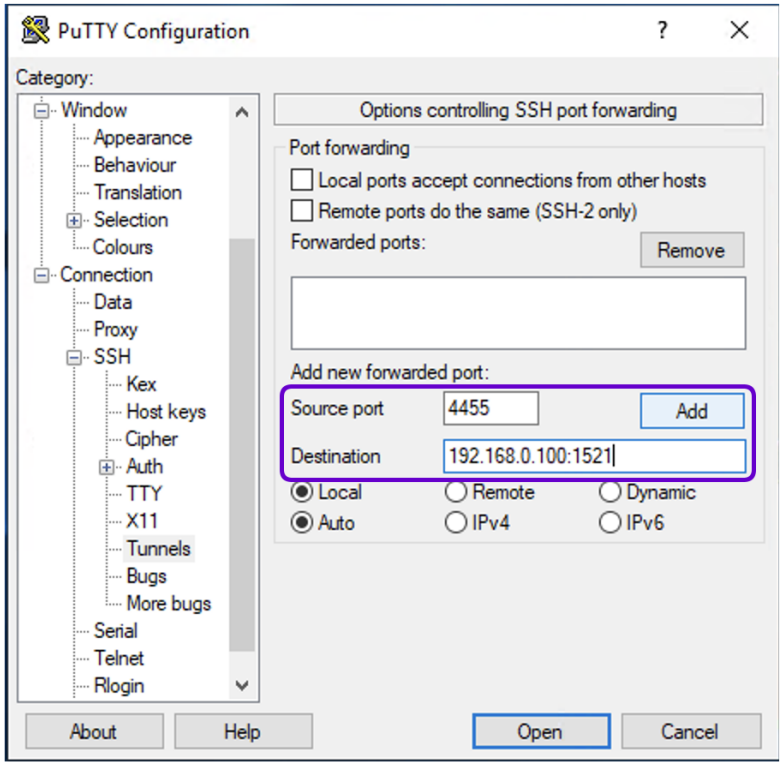


4. Go to the **SSH** tab and check **Don't start a shell or command at all**.

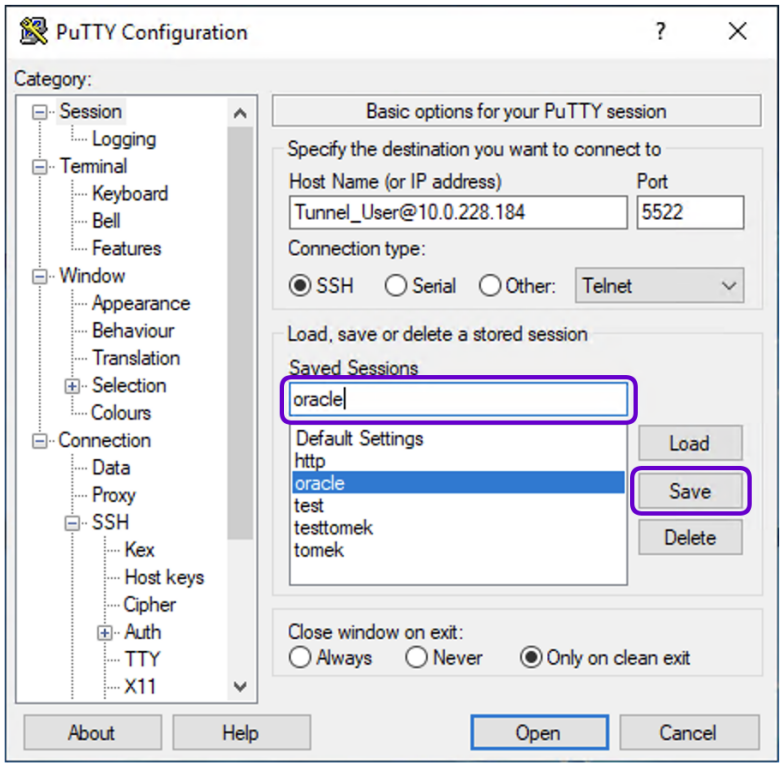


5. Go to the **Tunnels** tab and add a forwarded port:
   - **Source port**: the port you want to forward (e.g., `4455`).
   - **Destination**: target server address and port in the format `<destination_server_address>:<port>` (e.g., `192.168.0.100:1521`).

- Click **Add**.



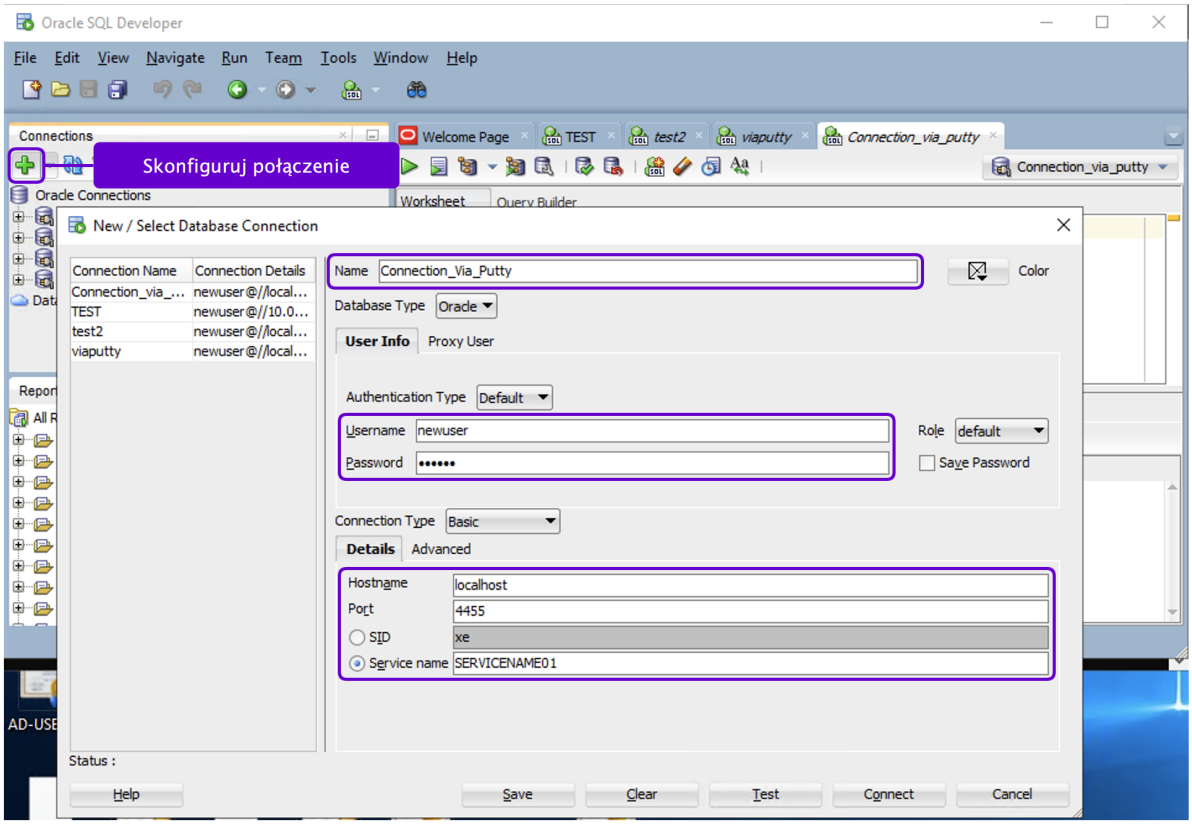
6. Return to the **Sessions** tab, save the configuration, and click **Open**.



7. Enter the password set for `Tunnel_User` (e.g., `TestPassw0rd`) and press **Enter**.
8. The tunnel is established.

Connecting via Oracle Client

1. Launch your Oracle client (e.g., **Oracle SQL Developer**).
2. Click **New Connection** to create a new configuration.
3. Fill in the fields:
   - **Name** – connection name,
   - **Username** and **Password** – database login credentials,
   - **Hostname** – `localhost`,
   - **Port** – `4455` (as set in PuTTY *Source port*),
   - **Service name** – the Oracle database service name (e.g., `orcl`).
4. Click **Connect** to establish the connection to the database.

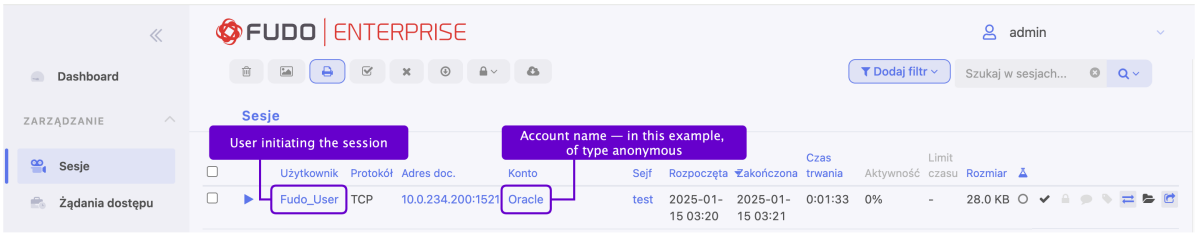


Session List View

Once the connection is established, an entry for the session established through the tunnel will appear under **Management** > **Sessions**. The following details will be visible:

- Fudo username (also if an anonymous account was used),
- Session protocol,
- Destination server address,
- Name of the account used for the connection,
- Safe name,

- Session start and end time,
- Session duration.



20.10.1.4 Connection to a Server with Reverse Tunnel via Tunnel-type Listener

This scenario describes the case when:

- The listener is configured in *Tunnel* mode.
- The target server uses an SSH reverse tunnel (the **Use SSH tunnel** option) through a **jump host** (an intermediary server) that has access to both Fudo Enterprise and the target server.

User Configuration

1. Go to *User Management* > *Users* and click *+ Add user*.
2. Enter a name (e.g., `Tunnel_User`) and click *Save*.
3. Select the user authentication method:
   - Choose e.g. *Static password* from the *Add authentication method* dropdown.
   - Enter the password for the created user (e.g., `TestPassw0rd`).
   - Click *Save* to close the dialog.
4. Click *Save and exit*.

Creating a Listener

1. From the left menu, select **Management** > **Listeners** and click **+ Add listener**.
2. Enter a unique name (e.g., `SSH_Tunnel`).
3. Go to the **Settings** tab and press the **SSH** button in the **Protocol** field.
4. In the **Connection mode** section, select **Tunnel**.
5. From the **Local address** list, select an IP address and port for the listener (np: `10.31.135.179` i `3455`).
6. Click **Save**.

> **Note**
>
> The **Keys** field displays generated SSH, TLS, and Standard RDP Security keys as well as a TLS certificate required for proper operation of a "Tunnel"-type listener.

RDP Server Configuration with Reverse Tunnel

1. From the left menu, select **Management** > **Servers** and click + **Add server**.
2. Enter a name (e.g., `RDP_Reverse_Server`).
3. In the **Settings** section, choose **RDP** as the protocol.
4. Select the *Use SSH tunnel* option, and paste the *jump host* public key into the *SSH tunnel key* field.
5. Click **Save**.
6. After saving the server, copy the command displayed in the *Command to establish SSH tunnel* field.

> **Note**
>
> Unlike in a standard server configuration, the IP address and port are not defined in the **Destination** section, because the server is accessed through an SSH reverse tunnel.

Account Configuration

1. Select **Management** > **Accounts**, click + **Add account**.
2. Enter a name (e.g., `Reverse_Tunnel_Account`).
3. In the **Settings** tab, under **Type**, select **REGULAR**.
4. In the **Target** section, select the `RDP_Reverse_Server`.
5. In the **Credentials** section:
   - Enter the login used on the target server (e.g., `admin`).
   - Click the button in the **Replace secret** section, choose e.g. **Password**, and enter the password used to authenticate on the target server.
6. Click **Save**, then **Save and exit**.

Safe Configuration

1. Select **Management** > **Safes** and click + **Add safe**.
2. Enter a name (e.g., `Reverse_Tunnel_Safe`), click **Save**.
3. In the **Users** tab, click **Manage users** and select the `Tunnel_User`.
4. Click **Save**.
5. In the **Accounts** tab, click **Manage accounts** and select `Reverse_Tunnel_Account`.
6. Click **Save**.
7. Select `Reverse_Tunnel_Account`, click **Manage listeners**, select `SSH_Tunnel`.
8. Click **Save**, then **Save and close**.

Establishing Tunnels and Initiating the Connection

1. On the **jump host** server, run the command generated when creating the server in Fudo Enterprise to establish the tunnel. The command contains the identifier of the created server (`8754997675608244234`), which is used when establishing the tunnel and initiating the connection.

   Example:

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

   where you should replace:

   - `<target>` - with the IP address of the target server
   - `<port>` - with the port of the target server

2. On the user's machine, from which the connection to the target server will be initiated, establish a tunnel to the listener.

   ```
   ssh -N -l <fudo_username> <fudo_listener_ip> -p <listener_port_tunnel>
   ↪ -L <listener_port_tunnel>:/tunnel/<server_id_on_fudo>
   ```

   Example:

   ```
   ssh -N -l 'tunnel_user' 10.31.135.179 -p 3455 -L 3455:tunnel/
   ↪8754997675608244234
   ```

   where:

   - `'tunnel_user'` - the username in Fudo Enterprise.
   - `10.31.135.179` - the listener address.
   - `3455` - the port of the Tunnel-type listener.
   - `8754997675608244234` - the ID number of the server created in Fudo Enterprise.

3. Initiate the connection through the tunnel using the server name configured in Fudo Enterprise.

   ```
   ssh -l '<fudo_username>#<server_username>#<name_of_server_on_fudo>'␣
   ↪localhost -p <listener_port_tunnel>
   ```

   Example:

   ```
   ssh -l 'tunnel_user#admin#RDP_Reverse_Server' localhost -p 3455
   ```

4. Depending on the protocol of the target server (in this case, RDP), launch the appropriate native client and connect to `localhost:3455`.

Related topics:

- *Establishing an SSH Connection*

- *Creating an SSH Server*
- *Setting up the SSH Listener*

20.11 Master Key Protection with a Thales Luna HSM

This guide describes the integration of Fudo Enterprise with Thales Luna HSMs, both Luna Cloud HSM and Luna Network HSM.

Fudo Enterprise can use a Hardware Security Module (HSM) to provide hardware-backed protection for its master key. When HSM integration is enabled, Fudo Enterprise communicates with the HSM through the PKCS#11 interface and uses a *Key Encryption Key* (KEK) protected by the HSM to secure the Fudo Enterprise master key.

HSM integration is optional. By default, Fudo Enterprise uses its standard software-based key protection mechanism.

Note

Fudo Enterprise supports network-accessible HSM providers that provide a Linux x86-64 PKCS#11 client.

20.11.1 How Fudo Enterprise Protects the Master Key

Enabling HSM integration does not replace the Fudo Enterprise master key with an HSM-generated key. Fudo Enterprise continues to use its own master key, which is protected using key wrapping.

A *Key Encryption Key* (KEK) is protected by the HSM and is non-exportable. The Fudo Enterprise master key is stored in a wrapped form, encrypted using the HSM-protected KEK.

When Fudo Enterprise starts, it contacts the HSM to unwrap the master key. The KEK remains protected within the HSM throughout this operation.

20.11.2 Before You Begin

Before configuring Fudo Enterprise, prepare the HSM environment using the standard Thales administration tools.

You will need:

- an HSM service or application partition prepared for Fudo Enterprise;
- the token/partition label;
- the corresponding Crypto Officer (CO) PIN;
- a Luna HSM Client package and credentials/certificates allowing the client to access the HSM;
- network connectivity between Fudo Enterprise and the HSM service.

The HSM, its application partition, authentication policy and client credentials should be configured by the administrator responsible for the Thales environment before starting the Fudo Enterprise configuration.

20.11.3 Option 1: Thales Luna Cloud HSM

Create or prepare the Luna Cloud HSM service

1. Sign in to the Thales Data Protection on Demand portal and create a Luna Cloud HSM service, or use an existing service intended for Fudo Enterprise.

> **Note**
>
> When creating the service, keep FIPS restrictions enabled unless your security policy explicitly requires otherwise.

2. Prepare the partition that Fudo Enterprise will use and note:
   - the token label;
   - the required PIN.

Create and download a service client

1. Go to *Services* > *My Services* and open your service.
2. Click *Create Service Client*.
3. Download the resulting client package.

> **Note**
>
> - Use the Linux x86-64 client.
> - The downloaded package contains considerably more functionality than Fudo Enterprise requires. It must therefore be prepared before it is uploaded to Fudo Enterprise.

Prepare the package for Fudo Enterprise

1. Extract the Luna client package.
2. Find and extract the Linux client components packaged as a `.tar` archive, for example `cvclient-min.tar`.

> **Note**
>
> Do not upload the original complete client archive directly to Fudo Enterprise. Fudo Enterprise requires the selected Linux client components packaged as a `.tar` archive.

3. Create a new `.tar` archive containing the files required by Fudo Enterprise, including:

```
libs/
plugins/
Chrystoki.conf
*.pem
```

> **Note**
>
> The PKCS#11 module required by Fudo Enterprise is normally `libs/64/libCryptoki2.so`.

20.11.4 Option 2: Thales Luna Network HSM

The Fudo Enterprise-side configuration is the same as for Luna Cloud HSM, but the preparation of the Luna client package usually requires additional attention.

Prepare the HSM

Before configuring Fudo Enterprise, the Luna administrator should prepare the HSM using the standard Thales administration workflow. This includes, as appropriate:

- configuring the Luna Network HSM;
- configuring network connectivity;
- creating or selecting an application partition;
- assigning client access to the partition;
- configuring authentication;
- generating or installing the required client credentials and certificates;
- configuring the Luna HSM Client.

The Luna administrator should then provide:

- the Linux x64 Luna HSM Client files;
- the associated credentials/certificates;
- the token label;
- the PIN required by Fudo Enterprise.

Obtain the Luna HSM Client files

1. Obtain the Linux version of the Luna HSM Client configured for the partition that Fudo Enterprise will use.

> **Note**
>
> Depending on how the Luna environment was prepared, administrators may provide the client software and the connection credentials/certificates as separate archives.

2. Combine all the connection credentials/certificates and the selected components from the client software archive in one directory. For example:

```
fudo-luna-client/
├── libs/
│   └── 64/
│       └── libCryptoki2.so
├── lock/
```

(continues on next page)

(continued from previous page)

```
├── plugins/
├── Chrystoki.conf
├── Openssl.cnf
└── *.pem
```

Note

- The number and purpose of the certificates in the archive depends on the client's trust configuration and the HSM topology. The exact set of files depends on the Luna deployment.
- Additional configuration files referenced by `Chrystoki.conf`, such as `openssl.cnf`, must also be included when they are required by the supplied Luna configuration.

Adjust Chrystoki.conf

Note

When the Luna Client files are moved to a different runtime environment, library, certificate and configuration paths in `Chrystoki.conf` must be adjusted to the paths visible to that environment.

Review `Chrystoki.conf` and adjust the following elements:

1. Change file paths.

   Update any absolute paths so that they match the layout of the files inside the archive uploaded to Fudo Enterprise. For example:

   ```
   /usr/safenet/lunaclient/openssl.cnf
   ```

   may need to become:

   ```
   Openssl.cnf
   ```

   Similarly, library paths should point to the location used inside the Fudo Enterprise package, for example:

   ```
   libs/64/libCryptoki2.so
   ```

2. Disable HA logging.

   In the `HAConfiguration` section, set `haLogStatus = disabled;`. For example:

   ```
   HAConfiguration = {
           haLogStatus = disabled;
           reconnAtt = -1;
           AutoReconnectInterval = 60;
   }
   ```

This disables local Luna Client HA logging while leaving the reconnect settings unchanged.

3. Review the Secure Trusted Channel configuration.

   If the configured HSM connection does not use Secure Trusted Channel (STC), remove the Secure Trusted Channel section. This section references additional Luna Client components and identity directories that are not included in the standard Fudo Enterprise client package.

Create the Fudo Enterprise package

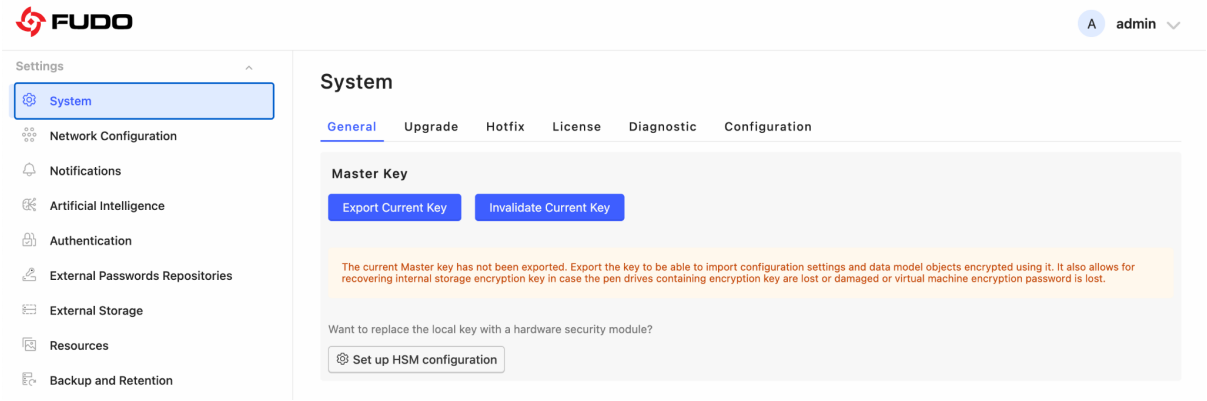
1. After adjusting `Chrystoki.conf`, verify that all file paths referenced in the configuration match the actual locations of the files in the prepared directory.
2. Package the entire prepared directory as a `.tar` archive.

20.11.5 Configuring Fudo Enterprise

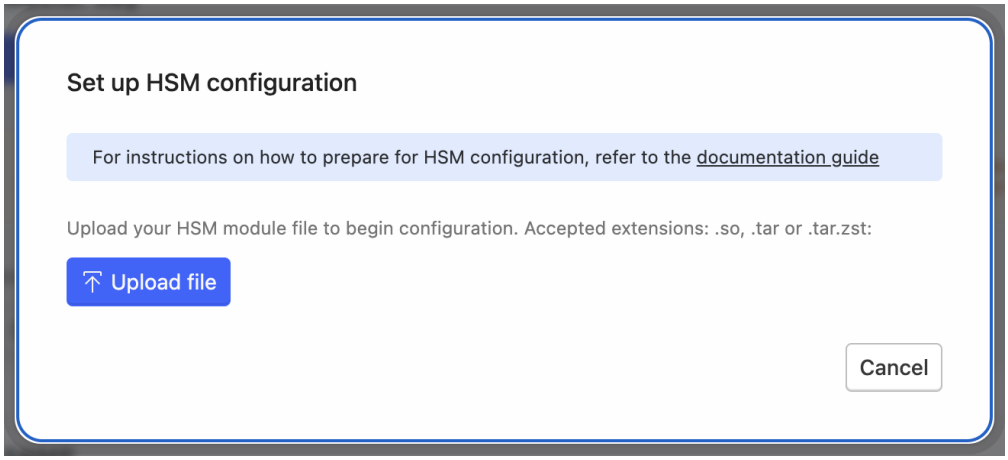
Enabling HSM protection

> **Note**
>
> Fudo Enterprise requires a CPU supporting the **x86-64-v2** microarchitecture level (SSE4.2, SSSE3, POPCNT, CMPXCHG16B). Every physical x86 CPU since ~2009 (Intel Nehalem, AMD Bulldozer) supports x86-64-v2. If you are unable to see the *Set up HSM configuration* button in *System* > *Settings*, the hypervisor is presenting a generic vCPU model that masks these instructions.

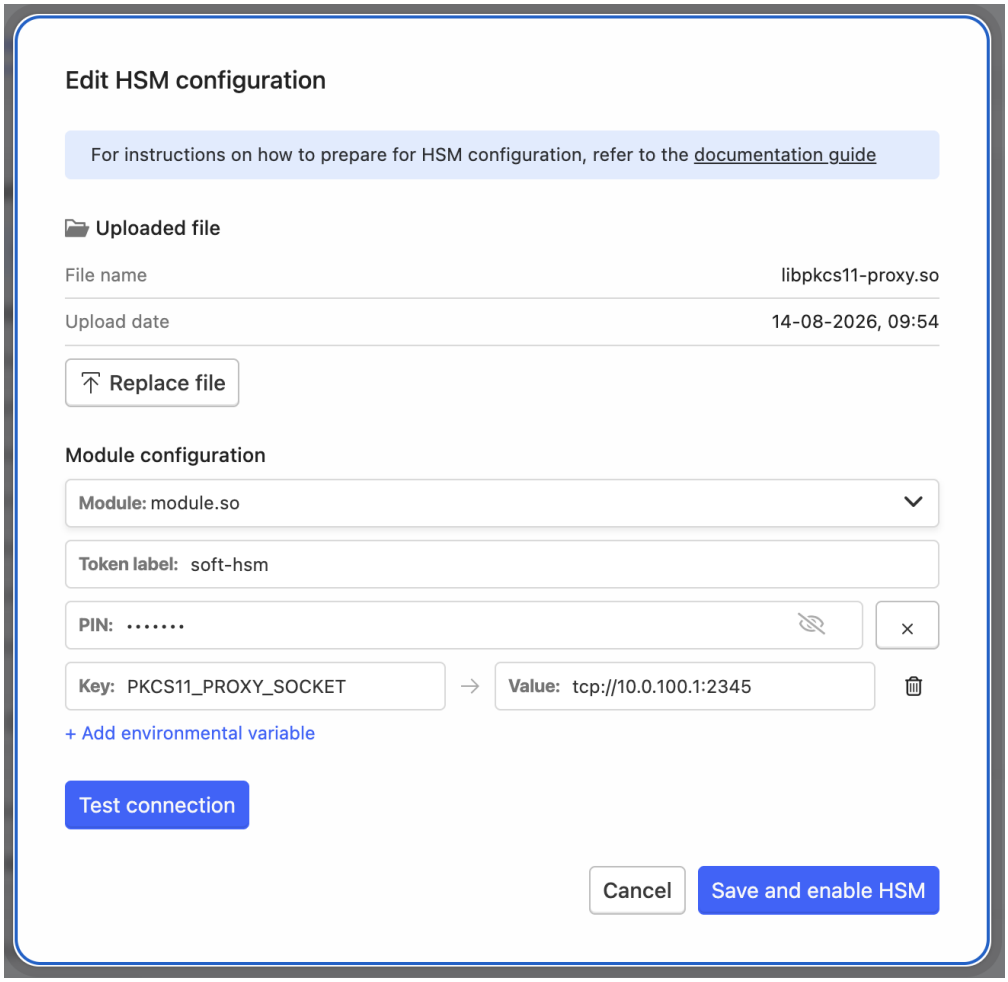
1. Select *Settings* > *System*.
2. Select the *General* tab.
3. In the *Master Key* section click *Set up HSM configuration*.



4. Click *Upload file* and select the archive prepared for your HSM client. Accepted file extensions are `.so`, `.tar` and `.tar.zst`.



5. Configure the following fields:
   - *Module* - select the PKCS#11 library included in the uploaded package. For a standard Luna HSM client this is `libs/64/libCryptoki2.so`.
   - *Token label* - enter the label of the HSM partition prepared for Fudo Enterprise.
   - *PIN* - enter the Crypto Officer (CO) PIN associated with the partition.

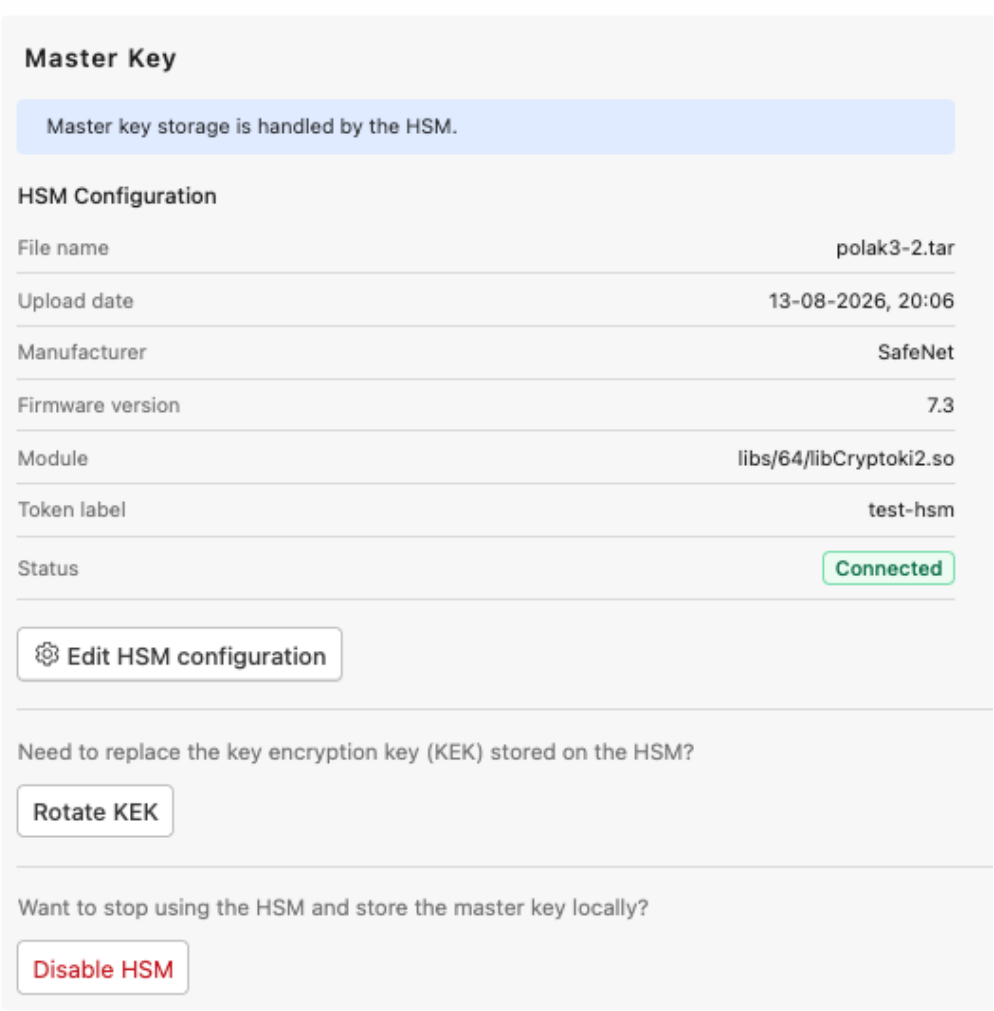


6. If the PKCS#11 module requires environment variables, click *+ Add environmental variable* and provide them as *Key* and *Value* pairs.

> **Note**
>
> The names and values of the environment variables are defined by the documentation of the PKCS#11 module vendor.

7. Click *Test connection* to verify that Fudo Enterprise can reach the HSM with the provided credentials.
8. Once the test succeeds, click *Save and enable HSM*.

The *Master Key* section now displays the details of the uploaded package, the module and token label in use, and the connection status.



Rotating the key encryption key

The *KEK* (Key Encryption Key) is the HSM-protected key used to wrap the *Master key*. Rotating the *KEK* generates a new key encryption key on the HSM and re-wraps the *Master key* with it.

> **Note**
>
> Rotating the *KEK* does not change the *Master key* itself, so the data encrypted with the

Master key is not re-encrypted.

1. Select *Settings* > *System*.
2. Select the *General* tab.
3. In the *Master Key* section click *Rotate KEK*.

Disabling HSM protection

Disabling HSM protection unwraps the *Master key* and stores it locally again.

Warning

Disabling HSM protection requires access to the currently configured HSM. Do not decommission or disconnect the HSM before HSM protection has been disabled in Fudo Enterprise.

1. Select *Settings* > *System*.
2. Select the *General* tab.
3. In the *Master Key* section click *Disable HSM*.

Related topics:

- *Configuration Encryption*
- *Security Measures*

CHAPTER 21

Frequently Asked Questions

1. How many user sessions can be stored on at once?

2. How Fudo Enterprise supports sessions archiving?

3. How to calculate storage space required for archiving sessions?

4. How users can hide their activities on servers which they access through Fudo Enterprise?

5. How to determine unauthorized access attempts to supervised servers?

6. Is it possible to hide the login screen when connecting over the RDP protocol?

7. Why the users list in the connection's properties is incomplete?

8. Why is a user removed from the LDAP/AD server still present on the users list?

9. How frequently are users' definitions synchronized with an LDAP/AD server?

*10. I see * instead of the keystrokes in the session player. Is it possible to see the actual keyboard input?*

11. Can I deactivate a session URL?

12. What should I do before returning a demonstration unit after testing?

AI session processing

13. How long does it take for the model to learn? How many sessions do I have to record to see results?

14. We have 20 accounts and 20 users in our company - how long will it take to see differences?

15. If I connect to different servers, does Fudo create a separate model for each of them?

16. If I give my login credentials to another person, will the AI detect that someone else has logged in and terminate the session?

17. Session status icon is yellow all the time - what does it mean?

18. Five users use the same account to establish connections - will the system be able to determine who and when has logged in onto the server?

19. How will the system determine that it wasn't me if we all use the same commands?

20. Sessions are not analyzed, why is that?

Administration and API

21. An operation failed with the "CPU time exceeded." error. What does it mean and what should I do?

1. How many user sessions can be stored at once?

Fudo Enterprise F1000 series is delivered with 24 TB of RAW hard drive space (15.9 TB usable) while the F3000 series appliances come with 96 TB of RAW storage space (59.9 TB usable) dedicated for storing users sessions.

Size of the stored session is determined by user's activity. An hour of recorded connection takes on average:

RDP	218 MB active user session (no activity generates almost no data). Definite session size depends on the screen resolution, color depth and actual user activity.
SSH	41.5 MB active session.

Given that assumptions, internal storage space enables recording of:

	RDP	SSH
F1000	28.6 years	150.2 years
F3000	112.8 years	592.5 years

Note

- Disk usage figures include space taken up by the filesystem's redundancy mechanism. The filesystem reserves a portion of available storage, which results in some of the storage space being reported as used on a newly initiated system.
- Fudo Enterprise allows specifying how long sessions data should be stored, and will automatically delete session data after a certain time, determined by *retention parameter*, elapses.

2. How Fudo Enterprise supports sessions archiving?

All sessions are stored on Fudo Enterprise internal storage space. In addition to that, Fudo Enterprise allows exporting sessions in native format or a video record.

3. How to calculate storage space required for archiving sessions?

File size of sessions in native format are the same as in question 1. In case of video record, file size depends on the codec and resolution settings.

4. How users can hide their activities on servers which they access through the Fudo Enterprise?

In case of the SSH protocol, Fudo Enterprise supports SCP channel and monitors all transferred files, including scripts. This allows auditing given session searching for malicious code embedded in software sent to the server.

Protection of other communication channels (e.g. web browser or other applications) are task for different kind of solutions. There is no solution similar to Fudo Enterprise which are able to monitor such channels, thus it is important to create proper server configuration by the system administrator.

5. How to determine unauthorized access attempts to supervised servers?

Unauthorized access and DoS attacks attempts, can be determined by analyzing event log entries. Each ERROR or WARNING severity entries should be closely examined. Cases of login timeout errors can be potential DoS attack attempts.

6. Is it possible to hide the login screen when connecting over the RDP protocol?

Hiding the Fudo Enterprise login screen requires using the `Enhanced RDP Security (TLS) + NLA` security mode.

7. Why the users list in the connection's properties is incomplete?

The users list in the connection's properties does not contain users synchronized with the LDAP service. To assign a connection to an LDAP synchronized user, define a group mapping in the *LDAP synchronization properties* or disable the synchronization option for the given user.

8. Why is a user removed from the LDAP/AD server still present on users list?

Deleting a user object from an AD or an LDAP server requires performing the full synchronization to reflect those changes on Fudo Enterprise. The full synchronization process is triggered automatically once a day at 00:00, or can be triggered manually in the *LDAP synchronization* settings view.

9. How frequently are users' definitions synchronized with an LDAP/AD server?

New users definitions and changes in existing objects are imported from the directory service periodically every 5 minutes. The full synchronization process is triggered automatically once a day at 00:00.

10. I see * instead of the keystrokes in the session player. Is it possible to see the actual keyboard input?

Presenting keyboard input qualifies as a sensitive feature and it is disabled by default. Enabling displaying keystrokes in the session player requires a consent from two `superadmin` users. Refer to the *Sensitive Features* topic for the details on enabling this functionality.

11. Can I deactivate a session URL?

Active session URL can be deactivated anytime. URL revoking procedure is described in the *Sessions sharing* topic.

12. What should I do before returning a demonstration unit after testing?

After testing Fudo, you should delete all session and configuration data by *resetting configuration to default settings* and erase the flash drive with the encryption key.

13. How long does it take for the model to learn? How many sessions do I have to record to see results?

Models are trained as scheduled in the *AI system settings*.

- For the SSH model the minimum are 65 sessions (with at least 25 different commands) and 5 unique predictors (e.g. users). Optimal results require 300 sessions per predictor (e.g. user) and 10 unique predictors (e.g. users).

- For the RDP model, the minimum are 5 hours of session recordings per predictor (e.g. user). Optimal results require 30 hors of session recordings and 10 unique predictors (e.g. users).

14. We have 20 accounts and 20 users in our company - how long will it take to see differences?

This solely depends on the availability of session data. If there is enough session information available to build models, you can expect model to be trained the next day after first predictor session is recorded.

- For SSH model the minimum are 65 sessions (with at least 25 different commands) and 5 unique predictors (e.g. users). Optimal results require 300 sessions per predictor (e.g. user) and 10 unique predictors (e.g. users).
- For RDP model, the minimum are 5 hours of session recordings per predictor (e.g. user). Optimal results require 30 hours of session recordings and 10 unique predictors (e.g. users).

15. If I connect to different servers, does Fudo create a separate model for each of them?

Fudo creates and maintains one RDP and one SSH model for a single user.

16. If I give my login credentials to another person, will the AI detect that someone else has logged in and terminate the session?

Fudo Enterprise will detect that someone else has logged in and will set the session risk status to high. The session will be terminated if the appropriate AI policy is set.

17. Session status icon is yellow all the time - what does it mean?

Yellow color indicates that the model could not determine whether the session poses a threat or not. Under normal circumstances, these sessions should be considered as non-threatening. But if you suspect there has been a security incident, these sessions should be reviewed.

18. Five users use the same account to establish connections - will the system be able to determine who and when has logged in onto the server?

Users must have individual accounts created on Fudo Enterprise so it can correctly determine if an account security has been breached.

19. How will the system determine that it wasn't me if we all use the same commands?

Every user runs the same commands differently. E.g. one user will execute `ls -la` and another will run `ls -al`. Combination of such subtle differences allows for determining a if the currently logged in user matches the profile.

20. Sessions are not analyzed, why is that?

In order for a session to be analyzed, there must be a matching model available. Also, session has to meet volumetric requirements - it must be long enough and carry enough information. Refer to *AI Behavioral Analysis in Sessions* for more information.

21. An operation failed with the "CPU time exceeded." error. What does it mean and what should I do?

The error means a safety limit stopped your request. It is not a bug or a crash, and no data is lost. Fudo Enterprise limits how much processor time a single request to the Admin Panel, the User Access Gateway or the API may use. That way one heavy or malicious request cannot slow

down the system for everyone else. A request that goes over its limit is stopped and returns the `CPU time exceeded.` message.

When it shows up

The error typically appears during bulk operations that process many items in a single save or request, for example adding many IP addresses to a network interface at once, or creating many users through the API.

What happened to my change

The request was stopped before it was saved, so none of the changes it carried were applied and nothing was corrupted. It is safe to repeat the operation.

If a task needs several requests, such as creating a user and then setting the user's password through the API, only the failed request is left out. Check the object and repeat the failed step.

What to do

1. Try the operation again.
2. If it fails again, split it into smaller batches, for example save fewer IP addresses or create fewer users per request.
3. If the error keeps appearing for the same operation even with small batches, contact technical support. Say which operation fails, how many items it contains and when the error occurred. The limit can be raised for specific operations that legitimately need more processing time.

How to recognize it

- The Admin Panel or the User Access Gateway shows the `CPU time exceeded.` error message.
- The API returns the `400` HTTP status code with the `CPU time exceeded.` message.
- The logs contain an entry with the `CPU time exceeded.` message, reported by the `apid` service.

CHAPTER 22

Glossary

account
accounts
: Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); secret changing policy as well as the secret changer itself.

Active Directory
: Users authorization and authentication in Windows domain.

AD
: Active Directory - users authorization and authentication in Windows domain.

Azure
: Microsoft Azure is a cloud computing service operated by Microsoft for application management via Microsoft-managed data centers.

anonymous safe
: An anonymous safe has at least one anonymous account assigned to it and it can only have that type of accounts assigned. You cannot assign users to anonymous safes.

AUROC
: Area Under ROC curve (AUROC) is a single metric representing model quality (the higher the better).

ARP
: Address Resolution Protocol - protocol used for mapping Internet layer addresses (IP addresses) to the physical - link layer addresses (MAC addresses).

CERB
: Complete user authentication and authorization solution, supporting different authentication methods i.e., mobile token (mobile phone application), static password, SMS one-time passwords, etc.

CIDR
: Short notation of network addressing, in which the IP address is written according to the

IPv4 standard, and the subnet mask is provided as a number of *1* in the subnet mask in binary system (192.168.1.1 - 255.255.255.0; 192.168.1.1/24).

data retention
Data retention mechanism automatically deletes session data after define time period transpires.

DHCP
Mechanism for dynamic IP addressing management i LAN networks.

DNS
Domain Name Server - name server service which maps IP addresses to hosts names which are easier to remember.

DUO
is a mobile application that works with Duo Security's two-factor authentication service. The application generates passcodes for login and can receive push notifications for authentication.

Efficiency Analyzer/Productivity Analyzer
Efficiency Analyzer/Productivity Analyzer module delivers statistical information on users' activity.

external authentication server
Server storing user data used for verification of user login credentials when connecting to Fudo Enterprise or the monitored server.

False Positive Rate
False Positive Rate (FPR) is the percentage of legitimate sessions inappropriately identified as malicious (the lower the better).

Fingerprint
Characters string being a result of a hash function on input data, allowing to determine if the input data has been altered.

heartbeat
Network packet used for informing other cluster nodes about machine's current state. If a cluster node does not receive a heartbeat packet in a given timeframe, it will take over the master node role and will start processing users' requests.

hot-swap
Hot-swap mechanism enables replacing hardware components without the necessity to turn the system off.

JWKS
JSON Web Key Set - a document published by a token issuer over HTTPS, containing the public keys used to verify the signatures of the tokens it issues.

JWT
JSON Web Token - a signed token carrying claims about an authenticated user, presented in an HTTP header of a request.

Kerberos
A network authentication protocol that uses secret-key cryptography to provide strong authentication for client-server applications by enabling secure identity verification over non-secure network connections.

LDAP
Lightweight Directory Access Protocol - distributed catalog services management and access protocol in IP networks.

listener
Listener determines server connection mode (proxy, bastion) as well as its specifics.

OATH
Open Authentication - open standard enabling implementation of strong, two-factor user and devices authentication.

OCR
Optical Character Recognition - image processing for identifying and indexing text.

Okta
Okta provides cloud software to manage and secure user authentication into applications.

OpenID Connect
OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol.

secret changer
Tool which enables facilitating automated secret changing on a server.

passwords repository
Passwords repository manages password to privileged accounts on monitored hosts.

policy
Mechanism which enables defining patterns which in case of being detected will trigger defined actions.

PSM (Privileged Session Management)
PSM module is used for recording remote access sessions.

PSM
PSM (Privileged Session Monitoring) module enables monitoring and recording remote access sessions.

Public key
Authentication method which uses a pair of keys - private (held only by the user) and public (publicly available) to determine user's identity.

RADIUS
Remote Authentication Dial In User Service - networking protocol used to control access to different services within IT infrastructure.

RDP
Remote Desktop Protocol - remote access protocol to computer systems running Microsoft operating system.

RDP connections broker
Remote sessions management mechanism for server farms.

redundancy group
Defined group of IP addresses, which in case of a system failure, will be seamlessly carried over to another cluster node to maintain the availability of the services.

safe
Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

server
servers
: Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

shared session
: User session which was joined by another user.

SMS
: is a text messaging service component of most telephone, and mobile device systems.

SSO
: is a user authentication process that allows a user to access multiple applications with one set of login credentials, enhancing convenience and security by reducing the need for multiple passwords.

SSH
: Secure Shell - networking protocol for secure communication with remote systems.

SSH access
: Service access to Fudo Enterprise over SSH protocol.

Static password
: Basic user authorization method which uses login and password combination to determine users's identity.

Syslog
: Events logging standard in computer systems. Syslog server collects and stores log data from networked devices, which can be later used for analysis and reporting.

TACACS+
: Terminal Access Controller Access-Control System Plus - networking protocol used to authenticate users against a central server, defined in RFC 8907. It can be used over TLS (RFC 9887).

Threat Probability
: Threat probability is a percentage-wise value that reflects a threat level of the session.

time policy
: Time policy mechanism enables defining time periods during which users are allowed to connect to monitored hosts. On a safe using time-based Just-in-Time access, the time policy also decides when a connection requires an approved access request and when it does not.

timestamp
: Session data hash value, which enables verifying that the data has not been modified.

True Positive Rate
: True Positive Rate (TPR), sometimes called Recall - is a percentage of malicious sessions properly flagged by the model as suspicious (the higher the better).

user
: User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

VLAN
Virtual networks mechanism, enabling separation of broadcast domains.

VNC
Remote access protocol to graphical user interfaces.

WAF
Web Application Firewall - a device or service placed in front of a web application that inspects HTTP traffic and can authenticate users at the perimeter.

WWN
World Wide Name - unique object identifier in external storage solutions.

Index

A

account, **995**
accounts, **995**
Active Directory, **995**
AD, **995**
administration
    configuration export/import, 552
AI, 585, 586, 590, 592
    live session monitoring, 592
anonymous safe, **995**
API
    users, 204
ARP, **995**
AUROC, **995**
Azure, **995**

C

CERB, **995**
CIDR, **995**
configuration
    Network configuration, 565, 575
    notifications, 582
    SCIM provisioning, 693
    users synchronization, 686
connection mode
    bastion, 27
    proxy, 26
creating
    servers, 257

D

data retention, **996**
deleting
    servers, 309
deployment scenario
    forced routing, 25
DHCP, **996**
DNS, **996**
DUO, **996**

E

editing
    servers, 305
Efficiency Analyzer/Productivity Analyzer, **996**
external authentication server, **996**

F

False Positive Rate, **996**
Fingerprint, **996**

H

heartbeat, **996**
hot-swap, **996**
HTTP
    protocol, 12
    protocols, 12
    servers, 257

I

import
    servers, 304

J

JWKS, **996**
JWT, **996**

K

Kerberos, **996**
    Protected Users, 634

L

LDAP, **997**
listener, **997**
listeners
    Oracle, 361
live session monitoring
    AI, 592

M

Modbus
    protocol, 13
    protocols, 13
    servers, 261
MS SQL
    servers, 264
MS SQL (*TDS*)
    protocol, 13
    protocols, 13
MySQL
    protocol, 14
    protocols, 14
    servers, 267

N

Network configuration
    IP labels, 575
    network interface configuration, 565
network configuration
    automatic interface routes, 577
    routing, 576
network settings
    reverse proxy, 554

O

OATH, **997**
OCR, **997**
Okta, **997**
OpenID Connect, **997**
Oracle
    listeners, 361
    protocol, 14
    protocols, 14
    servers, 271

P

passwords repository, **997**
policy, **997**
pools
    servers, 310
PostgreSQL
    protocols, 15
    servers, 274
Protected Users, 634
    Kerberos, 634
protocol
    HTTP, 12
    Modbus, 13
    MS SQL (*TDS*), 13
    MySQL, 14
    Oracle, 14
    RDP, 15
    secret, 24
    SSH, 18
    TCP, 24
    Telnet, 22
    Telnet 3270, 21
    Telnet 5250, 22
    VNC, 23
    X11, 24
protocols
    HTTP, 12
    Modbus, 13
    MS SQL (*TDS*), 13
    MySQL, 14
    Oracle, 14
    PostgreSQL, 15
    RDP, 15
    secret, 24
    SSH, 18
    TCP, 24
    Telnet, 22
    Telnet 3270, 21
    Telnet 5250, 22
    VNC, 23
    X11, 24
PSM, **997**
PSM (*Privileged Session Management*), **997**
Public key, **997**

R

RADIUS, **997**
RDP, **997**
    protocol, 15
    protocols, 15
    servers, 277
RDP Connections Broker, 737
RDP connections broker, **997**
redundancy group, **997**
reverse proxy
    configuration, 554

S

safe, **997**
SCIM provisioning, 693
    configuration, 693
secret
    protocol, 24
    protocols, 24
secret changer, **997**
server, **998**
servers, **998**

creating, 257
deleting, 309
editing, 305
HTTP, 257
import, 304
Modbus, 261
MS SQL, 264
MySQL, 267
Oracle, 271
pools, 310
PostgreSQL, 274
RDP, 277
ssh, 281
TCP, 298
Telnet, 284
Telnet 3270, 287
Telnet 5250, 291
VNC, 294
sessions
commenting, 168
filtering, 147
play and preview, 151
shared session, **998**
SMS, **998**
SSH, **998**
protocol, 18
protocols, 18
ssh
servers, 281
SSH access, **998**
SSH tunnel, 302
SSO, **998**
Static password, **998**
Syslog, **998**

T

TACACS+, **998**
TCP
protocol, 24
protocols, 24
servers, 298
Telnet
protocol, 22
protocols, 22
servers, 284
Telnet 3270
protocol, 21
protocols, 21
servers, 287
Telnet 5250
protocol, 22
protocols, 22
servers, 291
Threat Probability, **998**
time policy, **998**
timestamp, **998**
True Positive Rate, **998**
tunnel to tunneled server
use case, 979

U

use case
tunnel to tunneled server, 979
Use SSH tunnel, 302
user, **998**
users
access rights, 204
API, 204
roles, 204
users synchronization, 686
configuration, 686

V

VLAN, **999**
VNC, **999**
protocol, 23
protocols, 23
servers, 294

W

WAF, **999**
WWN, **999**

X

X11
protocol, 24
protocols, 24