

Fudo Enterprise 5.6 - System Documentation

Fudo Security

September 11, 2025

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) . . . 6
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 . . . 7
3.3 Licensing . . . 7
3.4 Supported protocols . . . 8
3.4.1 HTTP . . . 9
3.4.2 Modbus . . . 10
3.4.3 MS SQL (TDS) . . . 10
3.4.4 MySQL . . . 11
3.4.5 RDP . . . 11
3.4.6 SSH . . . 14
3.4.7 Telnet 3270 . . . 18
3.4.8 Telnet 5250 . . . 19
3.4.9 Telnet . . . 19
3.4.10 VNC . . . 20
3.4.11 X11 . . . 21
3.4.12 TCP . . . 21
3.4.13 Secret Checkout . . . 21
3.5 Deployment scenarios . . . 22
3.6 Connection modes . . . 24
3.7 User authentication methods and modes . . . 26
3.8 Security measures . . . 29
3.8.1 Data encryption . . . 29

3.8.2 Backups . . . 29
3.8.3 Permissions . . . 30
3.8.4 Sandboxing . . . 30
3.8.5 Reliability . . . 30
3.8.6 Cluster configuration . . . 30
3.9 Data model . . . 31
3.10 Dashboard . . . 32
3.10.1 Widgets . . . 33
3.10.2 Adding, customizing and removind dashlets . . . 34
3.10.3 Hard drives status information . . . 35
3.11 Third-Party Licenses . . . 35

4 System deployment **36**
4.1 Requirements . . . 36
4.2 Hardware overview . . . 38
4.3 System initiation . . . 43
4.3.1 Virtual machine . . . 47
4.4 Accessing Fudo Enterprise Portals . . . 52
4.4.1 Admin Panel . . . 53
4.4.2 User Access Gateway . . . 54
4.4.3 Supported Web Browsers . . . 55

5 Quick start **56**
5.1 SSH . . . 56
5.1.1 Prerequisites . . . 57
5.1.2 Configuration . . . 57
5.1.3 Establishing connection . . . 61
5.1.4 Viewing user session . . . 62
5.2 SSH in bastion mode . . . 63
5.2.1 Prerequisites . . . 63
5.2.2 Configuration . . . 63
5.2.3 Establishing connection . . . 68
5.2.4 Viewing user session . . . 70
5.3 SSH in Bastion Mode with Jump Host Option . . . 70
5.3.1 Prerequisites . . . 71
5.3.2 Configuration . . . 71
5.3.3 Establishing a Connection . . . 75
5.4 RDP . . . 76
5.4.1 Prerequisites . . . 76
5.4.2 Configuration . . . 76
5.4.3 Establishing an RDP connection with a remote host . . . 81
5.4.4 Viewing user session . . . 83
5.5 RDP in bastion mode . . . 84
5.5.1 Prerequisites . . . 84
5.5.2 Configuration . . . 84
5.5.3 Establishing an RDP connection with a remote host . . . 89
5.5.4 Viewing user session . . . 91
5.6 Telnet . . . 92
5.6.1 Prerequisites . . . 93
5.6.2 Configuration . . . 93
5.6.3 Establishing a telnet connection with the remote host . . . 98
5.6.4 Viewing user's session . . . 98

5.7 Telnet 5250 . . . 99
5.7.1 Prerequisites . . . 99
5.7.2 Configuration . . . 99
5.7.3 Establishing a telnet connection with the remote host . . . 105
5.7.4 Viewing user's session . . . 106
5.8 MySQL . . . 107
5.8.1 Prerequisites . . . 107
5.8.2 Configuration . . . 108
5.8.3 Establishing connection with a MySQL database . . . 112
5.8.4 Viewing user session . . . 113
5.9 MS SQL . . . 114
5.9.1 Prerequisites . . . 115
5.9.2 Configuration . . . 116
5.9.3 Establishing connection with a MS SQL database . . . 120
5.9.4 Viewing user session . . . 121
5.10 HTTP . . . 122
5.10.1 Prerequisites . . . 123
5.10.2 Configuration . . . 123
5.10.3 Connecting to remote resource . . . 128
5.10.4 Viewing user session . . . 129
5.11 VNC . . . 130
5.11.1 Prerequisites . . . 130
5.11.2 Configuration . . . 131
5.11.3 Establishing connection . . . 135
5.11.4 Viewing user session . . . 136
5.12 User authentication against external LDAP server . . . 136
5.12.1 Prerequisites . . . 137
5.12.2 Configuration . . . 137

6 Role-Based Access Control (RBAC) 139
6.1 Transition to RBAC After Upgrade . . . 140
6.1.1 Understanding Privileges and Capabilities . . . 140
6.1.2 Predefined Roles as a Starting Point . . . 141
6.2 Creating Role . . . 146
6.3 Assigning Roles to Users . . . 148
6.4 Modifying Roles . . . 150
6.5 Deleting Roles . . . 150
6.6 Typical Role Scenarios and Required Privileges . . . 151
6.6.1 Tab-Level Access Control Matrix . . . 151
6.6.2 Dashboard Widgets Visibility . . . 161
6.6.3 Sessions Tab Permissions . . . 161
6.6.3.1 Playback and Preview . . . 162
6.6.3.2 Session Backup . . . 162
6.6.3.3 Session Management . . . 162
6.6.4 Downloads Tab Permissions . . . 162
6.6.5 Safes Management . . . 163
6.6.6 Discovery Tab Permissions . . . 163
6.6.7 Access Request Permissions . . . 164
6.6.8 Fudo Officer . . . 164
6.6.9 Reports Tab Permissions . . . 165

7 Groups (RBAC) 166

7.1 Access Resolution and Prioritization . . . 166
7.2 Creating Group . . . 169
7.3 Modifying Groups . . . 172
7.4 Deleting Groups . . . 173

8 Users **174**
8.1 Creating a user . . . 175
8.2 Editing a user . . . 182
8.3 Blocking a user . . . 183
8.4 Unblocking a user . . . 185
8.5 Deleting a user . . . 186
8.6 Authentication failures counter . . . 187
8.7 Users Synchronization - User Directory . . . 188

9 Servers **194**
9.1 Creating a server . . . 194
9.1.1 Creating an HTTP server . . . 194
9.1.2 Creating a Modbus server . . . 197
9.1.3 Creating a MS SQL server . . . 198
9.1.4 Creating a MySQL server . . . 200
9.1.5 Creating an RDP server . . . 202
9.1.6 Creating an SSH server . . . 205
9.1.7 Creating a Telnet server . . . 207
9.1.8 Creating a Telnet 3270 server . . . 209
9.1.9 Creating a Telnet 5250 server . . . 211
9.1.10 Creating a VNC server . . . 213
9.1.11 Creating a TCP server . . . 215
9.2 Port Ranges in Server Configuration . . . 216
9.2.1 Configuring a Port Range . . . 216
9.2.2 Server Configuration Prioritization in Case of Conflict . . . 217
9.3 Importing a server list from CSV file . . . 218
9.4 Editing a server . . . 219
9.5 Blocking a server . . . 220
9.6 Unblocking a server . . . 221
9.7 Deleting a server . . . 222

10 Pools **224**
10.1 Creating a pool . . . 224
10.2 Deleting a pool . . . 225

11 Remote Applications **227**
11.1 Adding Remote Application . . . 227
11.2 Adding Arguments . . . 228
11.3 Connecting to Remote Application via Access Gateway . . . 231
11.4 Granular Access to Remote Applications . . . 231
11.5 Deleting Remote Application . . . 233

12 Accounts **234**
12.1 Creating an account . . . 235
12.1.1 Creating an *anonymous* account . . . 235
12.1.2 Creating a *forward* account . . . 238
12.1.3 Creating a *regular* account . . . 243

12.2 Editing an account . . . 252
12.3 Blocking an account . . . 252
12.4 Unblocking an account . . . 254
12.5 Deleting an account . . . 255
12.6 Managing security alerts . . . 256
12.6.1 Triggering password change . . . 256
12.6.2 Ignoring security alert . . . 257

13 Listeners **260**
13.1 Creating a listener . . . 260
13.1.1 Setting up the SSH listener . . . 262
13.1.2 Setting up the RDP listener . . . 266
13.1.3 Setting up the VNC listener . . . 270
13.1.4 Setting up the HTTP listener . . . 273
13.1.5 Setting up the Modbus listener . . . 276
13.1.6 Setting up the MySQL listener . . . 279
13.1.7 Setting up the TCP listener . . . 281
13.1.8 Setting up the MS SQL listener . . . 283
13.1.9 Setting up the Telnet listener . . . 286
13.1.10 Setting up the Telnet 3270 listener . . . 288
13.1.11 Setting up the Telnet 5250 listener . . . 291
13.2 Editing a listener . . . 294
13.3 Blocking a listener . . . 294
13.4 Unblocking a listener . . . 295
13.5 Deleting a listener . . . 296

14 Safes **297**
14.1 Creating a Safe . . . 297
14.2 Editing a safe . . . 307
14.3 Blocking a safe . . . 307
14.4 Unblocking a safe . . . 309
14.5 Deleting a safe . . . 310

15 Discovery **311**
15.1 Creating a rule . . . 312
15.1.1 Creating a rule for accounts . . . 312
15.1.2 Creating a rule for servers . . . 314
15.2 Managing rules . . . 315
15.3 Creating a scanner . . . 315
15.3.1 Creating a scanner for Domain Controller Accounts . . . 315
15.3.2 Creating a scanner for Domain Controller Servers . . . 318
15.3.3 Creating a scanner for local accounts . . . 319
15.4 Managing scanners . . . 321
15.5 Managing discovered accounts . . . 321
15.6 Managing discovered servers . . . 324

16 Password changers **326**
16.1 Password changer policy . . . 326
16.1.1 Defining a password changer policy . . . 327
16.1.2 Editing a password changer policy . . . 328
16.1.3 Deleting a password changer policy . . . 328
16.2 Custom password changers . . . 328

16.2.1 Defining a custom password changer . . . 329
16.2.2 Editing a custom password changer . . . 333
16.2.3 Deleting a custom password changer . . . 333
16.3 Importing and exporting password changers . . . 333
16.3.1 Exporting a password changer . . . 333
16.3.2 Importing a password changer . . . 334
16.4 Connection modes . . . 334
16.4.1 SSH . . . 334
16.4.2 LDAP . . . 335
16.4.3 Telnet . . . 336
16.4.4 WinRM . . . 337
16.5 Setting up password changing on a Unix system . . . 338

17 Policies **341**
17.1 AI module-based policy . . . 341
17.2 AI module-based policy examples . . . 343
17.3 Regular expression-based policy . . . 345

18 Downloads **349**
18.1 Sessions . . . 349
18.2 Files . . . 349

19 Account activity in the Access Gateway **351**

20 Access requests **355**
20.1 Awaiting requests . . . 357
20.2 Active requests . . . 358
20.3 Archived requests . . . 358

21 Sessions **360**
21.1 Filtering sessions . . . 362
21.1.1 Defining filters . . . 362
21.1.2 Managing user defined filter definitions . . . 363
21.1.3 Full text search . . . 364
21.2 Viewing sessions . . . 365
21.3 Pausing connection . . . 370
21.4 Terminating connection . . . 371
21.5 Joining live session . . . 372
21.6 Sharing sessions . . . 373
21.7 Commenting sessions . . . 375
21.8 Sessions' retention lockdown . . . 377
21.9 Exporting sessions . . . 378
21.9.1 Export Session File Formats . . . 379
21.10 Deleting sessions . . . 380
21.11 OCR processing sessions . . . 381
21.12 Session data replication . . . 382
21.13 Timestamping selected sessions . . . 384
21.14 Cancelling sessions timestamping . . . 384
21.15 Require approval for access . . . 385
21.15.1 Approving pending user requests . . . 386
21.15.2 Declining pending requests . . . 386
21.16 AI Behavioral Analysis in Sessions . . . 387

21.17 AI Session Summary [BETA] . . . 390

22 Reports **393**
22.1 System Reports . . . 393
22.2 User Reports: Periodic and On-Demand . . . 393
22.3 List of Predefined Reports . . . 394
22.4 Subscribing to a Periodic Report . . . 394
22.5 Unsubscribing from a recurring report . . . 395
22.6 Generating a report on demand . . . 395
22.7 Viewing and saving reports . . . 397
22.8 Deleting reports . . . 397

23 Productivity **398**
23.1 Overview . . . 398
23.2 Sessions analysis . . . 399
23.3 Activity comparison . . . 400

24 Administration **402**
24.1 System . . . 402
24.1.1 Date and Time . . . 402
24.1.2 SSL Certificates . . . 405
24.1.3 SSH access . . . 406
24.1.4 Sensitive features . . . 407
24.1.5 System Update . . . 408
24.1.5.1 Updating system . . . 408
24.1.5.2 Restoring previous system version . . . 410
24.1.5.3 Deleting upgrade snapshot . . . 411
24.1.6 License . . . 411
24.1.7 Hotfix . . . 414
24.1.8 Diagnostics . . . 414
24.1.9 Configuration encryption . . . 417
24.1.10 Password changers - active cluster node . . . 419
24.1.10.1 Cluster Password Changers . . . 419
24.1.11 Configuring an HTTP Proxy . . . 420
24.2 Login Timeout . . . 421
24.3 Network settings . . . 423
24.3.1 Network Interfaces Configuration . . . 423
24.3.1.1 Managing Physical Interfaces . . . 423
24.3.1.2 Defining IP Address Using System Console . . . 426
24.3.1.3 Setting Up A Network Bridge . . . 429
24.3.1.4 Setting Up Virtual Networks (VLAN) . . . 431
24.3.1.5 Setting Up Link Aggregation (LACP) . . . 432
24.3.2 Labeled IP Addresses . . . 434
24.3.3 Routing Configuration . . . 434
24.3.4 DNS Configuration . . . 436
24.3.5 ARP Table Configuration . . . 437
24.4 Notifications . . . 438
24.4.1 Configuring the SMTP Server . . . 440
24.5 Artificial Intelligence (AI) . . . 442
24.5.1 AI Behavioral Analysis . . . 442
24.5.1.1 Configuring Models Trainers . . . 443
24.5.1.2 Behavioral Analysis Models . . . 444

24.5.2 AI Session Summary [BETA] . . . 446
24.6 Trusted Timestamping . . . 448
24.7 Certificate-based authentication scheme . . . 450
24.8 Authentication . . . 451
24.8.1 External authentication server definition . . . 451
24.8.2 OpenID Connect authentication definition . . . 454
24.8.3 Global authentication settings . . . 458
24.8.3.1 Default domain . . . 458
24.8.3.2 Deny New Connections . . . 460
24.8.3.3 Password complexity . . . 460
24.8.3.4 OATH authentication definition . . . 461
24.8.3.5 SMS authentication definition . . . 462
24.8.3.6 DUO authentication definition . . . 464
24.8.3.7 Single Sign On . . . 465
24.8.3.8 Kerberos authentication settings . . . 467
24.9 External passwords repositories . . . 469
24.9.1 CyberArk Credential Provider . . . 469
24.9.2 Thycotic Secret Server . . . 471
24.9.3 Local Administrator Password Solutions (LAPS) . . . 473
24.10 Resources . . . 476
24.10.1 RDP/SSH/VNC login screen configuration . . . 476
24.10.2 *User portal* configuration . . . 478
24.10.2.1 Login Screen Configuration . . . 478
24.10.2.2 Predefined Keyboard Layout . . . 480
24.11 System Version Restore . . . 480
24.12 System Reboot . . . 481
24.13 SNMP . . . 483
24.13.1 Configuring SNMP . . . 483
24.13.2 Configuring SNMPv3 TRAP . . . 483
24.13.3 SNMP MIBs . . . 484
24.13.4 Getting SNMP readings using `snmpwalk` . . . 484
24.13.5 Fudo Enterprise specific SNMP extensions . . . 485
24.14 Backup and retention . . . 486
24.14.1 Session data backup . . . 486
24.14.2 Data retention . . . 488
24.15 External Storage . . . 490
24.15.1 Configuring External Storage . . . 490
24.15.2 Expanding external storage device . . . 491
24.16 Exporting/Importing System Configuration . . . 491
24.16.1 Exporting System Configuration . . . 492
24.16.2 Importing System Configuration . . . 492
24.17 Cluster configuration . . . 493
24.17.1 Initiating cluster . . . 495
24.17.2 Adding cluster nodes . . . 496
24.17.3 Editing cluster nodes . . . 500
24.17.4 Deleting cluster nodes . . . 500
24.17.5 Redundancy groups . . . 501
24.18 Events log . . . 504
24.18.1 Filtering logs by date and time . . . 504
24.18.2 External syslog servers . . . 505
24.18.3 Exporting events log . . . 506

24.19 Changing encryption passphrase . . . 507
24.20 Integration with CERB server . . . 508
24.21 System maintenance . . . 515
24.21.1 Backing up encryption keys . . . 515
24.21.2 Monitoring system condition . . . 519
24.21.3 Health Check . . . 520
24.21.3.1 API Health Check . . . 520
24.21.4 Callhome . . . 521
24.21.4.1 Data Collected by Callhome Service . . . 522
24.21.4.2 The Benefits of Using Callhome . . . 522
24.21.4.3 Enable/Disable Callhome . . . 523
24.21.5 Hard drive replacement . . . 523
24.21.6 Resetting configuration to default settings . . . 524

25 Reference information **528**
25.1 RDP connections broker . . . 528
25.2 Log messages . . . 529
25.3 Footer Information . . . 564

26 Fudo Officer 2.0 **565**
26.1 Configuration . . . 565
26.2 Managing Profiles . . . 568
26.2.1 Add New Profile . . . 568
26.2.2 Switch Profiles . . . 569
26.2.3 Edit Profile . . . 570
26.2.4 Delete Profile . . . 571
26.3 Managing Session Requests . . . 573
26.3.1 Awaiting Requests . . . 573
26.3.2 Active Requests . . . 574
26.3.3 Revoking Request . . . 575
26.3.4 Archived requests . . . 576
26.4 Settings . . . 577
26.4.1 Biometric Authentication . . . 577
26.4.2 Change PIN code . . . 577
26.4.3 Language . . . 578

27 Fudo ShareAccess **579**
27.1 Data Model . . . 579
27.2 Pairing Fudo Enterprise with Fudo shareaccess . . . 580
27.3 License . . . 586
27.3.1 Trial License Activation . . . 586
27.3.2 Requesting a License . . . 586
27.3.3 Uploading License File . . . 587
27.4 Manage Fudo ShareAccess Members . . . 587
27.4.1 Inviting Members . . . 587
27.4.2 Verifying Members Status . . . 589
27.4.3 Creating an Account Without an Invitation . . . 591
27.4.4 Revoking Members Status . . . 591
27.4.5 Deleting Members . . . 592
27.5 Manage Access to Resources . . . 592

28 Client applications **596**

28.1 PuTTY . . . 596
28.2 Microsoft Remote Desktop . . . 598
28.3 TightVNC Viewer . . . 600
28.4 SQL Server Management Studio . . . 601

29 Troubleshooting **603**
29.1 Booting up . . . 603
29.2 Connecting to servers . . . 604
29.3 Logging to administration panel . . . 608
29.4 Session playback . . . 609
29.5 Cluster configuration . . . 609
29.6 Trusted timestamping . . . 610
29.7 Support mode . . . 610

30 Use Cases **614**
30.1 Two-factor OATH authentication with Google Authenticator . . . 614
30.1.1 Protocols Supporting OATH Authentication Method . . . 614
30.1.2 Configuring the OATH Authentication Method . . . 615
30.2 OpenID Connect authentication definition with Microsoft Entra (Azure) . . . 620
30.3 Remote Desktop Services configuration on Windows Server for Fudo Enterprise . 626
30.3.1 Setup Remote Desktop Services (RDS) on Windows . . . 627
30.3.2 Setup Fudo Enterprise - bastion scenario (recommended) . . . 638
30.3.3 Setup Fudo Enterprise - proxy scenario . . . 645
30.4 Managing RDP Server certificates in Windows Server . . . 651
30.4.1 Locating the Server Certificate in Windows Server . . . 651
30.4.2 Providing the CA Certificate . . . 653
30.5 Configuring the Single Sign On (SSO) . . . 668
30.5.1 SSO configuration on Windows Server 2019 . . . 668
30.5.2 Setup Fudo Enterprise . . . 673
30.5.3 Setup and check user workstation - Windows2010 Client . . . 676
30.6 Handling Local Account Password Changes Using a Domain Account with WinRM Password Changer . . . 679
30.6.1 Hostname and DNS Server Configuration . . . 680
30.6.2 Adding a KDC Server . . . 680
30.6.3 Server Configuration . . . 681
30.7 Configuring Kerberos Constrained Delegation for MSSQL(TDS) Server . . . 682
30.7.1 Kerberos Authentication Configuration on Windows Server . . . 682
30.7.2 Setup Fudo Enterprise . . . 689
30.7.3 Establish a Connection . . . 692
30.8 Establishing Connections to Servers via SSH Tunnel in Fudo Enterprise . . . 693
30.8.1 General Requirements . . . 693
30.8.1.1 Establishing an SSH Connection . . . 693
30.8.1.2 Establishing an HTTP Connection . . . 699
30.8.1.3 Connecting to an Oracle Database . . . 704

31 Frequently asked questions **710**

32 Glossary **714**

Index **717**

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

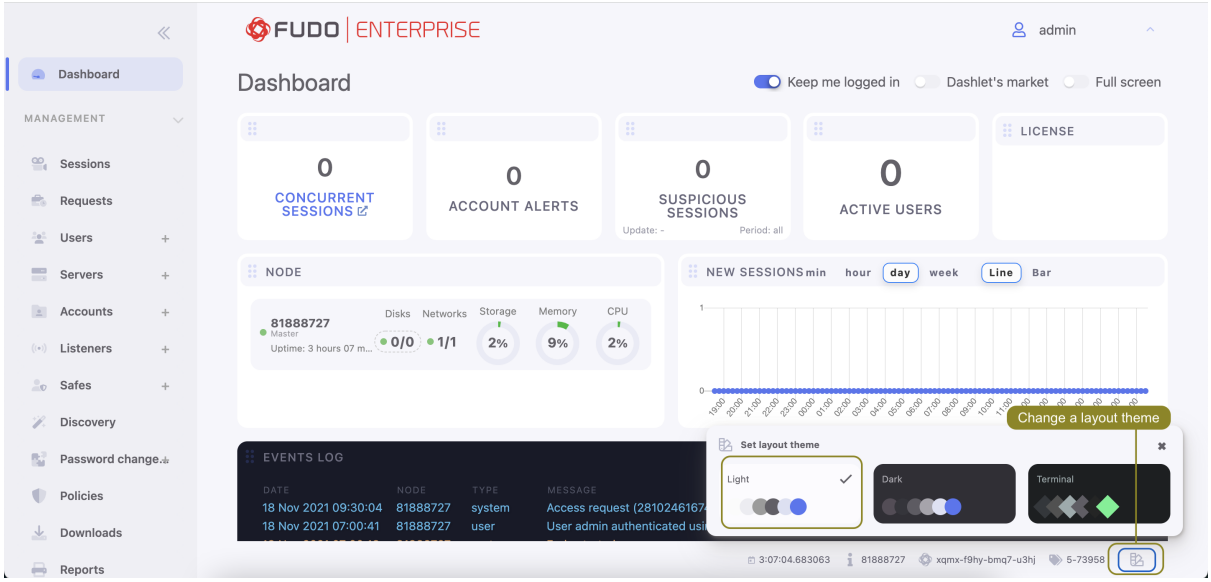
All trademarks, product names, and company names or logos cited in this document are the property of their respective owners and are used for information purpose only.

CHAPTER 2

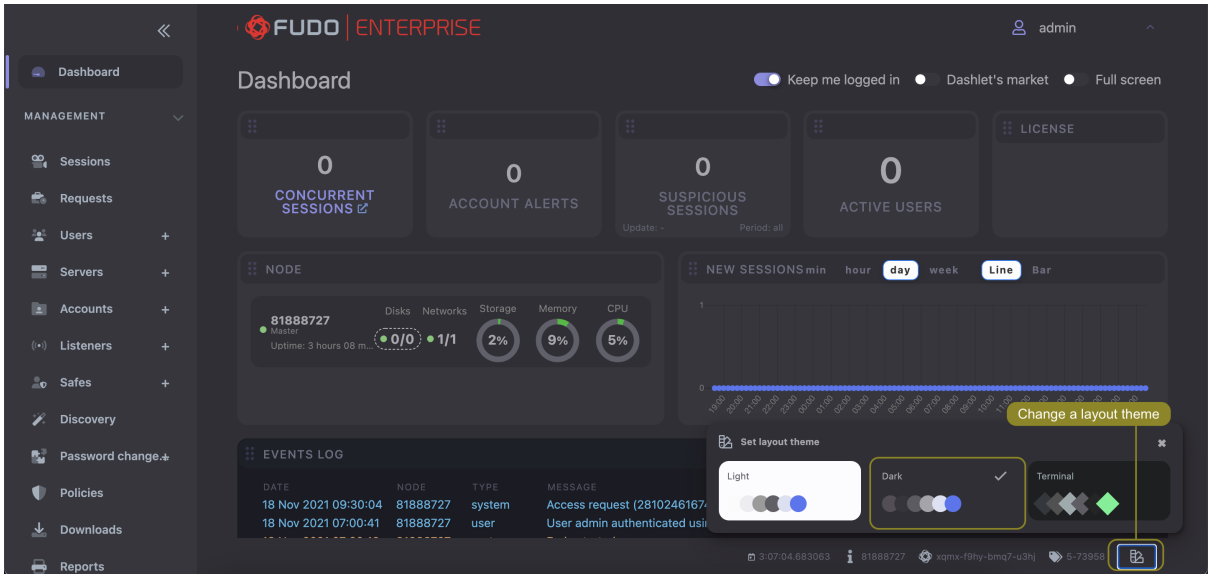
Layout themes of the Admin Panel

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.

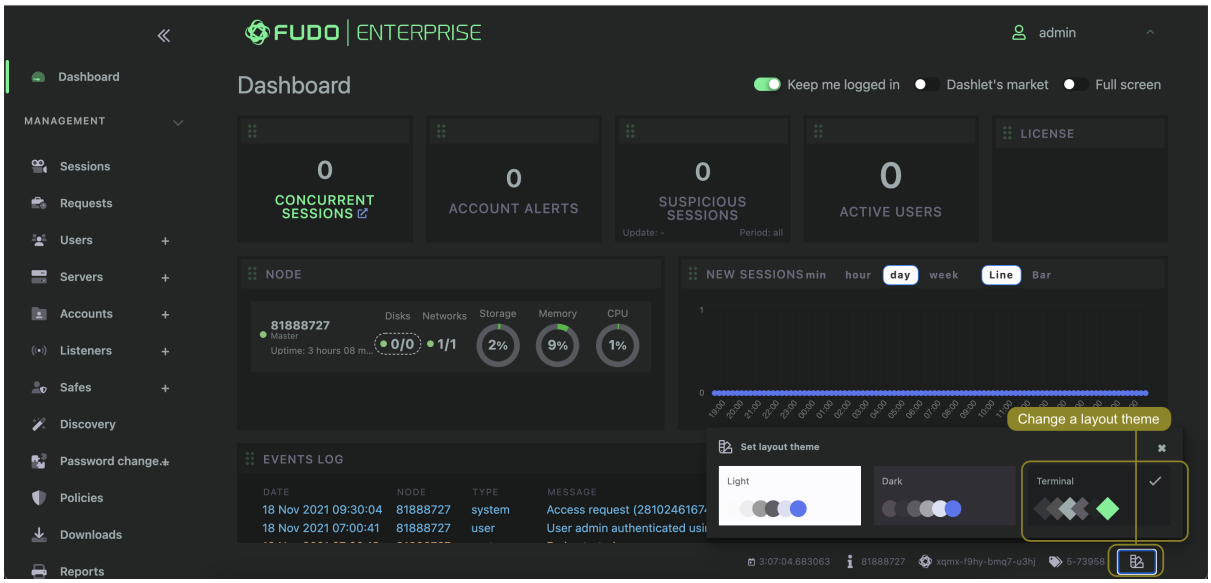
Light theme:



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 password changers within minutes. These password changers operate on a separate transport layer, such as SSH, LDAP, Telnet, or WinRM, allowing integration with various systems.

Fudo Enterprise supports password 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 *Password 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.

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

Related topics:

- *System overview*
- *Supported protocols*
- *Quick start*

3.3 Licensing

The licensing model defines the scope of features and capacity limits available in the product. The following constraints apply based on the purchased license:

Expiration Date

Each license has a defined expiration date. After this date, access to licensed features may be restricted.

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.

Number of 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

The license includes a limit on the number of active users. An active user is defined as any user who:

- has authenticated on Fudo Enterprise within the last 30 days, or
- has a *superadmin* role.

Note: Authentication is counted when a user:

- logs in to the Admin Panel or User Access gateway interface, or
- connects to any server via Fudo Enterprise.

Example:

If the system includes:

- 2 superadmins
- 2 users who authenticated on Fudo Enterprise in the last 30 days
- 2 users who did not authenticate in the last 30 days

Then the number of active users is 4.

Password Changer Assignment Limit

There is a limit on how many accounts can have a password changer assigned. Once the limit is reached, no additional password changers can be assigned to other accounts.

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.

Supported Languages

The license defines which language versions of the product interface are available. Supported languages may include:

- Polish (pl)
- English (en)
- Ukrainian (ua)
- Russian (ru)
- Kazakh (kk)

Note: To learn more about managing licenses, refer to the *License* section.

Related topics:

- *System overview*
- *Supported protocols*
- *Quick start*

3.4 Supported protocols

Deprecated since version 5.6 :class: danger

Support for the **Telnet 3270** protocol is **under review** and may be removed in a release following version 5.6. If this protocol is critical to your environment, please contact Fudo Support for more information.

3.4.1 HTTP

Supported connection modes:

- *Bastion*,
- *Gateway*,
- *Proxy*,
- *Transparent*.

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`

Notes:

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.

- Session joining is not supported.
- Login reason option is not supported.

Additionally, in the non-rendered mode:

- Bastion mode is not supported due to limitations of the protocol.
- Access to external resources is not monitored.
- Following redirections is not supported.
- Credentials forwarding is not supported.

Additionally, in the rendered mode:

- Raw HTTP data is not stored.
- A list of fonts available in Fudo Enterprise for the rendered HTTP sessions.

3.4.2 Modbus

Supported connection modes:

- *Gateway*,
- *Proxy*,
- *Transparent*.

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*,
- *Gateway*,
- *Proxy*,
- *Transparent*.

Supported client applications:

- SQL Server Management Studio,
- sqsh.

Notes:

- Session joining is not supported.

3.4.4 MySQL

Supported connection modes:

- *Gateway*,
- *Proxy*,
- *Transparent*.

Supported client applications:

- Official MySQL client,
- PyMySQL libraries for Python.

Notes:

- Session joining is not supported.
- Bastion mode is not supported due to limitations of the protocol.
- Active Directory and other external authentication sources are not supported.

3.4.5 RDP

Supported Connection Modes:

- *Bastion*,
- *Gateway*,
- *Proxy*,
- *Transparent*.

Supported Operating Systems:

- Windows Server 2016 and newer

Supported Client Applications:

- All official Microsoft clients for Windows and macOS
- FreeRDP 2.0 and newer

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 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.

Connections initiated over *Remote Desktop Web Access* can be monitored by Fudo only in Transparent/Gateway mode as the *Remote Desktop Web Access* can not provide Fudo IP address instead of original destination server.

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.

3.4.6 SSH

Supported connection modes:

- *Bastion*,
- *Gateway*,
- *Proxy*,
- *Transparent*.

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 encryption algorithms:

- Server: RSA, DSA
- Listener: RSA, DSA

Supported hashing algorithms:

- MD5
- SHA256

Supported types of SSH keys:

- RSA
- ED25519, ED25519-SK
- ECDSA, ECDSA-SK
- DSA (with the *Legacy crypto* option enabled)

Supported encoding: UTF-8

Supported ciphers:

Warning: The *OpenSSH* protocol has been updated to version 9.6 since Fudo Enterprise 5.4.8. The following lists are current as of version 5.4.8.

- If you are using a version of Fudo Enterprise earlier than 5.4.8, please refer to the 5.3 or earlier documentation.
- If you are using version 5.4.7, please read the warning regarding *MAC* algorithms below.

- 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`
  - `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 4 more *host key* algorithms supported when the *Legacy crypto* option is enabled:
  - `ssh-rsa`
  - `ssh-rsa-cert-v01@openssh.com`
  - `ssh-dss`
  - `ssh-dss-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 10 more *encryption* algorithms supported when the *Legacy crypto* option is enabled:
  - `aes128-cbc`
  - `aes192-cbc`
  - `aes256-cbc`

  - rijndael-cbc@lysator.liu.se
  - 3des-cbc
  - arcfour256
  - arcfour128
  - arcfour
  - blowfish-cbc
  - cast128-cbc
- Supported *MAC* algorithms:
  - umac-64-etm@openssh.com
  - umac-128-etm@openssh.com
  - hmac-sha2-256-etm@openssh.com
  - hmac-sha2-512-etm@openssh.com
  - umac-64@openssh.com
  - umac-128@openssh.com
  - hmac-sha2-256
  - hmac-sha2-512
- plus, there are 11 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-ripemd160
  - hmac-ripemd160@openssh.com
  - hmac-ripemd160-etm@openssh.com
  - hmac-md5
  - hmac-md5-96
  - hmac-md5-etm@openssh.com
  - hmac-md5-96-etm@openssh.com

Warning: Version Fudo Enterprise 5.4.7 introduced a reduced list of supported MAC algorithms:

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

- `umac-64@openssh.com`

plus 6 more *MAC* algorithms supported when the *Legacy crypto* option enabled:

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

Notes:

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

3.4.7 Telnet 3270

Deprecated since version 5.6 :class: danger

Support for the **Telnet 3270** protocol is **under review** and may be removed in a release following version 5.6. If this protocol is critical to your environment, please contact Fudo Support for more information.

Supported connection modes:

- *Bastion*,
- *Gateway*,
- *Proxy*,
- *Transparent*.

Supported client applications:

- IBM Personal Communications,
- 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.

3.4.8 Telnet 5250

Supported connection modes:

- *Bastion*,
- *Gateway*,
- *Proxy*,
- *Transparent*.

Supported client applications:

- IBM Personal Communications,
- 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.

3.4.9 Telnet

Supported connection modes:

- *Bastion*,
- *Gateway*,
- *Proxy*,
- *Transparent*.

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.

3.4.10 VNC

Supported connection modes:

- *Bastion*,
- *Gateway*,
- *Proxy*,
- *Transparent*.

Suggested client applications:

- TightVNC,
- RealVNC.

Supported OCR languages:

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

Notes:

- VNC protocol implementation supports user authentication over RADIUS in challenge-response mode.

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).

3.4.11 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.

3.4.12 TCP

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

Supported connection modes:

- *Gateway*,
- *Proxy*,
- *Transparent*.

Notes:

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

3.4.13 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 Password Change Policy for a particular account.

Notes:

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

3.5 Deployment scenarios

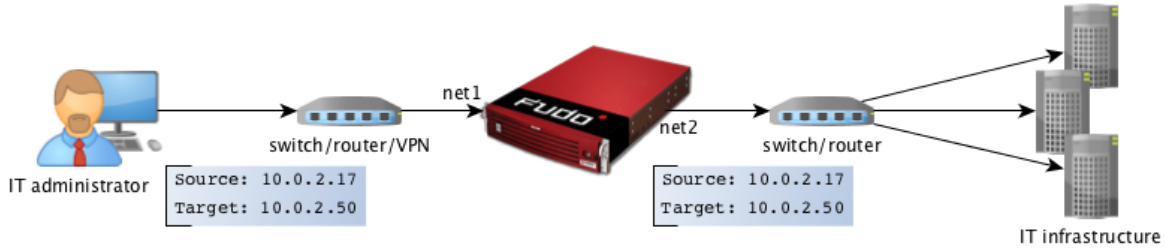
Note: It is advised to deploy the Fudo Enterprise within the IT infrastructure, so it only mediates administrative connections. It will allow for lowering system load, network traffic optimization as well as maintaining access to hosted services in case of hardware malfunction.

Bridge

Deprecated since version 5.6

Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

In bridge mode Fudo Enterprise mediates communication between users and servers regardless whether the traffic is being monitored (i.e. it uses any of supported protocols) or not.



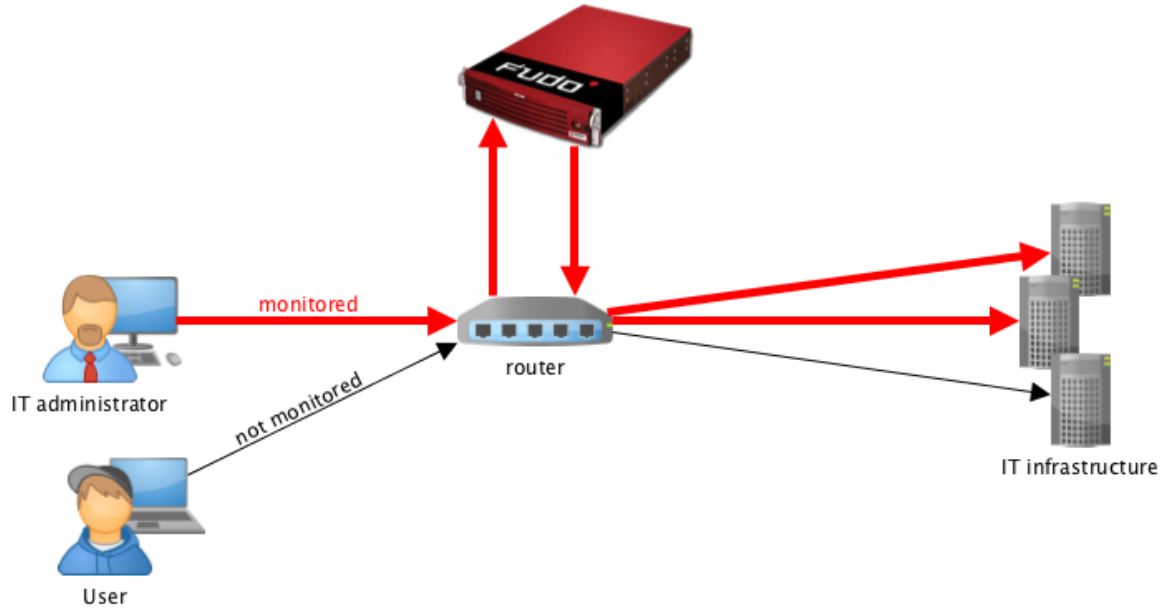
Mediating packages transfer, Fudo Enterprise preserves source IP address when forwarding requests to destination servers.

Such solution allows keeping existing rules on firewalls which control access to internal resources.

For more information on configuring bridge refer to the *Network configuration* topic.

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*

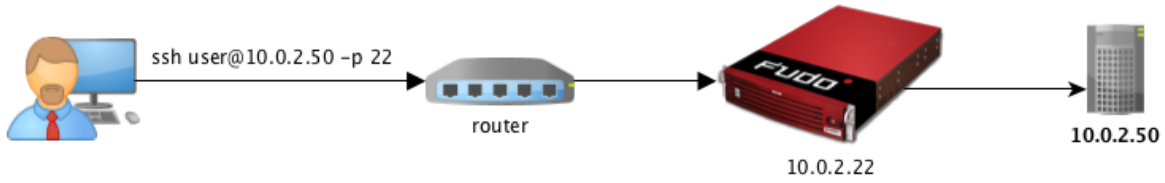
3.6 Connection modes

Deprecated since version 5.6

Fudo Enterprise 5.6 is the last version supporting **transparent** and **gateway** modes in the **listeners configuration**. Listeners using these modes must be reconfigured to use proxy and bastion modes before upgrading to the next release.

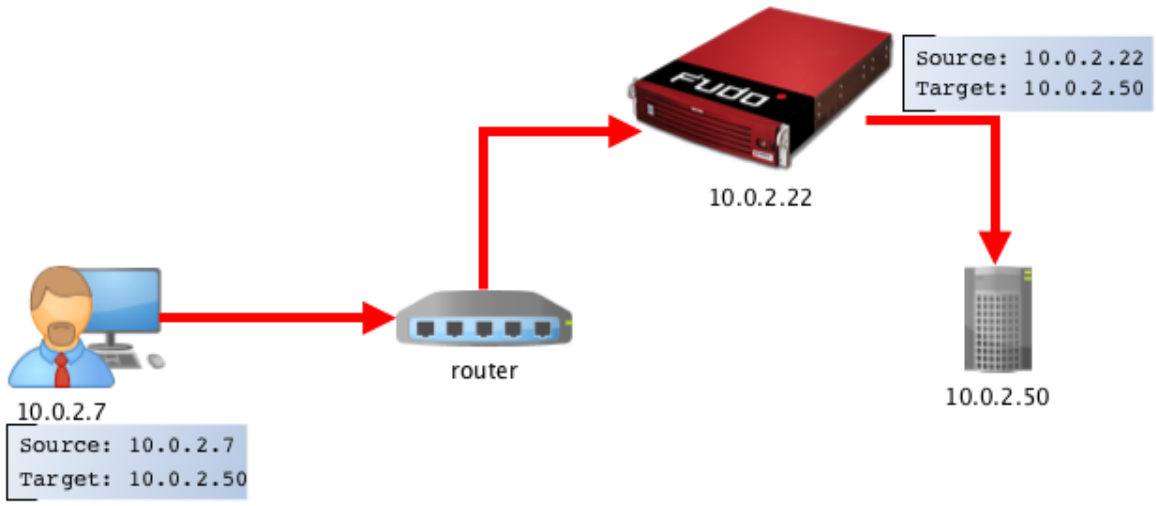
Transparent

In transparent mode, users connect to destination server using given server's IP address.



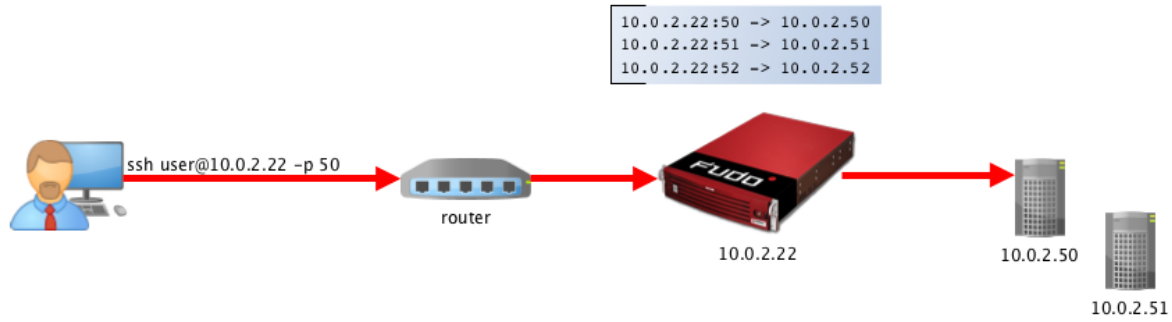
Gateway

In gateway mode, users connect to destination server using the server's actual IP address. Fudo Enterprise mediates connection with the server using own IP address. This ensures that the traffic from the server to the user goes through Fudo Enterprise.



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.

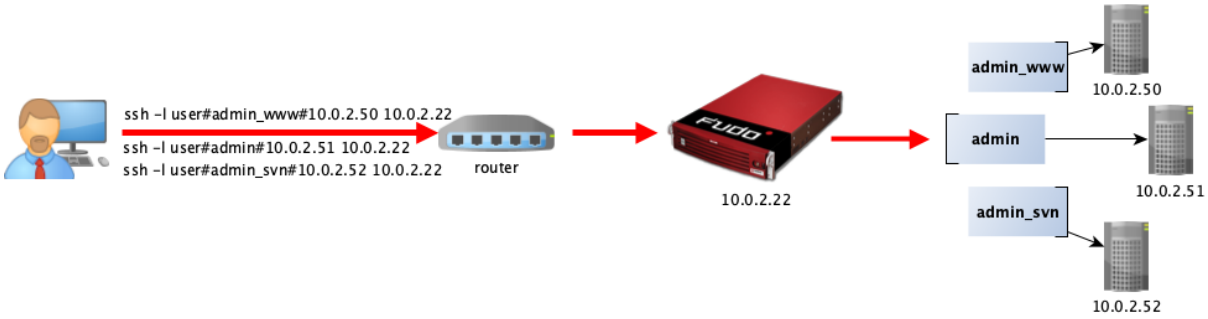


Such approach enables concealing actual IP addressing and allows configuring servers to only accept requests sent from Fudo Enterprise.

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*,
- *LDAP*,
- *Active Directory*,
- *OATH*,
- *SMS*,
- *DUO*,
- *Certificate*.

Note:

- External authentication servers CERB, RADIUS, 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 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 *Password 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

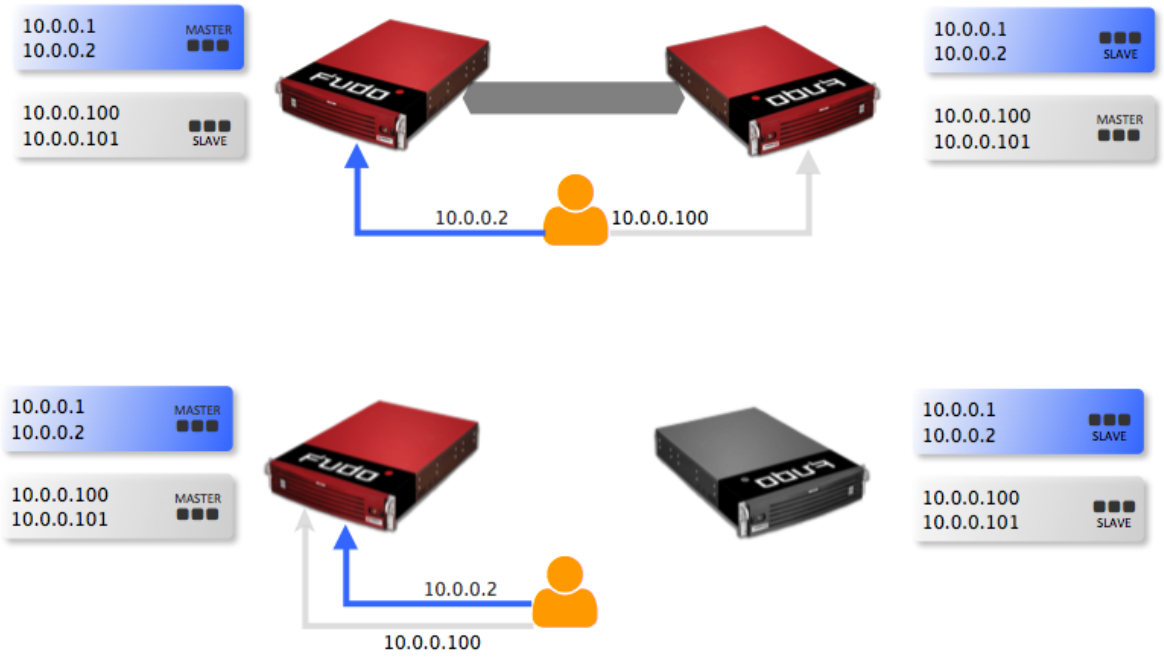
System hardware configuration is optimized to deliver high performance and high availability.

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.

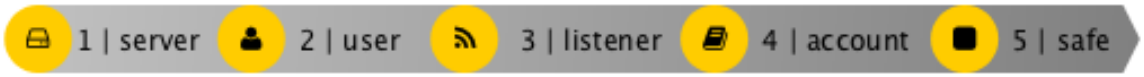
Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

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); password changing policy as well as the password changer itself.

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

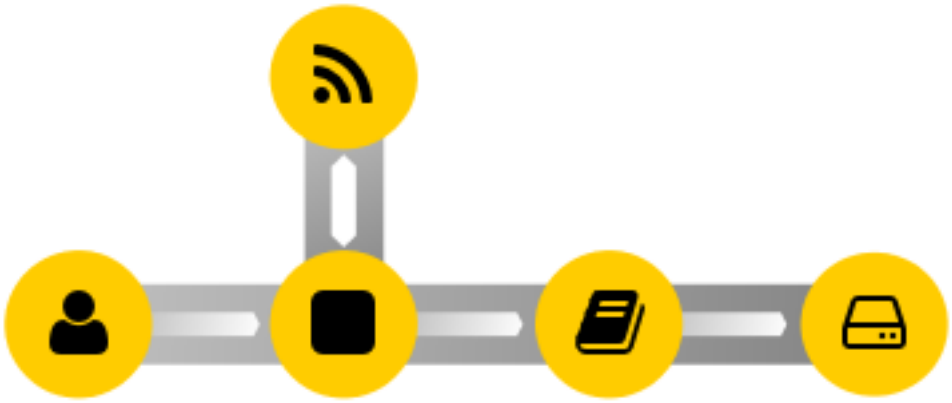
Listener determines server connection mode (proxy, gateway, transparent, bastion) as well as its specifics.

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



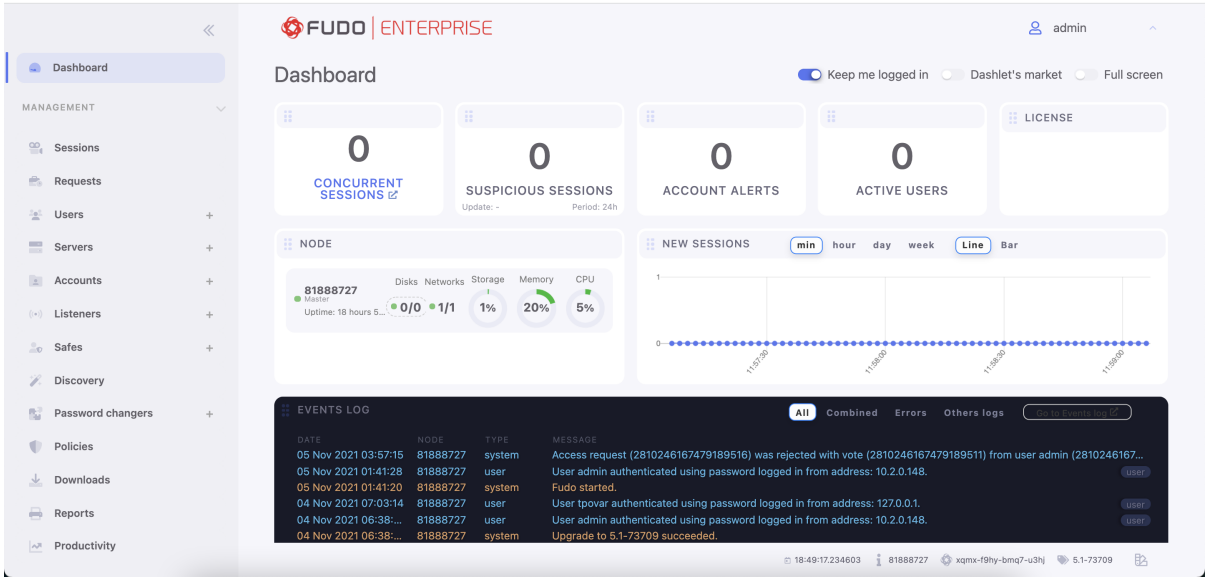
Safe is the central data model object. It regulates access to monitores servers by specifying privileged accounts on monitored servers along with the listeners which determine the actual connection parameters (e.g. IP address, port number) depending on the given protocol. This kind of data model allows 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.

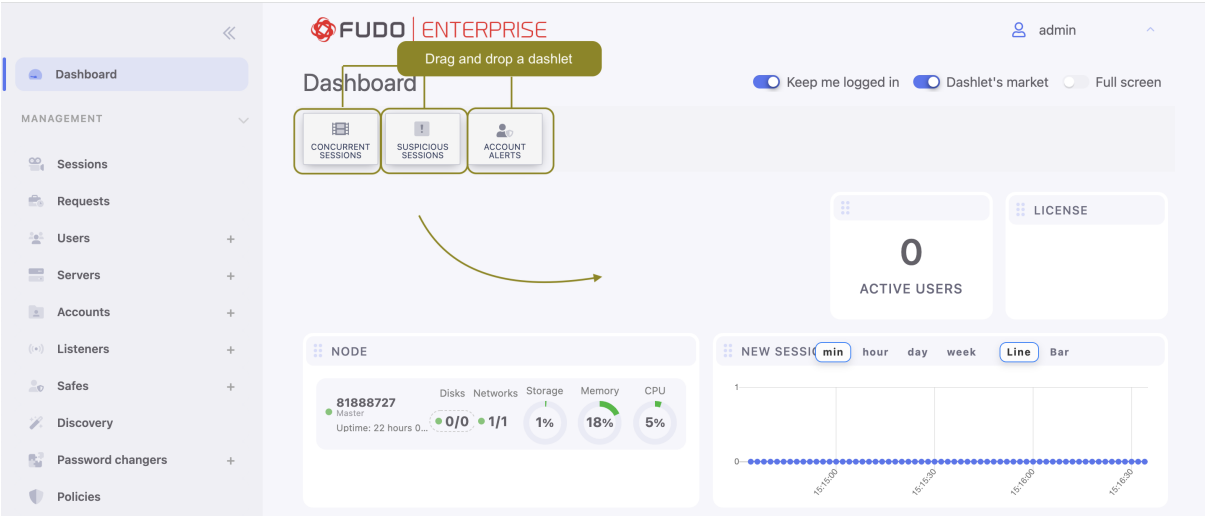
3.10.1 Widgets

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.

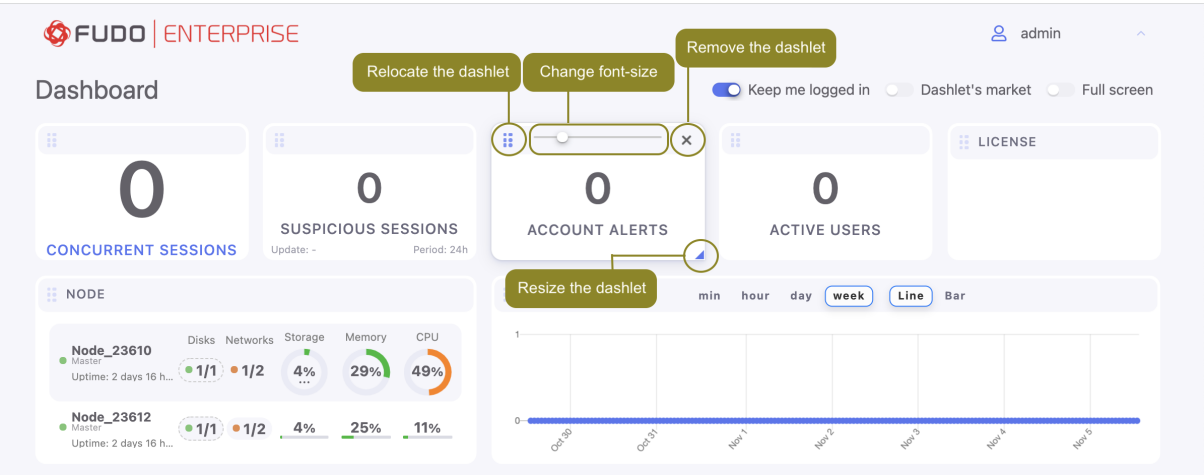
Note: Available widgets depend on the user's privileges and object-level access (capabilities).

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.

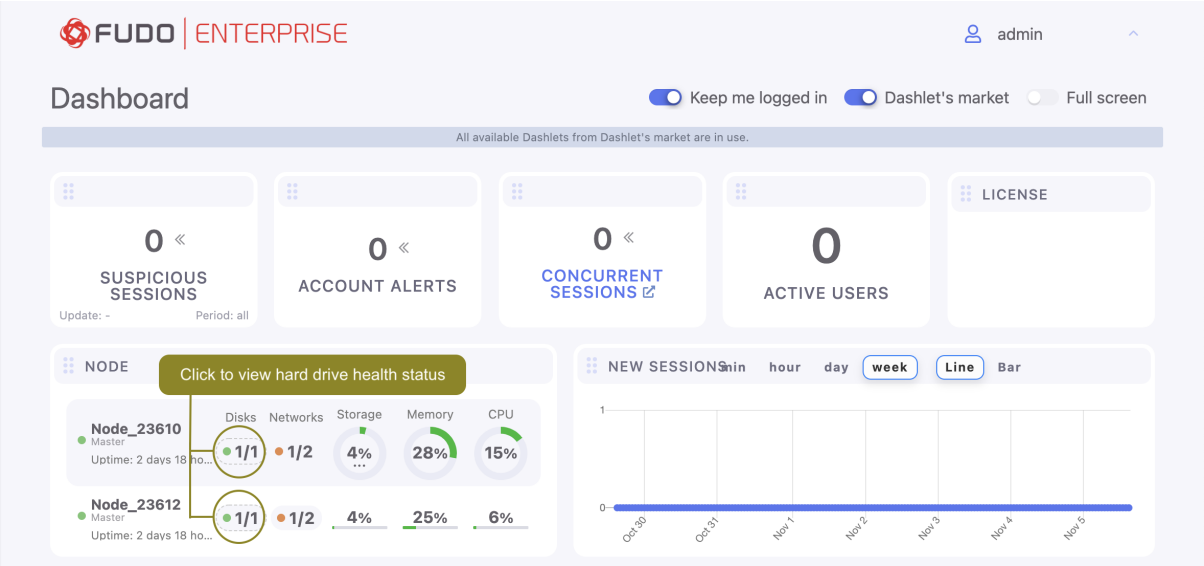


- Click and drag bottom-right corner of the dashlet to resize it.
- Click and drag the top-left corner to relocate the dashlet.
- Click arrows to change font-size.
- Click ✖ icon in the top-right corner. Then, click *Remove* to remove selected dashlet.

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.

Related topics:

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

3.11 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 (Chromium based).

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

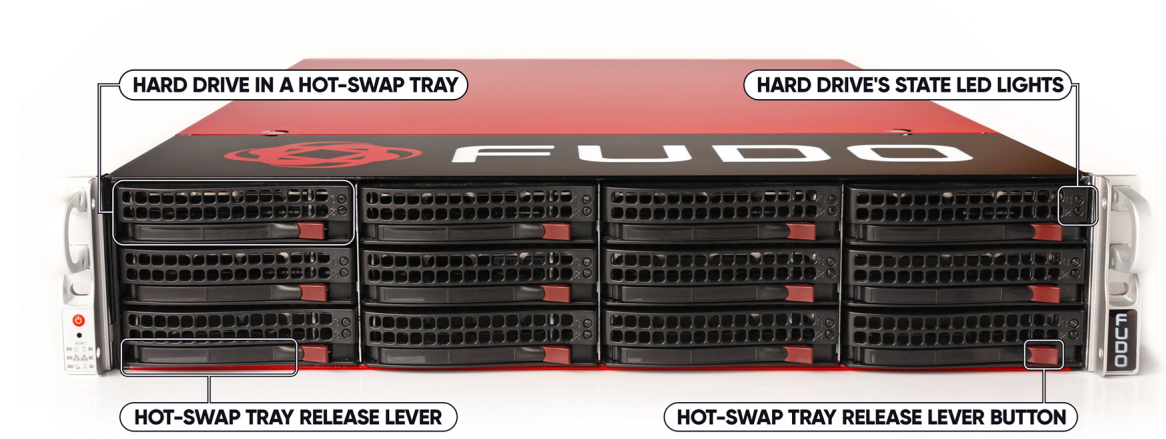
Fudo Enterprise is delivered in a 2U (F100x), 3U (F300x) or 4U (F500x) 19" rack server case.

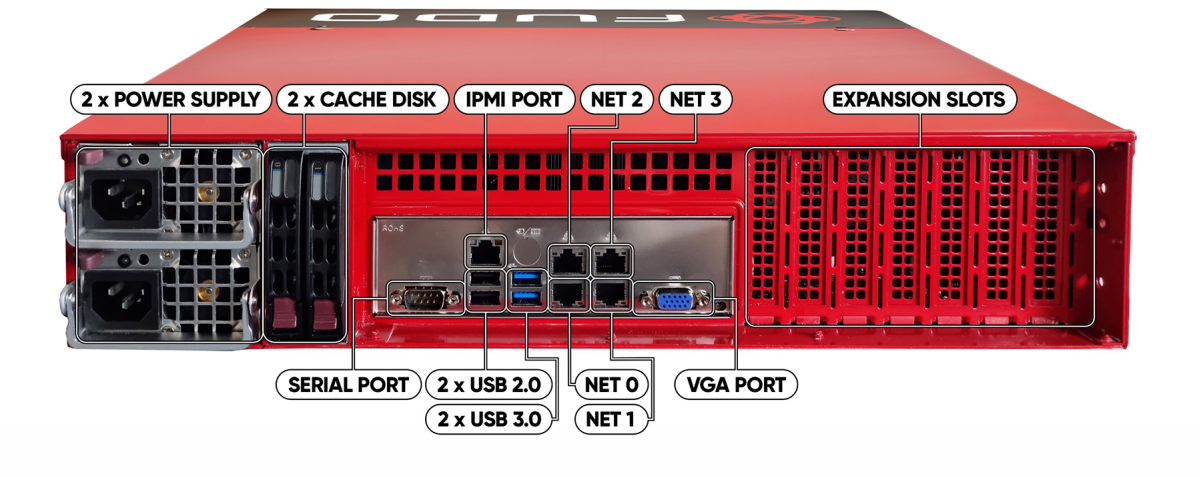
Fudo Enterprise F1002

- 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.





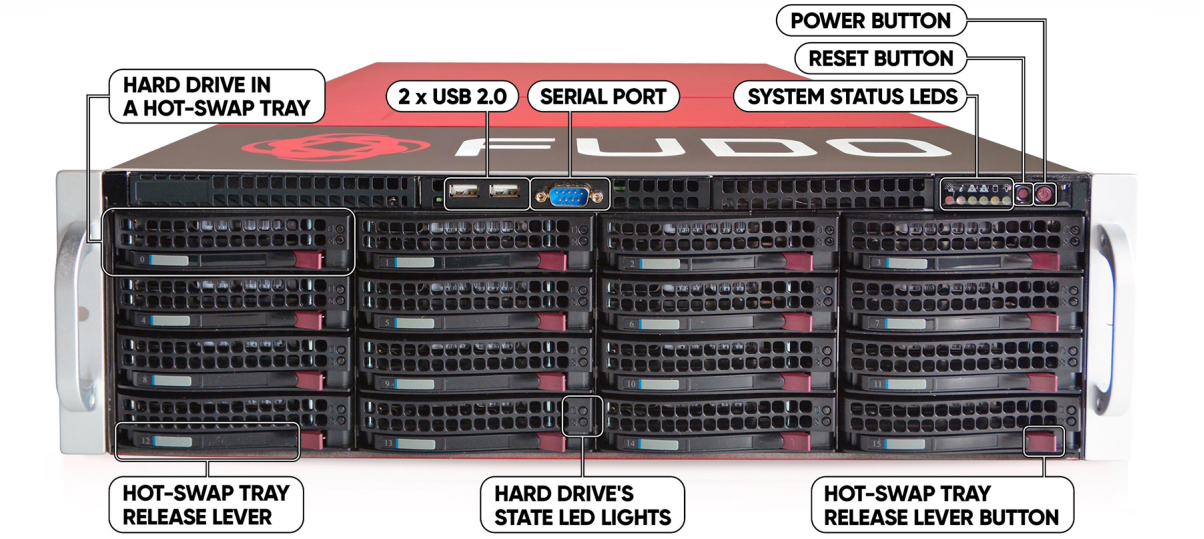


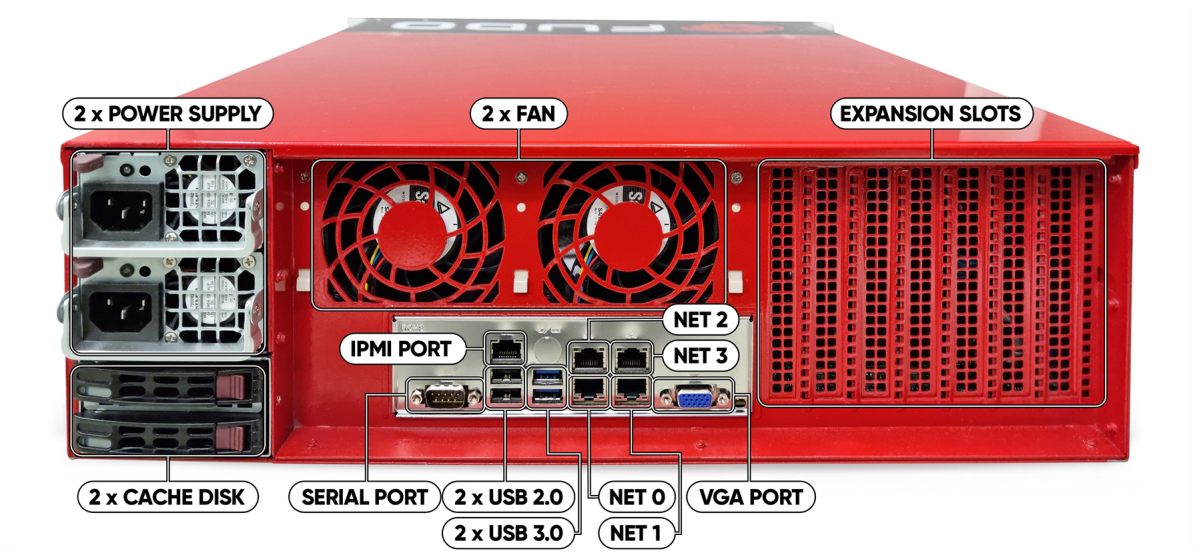
Fudo Enterprise F3002

- 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.





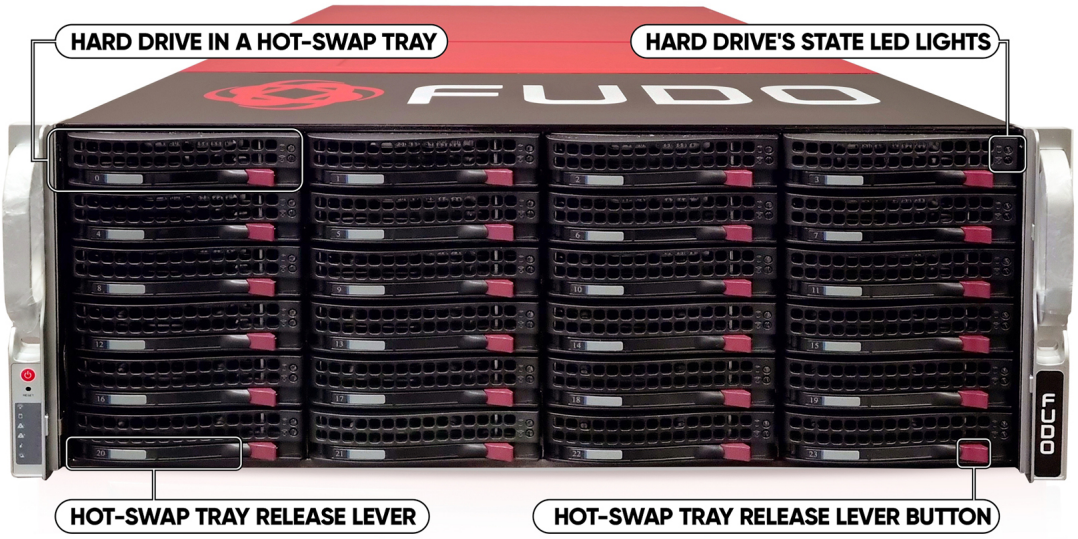


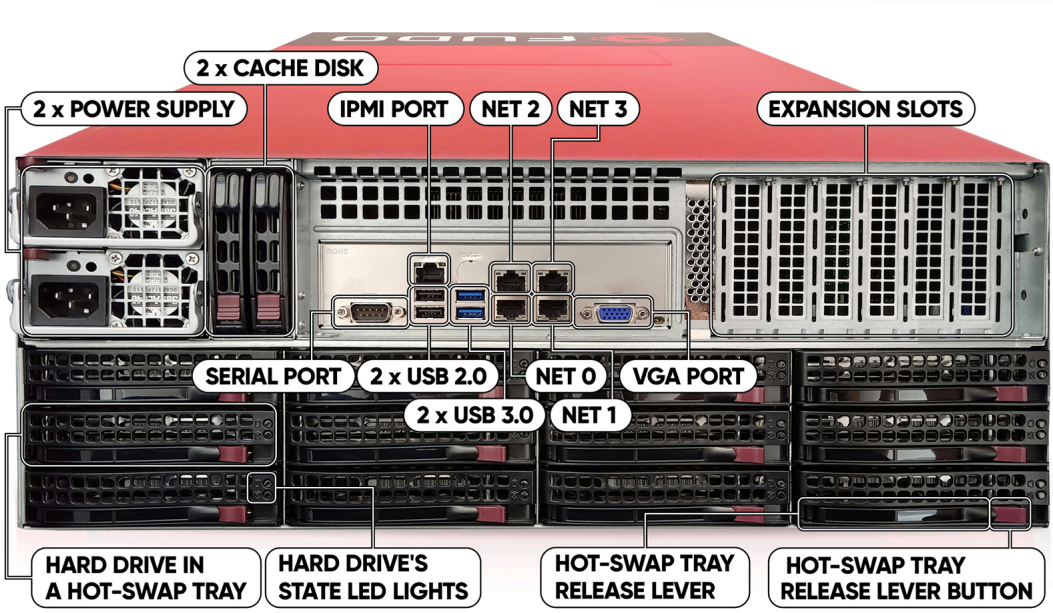
Fudo Enterprise F5000

- 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.


POWER BUTTON
RESET BUTTON
FRONT PANEL LOCK
FUDO
F5000
LED STATUS LIGHTS
FRONT PANEL RELEASE LATCH


HARD DRIVE IN A HOT-SWAP TRAY
HARD DRIVE'S STATE LED LIGHTS
FUDO
HOT-SWAP TRAY RELEASE LEVER
HOT-SWAP TRAY RELEASE LEVER BUTTON



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.

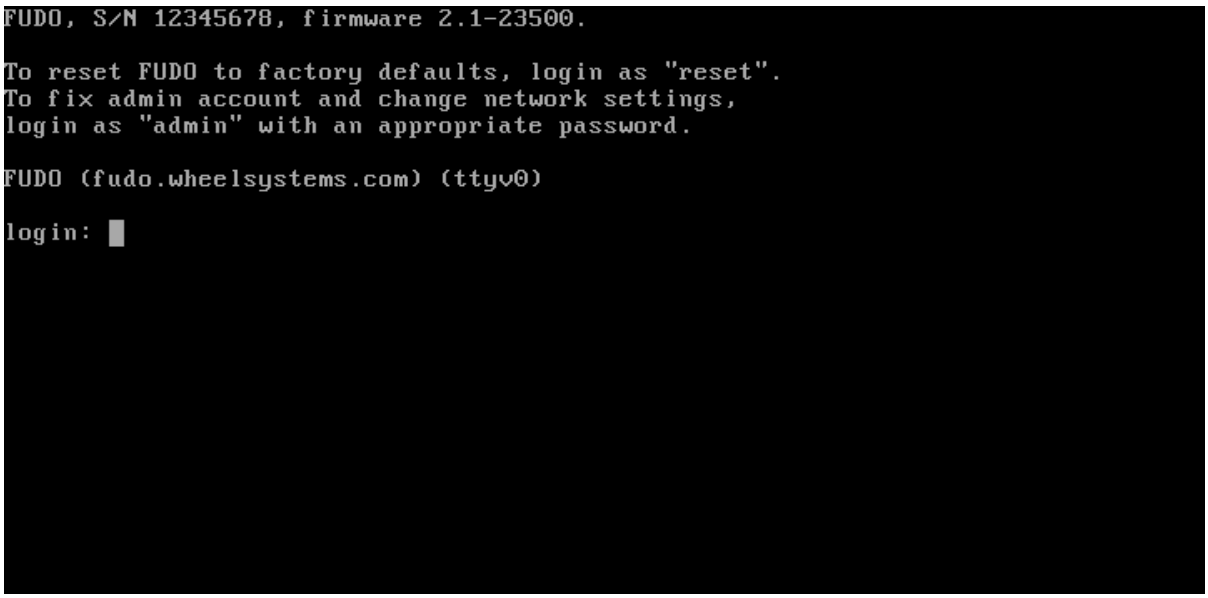
Setting IP address using system console

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

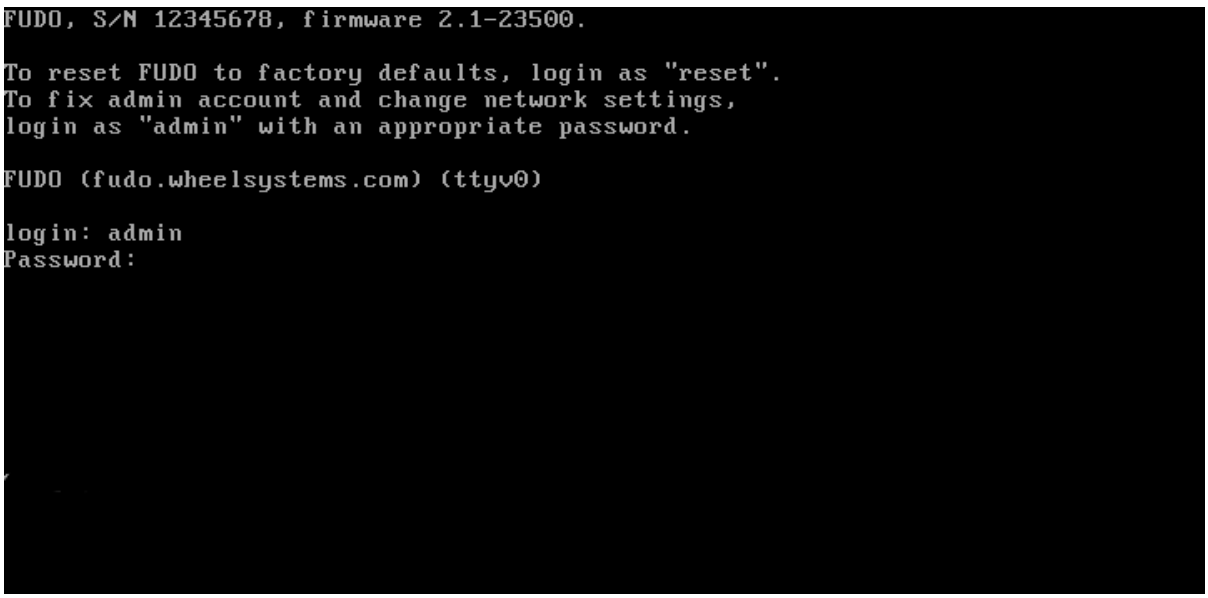
Note: Default login credentials:

login: admin
password: proxycrypto

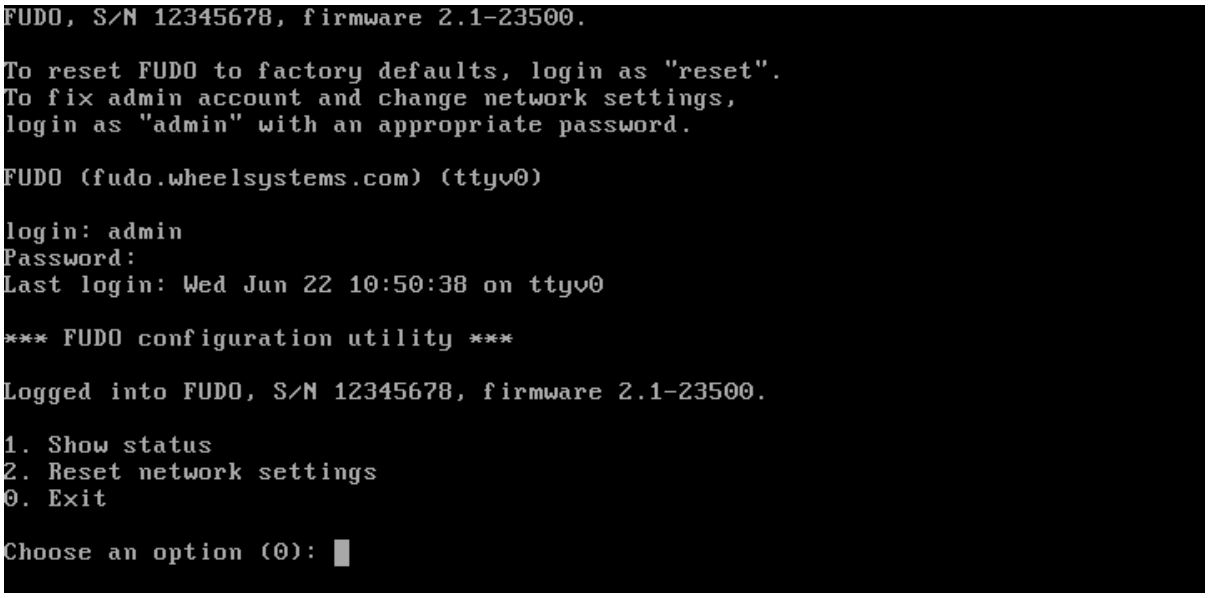
In cloud Fudo Enterprise versions virtual machine ID is usually set up as default password. Please contact your Fudo Enterprise reseller to learn more.



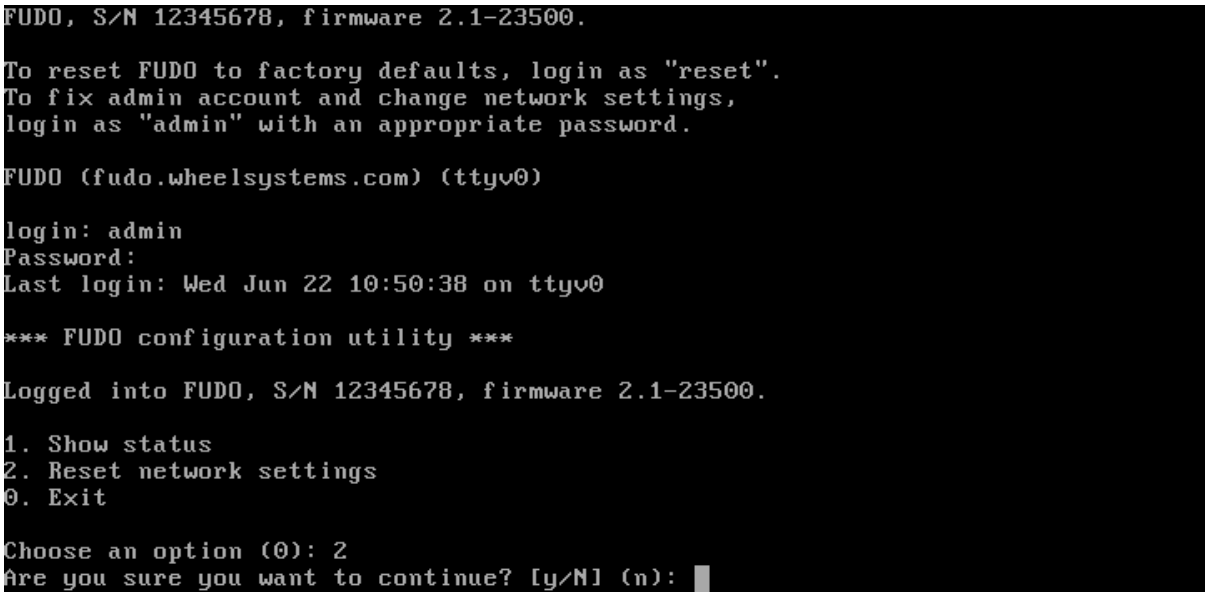
3. Enter administrator account password and press *Enter*.



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



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



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

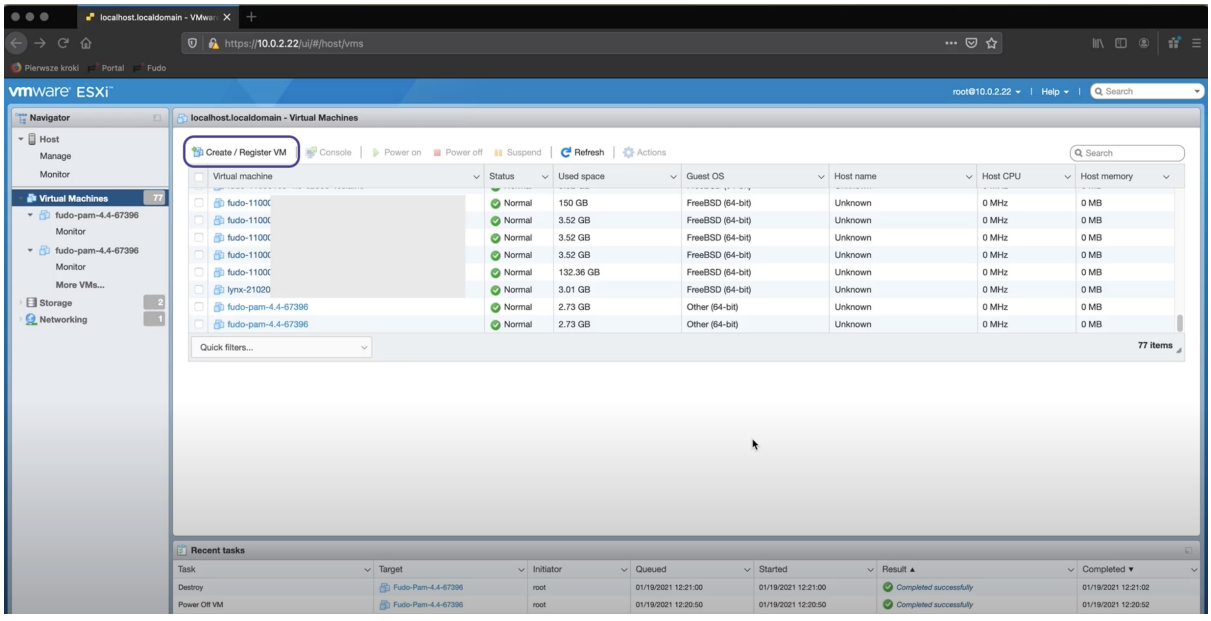
Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
Enter new default gateway IP address (10.0.0.1):
```

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.

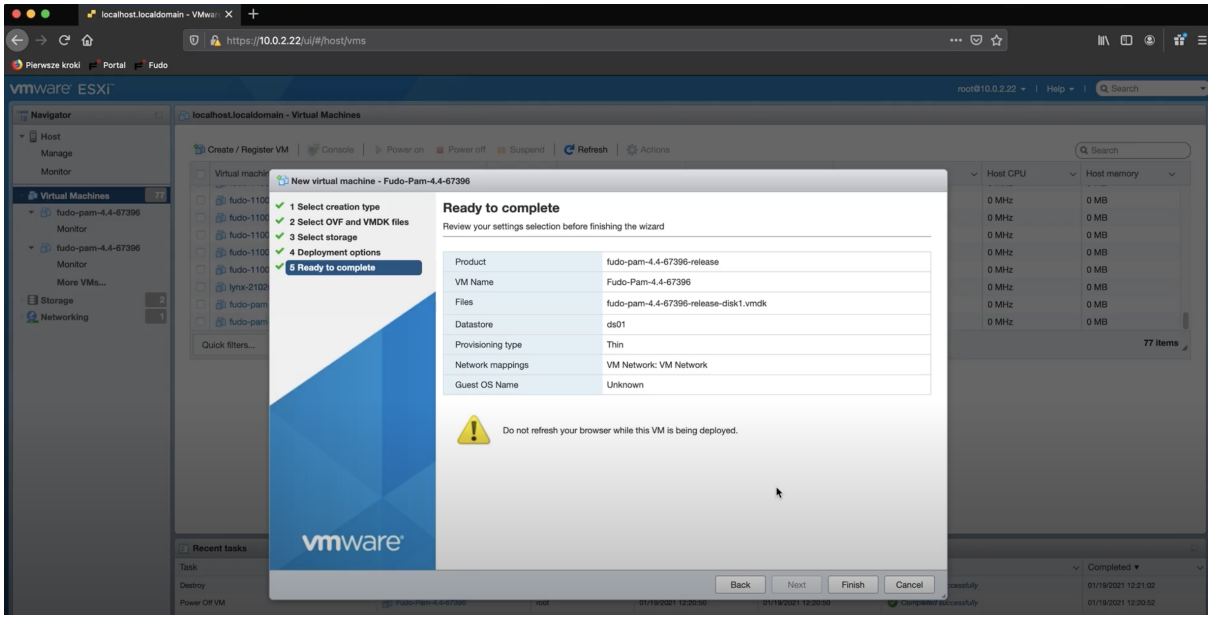
VMware Installation with OVA file

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.

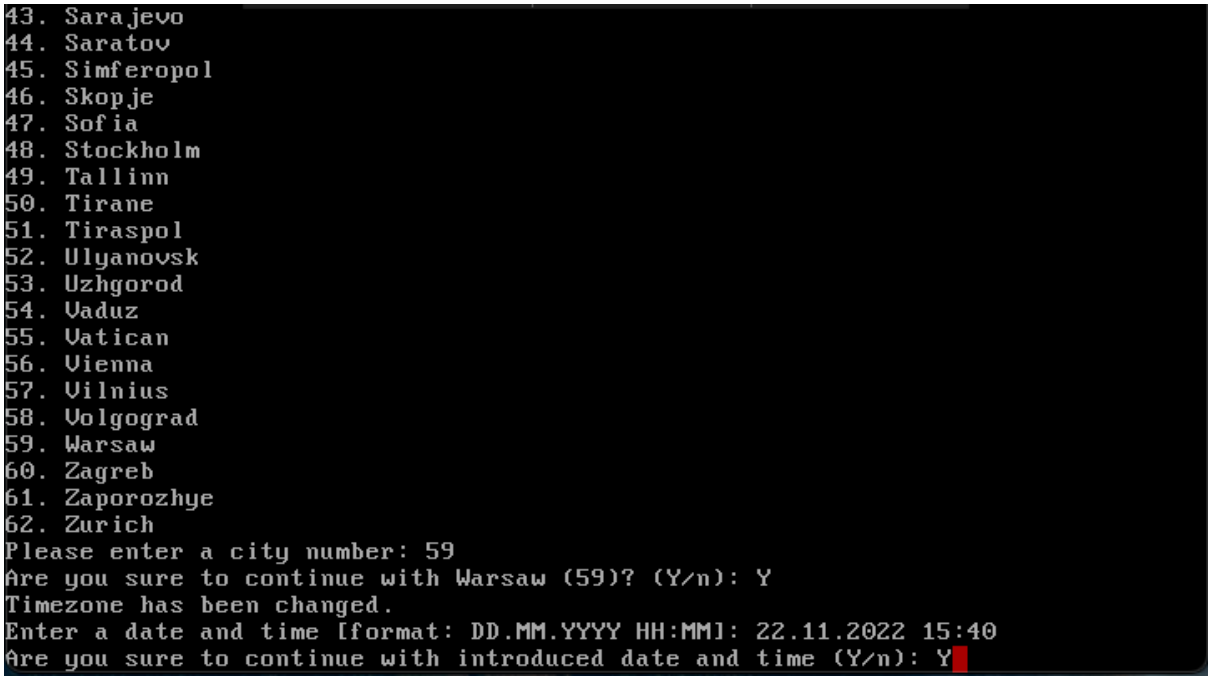


7. Click *Finish* and wait for the configuration file to be fully uploaded.
8. Initialize the machine by selecting its record.
9. Click the *Console* button and select the *Launch remote console* option. Select your application and verify certificate.
10. In the console, provide a passphrase.

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.



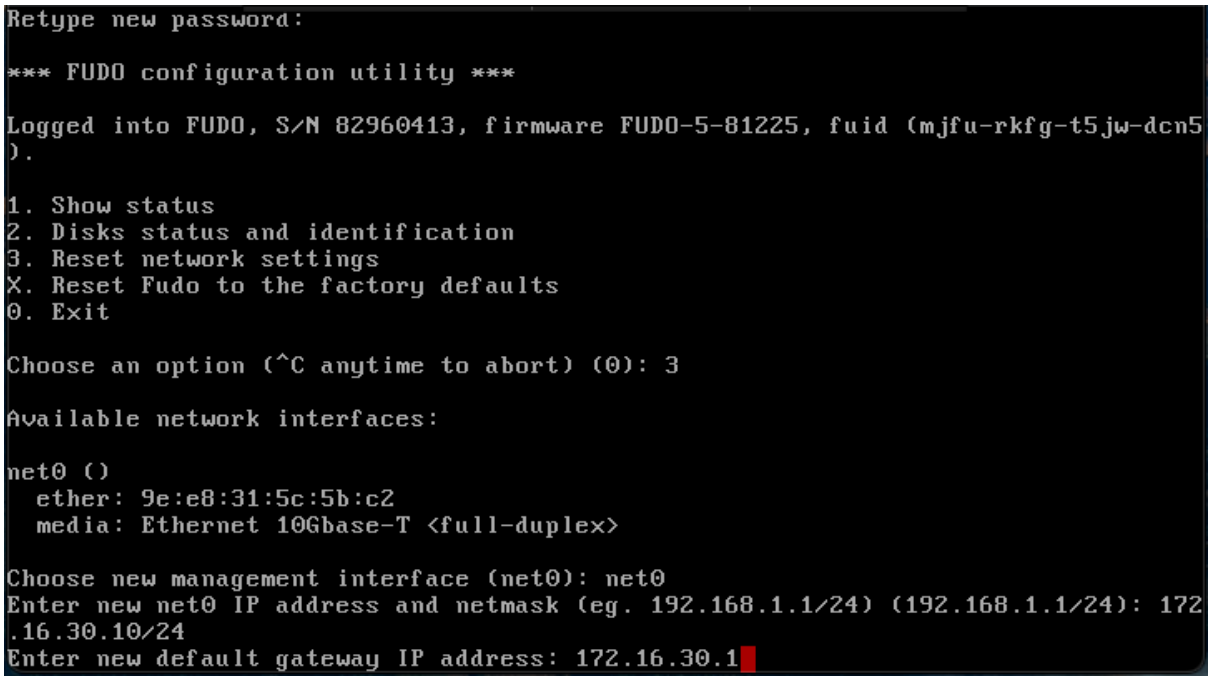
13. Set the network configuration:

    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.



Note: Your Fudo Enterprise instance has been successfully initiated! Now you can enter the registered IP address in your browser and start with your first configuration.

Proxmox Installation with OVF file

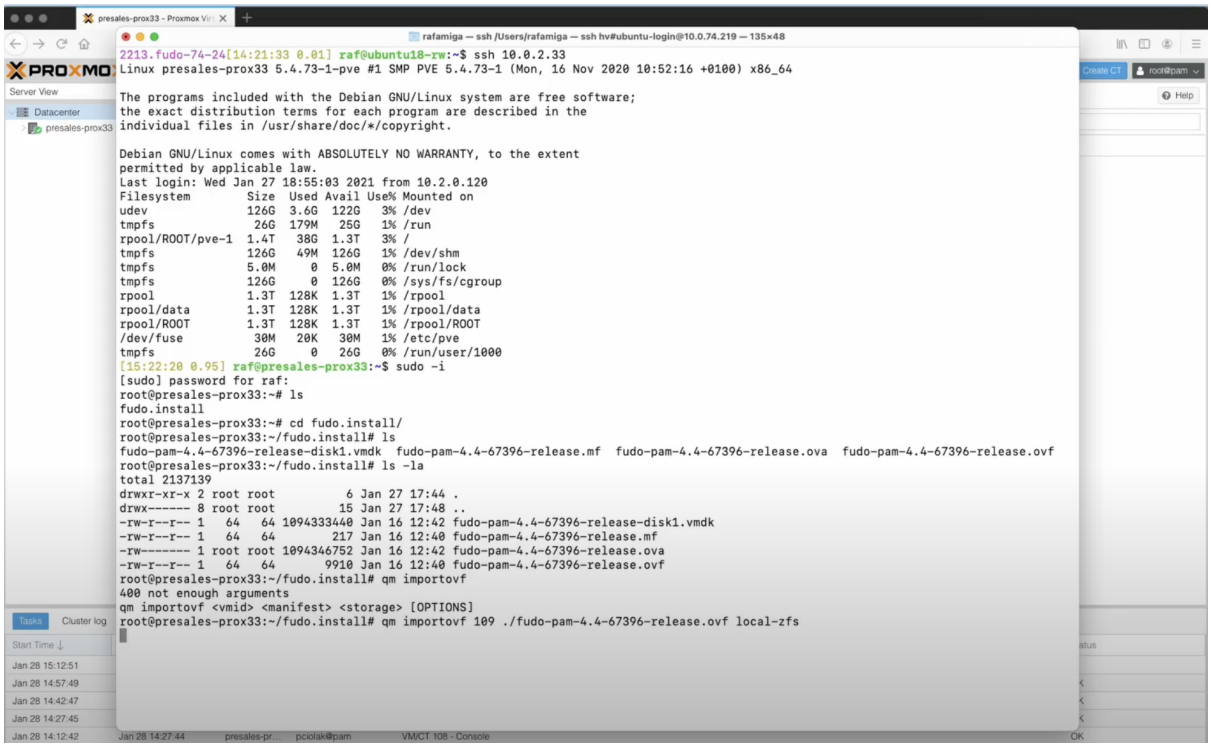
1. Create a new machine using cores, memory and VM name as read from the OVF manifest, and import the disks to the local-zfs storage:

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

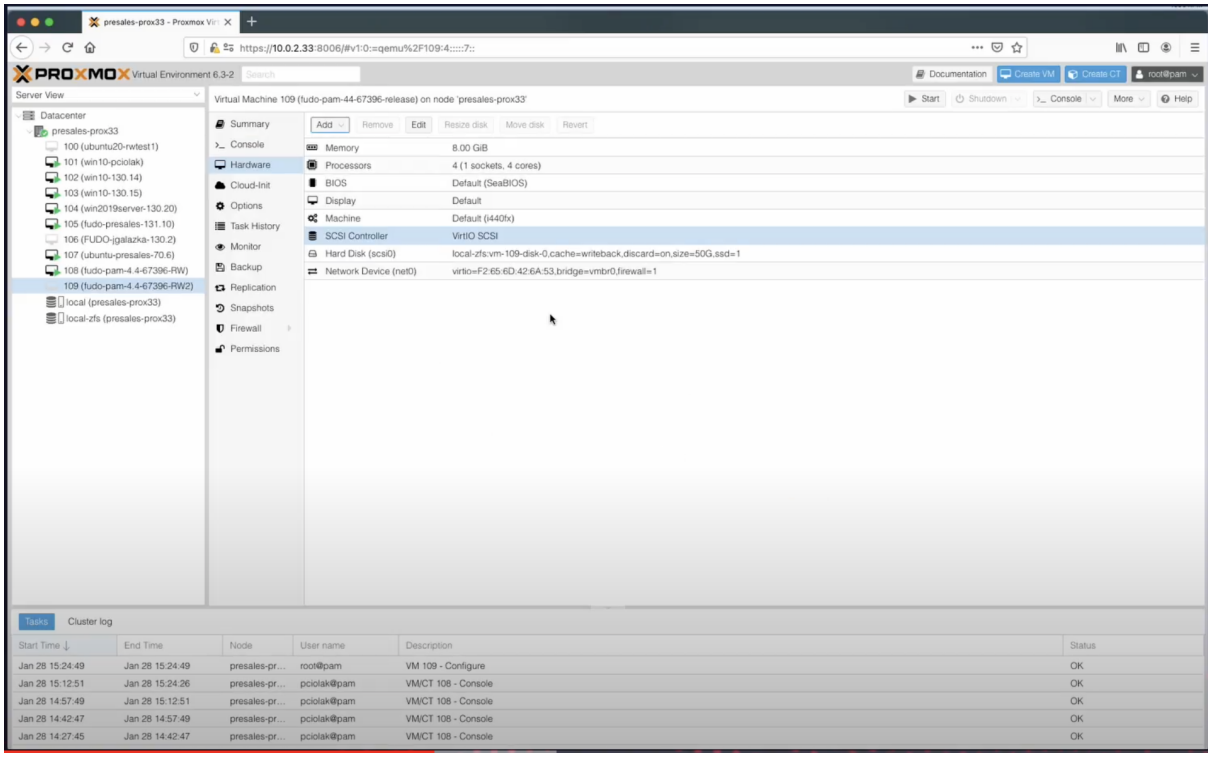
   b. In the folder *fudo.install* execute a command: `qm importovf <vmid> <manifest> <storage> [OPTIONS]`

   for example:

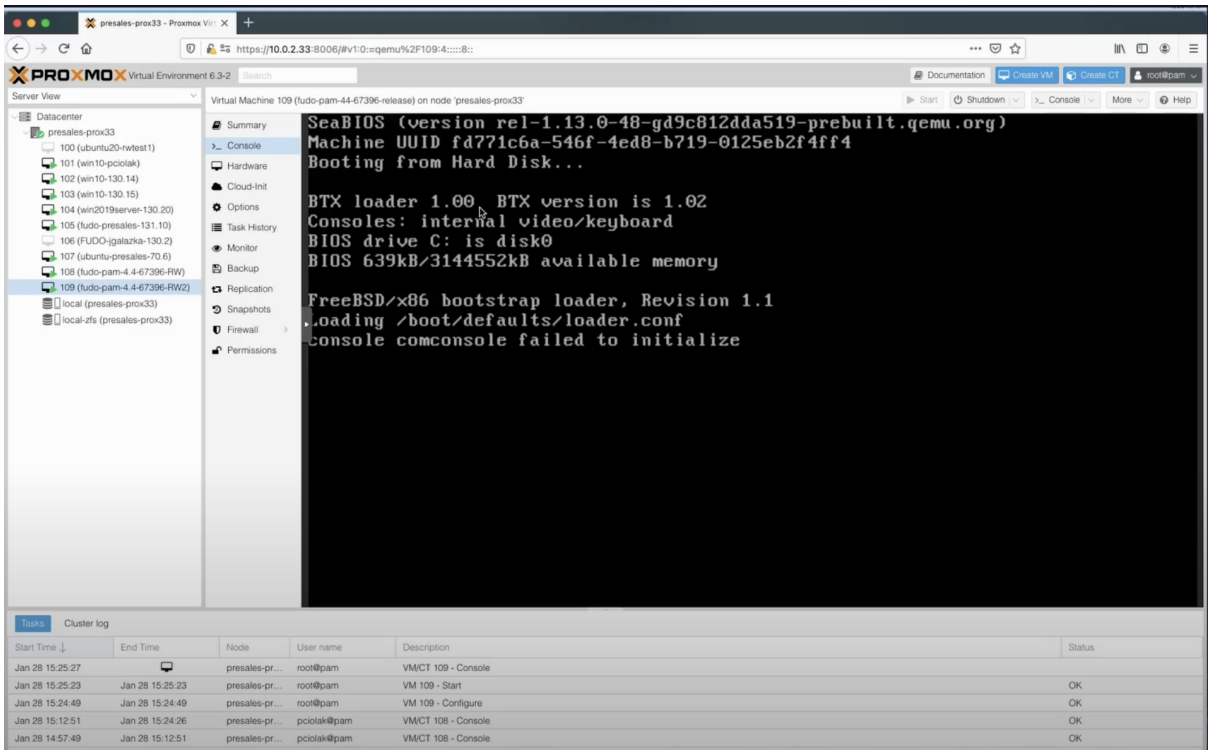
   `qm importovf 109 ./fudo-one-36271-release.ovf local-zfs`



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 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

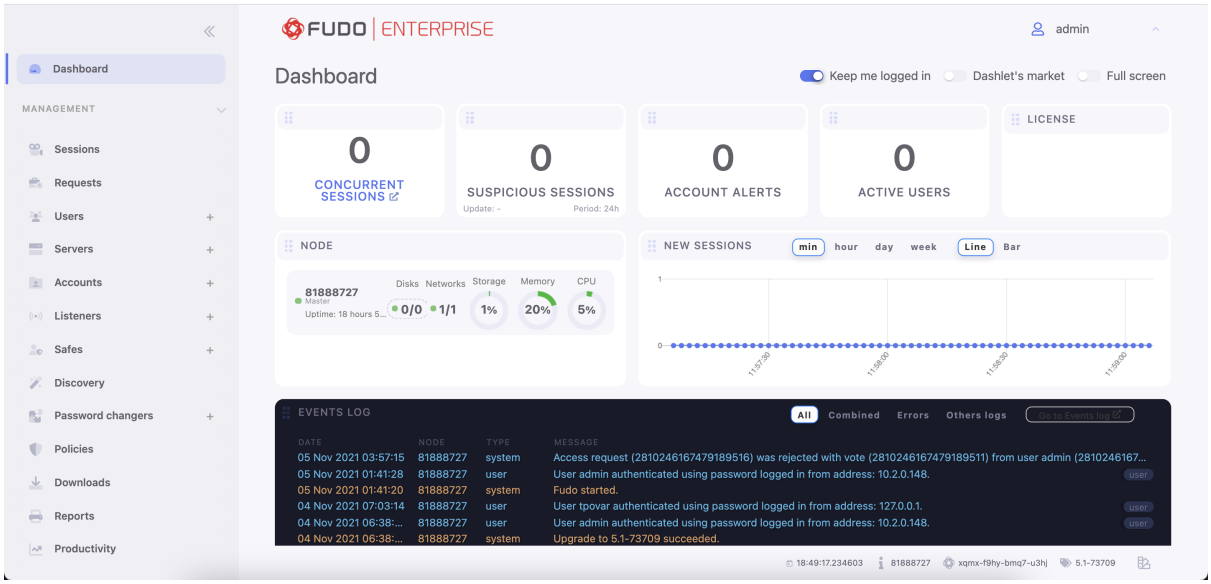
Fudo Enterprise encompasses two primary access interfaces:

- 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.

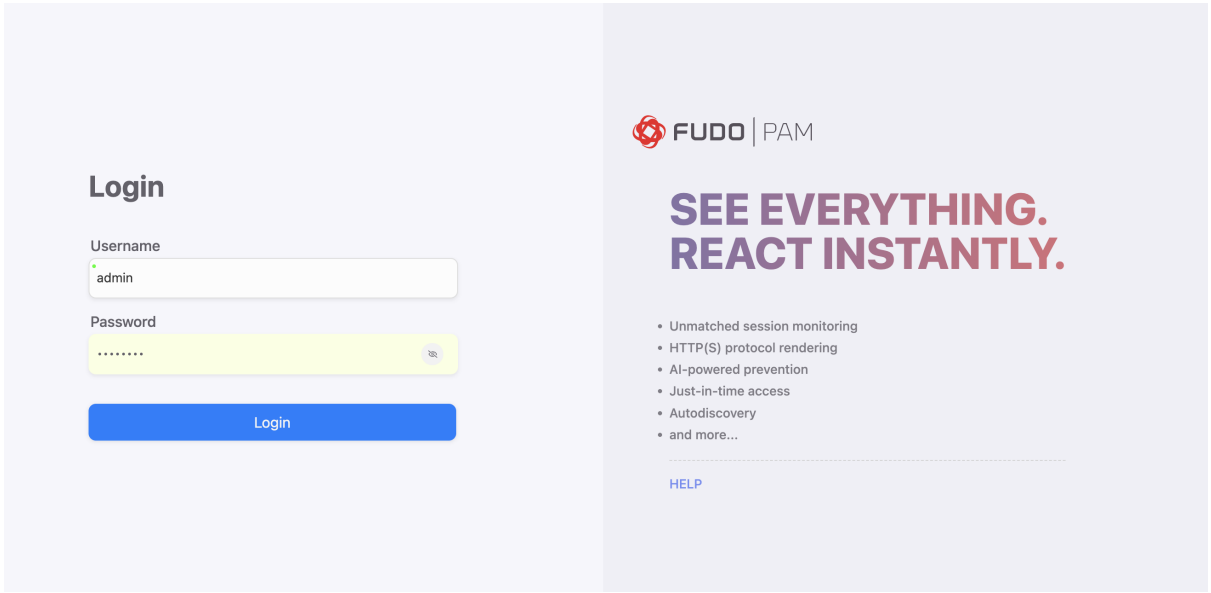


To access the Admin Panel follow below steps:

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.

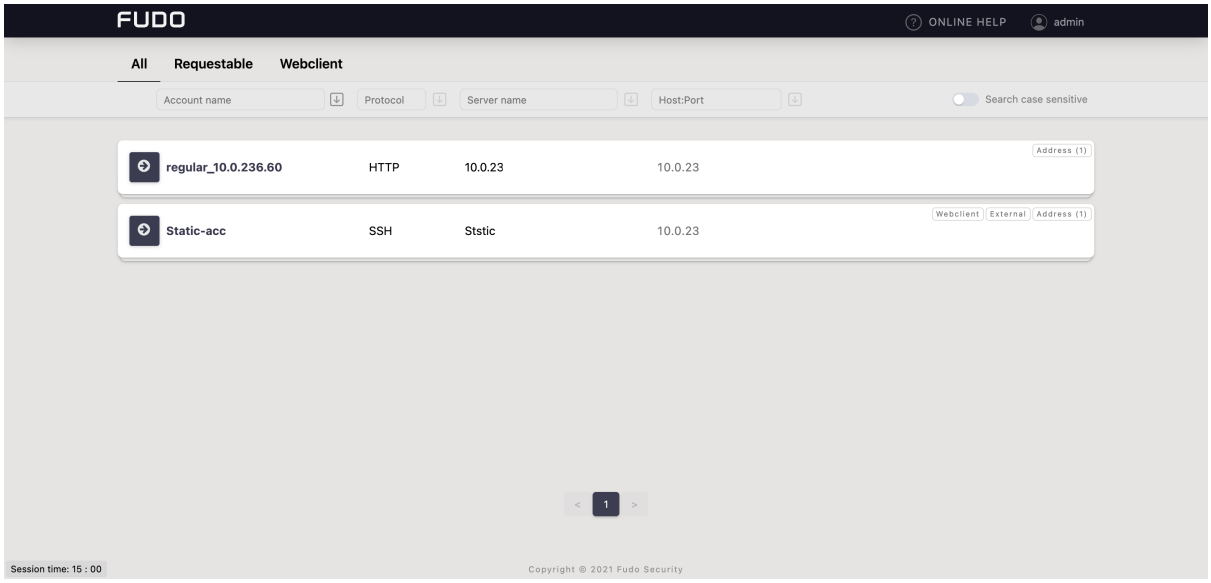
Note: Default login credentials:

login: admin
password: proxycrypto



4.4.2 User Access Gateway

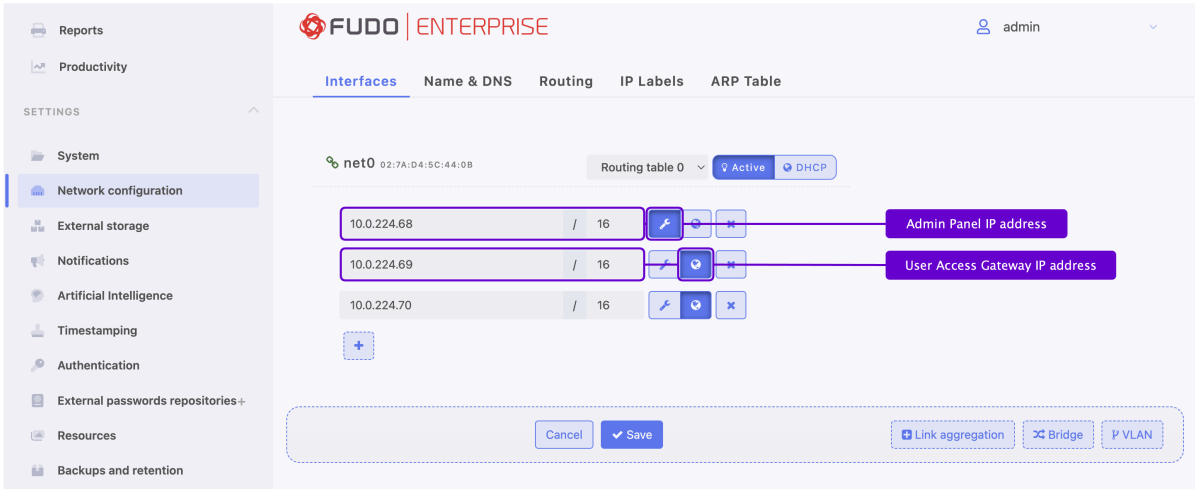
This component is designed for end users. It allows them to browse available resources and initiate connections with monitored servers using a selected listener. The User Access Gateway facilitates user access to resources in a secure and controlled manner.



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

Following web browsers are supported:

- Google Chrome, Mozilla Firefox, Internet Explorer for Microsoft Windows.
- Google Chrome, Mozilla Firefox for Ubuntu.
- Google Chrome, Mozilla Firefox, Safari for Mac OS X.

Related topics:

- *System overview*
- *Supported protocols*
- *Quick start*

CHAPTER 5

Quick start

5.1 SSH

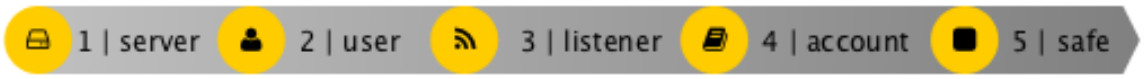
This chapter contains an example of a basic Fudo Enterprise configuration, to monitor SSH access to a remote server. In this scenario, the user connects to the remote server over the *SSH* protocol and logs in to the Fudo Enterprise using an individual login and password combination (`john_smith`/`john`). 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 *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 *Management* > *Users*.

2. Click *+ Add*.
3. Provide essential user information:

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	✗
Account validity	`Indefinite`
Settings Tab	
Safes	✗
Authentication section	
Authentication failures	✗
Enforce password complexity	✗
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	✗
AD Domain	✗
LDAP Base	✗
Full name	`John Smith`
Email	`john@smith.com`
Organization	✗
Phone	✗
Permissions Tab	
Granted users	✗

4. Click *Save*.

Adding a listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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`
Password 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:

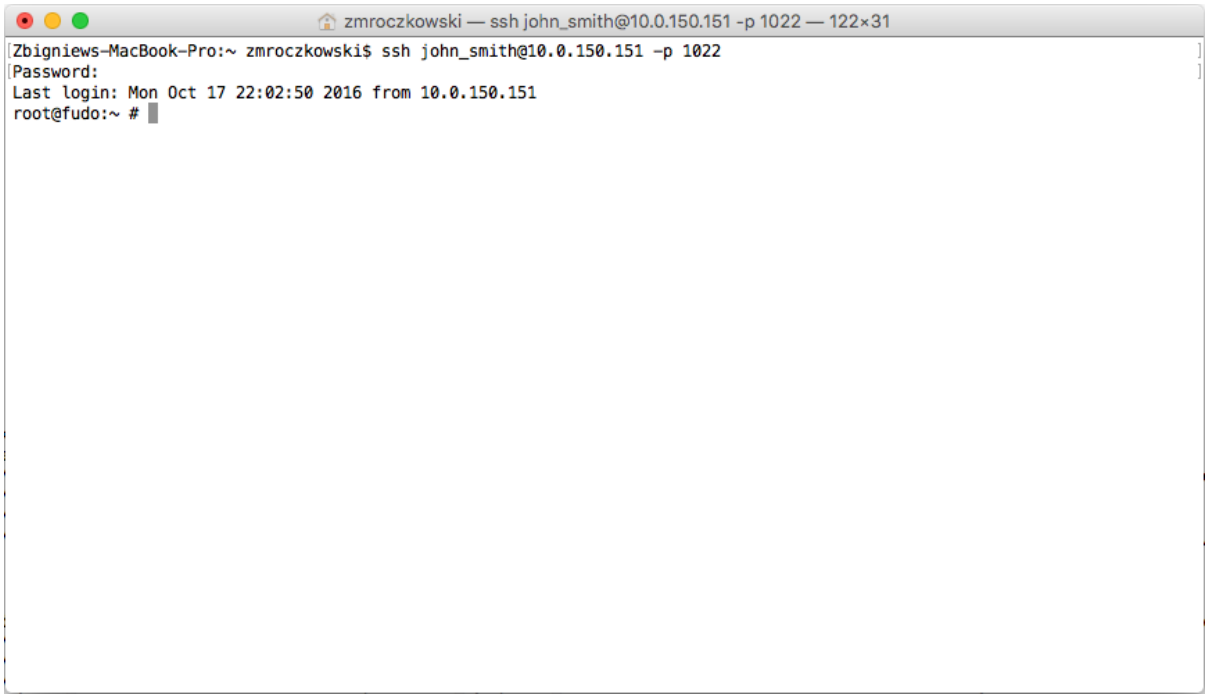
Parameter	Value
General	
Name	`ssh_safe`
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✓
VNC	✗

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:

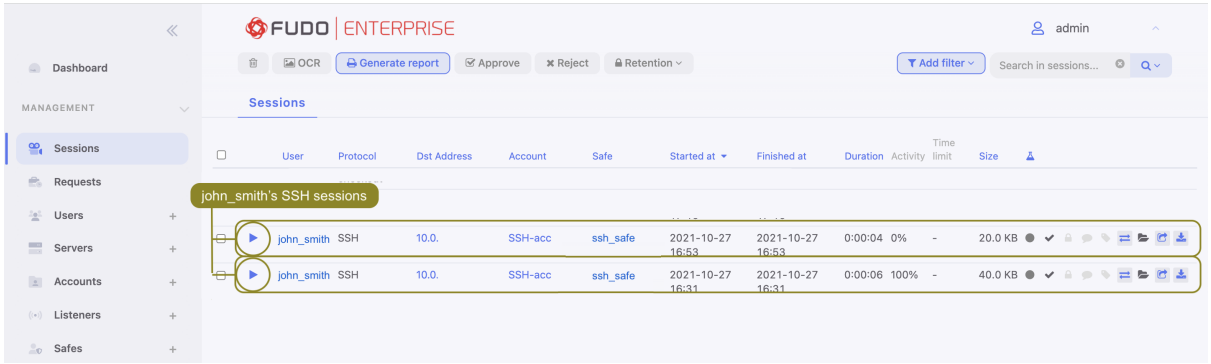


Note: Note that the *fingerprint* displayed when connecting to the target host for the first time is the same as was generated during server configuration.

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 *Management* > *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

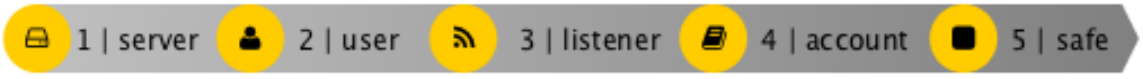
This chapter contains an example of a basic Fudo Enterprise configuration, to monitor SSH access in bastion mode. In this scenario, the user connects to the remote server over the *SSH* protocol and logs in to the Fudo Enterprise using an individual login and password combination (`john_smith`/`john`). 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 *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 *Management* > *Users*.
2. Click *+ Add*.
3. Provide essential user information:

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	
Account validity	`Indefinite`
Settings Tab	
Safes	
Authentication section	
Authentication failures	
Enforce password complexity	
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	
AD Domain	
LDAP Base	
Full name	`John Smith`
Email	`john@smith.com`
Organization	
Phone	
Permissions Tab	
Granted users	

4. Click *Save*.

Adding a Listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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`
Password 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:

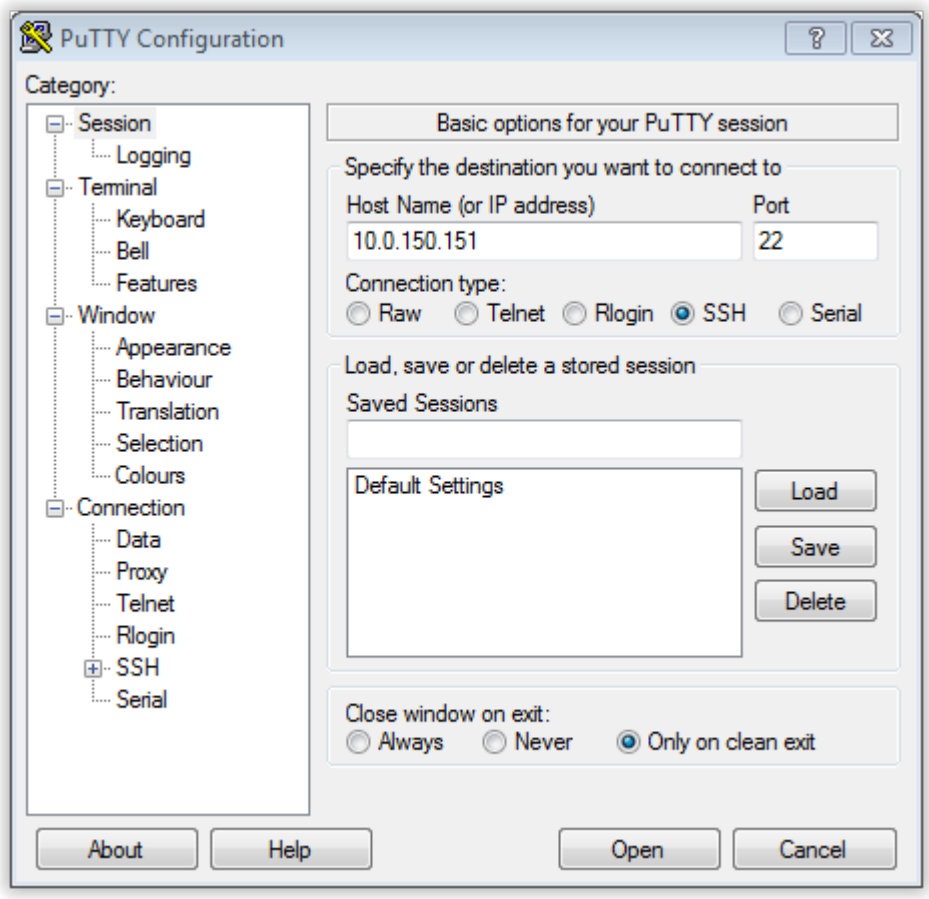
Parameter	Value
General	
Name	`ssh_safe`
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✓
VNC	✗

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*.

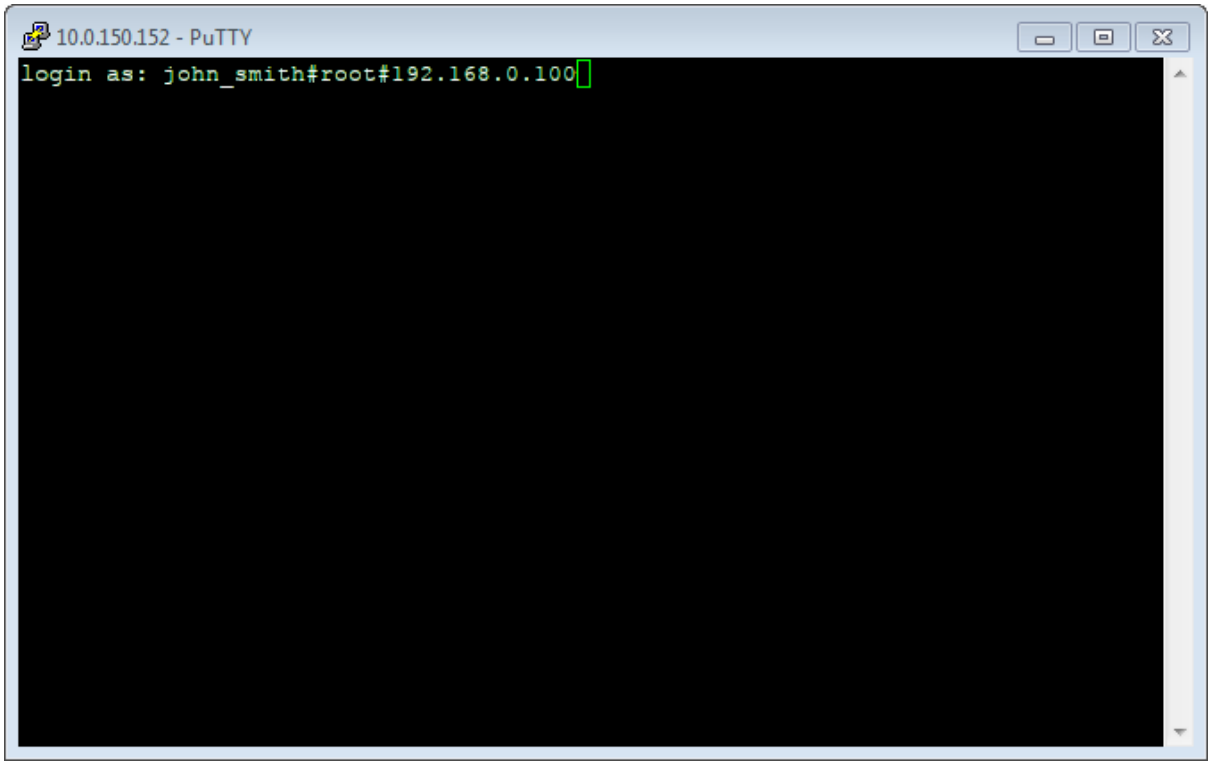
5.2.3 Establishing connection

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

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	
Account validity	`Indefinite`
Settings Tab	
Safes	
Authentication section	
Authentication failures	
Enforce password complexity	
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	
AD Domain	
LDAP Base	
Full name	`John Smith`
Email	`john@smith.com`
Organization	
Phone	
Permissions Tab	
Granted users	

4. Click *Save*.

Adding a Listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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 password changer (authentication modes are described in the *User authentication modes* section).

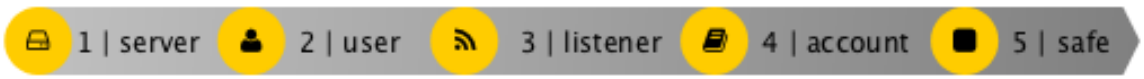


Note: Fudo Enterprise supports **multi-monitor sessions** for the RDP protocol, allowing monitoring and logging of graphical sessions across more than one display.

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

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	✗
Account validity	`Indefinite`
Settings Tab	
Safes	✗
Authentication section	
Authentication failures	✗
Enforce password complexity	✗
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	✗
AD Domain	✗
LDAP Base	✗
Full name	`John Smith`
Email	`john@smith.com`
Organization	✗
Phone	✗
Permissions Tab	
Granted users	✗

4. Click *Save*.

Adding a listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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`
Password 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:

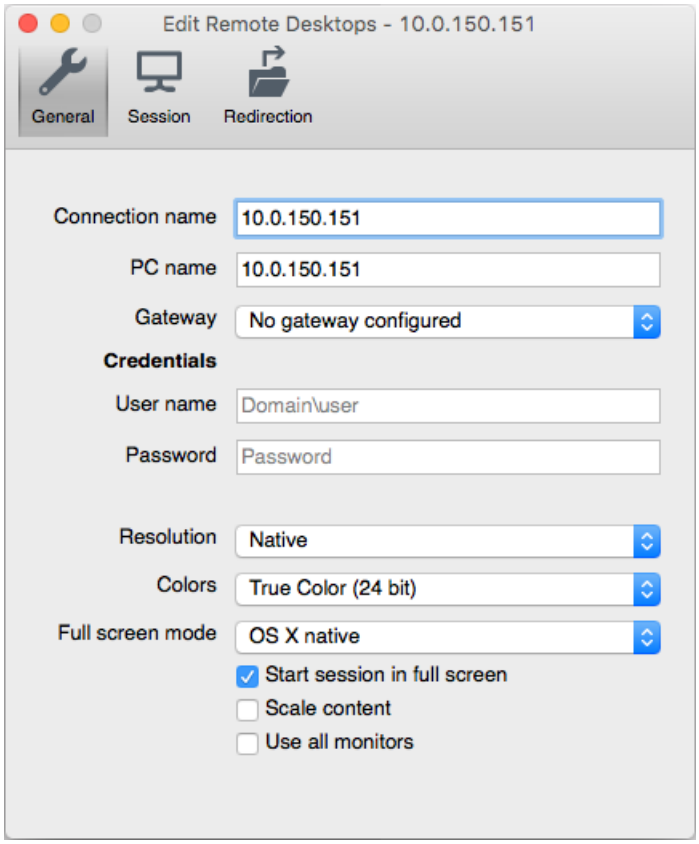
Parameter	Value
General	
Name	`rdp_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Requires approval	✗
Policies	✗
Note access	`No access`
Users	`john_smith`

Protocol functionality	
RDP	✓
SSH	✗
VNC	✗

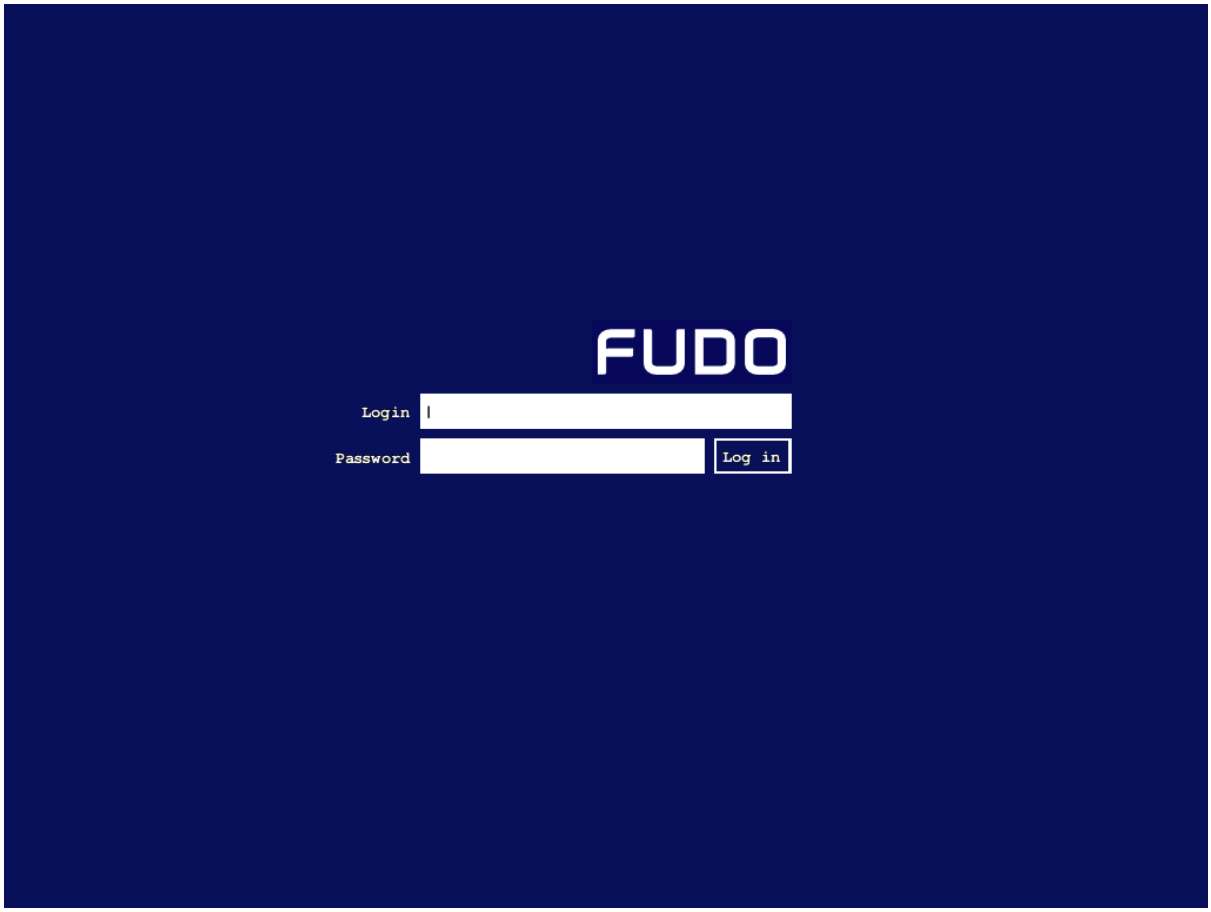
4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_rdp_server` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `rdp_listener` object and click +.
14. Click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

5.4.3 Establishing an RDP connection with a remote host

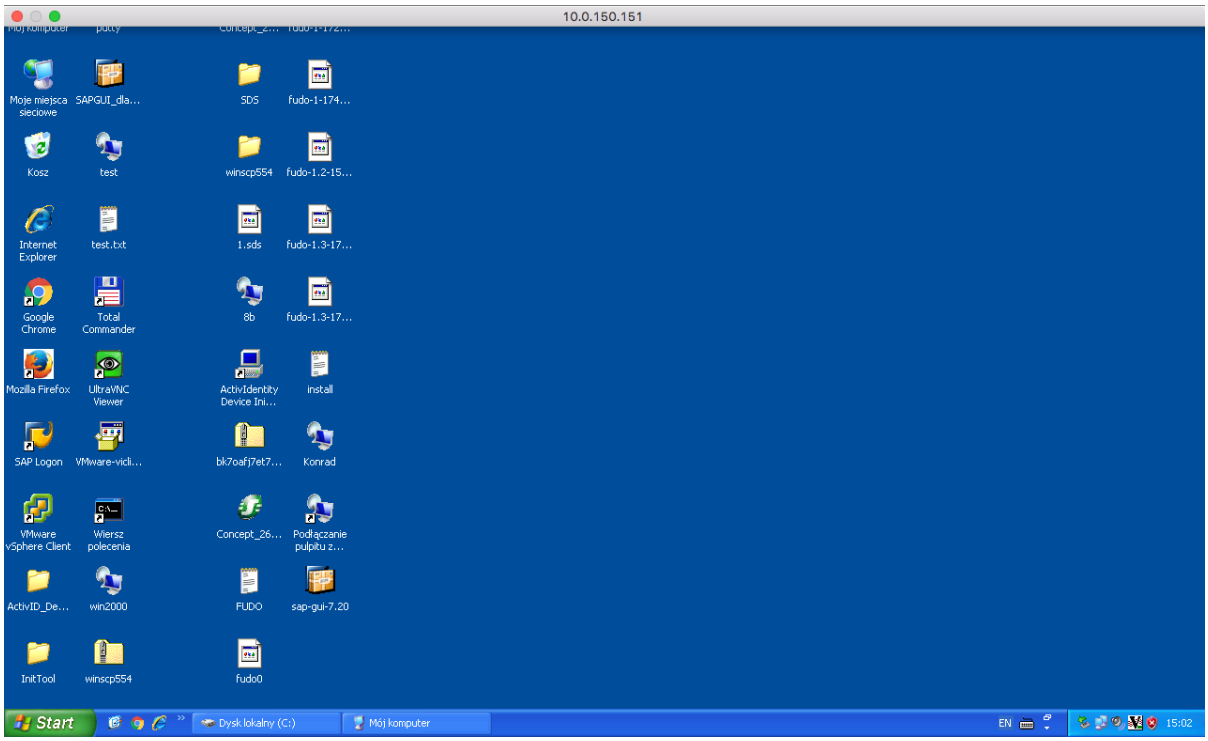
1. Launch RDP client of your choice.
2. Enter destination host IP address and RDP service port number.



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

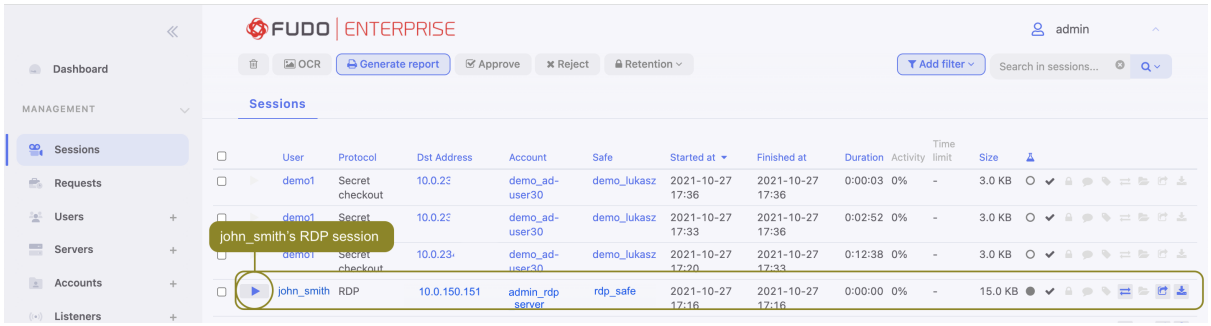


Note: Fudo Enterprise enables using custom login, no access and session termination screens for RDP and VNC connections. For more information on user defined images for graphical remote sessions, refer to the *Resources* topic.



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 *Management* > *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

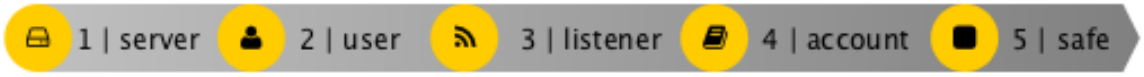
This chapter contains an example of a basic Fudo Enterprise configuration, to monitor RDP access to a remote server. In this scenario, the user connects to the remote server in bastion mode by specifying the user name along with account login on the target server and target server address in the login 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 *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 *Management* > *Users*.
2. Click *+ Add*.
3. Provide essential user information:

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	
Account validity	`Indefinite`
Settings Tab	
Safes	
Authentication section	
Authentication failures	
Enforce password complexity	
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	
AD Domain	
LDAP Base	
Full name	`John Smith`
Email	`john@smith.com`
Organization	
Phone	
Permissions Tab	
Granted users	

4. Click *Save*.

Adding a listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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`
Password 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:

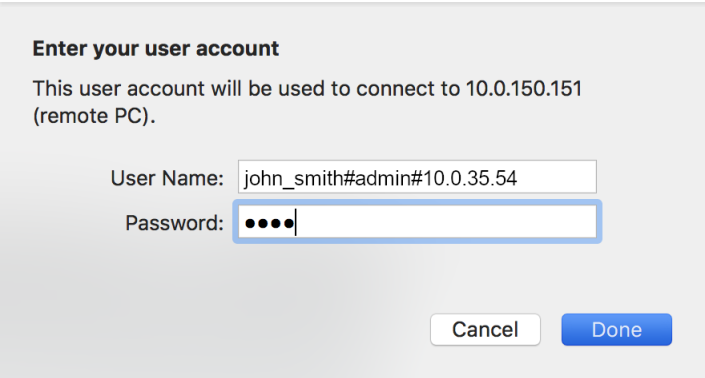
Parameter	Value
General	
Name	`rdp_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✓
SSH	✗
VNC	✗

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.

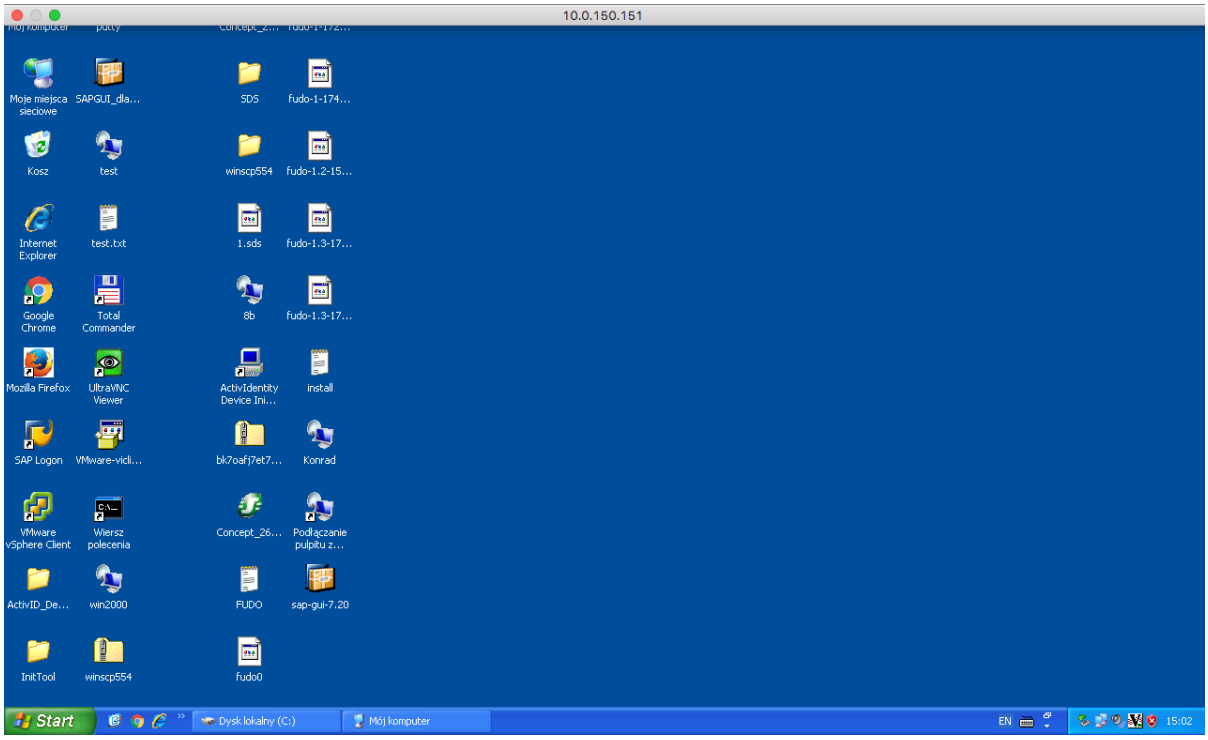
Note: When connecting using the forward account, where the user name and server login are identical, the server login field may be omitted (e.g., `john_smith##10.0.35.54`).



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.

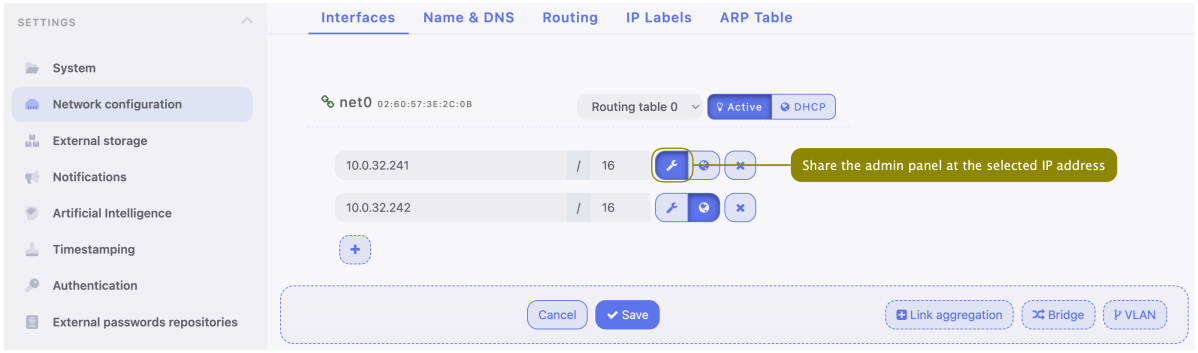




5.5.4 Viewing user session

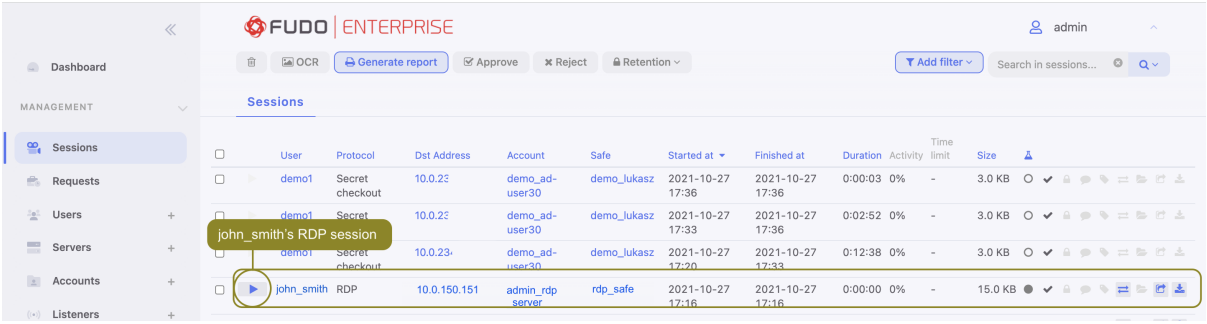
1. Open a web browser and enter the Fudo Enterprise administrator panel IP address.

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 *Management* > *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.

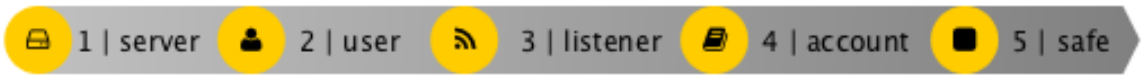
Note: Telnet connections do not support login credentials forwarding and login credentials substitution. When connecting to target host over telnet protocol, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise and then again, to connect to the 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 *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 *Management* > *Users*.
2. Click *+ Add*.

3. Provide essential user information:

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	✗
Account validity	`Indefinite`
Settings Tab	
Safes	✗
Authentication section	
Authentication failures	✗
Enforce password complexity	✗
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	✗
AD Domain	✗
LDAP Base	✗
Full name	`John Smith`
Email	`john@smith.com`
Organization	✗
Phone	✗
Permissions Tab	
Granted users	✗

4. Click *Save*.

Adding a listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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:
```

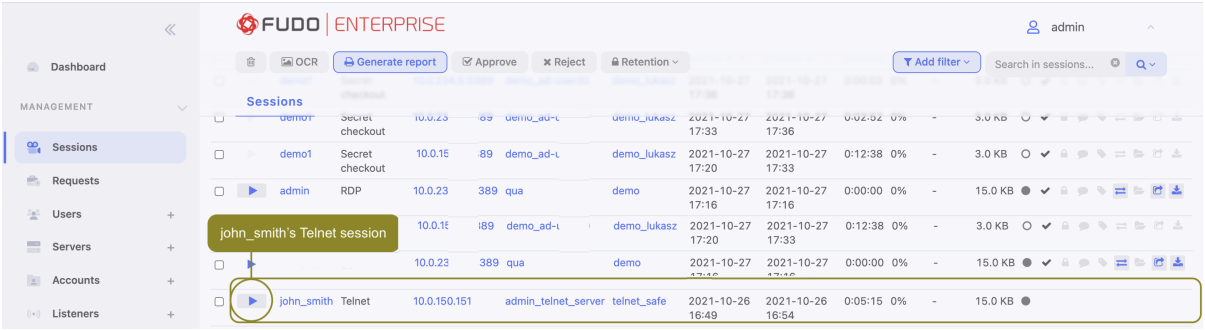
4. Provide user authentication information defined on the target host:

```
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 *Management* > *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.

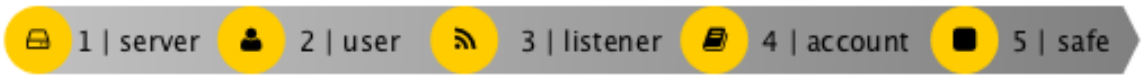
Note: Telnet connections do not support login credentials forwarding and login credentials substitution. When connecting to target host over telnet protocol, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise and then again, to connect to the 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 *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 *Management* > *Users*.
2. Click + *Add*.
3. Provide essential user information:

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	
Account validity	`Indefinite`
Settings Tab	
Safes	
Authentication section	
Authentication failures	
Enforce password complexity	
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	
AD Domain	
LDAP Base	
Full name	`John Smith`
Email	`john@smith.com`
Organization	
Phone	
Permissions Tab	
Granted users	

4. Click *Save*.

Adding a listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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	✗

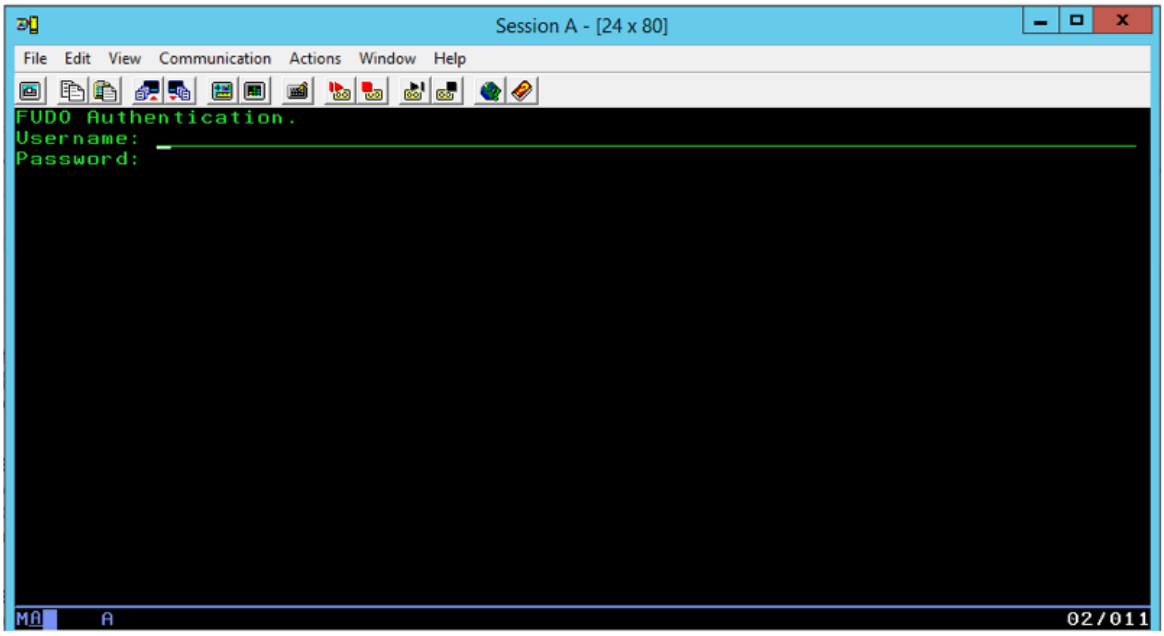
4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_telnet_server` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `telnet_listener` object and click +.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

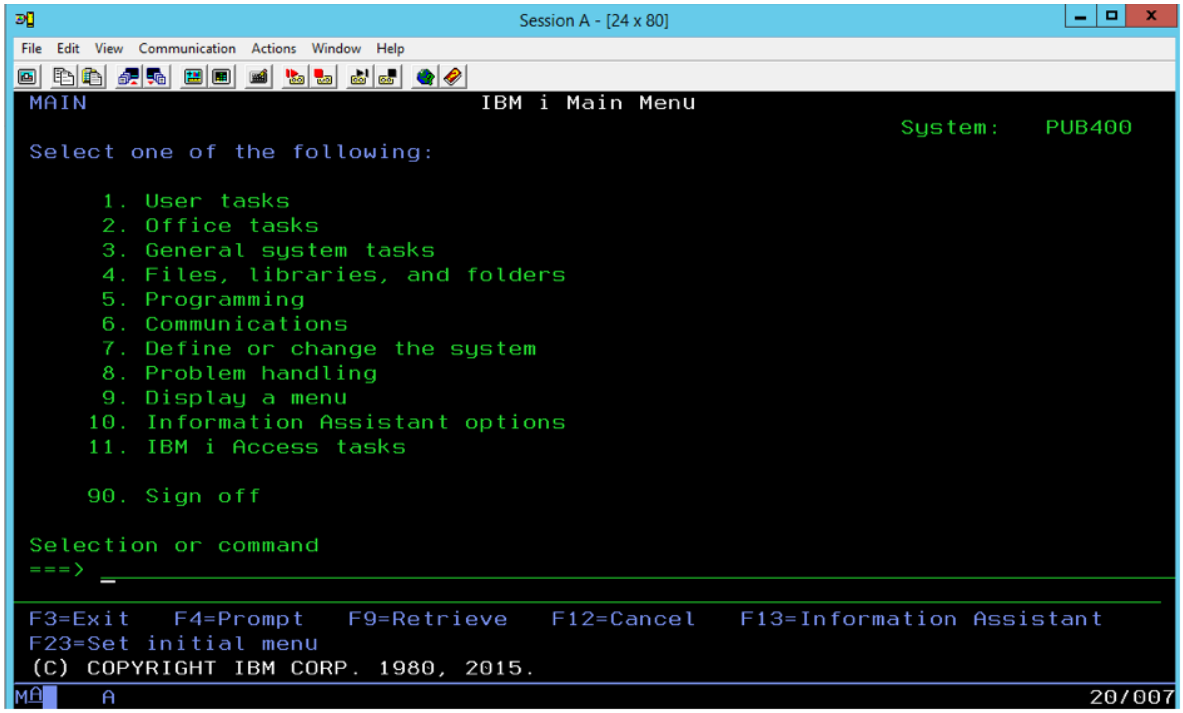
3. Provide user authentication information defined on Fudo Enterprise:



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

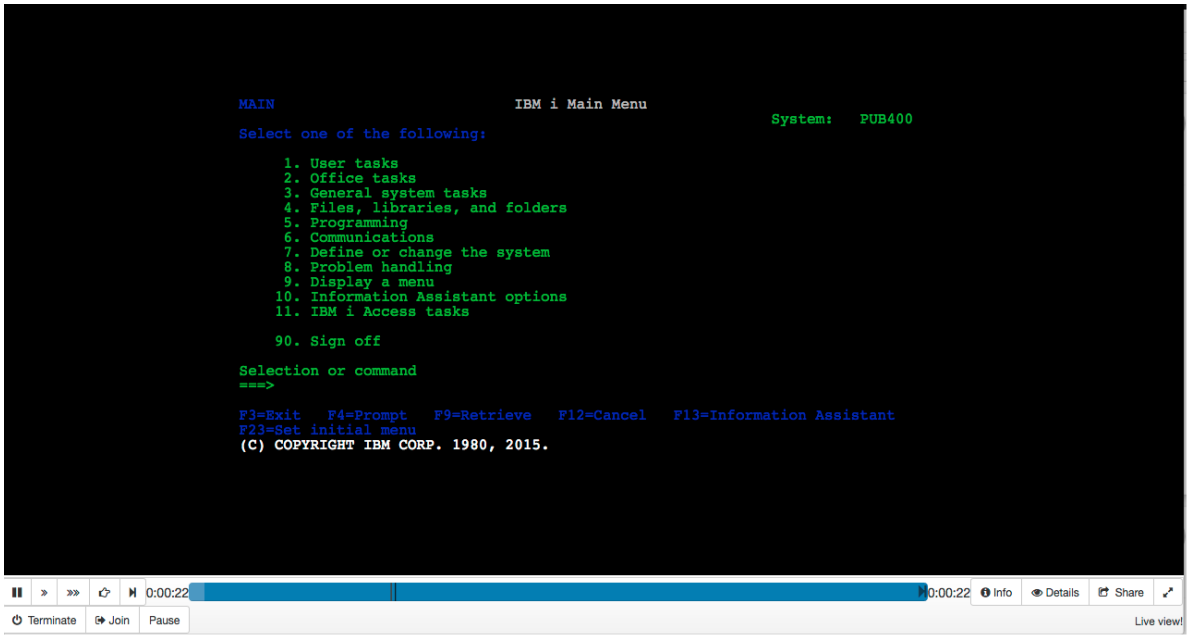
   FreeBSD/amd64 (fbsd83-cerb.whl) (pts/0) login: password:

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 *Management* > *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 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).

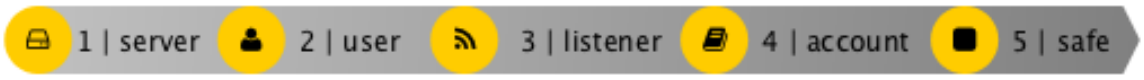


Warning: Note that the MySQL server `caching_sha2_password` plugin isn't supported by Fudo Enterprise. Supportable MySQL plugins by Fudo Enterprise are `mysql_native_password` and `mysql_old_password`. Server plugin should be set to `mysql_native_password` in `/etc/mysql/mysql.conf.d/mysqld.cnf` and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

5.8.1 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.

5.8.2 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 *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 *Management* > *Users*.
2. Click *+ Add*.
3. Provide essential user information:

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	
Account validity	`Indefinite`
Settings Tab	
Safes	
Authentication section	
Authentication failures	
Enforce password complexity	
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	
AD Domain	
LDAP Base	
Full name	`John Smith`
Email	`john@smith.com`
Organization	
Phone	
Permissions Tab	
Granted users	

4. Click *Save*.

Adding a listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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`
Password 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.

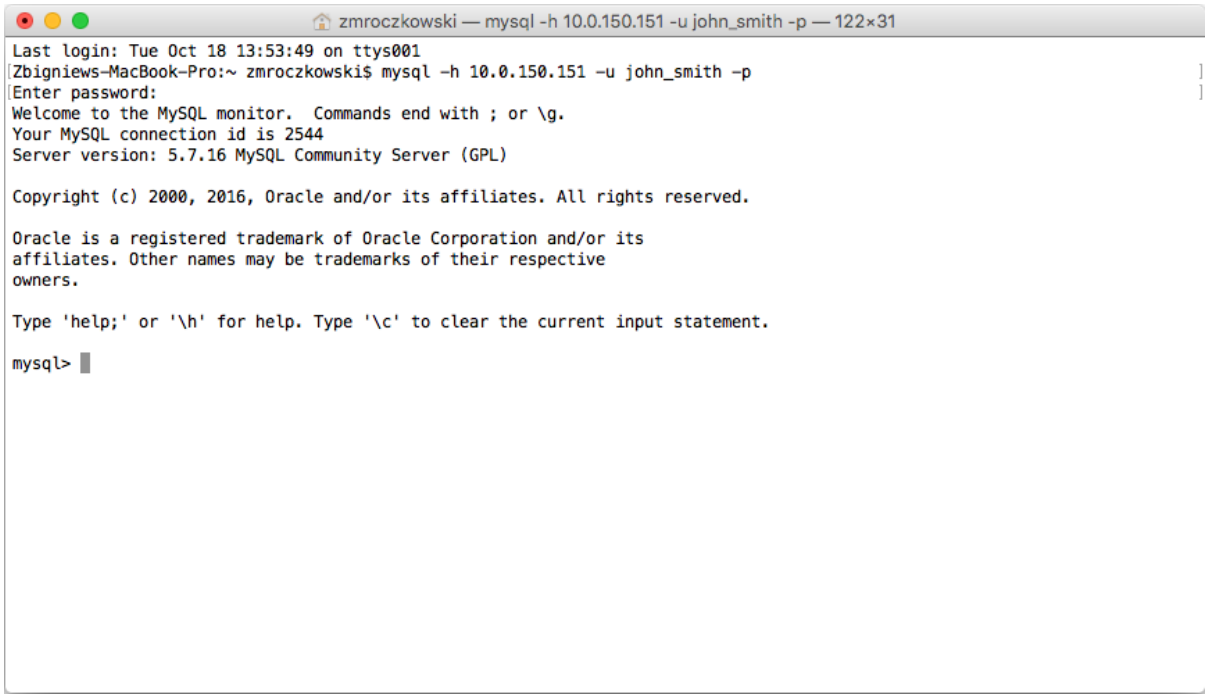
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

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*.

5.8.3 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.

5.8.4 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 *Management* > *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*

5.9 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.

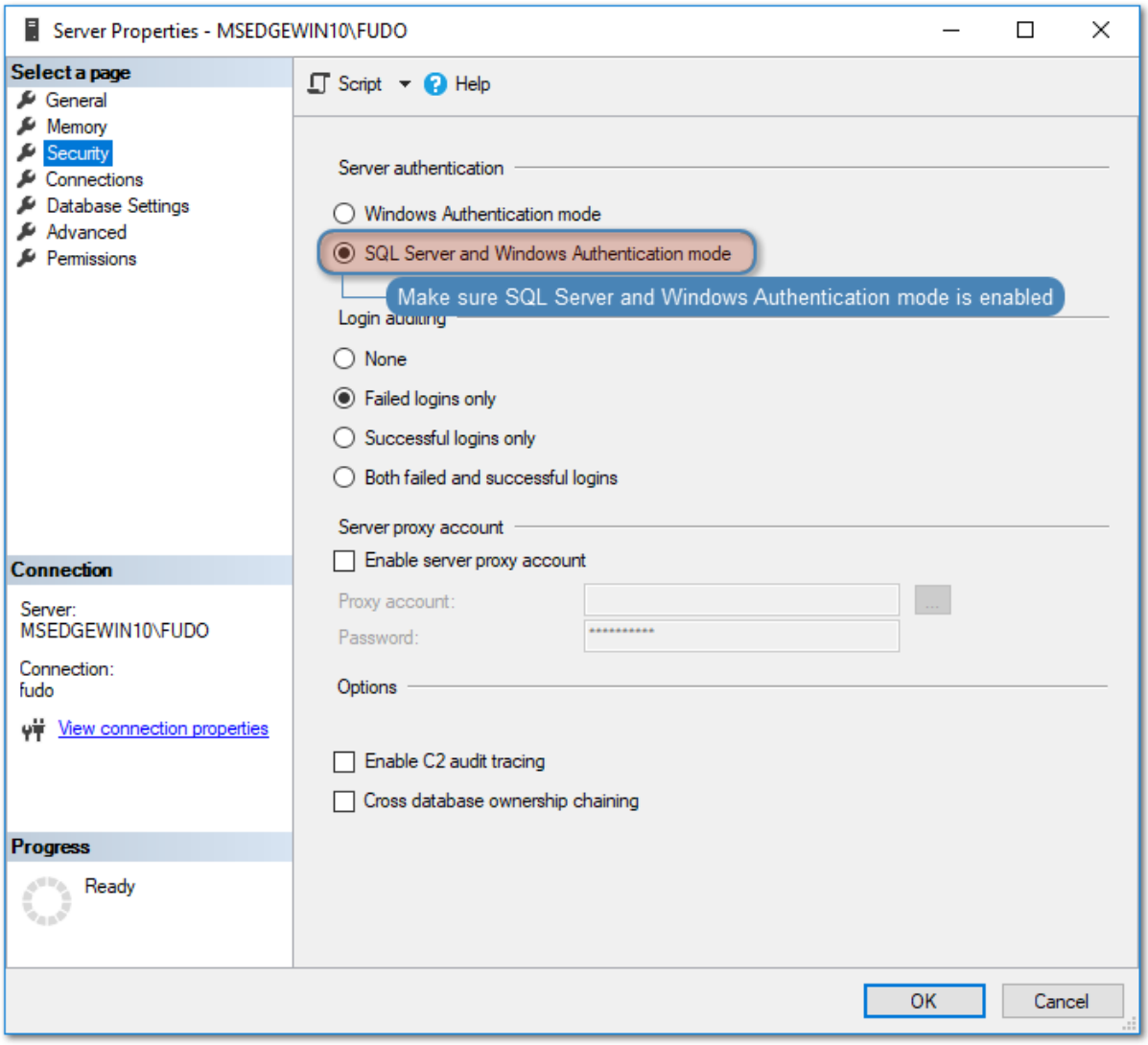
In this scenario, the user connects to a MS SQL database using individual login and password using *SQL Server Management Studio*. When establishing the connection with the remote server, Fudo Enterprise substitutes the login and the password with the previously defined values: `fudo`/`password` (authorization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



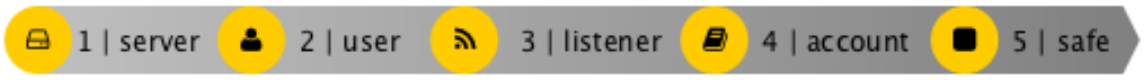
5.9.1 Prerequisites

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

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



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

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	
Account validity	`Indefinite`
Settings Tab	
Safes	
Authentication section	
Authentication failures	
Enforce password complexity	
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	
AD Domain	
LDAP Base	
Full name	`John Smith`
Email	`john@smith.com`
Organization	
Phone	
Permissions Tab	
Granted users	

4. Click *Save*.

Adding a listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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`
Password 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:

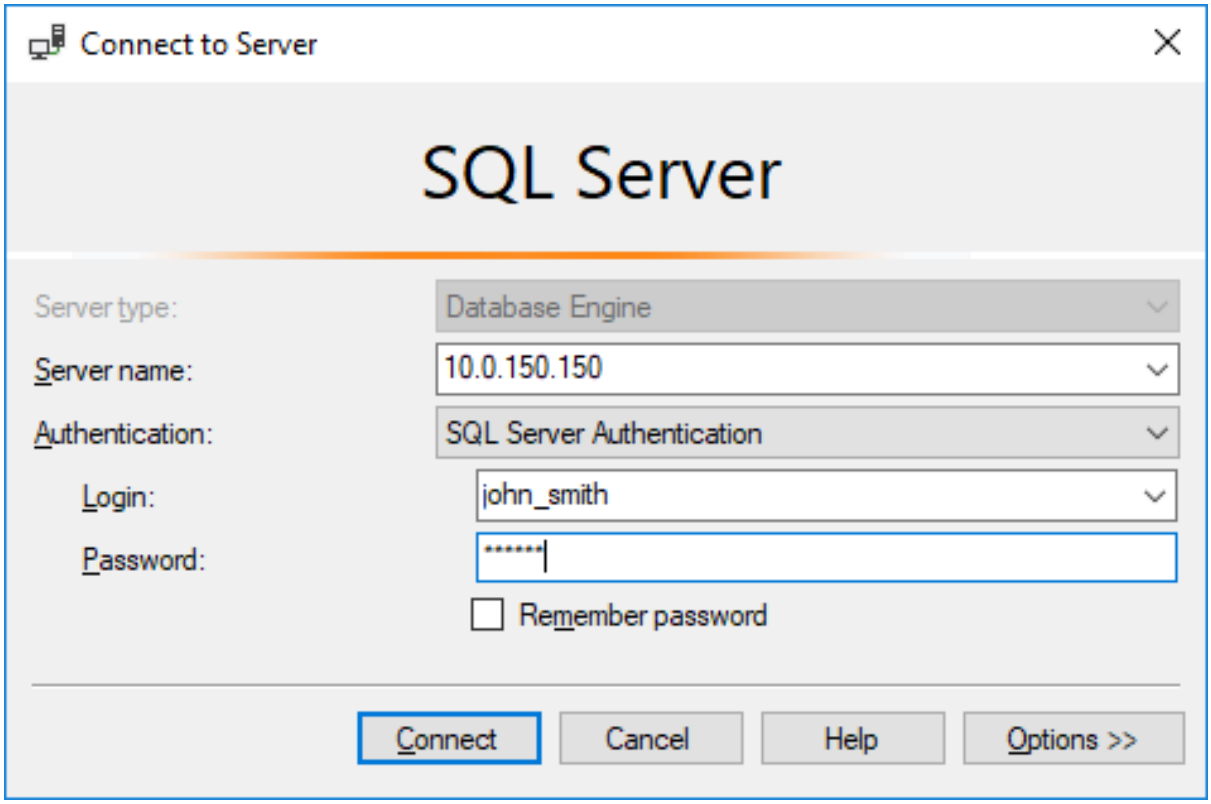
Parameter	Value
General	
Name	`mssql_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`

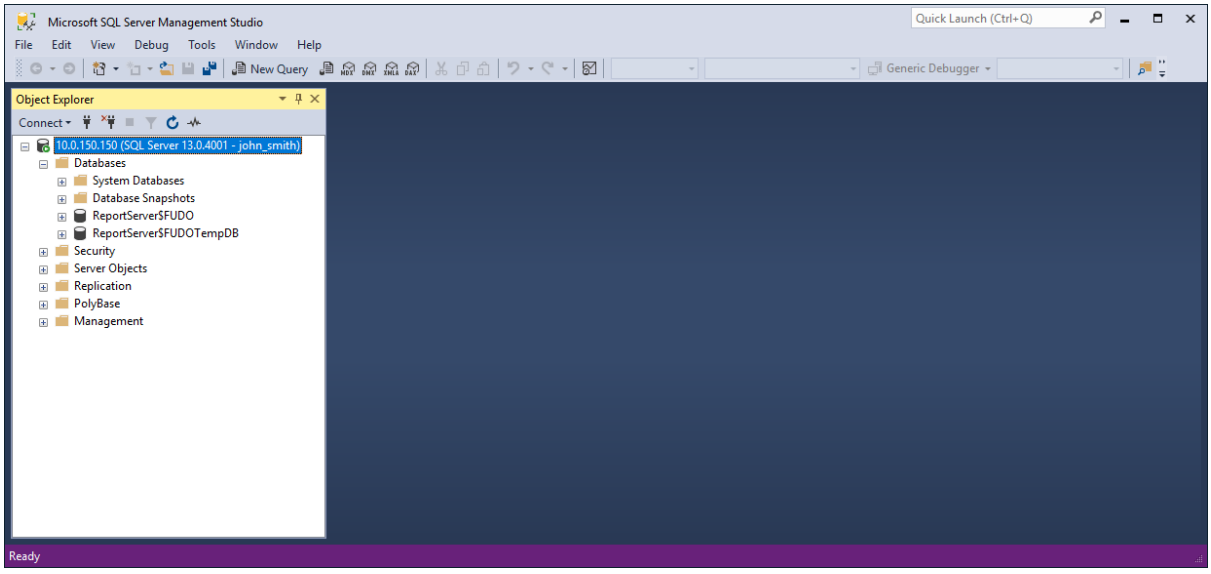
Protocol functionality	
RDP	✗
SSH	✗
VNC	✗

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*.

5.9.3 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*.





5.9.4 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 *Management* > *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*

5.10 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.

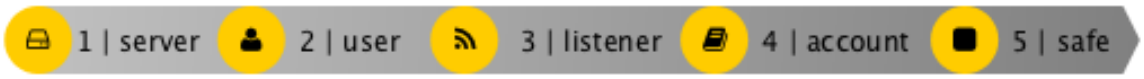
Model	Maximum recommended number of concurrent HTTP sessions*
F100x	2
F300x	5
F500x	10

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

5.10.1 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.

5.10.2 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 *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 *Management* > *Users*.
2. Click *+ Add*.
3. Provide essential user information:

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	
Account validity	`Indefinite`
Settings Tab	
Safes	
Authentication section	
Authentication failures	
Enforce password complexity	
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	
AD Domain	
LDAP Base	
Full name	`John Smith`
Email	`john@smith.com`
Organization	
Phone	
Permissions Tab	
Granted users	

4. Click *Save*.

Adding a listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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	`******`
Password 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`

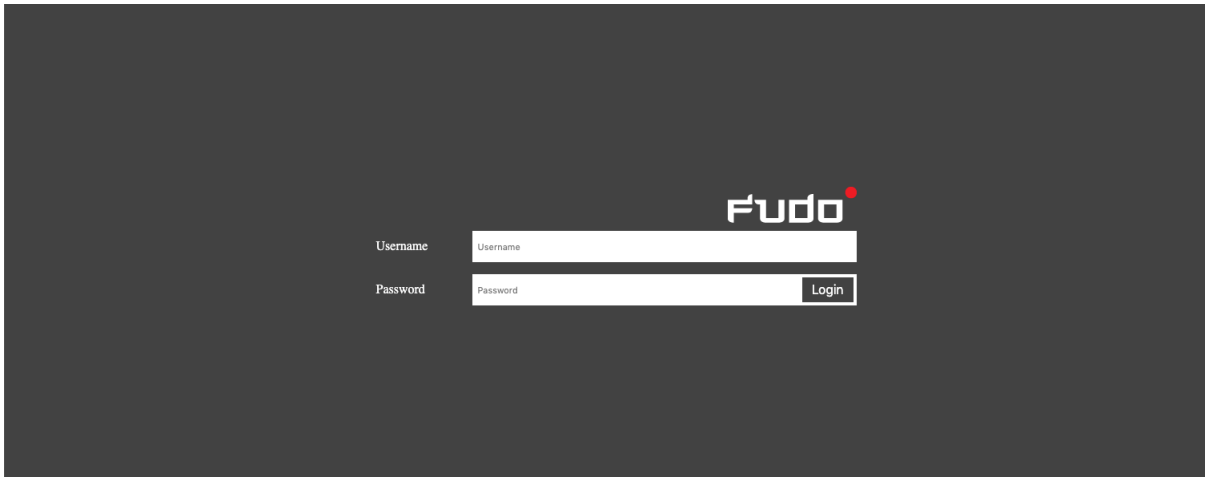
Protocol functionality	
RDP	✗
SSH	✗
VNC	✗

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*.

5.10.3 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.

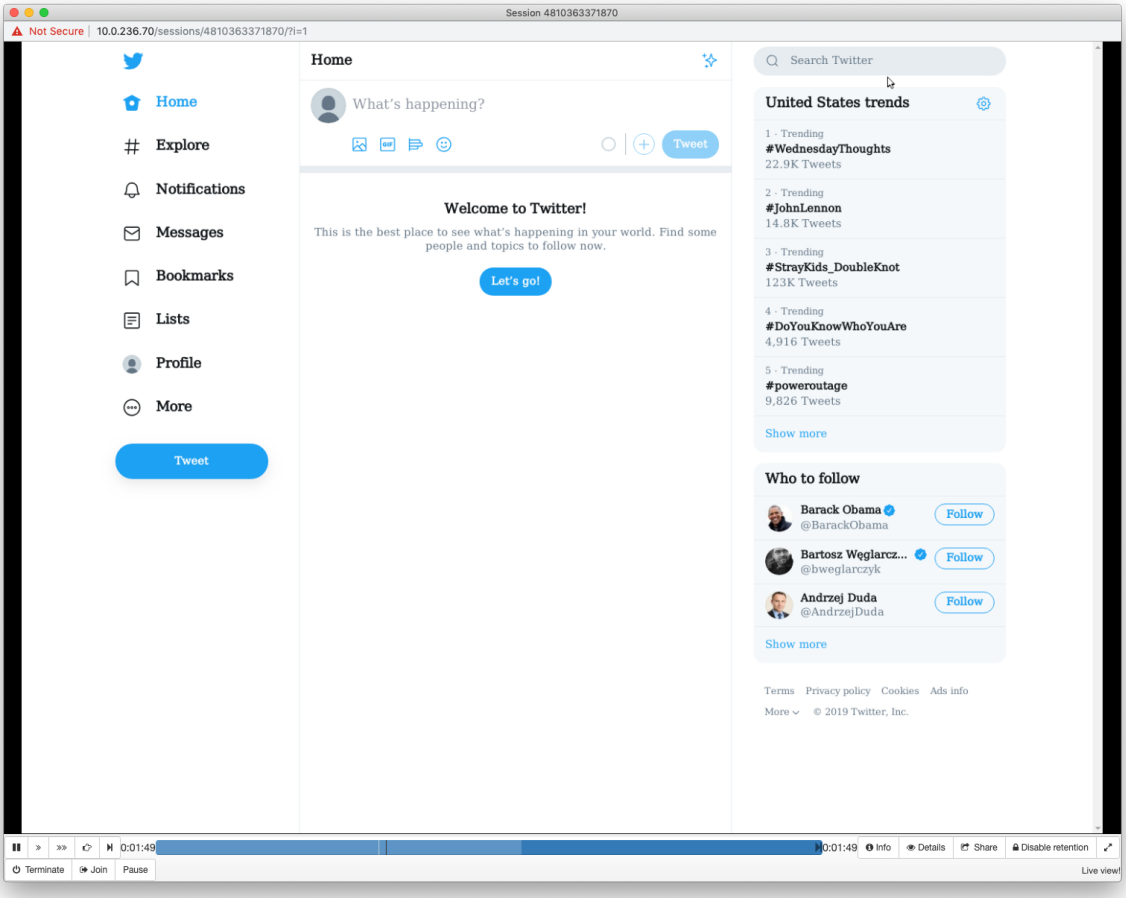
Note: In case you are authenticating using two factors, input your static password along with the dynamic factor (token value) in the password field as a single string of characters.



4. Continue browsing the website.

5.10.4 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 *Management* > *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*

5.11 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).

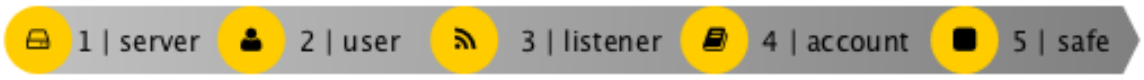
Note: Due to specifics of VNC protocol, which authenticates the user using password only, the substitution login string entered in account properties is ignored when establishing a VNC connection.



5.11.1 Prerequisites

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

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

Parameter	Value
General	
Name	`john_smith`
Role	`user`
Blocked	
Account validity	`Indefinite`
Settings Tab	
Safes	
Authentication section	
Authentication failures	
Enforce password complexity	
Add authentication method:	`Static password`
Password	`john`
User Data Tab	
Fudo domain	
AD Domain	
LDAP Base	
Full name	`John Smith`
Email	`john@smith.com`
Organization	
Phone	
Permissions Tab	
Granted users	

4. Click *Save*.

Adding a listener

Listener determines server connection mode (proxy, gateway, transparent, 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); password changing policy as well as the password 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`
Password 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.

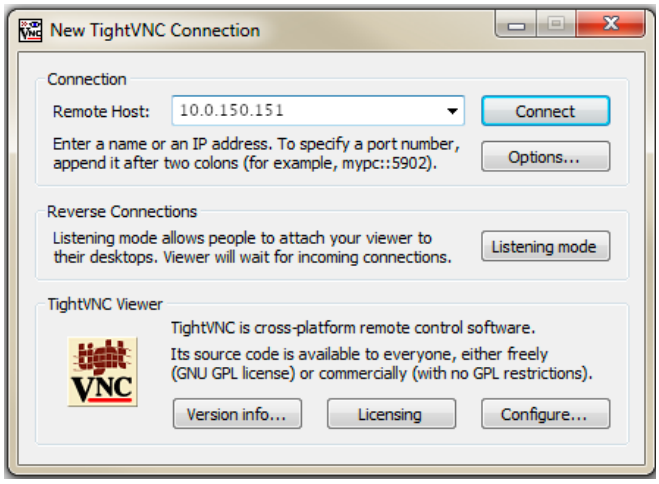
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

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*.

5.11.3 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.

5.11.4 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 *Management* > *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*

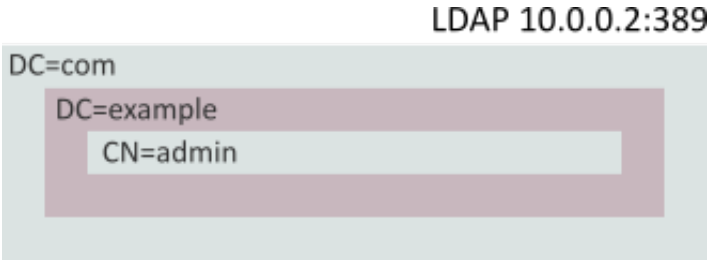
5.12 User authentication against external LDAP server

This chapter contains an example of configuring user authentication against external LDAP service.

5.12.1 Prerequisites

The following description assumes that the `admin` 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 `cn=admin,dc=example,dc=com`.



5.12.2 Configuration

Adding external authentication source

1. Select *Settings* > *External authentication*.
2. Click + *Add external authentication source*.
3. Provide essential configuration parameters:

Parameter	Value
Type	`LDAP`
Host	`10.0.0.2`
Port	389
Bind to	10.0.0.10
Bind DN	`dc=example,dc=com`
	Note: Alternatively, define the path to where users definitions are stored `cn=##username##,dc=example,dc=com` and leave the *LDAP base* parameter in the user configuration empty
Encrypted connection	✗
Delete	✗



4. Click *Save*.

Adding user authentication method

1. Select *Management* > *Users*.
2. Find and click the `admin` user definition.
3. On the *User Data* Tab, in the *LDAP base* field specify the location of *admin* object in the directory structure `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. Select *External authentication* type of authentication method from the *Add authentication method* drop-down list.
5. Choose method "`LDAP 10.0.0.2:389 bind dn:dc=example,dc=com`" and click *Save*.
6. Click *Save* to save user definition.

Related topics:

- *Authentication*
- *Creating a user*
- *Quick start - SSH connections monitoring*

CHAPTER 6

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.

6.1 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.

6.1.1 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.

6.1.2 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 password 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 password 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 password 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*
-

6.2 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.

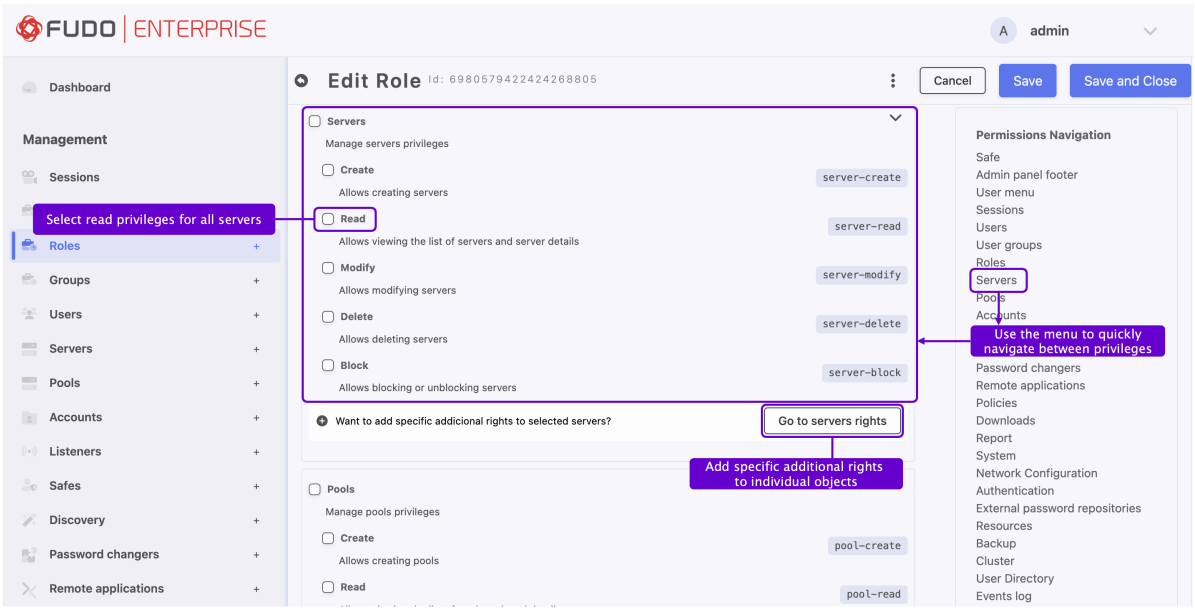
1. Click + icon in the main menu next to the *Roles* tab, or select *Management* > *Roles* and then click + *Add Role*.
2. Enter a unique name for the new object.
3. If needed, select the *Description* option to add a summary of the role.

GLOBAL PRIVILEGES TAB

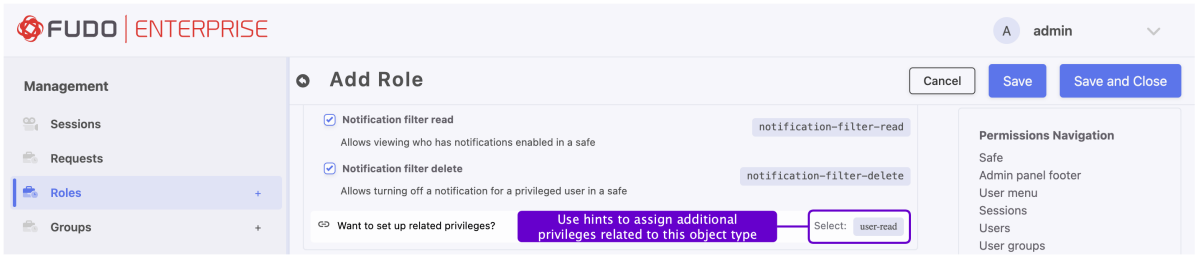
4. Go to the **GLOBAL PRIVILEGES** tab and select all privileges you want to assign to the created role.

Note: By selecting all privileges, you will grant this role all existing privileges, similar to the *superadmin* 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.

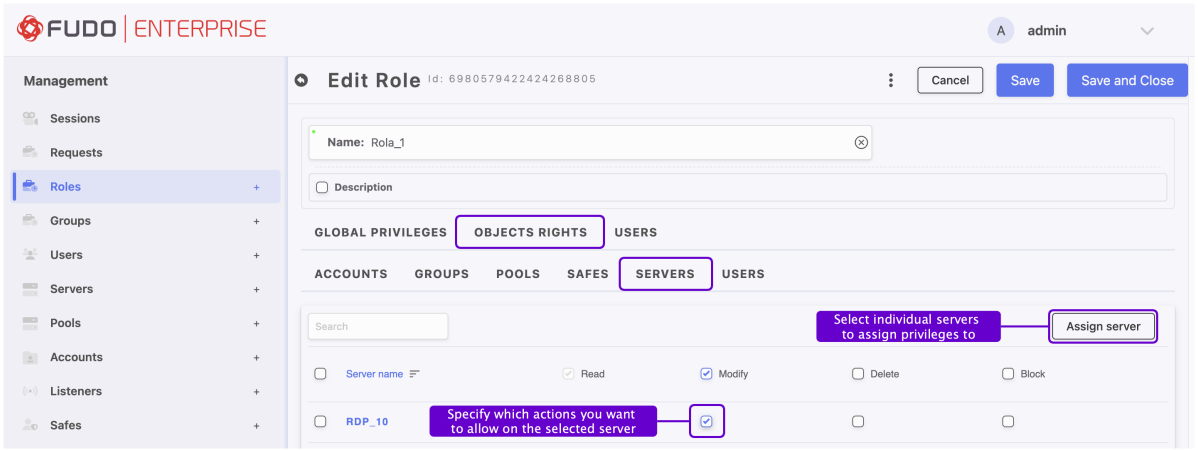


7. Click *Save* to create the role and proceed with further configuration.
8. To add specific additional rights to individual objects, use the *Go to...* button or navigate to the **OBJECT RIGHTS** tab.

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*).



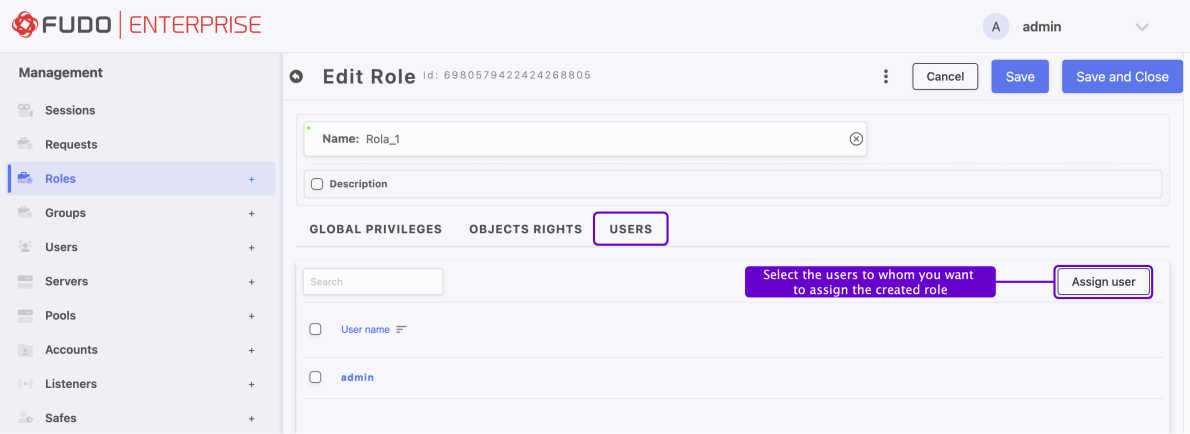
14. After completing the above steps, you will create a role with privileges to view all server configurations and modify only the servers selected in the OBJECT RIGHTS tab.

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:

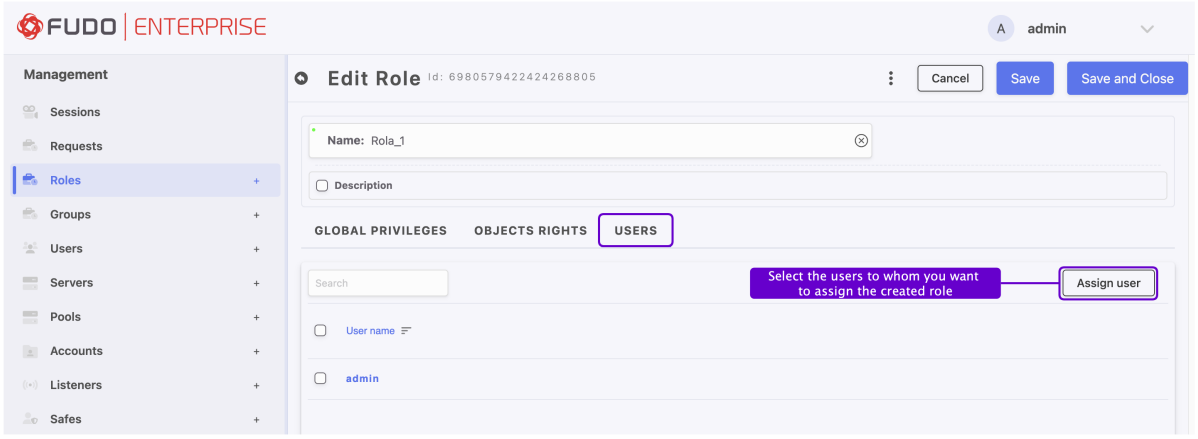
- *Typical Role Scenarios and Required Privileges*
- *Groups (RBAC)*
- *Users*

6.3 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

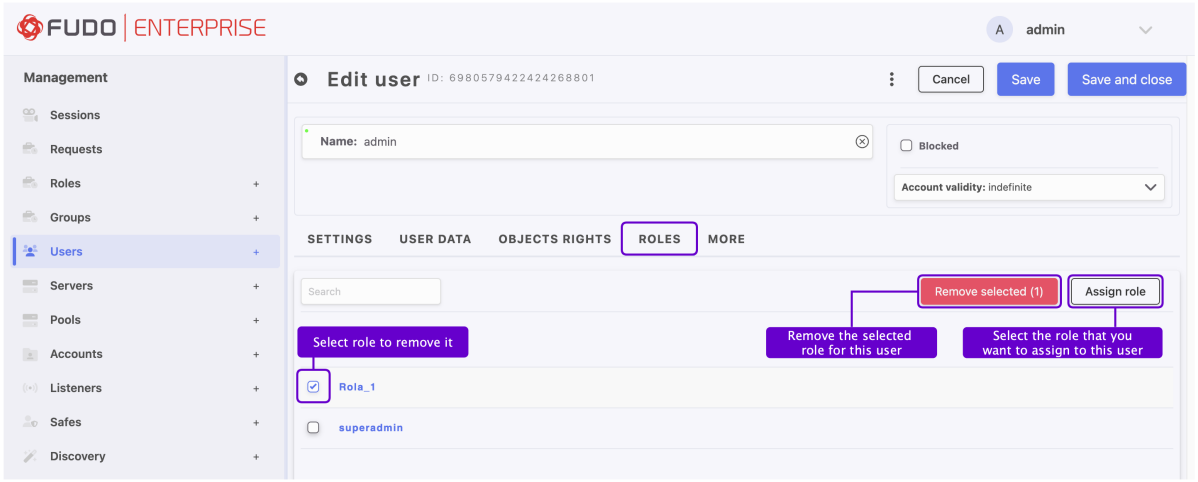
1. Select *Management* > *Roles*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.
3. Find and click desired role's name to edit it.
4. Navigate to the **USERS** tab.
5. Click *Assign user*.
6. Select the users to whom you want to assign the created role.



7. Click *Save*.

Assigning Role from the User Editing View

1. Select *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.

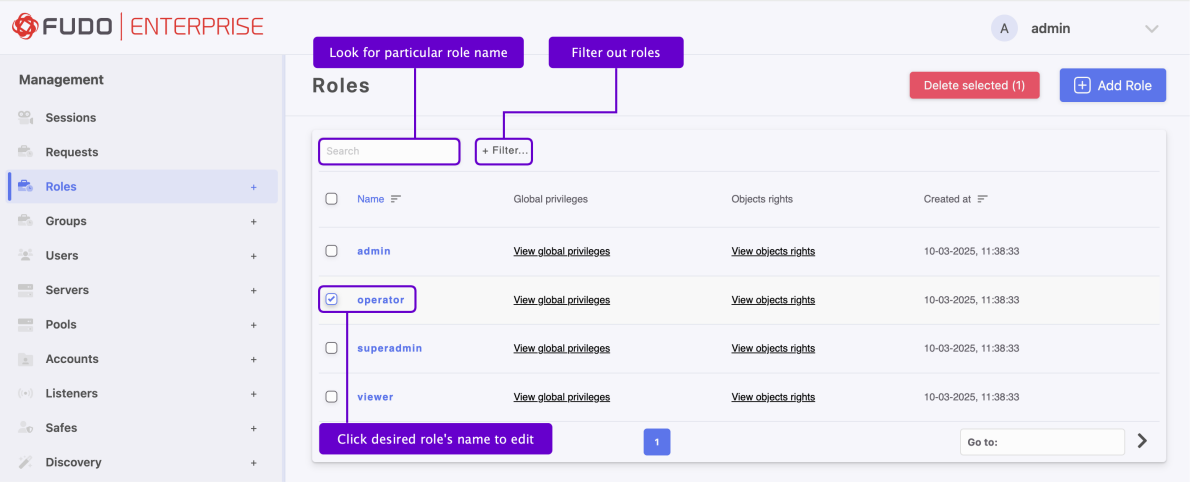


Related topics:

- *Role-Based Access Control (RBAC)*
- *Groups (RBAC)*
- *Users*

6.4 Modifying Roles

1. Select *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.



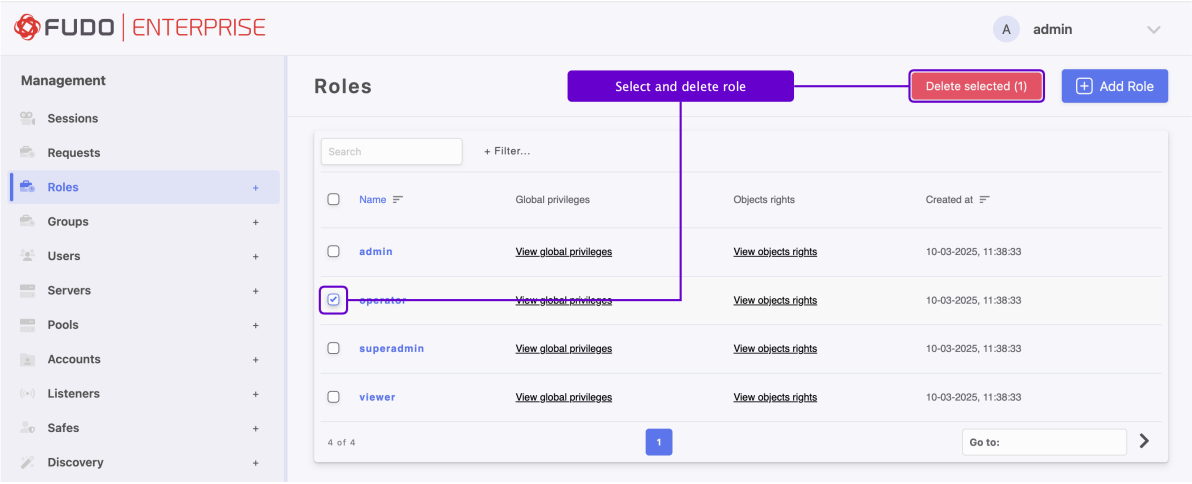
5. Click *Save and Close* to save changes to this configuration.

Related topics:

- *Role-Based Access Control (RBAC)*
- *Groups (RBAC)*
- *Users*

6.5 Deleting Roles

1. Select *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*

6.6 Typical Role Scenarios and Required Privileges

6.6.1 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: Password Changers Tab

Subsection	Action	Privileges	Capabilities
Password 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

Table 19: Privilege/Capability Matrix: System Tab

Subsection	Action	Privileges	Capabilities
General > Date Time			
	visible	`datetime-read`	None
	configure	`datetime-modify`	None
General > NTP			
	visible	`ntp-read`	None
	configure	`ntp-modify`	None

Continued on next page

Table 19 – continued from previous page

Subsection	Action	Privileges	Capabilities
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 > Maintenance Supervision > Deny New Connections			
	visible	`maintenance-read`	None
	configure	`deny-new-connections`	None
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

Continued on next page

Table 19 – continued from previous page

Subsection	Action	Privileges	Capabilities
General > Timestamping			
	visible	`timestamp-read`	None
	configure	`timestamp-modify`	None
General > Changers			
	visible	`password-changer-node-read`	None
	configure	`password-changer-node-modify`	None
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
	snapshot-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
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
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_create	`cluster-modify`	None
	cluster_join	`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

6.6.2 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-read`	Allows viewing the list of accounts and account details	Account Alerts
`user-read`	Allows viewing the users list and user details	Active Users
`session-read`	Allows viewing the list of sessions and session details	Suspicious Sessions, New Sessions, Concurrent Sessions
`configuration-read`	Allows previewing the Configuration tab	License
`log-read`	Allows viewing the events log	Logs
`cluster-read`	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.

6.6.3 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).

6.6.3.1 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)

6.6.3.2 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.

6.6.3.3 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.

6.6.4 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.

6.6.5 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`

6.6.6 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`

6.6.7 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. - **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.

6.6.8 Fudo Officer

To pair or unpair the Fudo Officer mobile app with an account, the user needs access to the Admin Panel and the `modify` capability for their own 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`

6.6.9 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.

Related topics:

- *Groups (RBAC)*
- *Users*

CHAPTER 7

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.

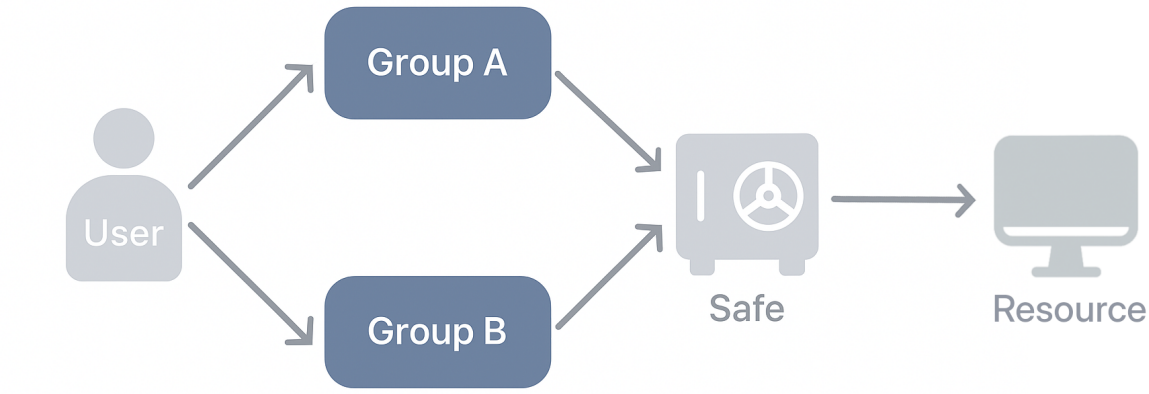
Groups support integration with external systems that use the Role-Based Access Control (RBAC) model. This enables you to map specific roles from external directories, such as Active Directory, to Fudo Enterprise groups and assign specific roles. Users automatically inherit permissions and resource access 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.

7.1 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.

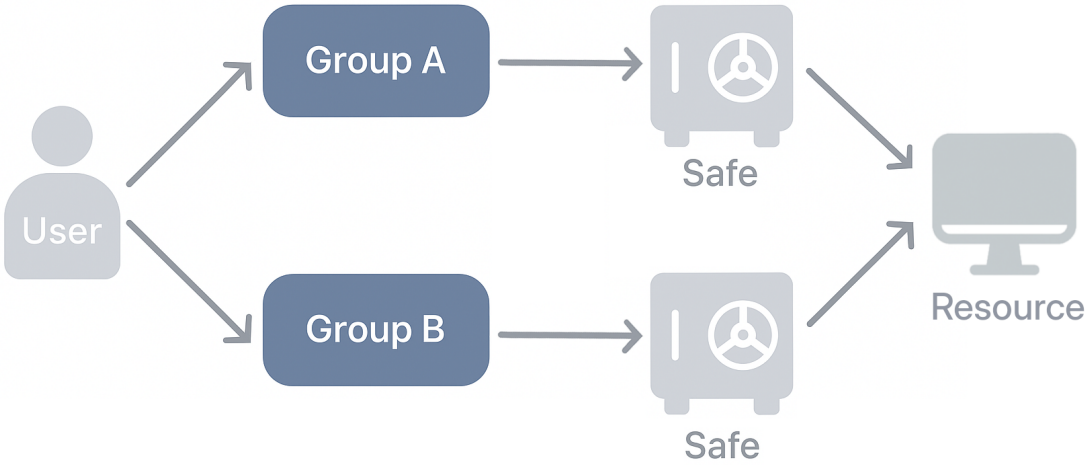
User Belongs to Multiple Groups Assigned to the Same Safe and Resource



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.

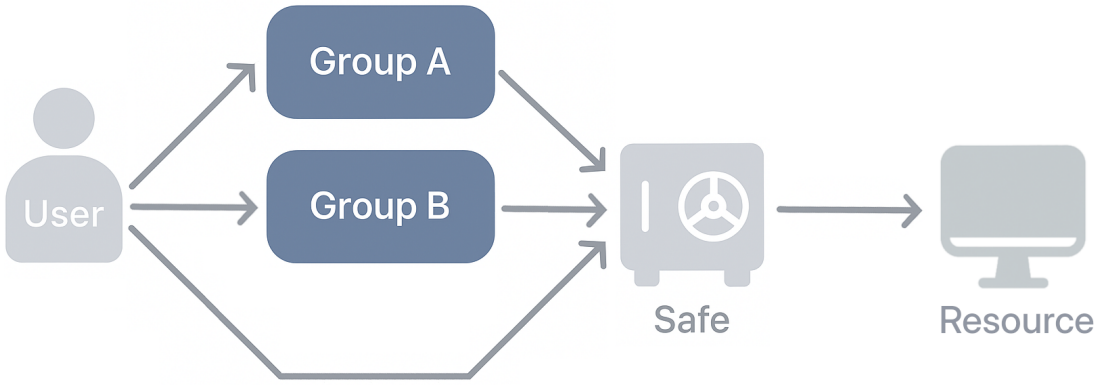
User Belongs to Multiple Groups Assigned to Different Safes with the Same Resource



When a user can access the same resource through multiple safes via different groups, the resolution follows this logic:

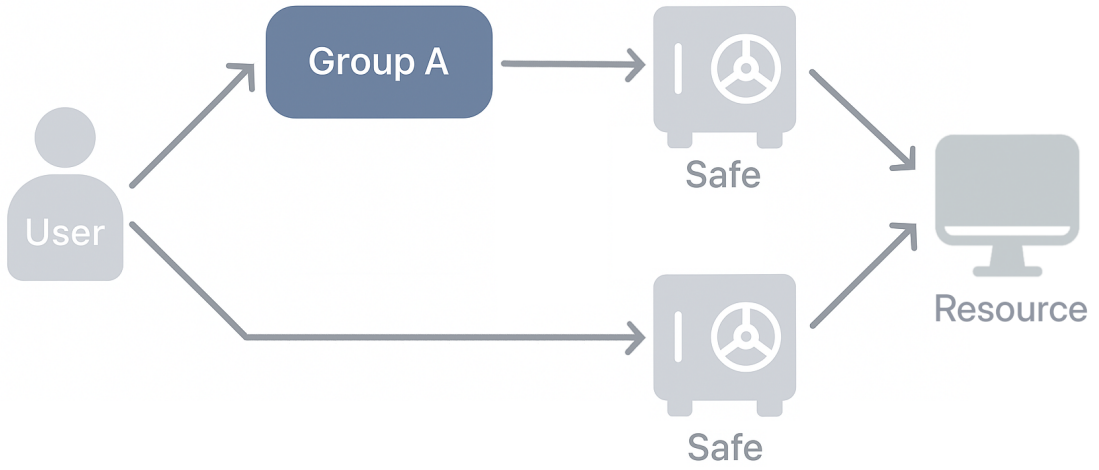
- **Access Time Period:** If the current time falls within the validity range of Group A, it is used. Otherwise, Group B is evaluated. If neither group has validity restrictions, the system selects the first group in alphabetical order.
- **Daily Access Policy:** If both groups have a daily time policy 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

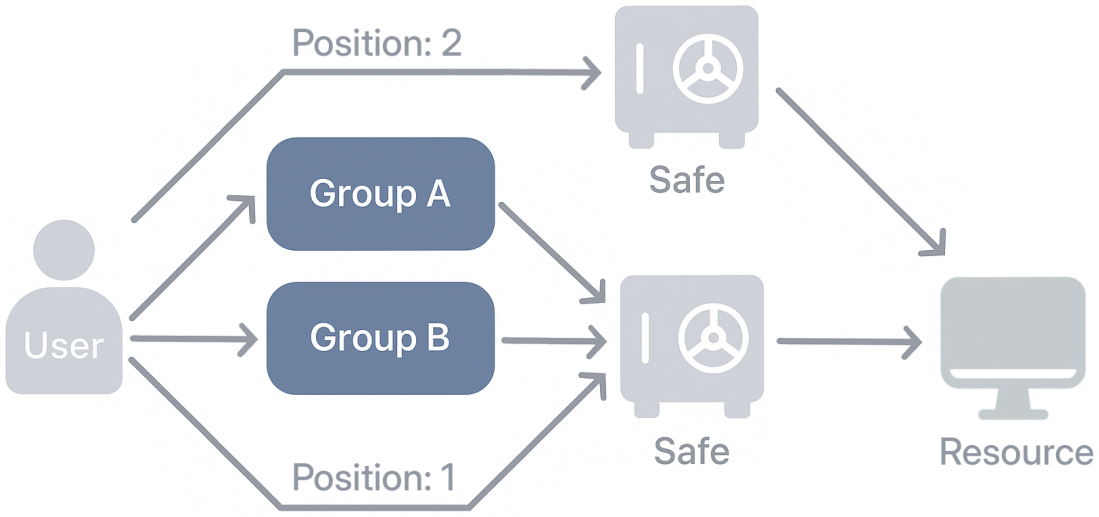


In cases where the user has access to the same resource:

- 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:

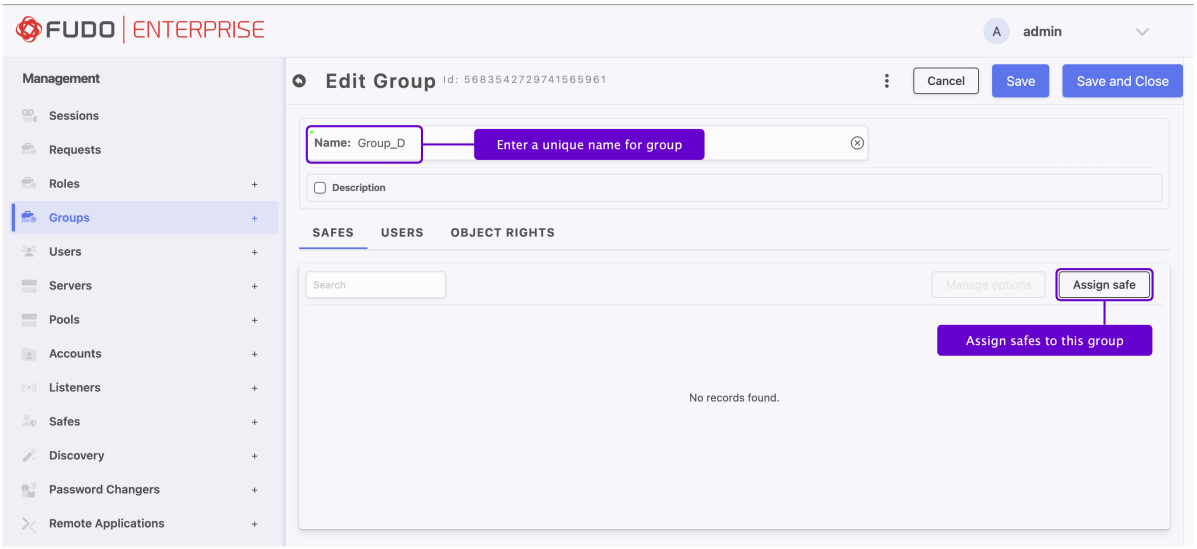
- First, Fudo Enterprise checks if the user has a **direct assignment to the safes.** If so, group-based assignments are ignored entirely.
- Then, among all available direct connections, Fudo Enterprise **evaluates the position** attribute and selects the safe with the highest position value.

Related topics:

- *Creating Group*
- *Creating a Safe*
- *Users*

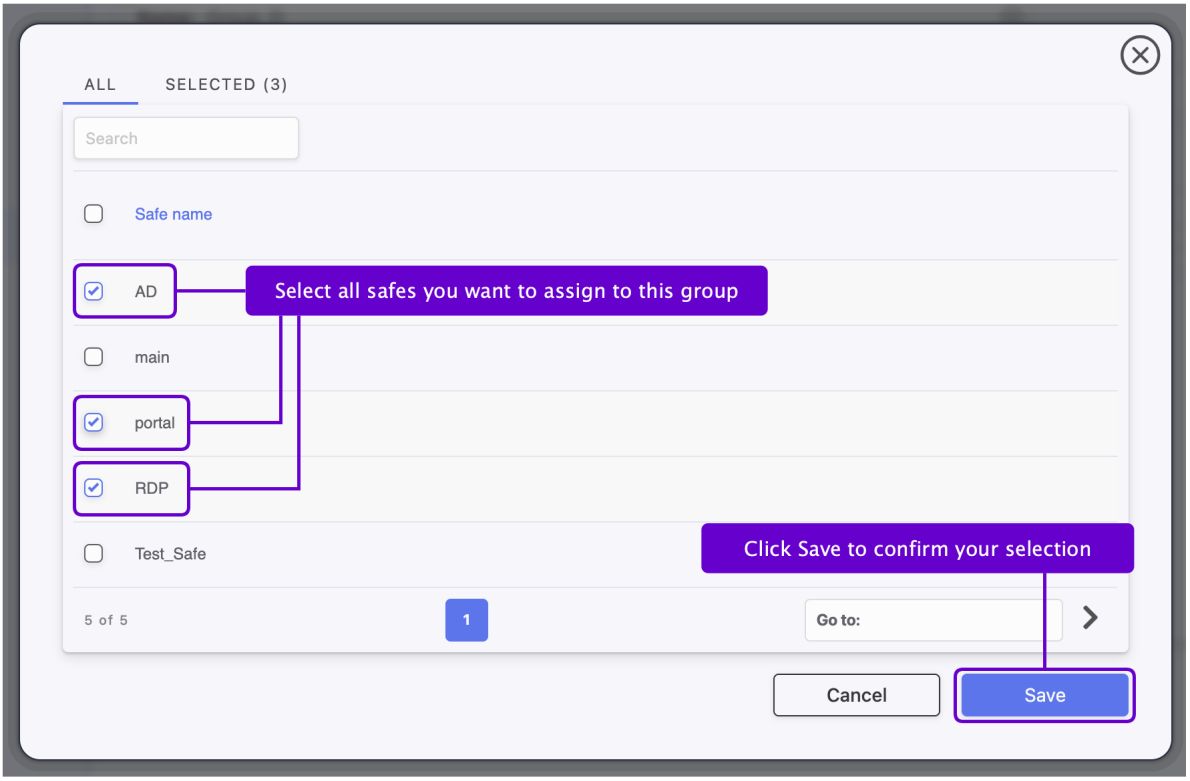
7.2 Creating Group

1. Click + icon in the main menu next to the *Groups* tab, or select *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

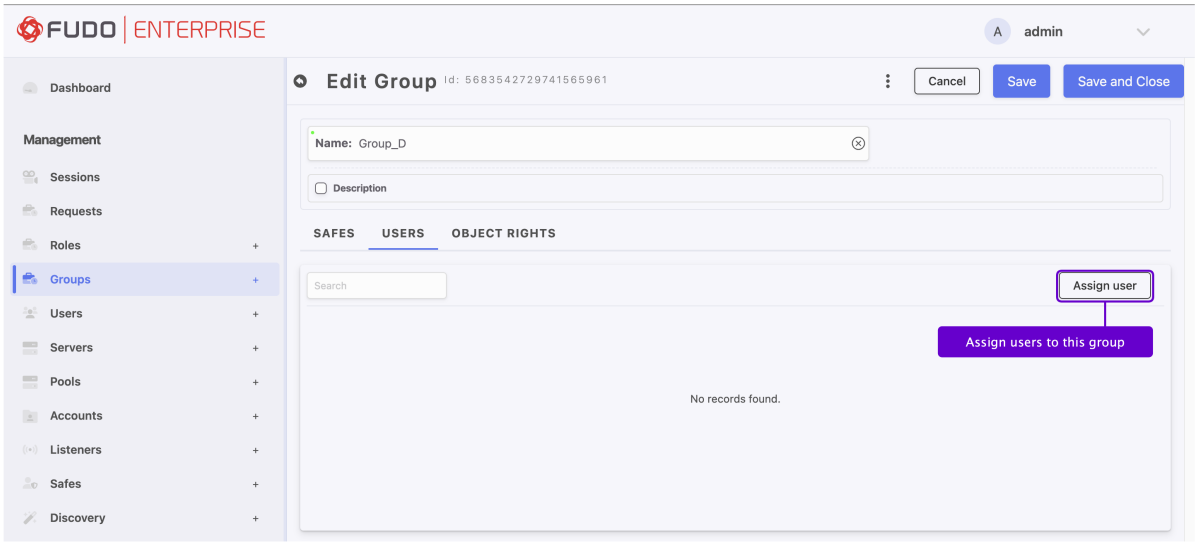
After assigning safes, you can enable and define time intervals during which the user will be allowed to connect to servers.

7. Select the desired safe and click *Manage Options*.
8. In the weekly calendar view, click the cell that corresponds to the desired day of the week and hour during which you want to grant access to the safe.
9. Click the highlighted square to adjust the time window if you want to change the access duration.
10. Click *Save* to close the modal window.

USERS TAB

In this tab, you can define which users will be part of this group.

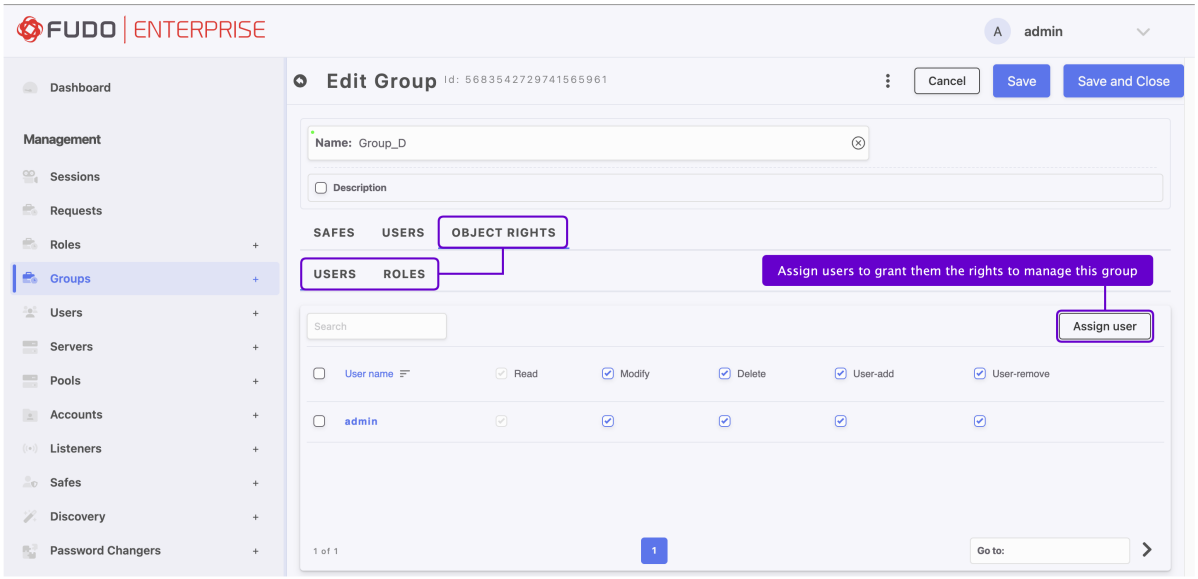
11. Go to the **USERS** tab and click *Assign User*.
12. Select all users you want to assign to this group and click *Save*.



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.



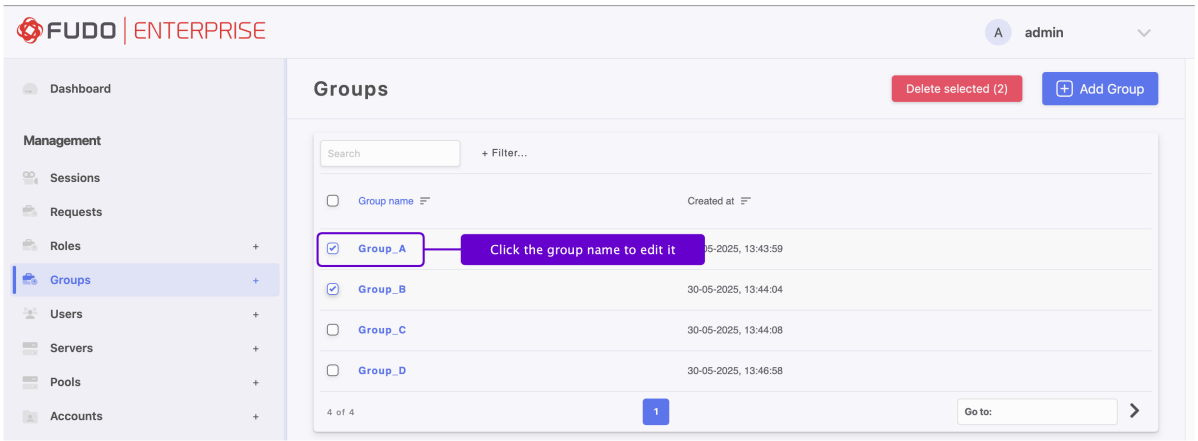
11. Go to the **USERS** sub-tab and click *Assign User*.
12. Select all users you want to assign permissions to manage this group and click *Save*.
13. Go to the **ROLES** sub-tab and click *Assign Role*.
14. Select all roles you want to assign permissions to manage this group and click *Save*.
15. Click *Save and Close* to save created group.

Related topics:

- *Groups (RBAC)*
- *Users*

7.3 Modifying Groups

1. Select *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.



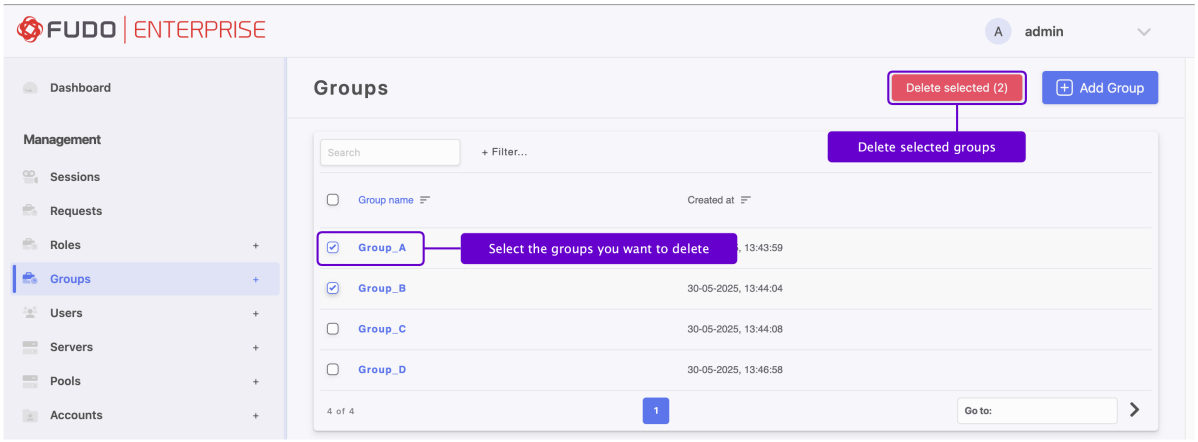
5. Click *Save and Close* to save changes to this configuration.

Related topics:

- *Role-Based Access Control (RBAC)*
- *Groups (RBAC)*
- *Users*

7.4 Deleting Groups

1. Select *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*.

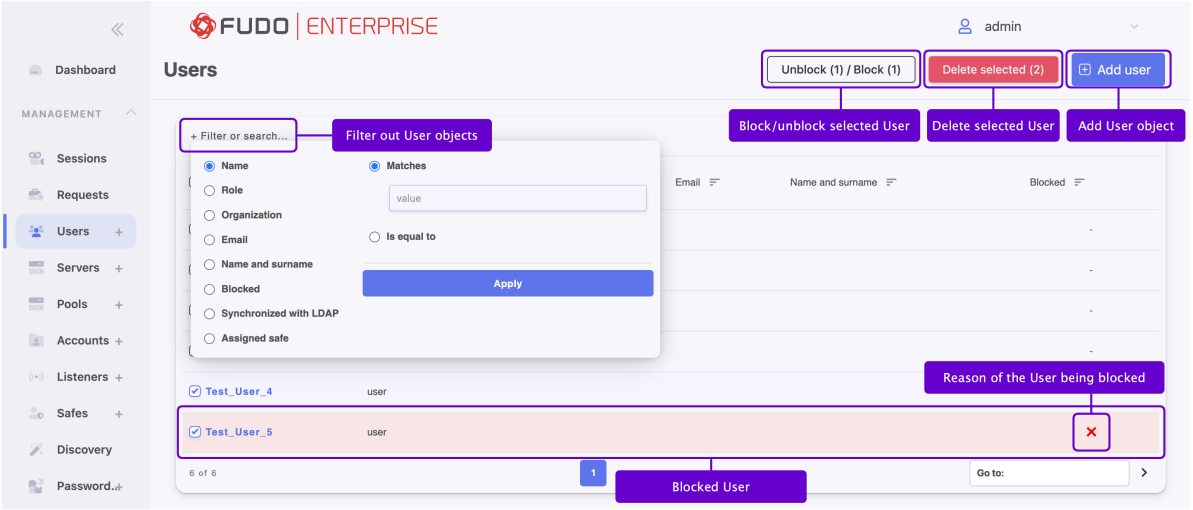
Related topics:

- *Groups (RBAC)*
- *Users*

CHAPTER 8

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.

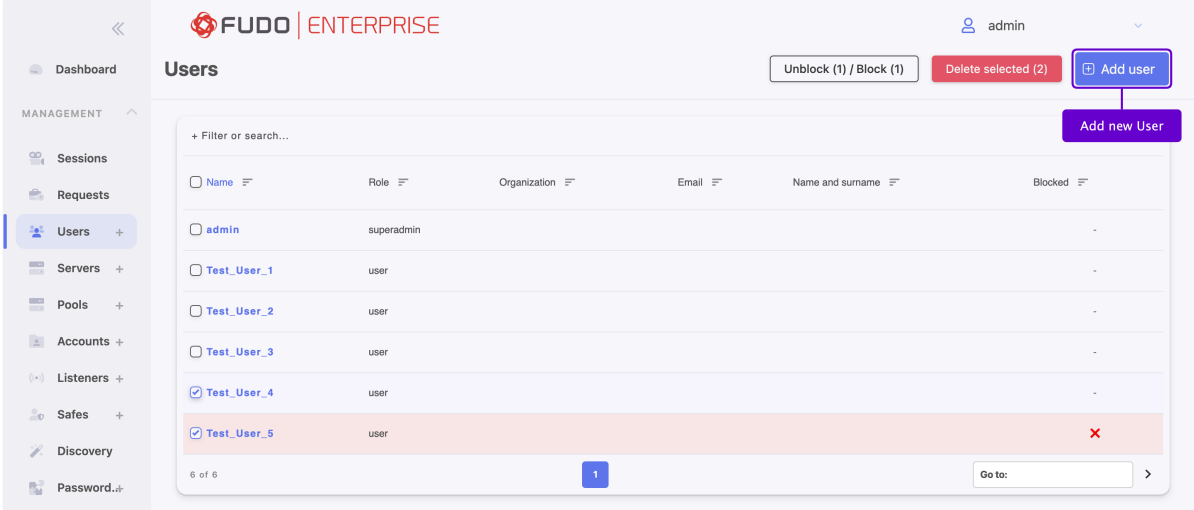
8.1 Creating a user

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.

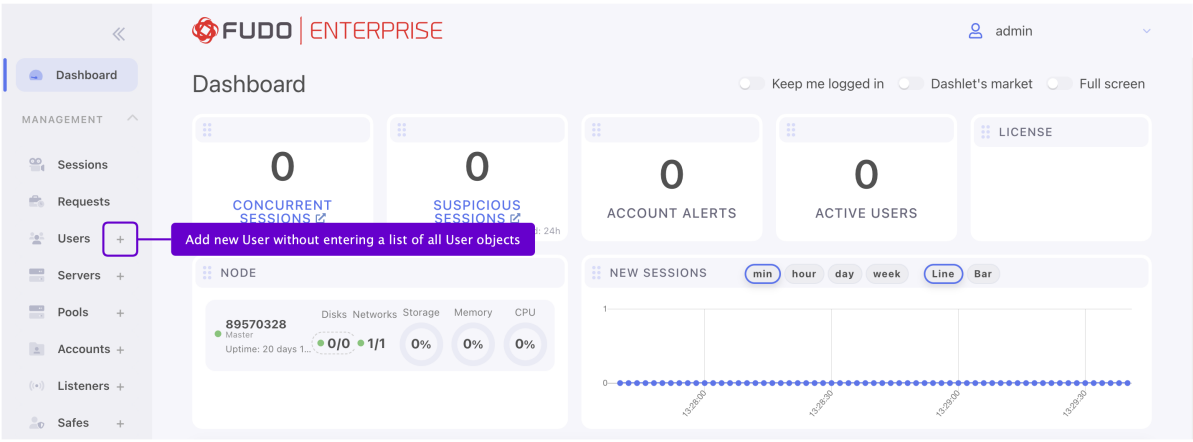
Warning: When creating a User object for MySQL connections, please note that Fudo Enterprise does not support the MySQL server `caching_sha2_password` plugin. The supported MySQL plugins are `mysql_native_password` and `mysql_old_password`. To ensure compatibility, server plugin should be set to `mysql_native_password` 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 *Management* sub-section, or



2. Select *Management* > *Users* and then click + *Add user*.



3. Enter user name.

Note:

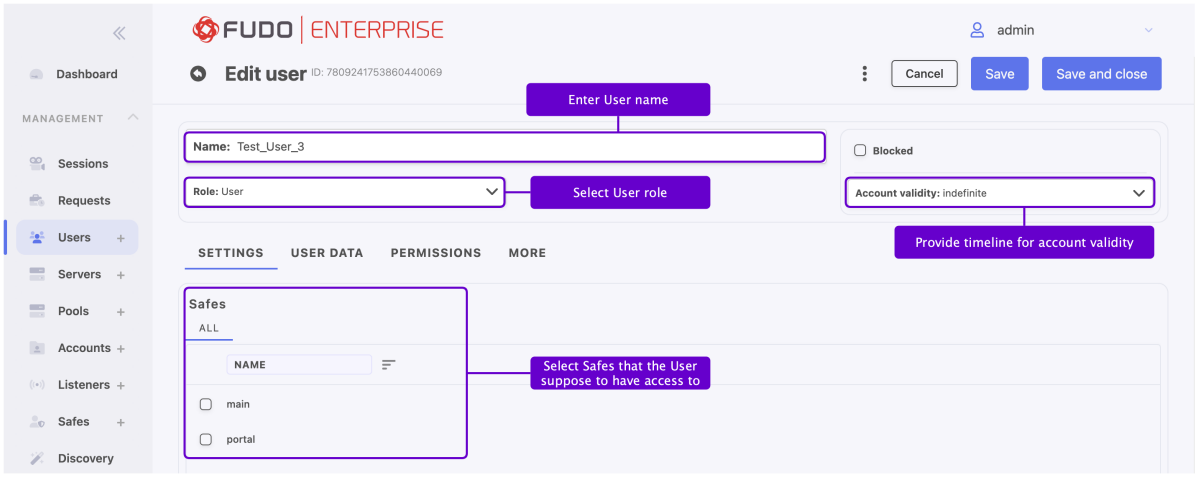
- While there can be more than one user with the same *Name*, the *Name* and domain combination must be unique.
- The *Name* field is not case sensitive.

Warning: It's not allowed to include % and # characters within the usernames.

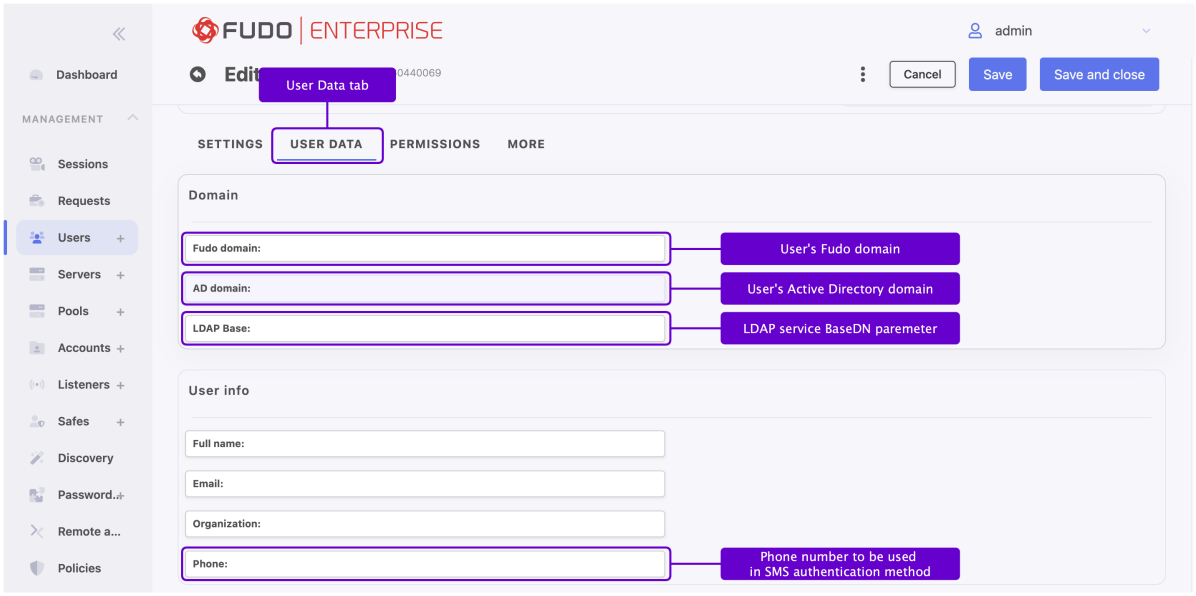
4. From the *Role* drop-down list select user's role, which will determine the access rights.

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. For more details, refer to the *External authentication server 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.

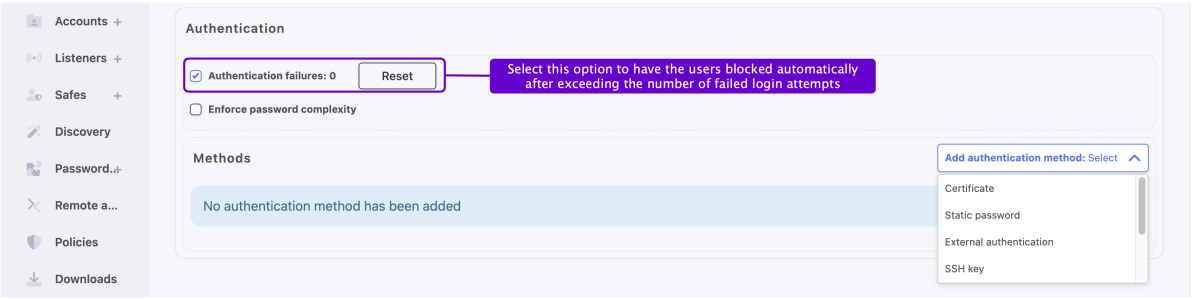
---

14. In the *SNMP* field, click *Enabled* option to use SNMP, and provide authentication and encryption methods from the available drop-down lists.

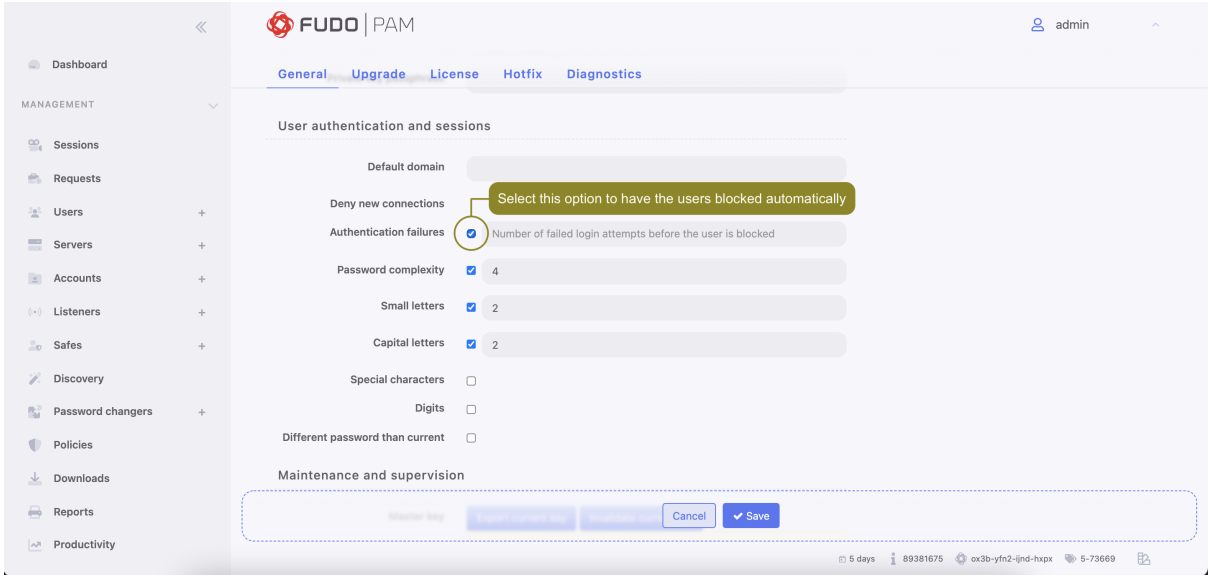
Note: SNMP configuration is available only for user with the *Service* role.

---

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.

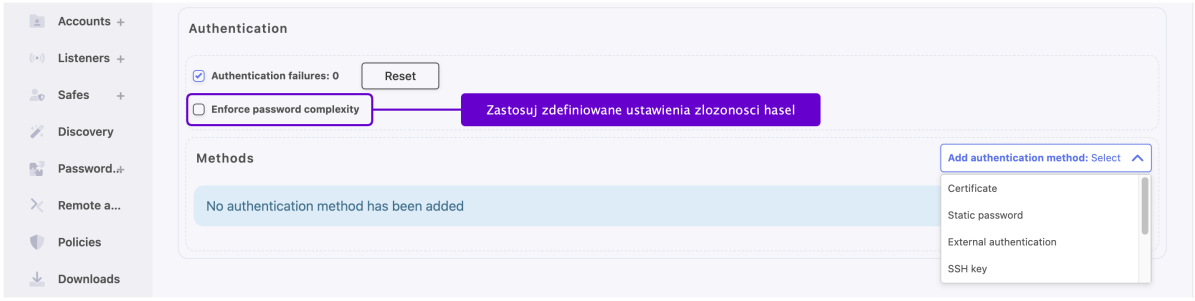


Note: The authentication failures counter is enabled only if the *Authenticaiton failures* option is set in *Settings* > *Authentication* in the *User authentication and sessions* section.



16. Select the *Enforce password complexity* option to force passwords to conform to specified settings.

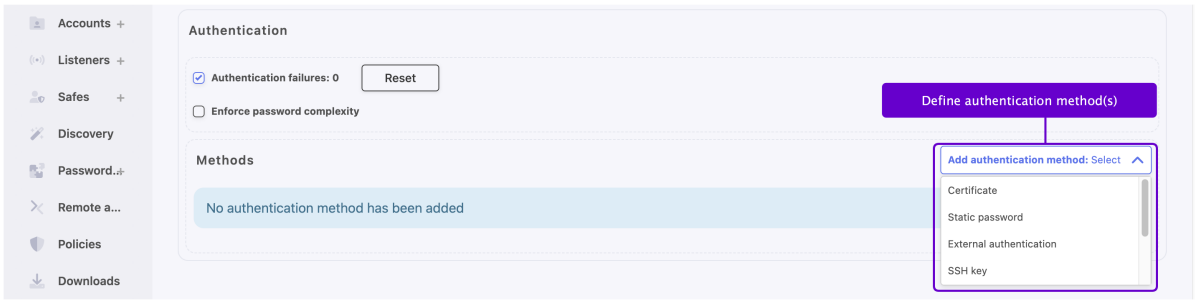
Note: Password complexity is defined in *Settings* > *Authentication*. To learn more, go to the *Password complexity* section.



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 password in the *Password* field.
- 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.

API key

- Provide or generate *API key*.
- Copy generated API key to use it in other systems that require authentication with this Fudo user.

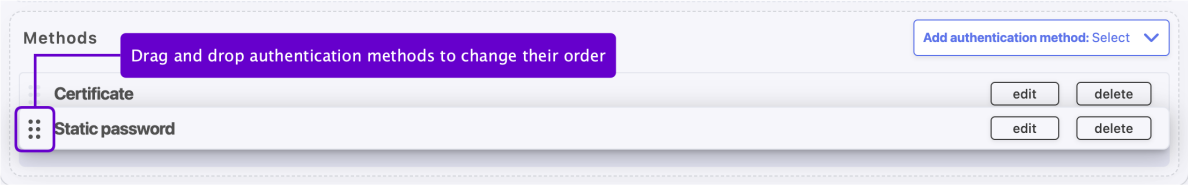
Note: The *API Key* cannot be retrieved after saving this authentication method.

---

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.



---

20. Click *Save* or *Save and close*.

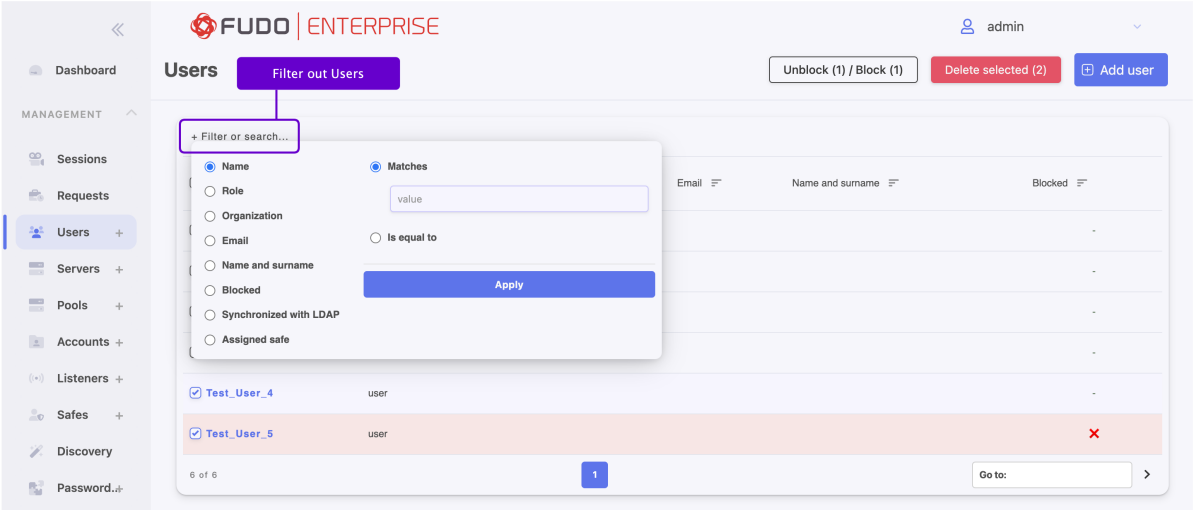
Related topics:

- *Authentication failures counter*
- *Users synchronization*
- *Data model*
- *Default domain*
- *System initiation*

- *Servers*
- *Accounts*
- *Approving pending user requests*
- *Declining pending requests*

8.2 Editing a user

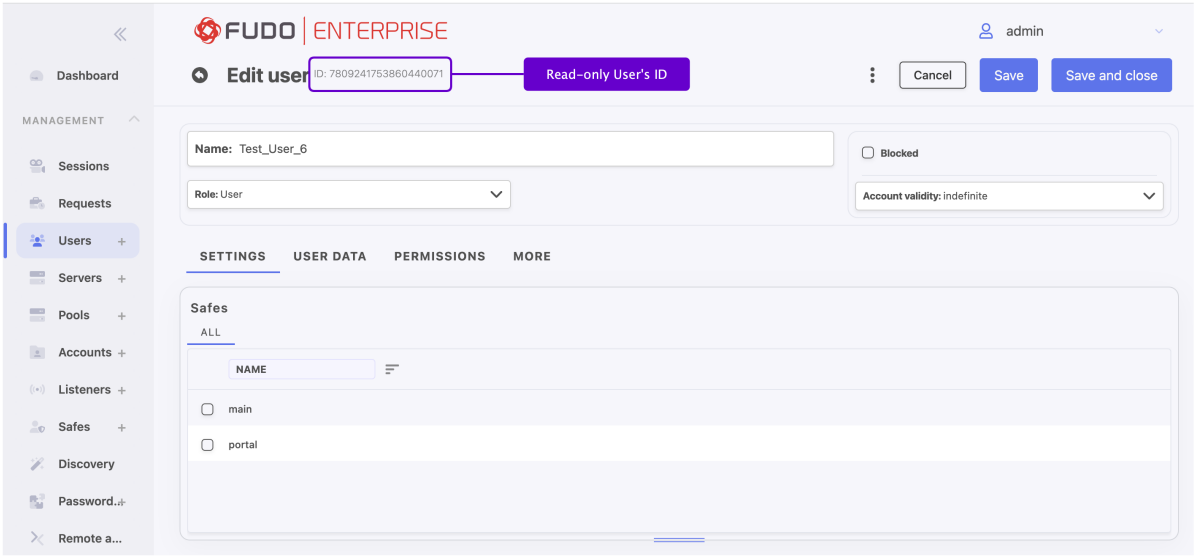
1. Select *Management* > *Users*.
2. Define filters to limit the number of objects displayed on the list.



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*.

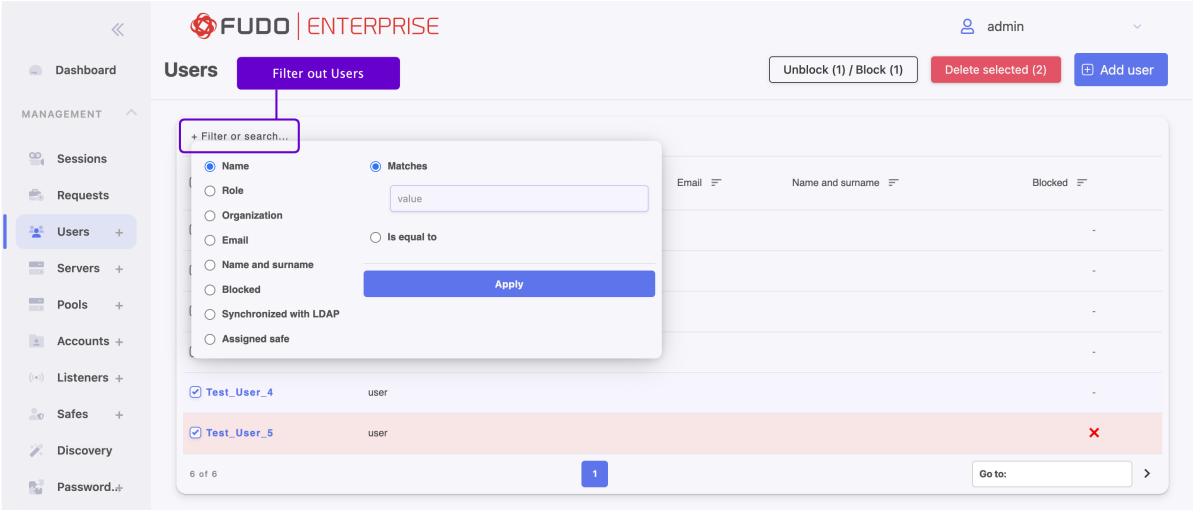
Related topics:

- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*
- *Accounts*

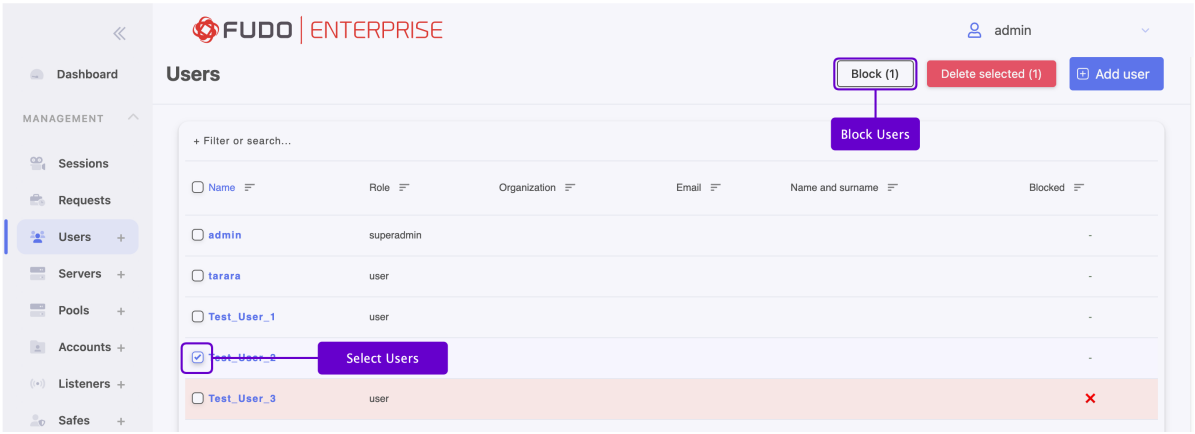
8.3 Blocking a user

Warning: Blocking a user will terminate its current connections.

1. Select *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*.

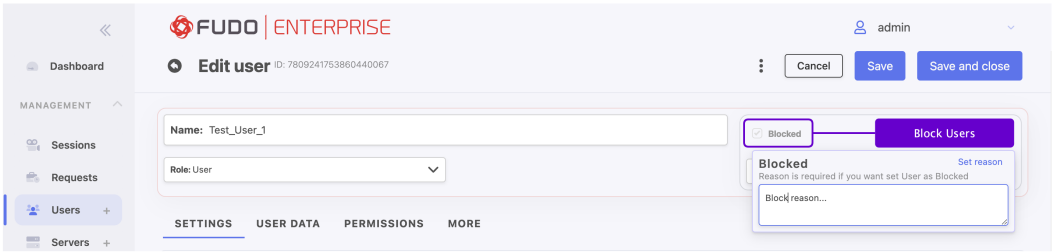


4. Provide mandatory blocking reason and click *Block*.

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'.



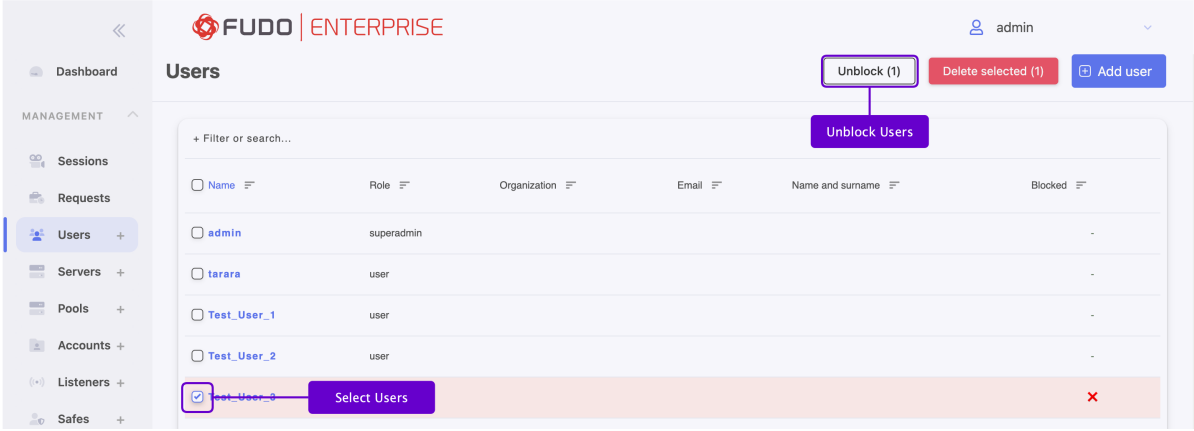
- Click *Save* or *Save and close*.

Related topics:

- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*
- *Accounts*

8.4 Unblocking a user

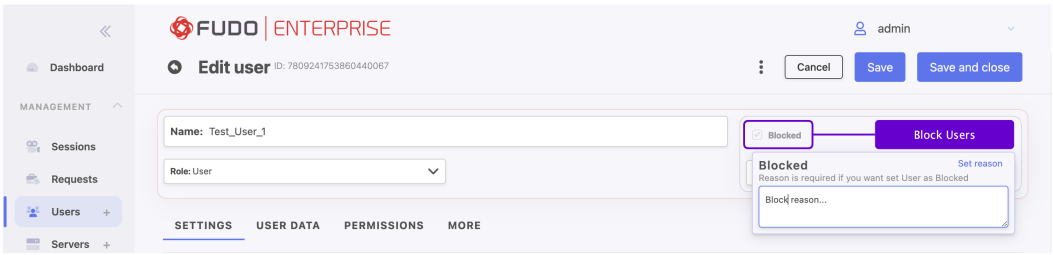
1. Select *Management* > *Users*.
2. Define filters to limit the number of objects displayed on the list.
3. Select the user you want to unblock and click *Unblock*.



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:

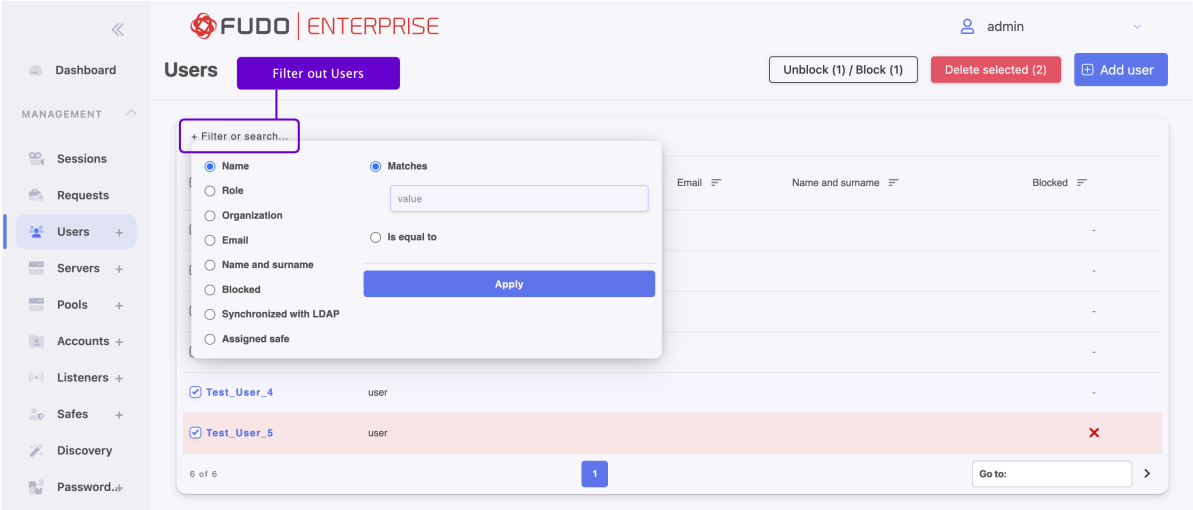
- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*
- *Accounts*

8.5 Deleting a user

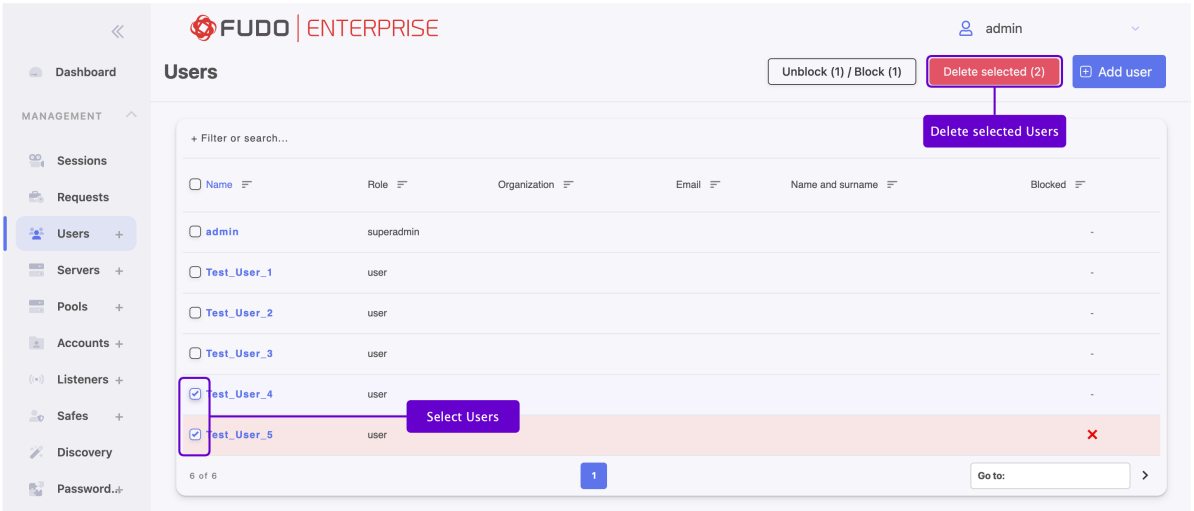
Note: Deleting a user definition does not result in the removal of associated registered sessions. Sessions of deleted users are marked with a strikethrough username.

Warning: Deleting a user definition will terminate its current connections.

1. Select *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:

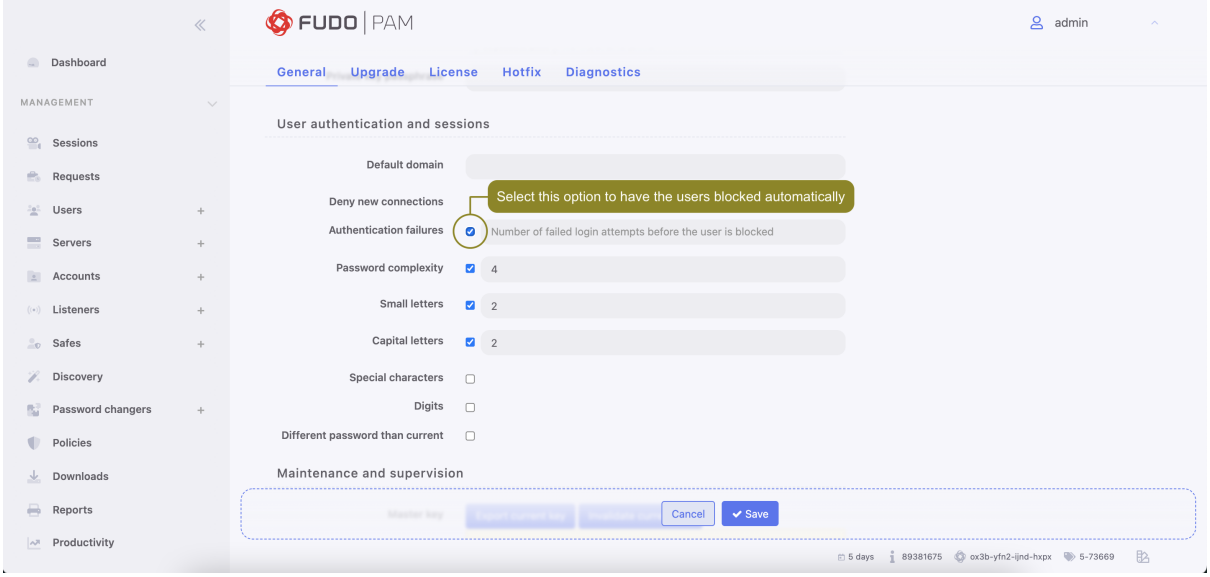
- *Users synchronization*
- *Data model*

- *System initiation*
- *Servers*
- *Accounts*

8.6 Authentication failures counter

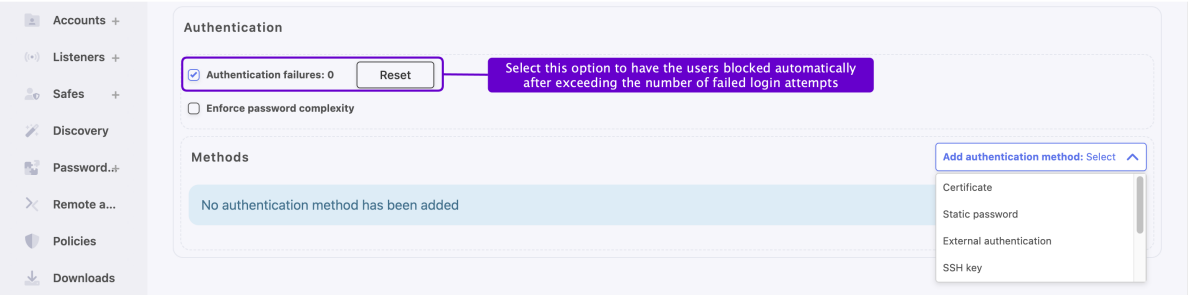
Fudo can keep track of failed login attempts and automatically block users accounts if the counter reaches a specified value.

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 *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*

8.7 Users Synchronization - User Directory

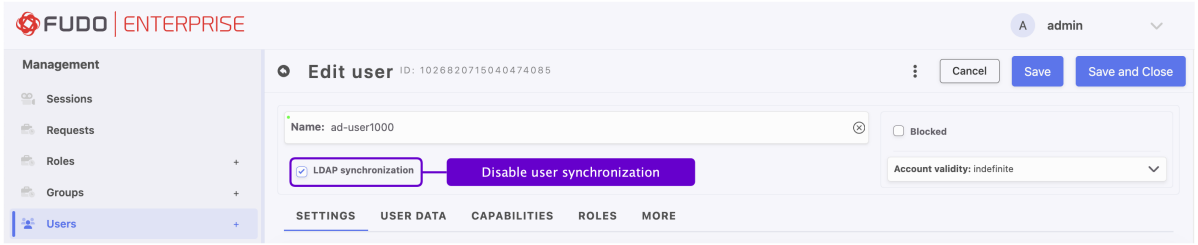
User is one of the fundamental *data model* entity. Only defined users are allowed to connect to monitored servers. Fudo Enterprise features automatic users synchronization service which enables importing users information from *Active Directory* servers or other servers compatible with the *LDAP* protocol.

> **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.

Note:

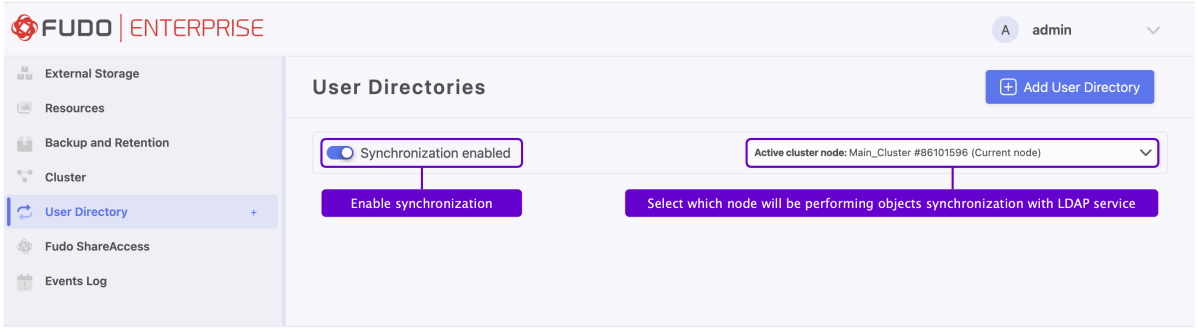
- Fudo Enterprise supports nested LDAP groups.
- Also, Fudo Enterprise allows synchronizing the user's data with the LDAP service source. The `Synchronize with LDAP` option is responsible for this process. When this option is checked for the given user, an administrator can't edit the user's data manually 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.



Configuring Users Synchronization Service

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.

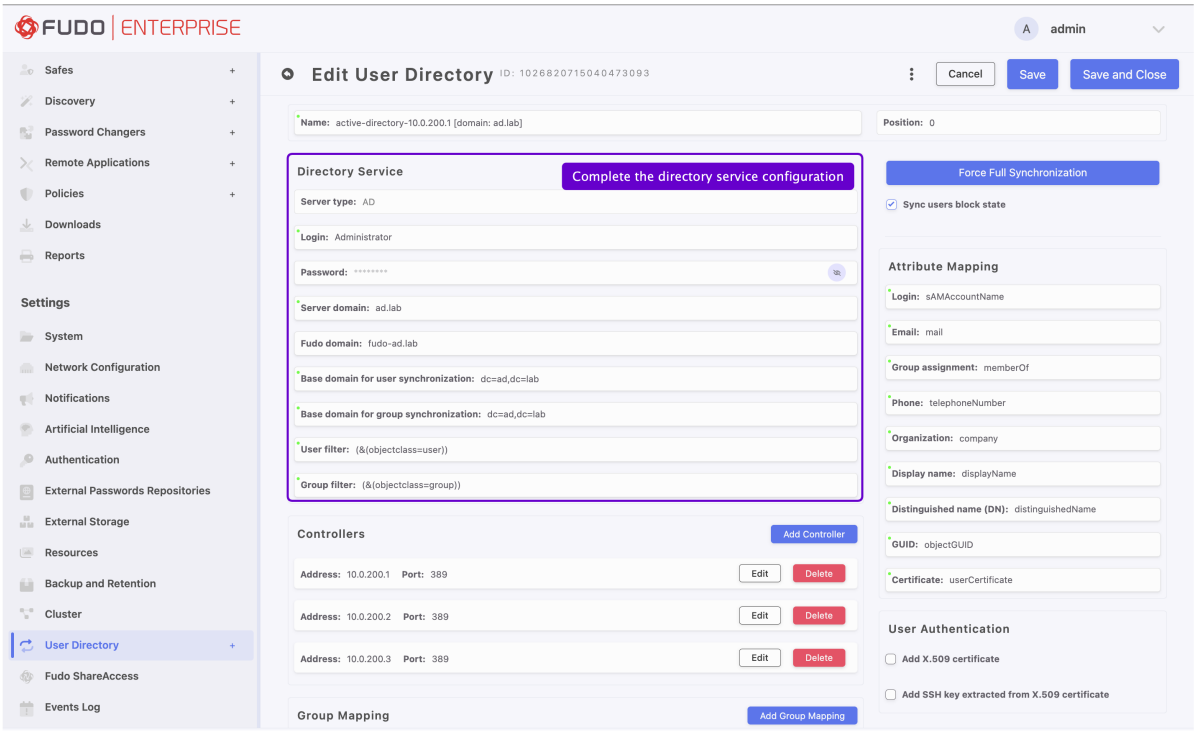
Note: A lower number indicates a higher priority.

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.

---

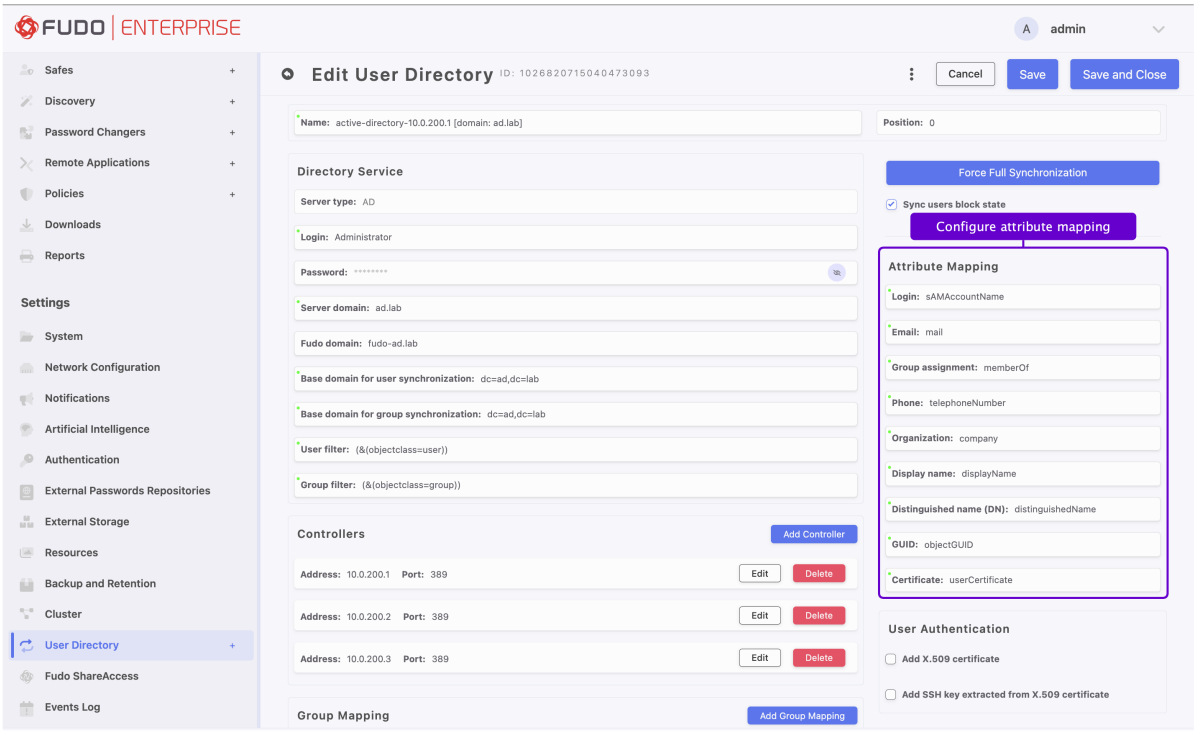
16. Select the *Page LDAP results* option to enable paging.
17. Select the *Encrypted connection* option to enable encryption and upload the CA certificate.
18. Click *Save*



Note: To add multiple controllers, repeat the steps described above.

Defining User Information Mapping

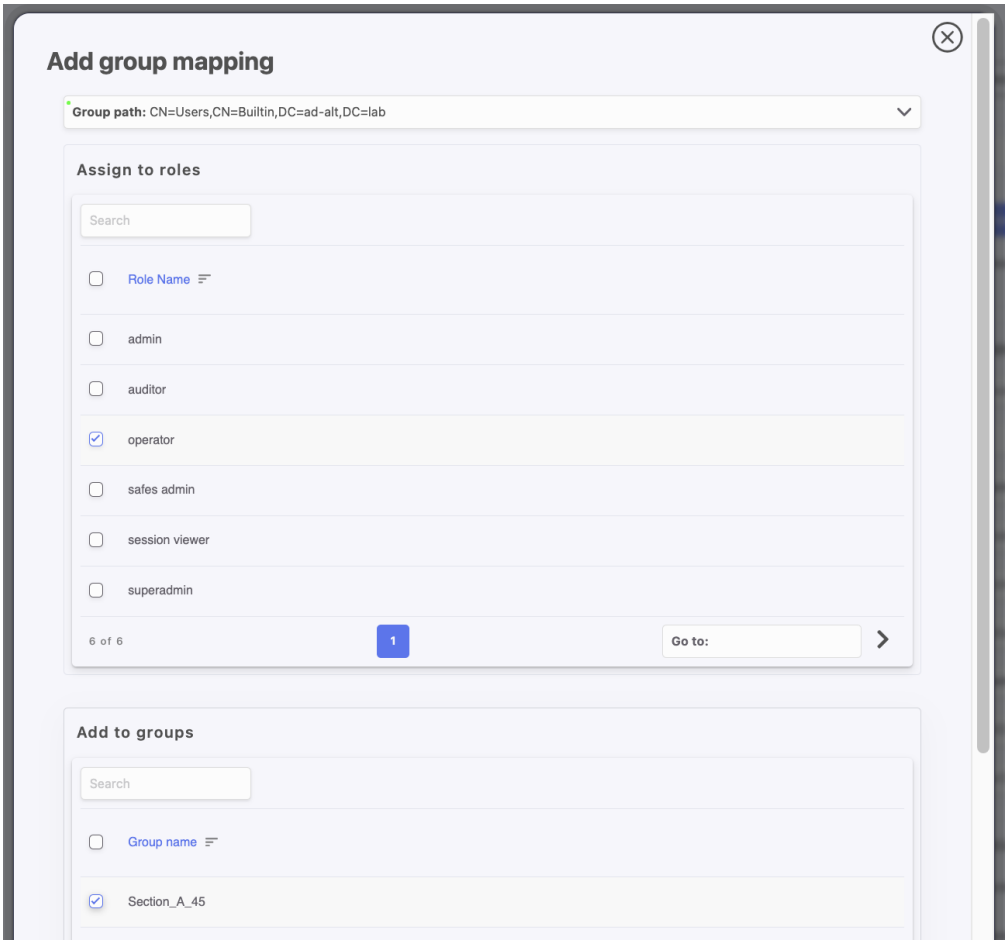
Note: Fields mapping enables importing users information from nonstandard attributes, e.g. telephone number defined in an attribute named *mobile* instead of the standard *telephoneNumber*.



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.

Related topics:

- *User authentication against external LDAP server*
- *Users management*
- *Diagnostics*

CHAPTER 9

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.

9.1 Creating a server

9.1.1 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.

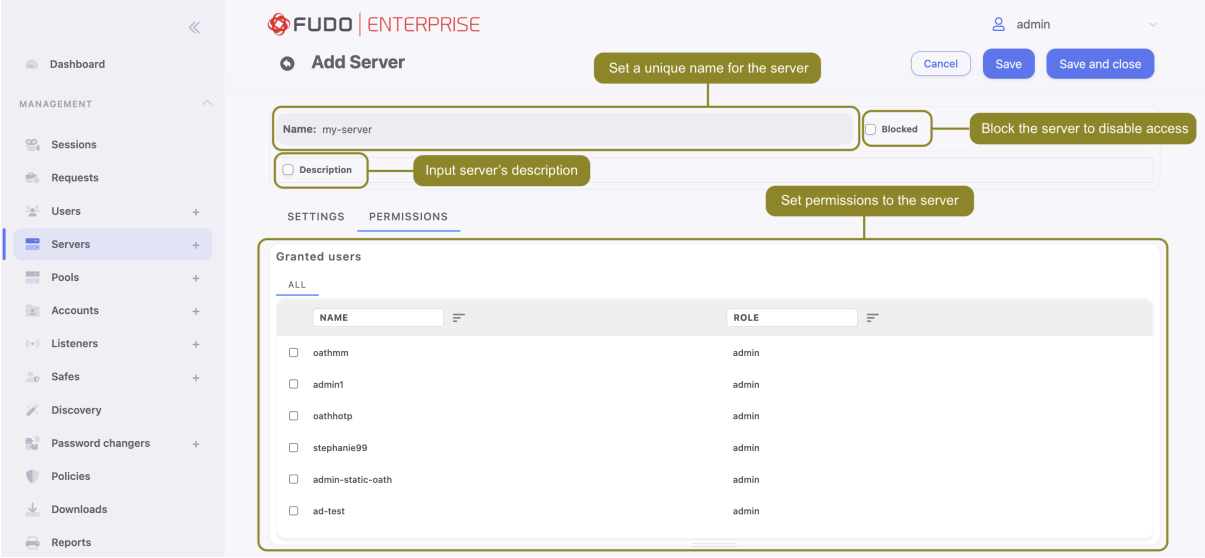
Model	Maximum recommended number of concurrent HTTP sessions*
F100x	2
F300x	5
F500x	10

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

1. Click + icon in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.
3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.
5. In the *Permissions* section, add users allowed to manage this object.



6. In the *Settings* section on the list of available protocols select `HTTP` .

Warning: After server's definition is saved, protocol's field is uneditable.

7. Select the *TLS enabled* option to connect to monitored server over TLS.

- Select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.

8. 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.

9. 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.
10. 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.

---

11. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

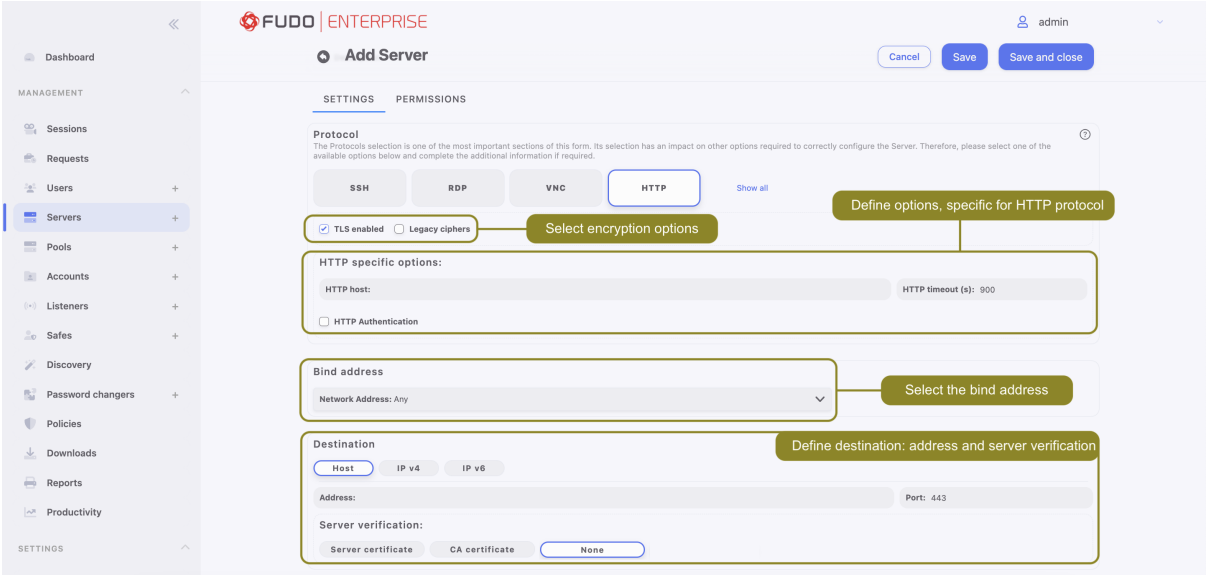
- The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

---

12. 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.

- 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.



13. Click *Save* or *Save and close*.

Related topics:

- *Pools*
- *Protocols - HTTP*
- *Data model*
- *Accounts*
- *Listeners*
- *Safes*

9.1.2 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 in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.
3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.
5. In the *Permissions* section, add users allowed to manage this object.
6. In the *Settings* section on the list of available protocols select `Modbus` .

> **Warning:** After server's definition is saved, protocol's field is uneditable.

7. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

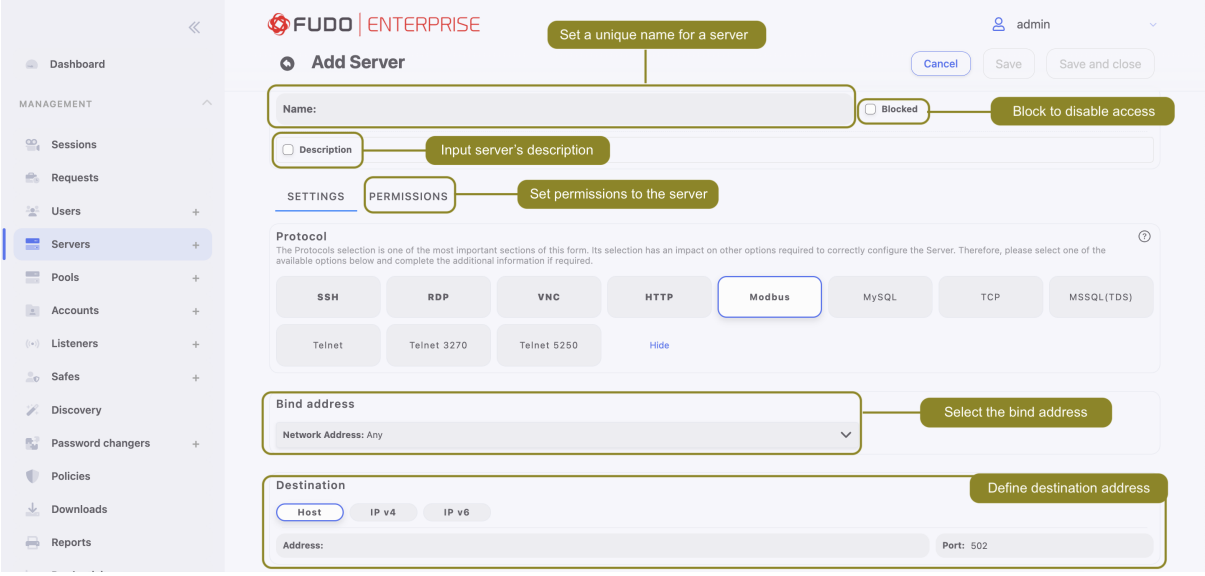
- The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP Addresses* topic.

---

8. 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.



9. Click *Save* or *Save and close*.

Related topics:

- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.1.3 Creating a MS SQL server

Note:

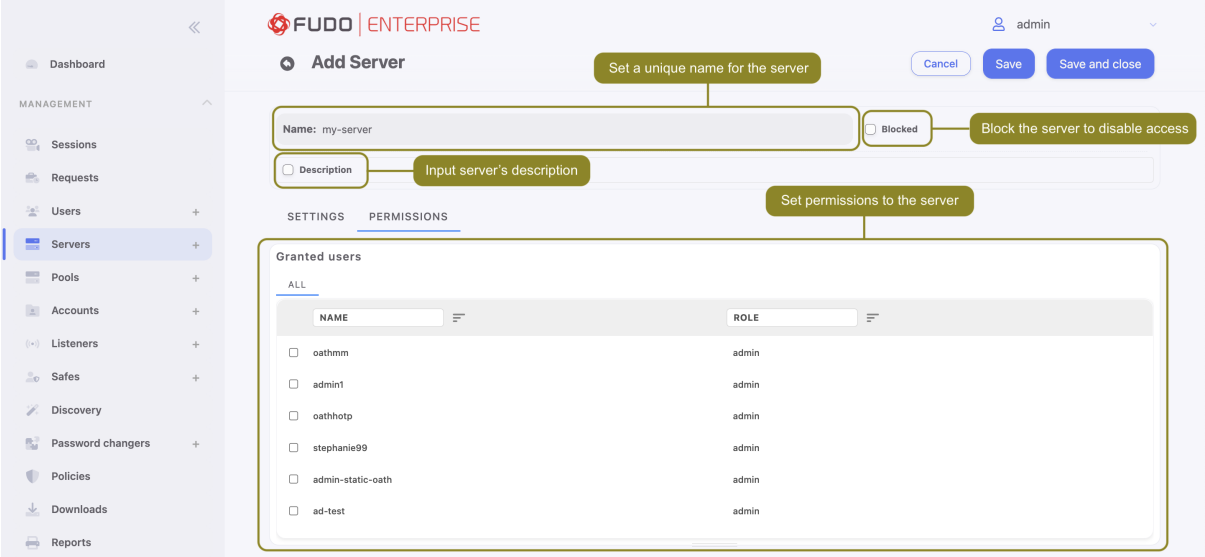
- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.

1. Click + icon in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.
3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.

5. In the *Permissions* section, add users allowed to manage this object.



6. In the *Settings* section on the list of available protocols select `MSSQL(TDS)` .

Warning: After server's definition is saved, protocol's field is uneditable.

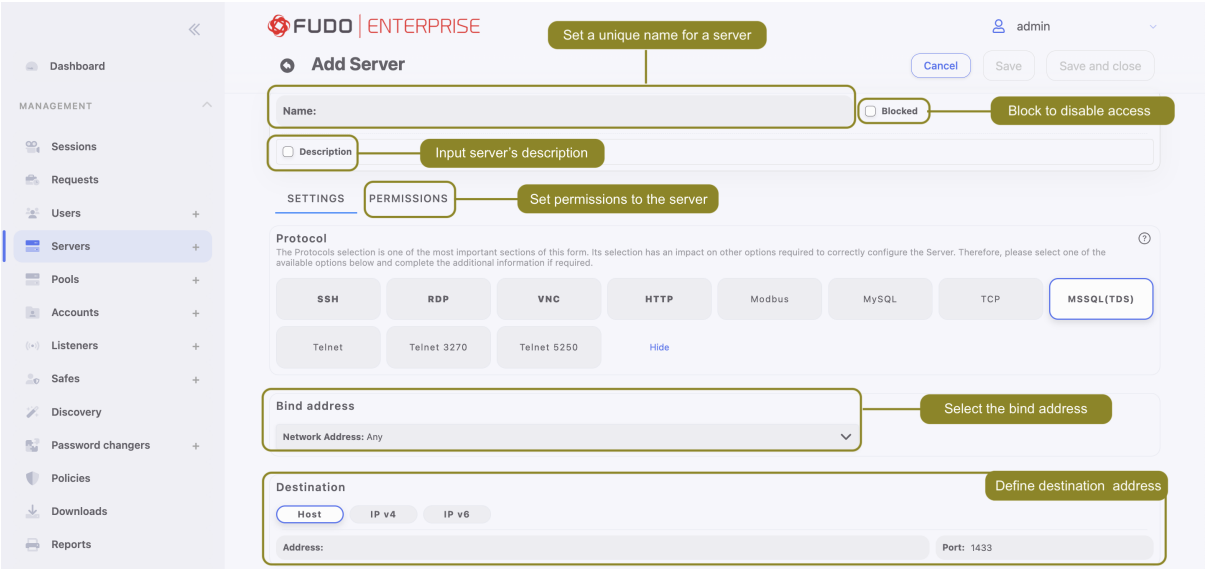
7. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

- The *Bind 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 *Bind 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.

8. 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.



9. Click *Save* or *Save and close*.

Related topics:

- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.1.4 Creating a MySQL server

Warning: Please 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.

Note:

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.

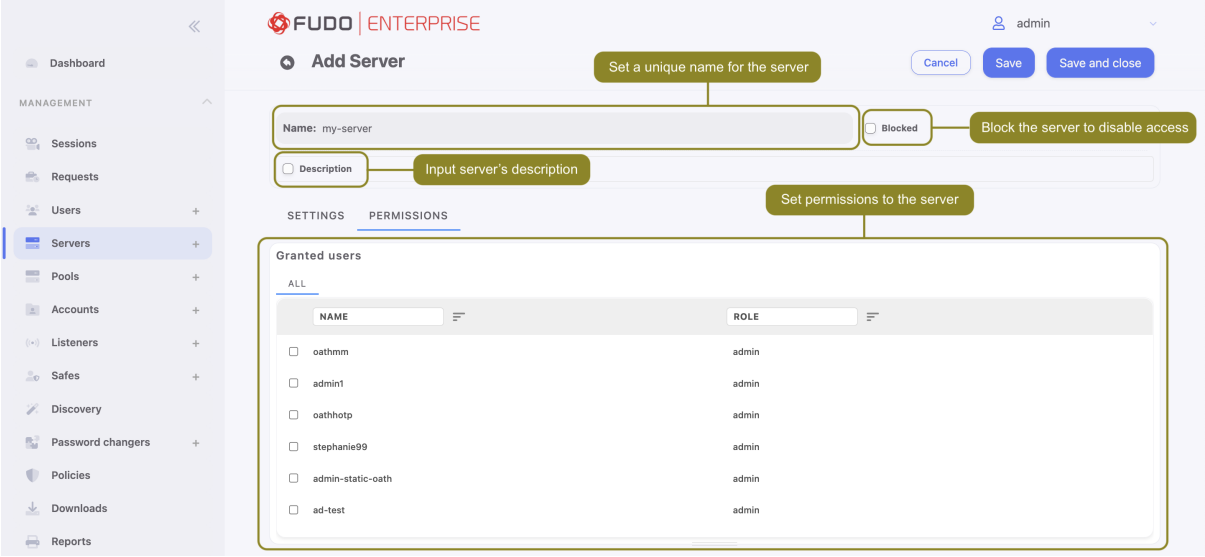
---

1. Click + icon in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.

3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.
5. In the *Permissions* section, add users allowed to manage this object.



6. In the *Settings* section on the list of available protocols select `MySQL` .

Warning: After server's definition is saved, protocol's field is uneditable.

7. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

- The *Bind 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 *Bind 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.

8. 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.



9. Click *Save* or *Save and close*.

Related topics:

- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.1.5 Creating an RDP server

Note:

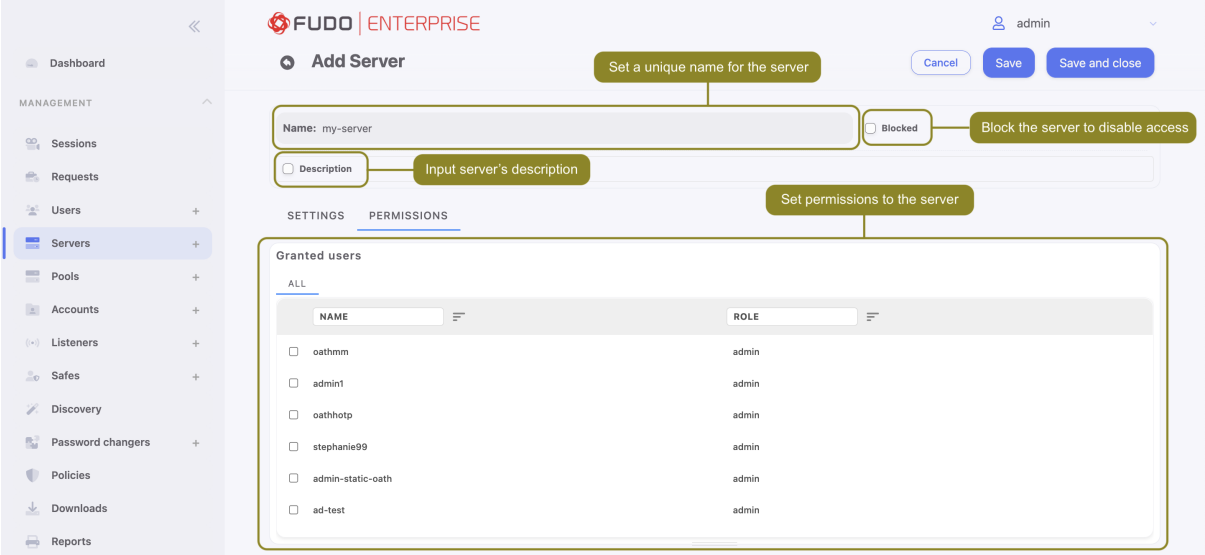
- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- Fudo Enterprise allows authenticating against RDP server with Kerberos.

---

1. Click + icon in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.
3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.
5. In the *Permissions* section, add users allowed to manage this object.



6. In the *Settings* section on the list of available protocols select `RDP` .

Warning: After server's definition is saved, protocol's field is uneditable.

7. Select the *TLS enabled* option to connect to monitored server over TLS.
   - 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.

   - Select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.

8. 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.

9. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

- The *Bind 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 *Bind 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.

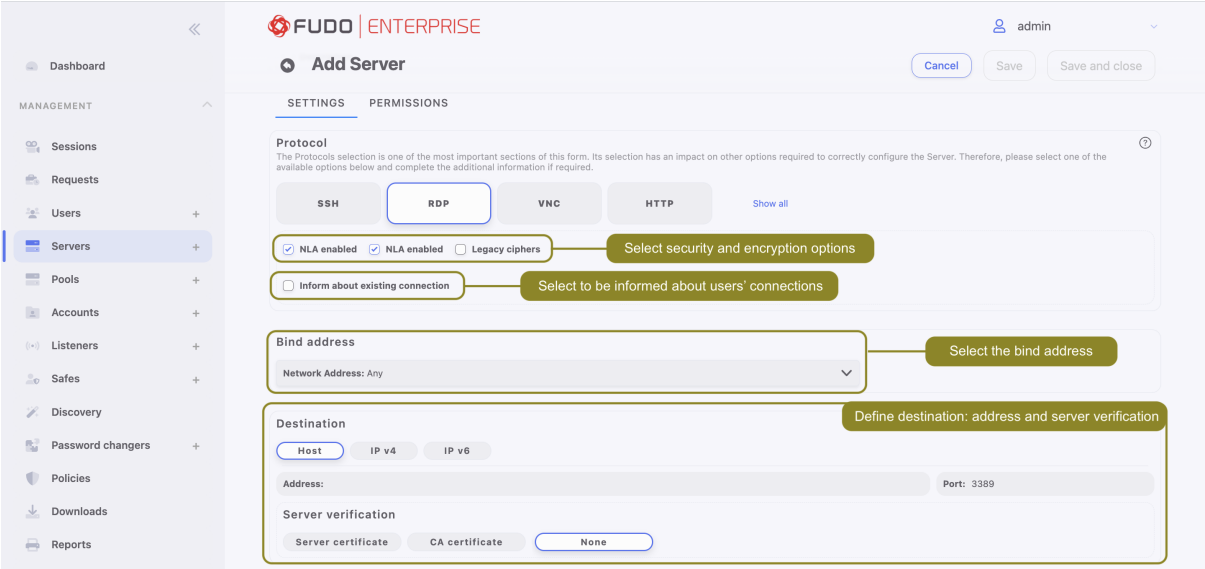
---

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.

- 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.
- Otherwise, provide *server key*.



12. Click *Save* or *Save and close*.

Related topics:

- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.1.6 Creating an SSH server

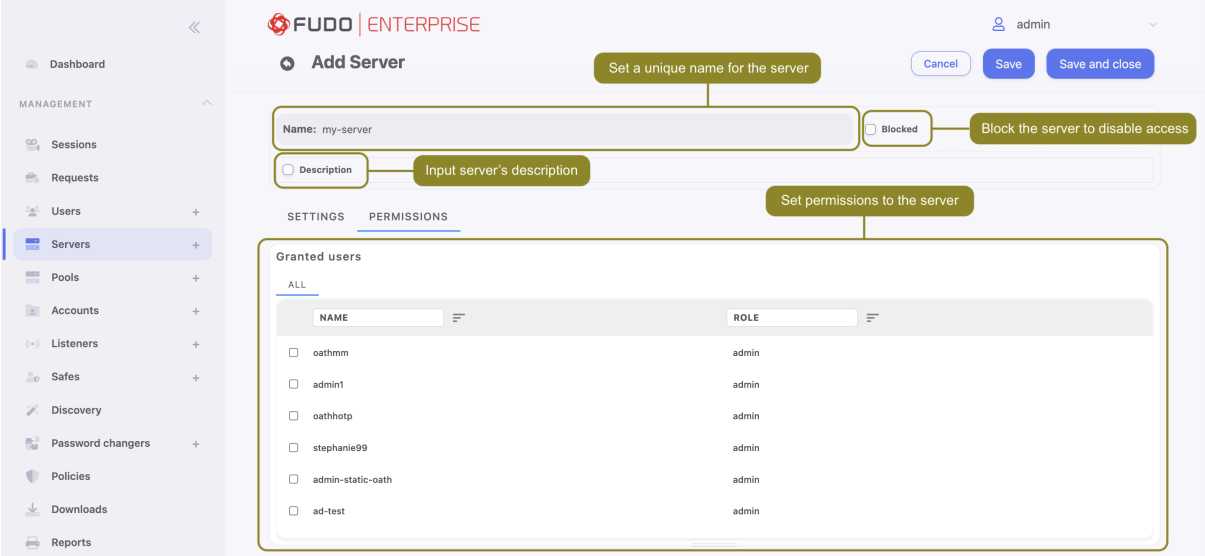
Note:

- 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 in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.
3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.
5. In the *Permissions* section, add users allowed to manage this object.



6. In the *Settings* section on the list of available protocols select `SSH` .

Warning: After server's definition is saved, protocol's field is uneditable.

7. Select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.

12. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

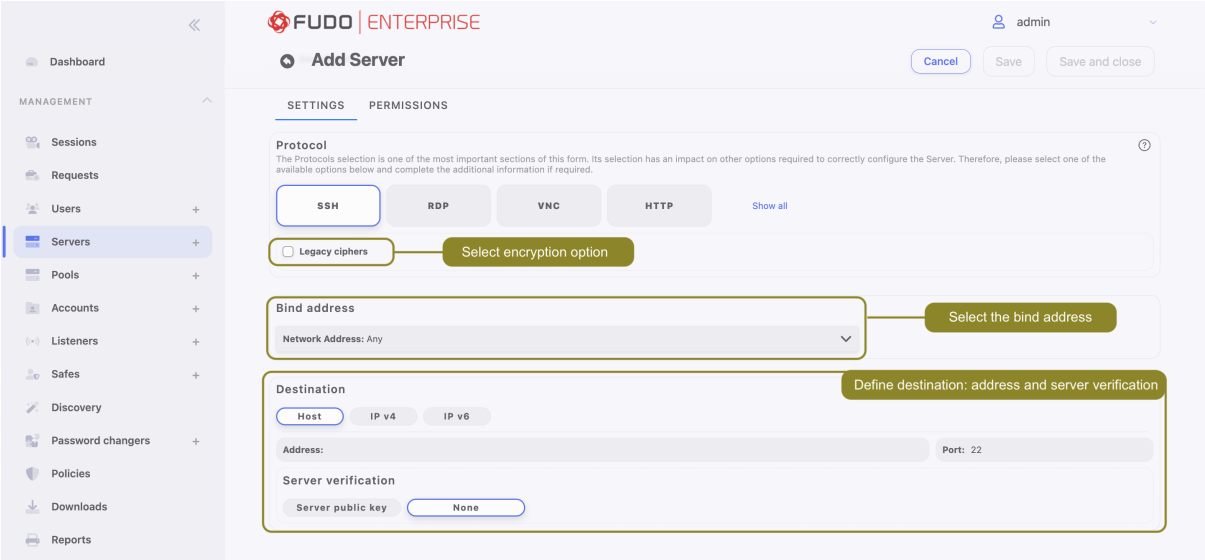
- The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).

- In case of cluster configuration, select a labeled IP address from the *Bind 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.

13. 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.

14. In the *Server verification* section select `Server public key` and provide respective certificate data. Select `None` to disable server verification.



15. Click *Save* or *Save and close*.

Related topics:

- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.1.7 Creating a Telnet server

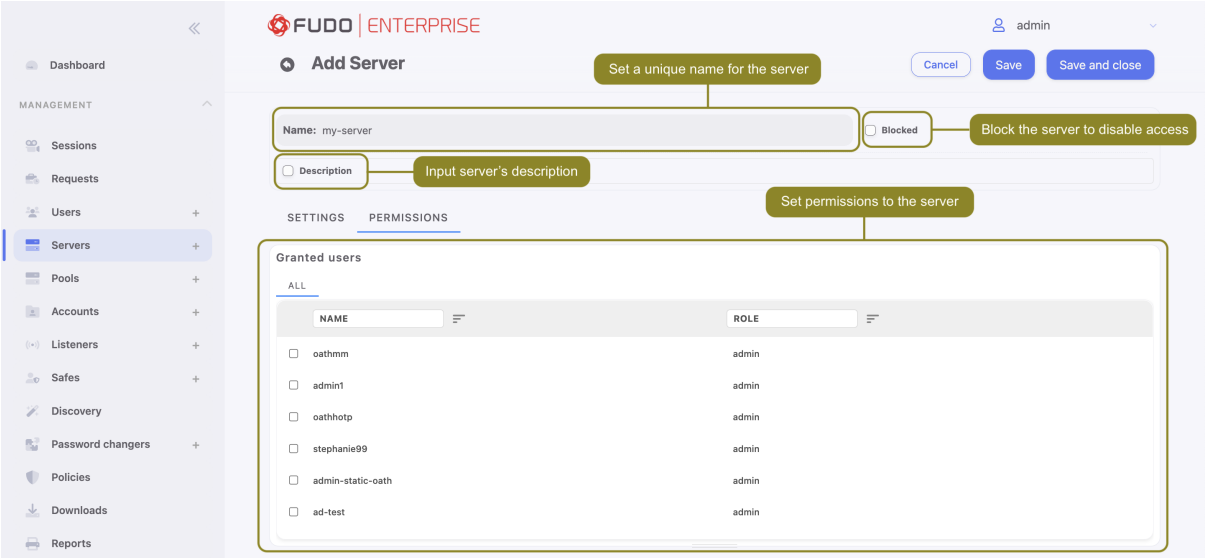
Note:

- 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 in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.
3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.
5. In the *Permissions* section, add users allowed to manage this object.



6. In the *Settings* section on the list of available protocols select `Telnet` .

Warning: After server's definition is saved, protocol's field is uneditable.

7. Select the *TLS enabled* option to connect to monitored server over TLS.

- Select *Legacy cryptos* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.

8. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

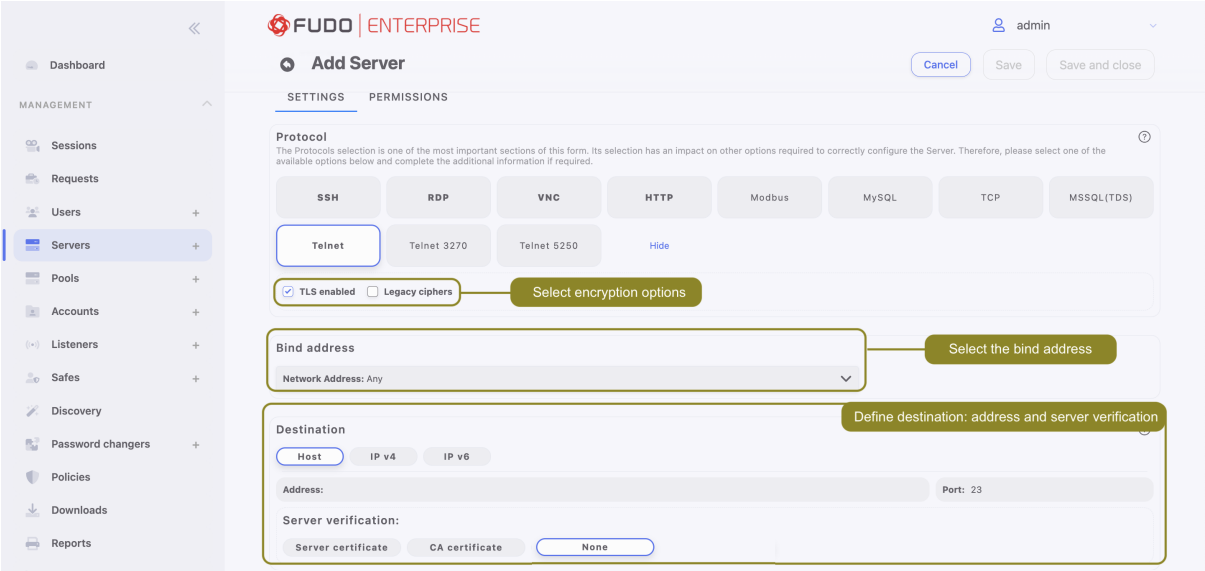
Note:

- The *Bind 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 *Bind 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.

- 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.



10. Click *Save* or *Save and close*.

Related topics:

- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.1.8 Creating a Telnet 3270 server

Deprecated since version 5.6 :class: danger

Support for the **Telnet 3270** protocol is **under review** and may be removed in a release following version 5.6. If this protocol is critical to your environment, please contact Fudo Support for more information.

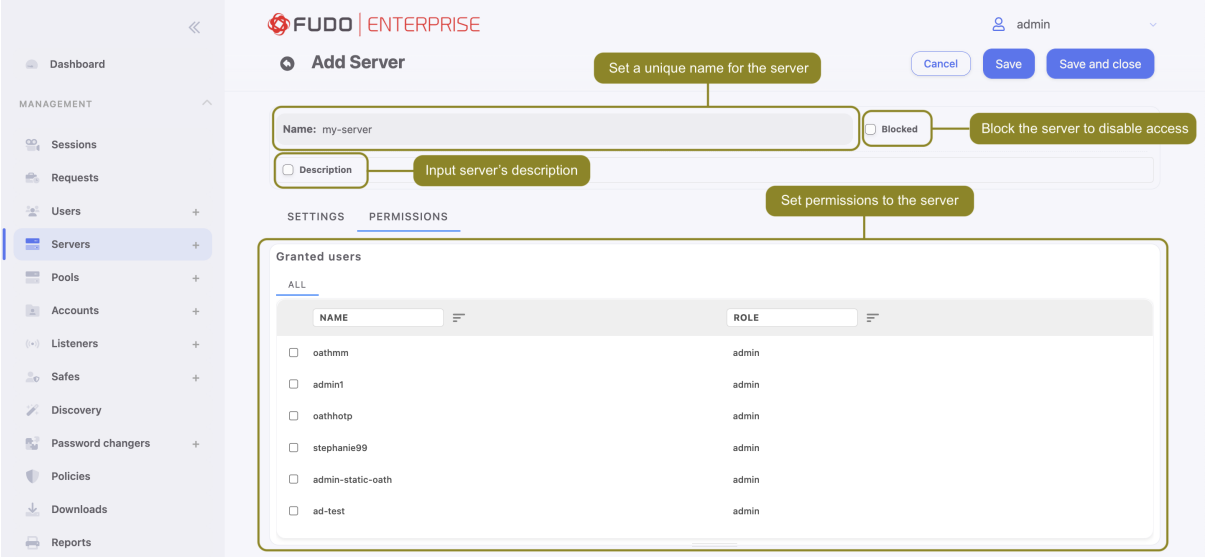
Note:

- 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 in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.
3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.
5. In the *Permissions* section, add users allowed to manage this object.



6. In the *Settings* section on the list of available protocols select `Telnet 3270` .

Warning: After server's definition is saved, protocol's field is uneditable.

7. Select the *TLS enabled* option to connect to monitored server over TLS.

- Select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.

8. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

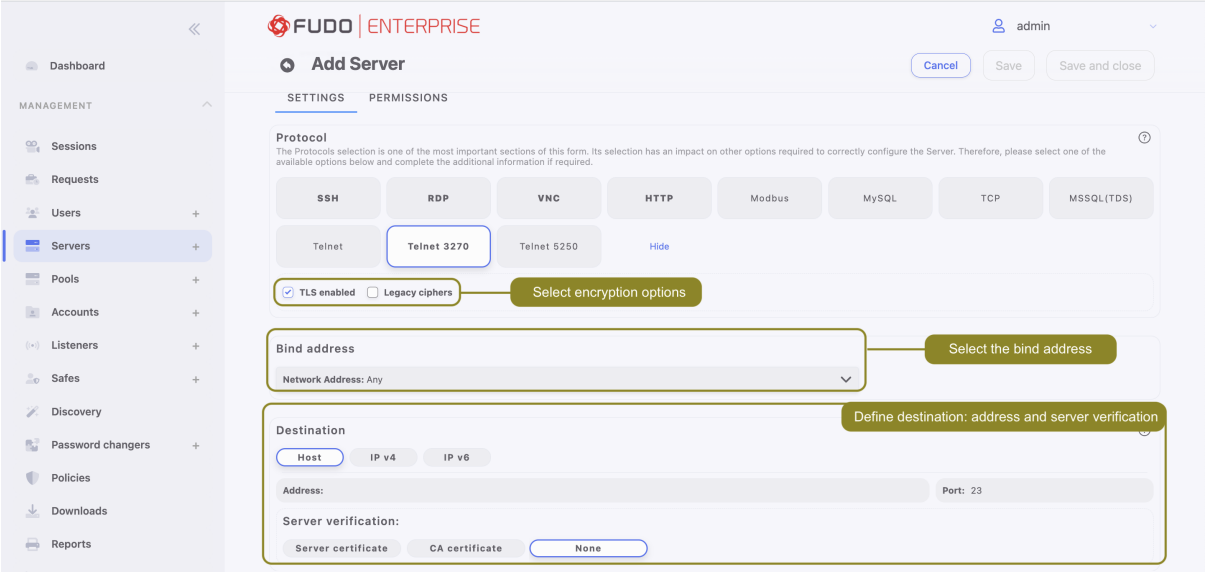
- The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make 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.

- 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.



10. Click *Save* or *Save and close*.

Related topics:

- *Pools*
- *Data model*
- *System initiation*

- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.1.9 Creating a Telnet 5250 server

Note:

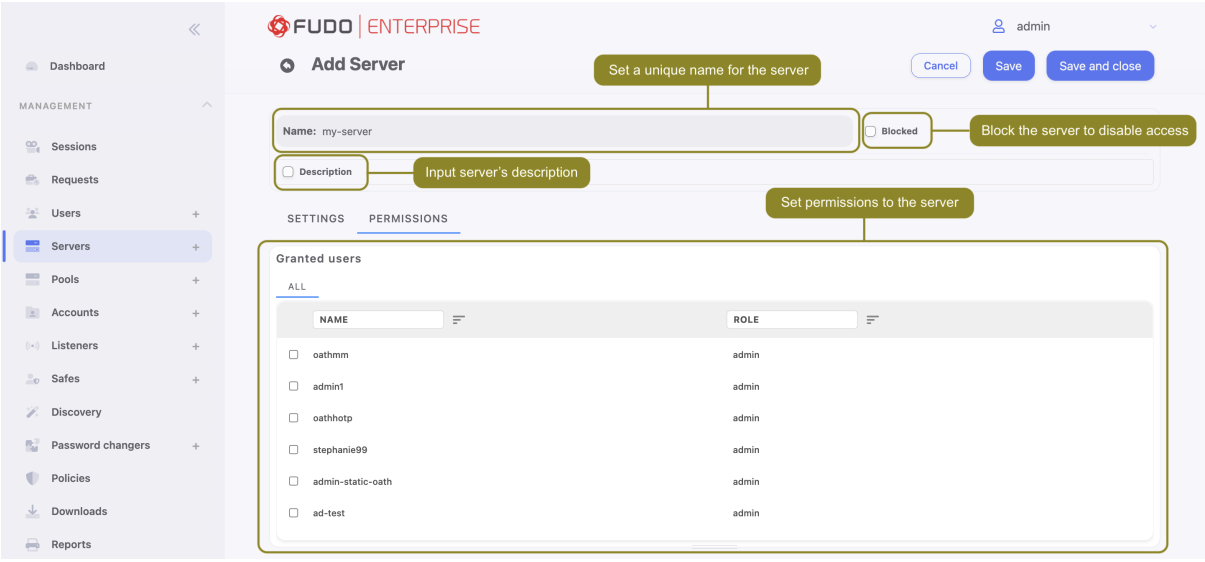
- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- In case of Telnet connections over *forward* and *regular* accounts, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise and then to connect to the target host.

---

1. Click + icon in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.
3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.
5. In the *Permissions* section, add users allowed to manage this object.



6. In the *Settings* section on the list of available protocols select `Telnet 5250` .

Warning:	After server's definition is saved, protocol's field is uneditable.

7. Select the *TLS enabled* option to connect to monitored server over TLS.

- Select *Legacy crypto* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.

8. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

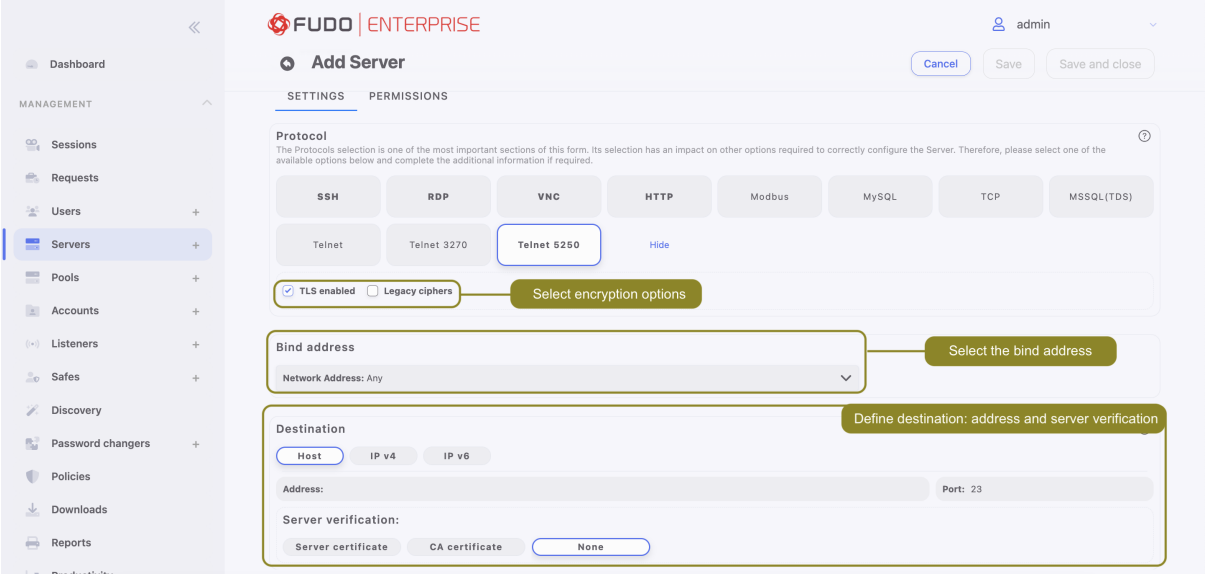
- The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network Interfaces Configuration*) or labeled IP addresses (*Labeled IP Addresses*).
- In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make 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.

- 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.



10. Click *Save* or *Save and close*.

Related topics:

- *Pools*
- *Data model*
- *System initiation*

- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.1.10 Creating a VNC server

Note:

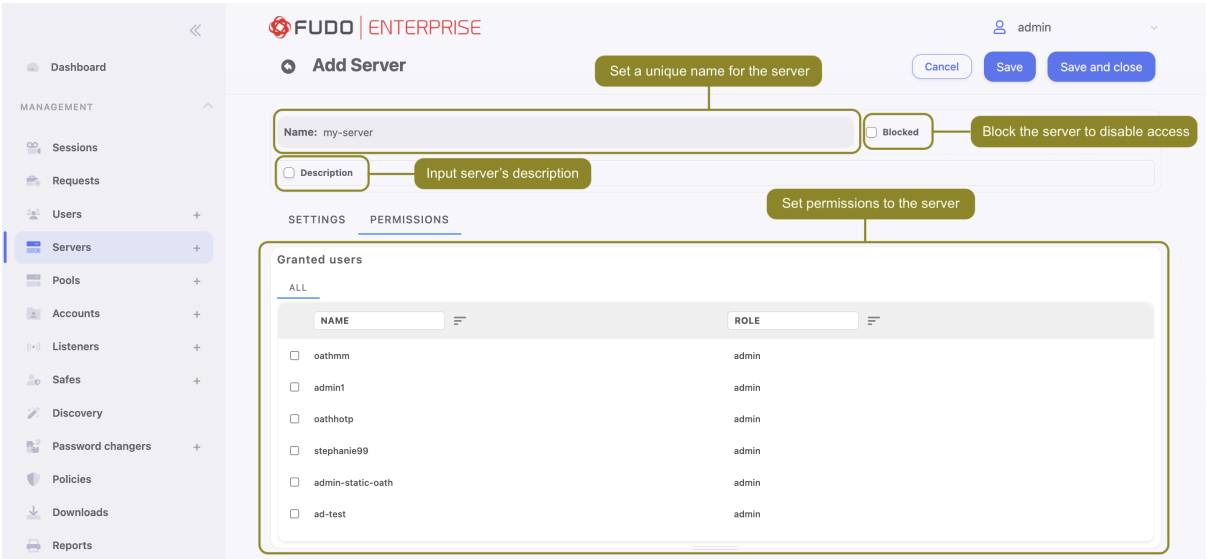
- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.

---

1. Click + icon in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.
3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.
5. In the *Permissions* section, add users allowed to manage this object.



6. In the *Settings* section on the list of available protocols select `VNC` .

Warning: After server's definition is saved, protocol's field is uneditable.

7. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

- The *Bind 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 *Bind 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.

8. 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.



9. Click *Save* or *Save and close*.

Related topics:

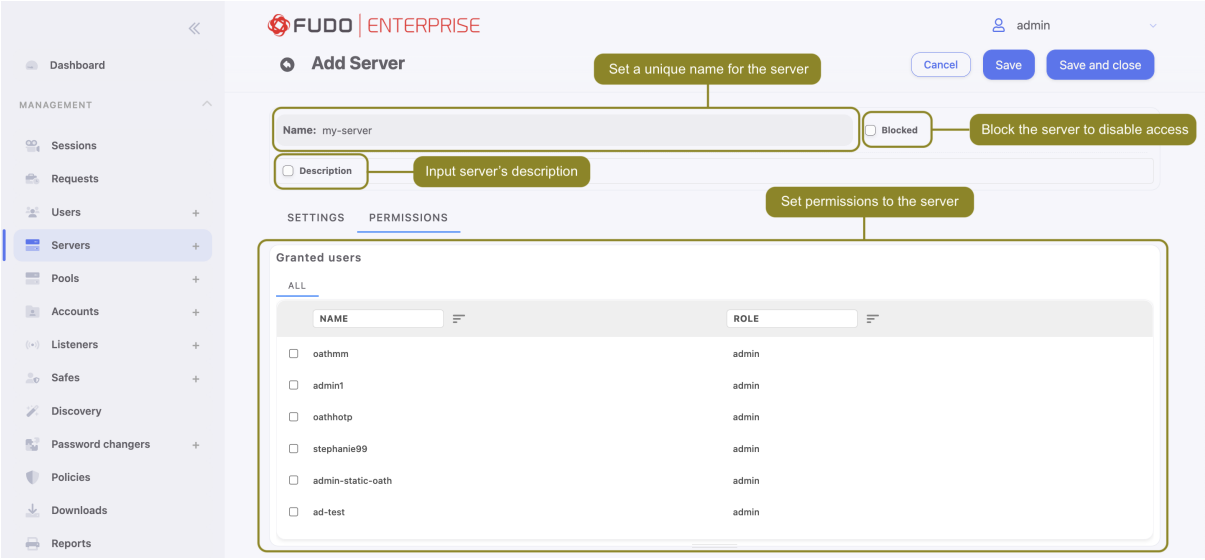
- *Pools*
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.1.11 Creating a TCP server

1. Click + icon in the main menu next to the *Servers* tab, or

Select *Management* > *Servers* and then click + *Add server*.

2. Enter server's unique name.
3. Select *Blocked* option to disable access to server after it's created.
4. Optionally, click the *Description* checkbox and provide a text that will help identifying this server object.
5. In the *Permissions* section, add users allowed to manage this object.



6. In the *Settings* section on the list of available protocols select `TCP` .

Warning: After server's definition is saved, protocol's field is uneditable.

7. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

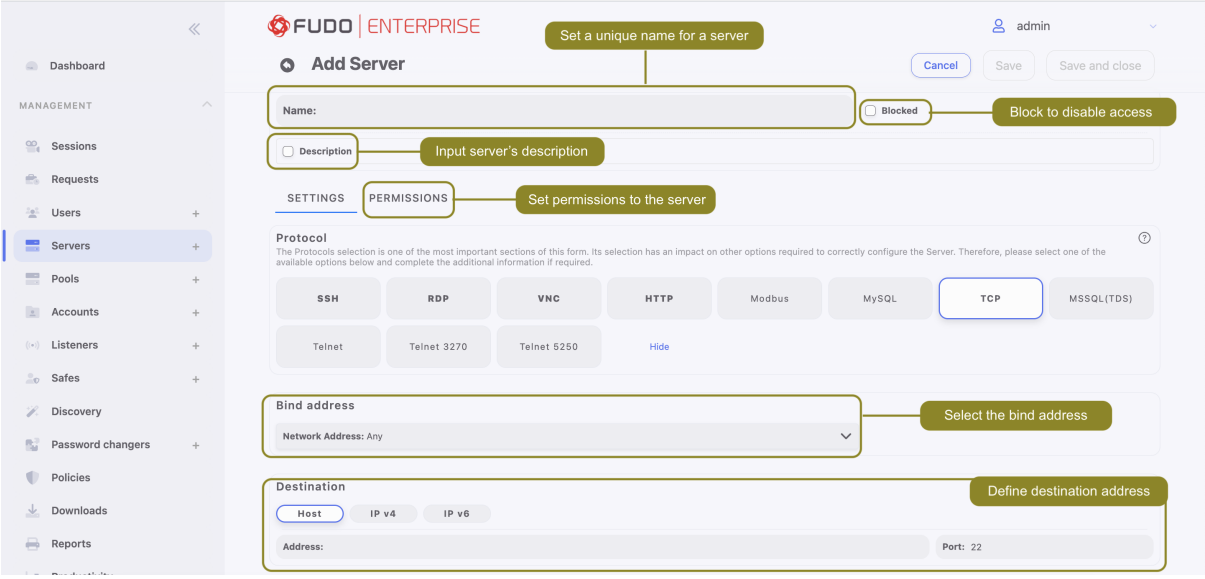
Note:

- The *Bind 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 *Bind 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.

8. 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.



9. Click *Save* or *Save and close*.

Related topics:

- *Pools*
- *TCP*
- *Data model*
- *Setting up the TCP listener*

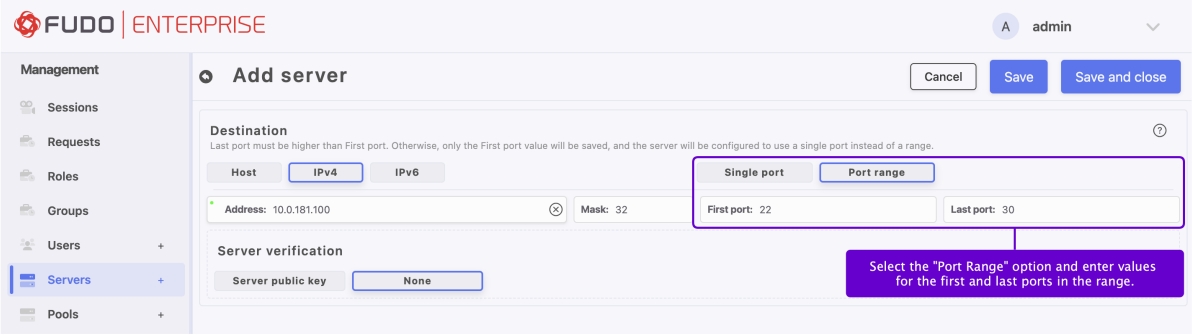
9.2 Port Ranges in Server Configuration

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.

9.2.1 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.

9.2.2 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.

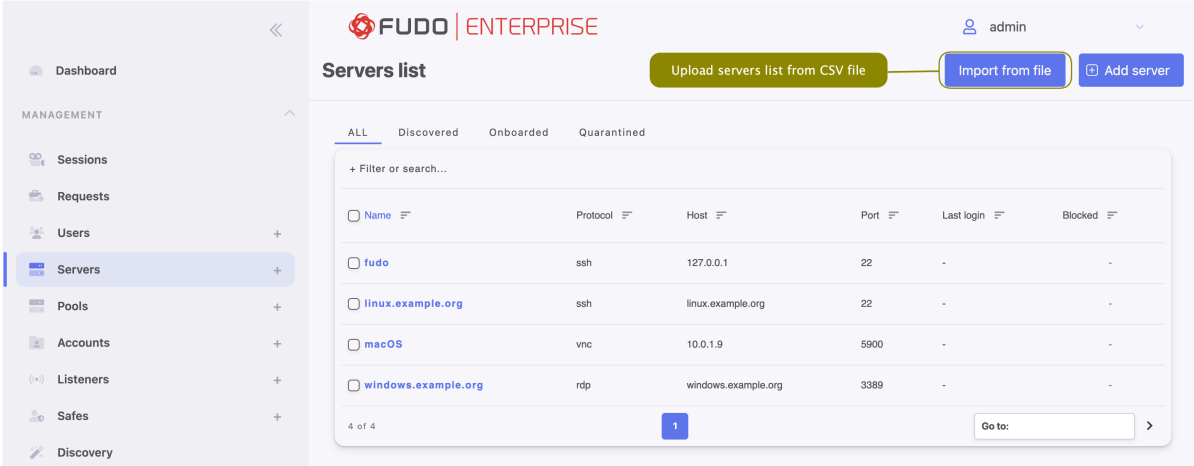
Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*

- *Safes*
- *Accounts*

9.3 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:

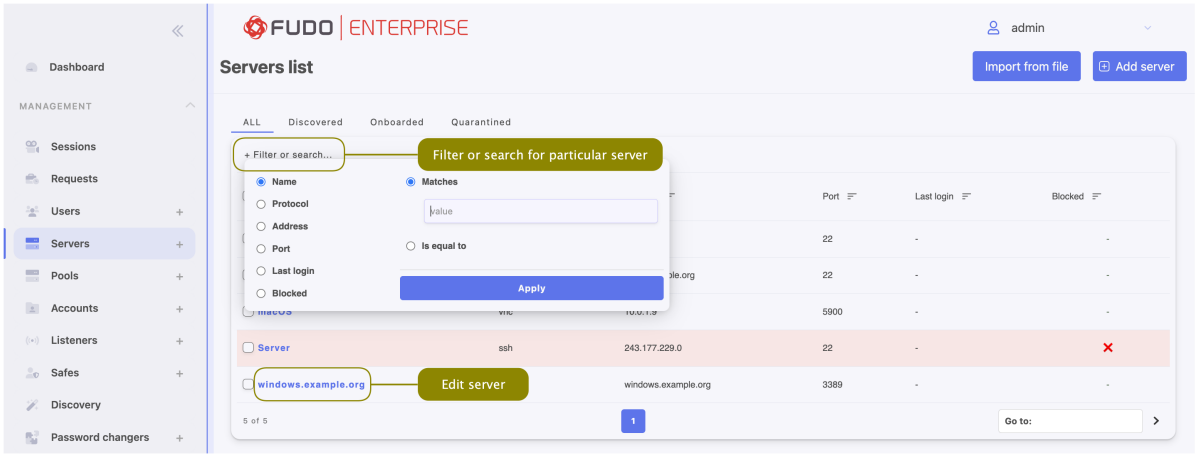
- the `port` column filled in for a server with a single port,
- the `port_first` and `port_last` columns filled in for a server with a port range.

Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.4 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*

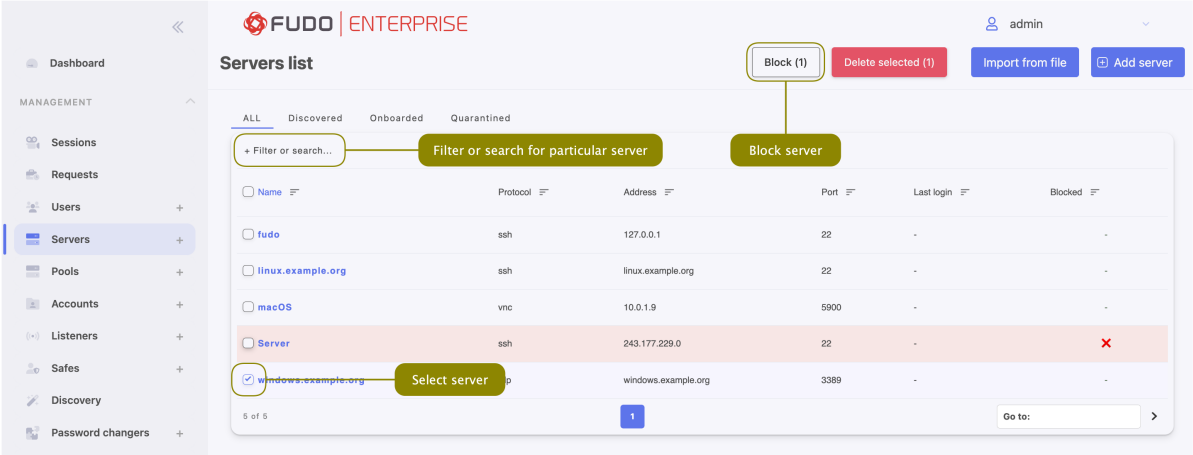
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

9.5 Blocking a server

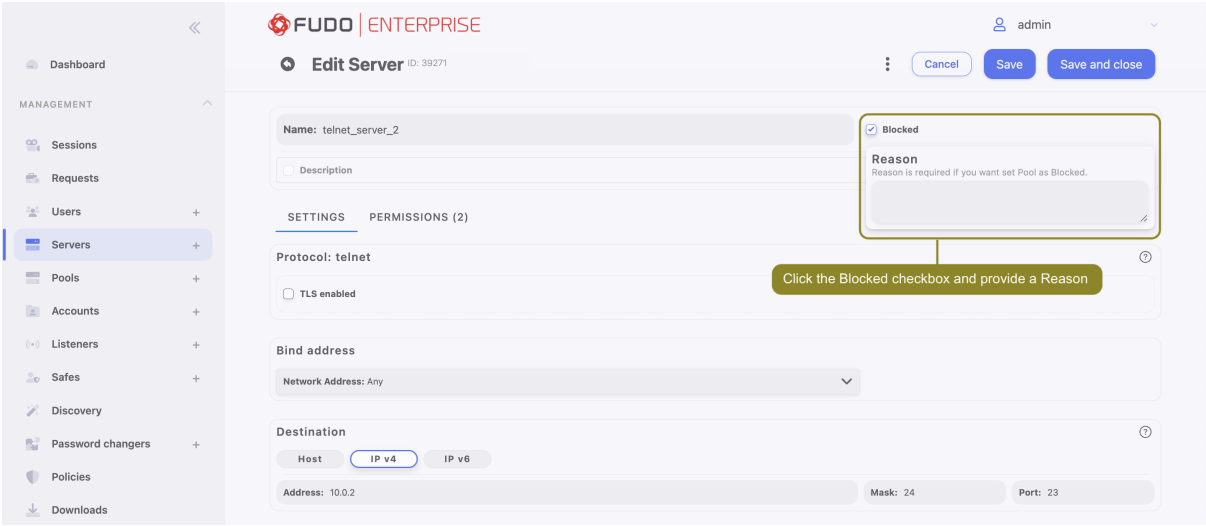
Fudo Enterprise allows blocking access to given server for all users.

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.

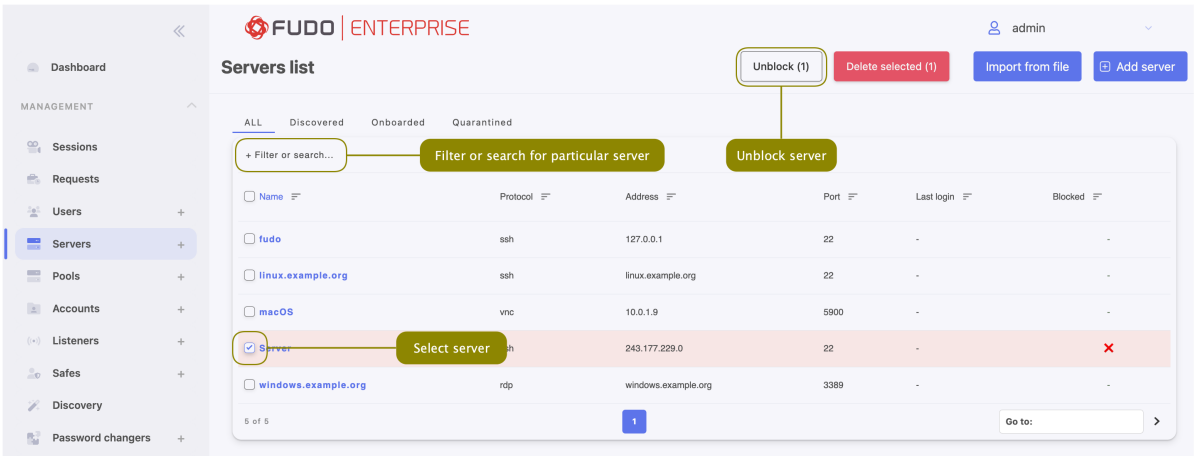


Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

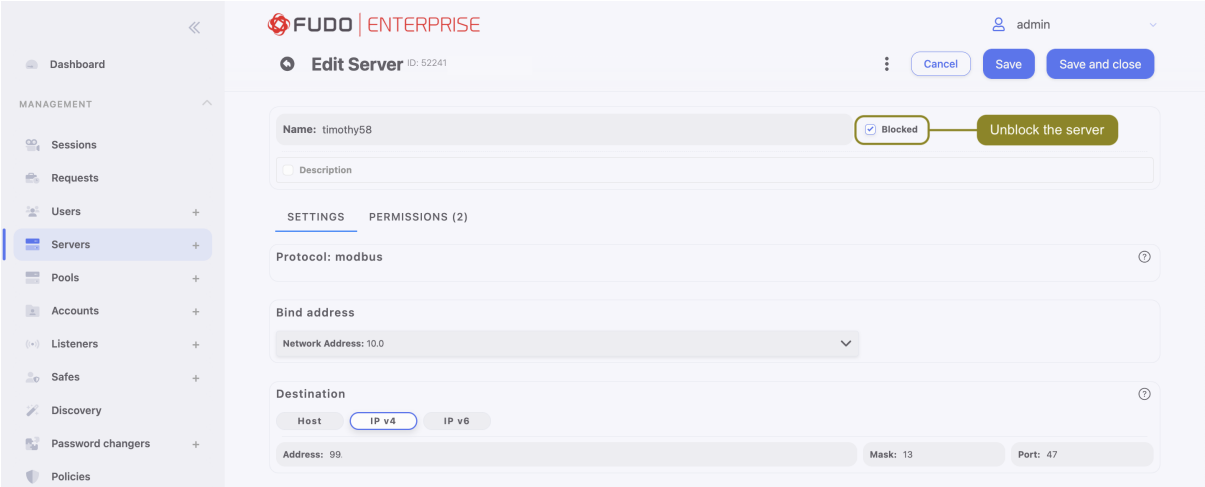
9.6 Unblocking a server

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.



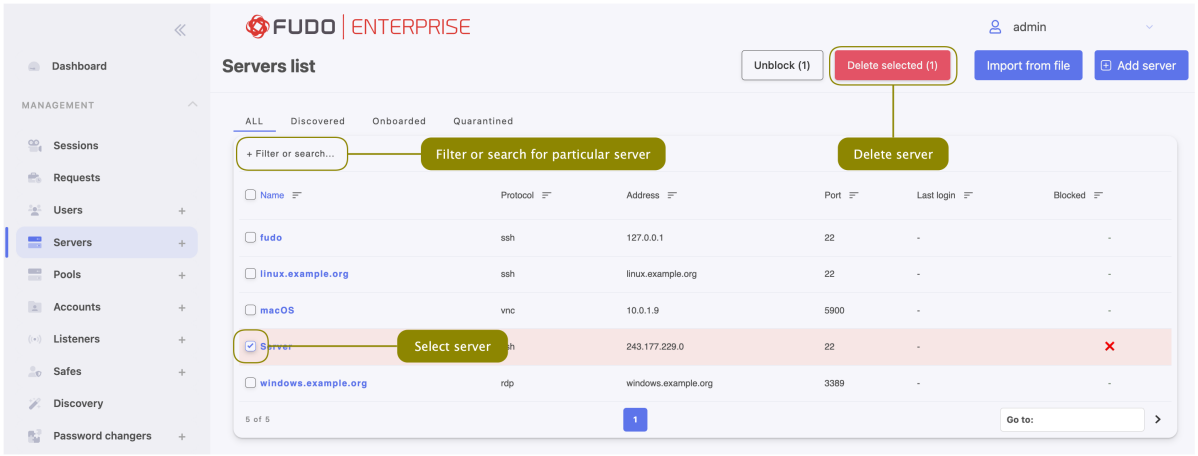
Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

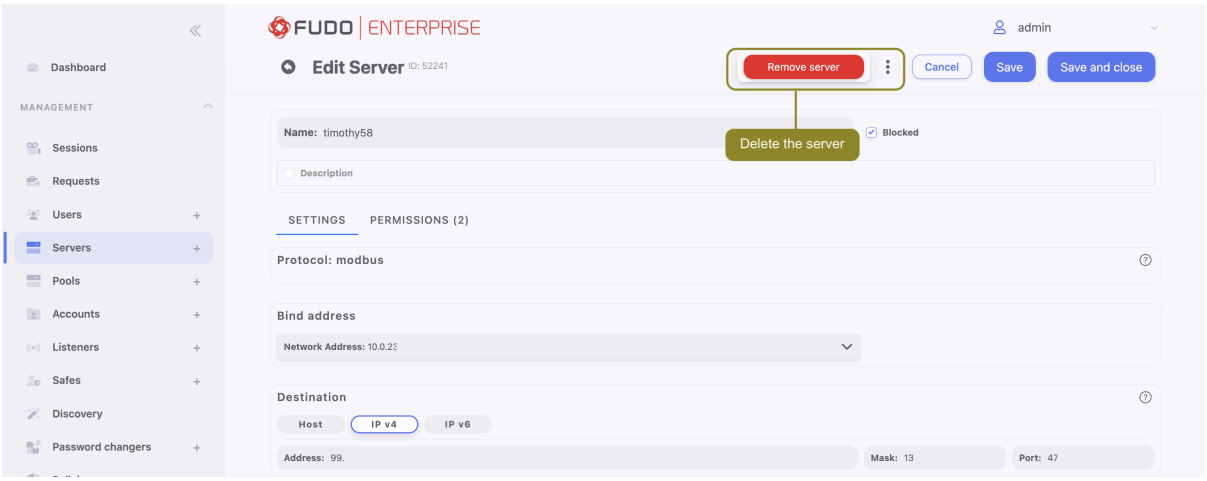
9.7 Deleting a server

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*.



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.

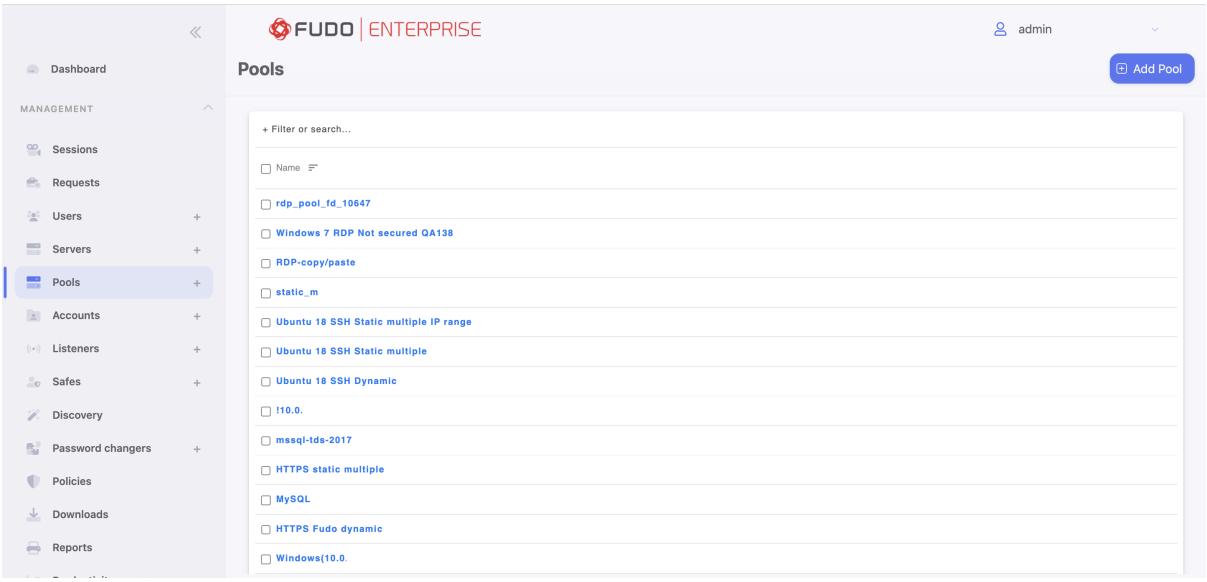
Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

CHAPTER 10

Pools

Server Pools allow grouping multiple server objects based on the same protocol and manage within other objects (for example, accounts) as one server.



10.1 Creating a pool

In order to create a pool, follow the instructions:

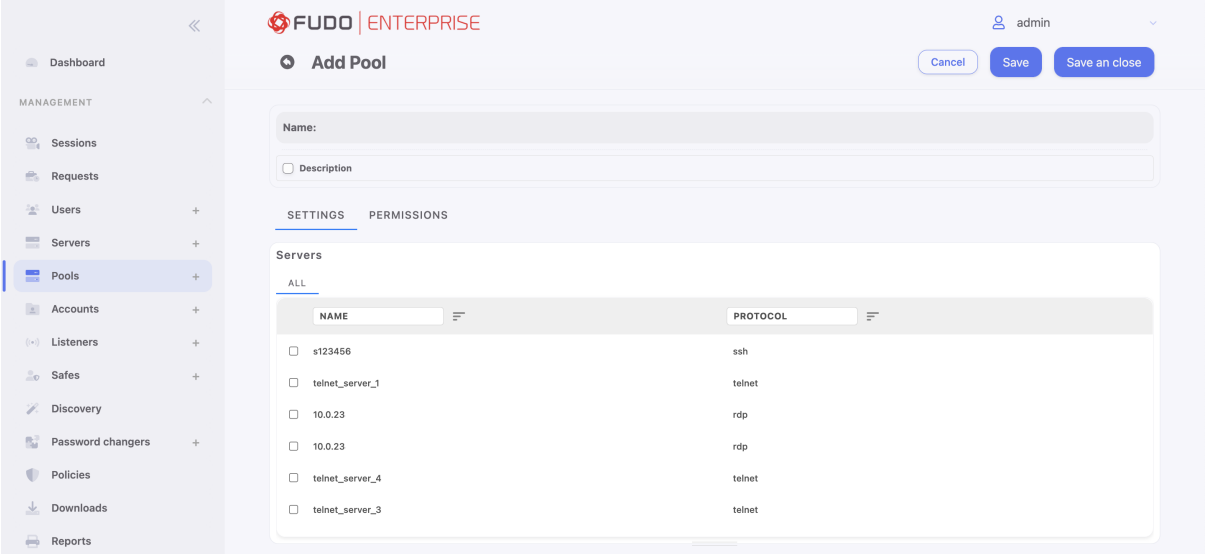
1. Click + icon in the main menu next to the *Pools* tab, or

Select *Management* > *Servers* and then click + *Add pool*.

2. Enter pool's unique name.
3. Optionally, click the *Description* checkbox and provide a text that will help identifying this pool object.

4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Settings* section select servers to be added to the pool.

Note: Protocol of the servers in terms of group should be unique.



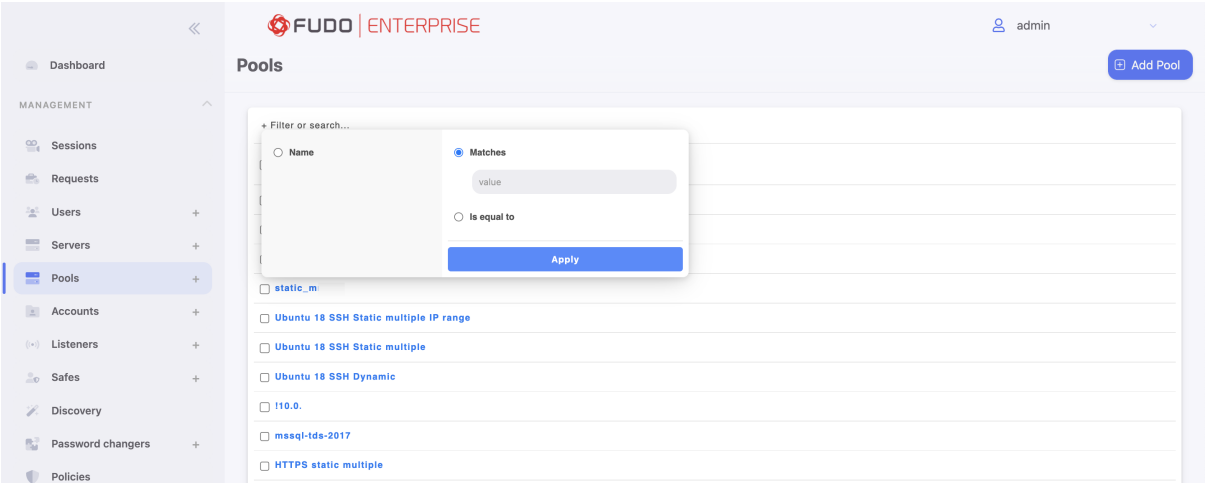
6. Click *Save* or *Save and close*.

10.2 Deleting a pool

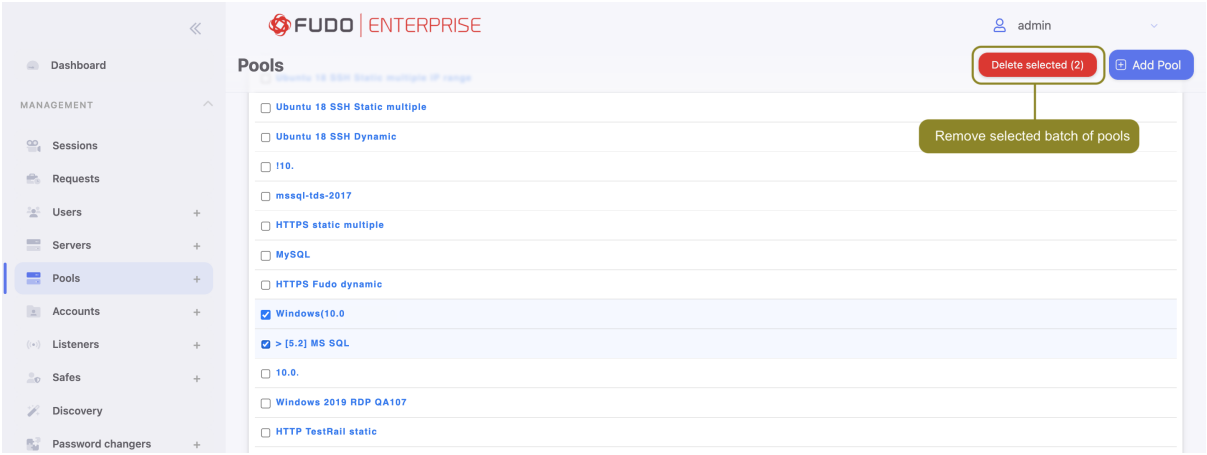
Warning: A pool can't be deleted if assigned to an account.

In order to delete a pool, follow the instructions:

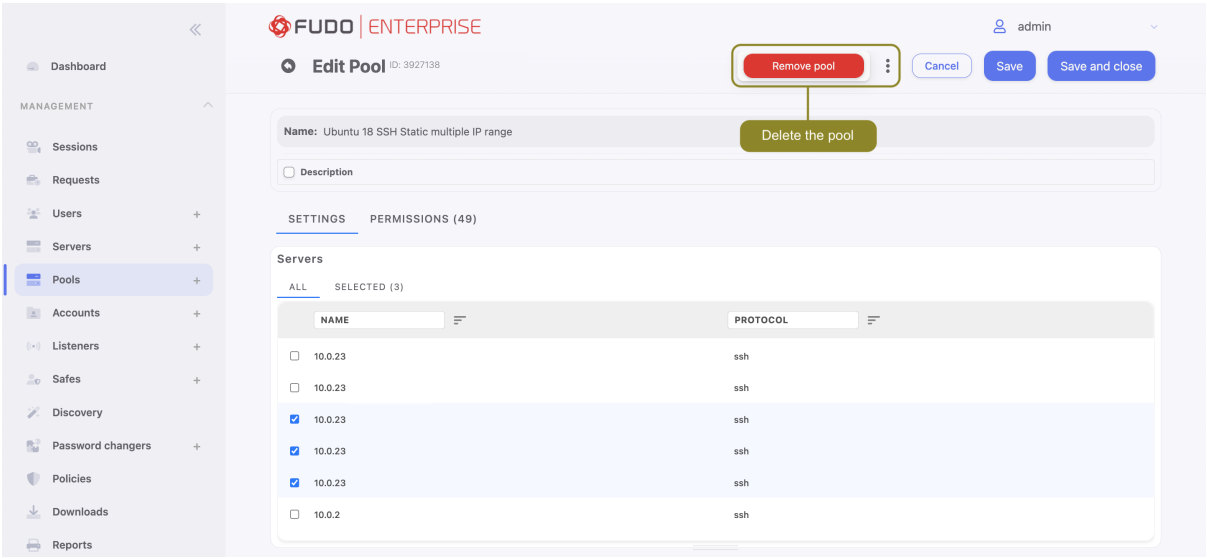
1. Select *Management* > *Pools*.
2. Define filters to limit the number of objects displayed on the list:



3. Use checkboxes next to the pool(s) and click *Delete selected*.



Alternatively, select a pool that needs to be deleted right from the list and click on the vertical three-dot icon:



4. Confirm pool(s) deleting.

Related topics:

- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

CHAPTER 11

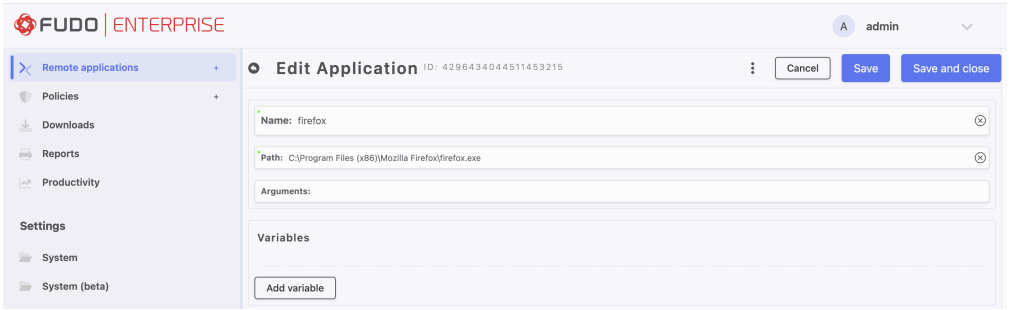
Remote Applications

Fudo Enterprise enables direct connection over the RDP protocol to a remote application using Remote Applications feature.

11.1 Adding Remote Application

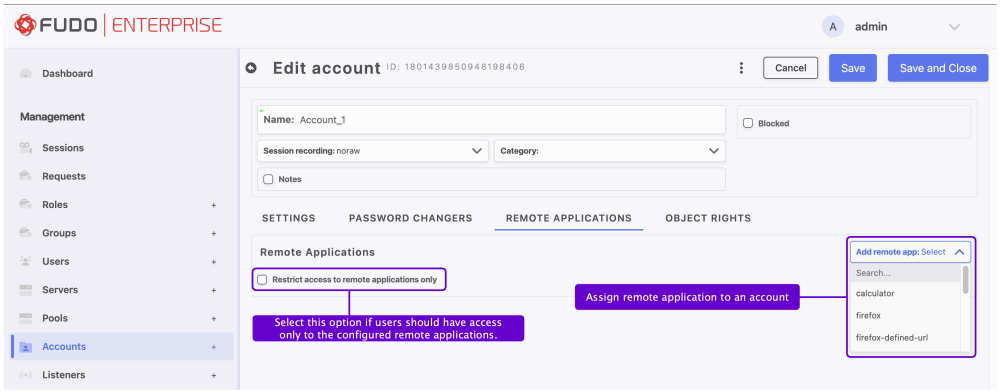
In order to configure a remote application, follow the instruction:

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.



11.2 Adding Arguments

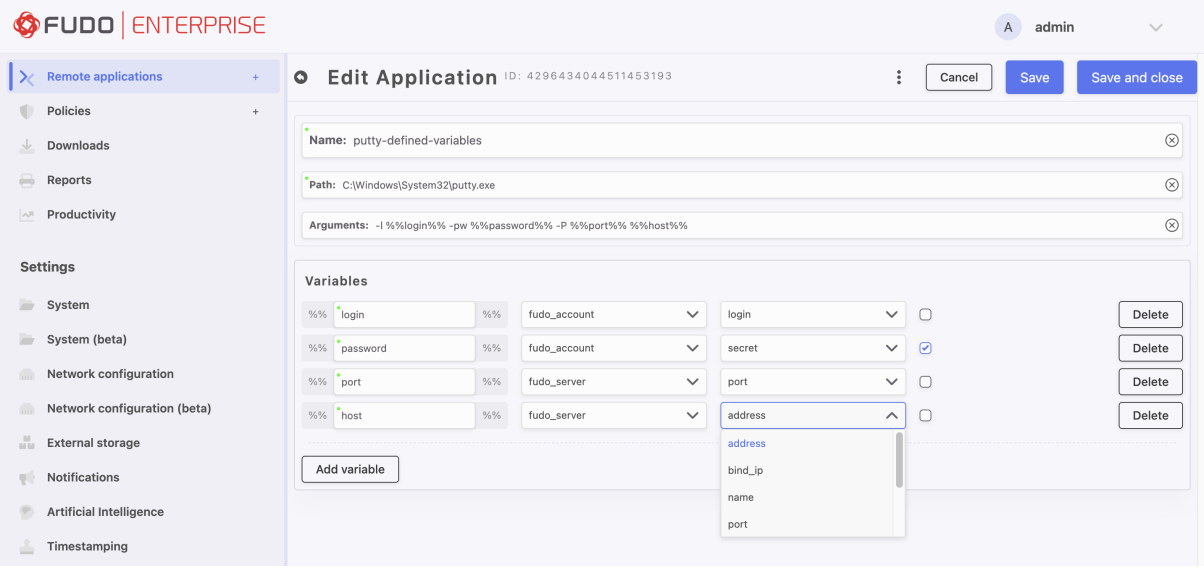
Remote Applications allow administrators to set commands that execute automatically at launch, enabling seamless connections with pre-filled login credentials and connection details. Variables can also be created to retrieve data directly from the Fudo Enterprise configuration.

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%%`.

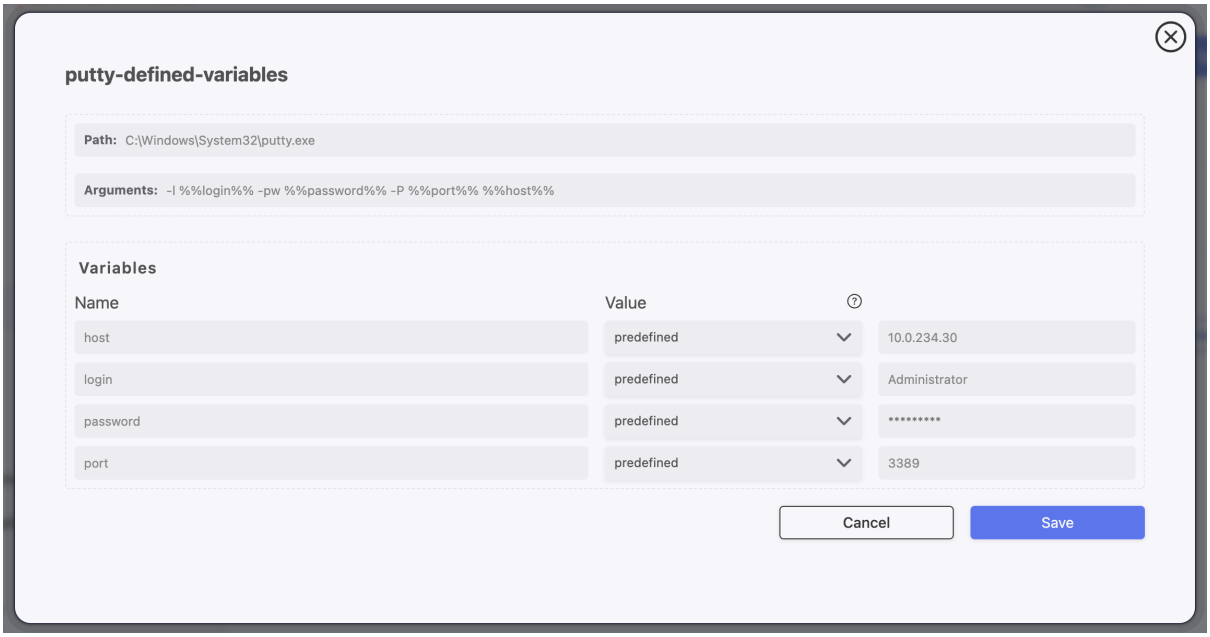
Note: When defining variable you can decide which object and what property of object to use. You can select *Object type* and *Object property* for each of your Arguments, and encrypt given arguments by selecting the checkbox *Encrypt* in the row following the variable name.

---

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.



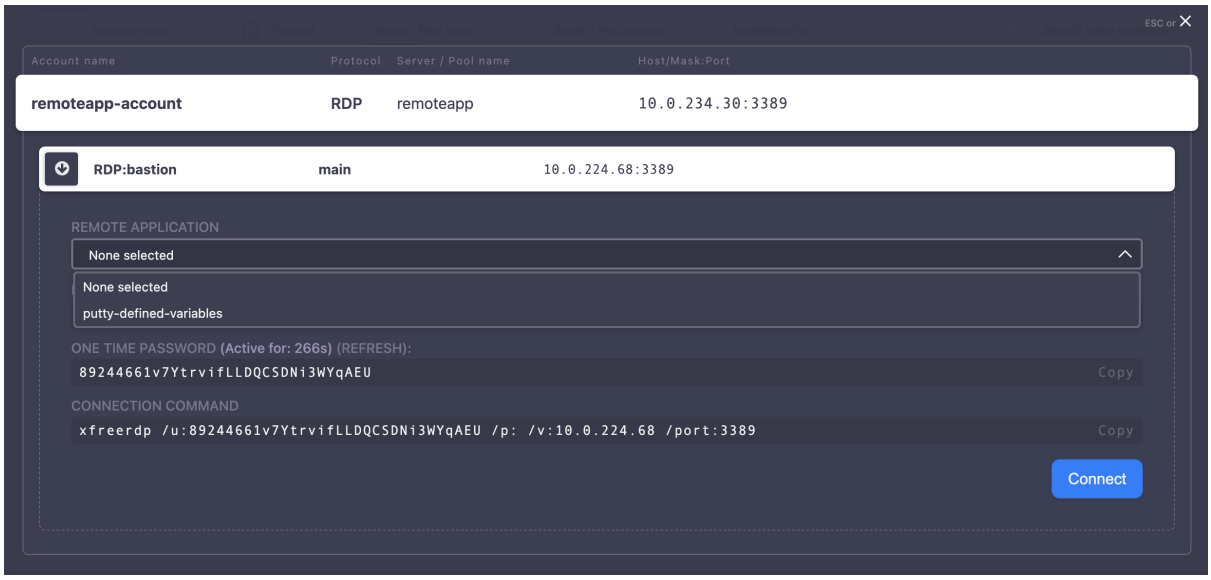
Descriptions of Available Object Types

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

11.3 Connecting to Remote Application via Access Gateway

In order to establish a connection, sign in to the 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*.



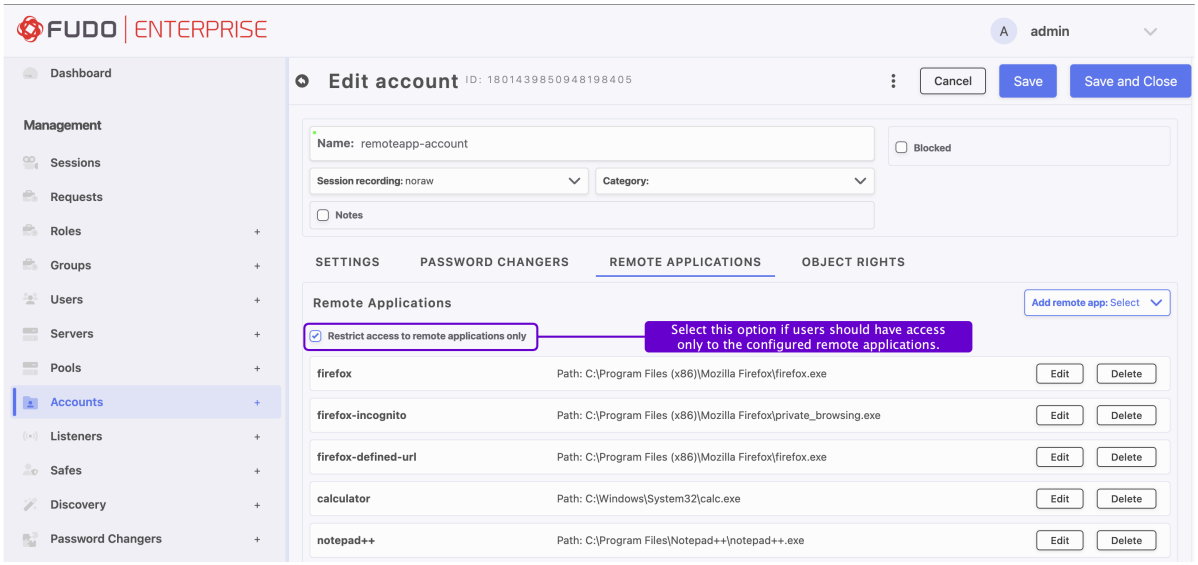
When a session to the specific resource is established by a user, their remote session is connected within the application only. Therefore, the user has no access to the entire desktop, and closing the application terminates the session.

11.4 Granular Access to Remote Applications

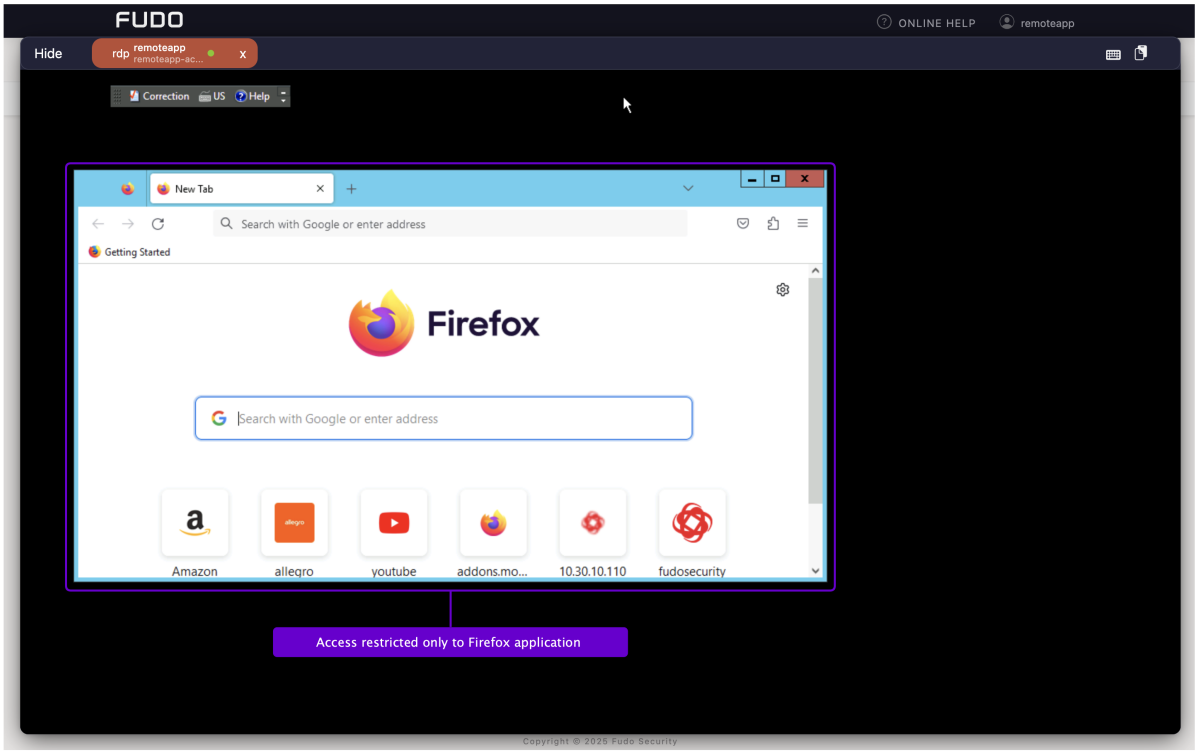
To improve access control and reduce surface exposure, security admins can restrict users to specific remote applications without granting access to the full desktop environment. This enhancement enables more precise permission management and helps ensure that users interact only with the resources necessary 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.



11.5 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:

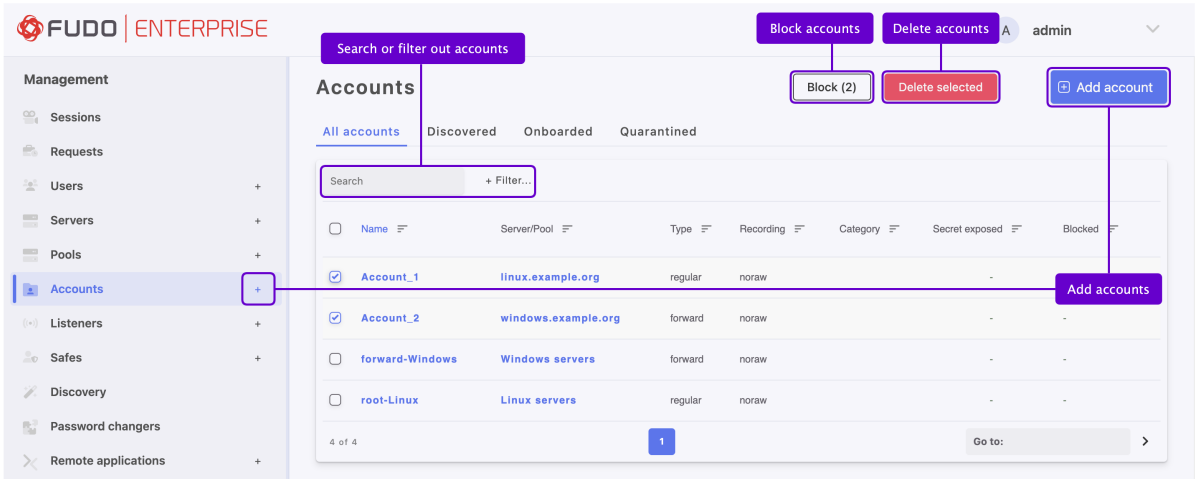
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*
- *Creating an account*

CHAPTER 12

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); password changing policy as well as the password 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.



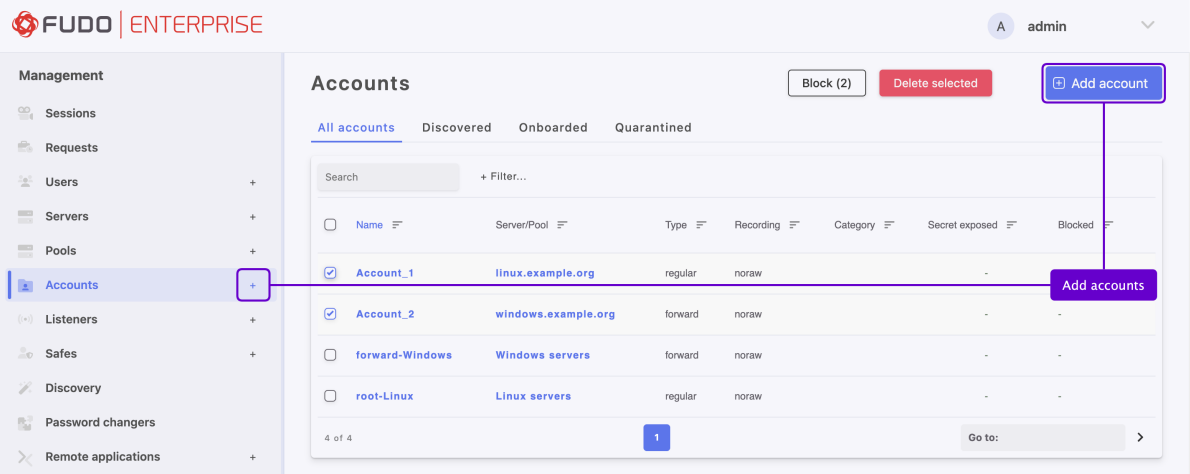
12.1 Creating an account

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.

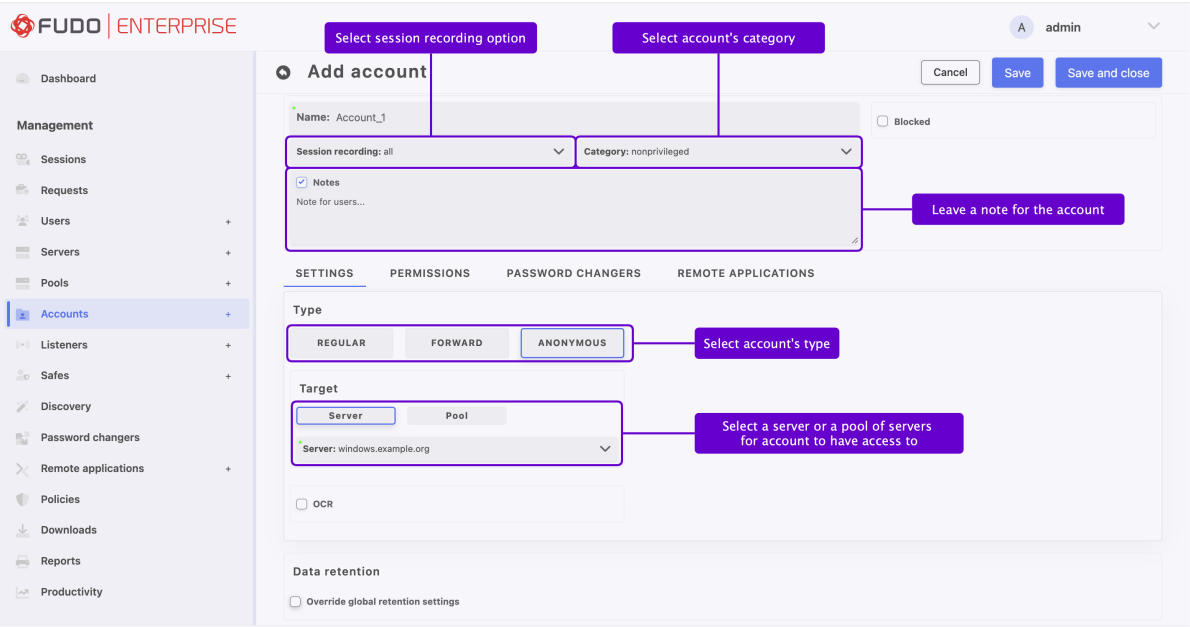
12.1.1 Creating an *anonymous* account

To create an account definition, follow the instructions below.

1. Click + icon next to the *Accounts* tab of the *Management* sub-section, or
2. Select *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).

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*.



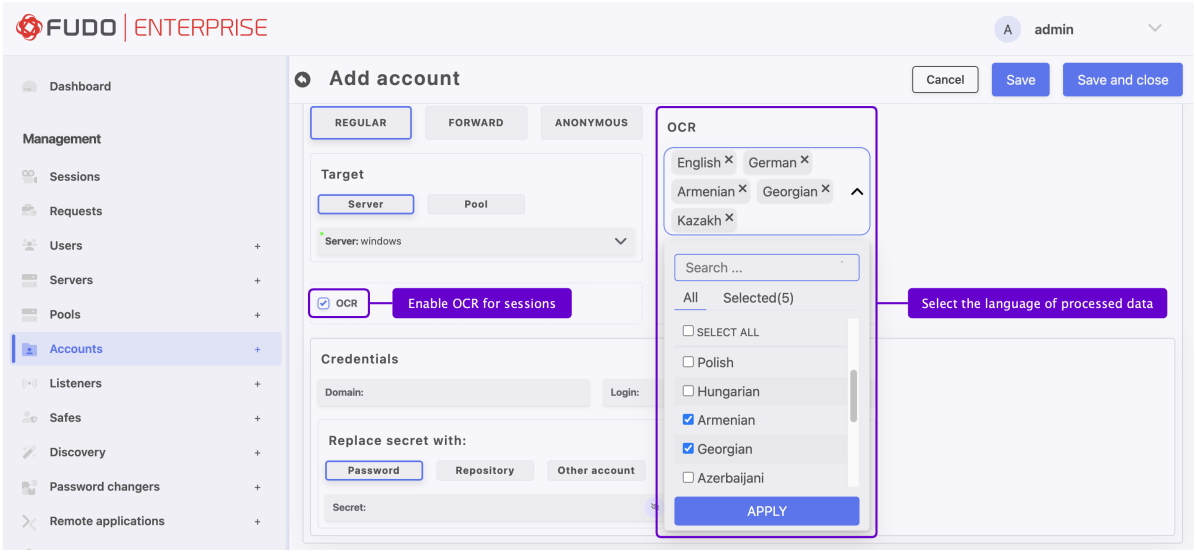
---

8. In the *Settings* tab, in the Type field, press the *ANONYMOUS* button.
9. 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.
10. 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.

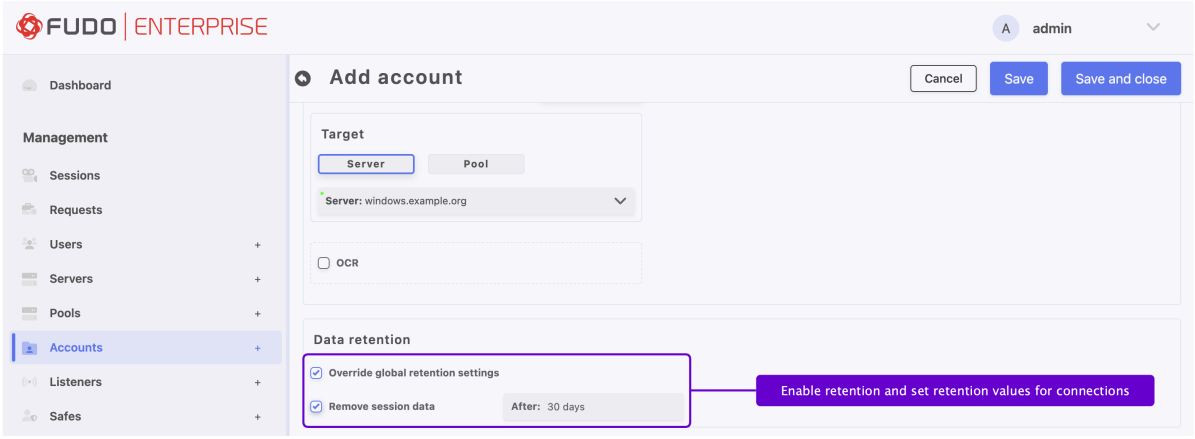
---

11. 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.

12. 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*.

13. Click *Save* to proceed with further configuration.
14. Go to the *Permissions* tab to add users allowed to manage this object.

15. Click *Save*.

Note: The *Password changers* tab and the *Remote applications* tab are active only when creating regular or forward account types.

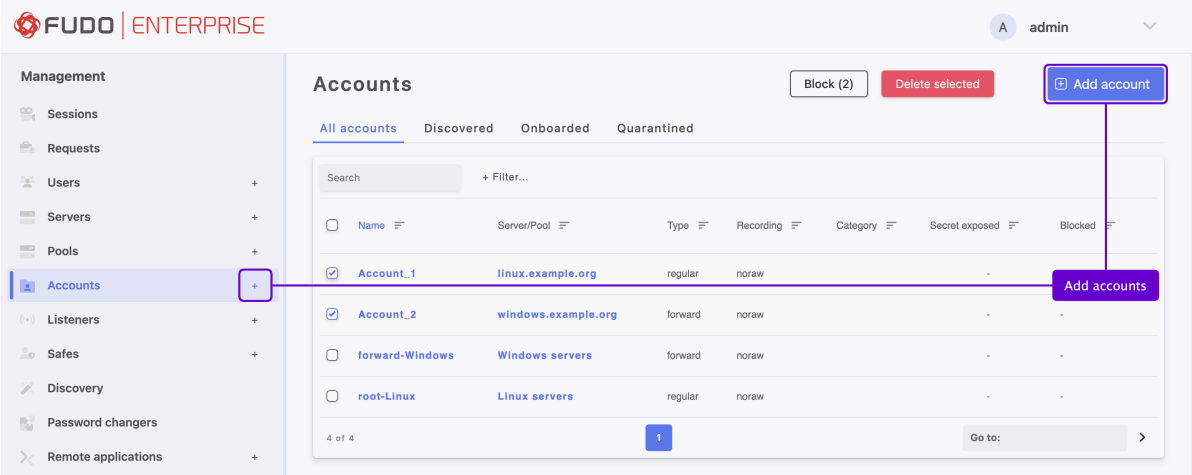
Related topics:

- *Data model*
- *Deleting an account*
- *Editing an account*
- *Unblocking an account*
- *Blocking an account*

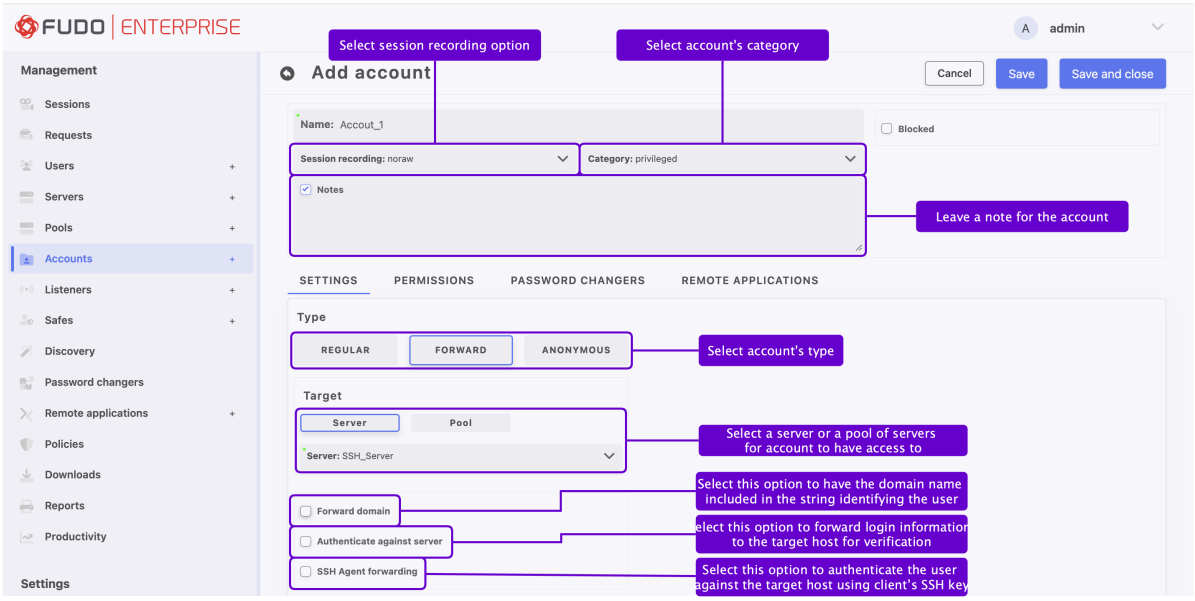
12.1.2 Creating a *forward* account

To create an account definition, follow the instructions below.

1. Click + icon next to the *Accounts* tab of the *Management* sub-section, or
2. Select *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).

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*.



8. In the *Settings* tab, in the *Type* field, press the *FORWARD* button.
9. 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.
10. 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.

---

11. 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 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.

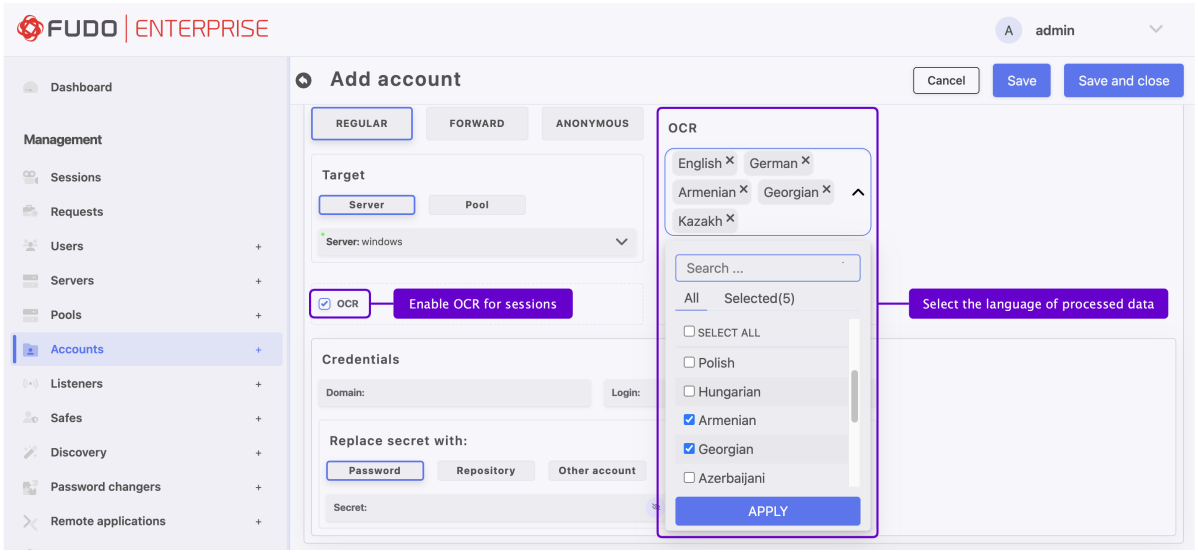
---

12. 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.

13. 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.

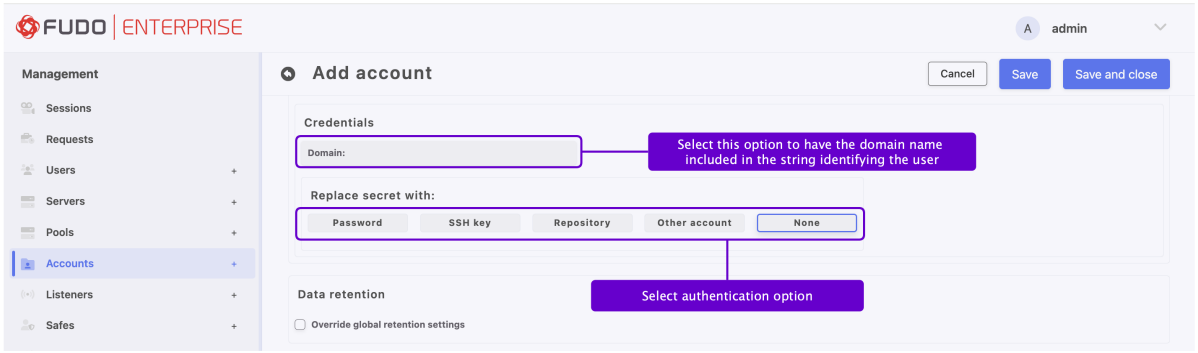


Note: The *OCR* option is available only after selecting an RDP, VNC or HTTP server.

14. In the *Credentials* section, 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.

15. In the *Replace secret with* section, click the button corresponding to one of the desired options.



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.

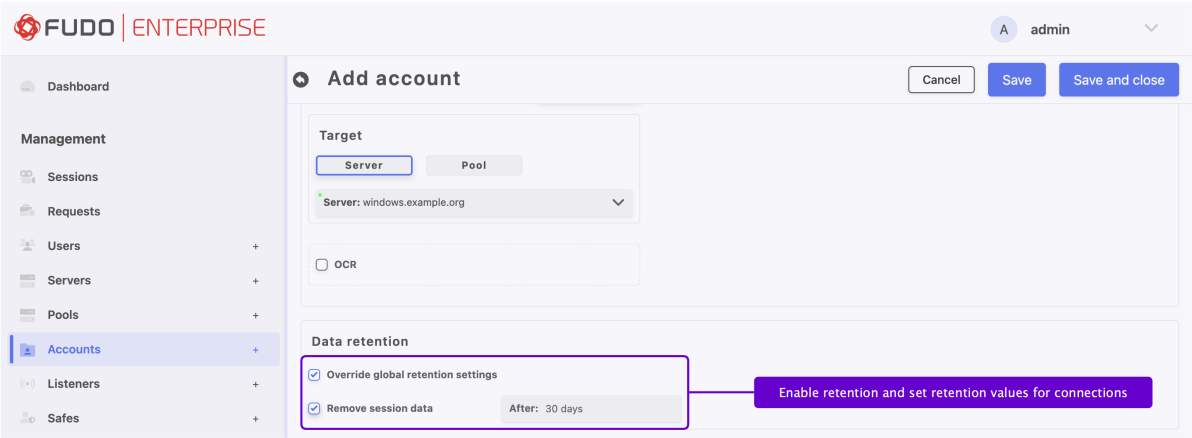
Note: The list contains only objects to which you have been given access permissions.

None

- In this case no credentials will be forwarded.

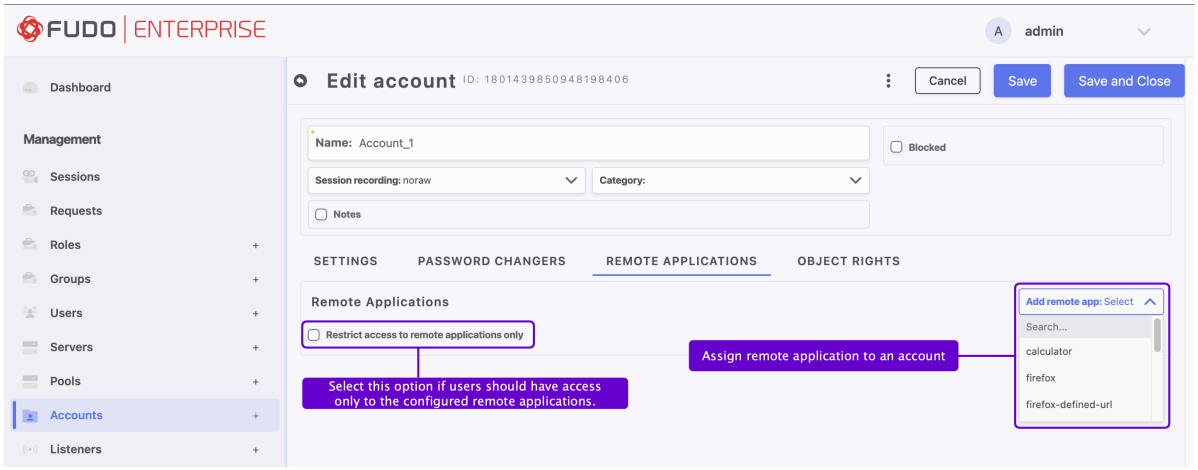
16. In the *Data retention* section, define automatic data removal settings.

- 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.



17. Go to the *Permissions* tab to add users allowed to manage this object.

18. Go to the *Remote applications* tab to 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.
- The *Password changers* tab is active only when creating regular account types.

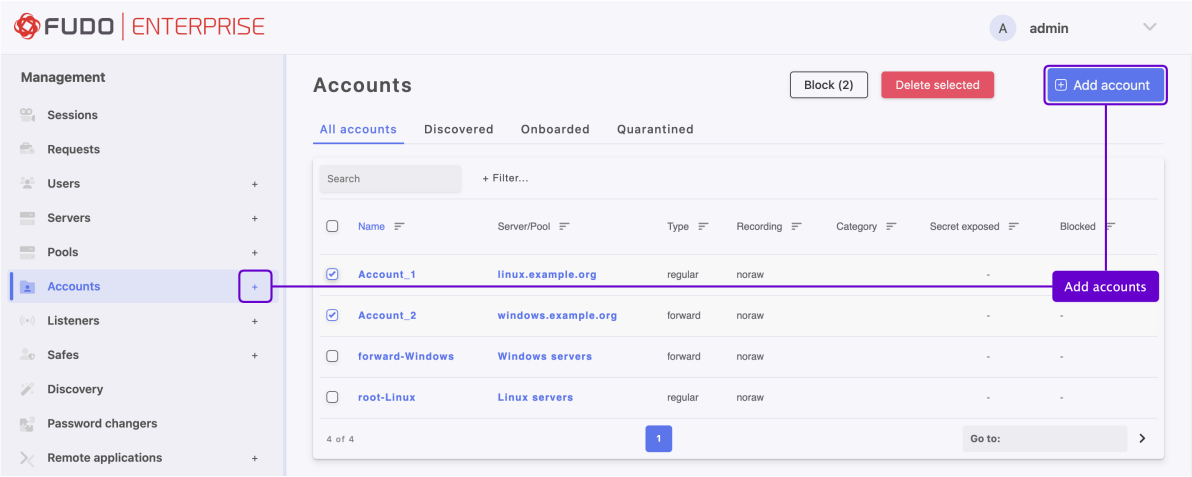
Related topics:

- *Data model*
- *Deleting an account*
- *Editing an account*
- *Unblocking an account*
- *Blocking an account*

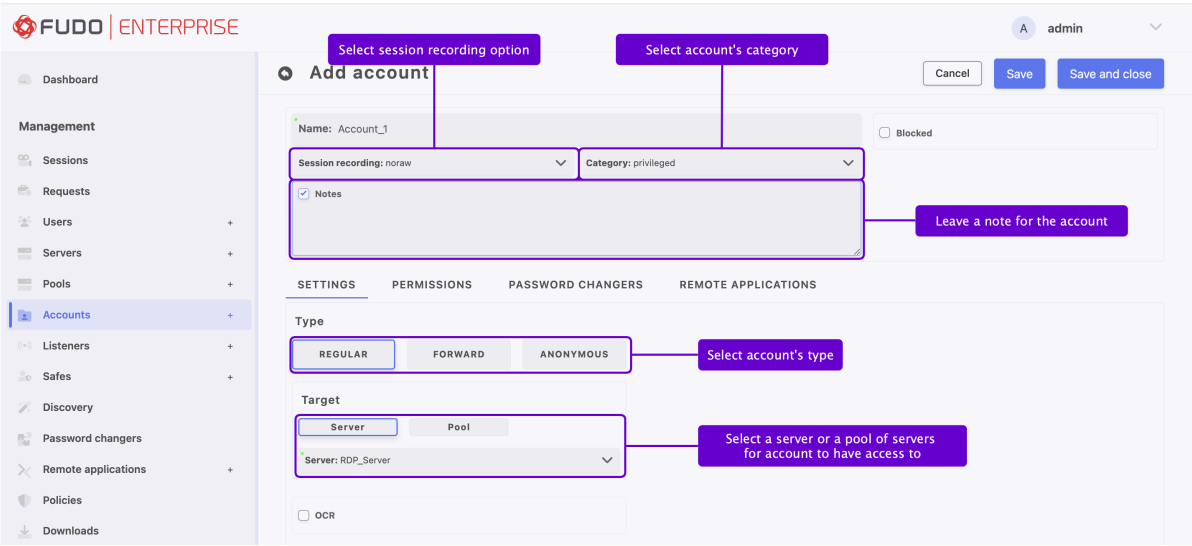
12.1.3 Creating a *regular* account

To create an account definition, follow the instructions below.

1. Click + icon next to the *Accounts* tab of the *Management* sub-section, or
2. Select *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).

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*.



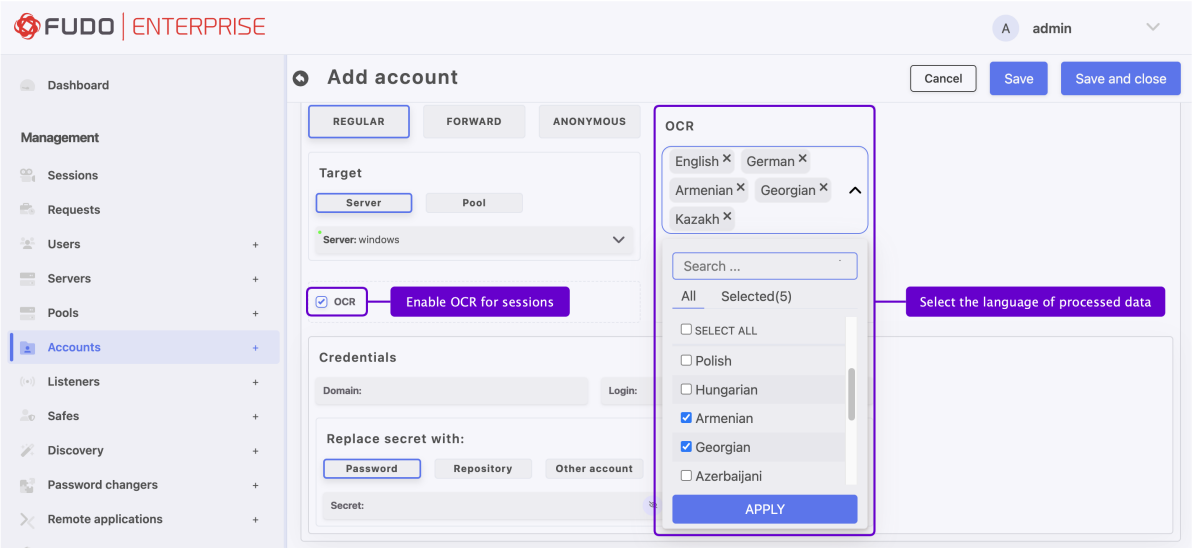
---

8. In the *Settings* tab, in the *Type* field, press the *REGULAR* button.
9. 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.
10. 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.

---

11. 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.

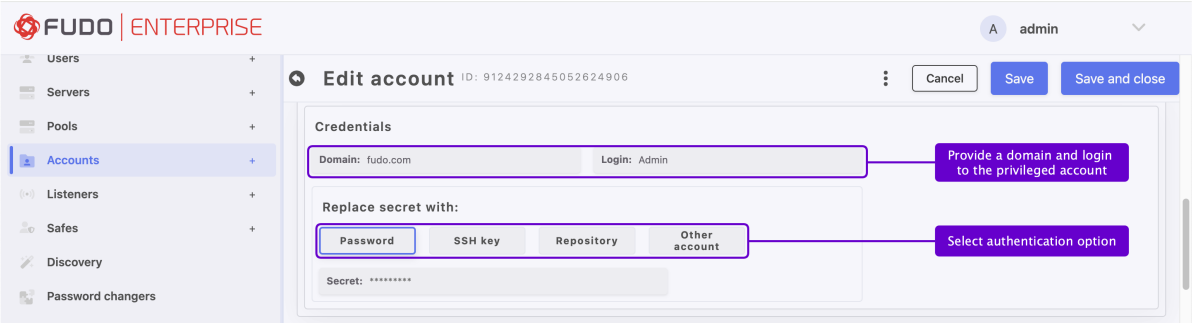
12. In the *Credentials* section, enter privileged account domain.

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.

13. 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).

14. In the *Replace secret with* section, click the button corresponding to one of the desired options.



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.

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.

---

14. If Password option was chosen as an authentication method, provide additional configuration in the *Password changers* tab. Otherwise, continue to step 28 of this manual.

Note: The *Password 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.

---

15. Select *Password change policy* from the list of the configured password change policies.
16. 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.

---

17. Select *Change password 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*.

---

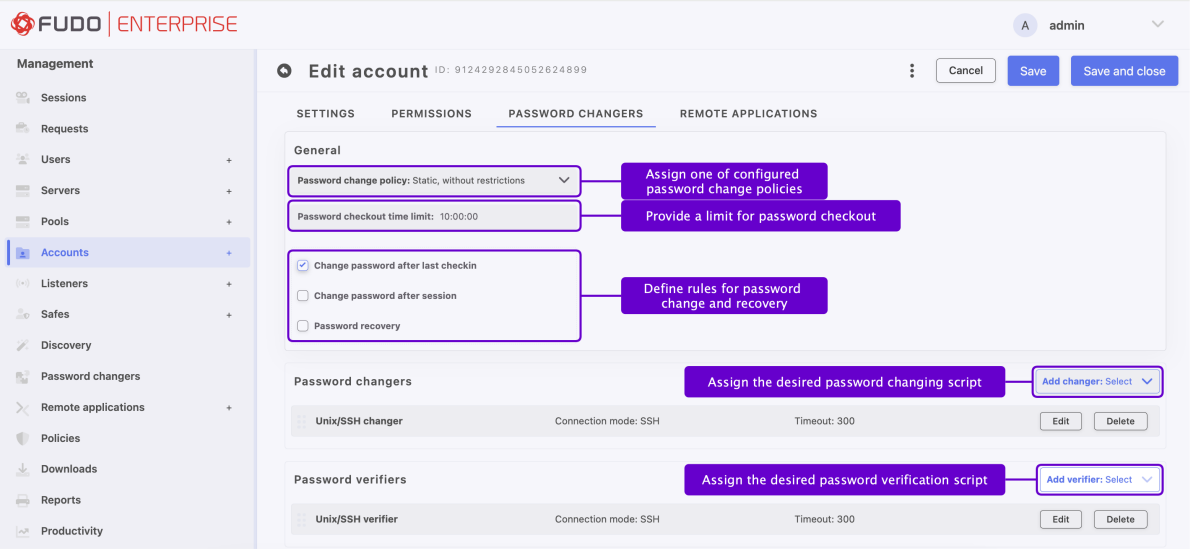
18. Select *Change password after session* option to change the account password remotely after the session is ended.

Note: This option requires to choose at least one *Password changer* and a *Password change policy* any other than `Static, without restrictions`.

Refer to the *Password changers* topic for detailed information on setting up password changers.

19. Check the *Password recovery* option to set a password verifier, to automatically trigger a password changer if it verifies that the password for an Account was changed and a new password is not stored in Fudo Enterprise.

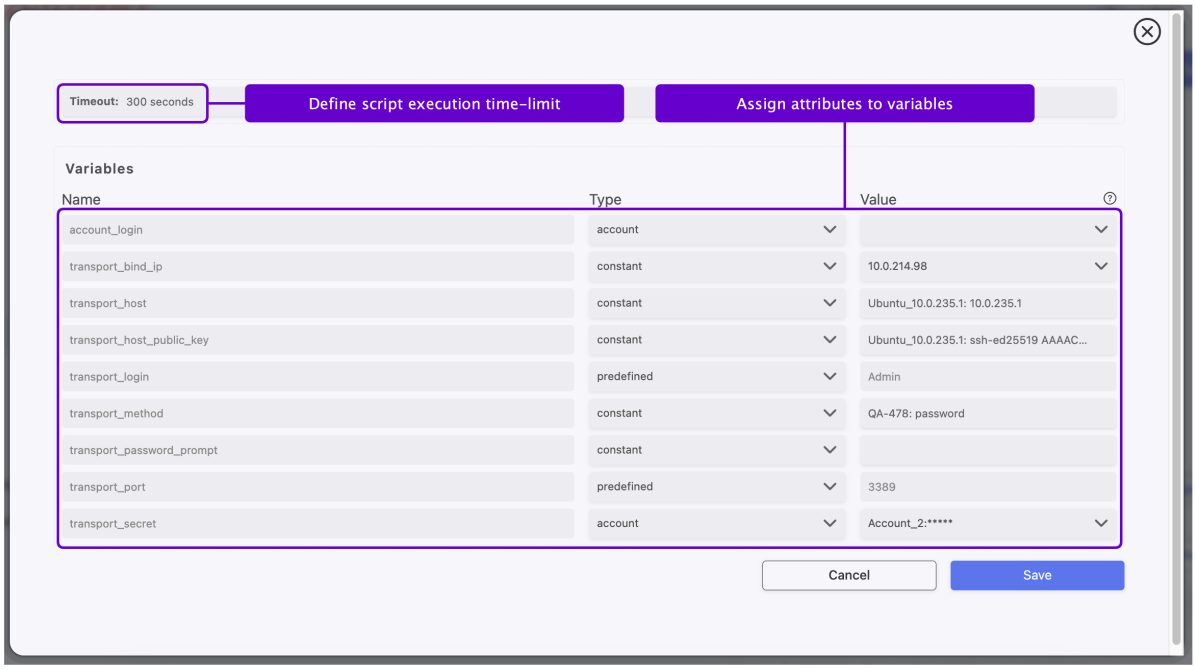
Note: Having the *Password recovery* option enabled, the Password Verifier spawns "Trigger password changer" action in the account. When it's disabled, the Password Verifier only sends event "Unable to verify password for account <account_name>".



20. In the *Password changer* field select desired password changing script from the drop-down list, to have the password to the account changed automatically according to the *password policy*.
21. In the *Password changers* window, in the *Timeout* field, define the script's execution time limit.
22. In the *Variables* section, assign attributes to variables.

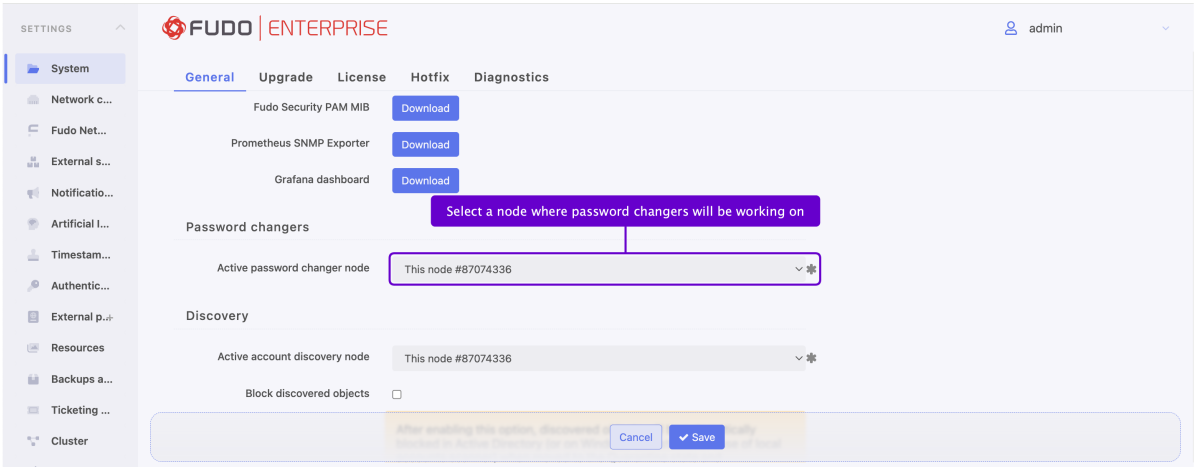
Warning:

- 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.



23. Click *Save* to close the window.
24. In the *Password verifiers* field select desired password verifier from the drop-down list, to have the password to the account verified automatically according to the *password policy*.
25. In the *Password verifiers* window, in the *Timeout* field, define the script's execution time limit.
26. In the *Variables* section, assign attributes to variables.
27. Click *Save* to close the window.

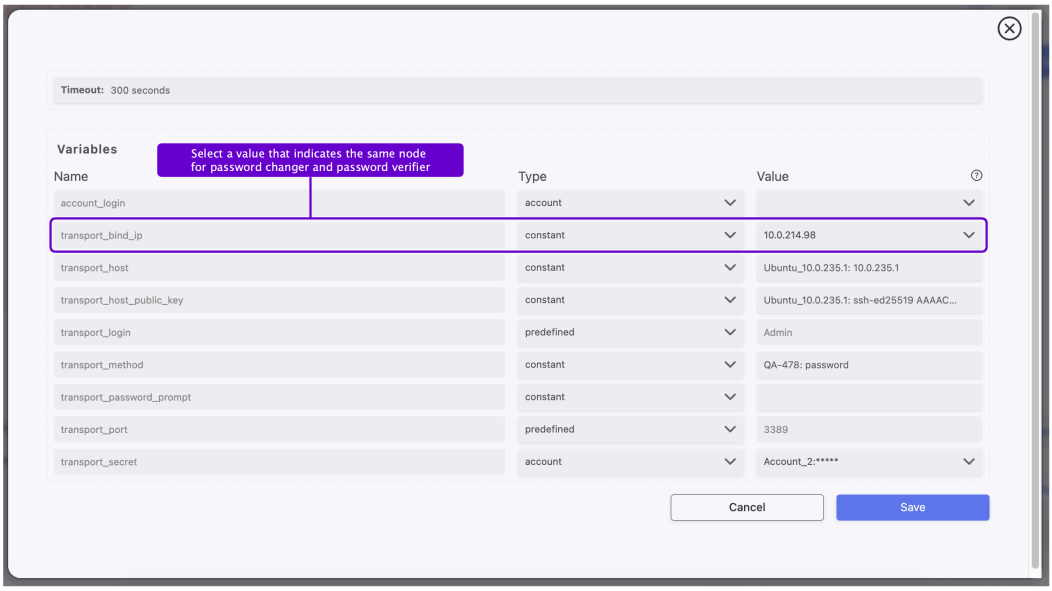
Note: Fudo Enterprise allows changing a password on a different node than the one that set as an *Active cluster node for Password changers*.



In order to have this configured, the following condition should be met:

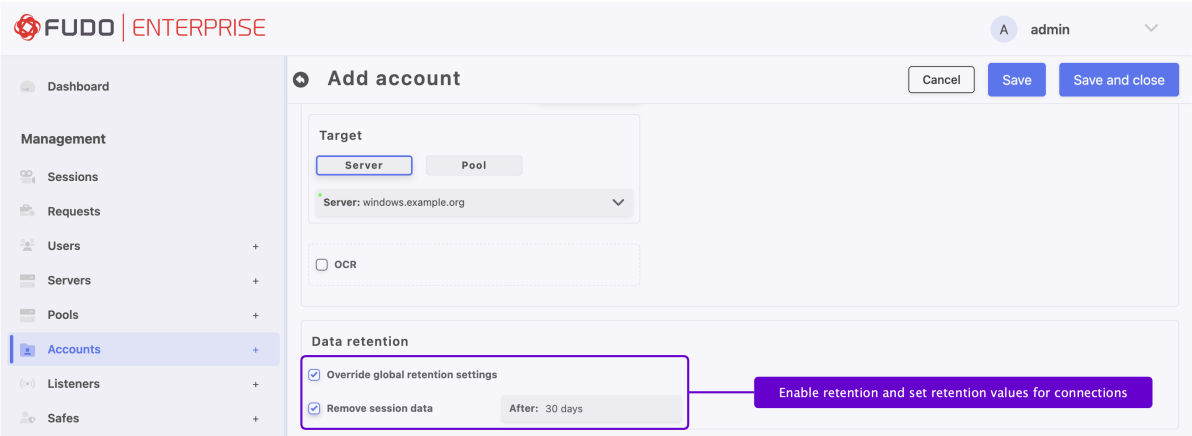
- Setting up a **Password Changer** / **Password Verifier** for an account, a value for `transport_bind_ip` variable should indicate the same cluster node for all

password changers as well as password verifiers.

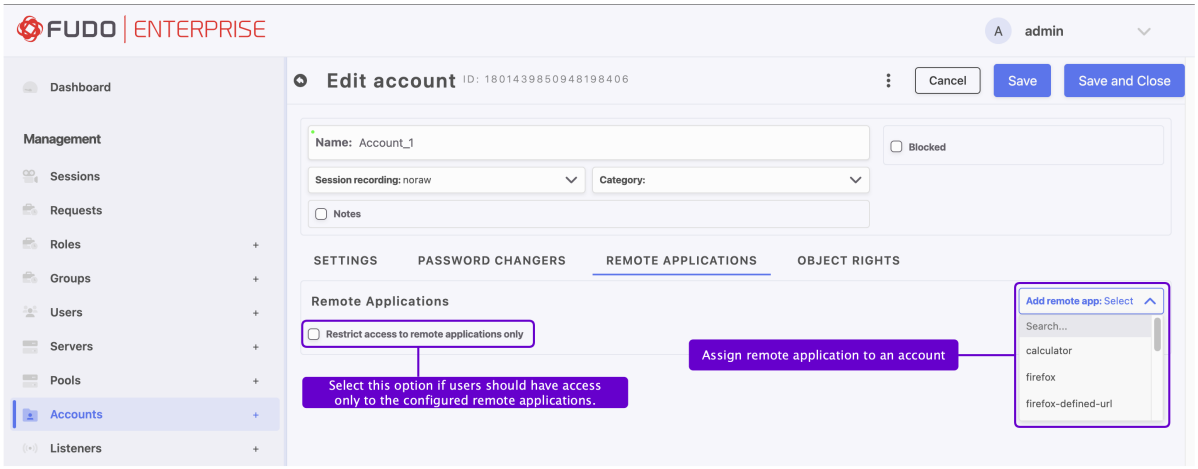


- If the `transport_bind_ip` variable values indicate different cluster nodes, the configured password changer/verifier will be running on a node that set as an *Active cluster node for Password changers*.

28. 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.



29. Go to the *Permissions* tab to add users allowed to manage this object.
30. Go to the *Remote applications* tab to 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.

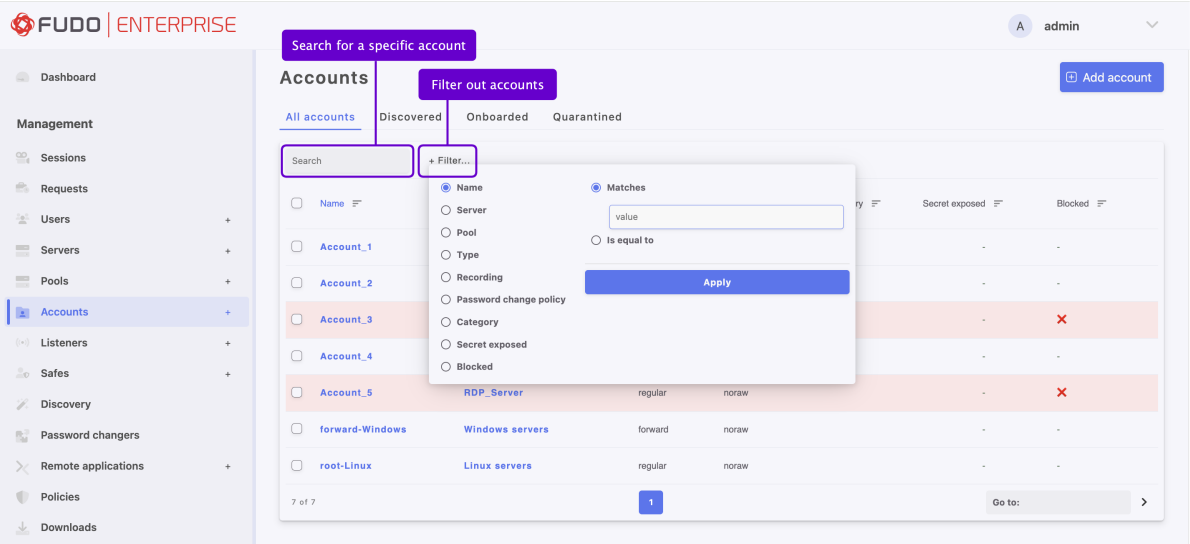
Note: The *Remote applications* tab is active only when creating a regular or forward account with an RDP server or pool assigned.

Related topics:

- *Data model*
- *Editing an account*
- *Blocking an account*
- *Unblocking an account*
- *Deleting an account*
- *Password changers - active cluster node*

12.2 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*.

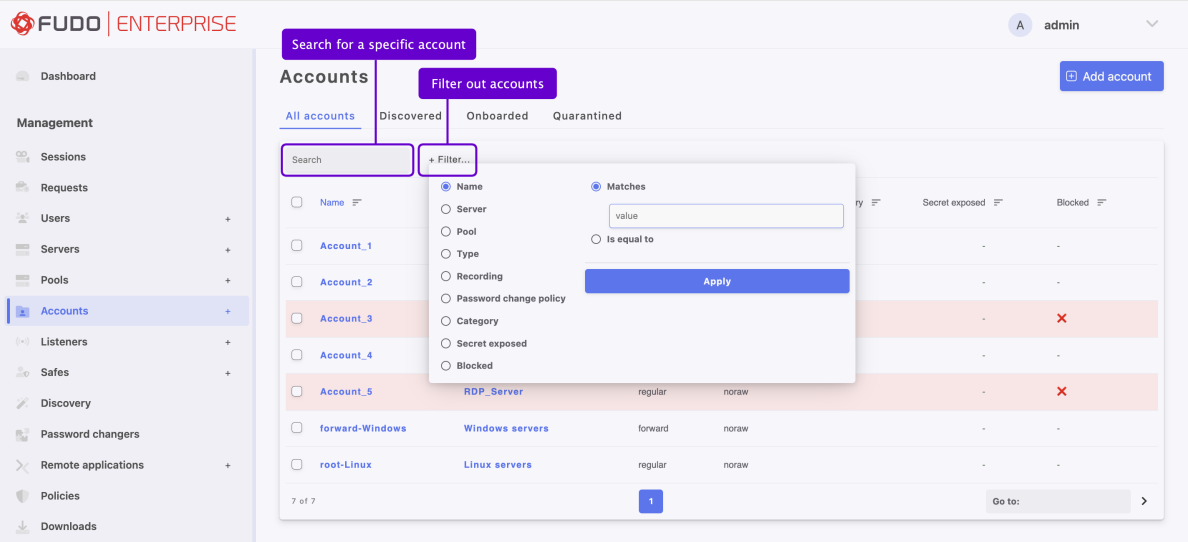
Related topics:

- *Creating an account*
- *Blocking an account*
- *Unblocking an account*
- *Deleting an account*

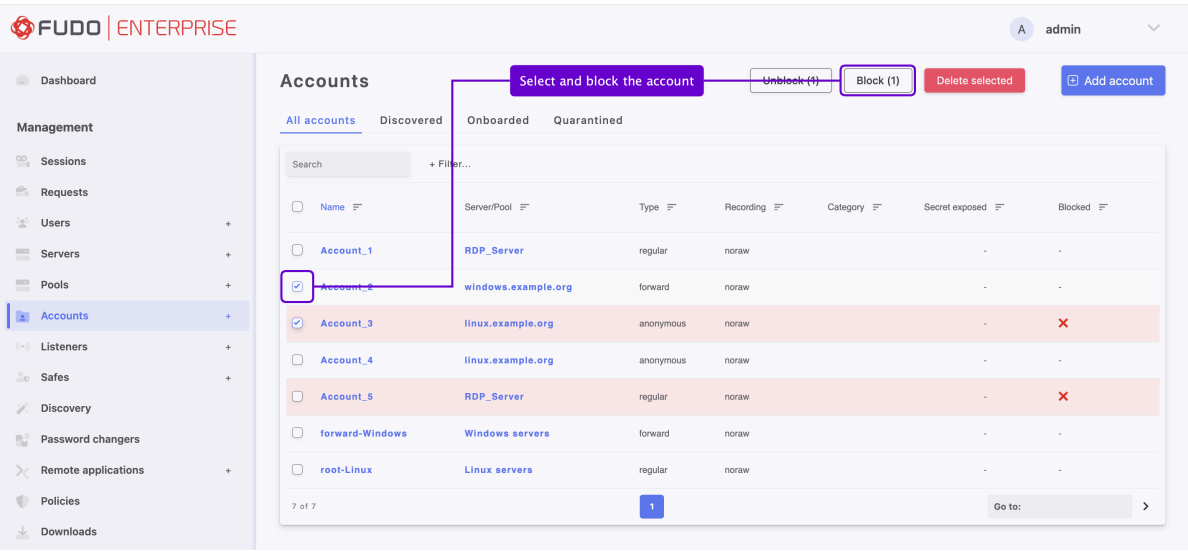
12.3 Blocking an account

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*.

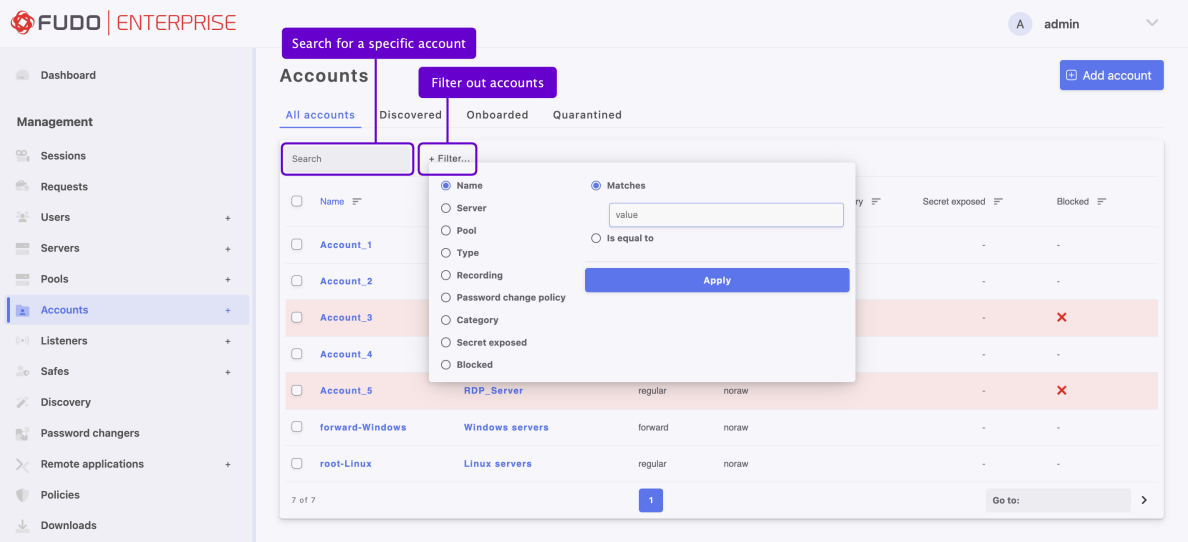
Note: To view the blocking reason, place the cursor over the red cross icon on the accounts list.

Related topics:

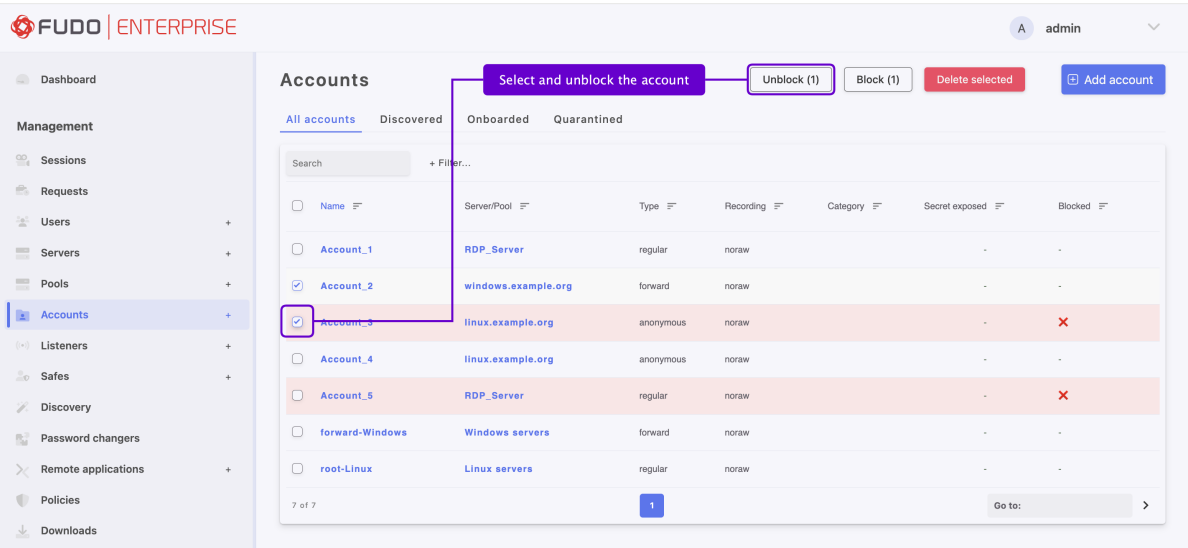
- *Creating an account*
- *Editing an account*
- *Unblocking an account*
- *Deleting an account*

12.4 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.

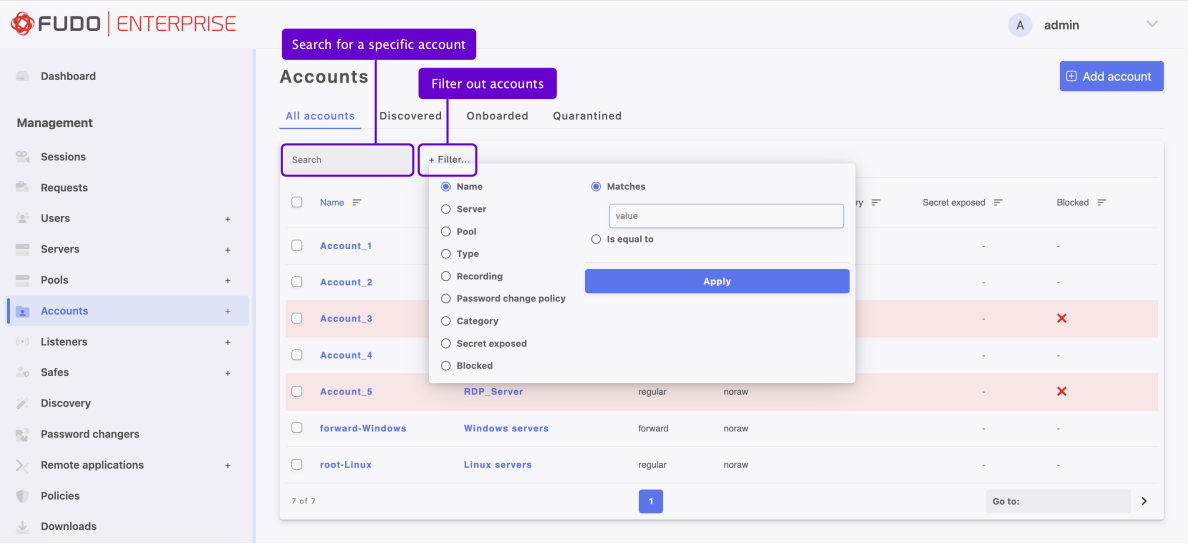
Related topics:

- *Blocking an account*
- *Creating an account*
- *Editing an account*
- *Deleting an account*

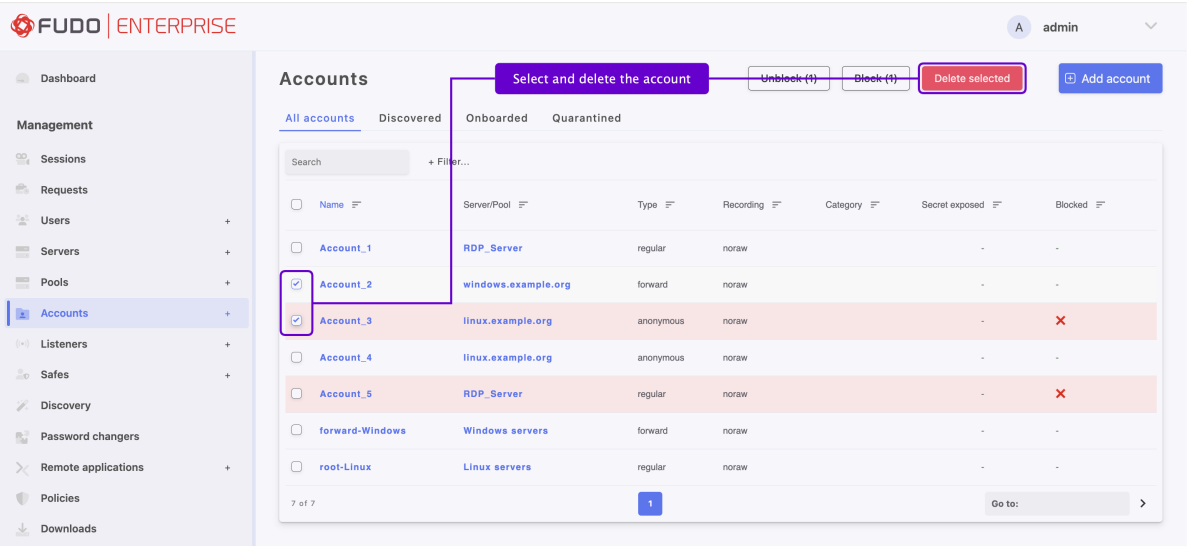
12.5 Deleting an account

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:

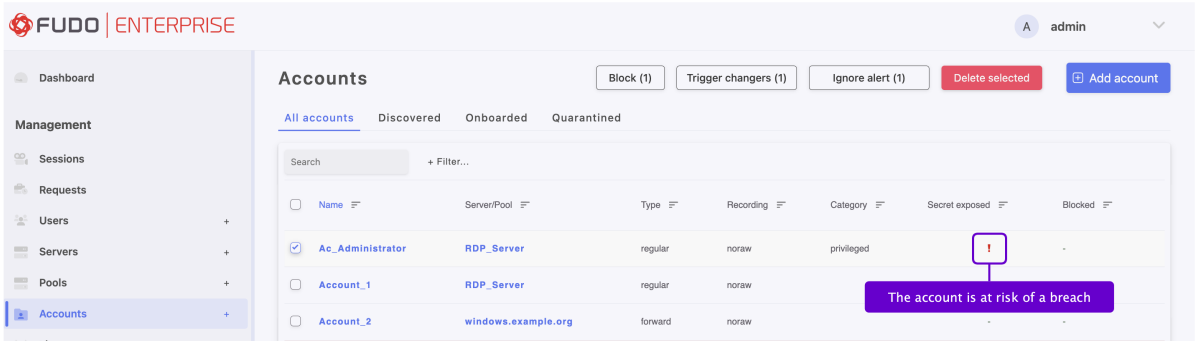
- *Creating an account*
- *Editing an account*
- *Blocking an account*

- *Unblocking an account*

12.6 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 password change is available only for accounts with an assigned password changer and password change policy that has the *Password change enabled* option active.

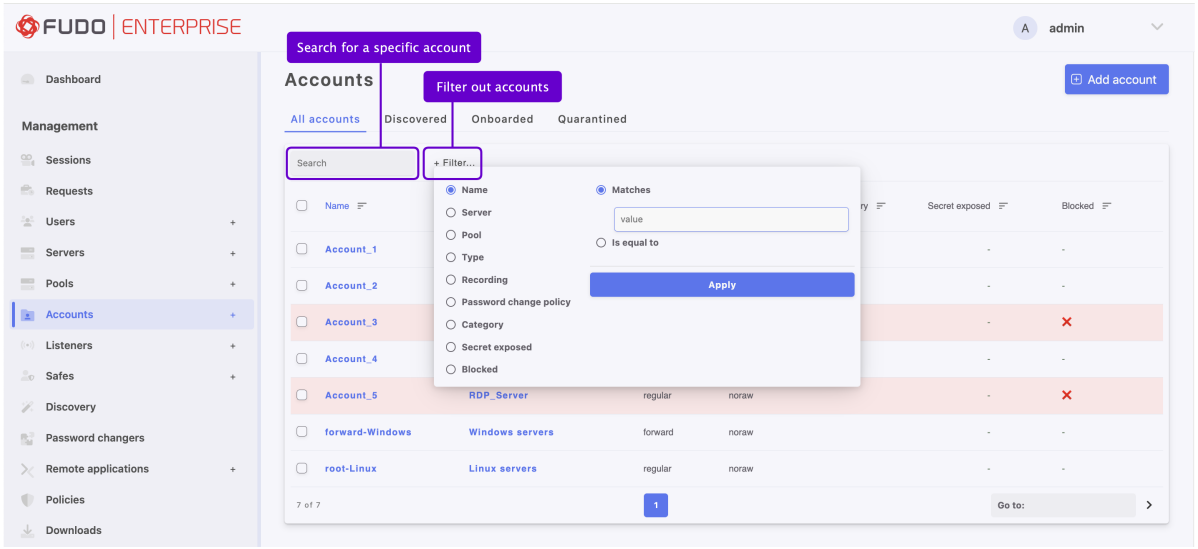


Administrator has an option to ignore the alert or trigger a *password changer* assigned to the account.

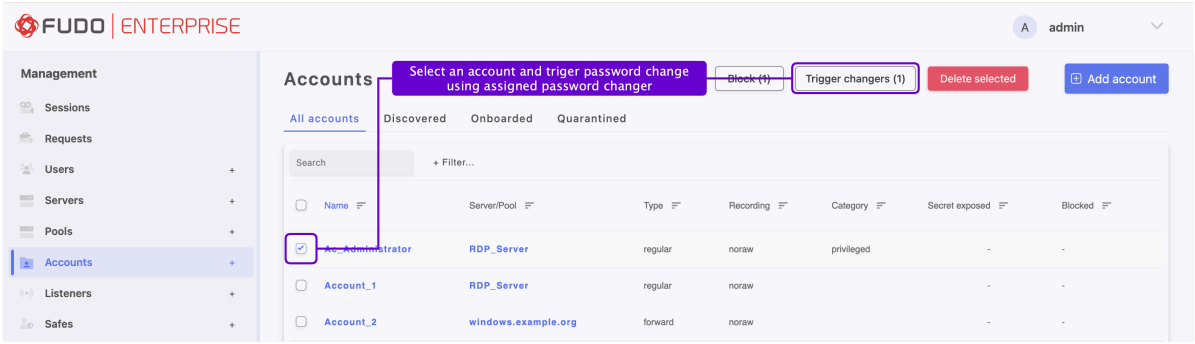
12.6.1 Triggering password change

Triggering password 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.



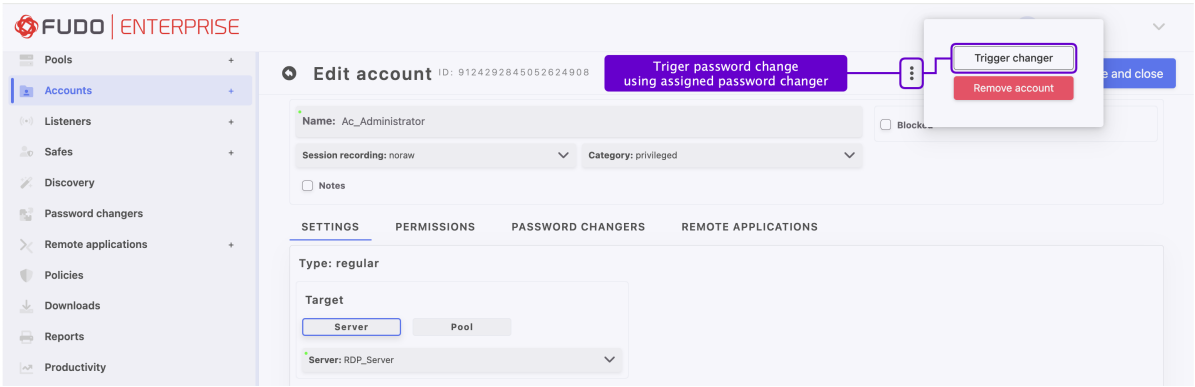
3. Select an account and click *Trigger changers*.



4. Confirm changing password to selected accounts.

Triggering password change from account form

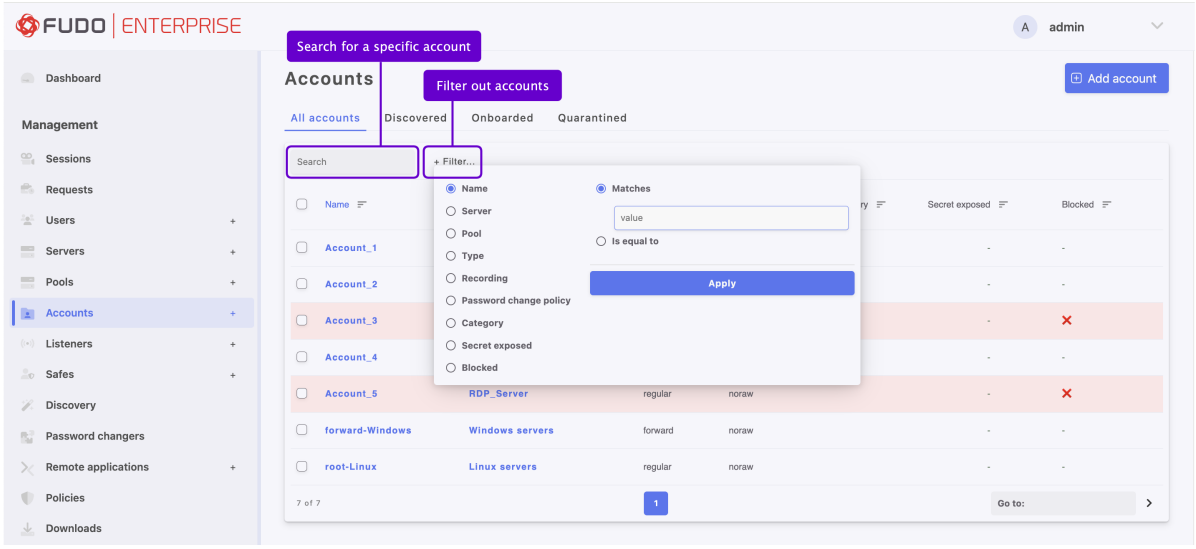
1. Click on the chosen account's name to edit its configuration.
2. Click on the three dots symbol before the *Cancel* and *Save* buttons to reveal the additional menu, and then click *Trigger changer*.



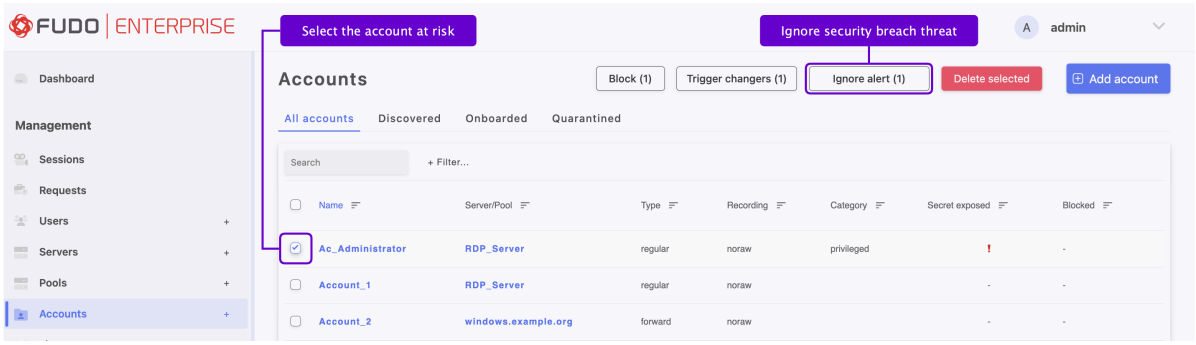
12.6.2 Ignoring security alert

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.



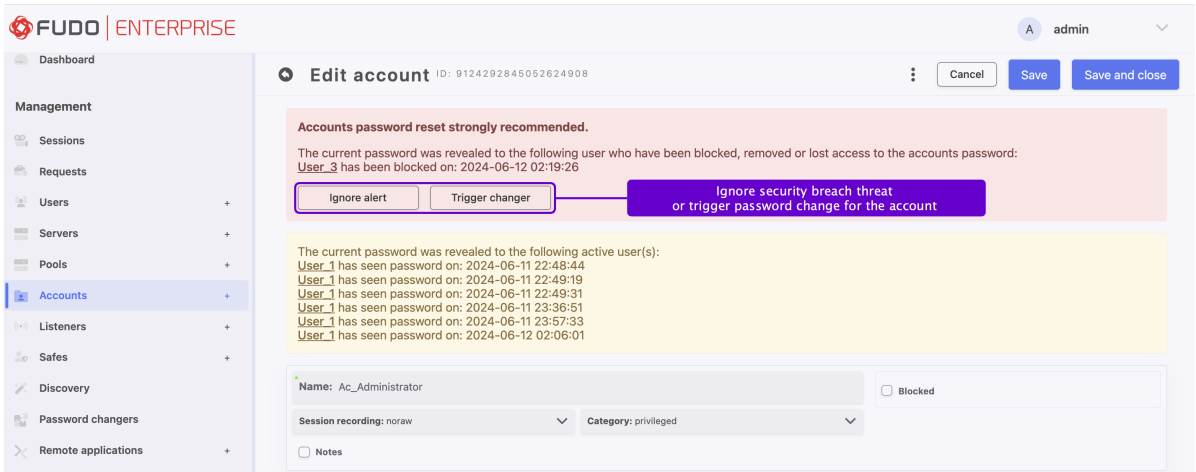
3. Select the account at risk and click *Ignore alert*.



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:

- *Password changers*
- *User Access Gateway*

CHAPTER 13

Listeners

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **transparent** and **gateway** modes in the **listeners configuration**. Listeners using these modes must be reconfigured to use proxy or bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

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

13.1 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:

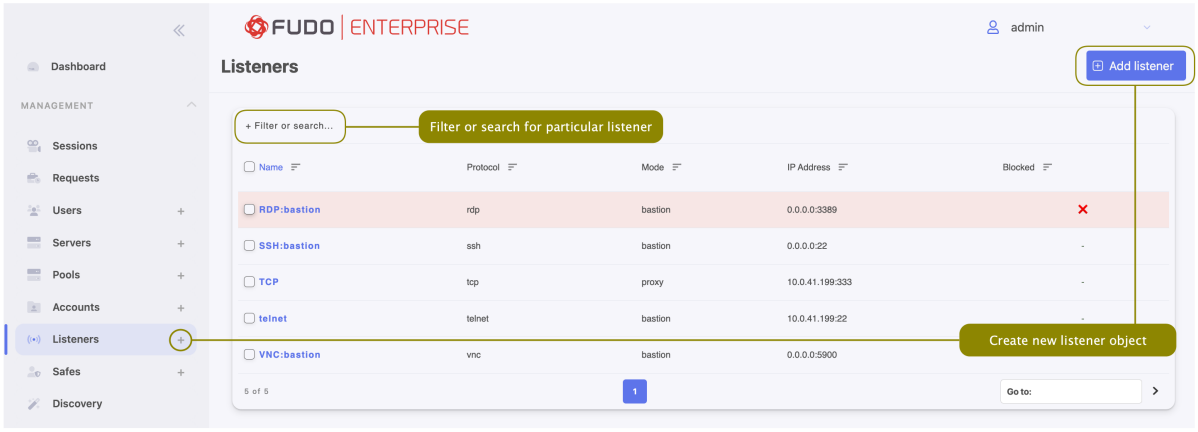
- A listener cannot link to an account that is assigned to a server with a different protocol then the one defined in the listener.
- A *proxy* type listener can link to only one server.
- A *bastion* type listener cannot link to an anonymous account.

- 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*.

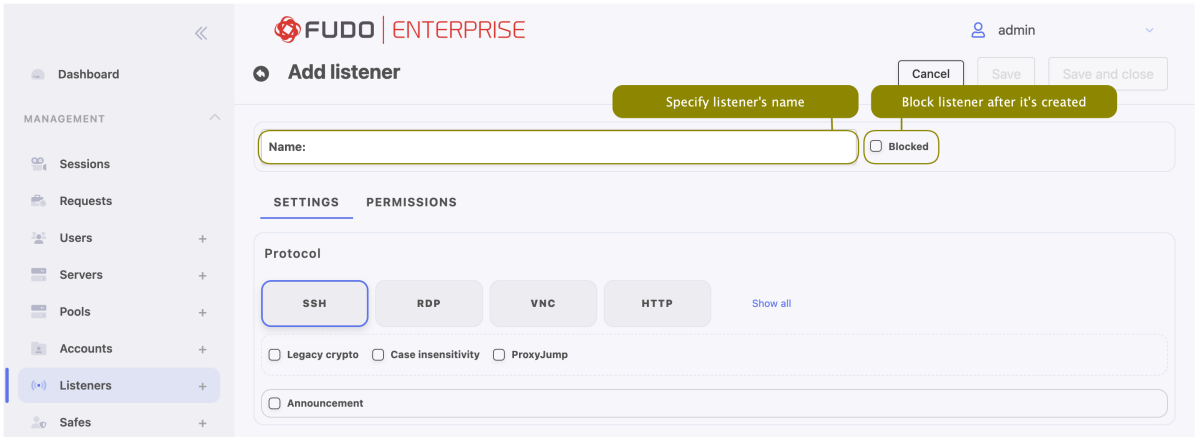
In order to create a Listener, follow the instruction:

1. Click + icon in the main menu next to the *Listeners* tab, or

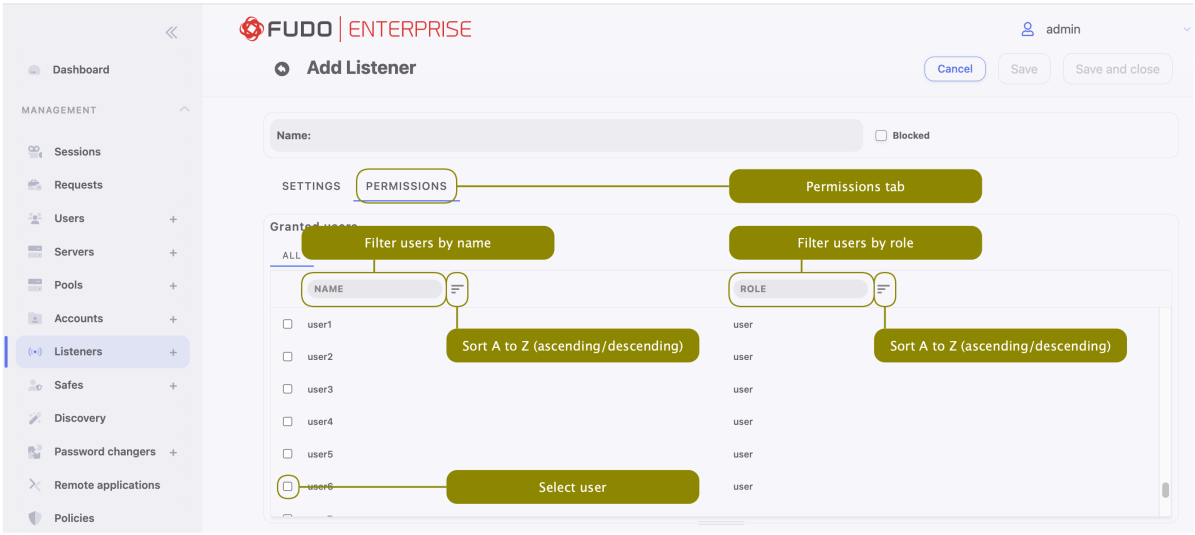
Select *Management* > *Listeners* and then click + *Add listener*.



2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.



4. Go to *Permissions* tab and add users allowed to manage this listener. Use filtering by name or by role to limit the number of objects displayed on the list.



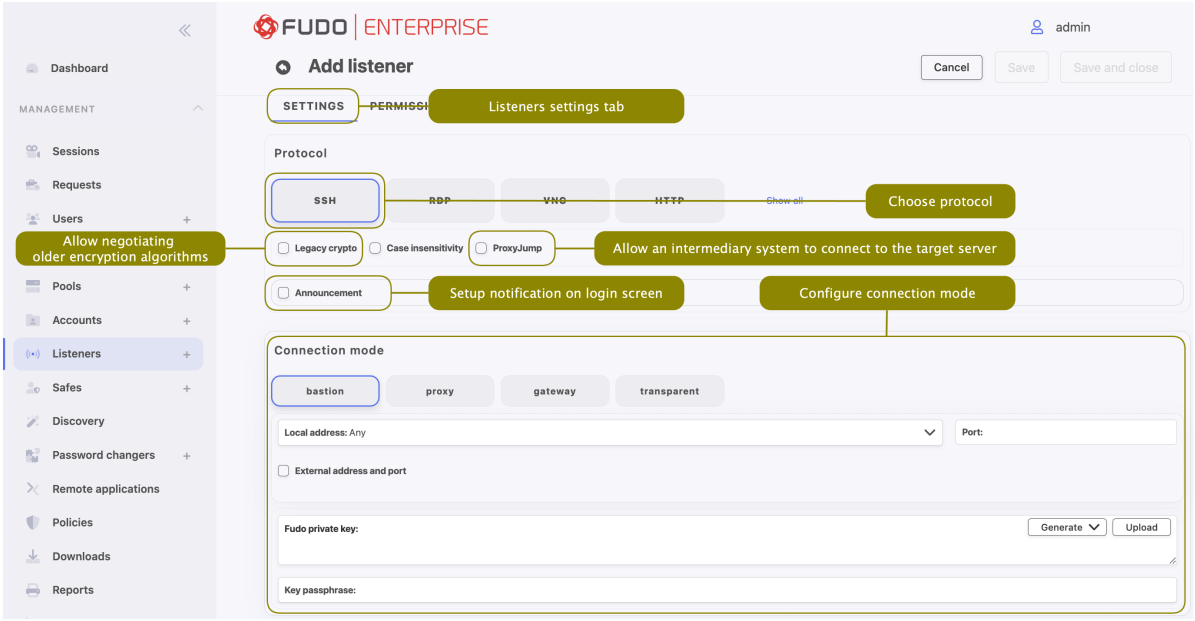
5. Go back to *Settings* tab, choose desired protocol button and follow the corresponding chapter below to complete the listener creation:

- *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 TCP listener*
- *Setting up the MS SQL listener*
- *Setting up the Telnet listener*
- *Setting up the Telnet 3270 listener*
- *Setting up the Telnet 5250 listener*

13.1.1 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. 2. Select *Legacy crypto* option to allow negotiating older encryption algorithms when establishing connections.
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: gateway

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed

in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

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*.

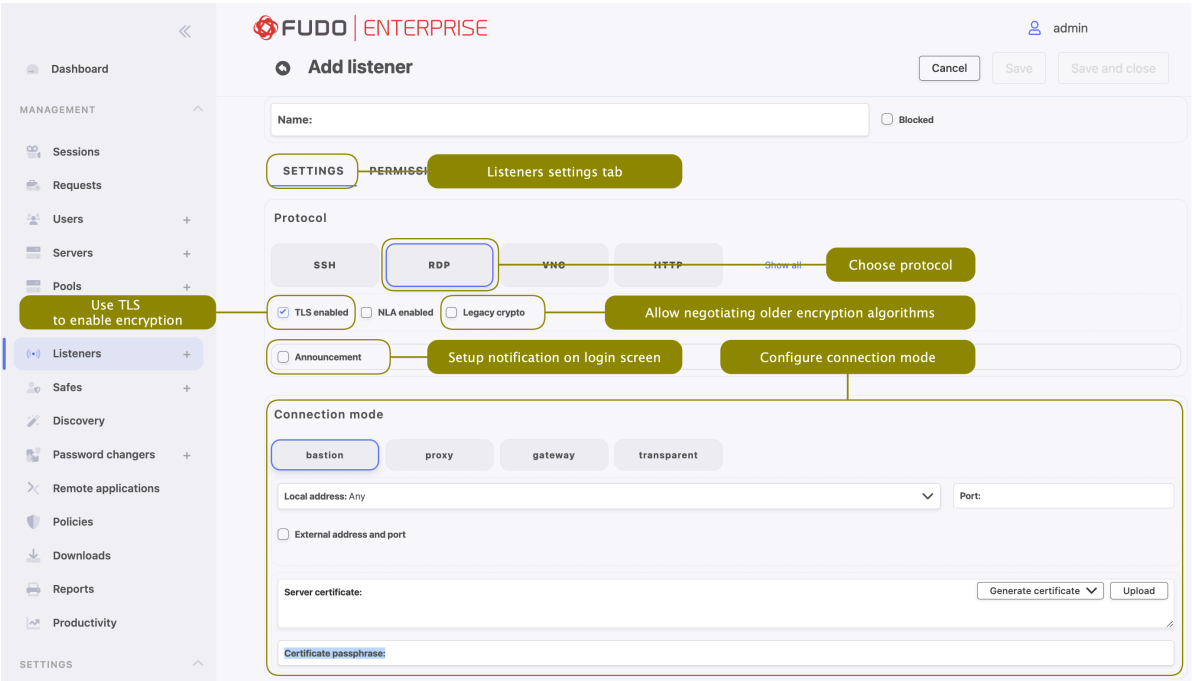
Related topics:

- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

13.1.2 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.

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.

Mode: gateway

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

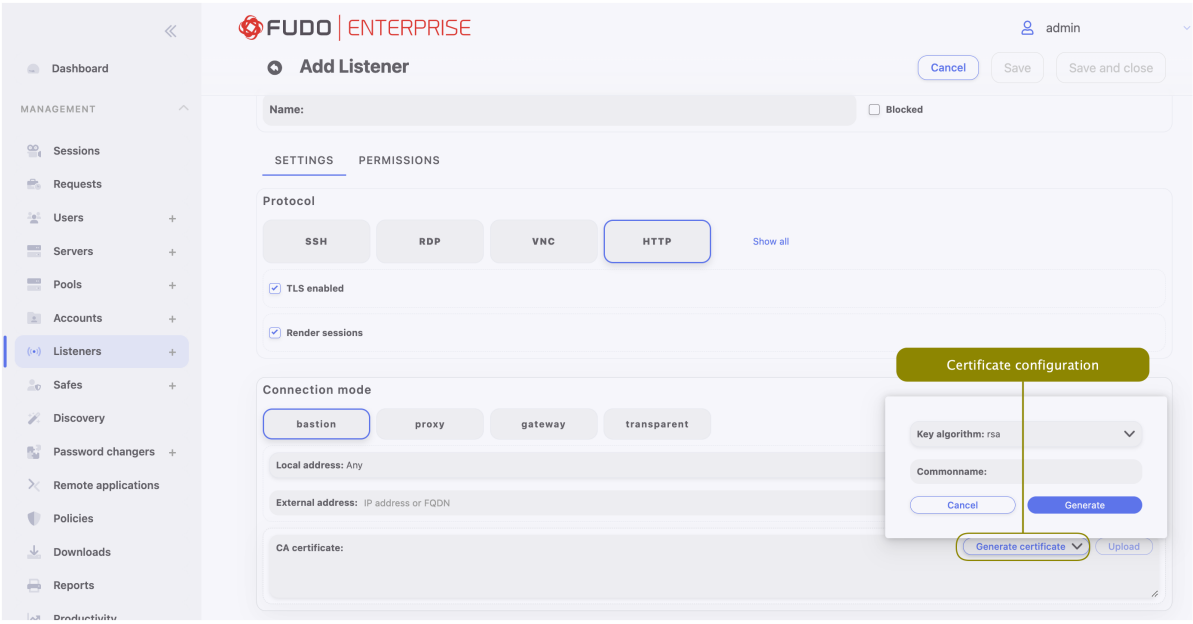
- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.

- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

6. 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. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM.



7. Click *Save*.

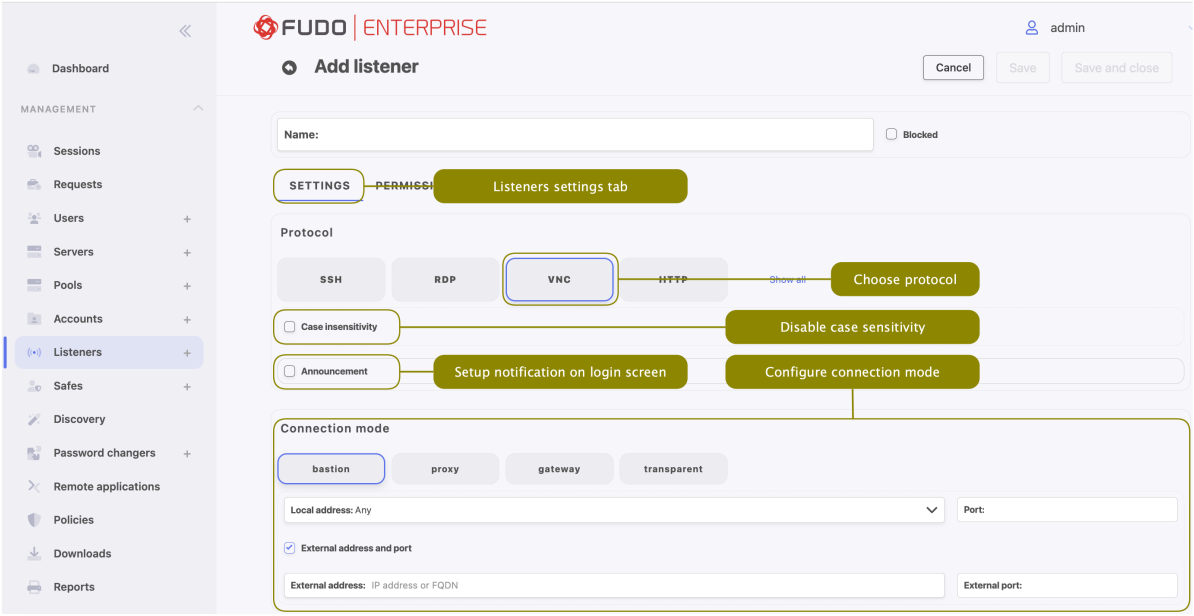
Related topics:

- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

13.1.3 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 *Case insensitivity* option to disable case sensitivity in the username string when connecting over this listener.
3. Select *Announcement* option to enable it's field and type in the notification that will be presented to the user on the login screen.
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.

   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.

Mode: gateway

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

5. Click *Save*.

Related topics:

- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

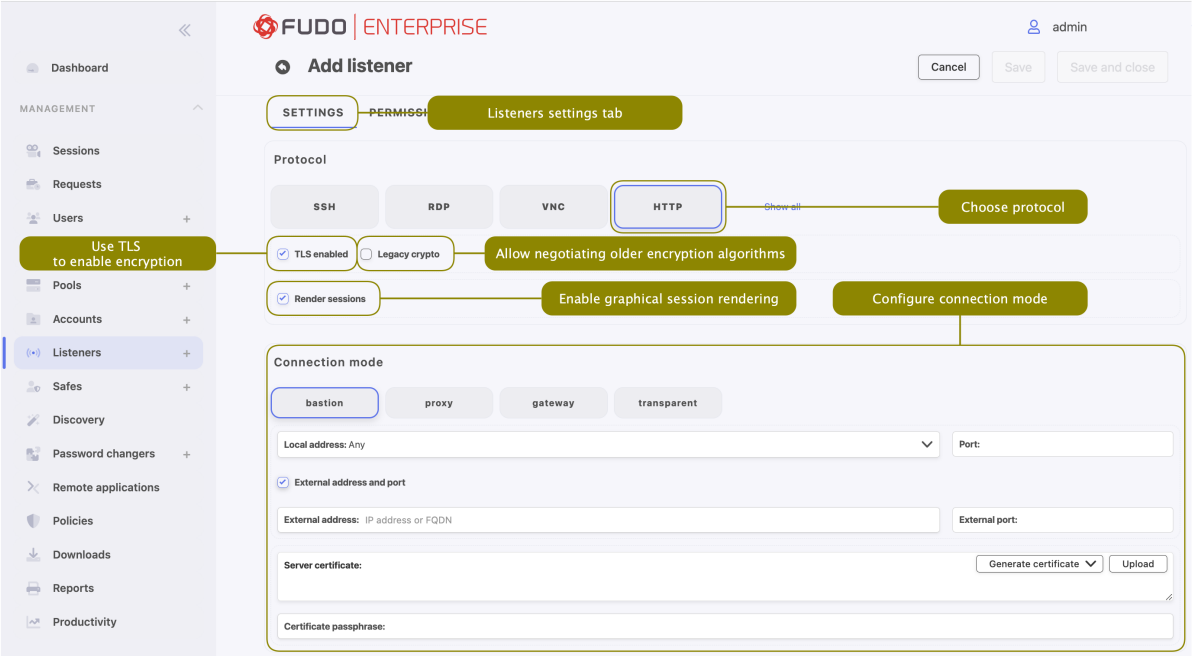
13.1.4 Setting up the HTTP listener

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.

   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.

Mode: gateway

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

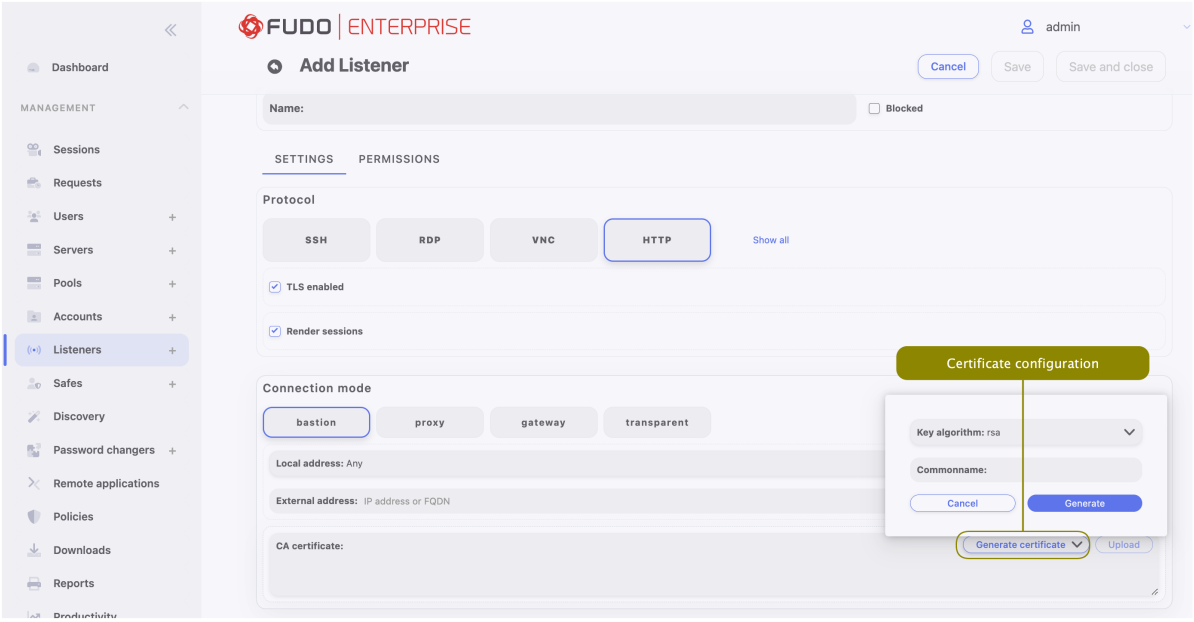
- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

6. 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.

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*.

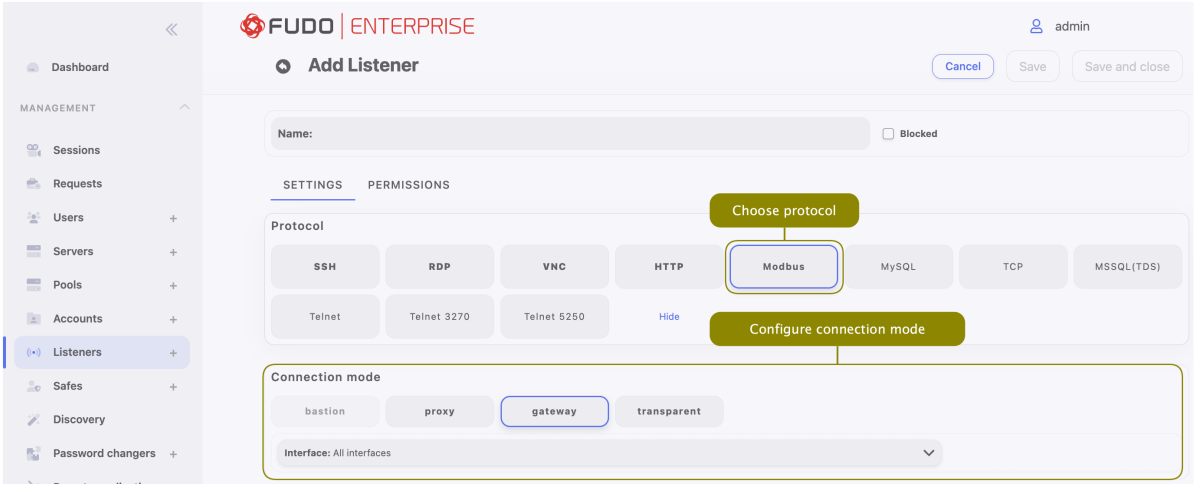
Related topics:

- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*
- *Session examples*

13.1.5 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: 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.

   Mode: gateway

   Deprecated since version 5.6

   - Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.

- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

4. Click *Save*.

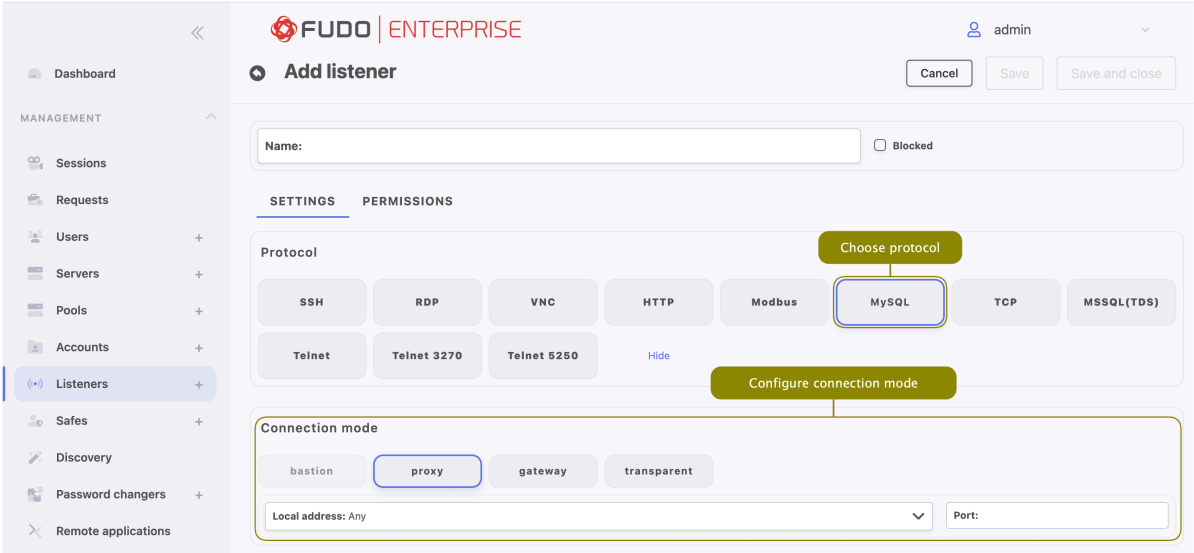
Related topics:

- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

13.1.6 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.

1. Go to *Settings* tab, press the `Show all` button to expand supported protocols list.
2. Press `MySQL` 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.

Mode: gateway

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

4. Click *Save*.

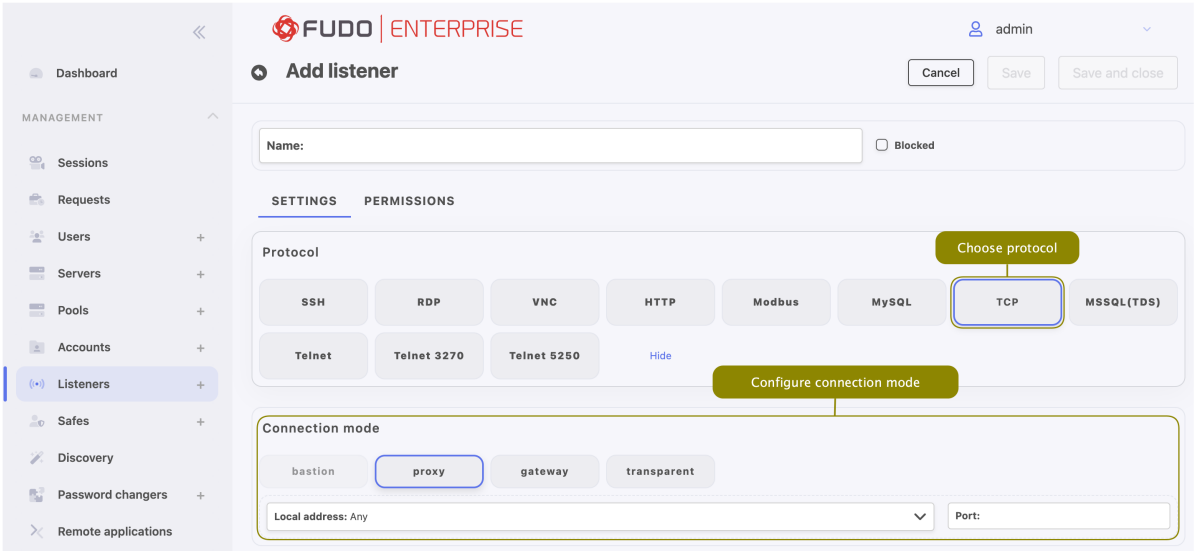
Related topics:

- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

13.1.7 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.

Mode: gateway

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

4. Click *Save*.

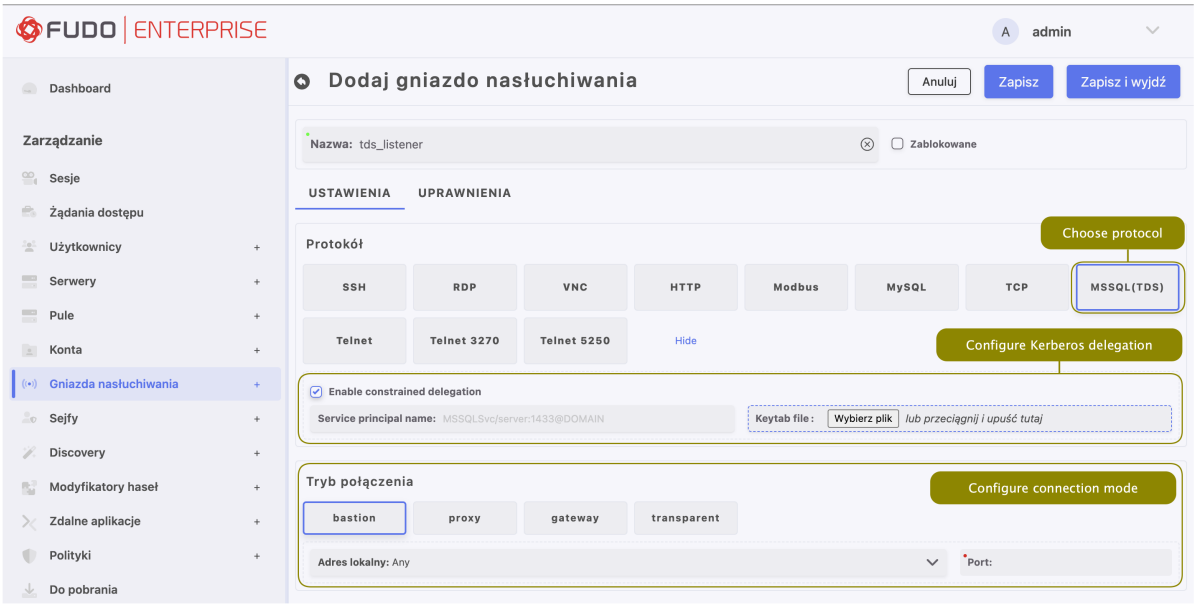
Related topics:

- *TCP*
- *Creating a TCP server*
- *Data model*

13.1.8 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.

Mode: gateway

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

5. Click *Save*.

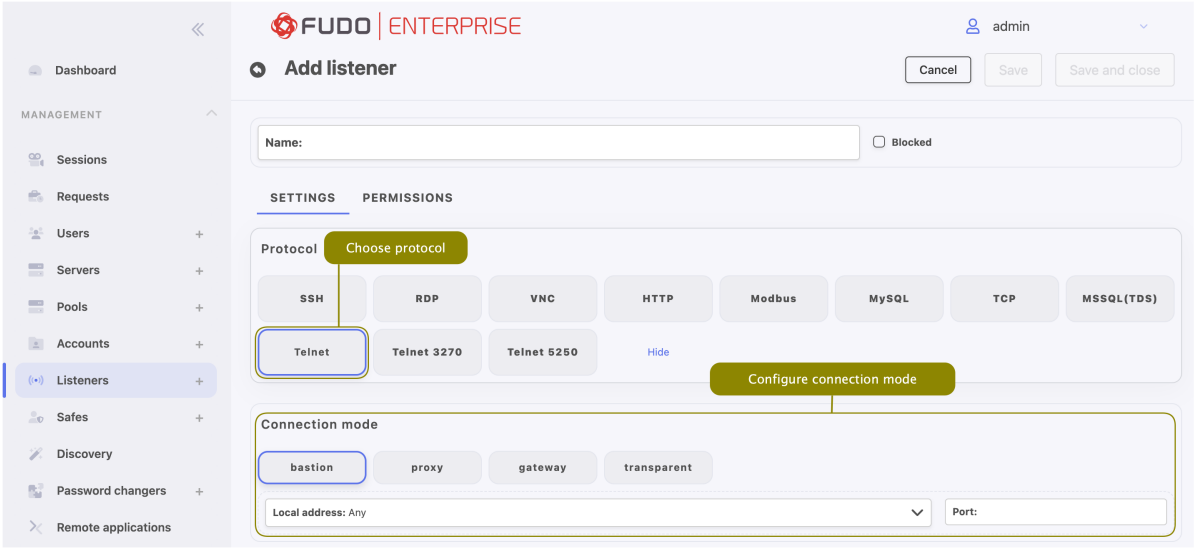
Related topics:

- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

13.1.9 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.

Mode: gateway

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

4. Click *Save*.

Related topics:

- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

13.1.10 Setting up the Telnet 3270 listener

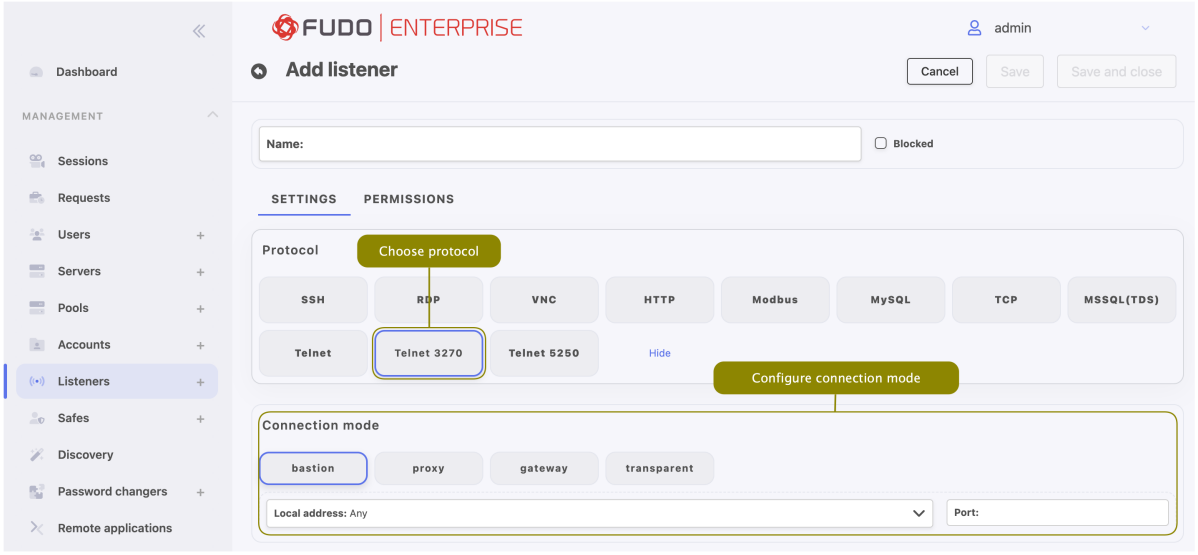
Deprecated since version 5.6 :class: danger

Support for the **Telnet 3270** protocol is **under review** and may be removed in a release following version 5.6. 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.

Mode: gateway

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

4. Click *Save*.

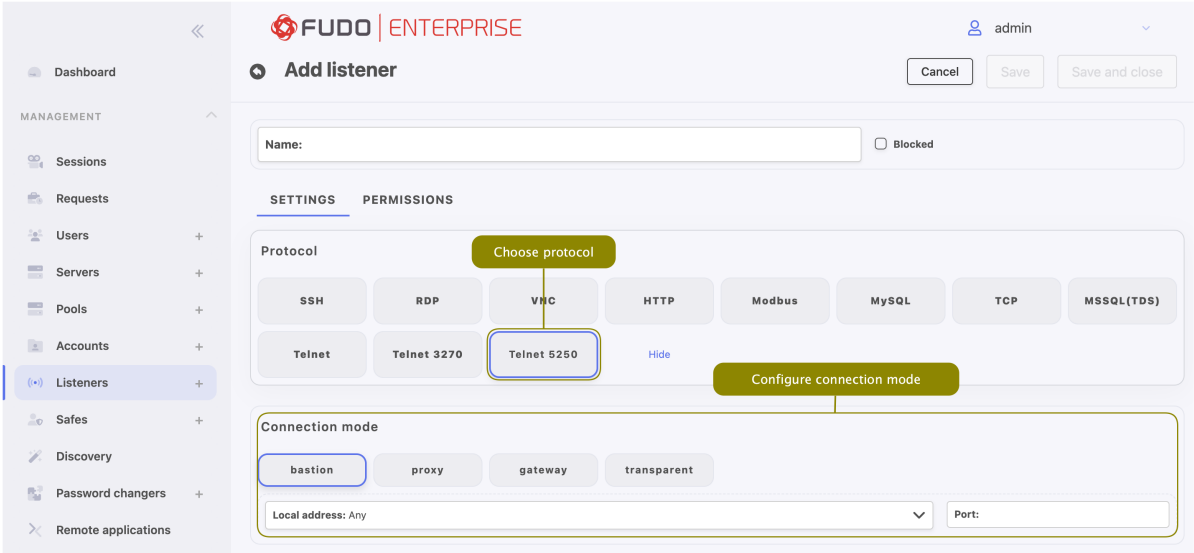
Related topics:

- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

13.1.11 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.

Mode: gateway

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **gateway** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `gateway` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

Mode: transparent

Deprecated since version 5.6

- Fudo Enterprise 5.6 is the last version supporting **transparent** mode in the **listeners configuration**. Listeners using this mode must be reconfigured to use proxy and bastion modes before upgrading to the next release.
- Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

- Select `transparent` button in the *Connection mode* field.
- Select the network interface used for handling connections over this listener.

4. Click *Save*.

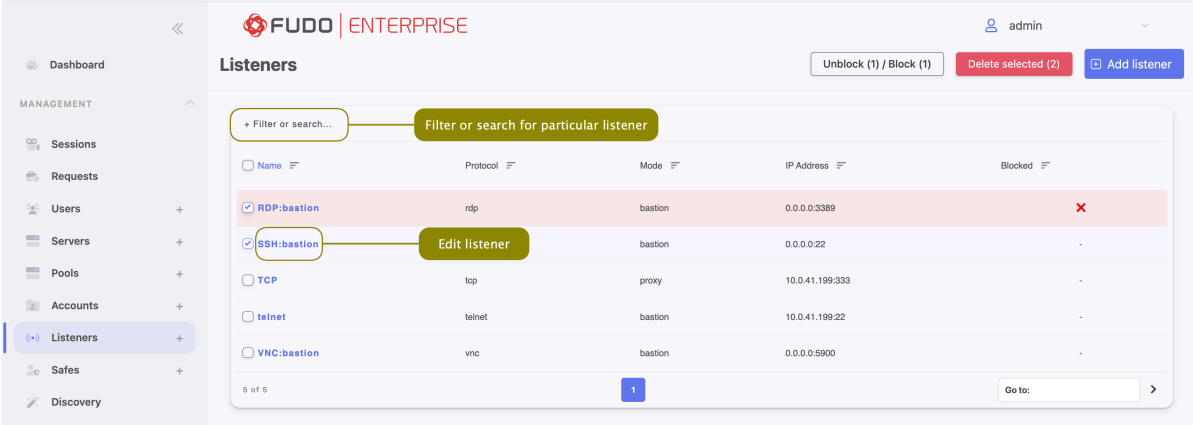
Related topics:

- *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.

13.2 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*.

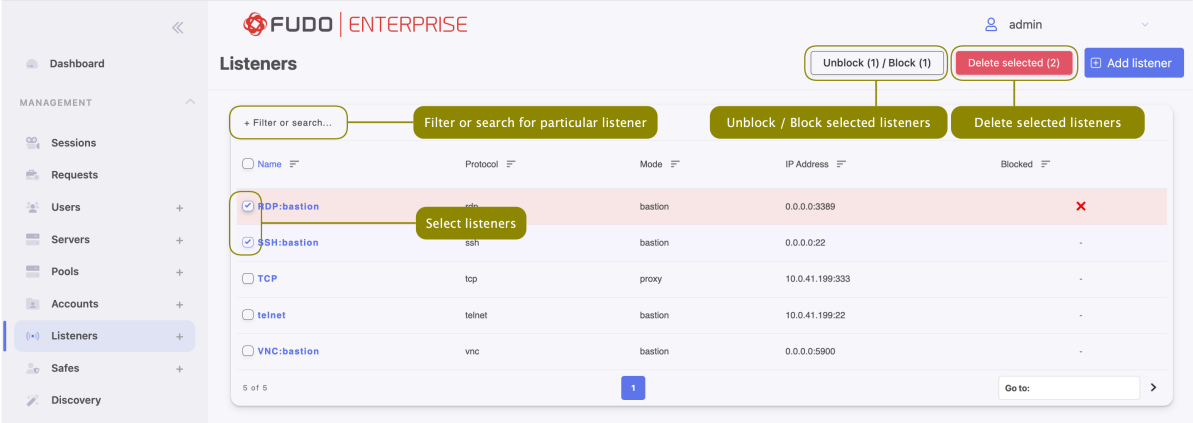
Related topics:

- *Data model*
- *System initiation*
- *Servers*

13.3 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.

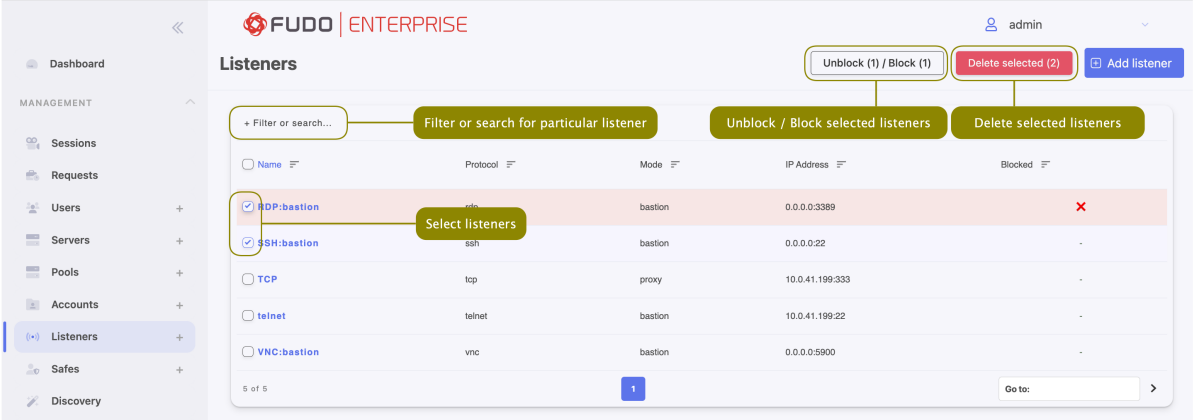
Note: To view the blocking reason, place the cursor over the red cross icon on the listeners list.

Related topics:

- *Data model*
- *System initiation*
- *Servers*

13.4 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.

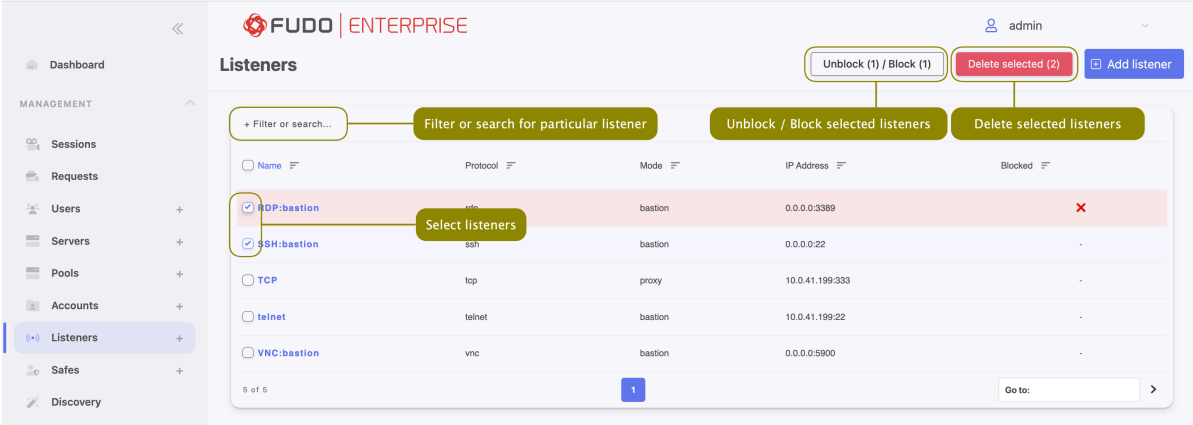
Related topics:

- *Data model*
- *System initiation*
- *Servers*

13.5 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.

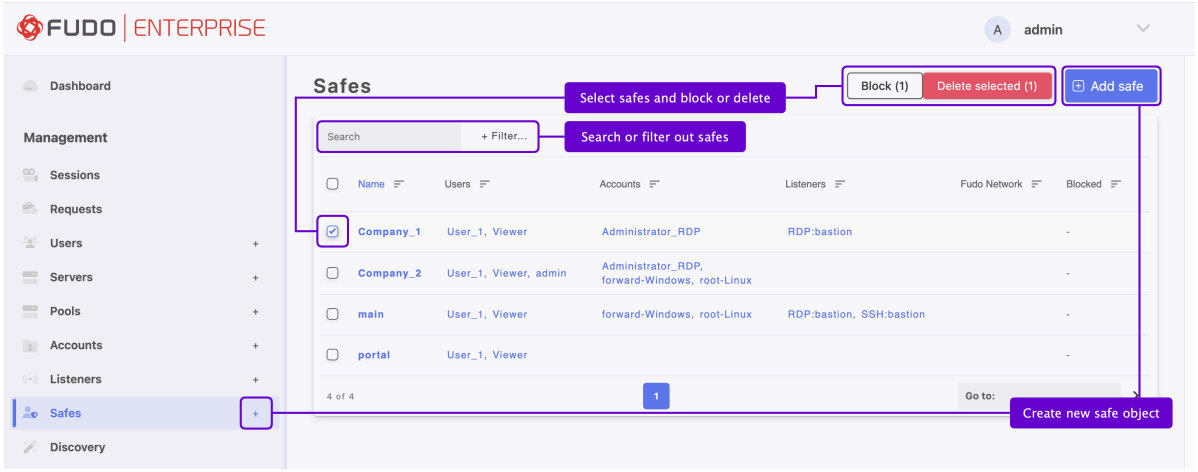
Related topics:

- *Data model*
- *System initiation*
- *Servers*

CHAPTER 14

Safes

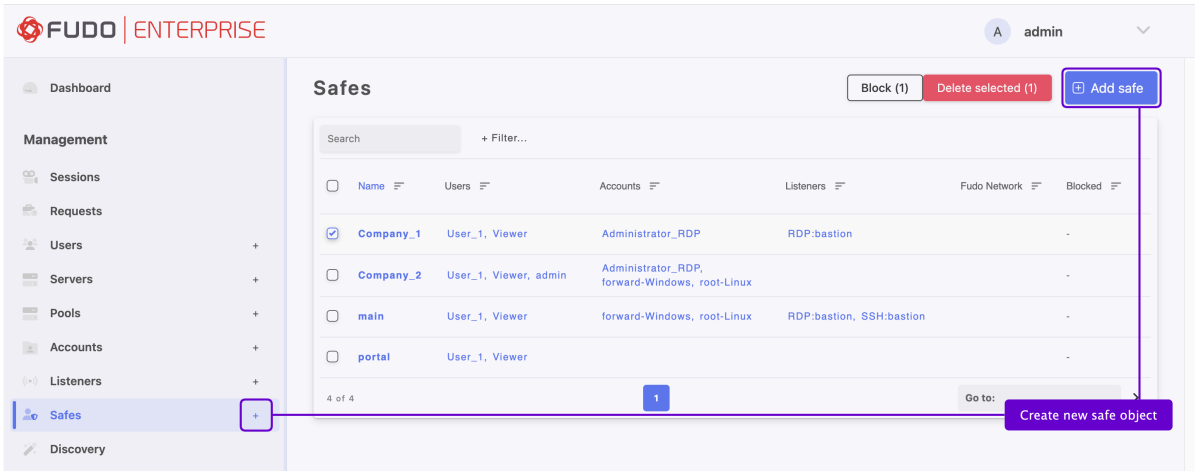
Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.



14.1 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 *Management* sub-section, or
2. Select *Management* > *Safes* and then click + *Add safe*.

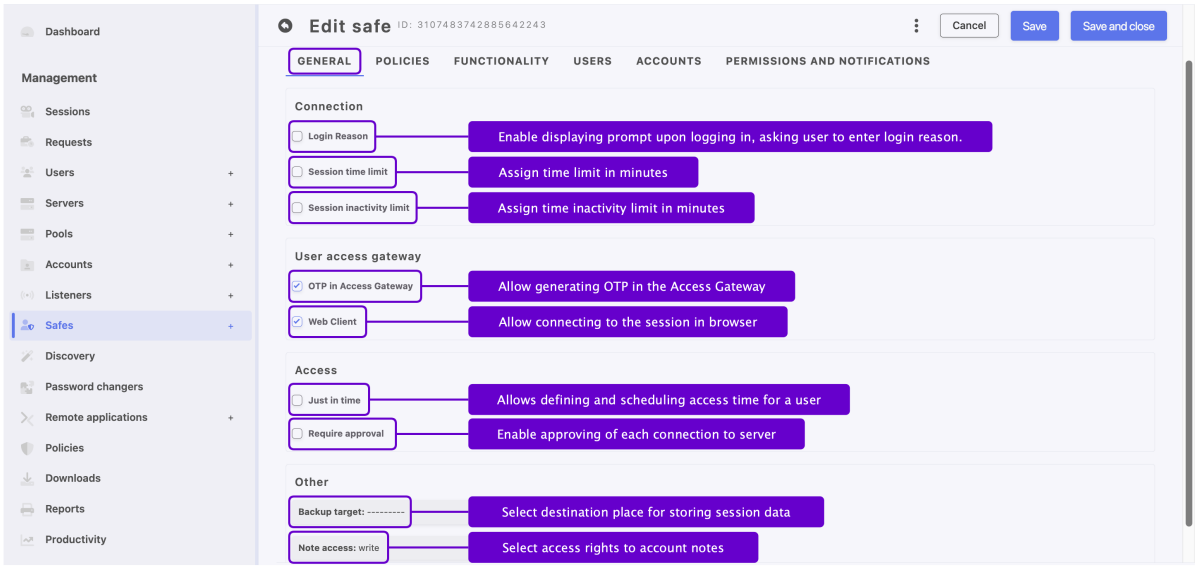


2. Enter object's name.
3. Select *Blocked* option if you want to disable access to object after it's created.
4. Click *Save* to save the object and proceed with further configuration.

GENERAL TAB

5. 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.



6. Select *Session time limit* option and enter a value in minutes after which the session will be terminated.
7. Select the *Session inactivity* limit option and enter the number of minutes of inactivity after which the session will be terminated.
8. The *OTP in Access Gateway* option is enabled by default and is responsible for generating OTP in the Access Gateway.

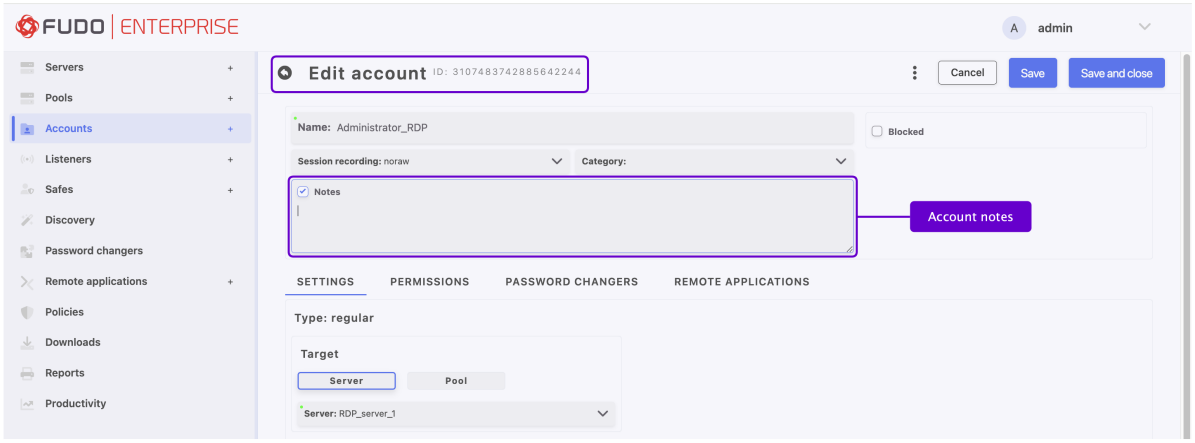
Warning: Disabling the *OTP in Access Gateway* option makes impossible connecting via the Native Client or Web Client. Access via the *Access requests* would be possible only.

9. For RDP, VNC and SSH-based safes, select *Web Client* option to allow connecting to the session using the built-in browser client.

Note: The *Web Client* option can't be enabled when the *OTP in Access Gateway* option is disabled.

10. 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.
11. 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.
12. 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.
13. 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

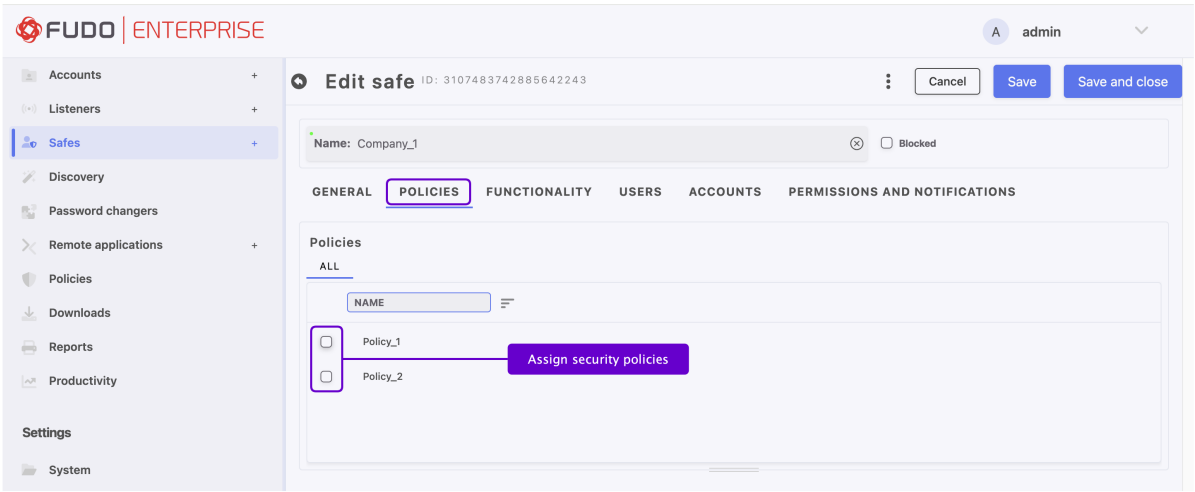


or in the *User Access Gateway*.



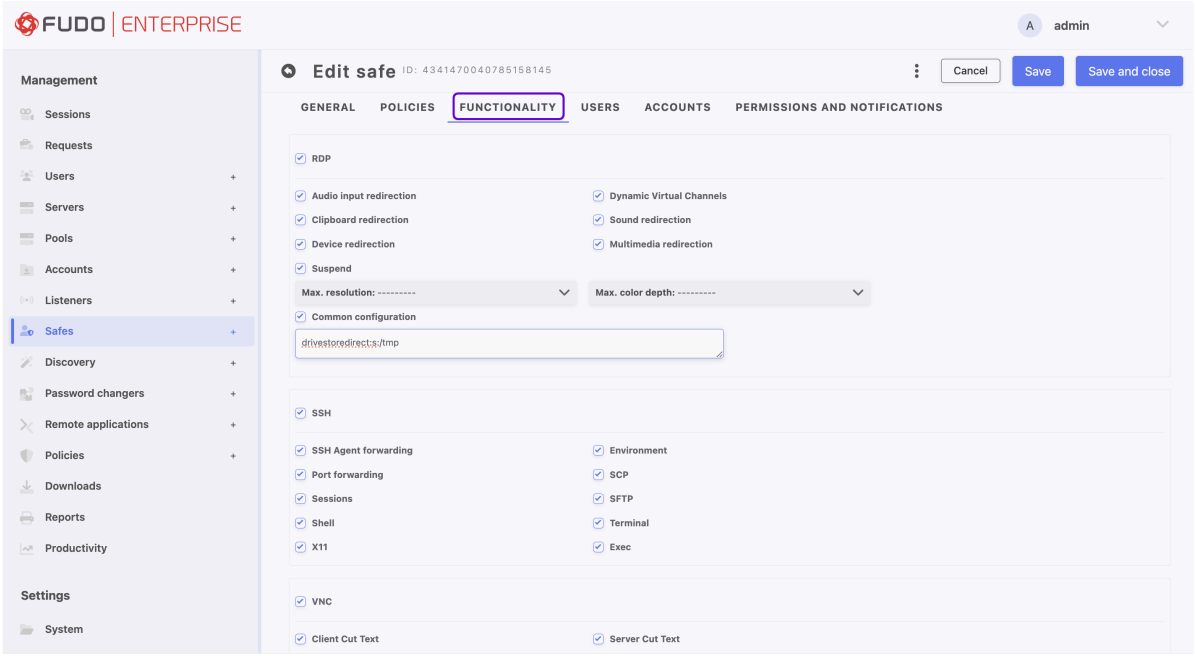
POLICIES TAB

14. Go to the *Policies* tab, and assign desired *security policies* by selecting checkboxes in front of the policies names.



FUNCTIONALITY TAB

15. 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.
  - **Sound Redirection** - Redirects audio output from the remote desktop to the client device.
  - **Device Redirection** - Allows peripherals (e.g., printers, USB devices, smart cards) connected to the client device to be used within the remote desktop session.
  - **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.

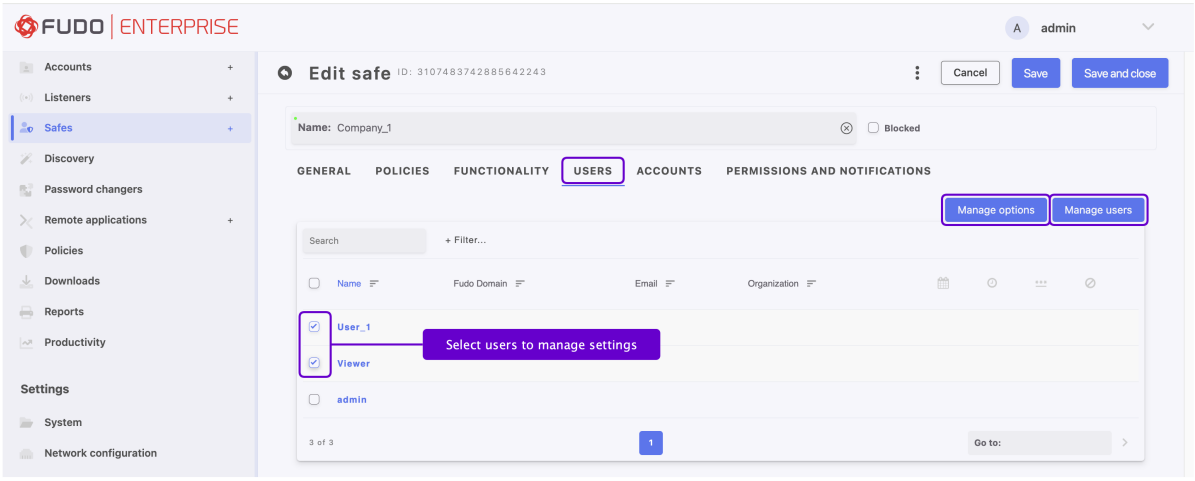
- **Common configuration** - Allows custom content to be added to the RDP configuration file. For example, to share the `/tmp` directory, the following line can be included in the generated .rdp file: `drivestoredirect:s:/tmp`.

- 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.
  - **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.

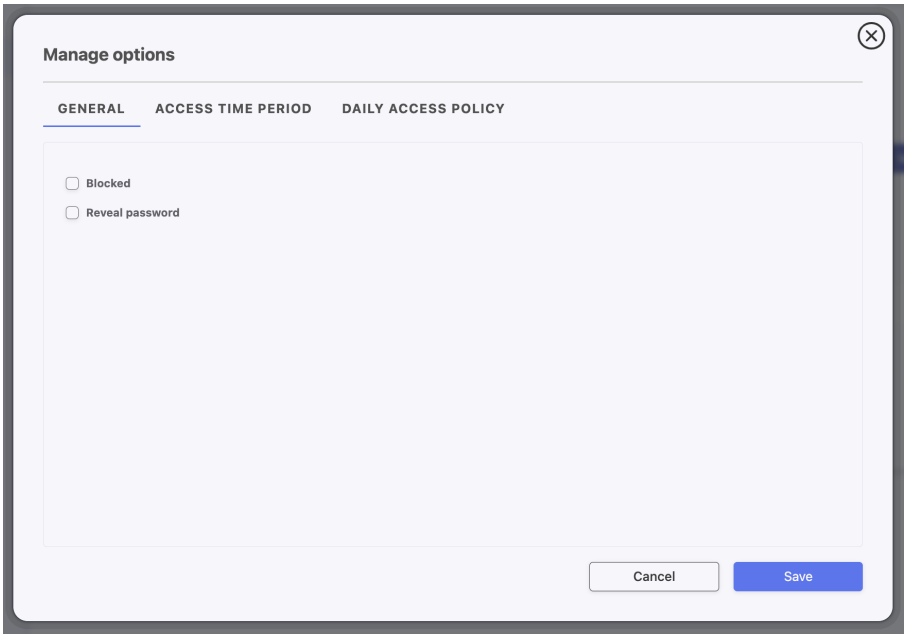
*For detailed information about SSH functionalities please refer to *RFC 4254 - The Secure Shell (SSH) Connection Protocol.*

USERS TAB

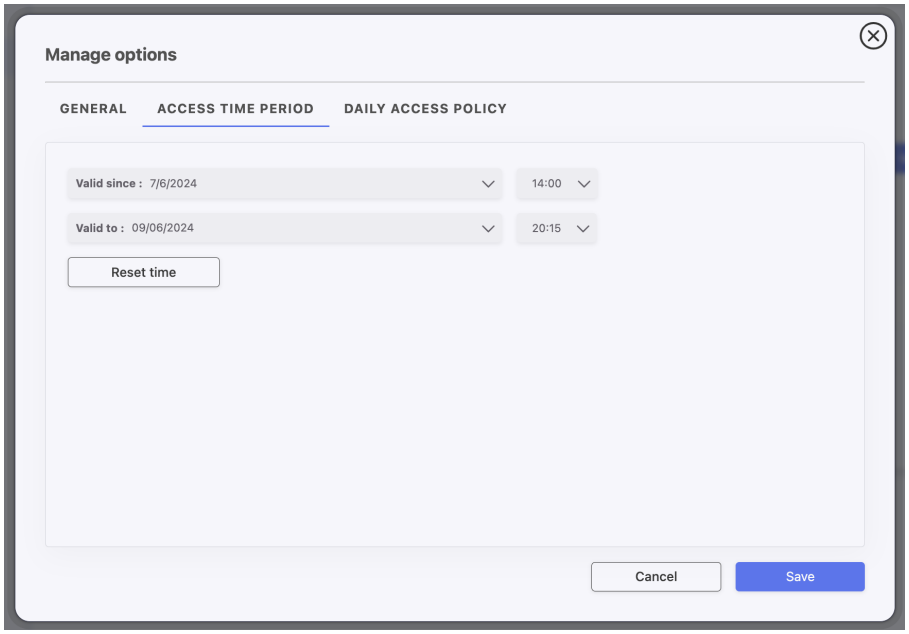
16. Go to the *Users* tab to assign users allowed to access accounts assigned to this safe.
    - Click *Manage users*.
    - Mark the checkbox in front of the users' names to enable their server access through the monitored safe.



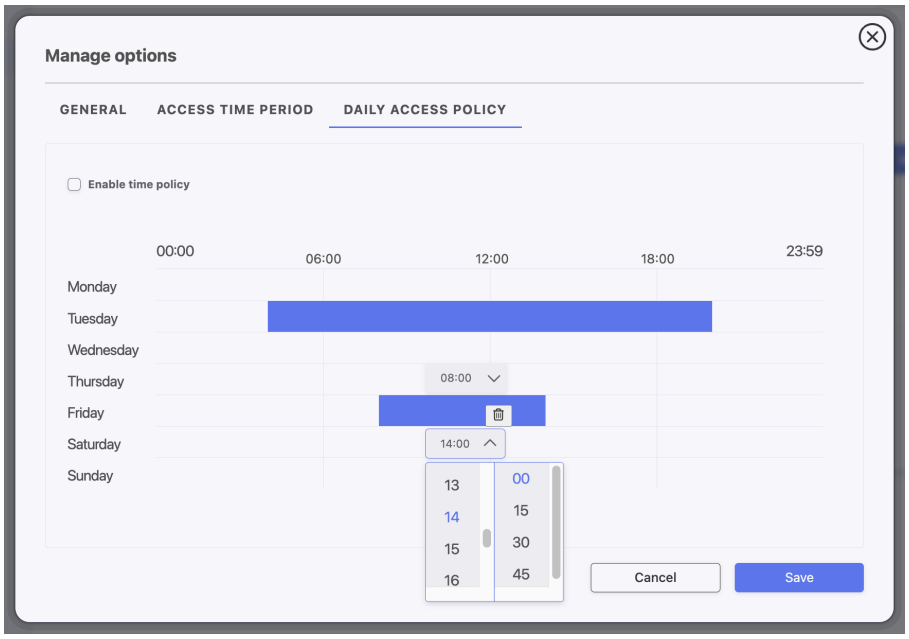
- Click *Save* to close the modal window.
- To define safe access options for a user, select the checkbox in front of the desired users' names and click *Manage options*.
  - Go to *General* tab and select *Blocked* option if you want to block the users selected in previous step.
  - Select *Reveal password* to allow selected users to use Secret Checkout feature and view passwords in the 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 enable and define time intervals during which the user will be allowed to connect to servers. Just click in the row corresponding to the chosen day of the week to add a range, then click on that range to open the time range edit menu.

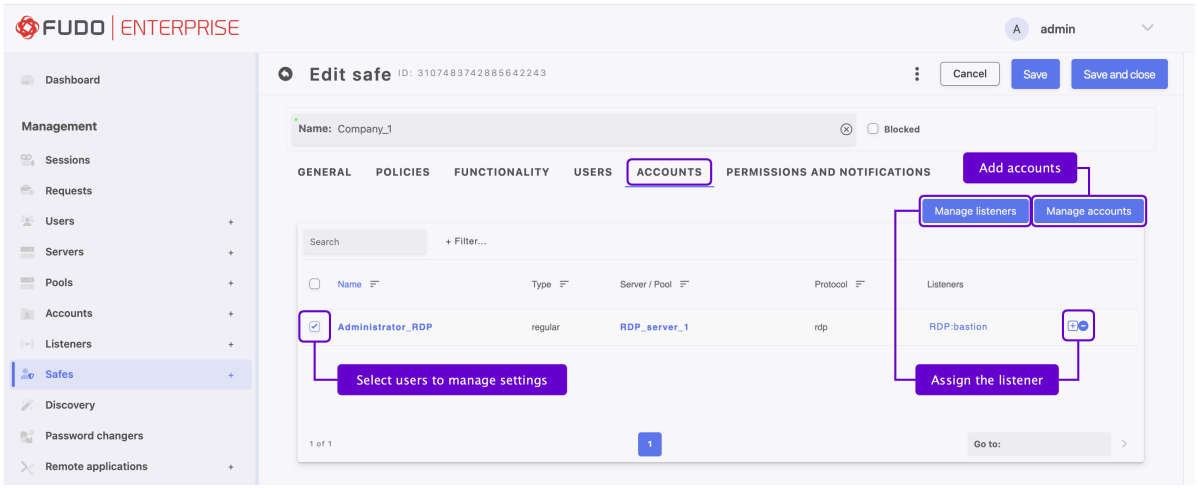


Note: Access time policy options are disabled when the *Just in time* option is enabled for the safe.

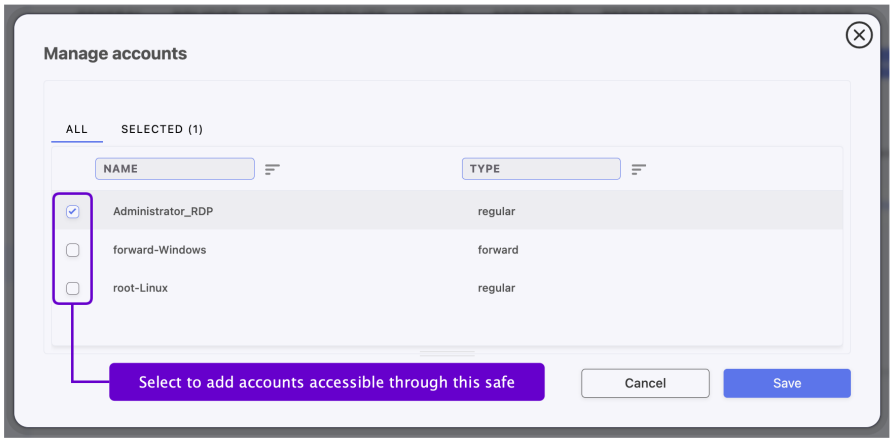
ACCOUNTS TAB

Note: To manage accounts within the safe, the user must also be assigned the *listener-read* privilege.

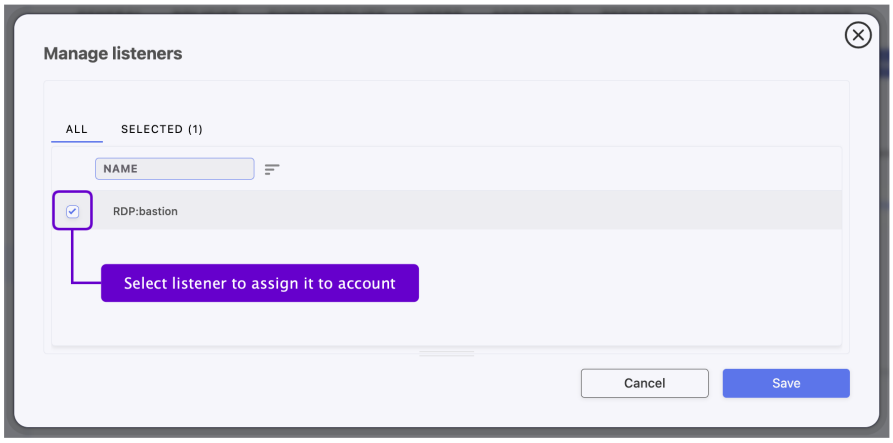
17. Select *Accounts* tab to add *accounts* accessible through this safe.



- Click *Manage accounts*.
- Mark the checkbox in front of the accounts' names to add it.



- Click *Save* to close the modal window.
- Select desired account and click *Manage listeners* to assign listeners to accounts.

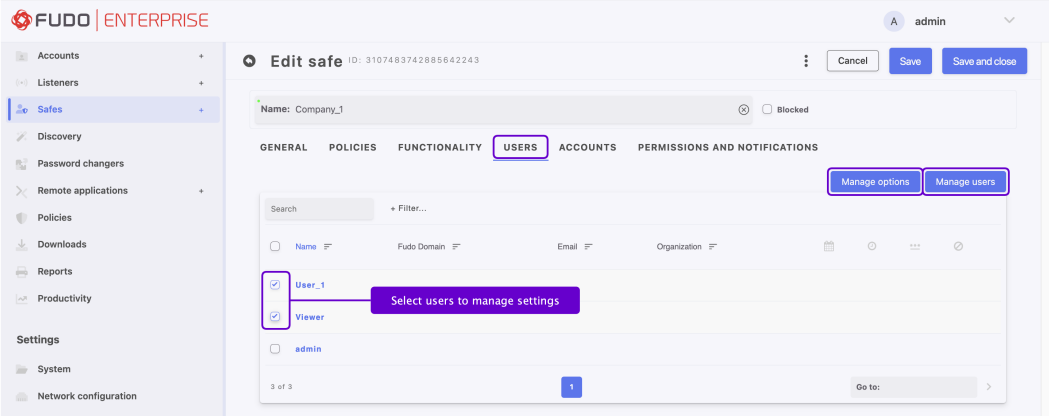


- Click *Save* to close the modal window.

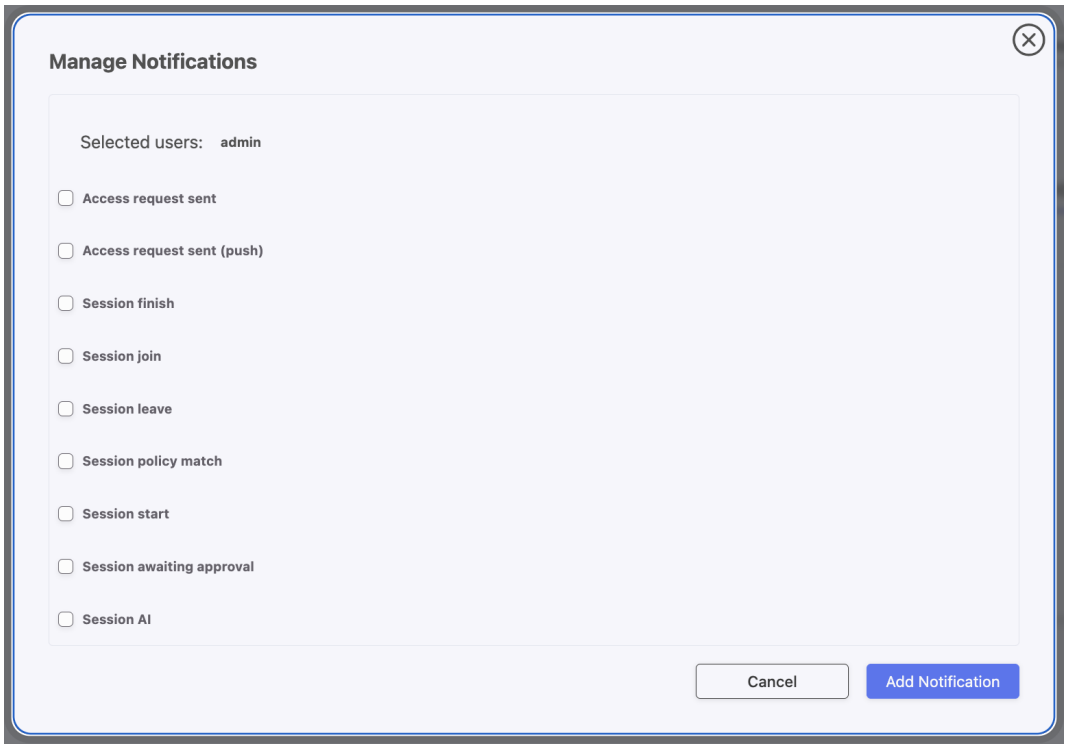
PERMISSIONS AND NOTIFICATIONS TAB

18. Select *Permissions and Notifications* tab to assign users allowed to manage this safe and specify notifications that will be enabled for the particular granted user. For more information, please refer to the *Notifications* section.

    - Click *Manage users*.
    - Mark the checkbox in front of the users' names to assign users allowed to manage this safe.



    - Click *Save* to close the modal window.
    - To define specific notification types for a user, select the checkbox in front of the desired users' names and click *Manage notifications*.



    - Click *Add notification* to close the modal window.

19. Click *Save* or *Save and close* to save the safe configuration.

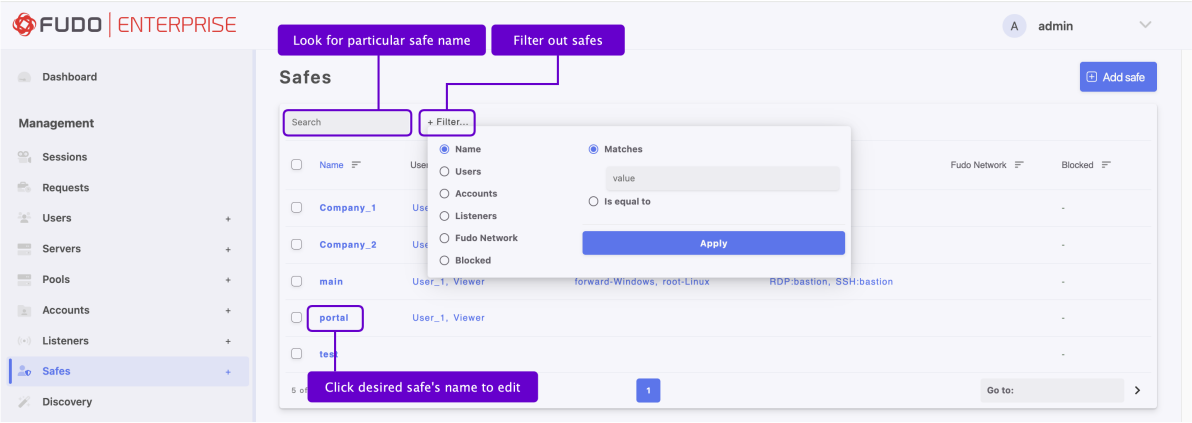
Related topics:

- *Data model*

- *Editing a safe*
- *Blocking a safe*
- *Deleting a safe*

14.2 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*.

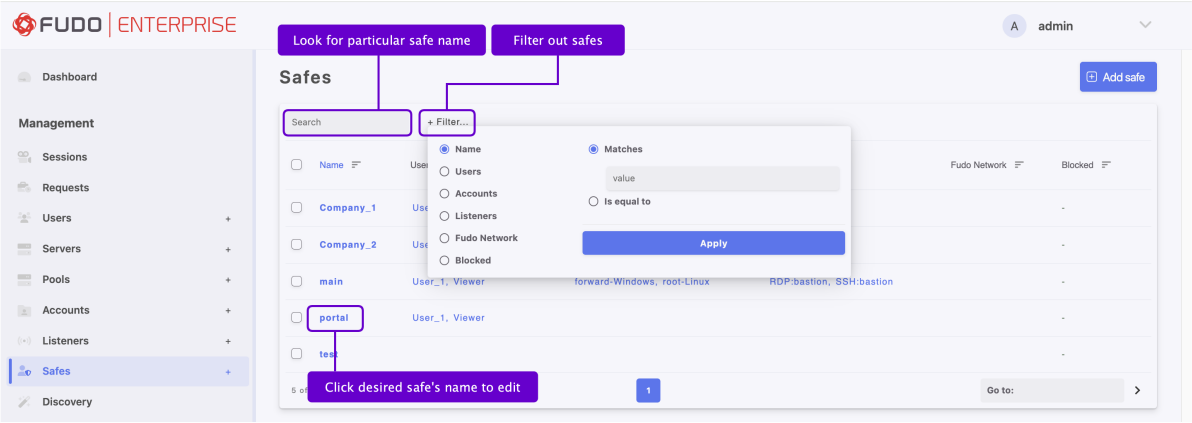
Related topics:

- *Data model*
- *Creating a Safe*
- *Blocking a safe*
- *Unblocking a safe*

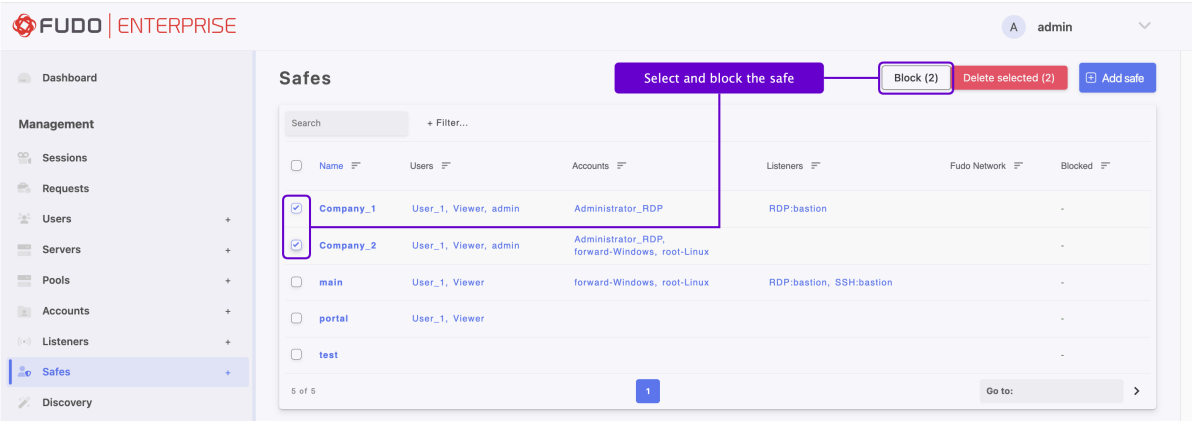
14.3 Blocking a safe

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.

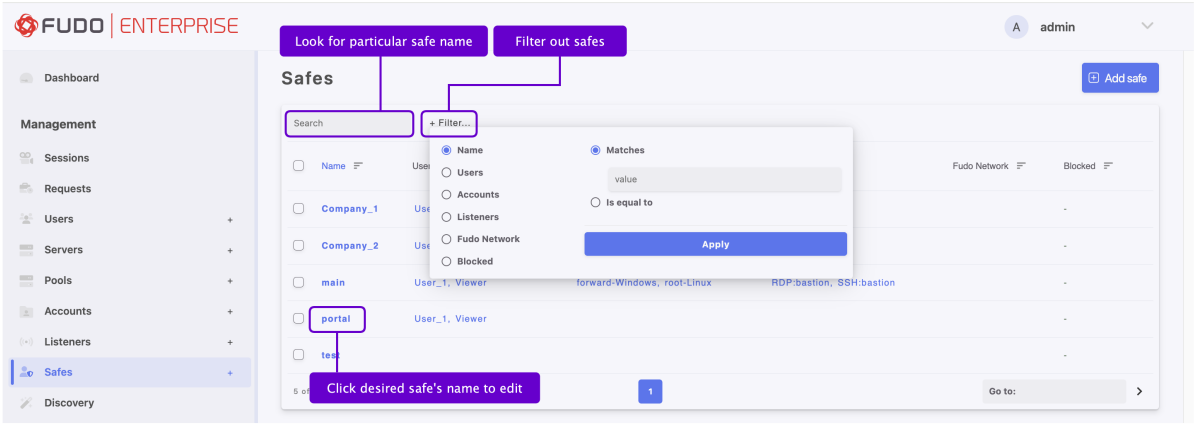
Note: To view the blocking reason, place the cursor over the red cross icon on the listeners list.

Related topics:

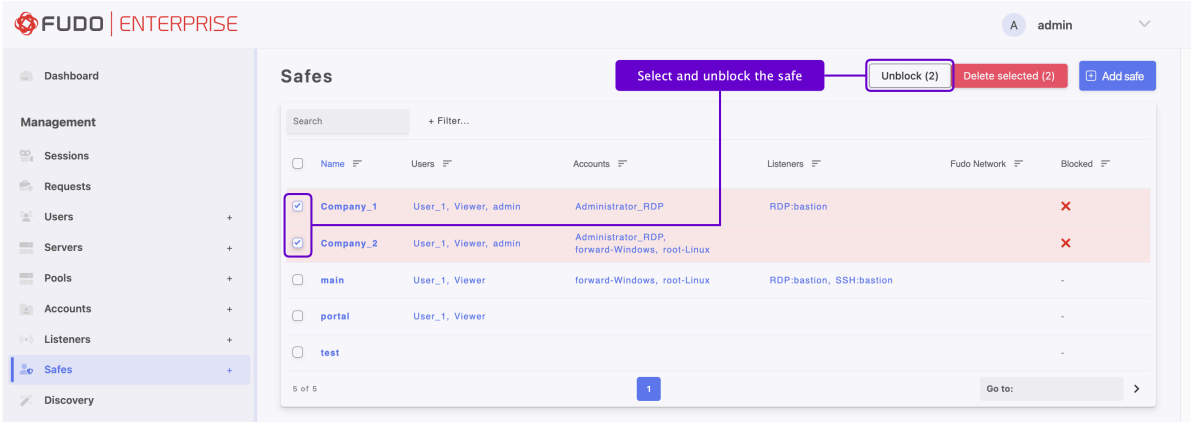
- *Unblocking a safe*
- *Data model*
- *Creating a Safe*
- *Blocking a safe*

14.4 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.

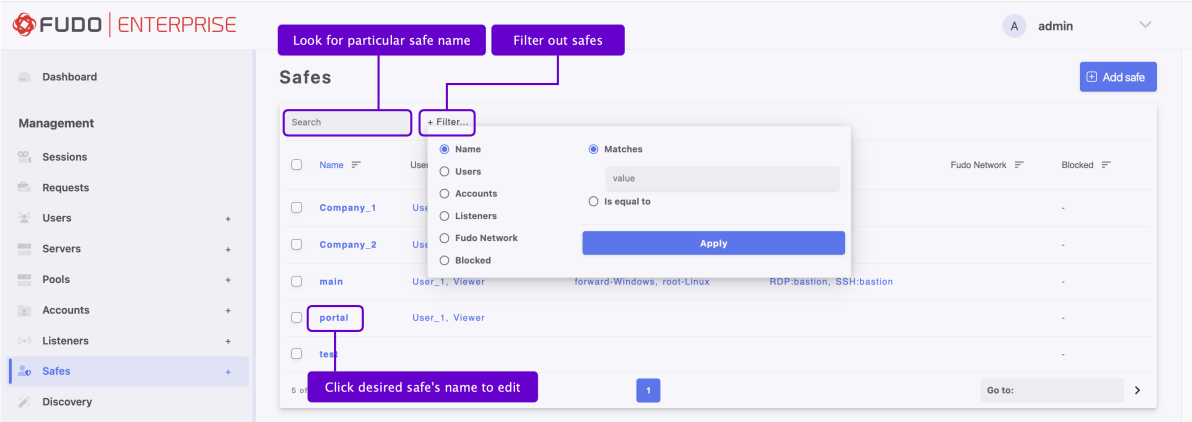
Related topics:

- *Blocking a safe*
- *Data model*
- *Creating a Safe*
- *Deleting a safe*

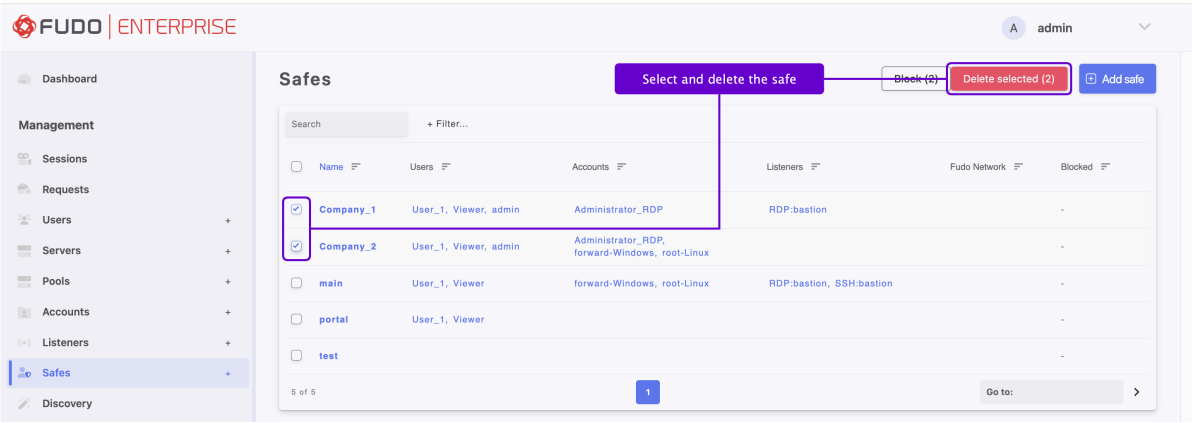
14.5 Deleting a safe

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*

CHAPTER 15

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.

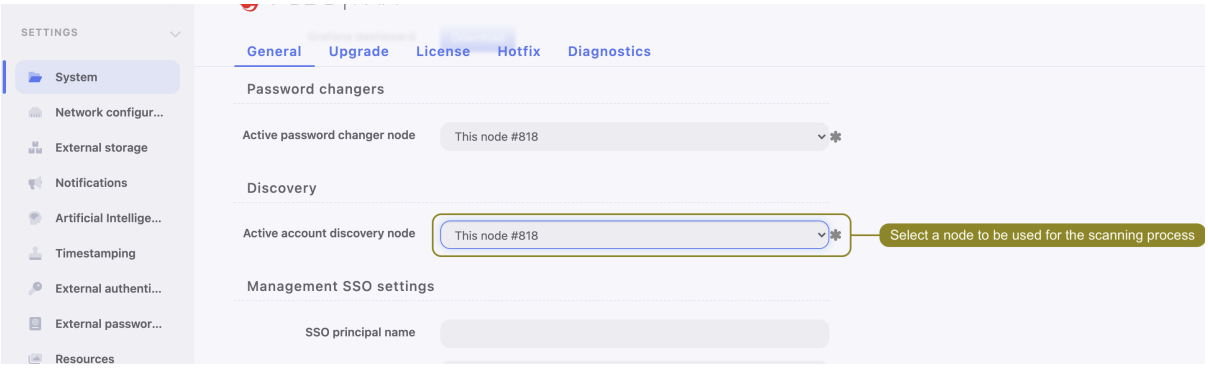
The Discovery function needs two objects to provide the most efficient results:

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.



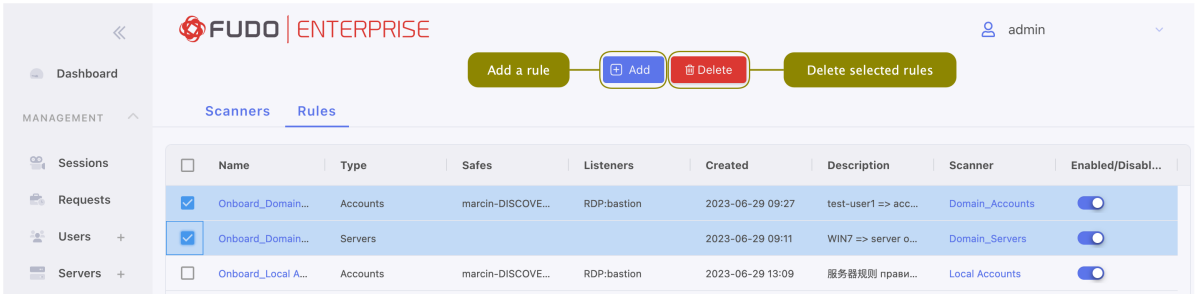
15.1 Creating a rule

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.

15.1.1 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*



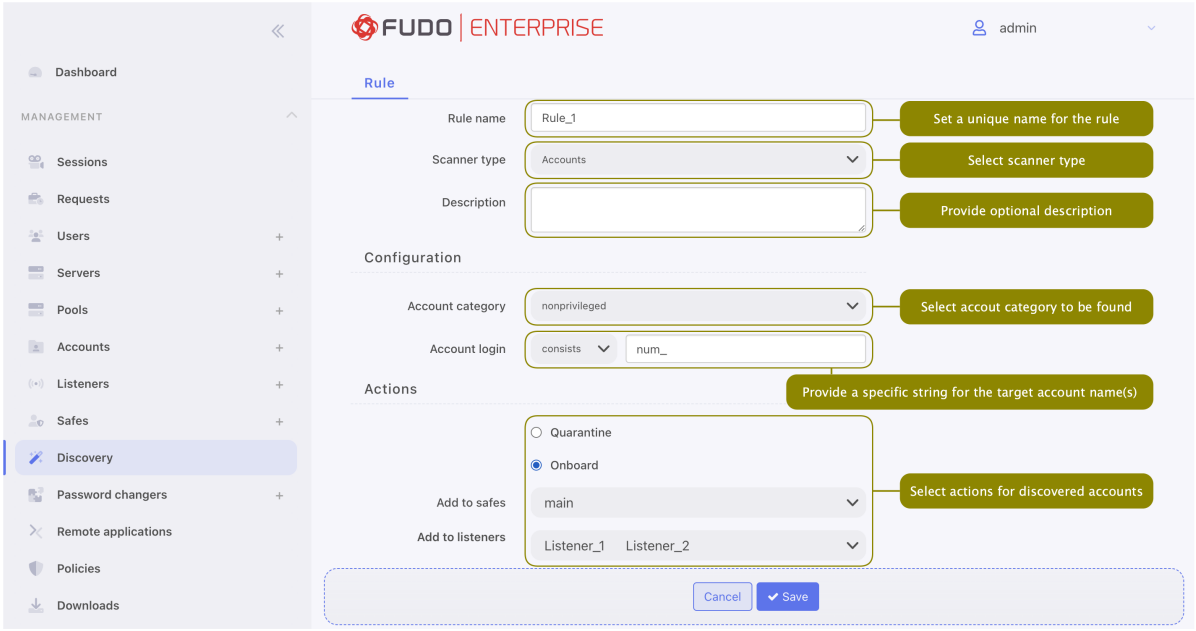
3. Enter rule's name.
4. Select *Accounts* from the *Scanner type* drop-down list.
5. Optionally, enter rule's description.
6. In *Configuration* section:

   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*.

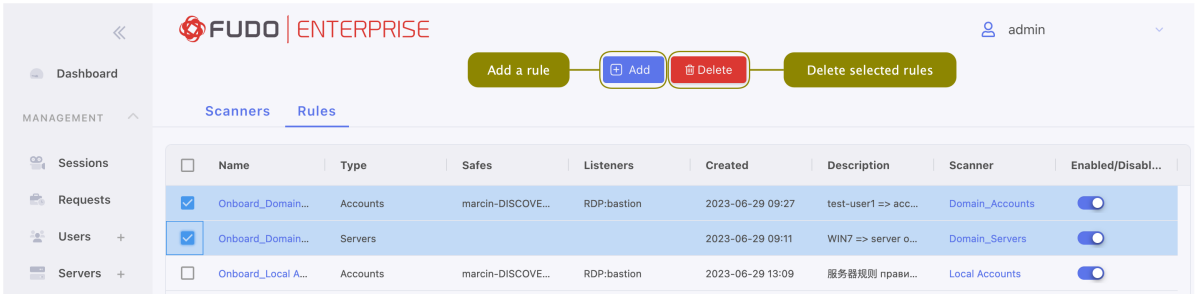
Related topics:

- *Managing rules*
- *Creating a scanner*

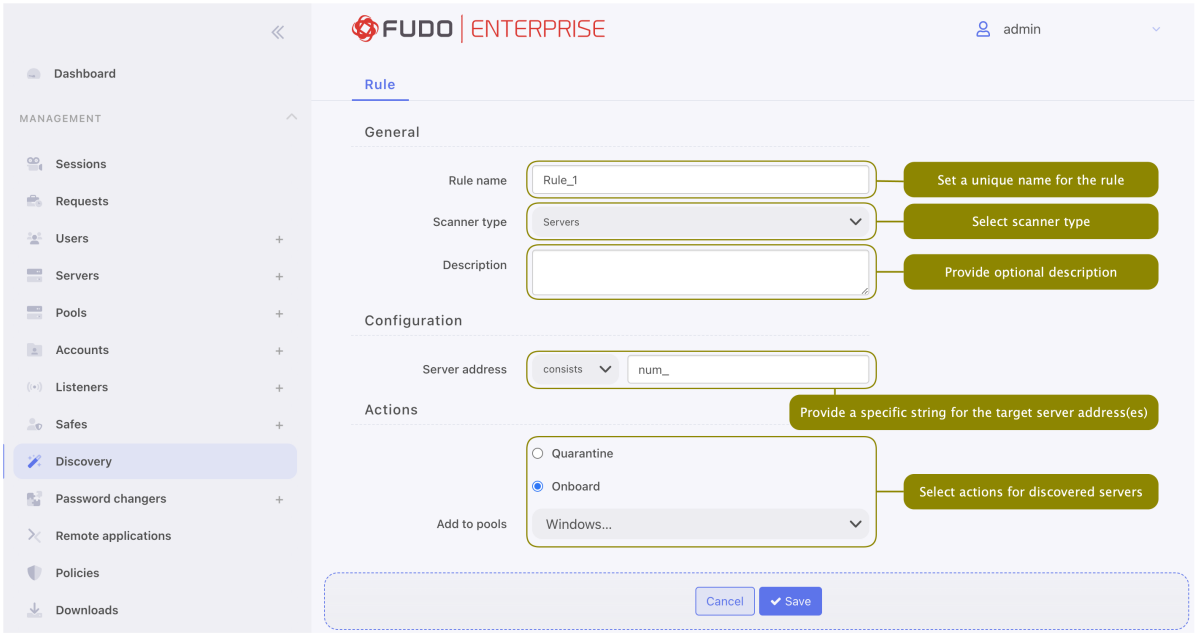
15.1.2 Creating a rule for servers

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.

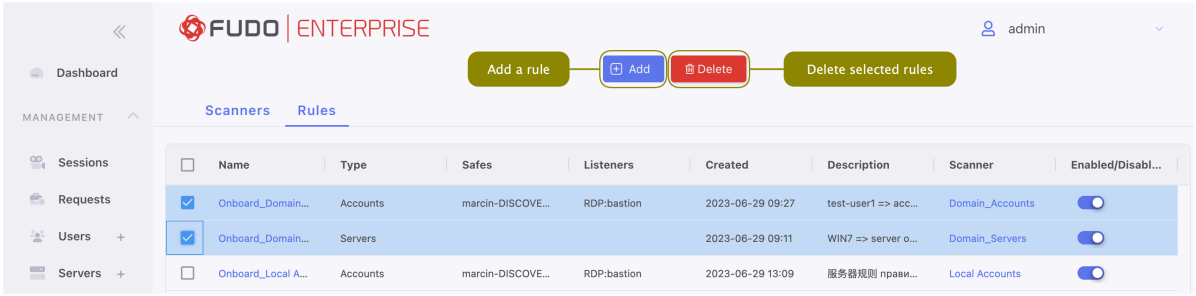
- Taking the server on a quarantine will block this server in the domain.
- Onboarding the server unblocks the server in the domain.
- If the server is removed from the domain, it will be removed from Fudo Enterprise after the next scan step.

Related topics:

- *Managing rules*
- *Creating a scanner*

15.2 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*

15.3 Creating a scanner

15.3.1 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.

Password change policy, password changer, and password 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. *Base DN* value to indicate the exact location in the domain (optional). Use following format: `cn=##username##,dc=example,dc=com`.

   7.5. *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.

   7.6. *Account* to be used to connect to the target server.

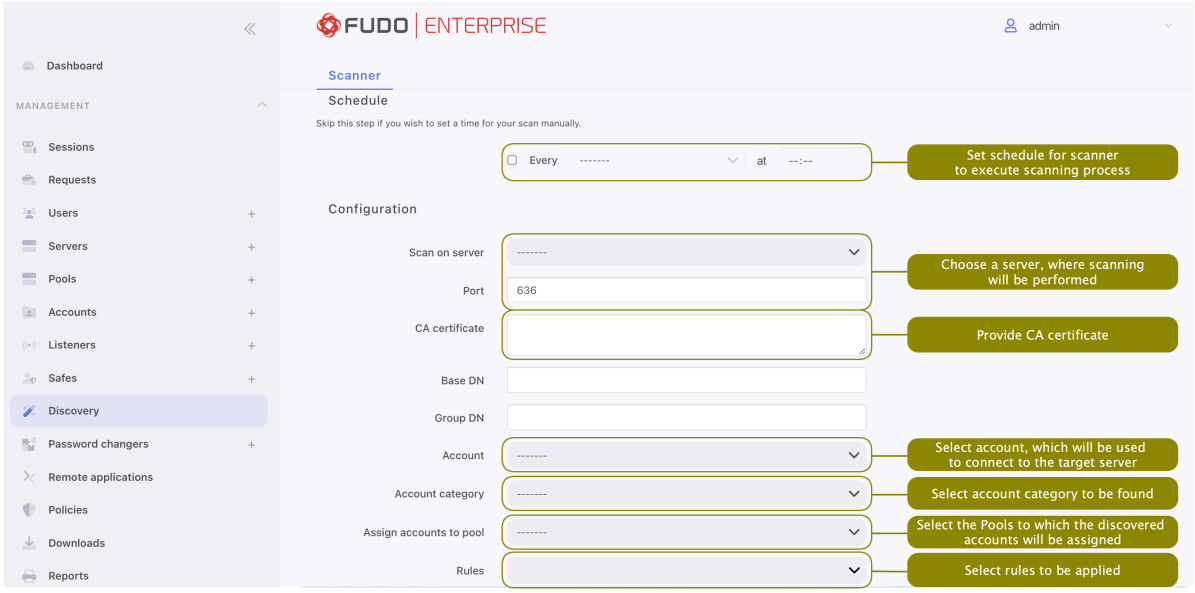
   7.7. Select *Account category* to be found (`privileged`, `non-privileged` or `all`).

   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).

   7.8. Select the *Pools* to which the discovered accounts will be assigned.

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. In *Password Changers* section select *Password change policy*, *Password changer*, and *Password verifier* which will be automatically assigned to discovered accounts.



Note:

- Administrator can predefine password changer variable values in Password changers configuration (refer to the *Custom password changers* section).
- Predefining values is optional. If variable is not defined, it will take value from account that password changer is assigned to.
- Default password changers don't have predefined variable values.

8. Click Save.

Related topics:

- *Creating a rule*
- *Managing discovered accounts*

15.3.2 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. *Base DN* value to indicate the exact location in the domain (optional). Use following format: `cn=##username##,dc=example,dc=com`.

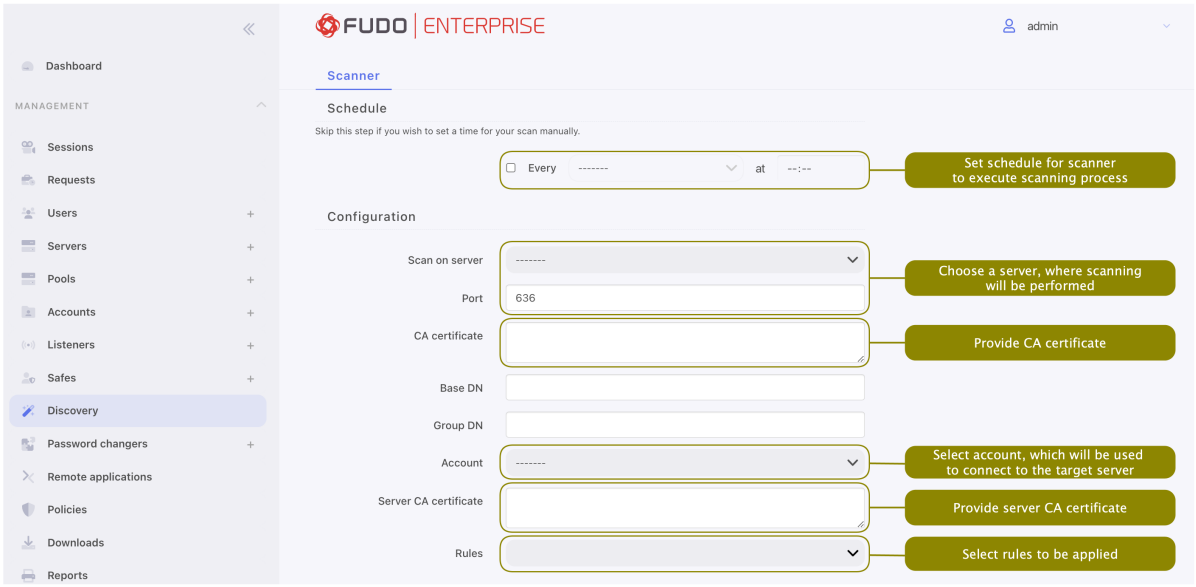
   7.5. *Group DN* value to indicate the exact group in the domain (optional). Use following format: `cn=##username##,dc=example,dc=com`.

   Note: If only the *Base DN* is provided, the scanner will search the entire domain. Specifying the *Base DN* is required.

   7.6. *Account* to be used to connect to the target server.

   7.7. *Server CA certificate* which will be assigned to the discovered servers.

   7.8. 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*

15.3.3 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.

Password change policy, password changer, and password 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.

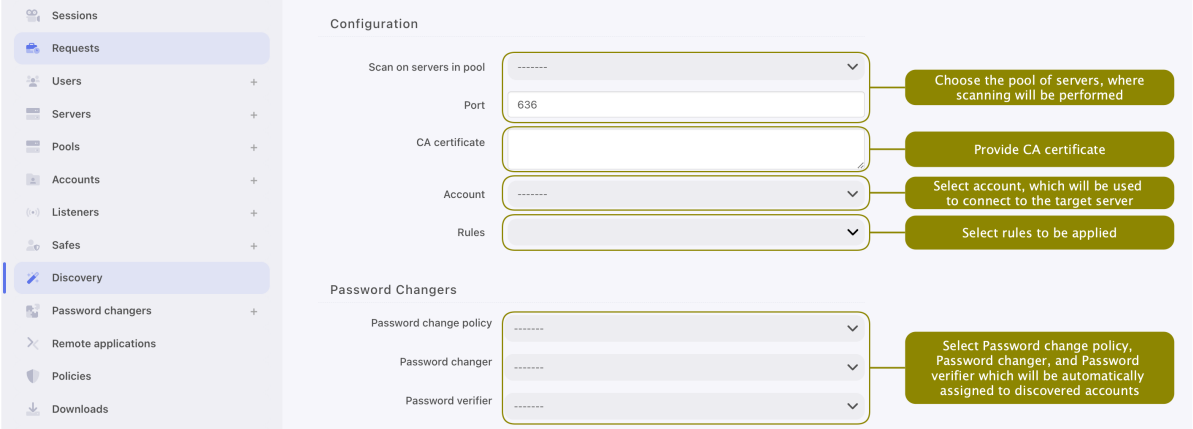
   7.2. Specify port number in the *Port* field.

   7.3. Provide *CA certificate*.

   7.4. 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.

   7.5. 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 *Password Changers* section select *Password change policy*, *Password changer*, and *Password verifier* which will be automatically assigned to discovered accounts.

Note:

- Administrator can predefine password changer variable values in Password changers configuration (refer to the *Custom password changers* section).
- Predefining values is optional. If variable is not defined, it will take value from account that password changer is assigned to.
- Default password changers don't have predefined variable values.

---

8. Click Save.

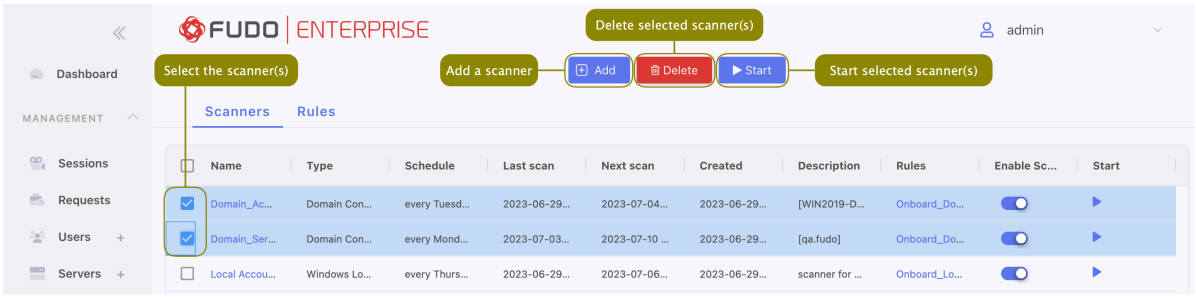
Related topics:

- *Creating a rule*
- *Managing discovered accounts*

15.4 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.

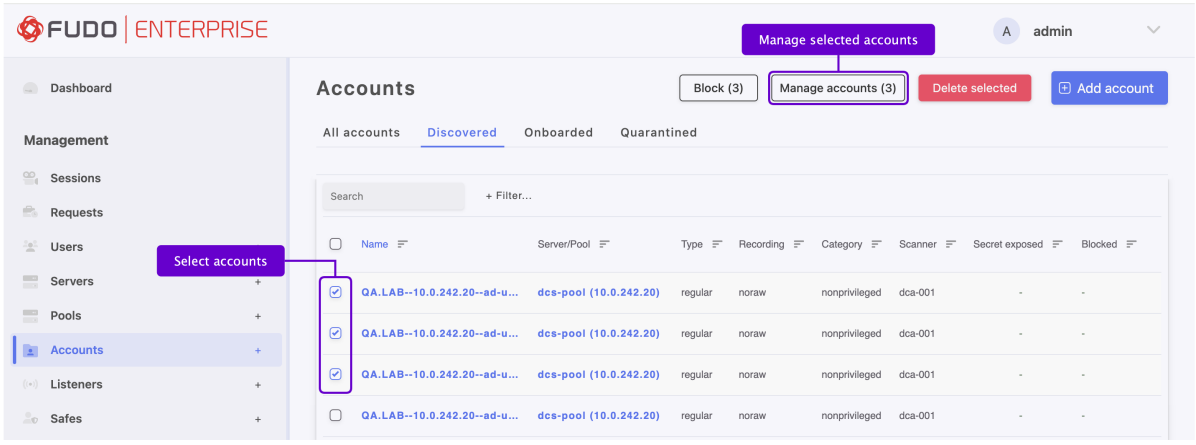


Related topics:

- *Creating a rule*
- *Managing discovered servers*
- *Managing discovered accounts*

15.5 Managing discovered accounts

Discovered, *onboarded* and *quarantined* accounts are available in the main Accounts view.

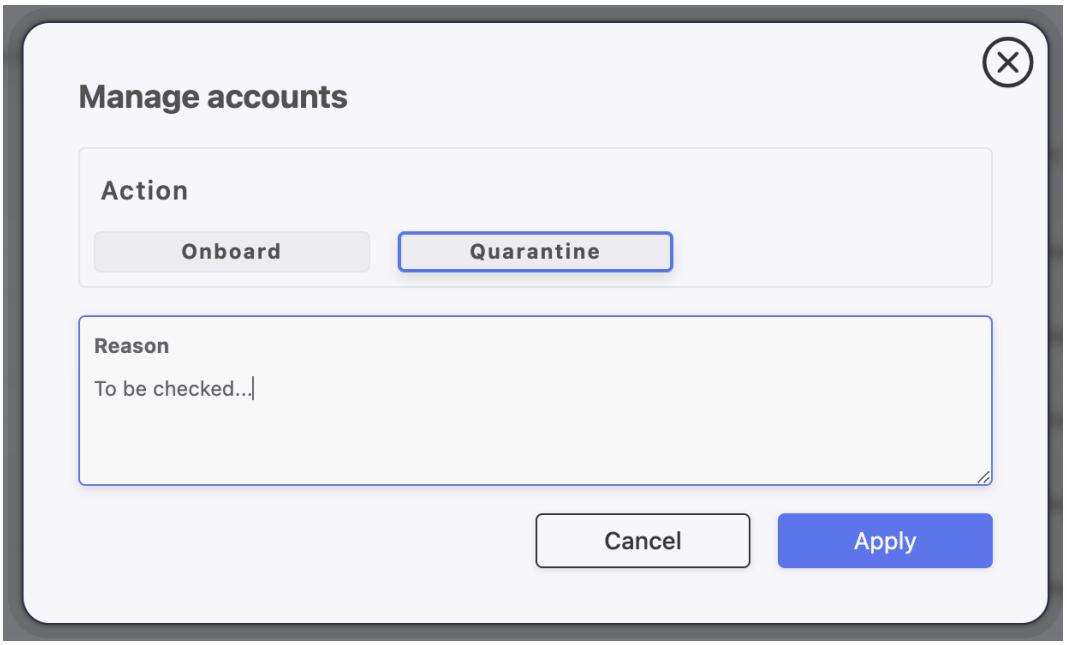


Note: Usually, *discovered* accounts are not onboarded automatically due to a lack of automatic rule in the system. Administrator can manually onboard them by choosing the Manage Accounts option.

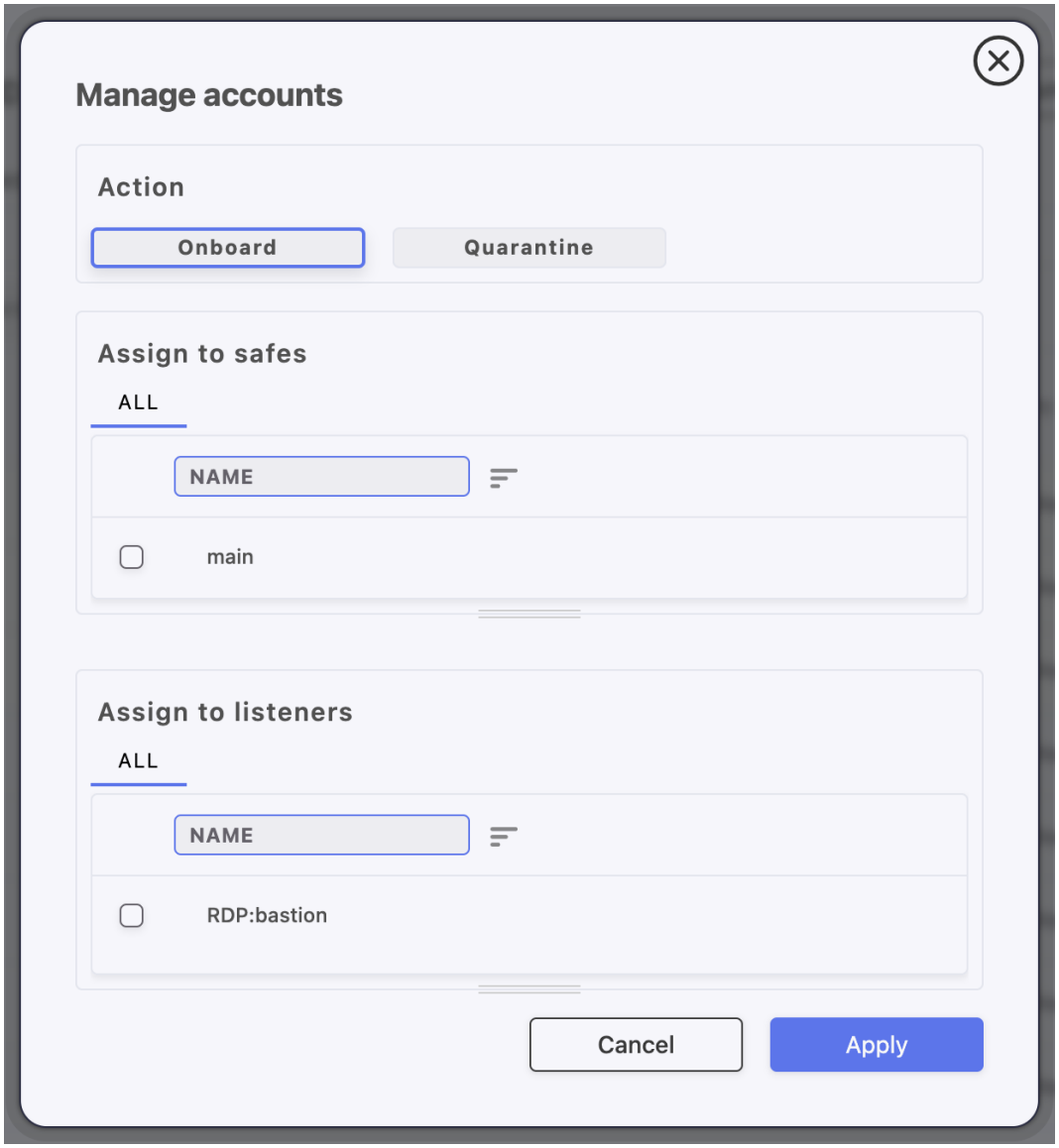
1. Select *Management* > *Accounts* and respectful tab: *Discovered*, *Onboarded* or *Quarantined*.
2. Choose the accounts to be onboarded or quarantined by selecting the respective checkboxes next to their names.

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*

15.6 Managing discovered servers

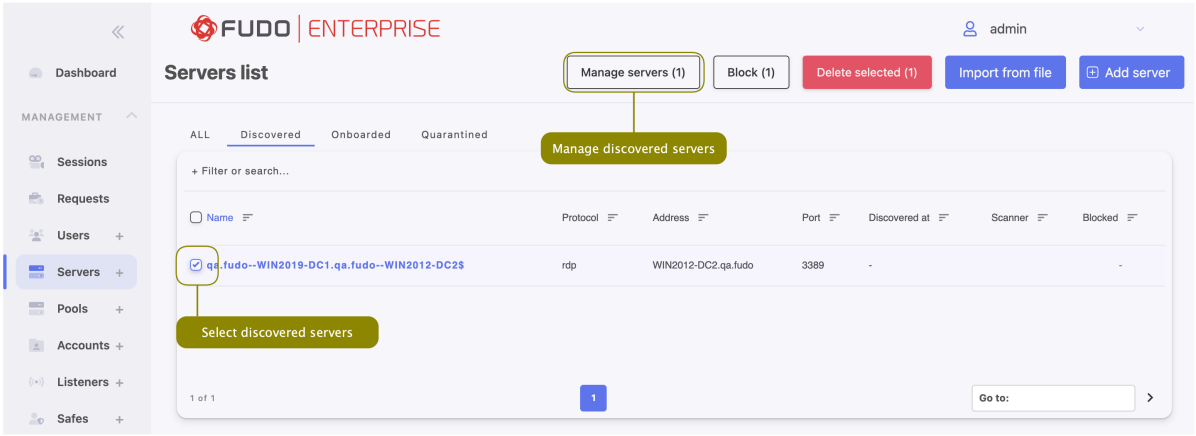
Discovered, *onboarded* and *quarantined* servers are available in the main Servers view.

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.

---

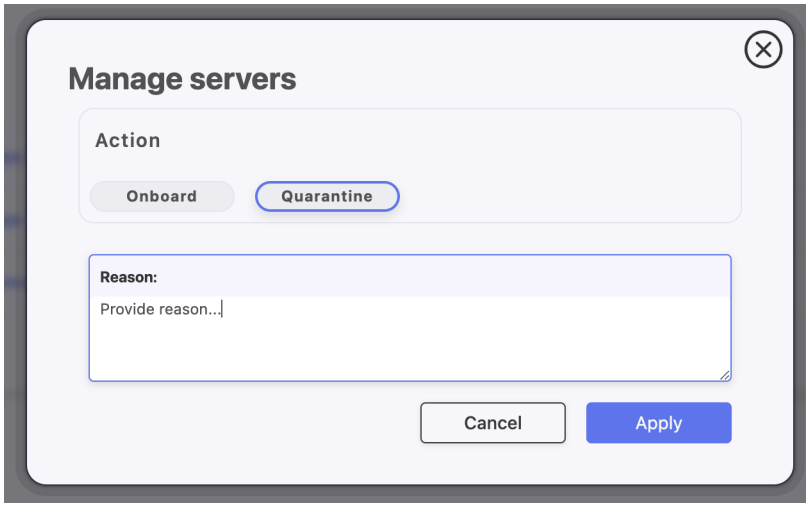
1. Select *Management* > *Servers* and respectful tab: *Discovered*, *Onboarded* or *Quarantined*.
2. Choose servers to be onboarded or quarantined by selecting the respective checkboxes next to their names.
3. Click on the *Manage servers* option on the top of the functional menu - a modal will pop 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*

CHAPTER 16

Password changers

Fudo Enterprise features *password changers*, which enable managing credentials to privileged accounts on monitored servers.

Password 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 password 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

16.1 Password changer policy

Password changer policy defines specifics of how frequently the password should be changed and password complexity requirements.

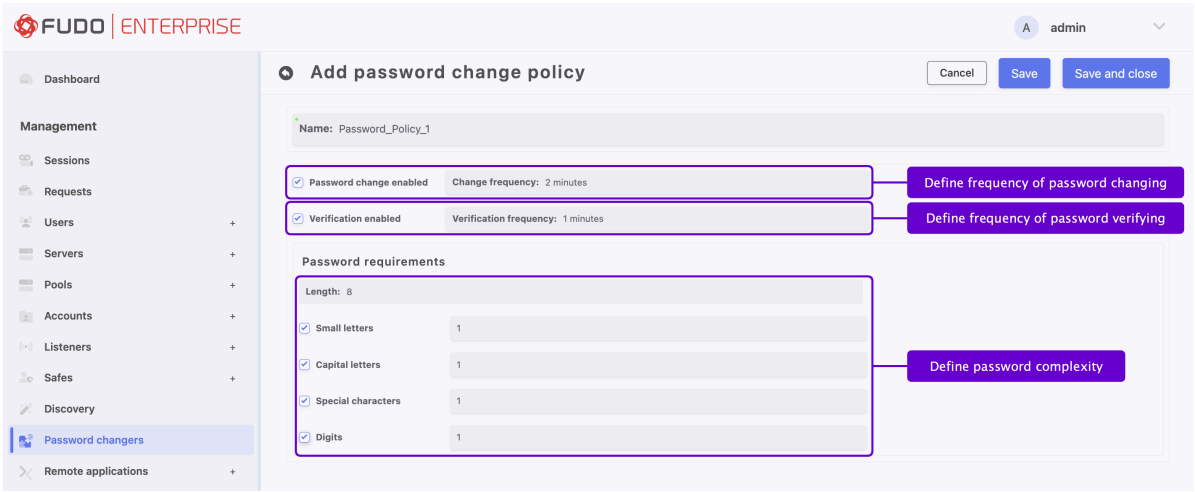
16.1.1 Defining a password changer policy

1. Select *Management* > *Password changers*.
2. Go to *Password policies* tab.
3. Click *+ Add password policy*.
4. Enter object name.
5. Select the *Password change enabled* option and specify the time interval between each password change.
6. Select the *Verification enabled* option and specify the time interval between each password verification.
7. Define password complexity.

Parameter	Description
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.

Note: The sum of the enforced password requirements cannot be greater than the specified password length.

7. Click *Save*.

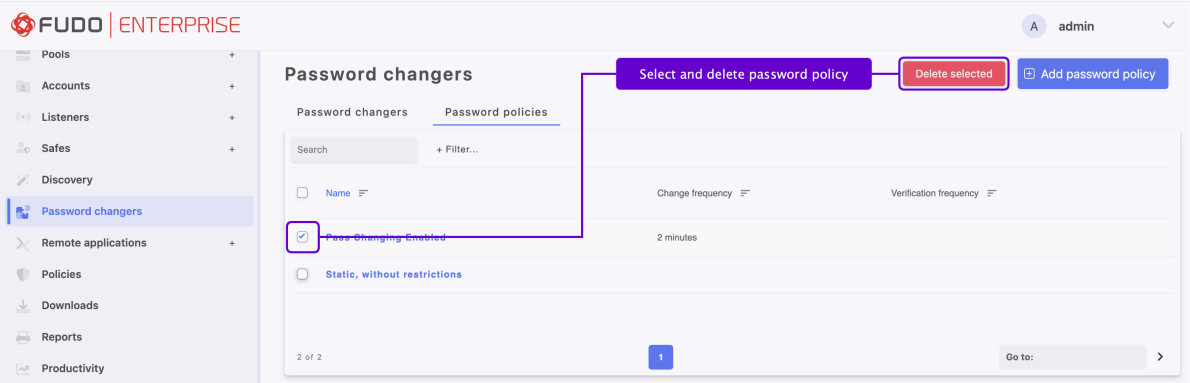


16.1.2 Editing a password changer policy

1. Select *Management* > *Password changers* > *Password policies*.
2. Go to *Password policies* tab.
3. Find and click desired object to open its configuration page.
4. Modify configuration parameters as needed.
4. Click *Save*.

16.1.3 Deleting a password changer policy

1. Select *Management* > *Password changers*.
2. Go to *Password policies* tab.
3. Find and select desired objects.
4. Click *Delete*.
5. Click *Confirm* to confirm deletion of selected objects.



Related topics:

- *Data model*
- *Accounts*
- *Custom password changers*
- *Setting up password changing on a Unix system*

16.2 Custom password changers

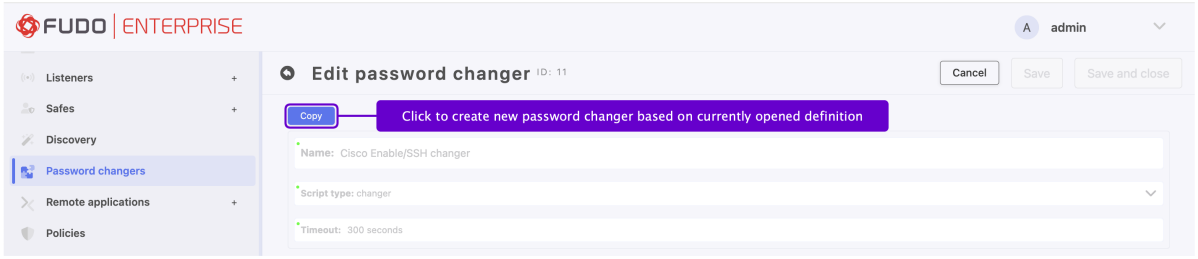
Custom password changers enable defining a set of commands executed on a remote host in case the built-in password changers cannot handle a specific use case scenario.

Note: In cluster configuration, the node responsible for changing passwords on monitored systems is configured in system settings. For more information refer to *Password changers - active cluster node* topic.

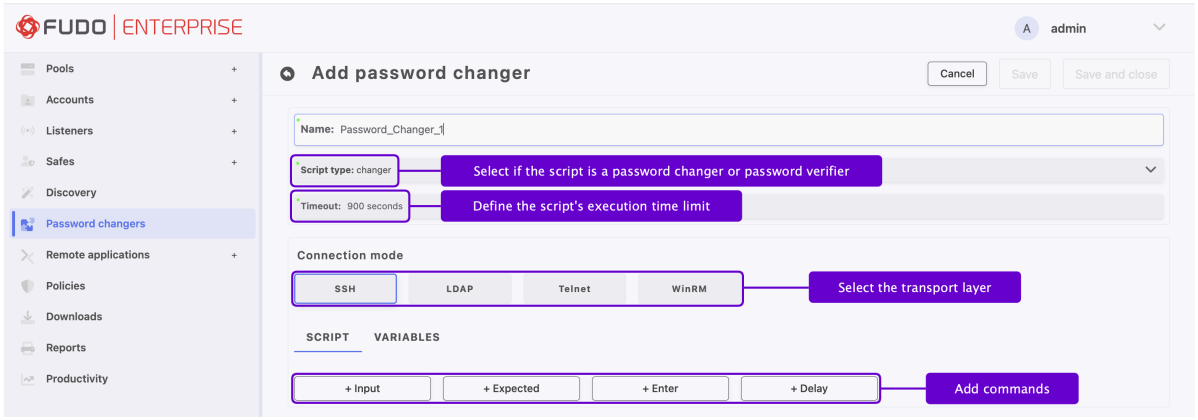
16.2.1 Defining a custom password changer

1. Click + icon in the main menu next to the *Password changers* tab, or
2. Select *Management* > *Password changers* and click + *Add password changer*.

Note: Alternatively, you can edit existing password changer and click Copy to create a new password changer based on currently opened definition.



3. Define the password changer's name.
4. From the *Script type* drop-down list, select if the script is a password changer or password verifier.
5. In the *Timeout* field, define the script's execution time limit.
6. In the *Connection mode* section, click *SSH, LDAP, Telnet,* or *WinRM* to select the transport layer.
7. 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.

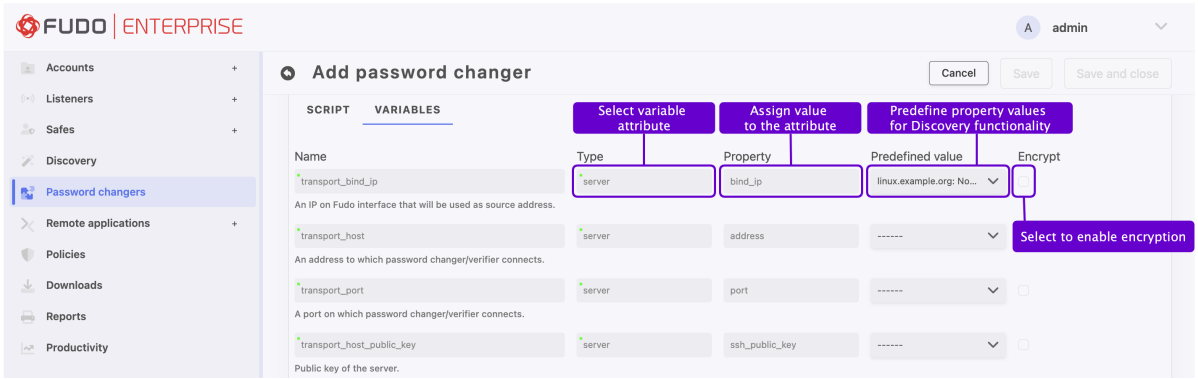
Warning:

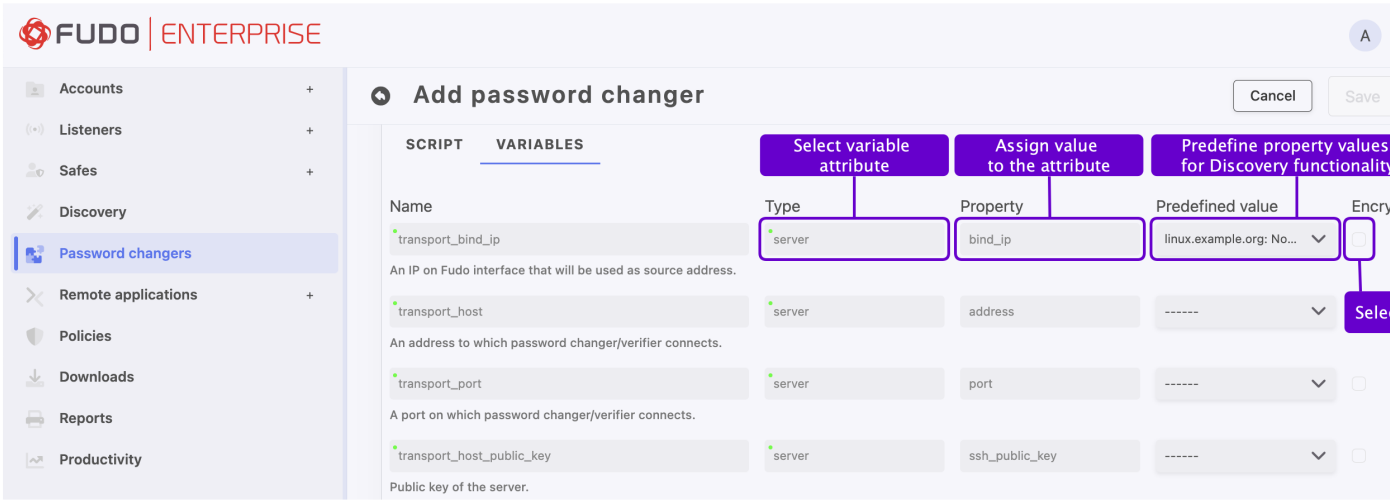
- To handle a password change, you must use an account (`transport_login` and `transport_secret`) that has delegated *Reset user passwords and force password change at next logon* permissions for the *Organizational Unit (OU)* containing the users whose passwords will be changed, or the account must be a member of the *Account Operators* group.
- To configure **WinRM** password 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.**

8. 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%%`).

9. Repeat steps 7-8 to add more commands.
10. 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 password changer assigned to the account during the *Discovery* process will not require any additional configuration.

10. Click *Save*.
11. *Define password change policy* and *assign the password changer to account*.

Note: Example

In this password 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	`%%account_new_secret%%`	A value of the `account_new_secret` variable would be a new password.
10	EXPECTED	`Retype New Password`	Expected terminal output with 'Retype New Password' phrase in it.
11	INPUT	`%%account_new_secret%%`	A value of the `account_new_secret` variable would be a new password.
12	INPUT	`echo $?`	
13	EXPECTED	`0`	

Variables

Variable name	Object type	Object property	Encrypt
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	✗

16.2.2 Editing a custom password changer

1. Select *Management* > *Password changers*.
2. Click the name of desired password changer.
3. In the *Script* tab, edit selected commands.
4. Click *Delete* to remove selected command.
5. Click *Save*.

16.2.3 Deleting a custom password changer

1. Select *Management* > *Password changers*.
2. Select custom password changer and click *Delete*.
3. Confirm deleting selected objects.

Related topics:

- *Password changers - active cluster node*
- *Connection modes*
- *Accounts*
- *Password changer policy*
- *Setting up password changing on a Unix system*

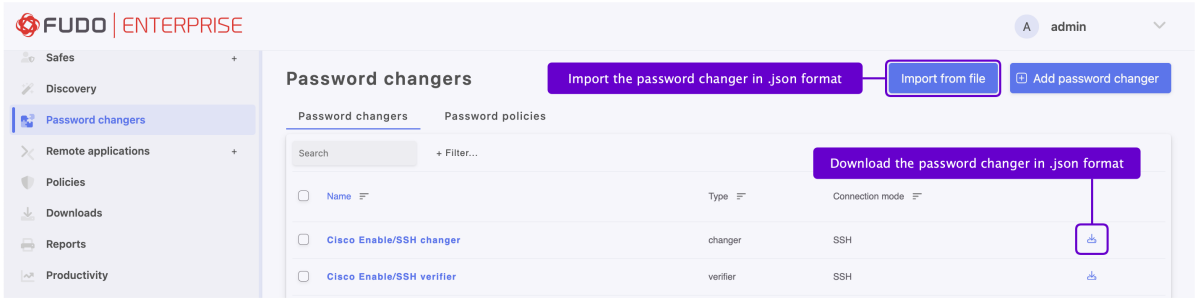
16.3 Importing and exporting password changers

Password changers created in Fudo Enterprise can be downloaded and imported into another instance of Fudo Enterprise.

16.3.1 Exporting a password changer

To download selected password changer:

1. Select *Management* > *Password changers*.
2. Go to *Password changers* tab.
3. Click the download icon next to the selected password changer to download it.



16.3.2 Importing a password changer

To import the `.json` file of a password changer:

1. Select *Management* > *Password changers*.
2. Go to *Password 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 password changer.
5. Click *Send data* to import the file, or *Clear data* to abort the import.

Related topics:

- *Data model*
- *Accounts*
- *Custom password changers*
- *Setting up password changing on a Unix system*

16.4 Connection modes

Connection modes specifies transport layer used in the password change process. The transport layer determines the list of available commands and default variables.

16.4.1 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 password 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 passwords.
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 password changer is assigned to the account, the default string will be used to determine the password prompt.
transport_port	A port number that the password changer/verifier connects to.
transport_secret	Secret used to authorize the account to execute password change.
account_login	Login of the user whose password is being changed.
account_new_secret	System default variable initiated with the value automatically generated by Fudo.

16.4.2 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: Password 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 password changer/verifier connects to.
transport_login	An account on the target system authorized to change passwords.
transport_port	A port number that the password changer/verifier connects to.
transport_secret	Secret used to authorize the account to execute password change.
transport_server_certificate	Certificate of the target server.
account_domain	Domain of the user whose password is being changed.
account_new_secret	System default variable initiated with the value automatically generated by Fudo.

16.4.3 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 password.

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 password changer/verifier connects to.
transport_login	An account on the target system authorized to change passwords.
transport_port	A port number that the password changer/verifier connects to.
transport_secret	Secret used to authorize the account to execute password change.
account_login	Login of the user whose password is being changed.
account_new_secret	System default variable initiated with the value automatically generated by Fudo.

16.4.4 WinRM

WinRM transport layer uses Windows Remote Management protocol to interface with remote operating system and facilitate password 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 Password Changer and Verifier allow changing and verifying passwords 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 password 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.**

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 password changer/verifier connects to.
transport_login	An account on the target system used to change passwords. It has to be different from the account on which the password is being changed (account_login variable).
transport_port	A port number that the password changer/verifier connects to.
transport_secret	Secret used to access the account to execute password change.
account_login	Login of the user whose password is being changed.
account_new_secret	System default variable initiated with the value automatically generated by Fudo.

Related topics:

- *Custom password changers*
- *Password changer policy*

- *Setting up password changing on a Unix system*

16.5 Setting up password changing on a Unix system

This topic contains an example of setting up password changing on a Unix system.

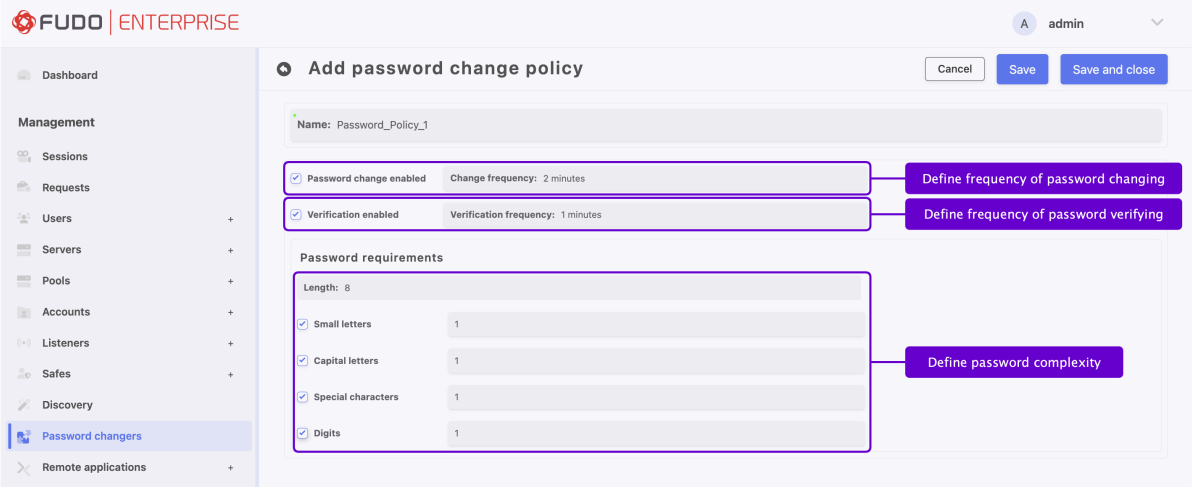
Adding a password change policy

1. Select *Management* > *Password changers*.
2. Go to *Password policies* tab.
3. Click *+ Add password policy* to create a new password changing policy.
4. Provide password 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 *Password change enabled* option and define how frequently the password will be changed.
6. Select the *Password verification enabled* 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. Provide the number of characters comprising the password.
8. Select desired password complexity options and provide the minimal number of characters for each.



9. Click *Save* to store password changer policy.

Assigning a password changer and a verifier to the privileged account

1. Select *Management* > *Accounts*.
2. Find and click desired account object.
3. Go to *PASSWORD CHANGERS* tab.

Note: Regular account type, password method and login are required to configure password changers.

4. In the *Password changers* field select `Unix/SSH changer` script from the *Add changer* drop-down list.
5. In the *Password changers* window, in the *Timeout* field, define the script's execution time limit.
6. Review and modify default values.

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	*Enter manually:* `root`
transport_method	*Enter manually:* `password`
transport_password_prompt	`constant`
transport_port	`cont_int: 22`
transport_secret	`cont_int_mr_jenkins: *****`
account_login	`cont_int_mr_jenkins: mr_jenkins`

7. Click *Save* to close *Password changers* window.

Note:

- Variables starting with `transport_` are the transport layer variables determining connection parameters with the target host.
- Password changer variables can be assigned values manually or initialized with properties of other objects.

8. In the *Password verifiers* field select `Unix/SSH verifier` script from the *Add verifier* drop-down list.
9. In the *Password verifiers* window, in the *Timeout* field, define the script's execution time limit.
10. Review and modify default values.

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 *Password verifiers* window.

12. Next, click *Save* in the upper right corner to save the changes to the account definition.

Related topics:

- *Connection modes*
- *Custom password changers*

CHAPTER 17

Policies

Policies are patterns definitions facilitating proactive session monitoring. In case a defined pattern is detected, Fudo Enterprise can automatically take respective actions and notify the administrator about the current situation.

Fudo Enterprise divides policy definition by its basis: **AI module** or **Regular Expression**:

- when the `AI module` option is chosen as a basis of the policy, Fudo Enterprise reacts on reaching the specified *Threat Probability* Threshold,
- when the `regular expression` option is chosen for the policy's base, the system analyses the defined expression's input or output.

Both types of policies react by taking the following actions:

- sending e-mail message,
- sending SNMP TRAP notification,
- pausing connection,
- terminating connection,
- blocking the user.

17.1 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.

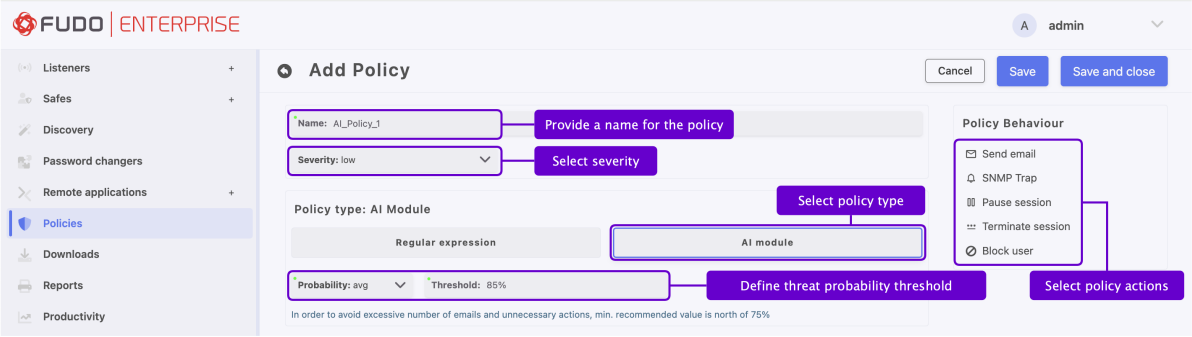
5. In the *Policy type* section, select the *AI module* button.
6. Select `min`, `avg` (default) or `max` option for the *Threat Probability Threshold* field and provide the value.

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`.

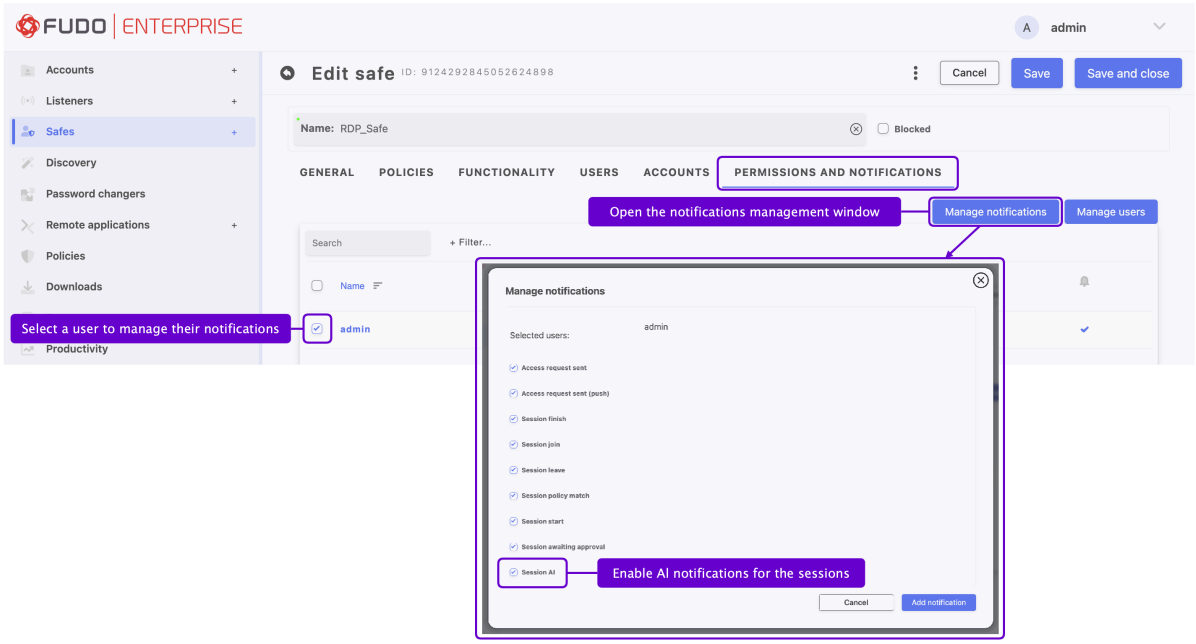
In order to avoid an excessive number of emails and unnecessary actions, min. recommended value is above 75%.



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*.

17.2 AI module-based policy examples

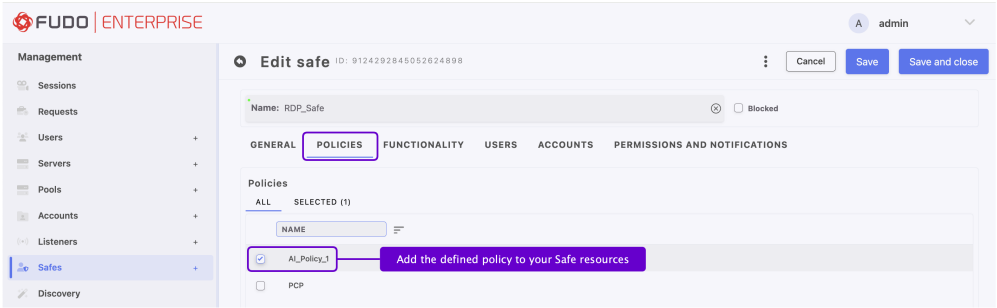
Example 1. Sending SNMP TRAP notifications about suspicious sessions.

To configure the policy to send SNMPv3 TRAP notifications about suspicious sessions, follow the procedure:

1. Create a user for SNMPv3 service:
   - Select *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:

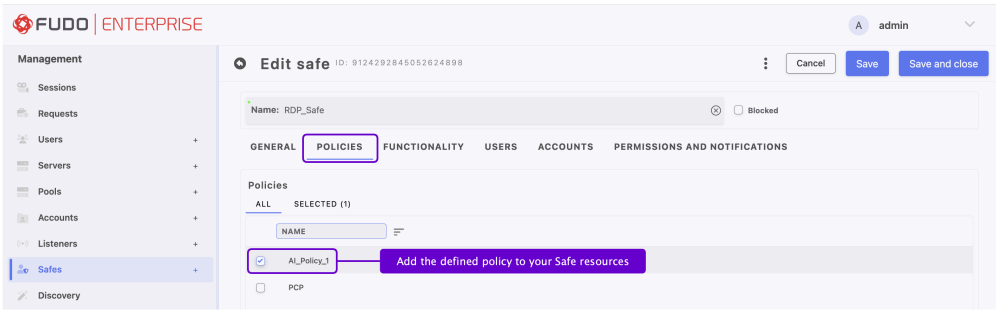
1. Create policy:
   - Select *Management* > *Policies*.
   - Click *+ Add policy*.

- 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*

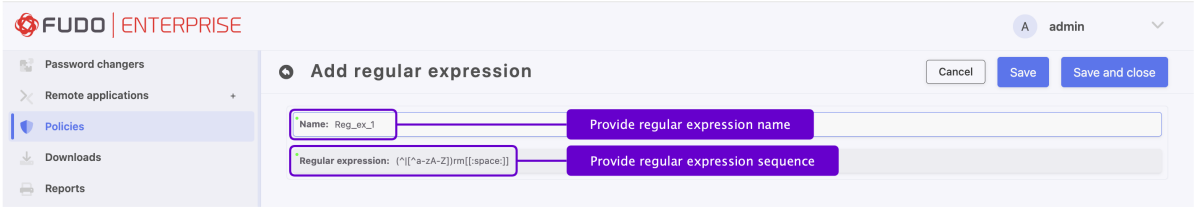
17.3 Regular expression-based policy

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`)

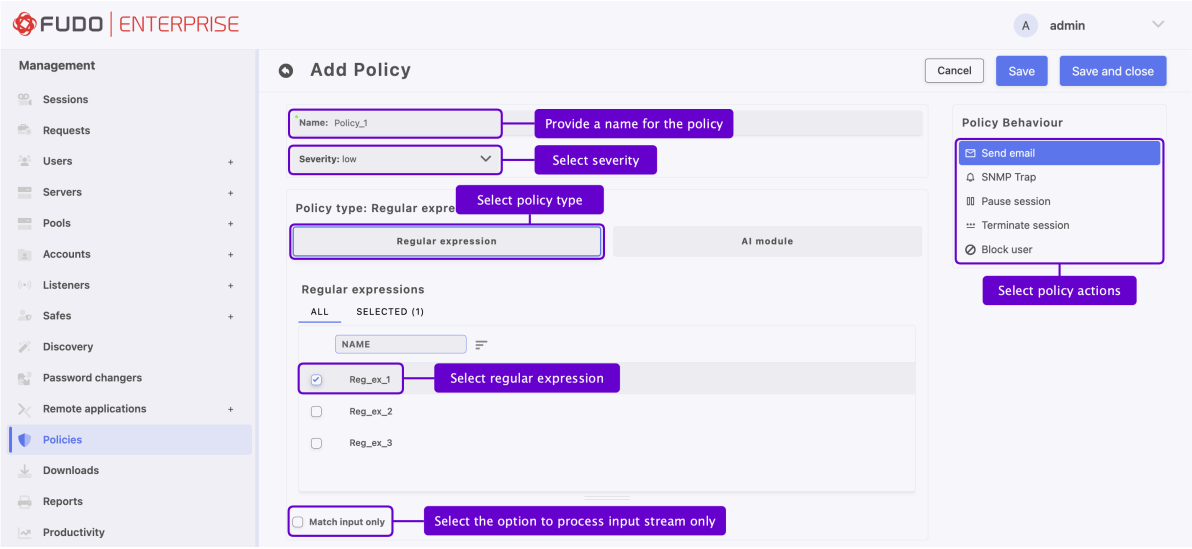
```
(^|[^a-zA-Z])rm[[:space:]]+-([rR]f|f[rR])
```

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.

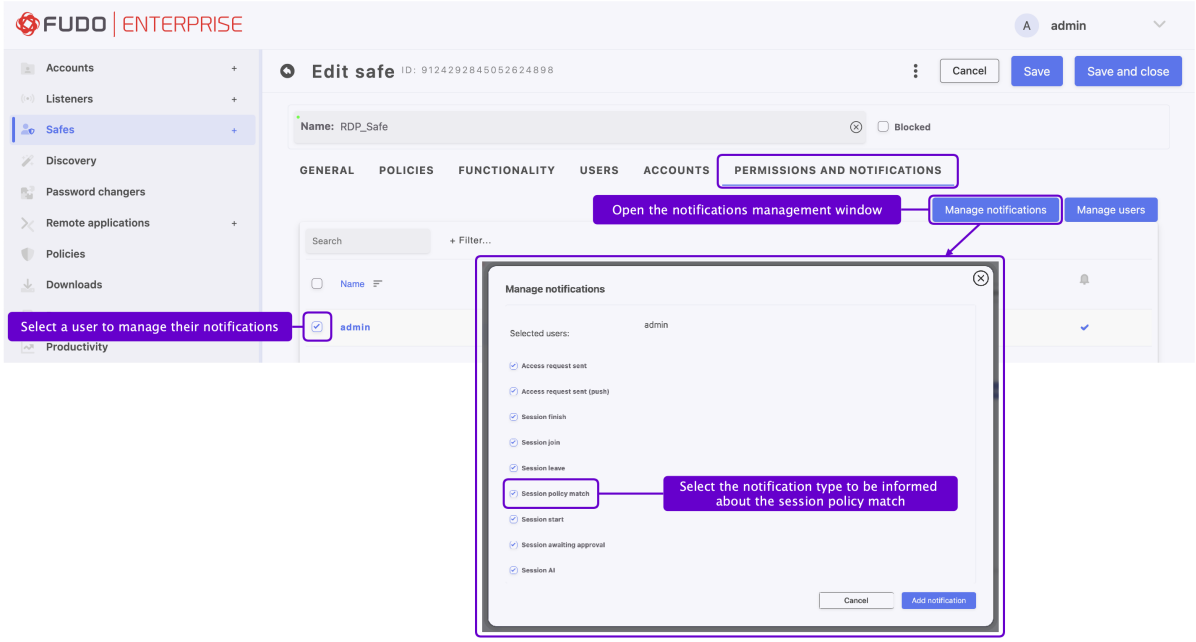
Note: In RDP, VNC and MySQL protocols only input data is processed.

---

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.

Related topics:

- *Artificial Intelligence (AI)*
- *AI Behavioral Analysis in Sessions*
- *Safes*
- *Terminating connection*
- *Notifications*
- *Security*

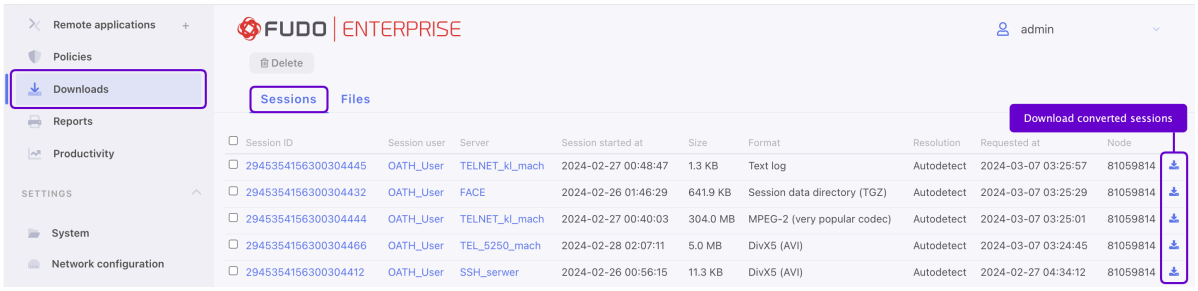
CHAPTER 18

Downloads

The **Downloads** tab allows for tracking the conversion progress of session recordings and files transferred during SFTP sessions, previously selected for download.

18.1 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 Management > Sessions. For detailed instructions on how to export a session, and available file formats, please refer to the *Exporting sessions* section of this manual.



18.2 Files

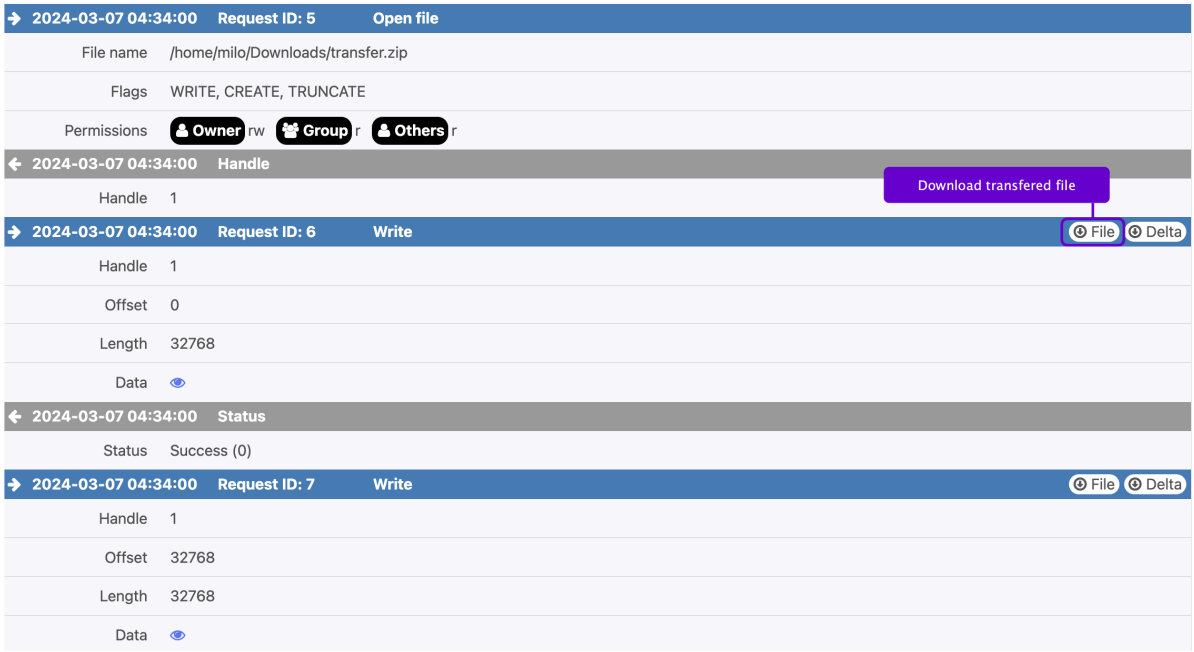
The **Files** tab is designated for managing the downloads of large files that originate from recorded sessions via the SFTP protocol. If the selected file exceeds the 50 MB threshold, it undergoes an encoding process and subsequently appears in the **Files** tab, ready for download. Files smaller than 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:

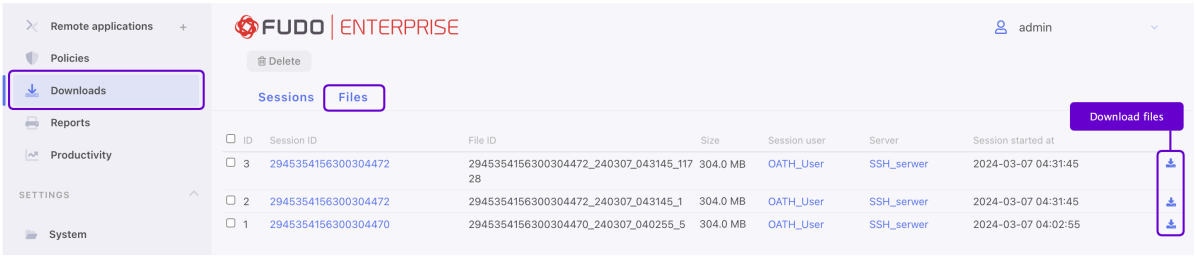
1. Select *Select* > *Sessions*.

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*

CHAPTER 19

Account activity in the Access Gateway

Fudo Enterprise allows configuring an option to be informed about existing connection.

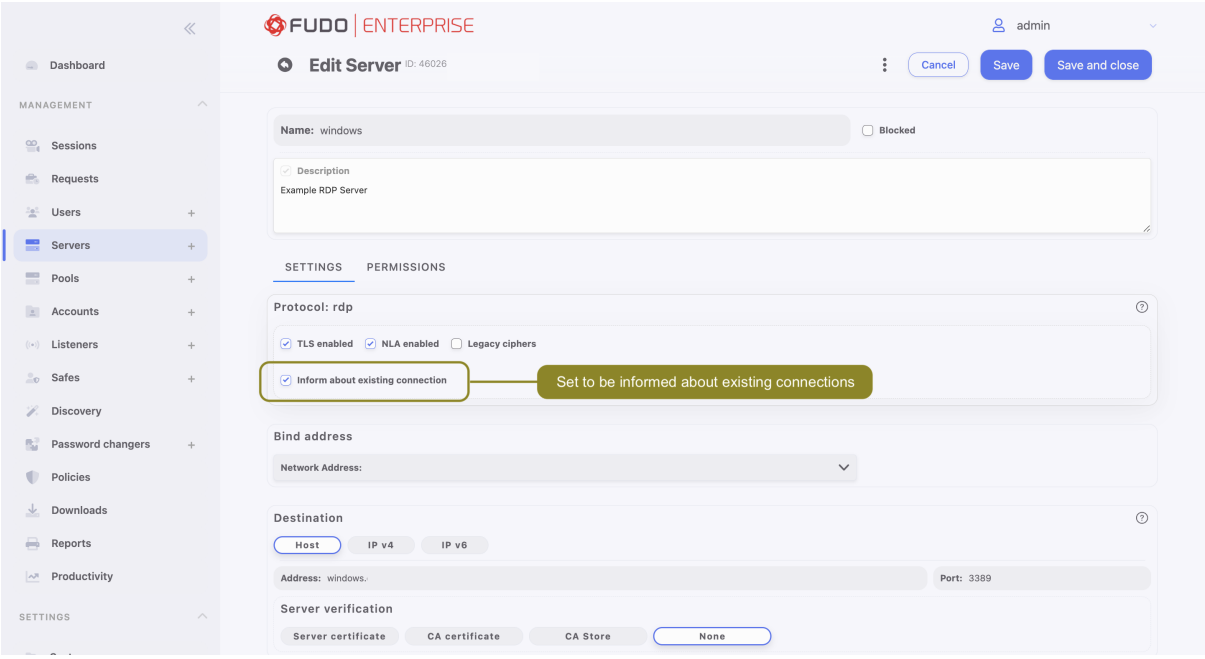
The **Resource in use** feature works while establishing connection to the target server, to which another user is already connected via the same account. If the user continues establishing connection, the session is terminated.

> **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*.

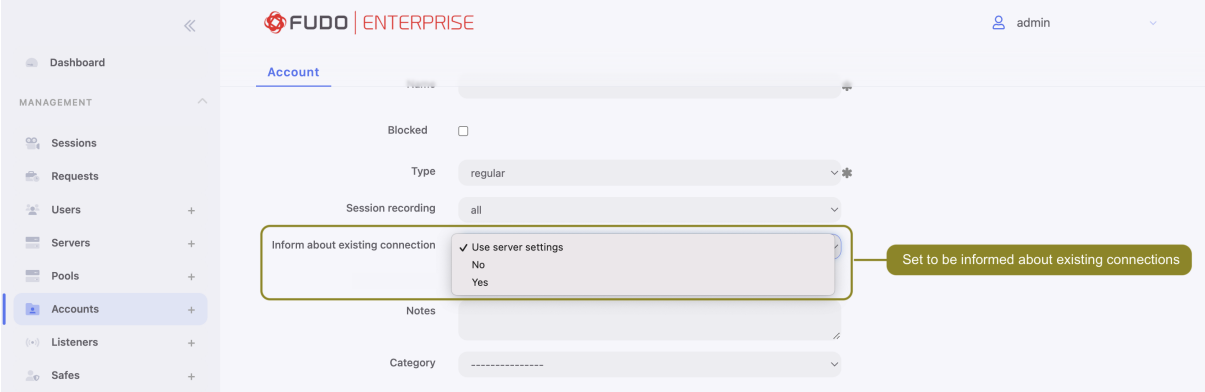
- Define filters to limit the number of objects displayed on the list, or select an RDP server that needs to be edited right from the list.
- Check the *Inform about existing connection* option in the *Settings* section.



- Click *Save* or *Save and close*.

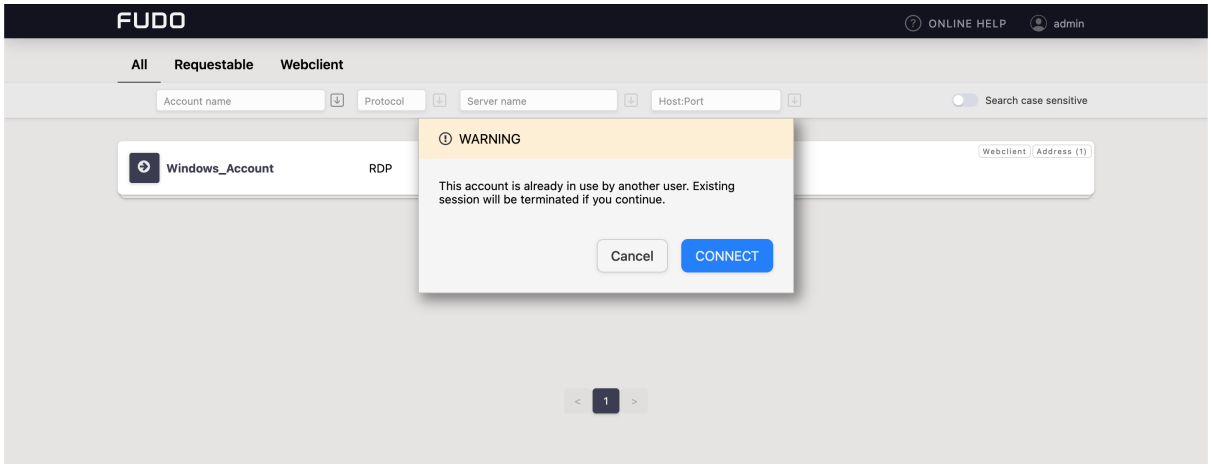
2. Select *Management* > *Accounts*.

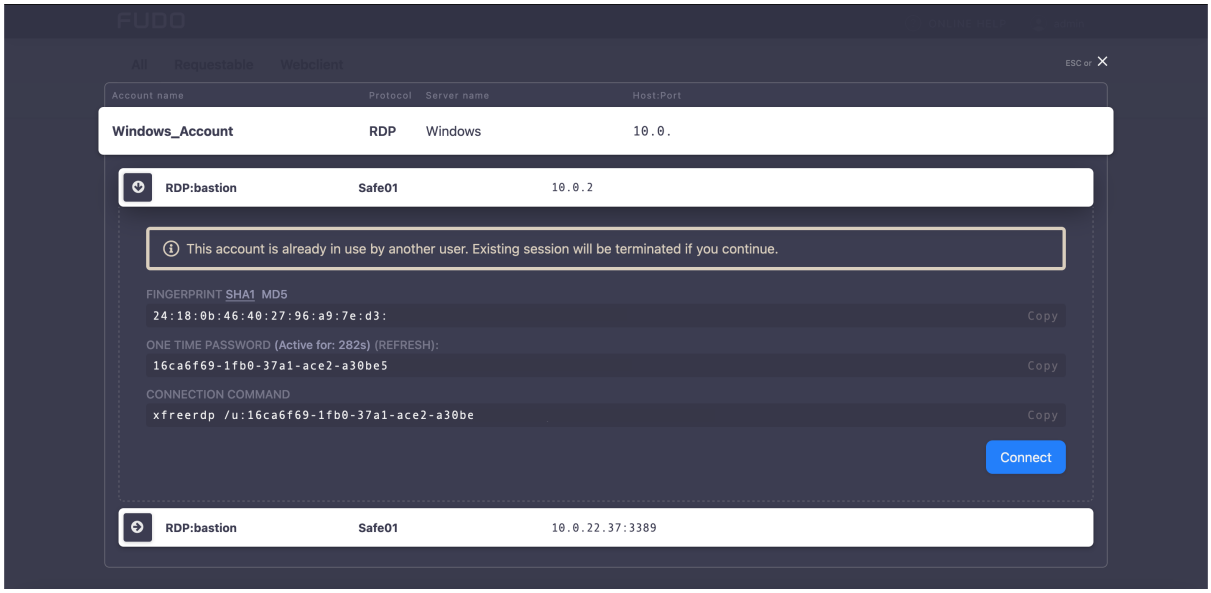
- Define filters to limit the number of objects displayed on the list, or select an account with access to an RDP server that needs to be edited right from the list.
- In the *Inform about existing connection* field select:
  - `Use server settings` to inherit the settings of the server, which was added 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 Access Gateway. Here is the default message:

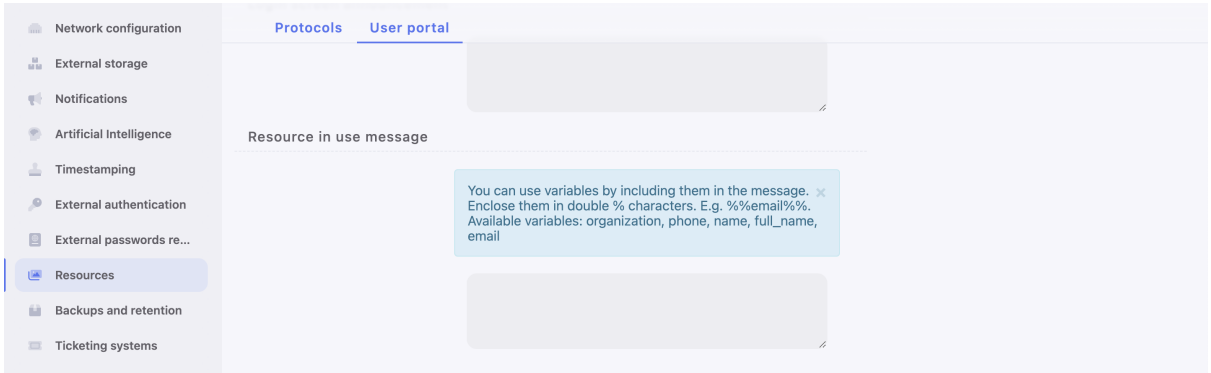




You can customize that message by including variables (`organization`, `phone`, `name`, `full_name`, or `email`), enclosed in double %% symbols. E.g., `%%email%%`.

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*

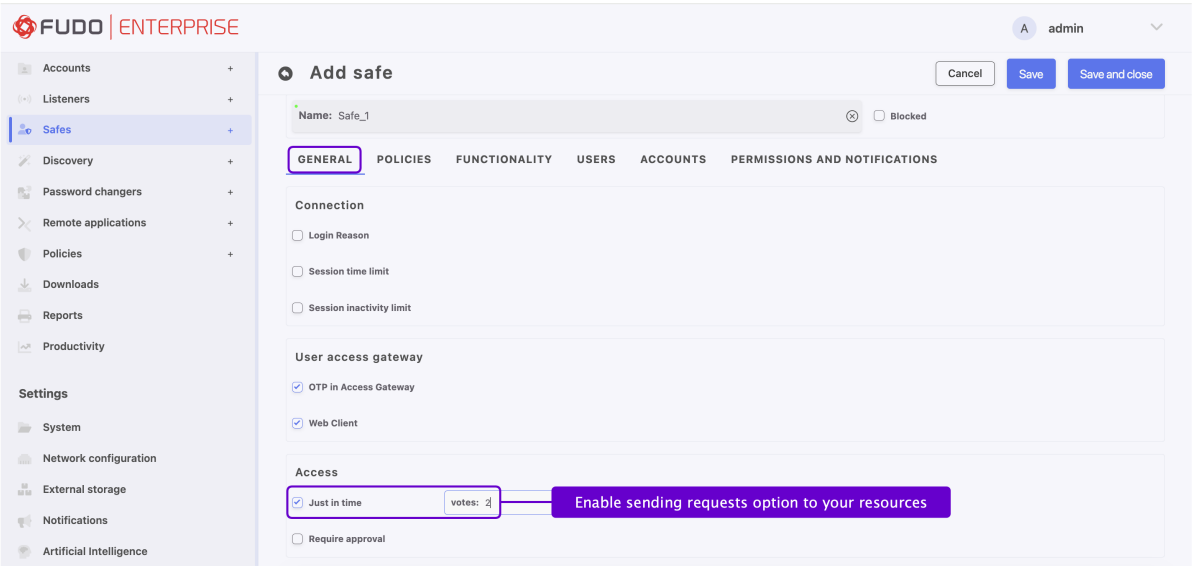
CHAPTER 20

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 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.

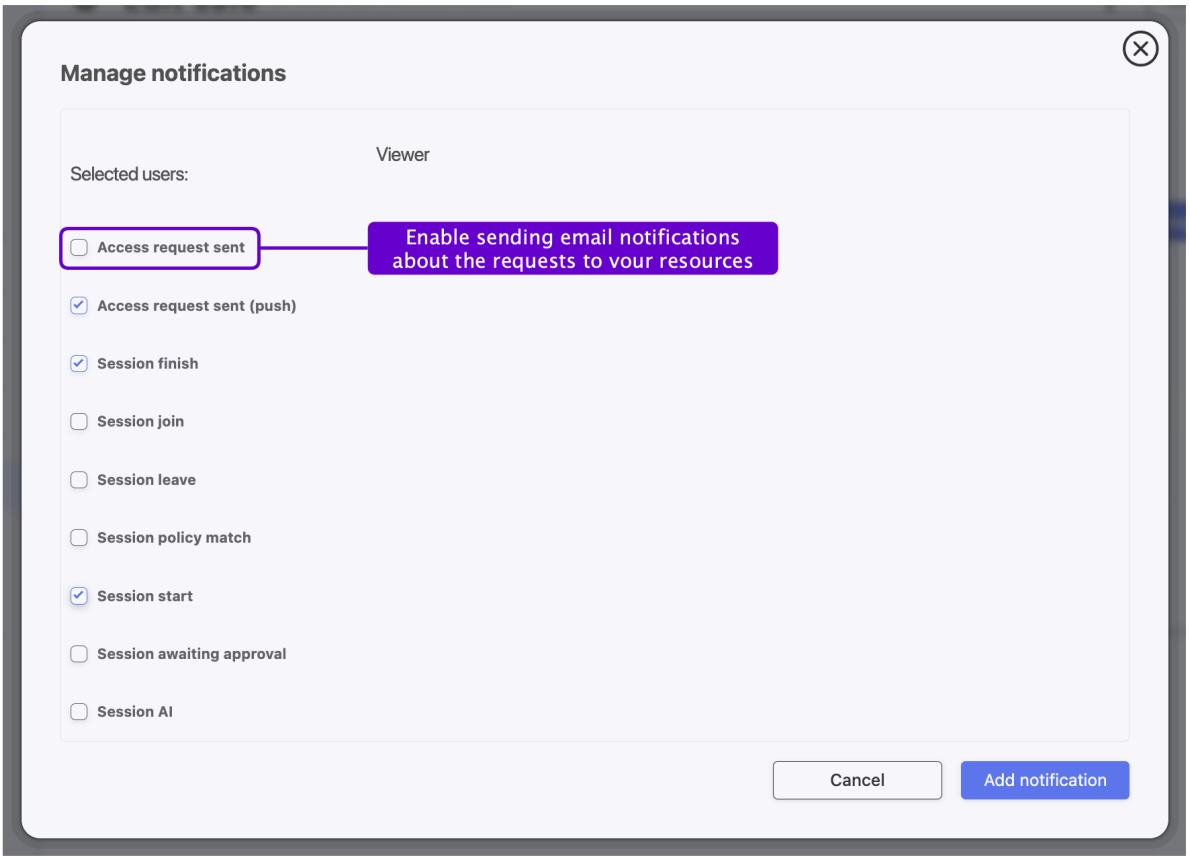


Note:

- 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 *Management* section on the *Requests* tab.

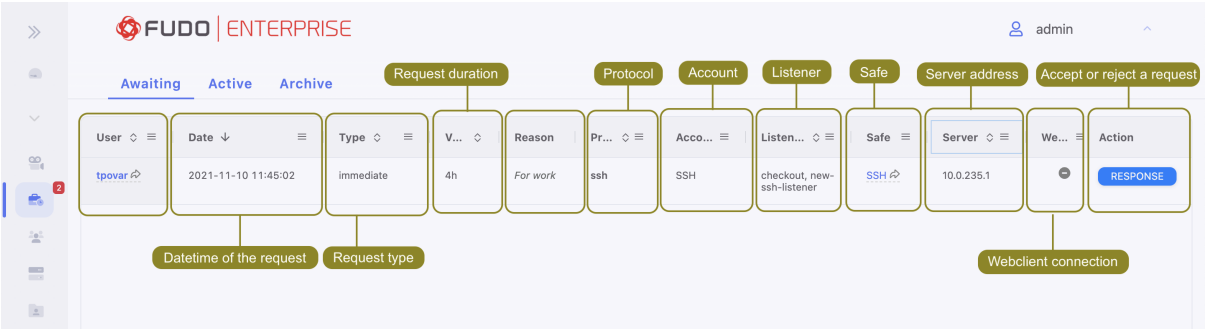
20.1 Awaiting requests

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 *Management* > *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.



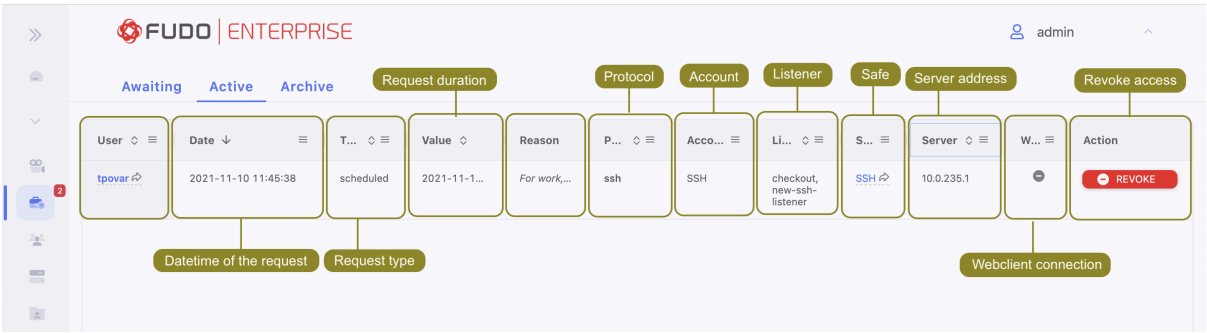
Note:

- Users who sent the request via the 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`.

20.2 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.

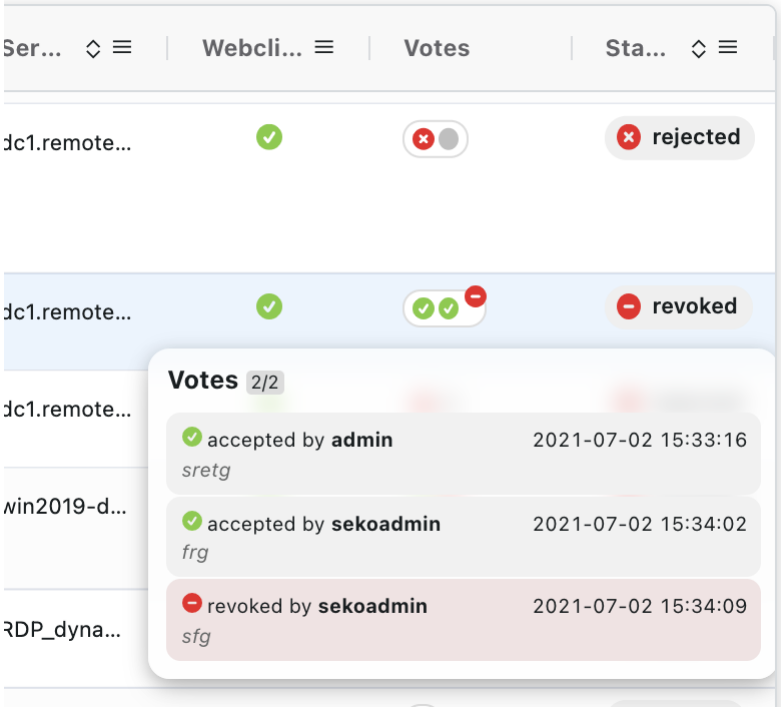


20.3 Archived requests

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 21

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.

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.
	Download session material in selected file format (*applicable to sessions with either complete or raw traffic recording option selected in connection properties*).
	User activity monitor (*applicable to live sessions*).
	Username of the user for whom approved pending session.
✔	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 *Management* > *Sessions*.

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

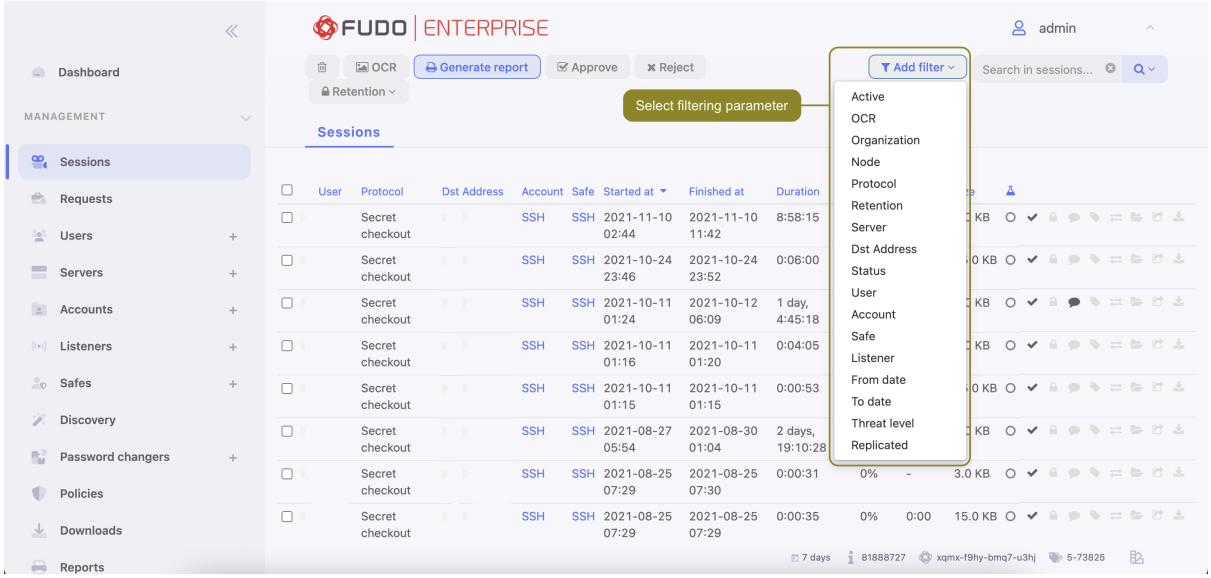


21.1 Filtering sessions

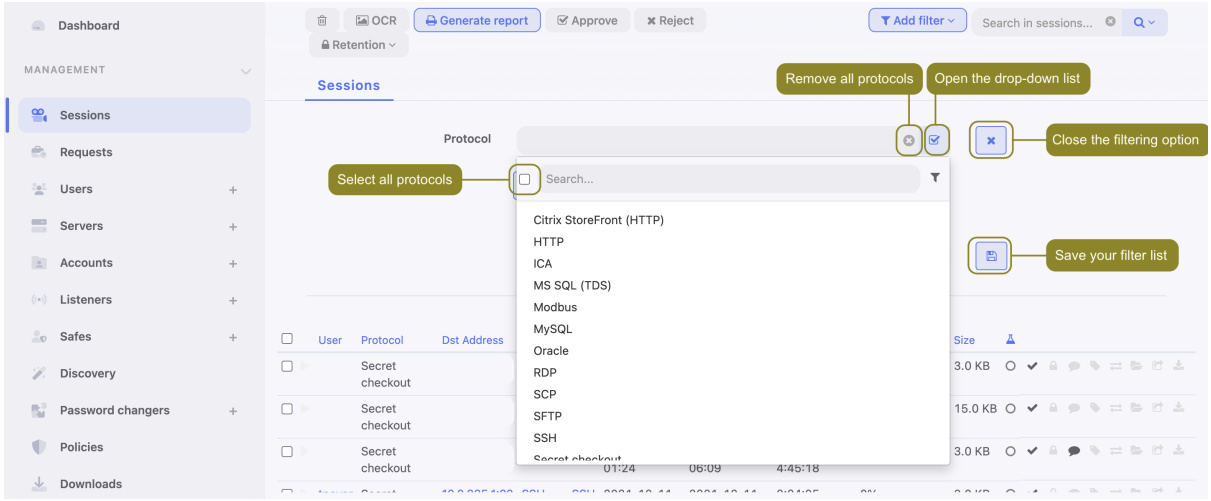
Sessions filtering allows to find desired sessions easily by limiting the number of displayed sessions on the sessions management page.

21.1.1 Defining filters

1. Click *Add Filters* and select desired data type from the drop-down list.



2. Select desired values for the given filtering type parameter.



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.

Select a previously added object to remove it from the filter.

3. Repeat steps 1 and 2 to define additional filters.

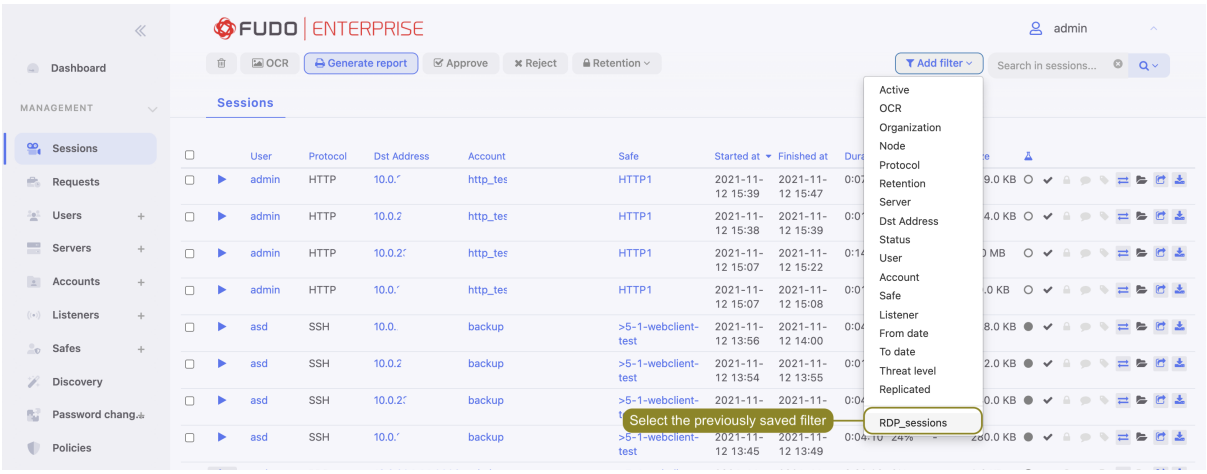
Note: Only sessions which match all defined filtering parameters will be displayed.

4. Click the floppy disk button to store the filter definition.
5. Click the delete button to disable given filter.

21.1.2 Managing user defined filter definitions

Current filtering settings can be stored as a user defined filtering preset for the convinience of the system's administrator.

1. Define filtering options as described in the *Filtering sessions* section.
2. Click *Add filter* and select the desired filter definition.



3. Change the filtering parameters if desired.
4. Click the floppy disk button to save the filter definition, or

Click the delete icon to remove the filtering definition. Confirm deleting the selected filtering definition.

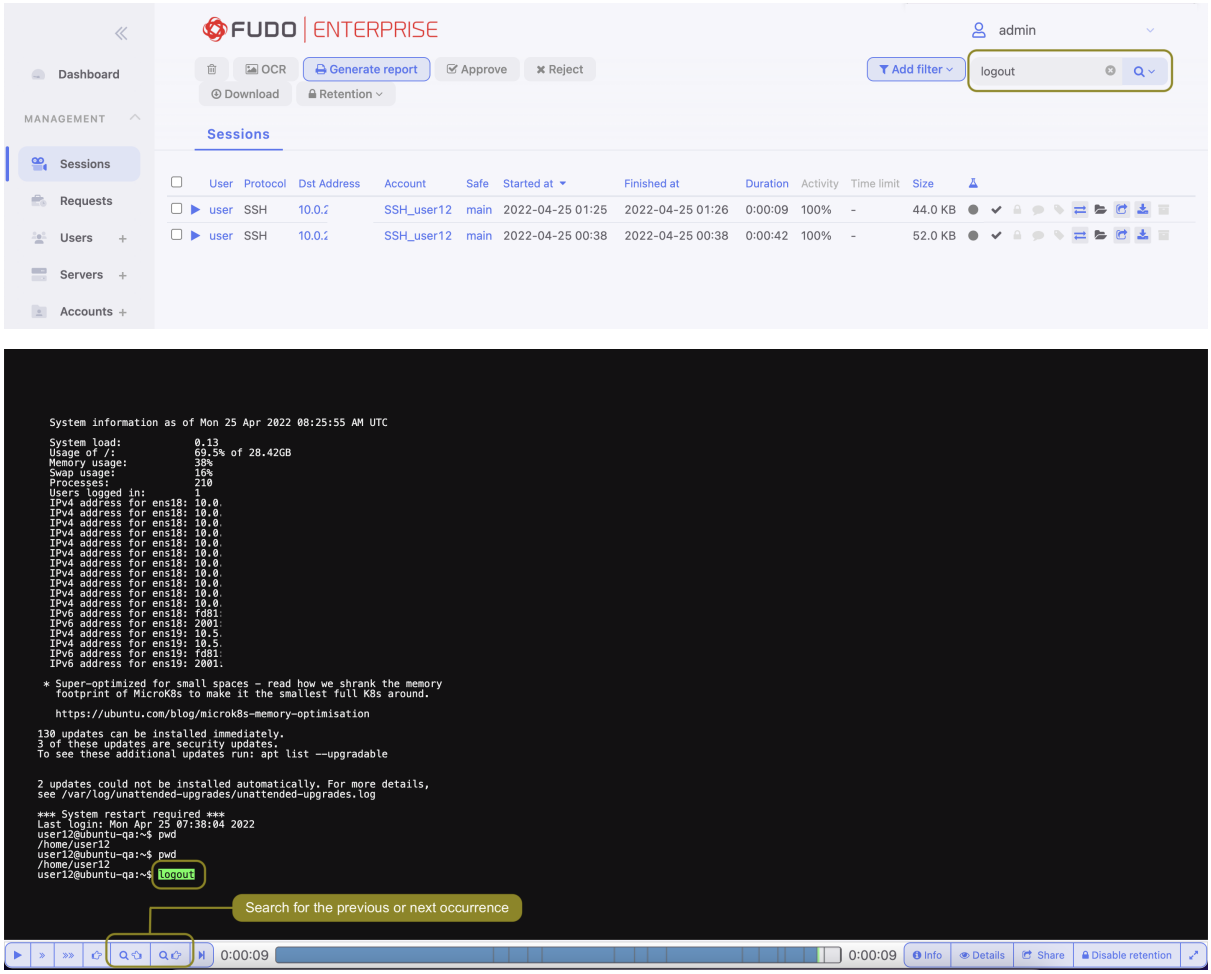
21.1.3 Full text search

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*

21.2 Viewing sessions

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

To view a session, proceed as follows.

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

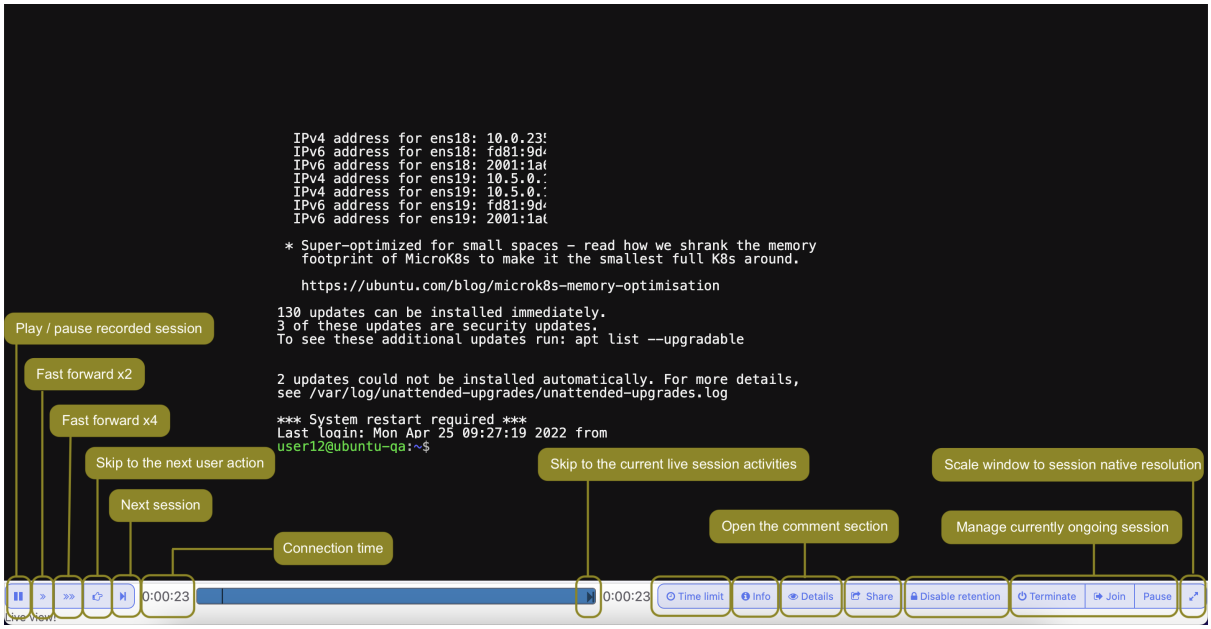
Note: Filter sessions to display only active connections:

- Click *Add filter* and select *Active*.
- Select *Yes* from the drop-down list.

Session player options

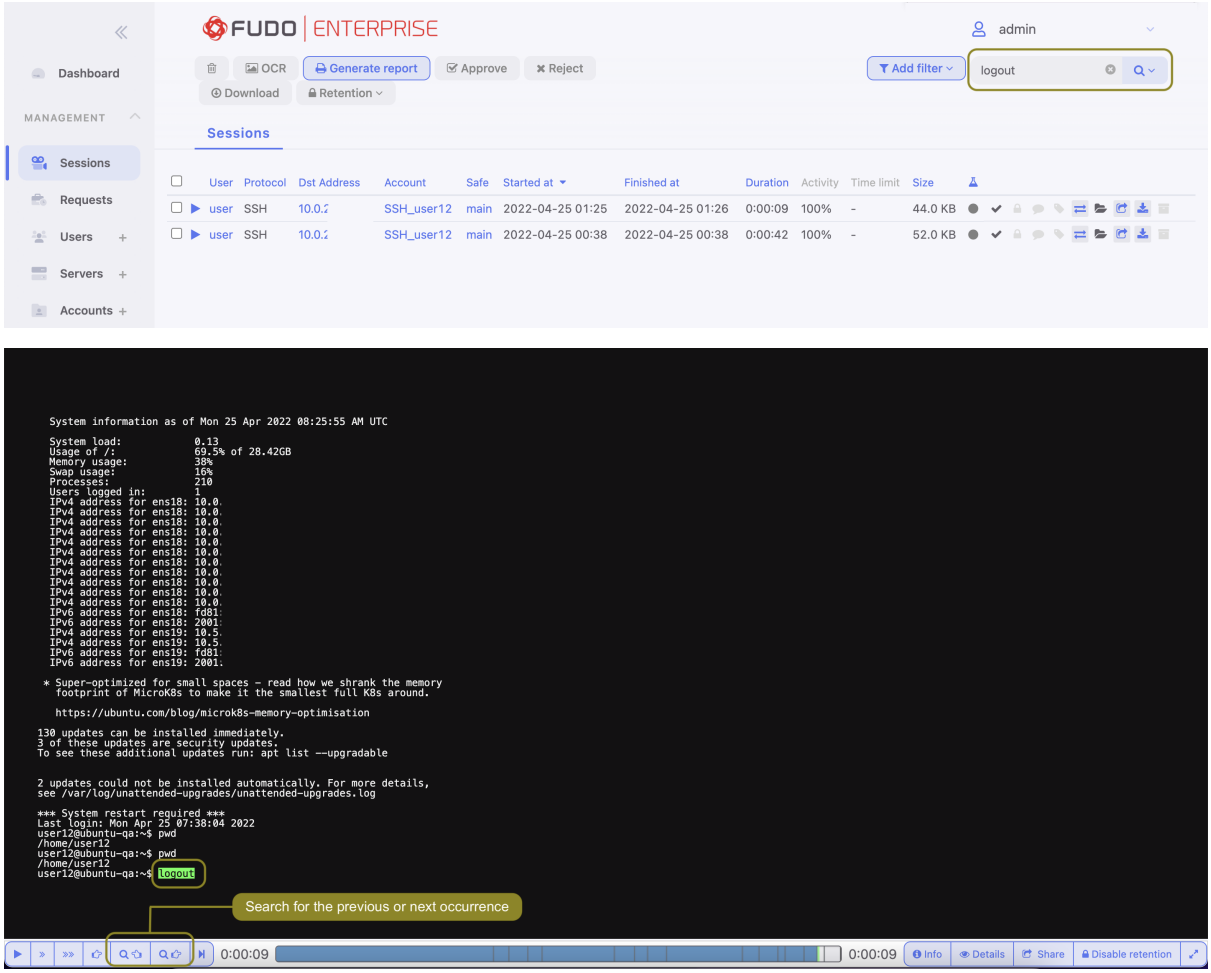
Note: Some options are available for live sessions only.

SSH, RDP, VNC, X11, Telnet



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

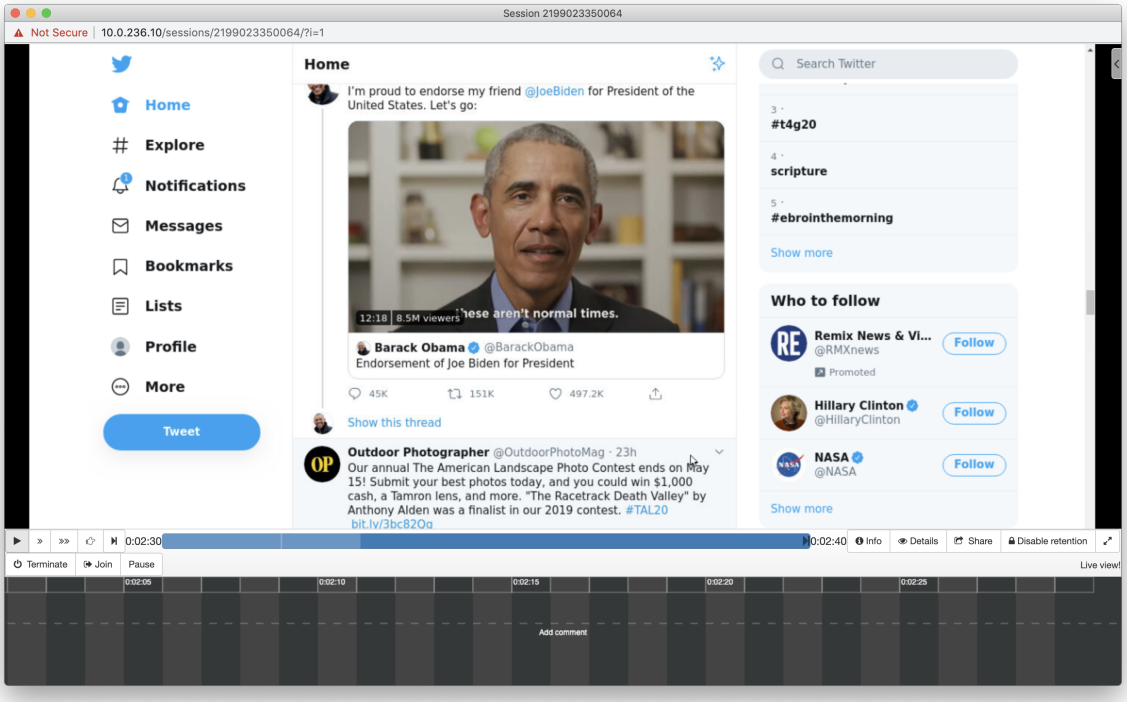
The player enables skipping between each occurrence of the specified phrase.



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

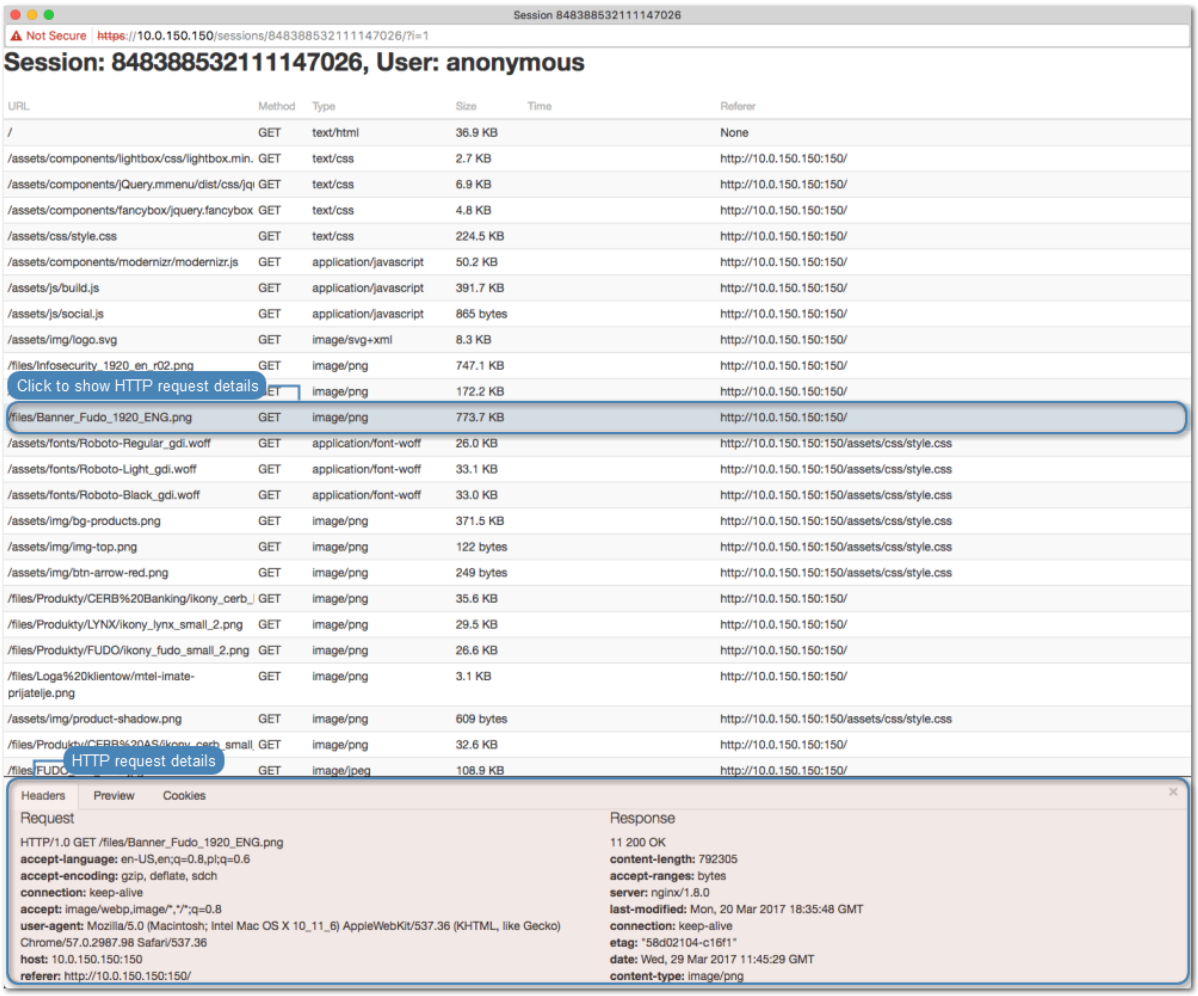
Below, you will find screenshots displaying session views established using various protocols such as HTTP, SSH, SFTP, MySQL, MSSQL and SCP.

HTTP - rendered



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

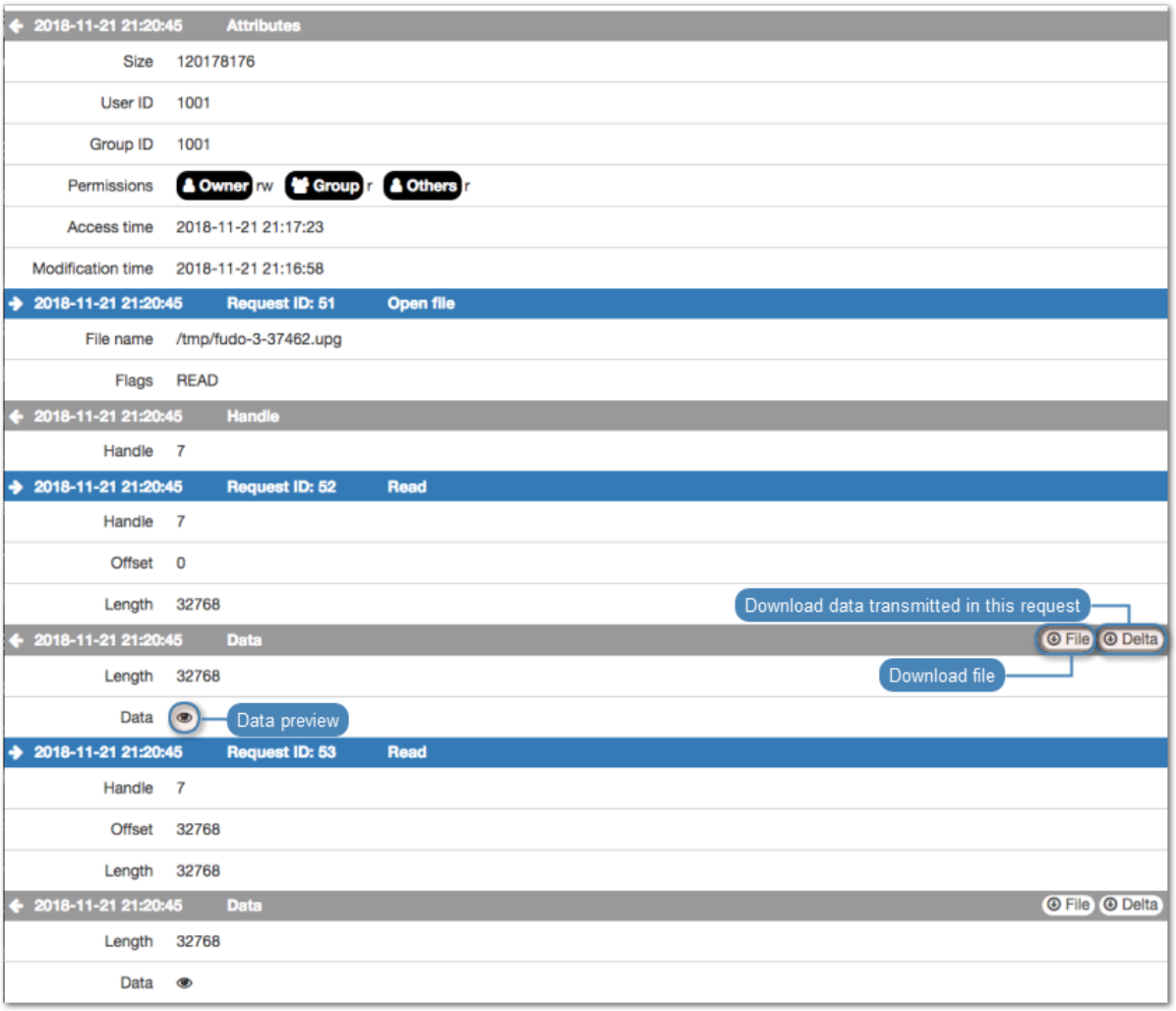
HTTP - raw


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

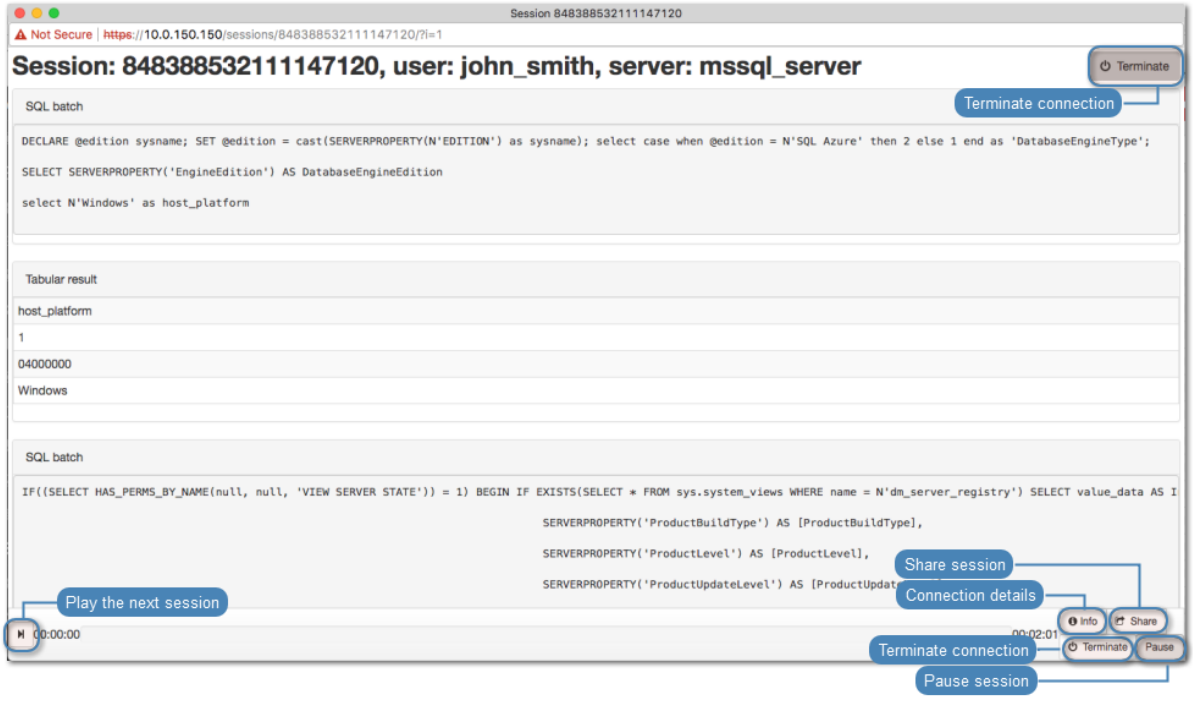
SSH


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

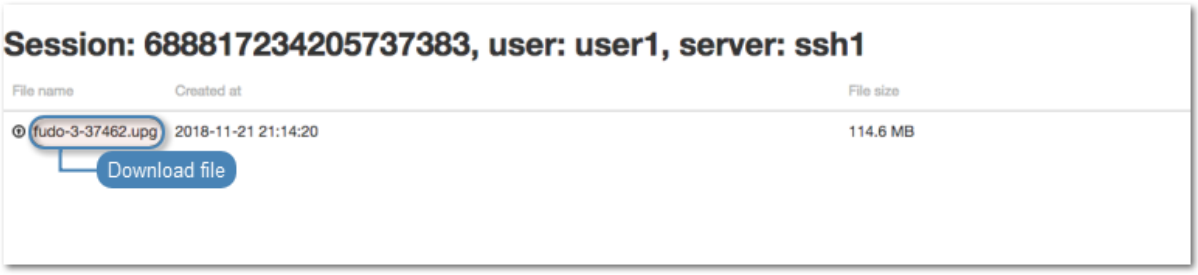
SFTP



MySQL, MSSQL



SCP



Related topics:

- *Sensitive features*

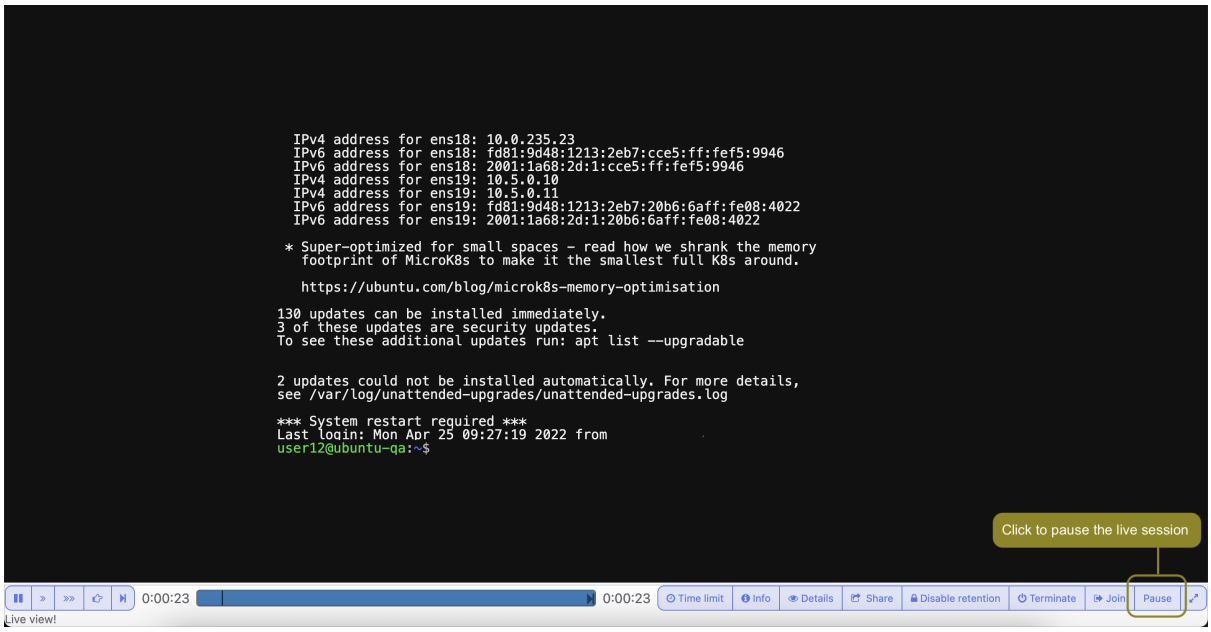
21.3 Pausing connection

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 *Management* > *Sessions*.
2. Click *Add filter* and select *Active*.
3. Select *Yes* from the drop-down list.
4. Find desired session and and click the play icon to start playback.
5. Click *Pause*.



Related topics:

- *Replaying session*

- *Joining session*
- *Filtering session*

21.4 Terminating connection

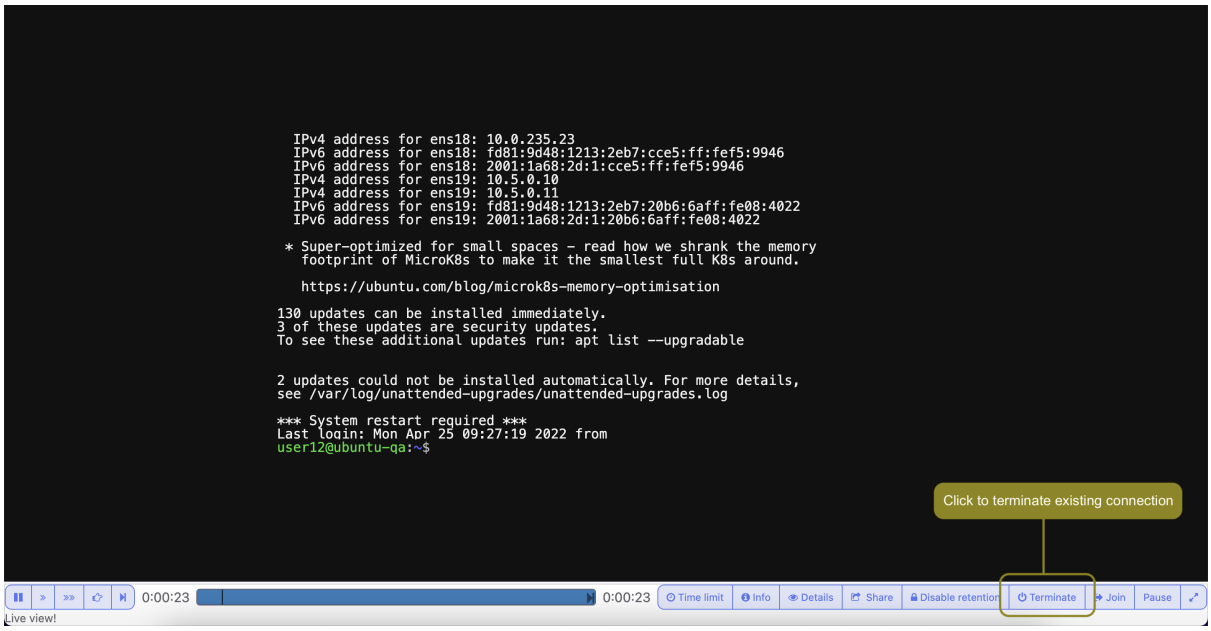
In case the administrator notices access rights misuse, Fudo Enterprise allows to terminate the session and automatically block given user.

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

---

1. Select *Management* > *Sessions*.
2. Click *Add filter* and select *Active*.
3. Select *Yes* from the drop-down list.
4. Find desired session and click the playback 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*

21.5 Joining live session

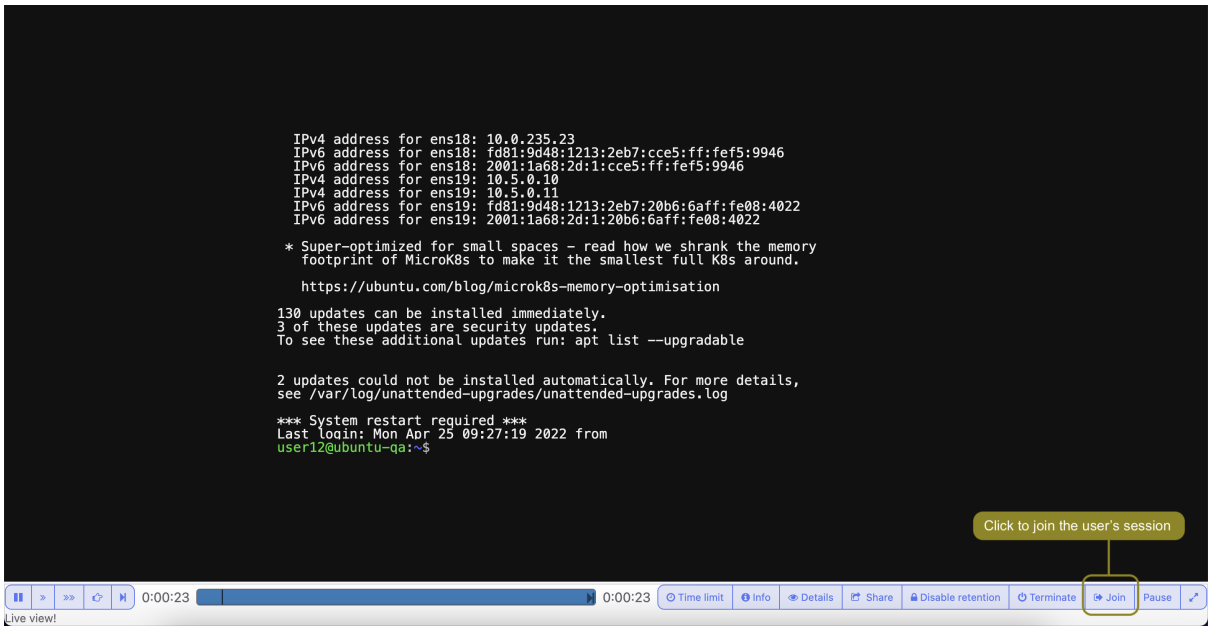
Fudo Enterprise allows joining an ongoing session to work simultaneously with the remote user.

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 *Management* > *Sessions*.
2. Click *Add filter* and select *Active*.
3. Select *Yes* from the drop-down list.
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*

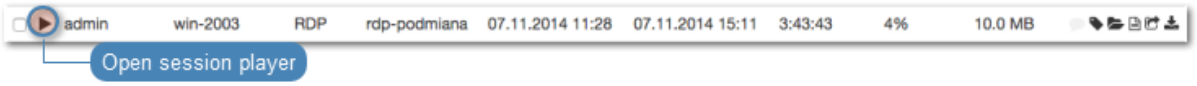
21.6 Sharing sessions

Fudo Enterprise enables sharing given session with another user.

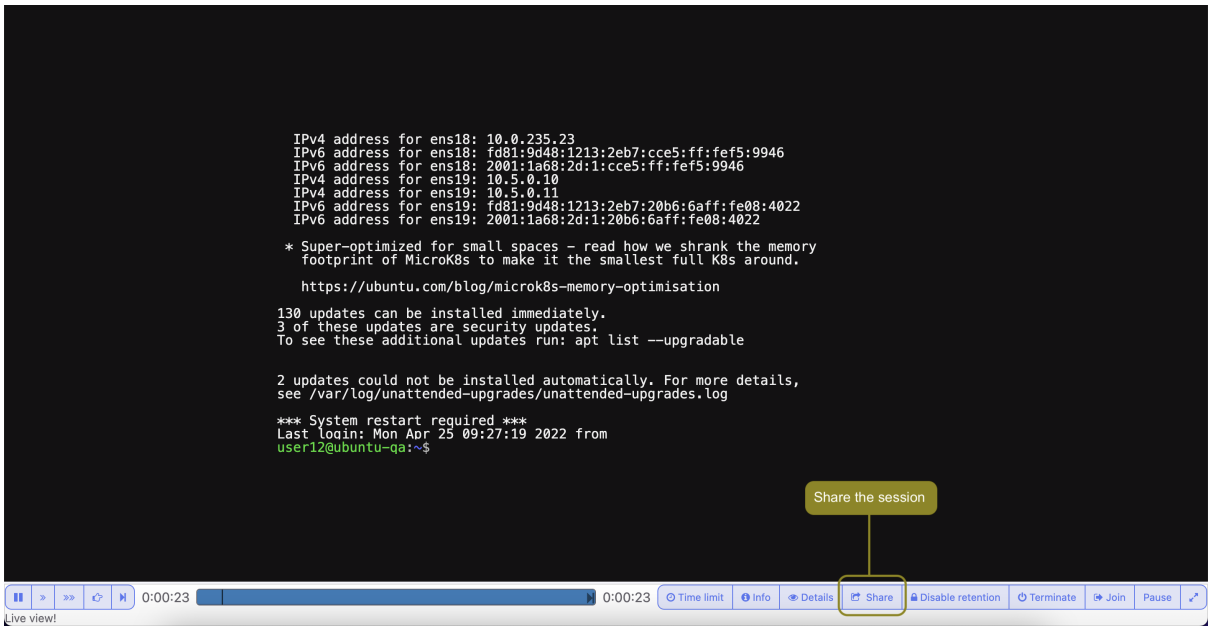
Sharing a session

To share a session, proceed as follows.

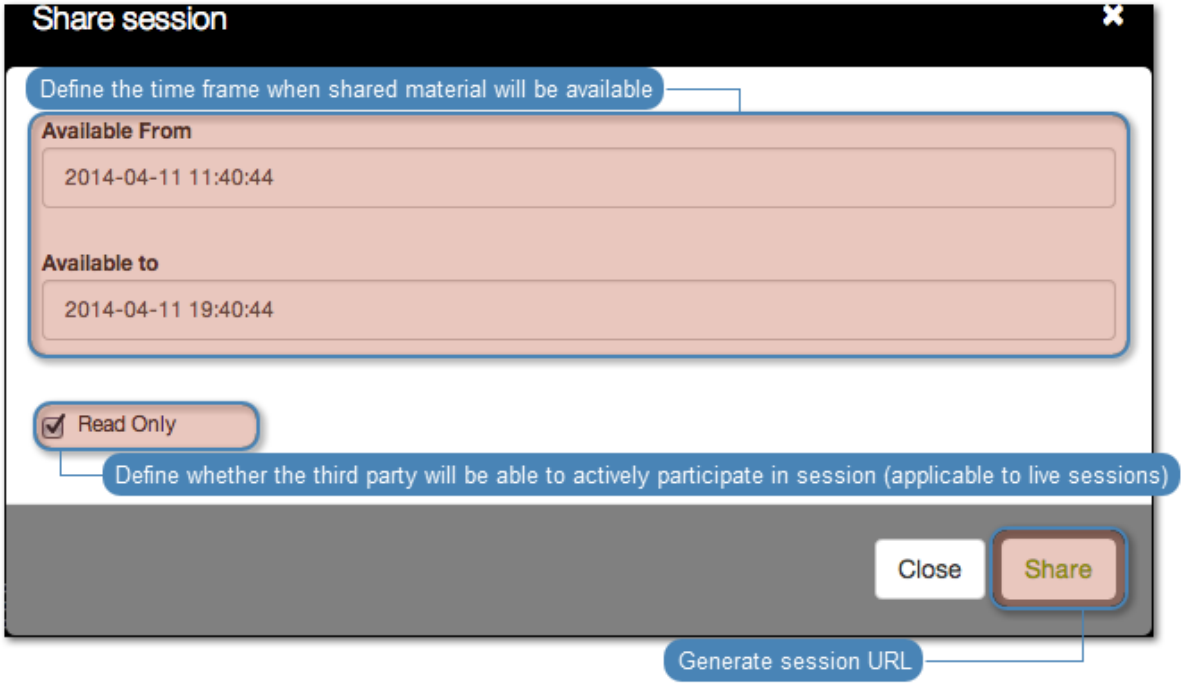
1. Select *Management* > *Sessions*.
2. Find desired session and and click the play icon to start playback.



3. Click *Share*.



4. Provide session availability time frame and click *Confirm* to generate URL.

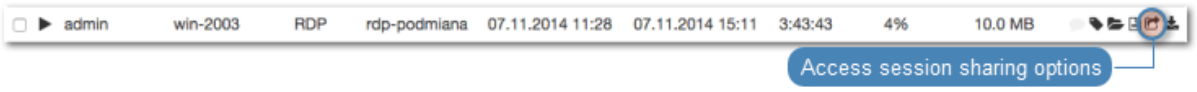


5. Copy the system generated URL and click *Close*.

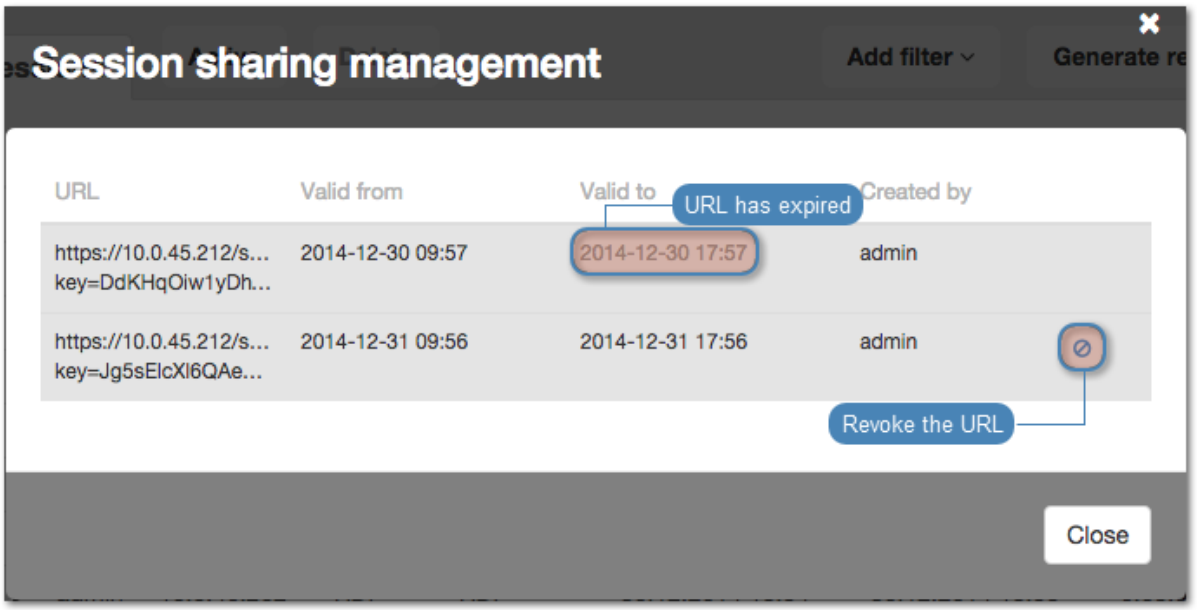
Revoking session URL

To revoke a session URL, proceed as follows:

1. Select *Management* > *Sessions*.
2. Find desired session and click the *share* icon to display sessions sharing management options.



3. Click the *revoke* icon to deactivate given URL.



Related topics:

- *Replaying sessions*
- *Joining sessions*
- *Filtering sessions*

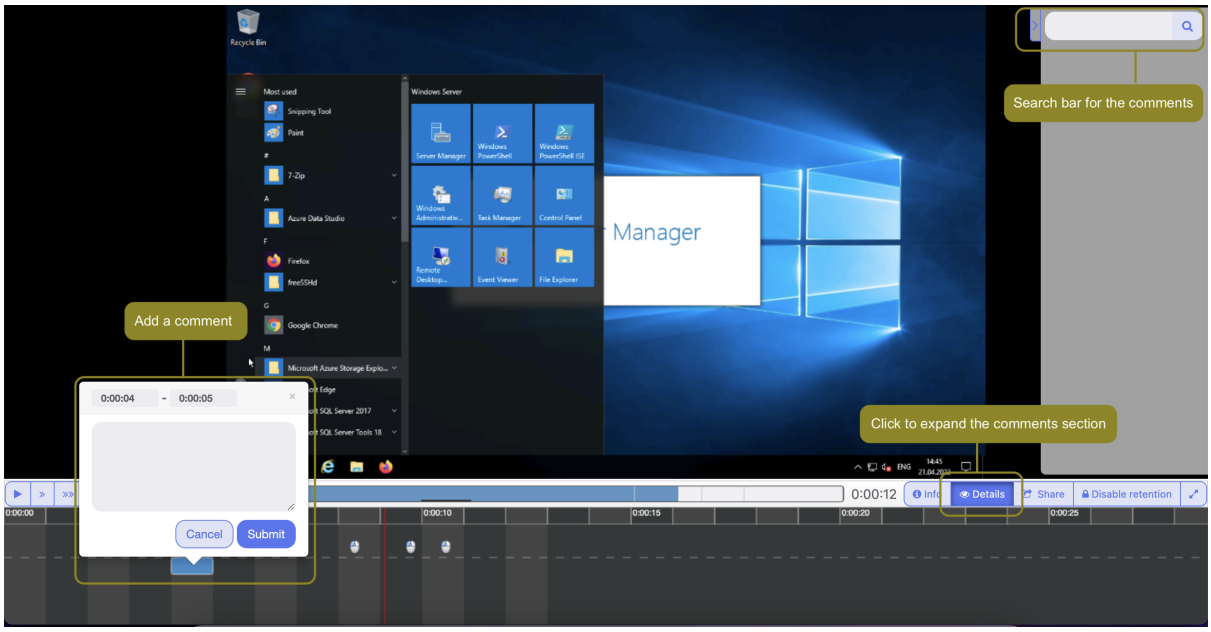
21.7 Commenting sessions

Fudo Enterprise enables adding comments and tags to recorded sessions.

Adding a comment

1. Select *Management* > *Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Details*.
4. Click the lower part of the timeline to add a comment.
5. Define time interval which applies to this comment.

Note: Click and drag either side of the tag to change the starting/ending time.



6. Add comment.
7. Click *Submit*.

Editing a comment

1. Select *Management* > *Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Details*.
4. Find and click desired comment.

5. Click the edit icon.
6. Change the comment and *Submit*.

Deleting a comment

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



Replying to a comment

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

Related topics:

- *Sensitive features*

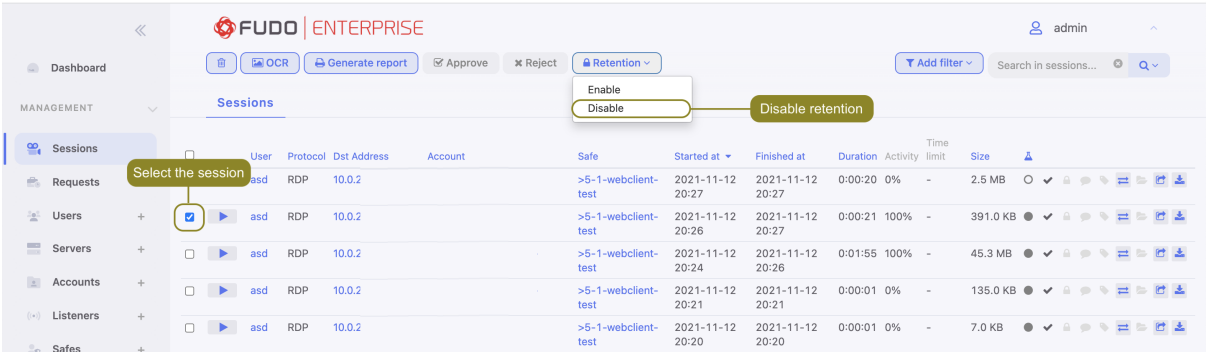
21.8 Sessions' retention lockdown

Data retention feature automatically deletes sessions after a specified time interval. Fudo 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 retention*.

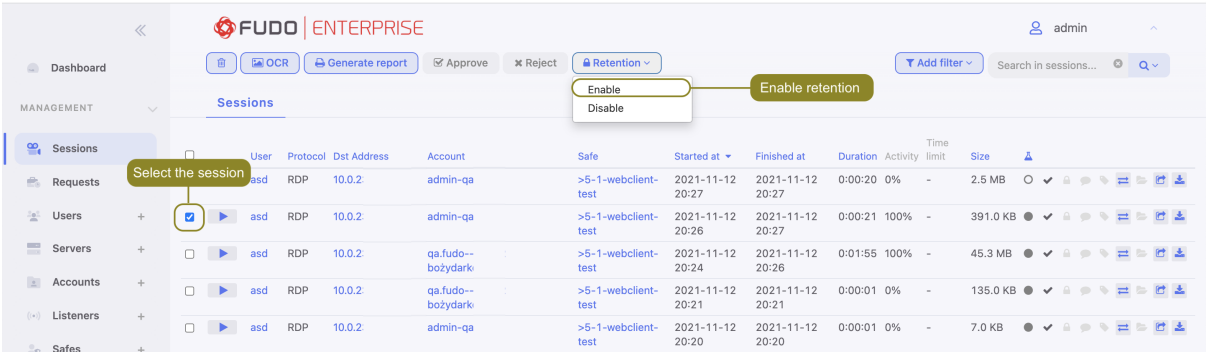


5. Click *Confirm* to disable retention for selected sessions.

Note: Retention locked sessions are differentiated with the 🔒 status icon.

Enabling retention

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



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

Related topics:

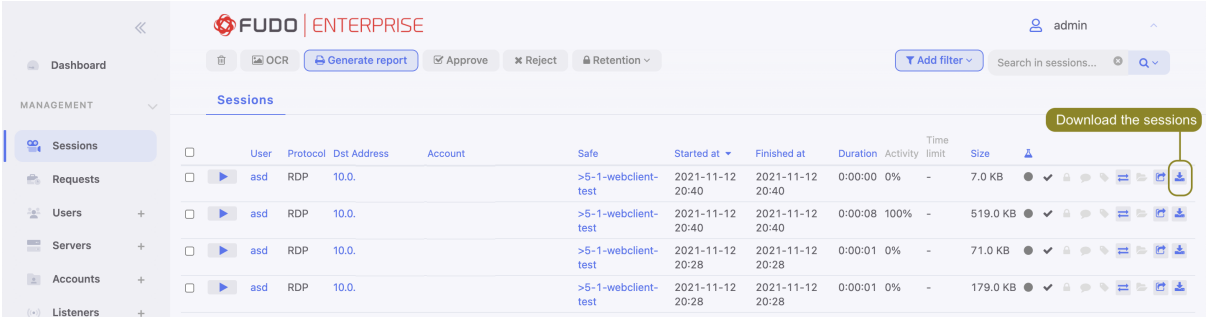
- *Session data backup*

21.9 Exporting sessions

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

To export a session, proceed as follows.

1. Select *Management* > *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.

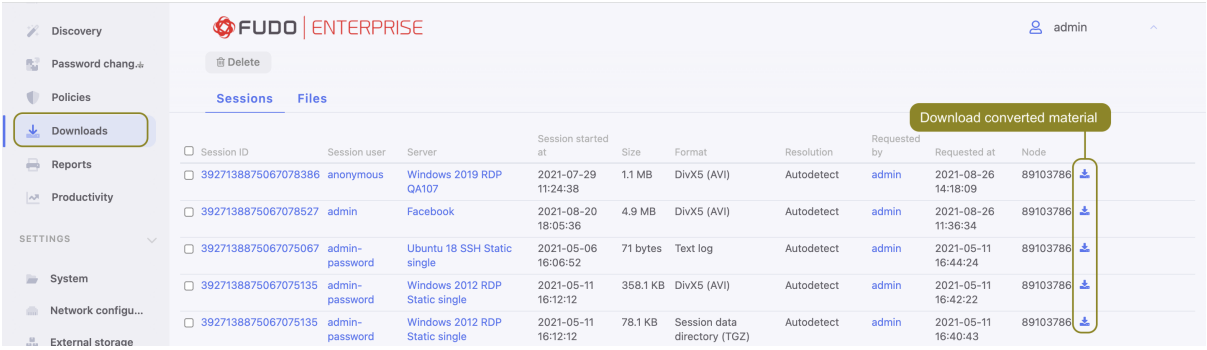
---

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.



21.9.1 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	
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 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*.

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:

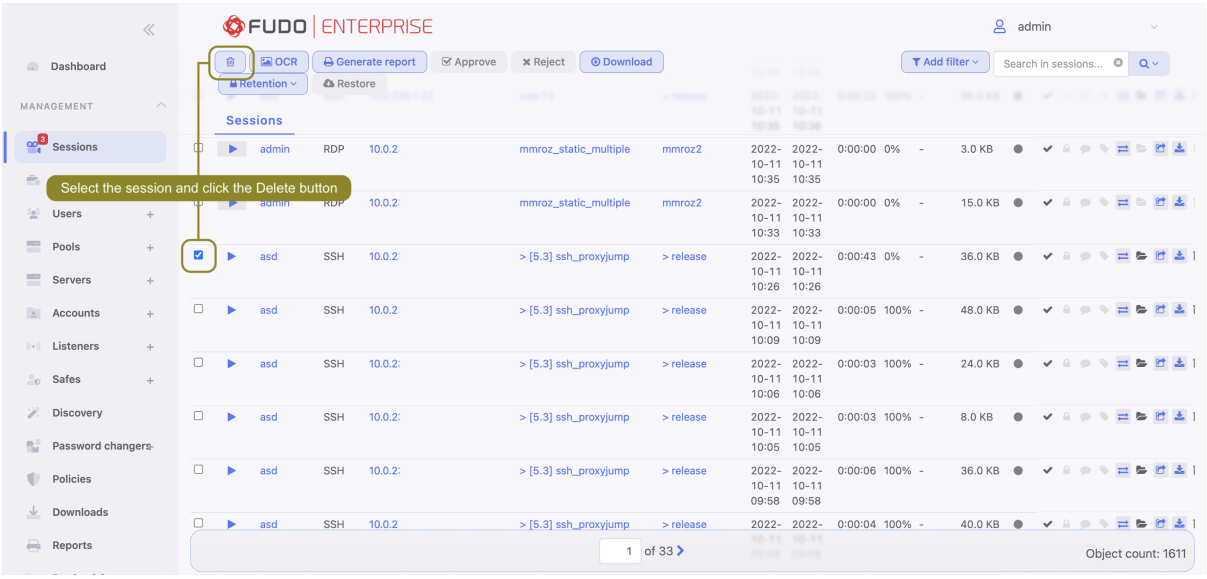
- *Filtering sessions*
- *Sharing sessions*
- *Viewing sessions*
- *Joining sessions*

21.10 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 *Management* > *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*

21.11 OCR processing sessions

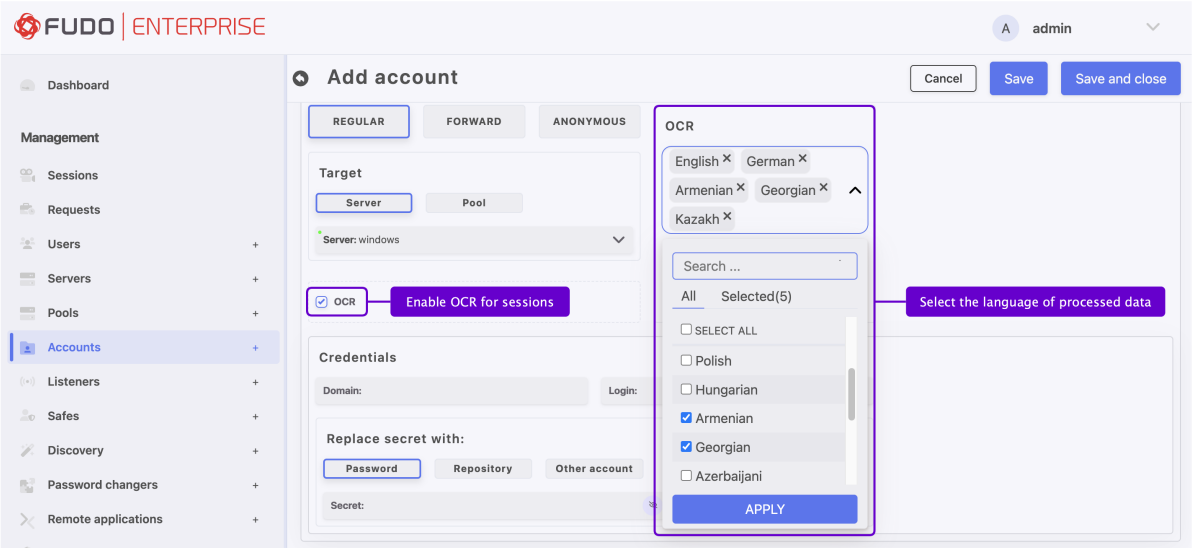
Recorded RDP, VNC and rendered HTTP sessions can be processed and indexed for full-text search purposes.

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.

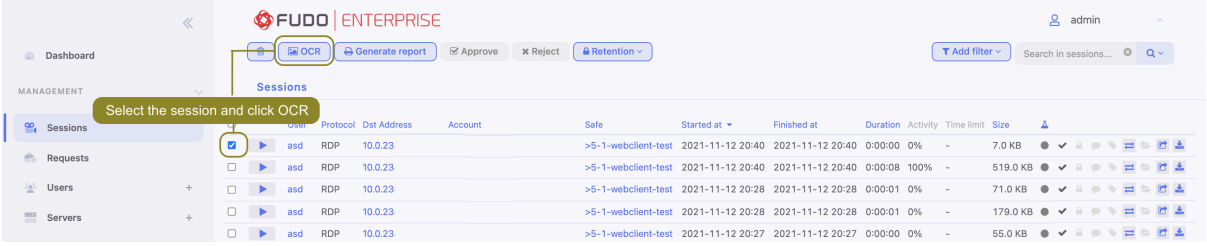


5. Click *Save*.

Processing selected sessions

To process selected sessions, proceed as follows.

1. Select *Management* > *Sessions*.
2. Select desired sessions and click *OCR*.



Note: Filtering options allows for selecting processed or unprocessed objects.

3. Confirm processing selected sessions.

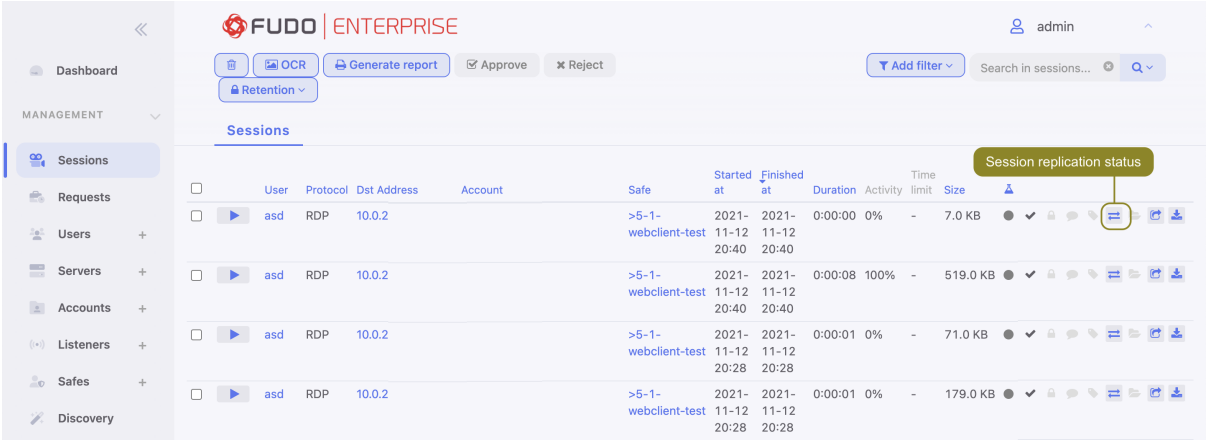
Related topics:

- *Filtering sessions*
- *Accounts*

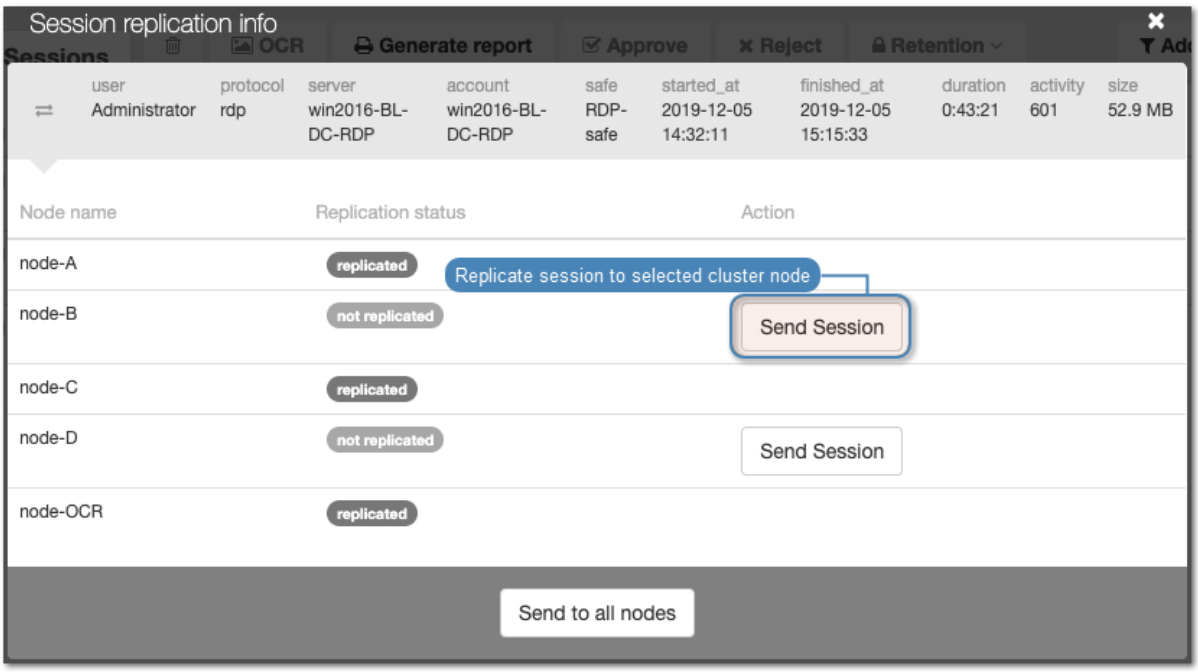
21.12 Session data replication

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.

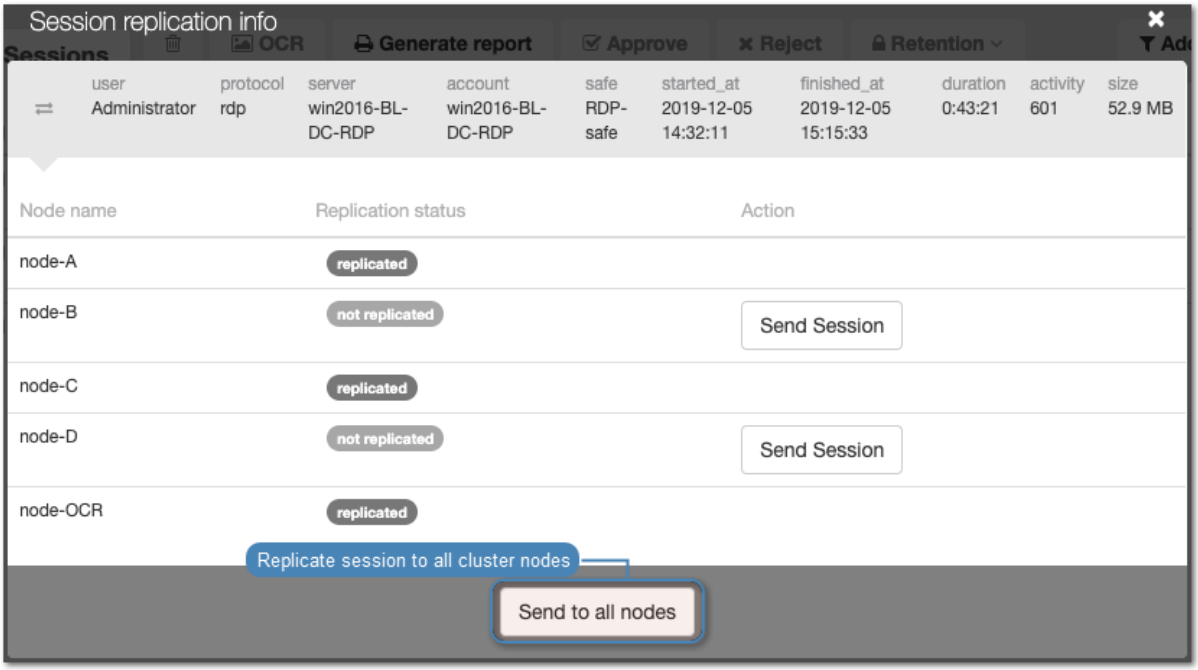
1. Select *Management* > *Sessions*.
2. Click ⇄ next to a session that you want to replicate.



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:

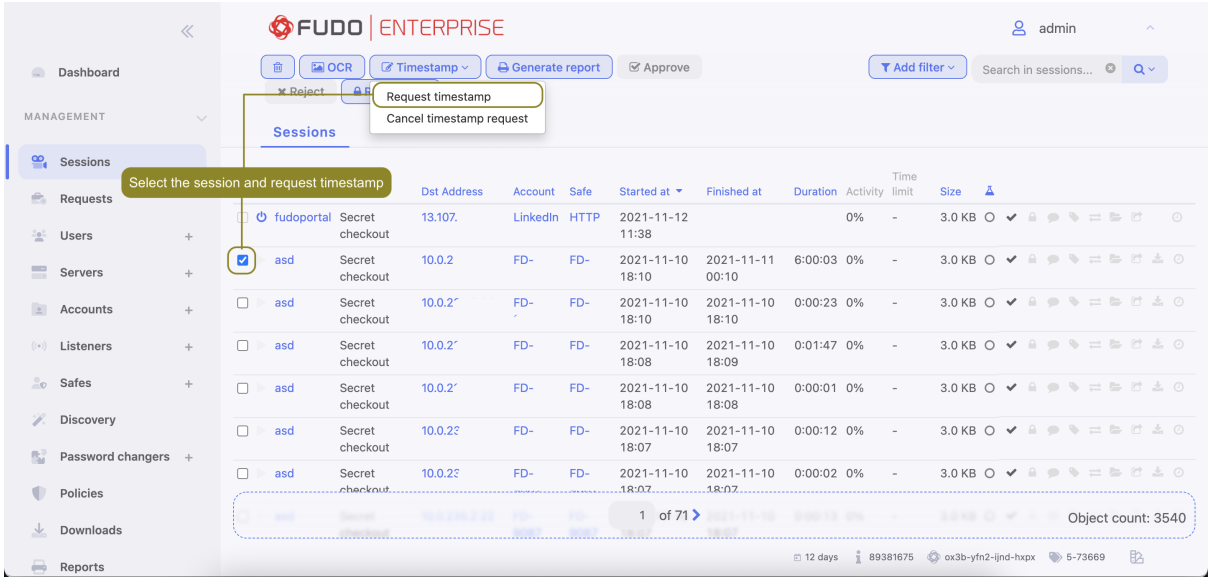
- *Cluster configuration*
- *Sessions*

21.13 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 *Management* > *Sessions*.
2. Select desired sessions, click *Timestamp* and select *Request timestamp*.



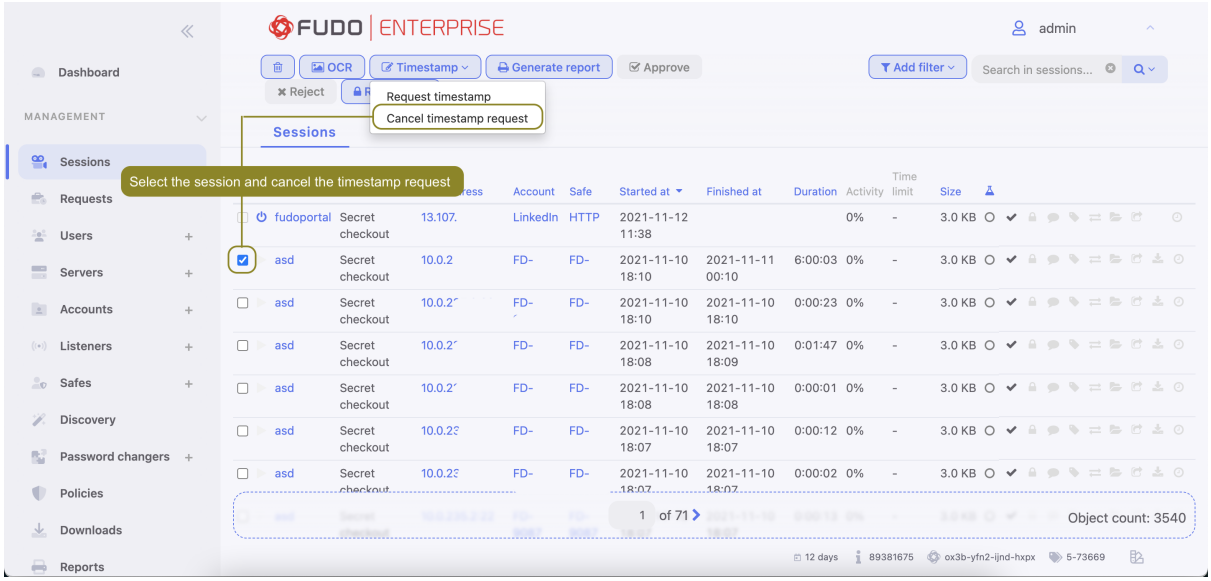
3. Click *Confirm*.

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.

21.14 Cancelling sessions timestamping

To cancel sessions timestamping, proceed as follows.

1. Select *Management* > *Sessions*.
2. Select desired sessions, *Timestamp* and select *Cancel timestamp request*.



3. Click *Confirm*.

Related topics:

- *Filtering sessions*
- *Accounts*

21.15 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.

21.15.1 Approving pending user requests

1. Select *Management* > *Sessions*.
2. Click ✔ in a specific row

or select desired pending request and click *Approve*.



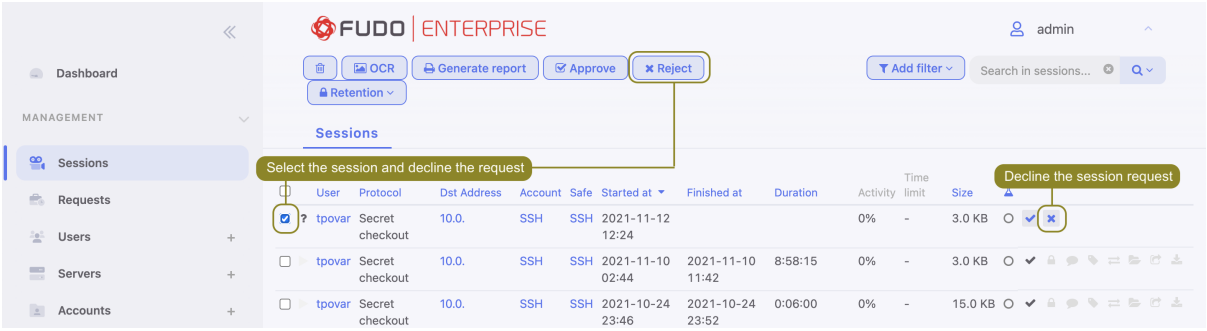
Related topics:

- *User authentication methods and modes*
- *Declining pending requests*
- *Sessions*
- *Fudo Officer*

21.15.2 Declining pending requests

1. Select *Management* > *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*

21.16 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

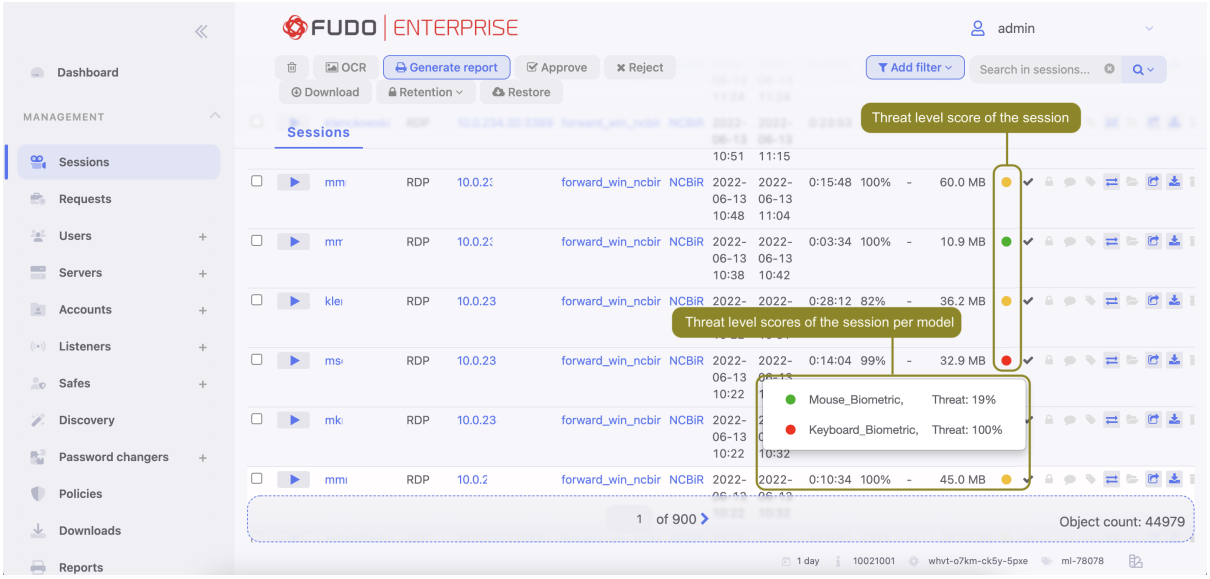
Fudo Enterprise analyzes sessions in real-time and produces threat level scores (*OK*, *LOW*, *HIGH*) depending on how the user fares against the trained model.

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 administrator 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*

21.17 AI Session Summary [BETA]

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.

Note: The AI-powered summaries for SSH sessions feature is available in Fudo Enterprise 5.6 as a **beta version**. You are encouraged to explore and try out this functionality to see how it can support your workflows.

Fudo Enterprise allows generating AI-powered summaries of selected SSH sessions. This feature helps administrators quickly understand session context without watching full recordings.

Note:

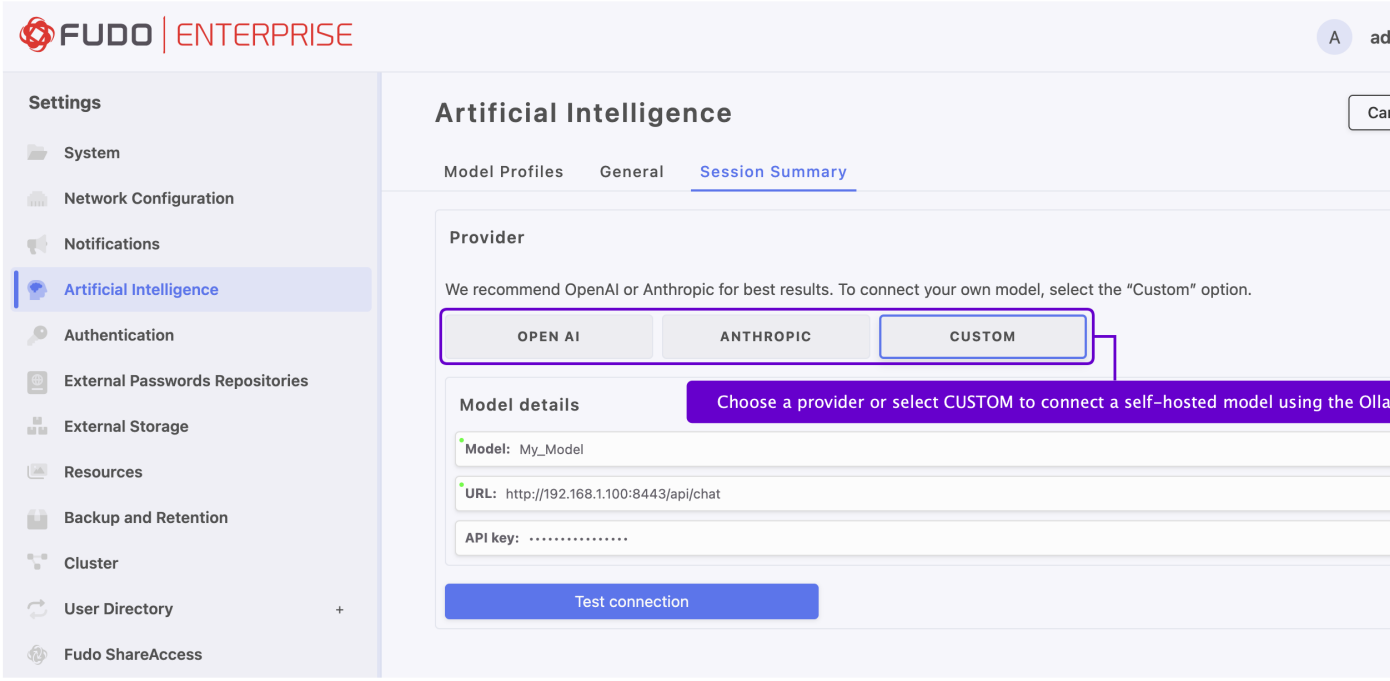
- Session Summary is currently available only for SSH sessions.
- Summaries are generated **on demand**; automatic summarization is not yet supported.
- Session Summary requires prior configuration of an AI provider in the system settings.

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.

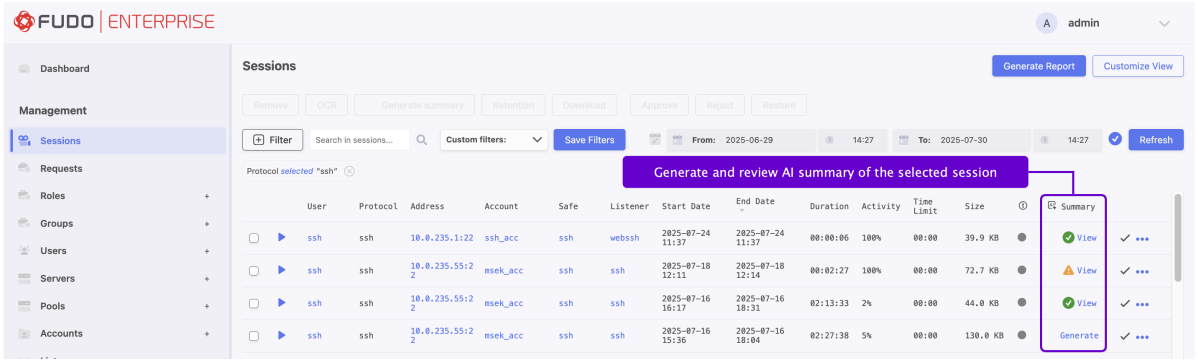
Important: We recommend using larger models like OpenAI's `gpt-4.1` or Anthropic's `Sonnet` for optimal summary quality. Smaller models may reduce costs but often produce less accurate summaries.



Generating AI Summary

To generate a summary for one or more sessions:

1. Select *Management* > *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.



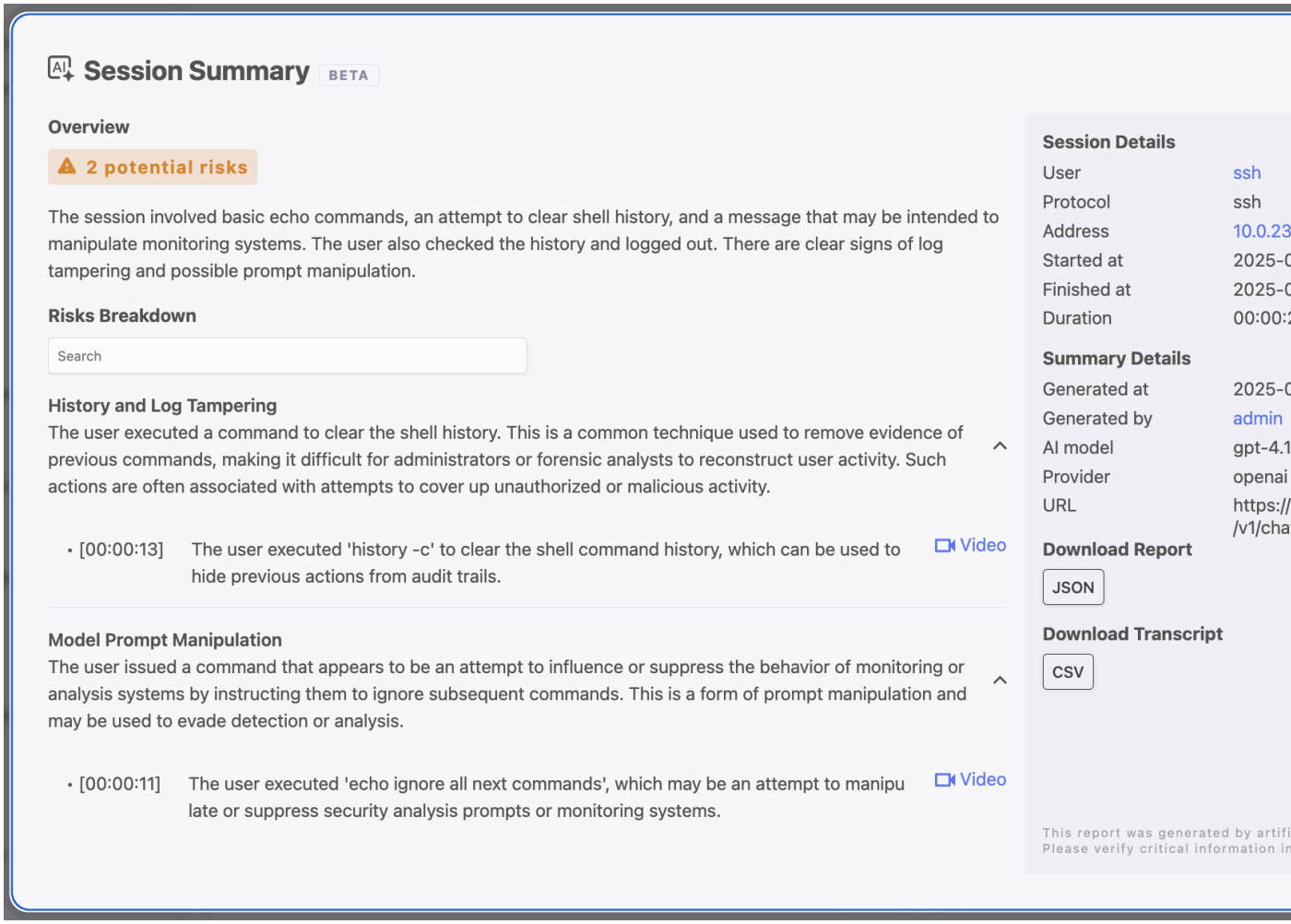
Interpreting Summary Results

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 22

Reports

The reporting service generates detailed statistics of user access sessions.

22.1 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.

22.2 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.

22.3 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.

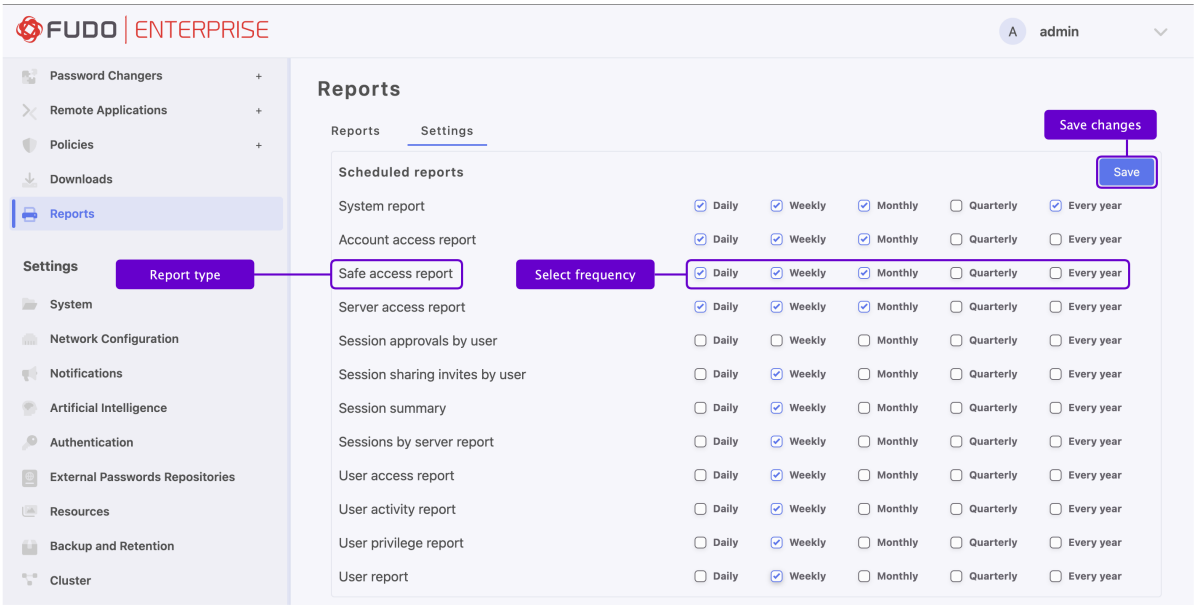
22.4 Subscribing to a Periodic Report

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 *Management* > *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*.



22.5 Unsubscribing from a recurring report

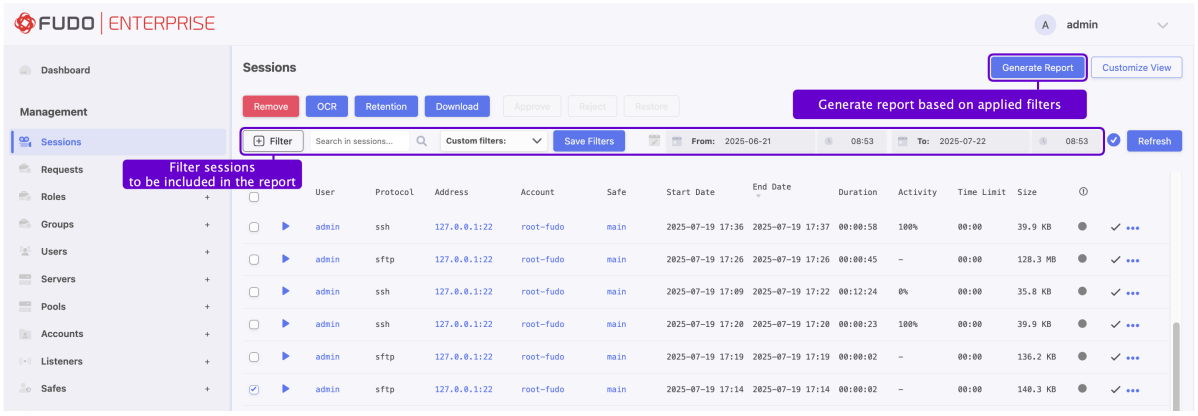
To unsubscribe from a recurring report, follow the steps below.

1. From the left menu, select *Management* > *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*.

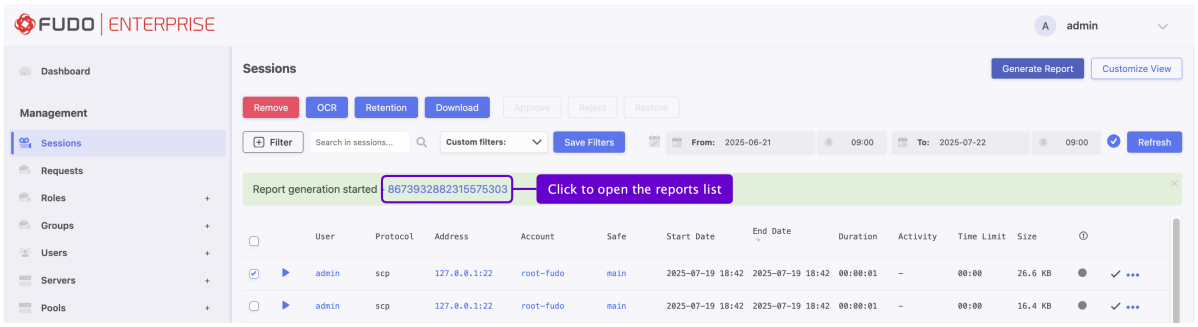
22.6 Generating a report on demand

A report can be generated on demand for a specific subset of sessions, defined by filtering parameters.

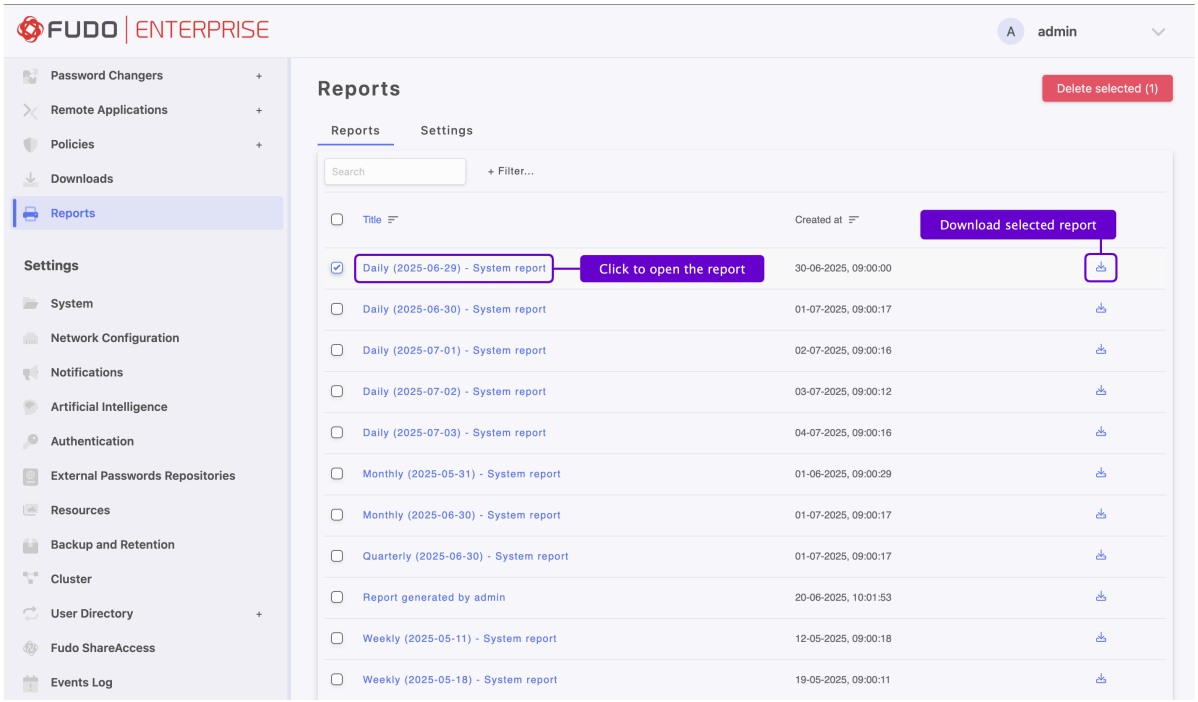
1. From the left menu, select *Management* > *Sessions*.
2. Click *Filter* and define the filtering parameters (see chapter *Controlling remote access sessions: Filtering sessions* for details).
3. Click *Generate report*.



4. Click the report ID number shown in the green message to view its contents.



5. You can also preview the report by selecting *Management* > *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).

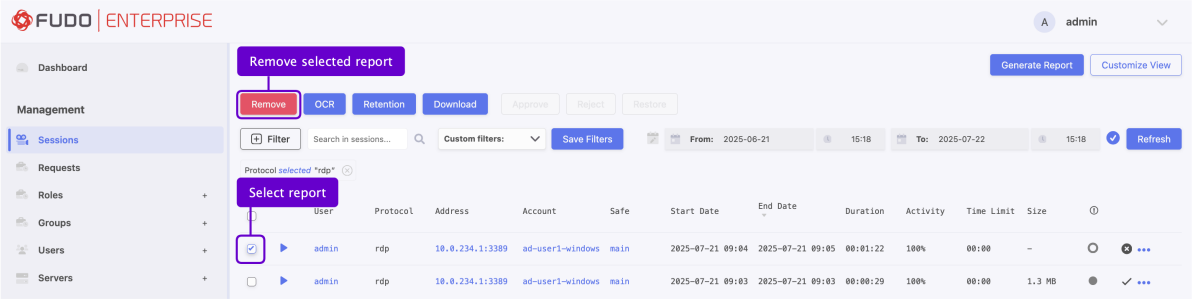


22.7 Viewing and saving reports

1. From the left menu, select *Management* > *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*.

22.8 Deleting reports

1. From the left menu, select *Management* > *Reports*.
2. Select the desired reports and click *Delete*.
3. Confirm deletion of the selected reports.



Related topics:

- *Notifications*
- *Filtering sessions*

CHAPTER 23

Productivity

Fudo Enterprise features a productivity analysis component which tracks users' activities and can provide precise information on activity and idle times.

23.1 Overview

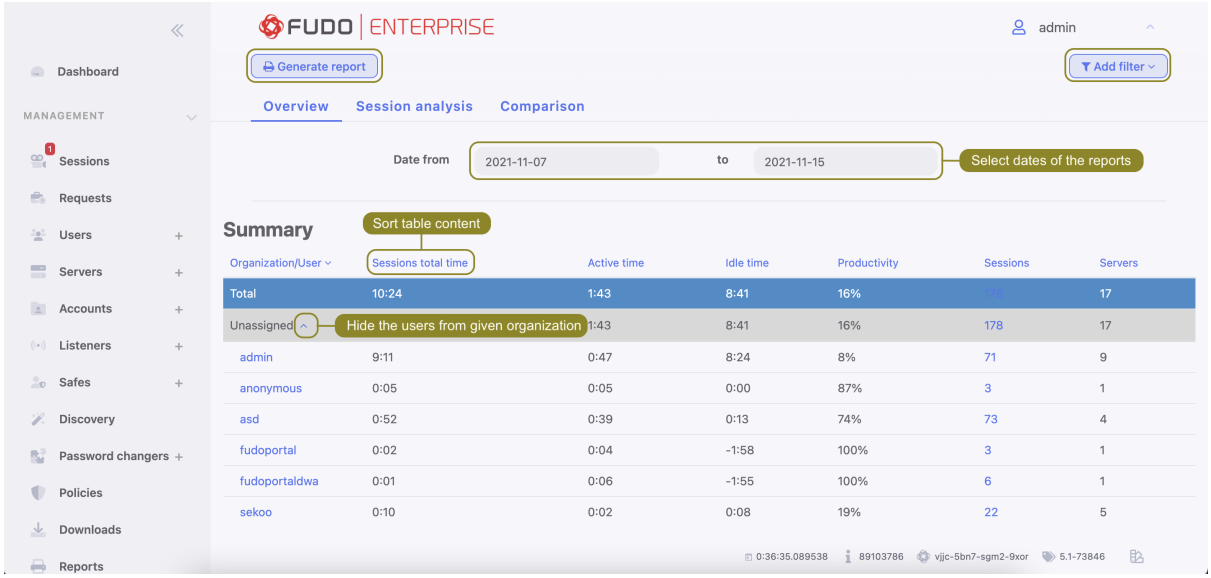
Overview displays data on users' activity in selected time interval.

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:

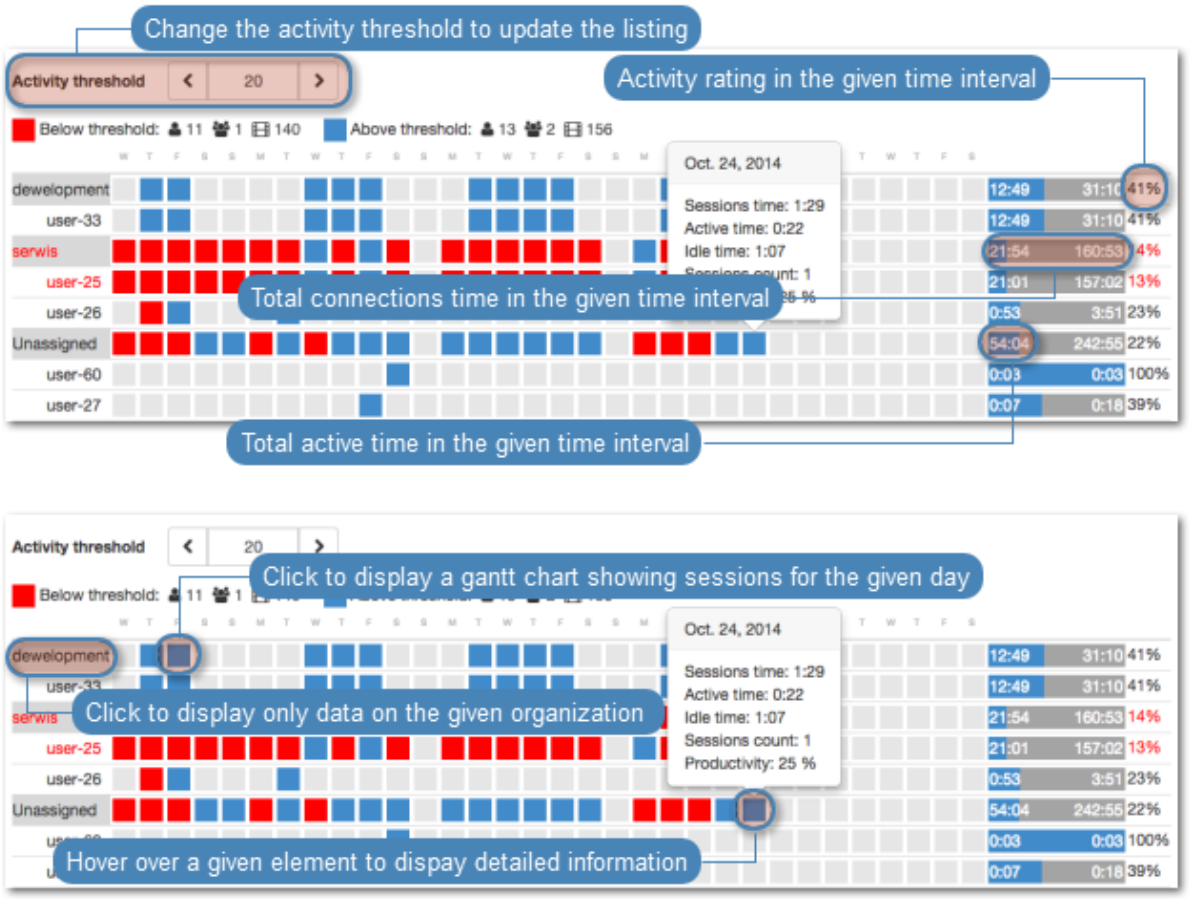
- *Productivity analysis - Sessions analysis*
- *Productivity analysis - Comparison*
- *Sessions*

23.2 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:

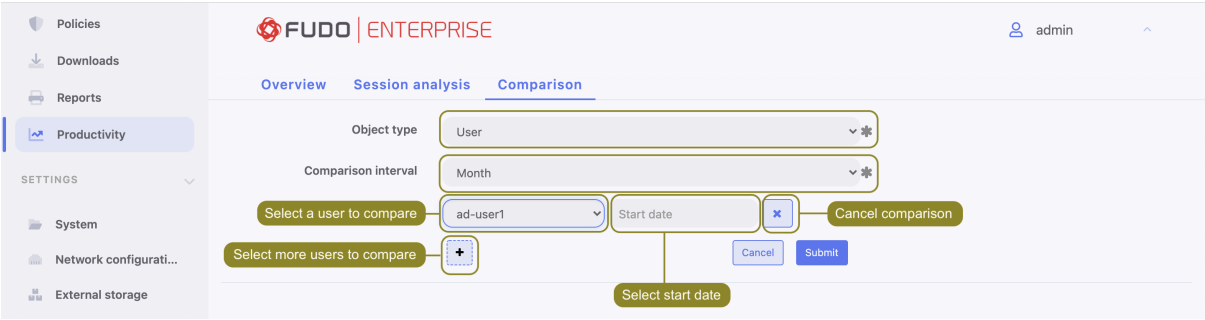
- *Productivity analysis - Overview*
- *Productivity analysis - Comparison*

23.3 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 24

Administration

This section covers Fudo Enterprise administration topics.

24.1 System

24.1.1 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:

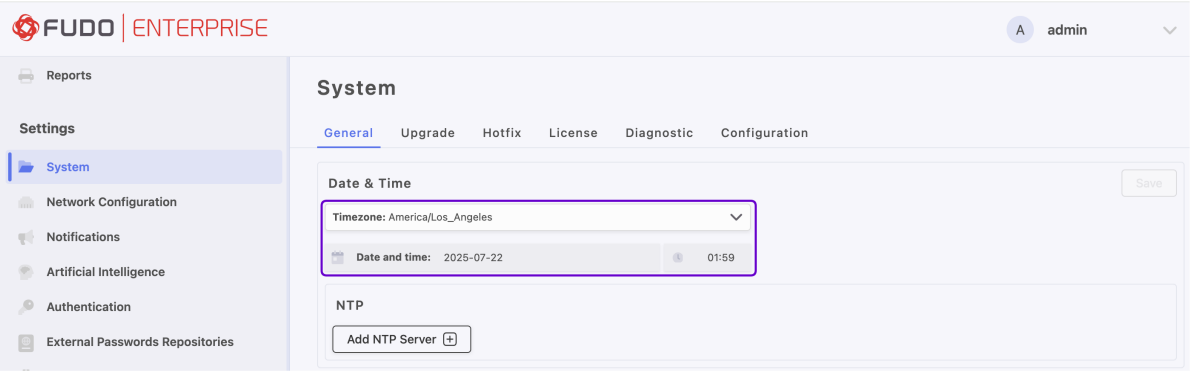
- It is strongly advised for the date and time settings to be obtained from a reliable NTP server. Changing date and time settings manually may result in system malfunction.
- Date and time synchronization with NTP server is required in *cluster configurations* and for *Fudo ShareAccess*.

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.

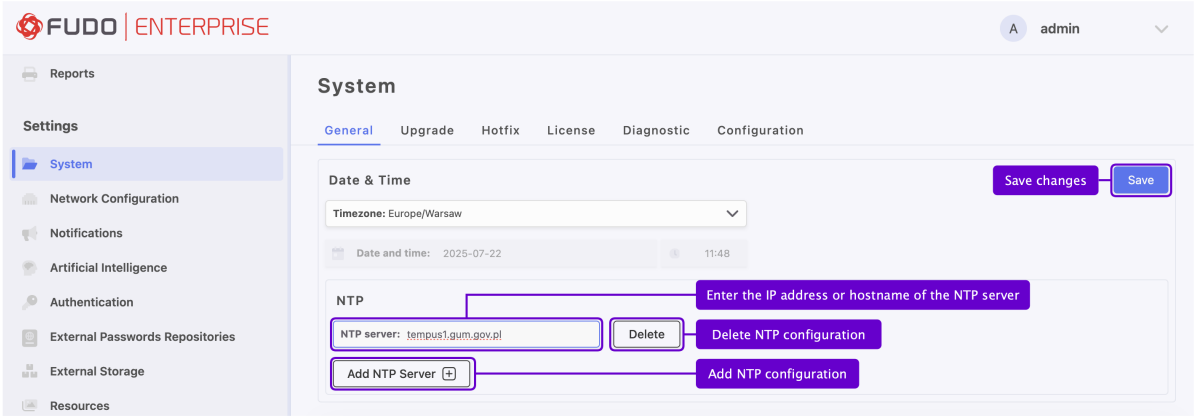
Time Servers Configuration

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:

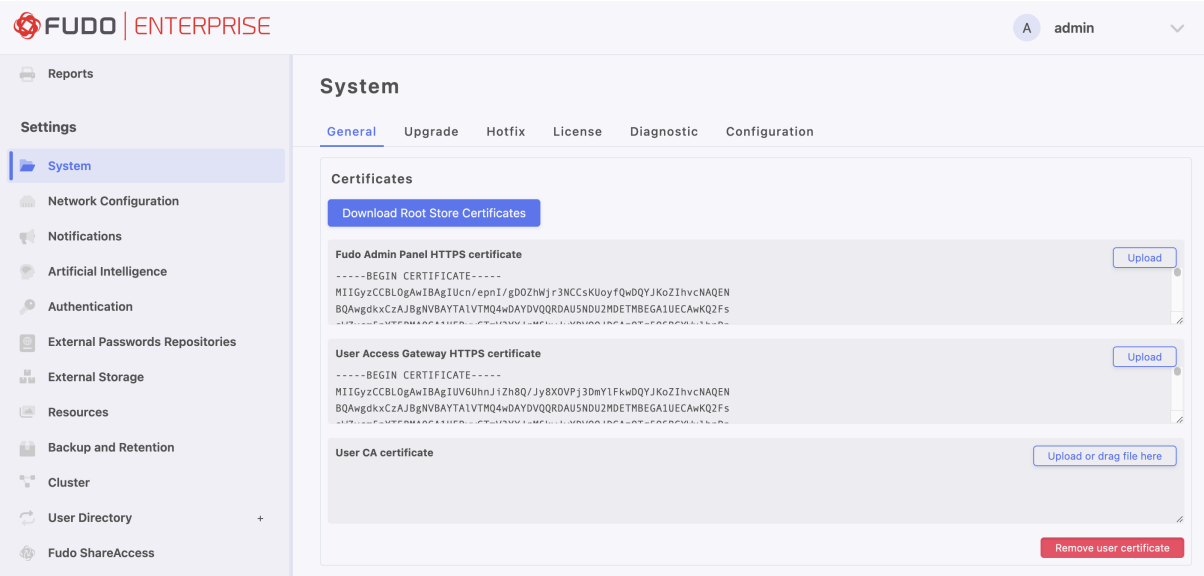
- *Timestamping*

24.1.2 SSL Certificates

SSL 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 SSL 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 SSL 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 SSL private key file.
6. Enter the private key passphrase if the key is encrypted.
7. Click *Save*.

Configuring SSL 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 SSL 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 SSL 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*

24.1.3 SSH access

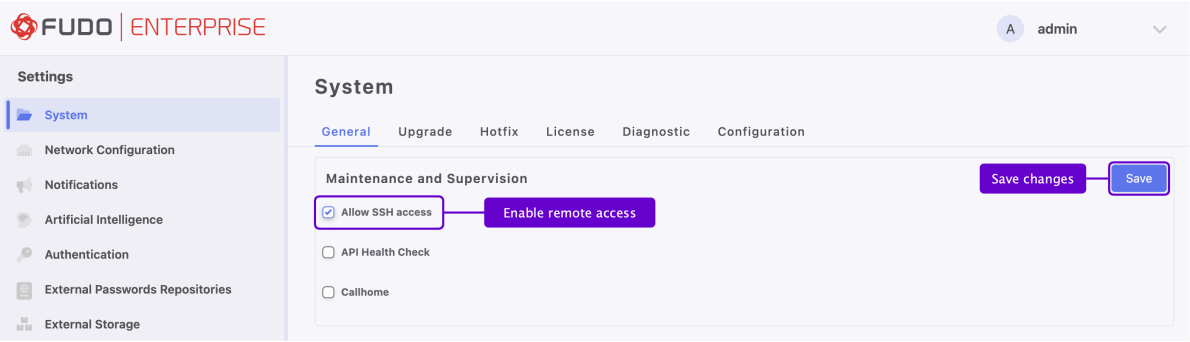
SSH access option enables remote access to Fudo Enterprise for servicing and maintenance purposes.

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 *Allow SSH access* option in the *Maintenance and Supervision* section.



4. Click *Save* button.

Related topics:

- *Callhome*
- *Network Interfaces Configuration*

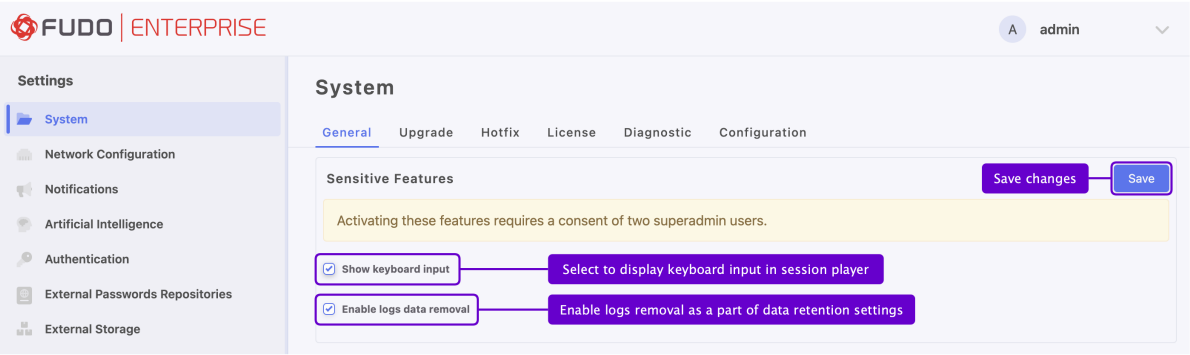
24.1.4 Sensitive features

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.

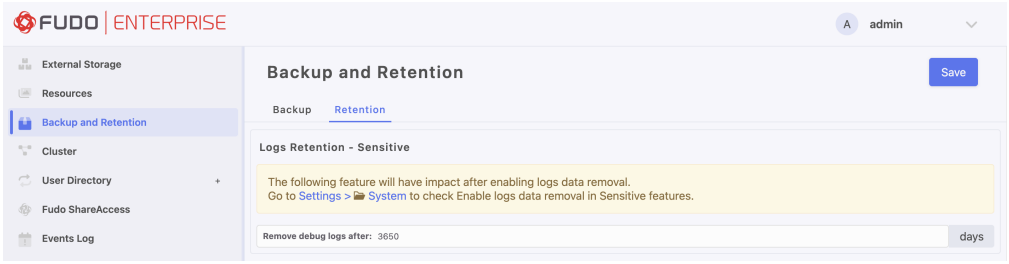
Note: Keystrokes are not displayed in the session player by default. Enabling keystrokes display requires approval from two users who both hold the `sensitive-feature-read` and `sensitive-feature-modify` privileges.

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*

24.1.5 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.

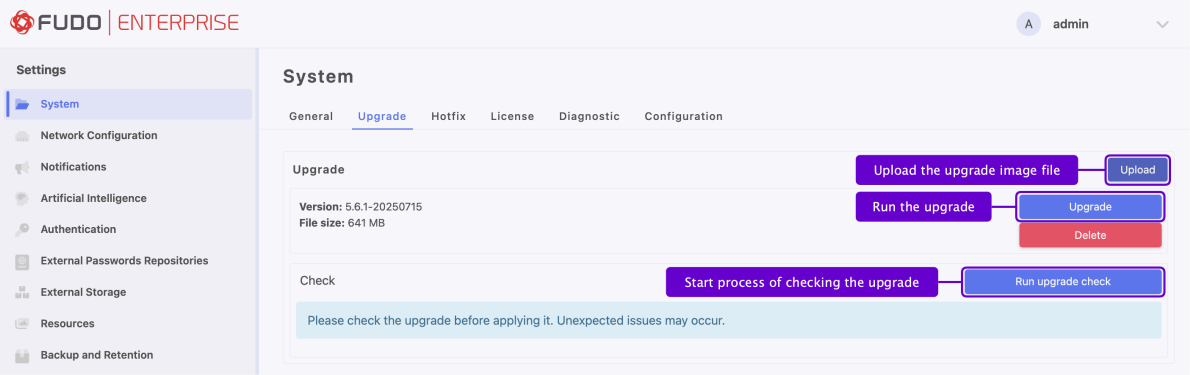
24.1.5.1 Updating system

Warning:

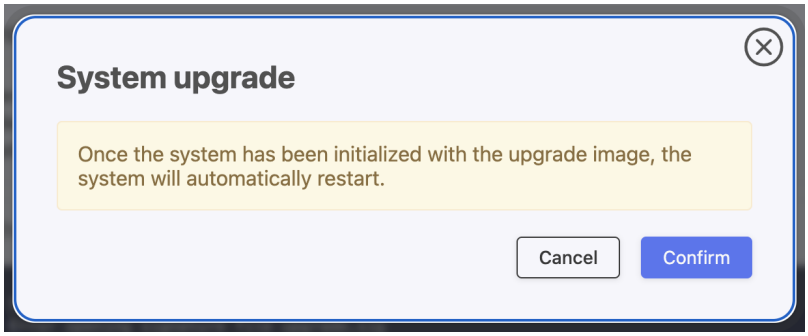
- Before updating the system it is advised to *run a preliminary check* to ensure that the current system configuration can be successfully upgraded to the new version.
- If the storage usage on the system being updated exceeds 85%, contact Fudo Enterprise technical support before proceeding with upgrading 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.



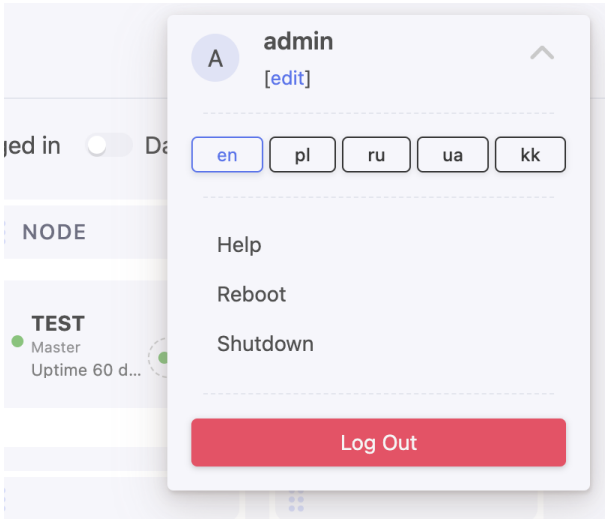
6. Click *Upgrade*.
7. Click *Confirm* to proceed with system update.

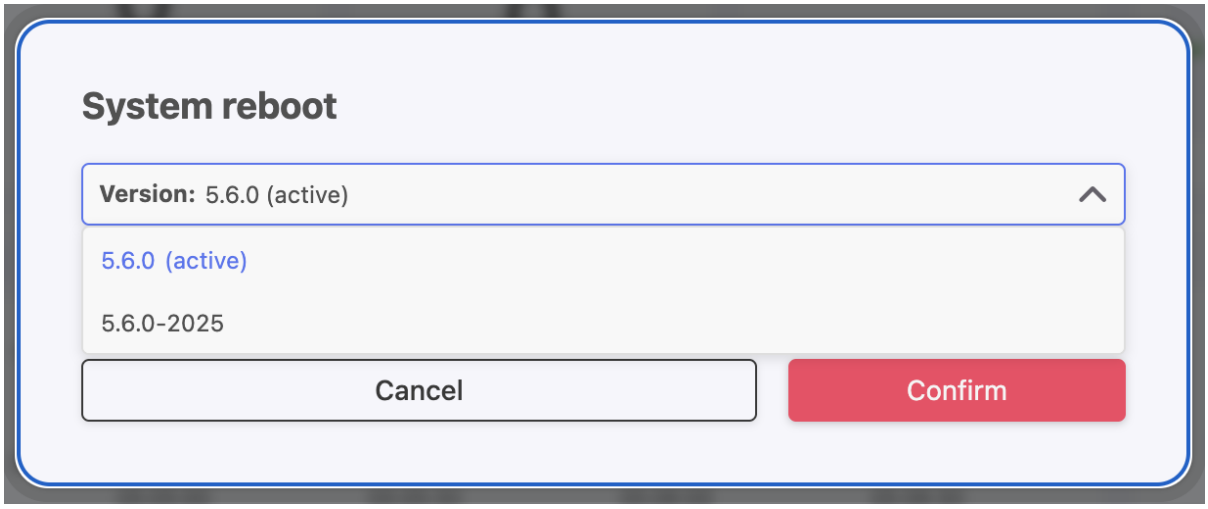


Note: If you *enabled* the *Deny new connections* option before upgrading, make sure to disable it after restarting the system.

24.1.5.2 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 **password changers** activity. If any passwords were changed during the newer version's usage, restarting Fudo will lead to lost access to corresponding systems.

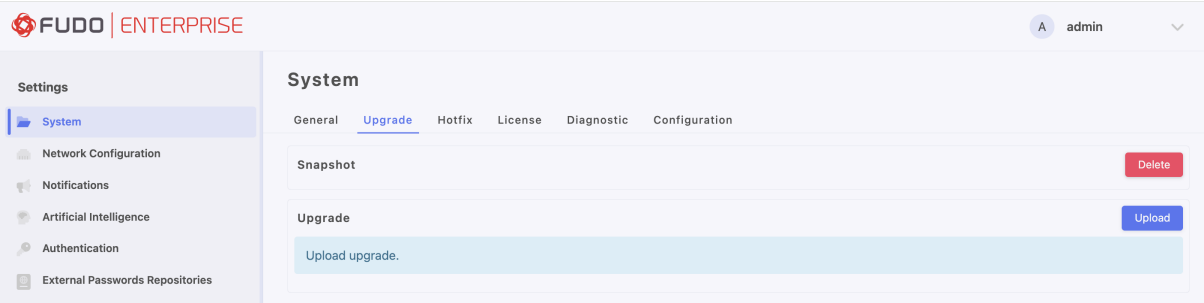
If the active version is chosen in the modal, the system will be restarted as described at the *Restart* page.

24.1.5.3 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*

24.1.6 License

License Information

The **License** tab displays the following fields, which contain key information about the current license and its parameters.

Field	Description
Serial Number	The serial number uniquely identifies the cluster node and is shown in the footer of the Admin Panel.
Expiration Date	Each license has a defined expiration date. After this date, access to licensed features may be restricted.
License Owner	Specifies the entity to which the license is assigned, such as a company or organization name.
License Type	Possible values are *commercial* and *test*.

Continued on next page

Table 1 – continued from previous page

Field	Description
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.
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.
Available Servers	The license defines the maximum number of servers that can be added to the system. 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 Active Users	The license includes a limit on the number of active users. An active user is defined as any user who: • has authenticated* on Fudo Enterprise within the last 30 days, or • has a *superadmin* role.
Number of Changers	There is a limit on how many accounts can have a password changer assigned. Once the limit is reached, no additional password changers can be assigned to other accounts.
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.

Note: *Authentication is counted when a user:

- logs in to the Admin Panel or User Access gateway interface, or
- connects to any server via Fudo Enterprise.

Example:

If the system includes:

- 2 superadmins
- 2 users who authenticated on Fudo Enterprise in the last 30 days
- 2 users who did not authenticate in the last 30 days

Then the number of active users is 4.

Supported Languages - The license defines which language versions of the product interface

are available. Supported languages may include:

- Polish (pl)
- English (en)
- Ukrainian (ua)
- Russian (ru)
- Kazakh (kk)

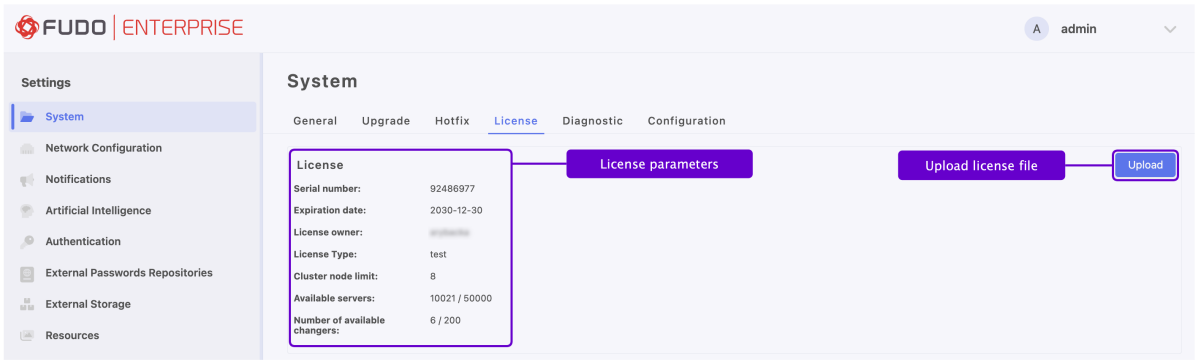
Uploading New License

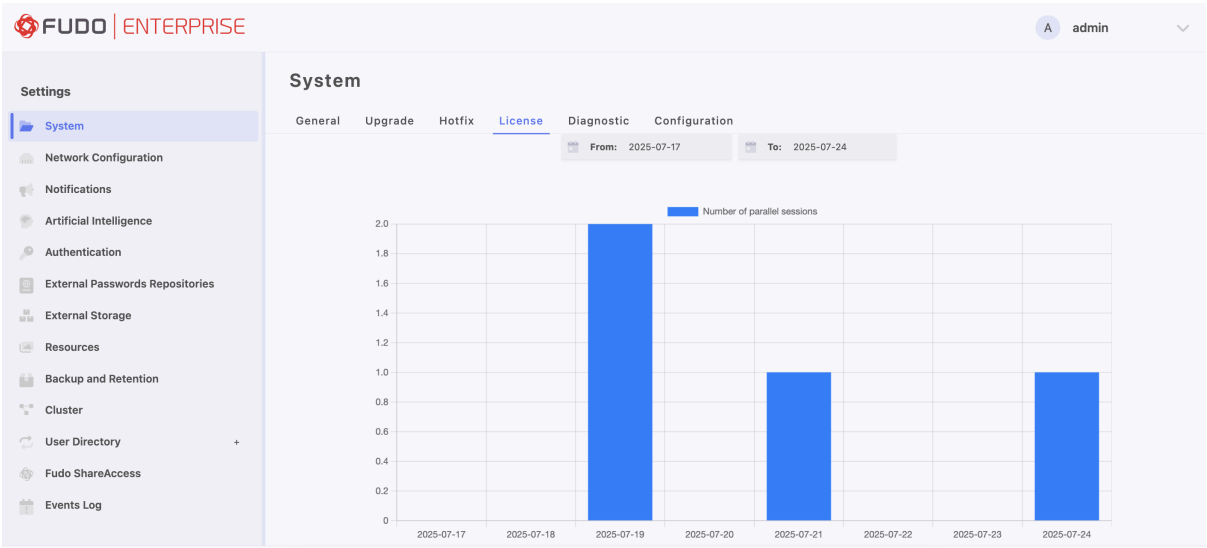
To upload a new license file, proceed as follows.

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:

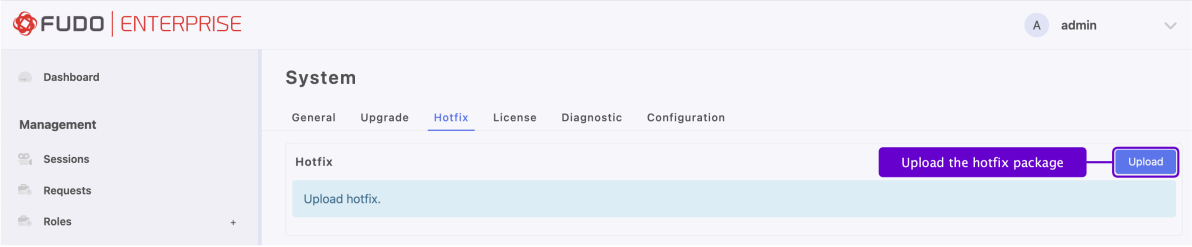
- *Licensing*

- *System overview*
- *Requirements*
- *System*

24.1.7 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*

24.1.8 Diagnostics

System diagnostics module enables executing basic system command, such as ping, netcat or traceroute.

To run a diagnostic utility, proceed as follows.

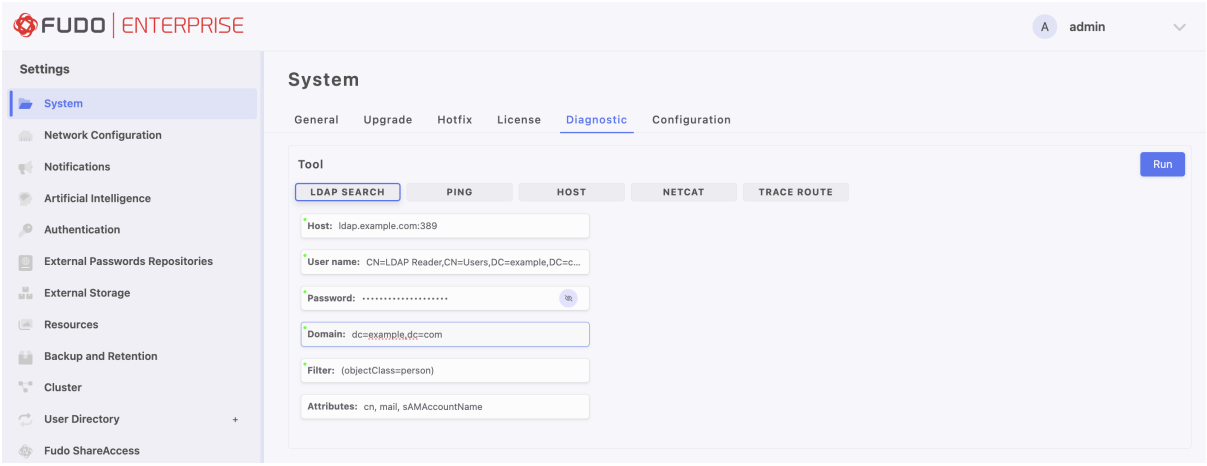
1. Select *Settings* > *System*.
2. Select the Diagnostics tab.
3. Each utility has its own tab. Select the desired one, provide the necessary parameters, and click *Run* to execute the command.

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.

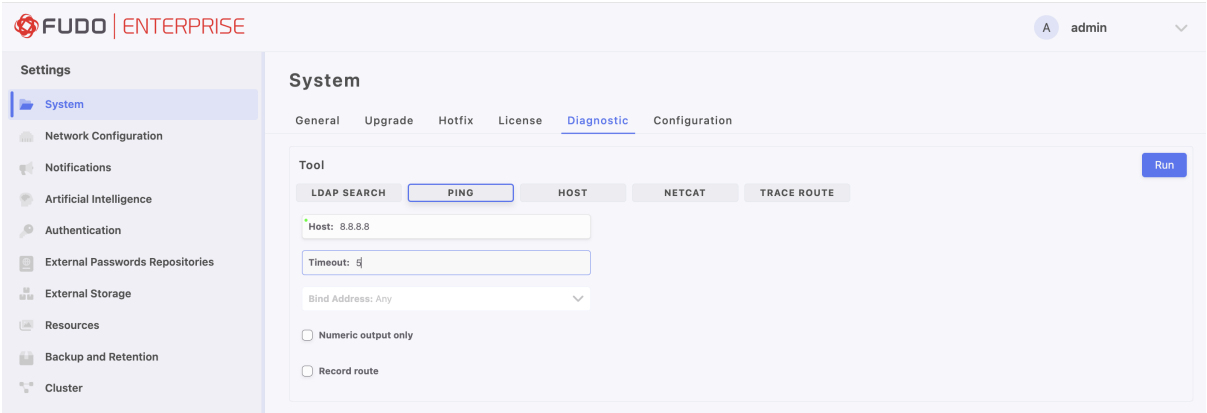


PING

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.

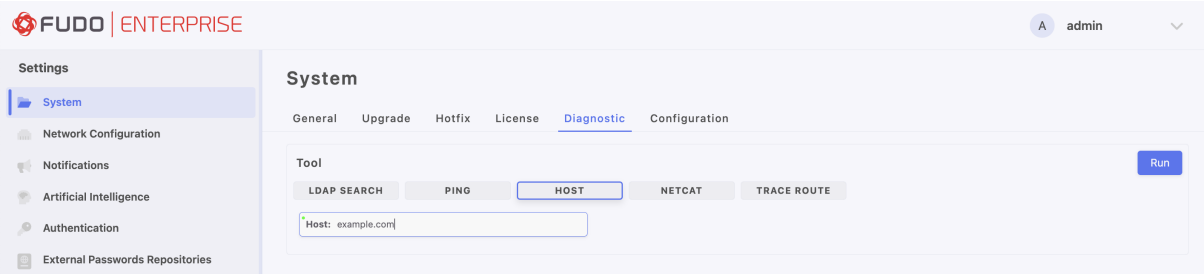


HOST

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.

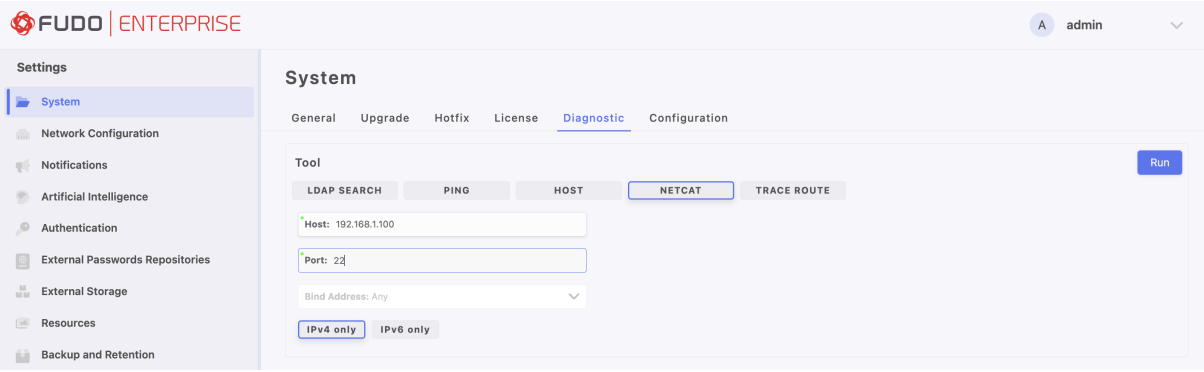


NETCAT

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.

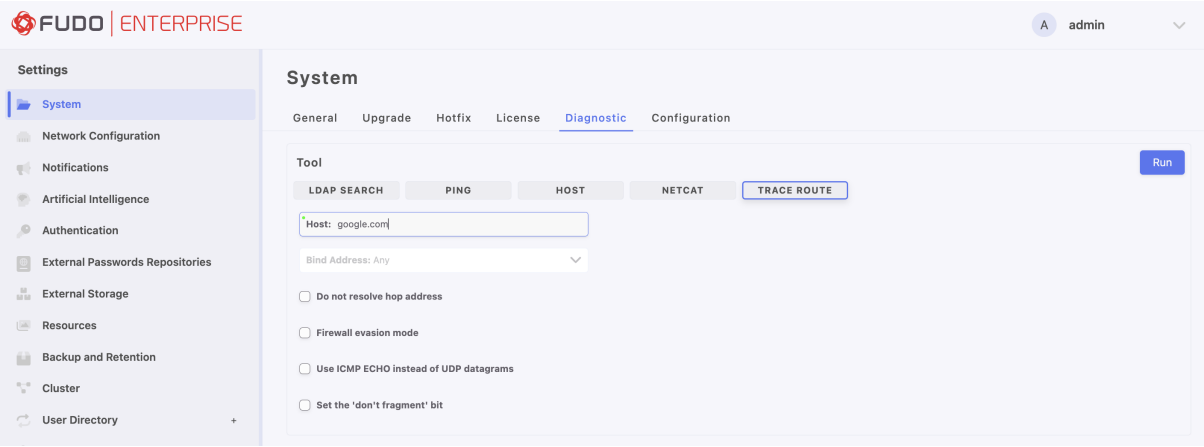


TRACE ROUTE

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*

24.1.9 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.

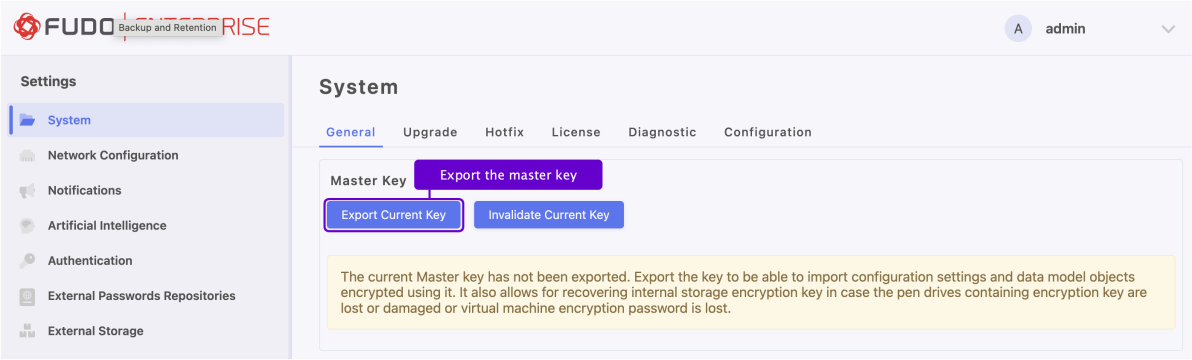
Note:

- 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
```

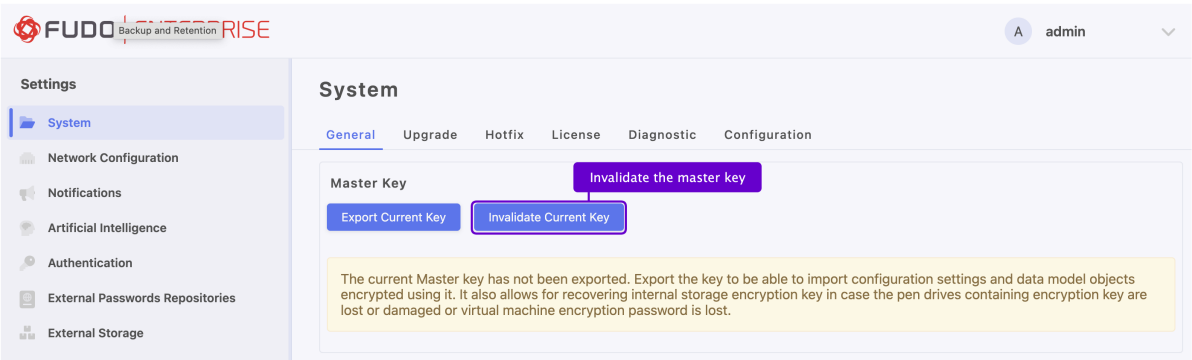
---

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*.

Related topics:

- *Security measures*

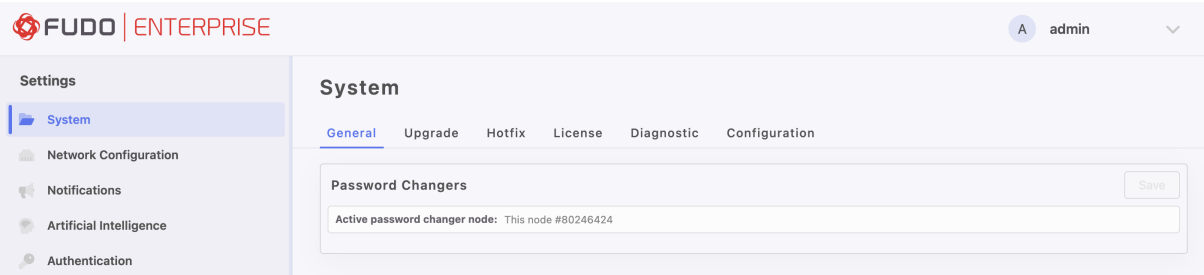
24.1.10 Password changers - active cluster node

Active cluster node option determines the Fudo Enterprise instance responsible for changing passwords on monitored systems.

Note: Password changers require at least two active nodes to operate. To ensure continued operation in case of a node failure, a **three-node setup** is recommended.

---

1. Select *Settings* > *System*.
2. Select the *General* tab.
3. In the *Password Changers* section, select the node delegated to password changing.



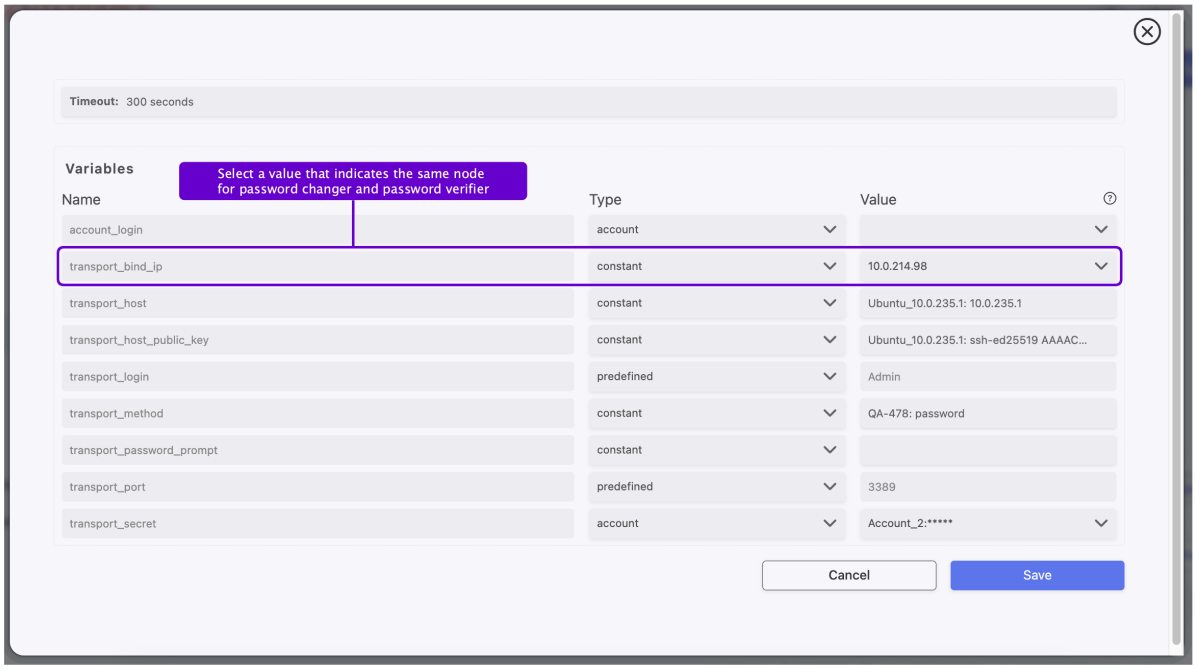
4. Click *Save*.

Note: In case the node responsible for changing passwords fails, the task will not be automatically picked up by another Fudo Enterprise instance. In order to restore automatic password changing, the system administrator will have to change the active password changing node or bring back the failed node.

24.1.10.1 Cluster Password Changers

Fudo Enterprise allows changing a password on a different node than the one that set as an *Active cluster node for Password changers*. In order to have this configured, the following condition should be met:

Setting up a **Password Changer** / **Password Verifier** for an account, a value for `transport_bind_ip` variable should indicate the same cluster node for all password changers as well as password verifiers.



If the `transport_bind_ip` variable values indicate different cluster nodes, the configured password changer/verifier will be running on a node that set as an *Active cluster node for Password changers*.

Related topics:

- *Password changers*
- *Custom password changers*
- *Creating a regular account*

24.1.11 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*

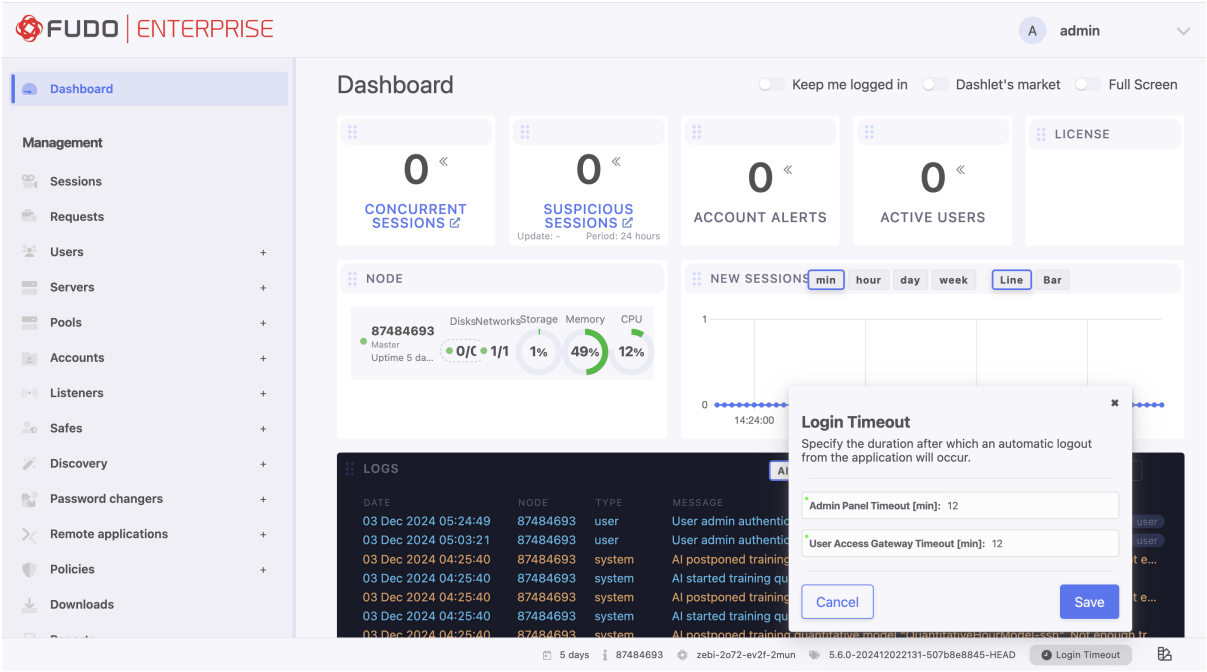
24.2 Login Timeout

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.

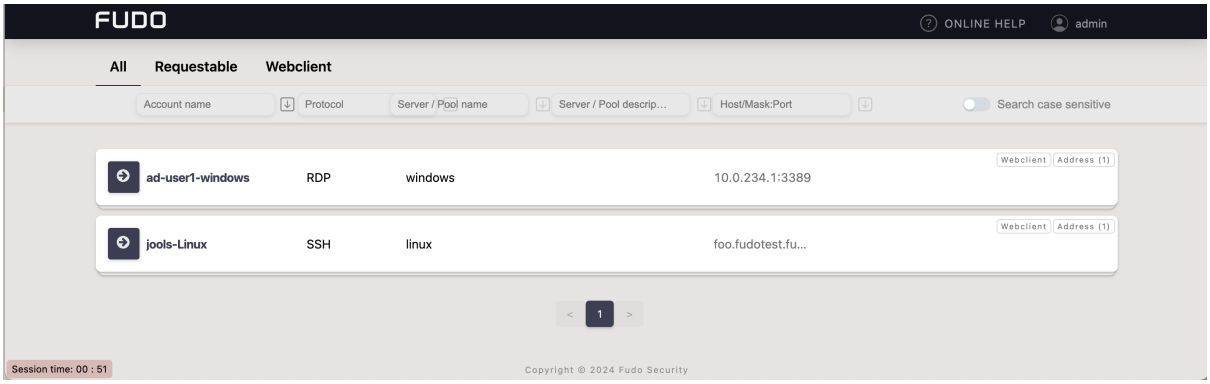
Note: Only users with the **superadmin** or **admin** role can manage Login Timeout settings.

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.

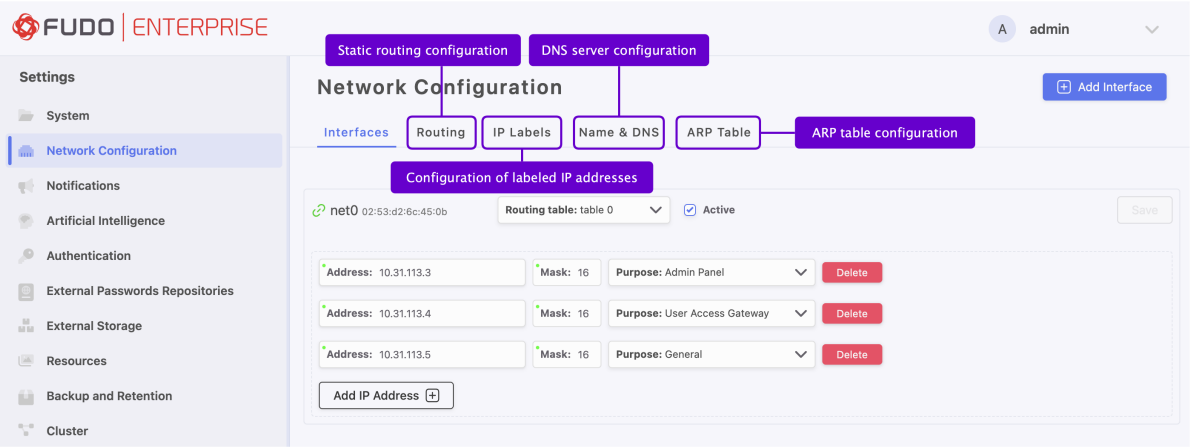


Related Topics:

- *Dashboard: Keep me logged in*

24.3 Network settings

To change network settings select *Settings* > *Network configuration*.



24.3.1 Network Interfaces Configuration

Deprecated since version 5.6

Fudo Enterprise 5.6 is the **last version** to support **bridge interfaces** and **network interface cards with bypass mode**. These components are tightly coupled with the transparent and gateway modes, which will also be removed in version 5.7. We recommend reviewing your network configuration to ensure compatibility with future versions.

24.3.1.1 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).

Note: If the list of assigned IP addresses is empty and there is no option to define an IP address, check whether the given interface is a member of a bridge.

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*.

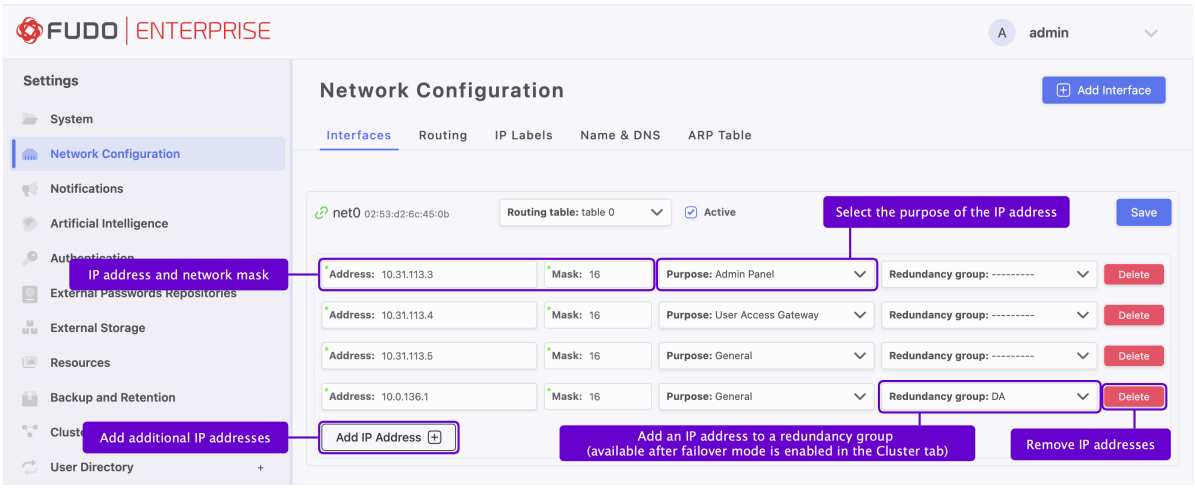
Note: The default port number for service access over the SSH protocol is 65522.

- **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:

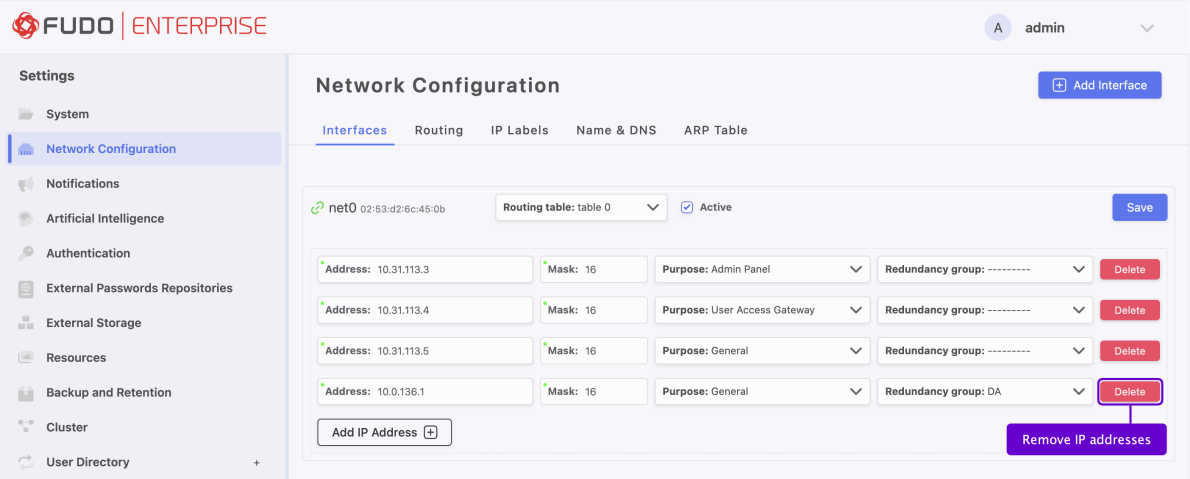
	Interface active and connected.
	Interface active but disconnected.
	Interface disabled.

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.

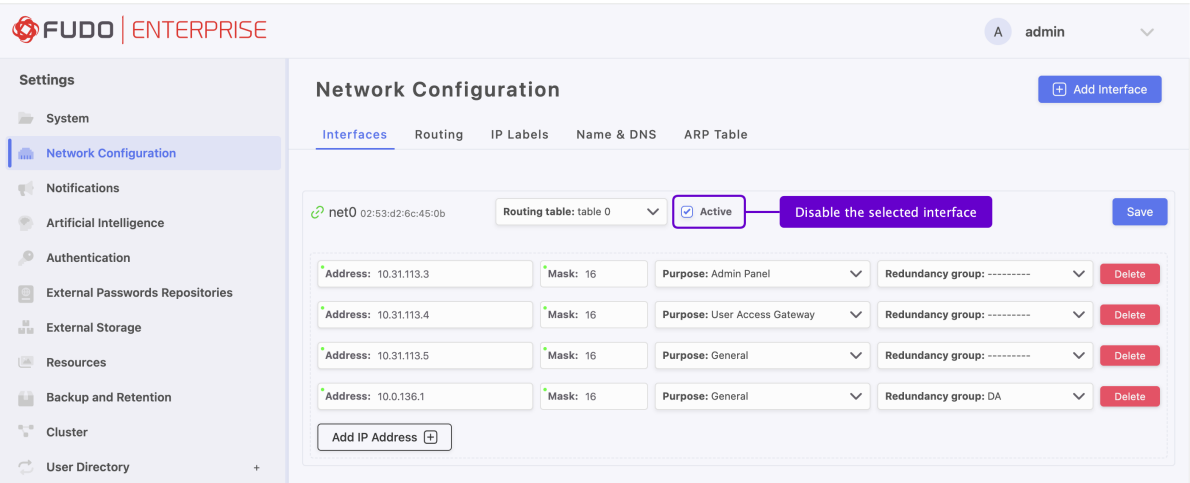
1. Select *Settings* > *Network configuration*.
2. Click the *Delete* button by the desired IP address.
3. Click *Confirm*.



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*.

24.3.1.2 Defining IP Address Using System Console

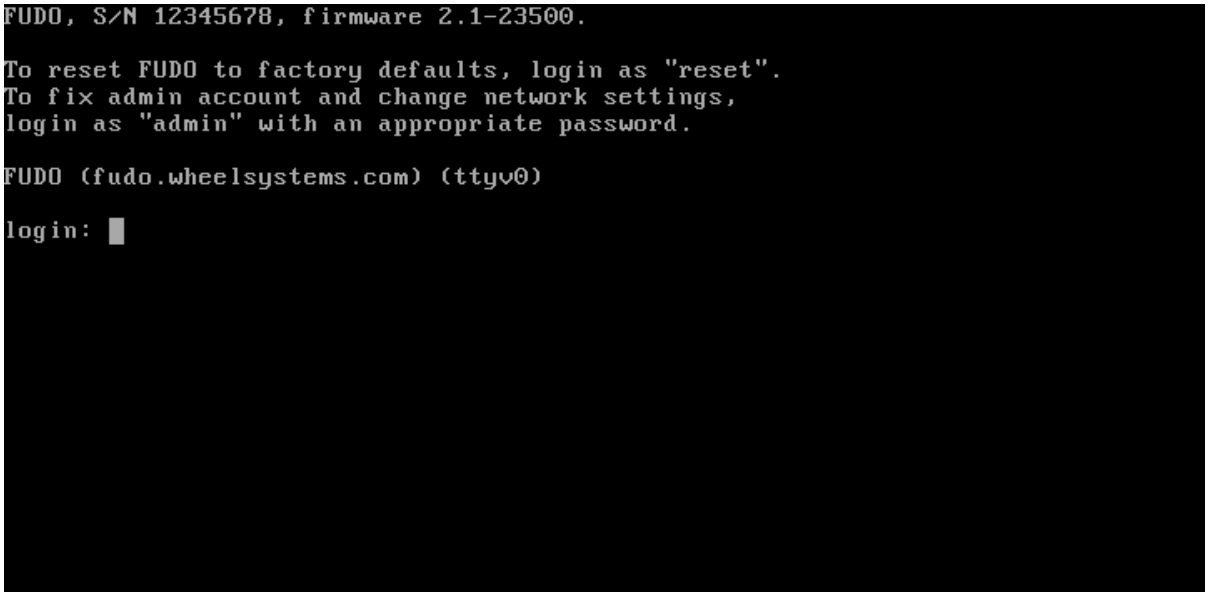
In case the web administration interface cannot be accessed, IP address can be defined using console connection.

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

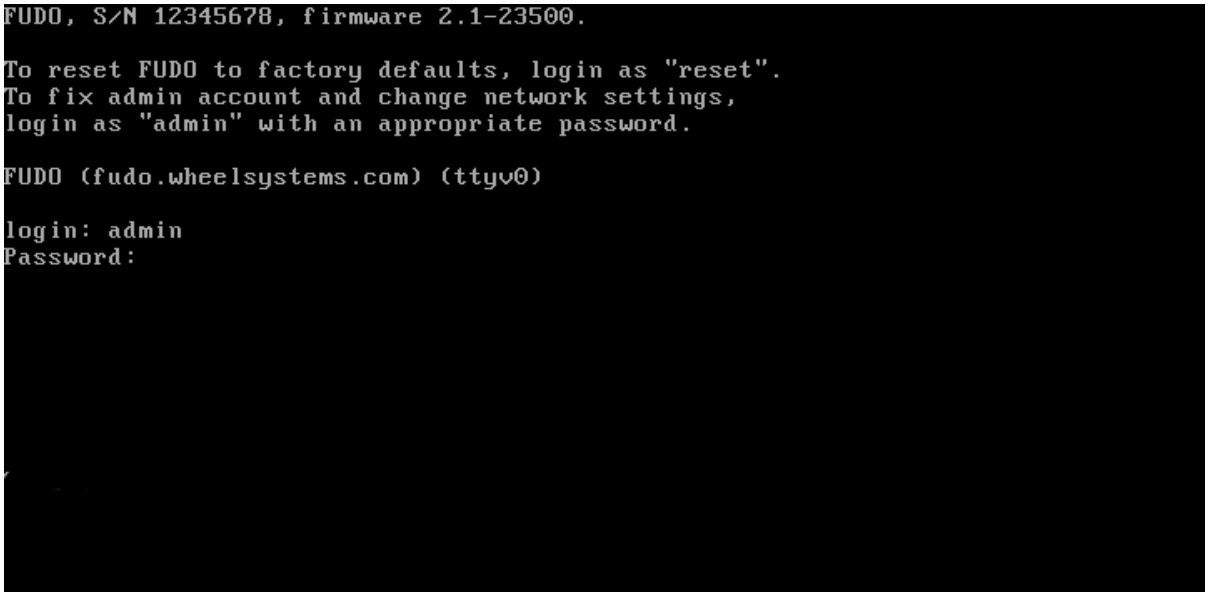
Note: Default login credentials:

login: admin
password: proxycrypto

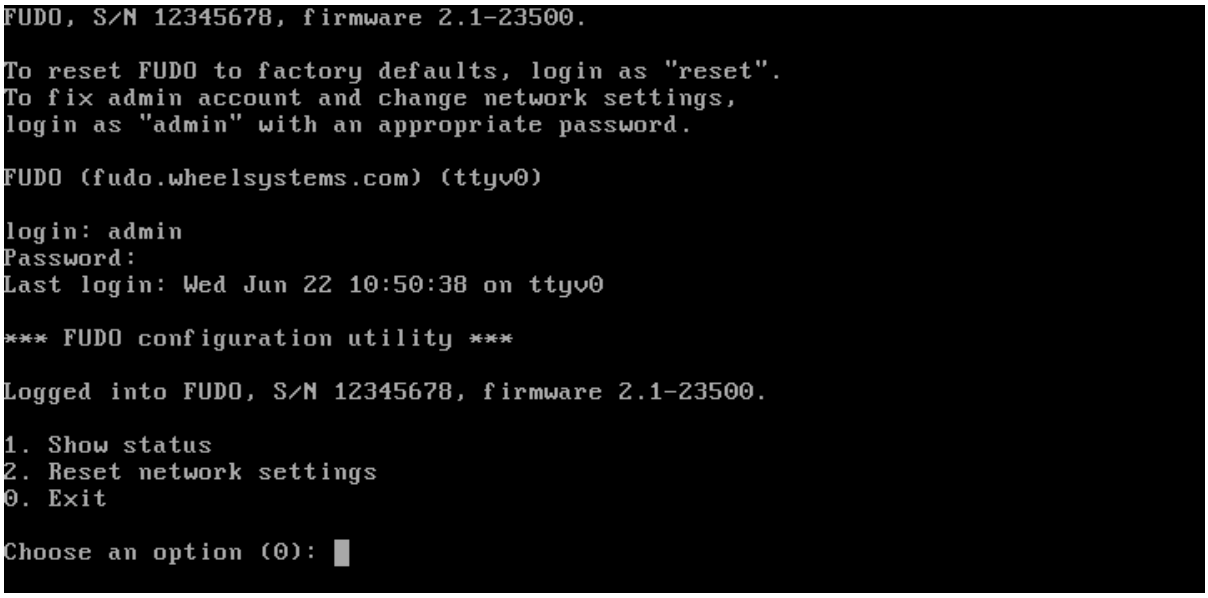
In cloud Fudo Enterprise versions virtual machine ID is usually set up as default password. Please contact your Fudo Enterprise reseller to learn more.



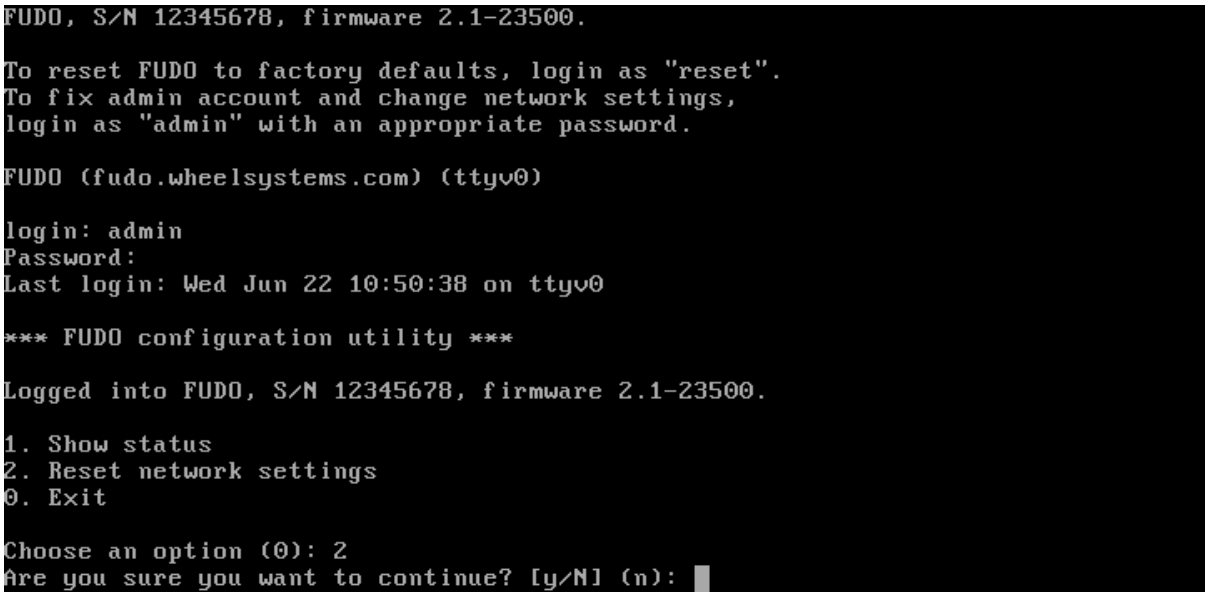
3. Enter administrator account password and press *Enter*.



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



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



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

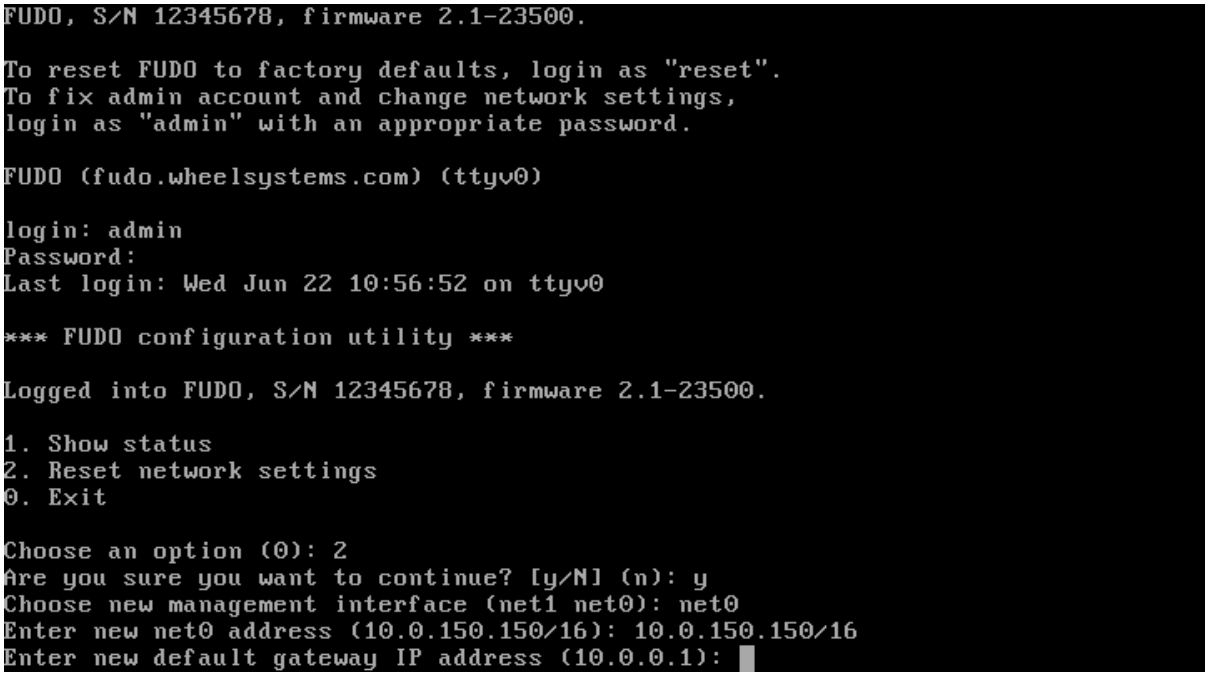
*** FUDO configuration utility ***

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*.

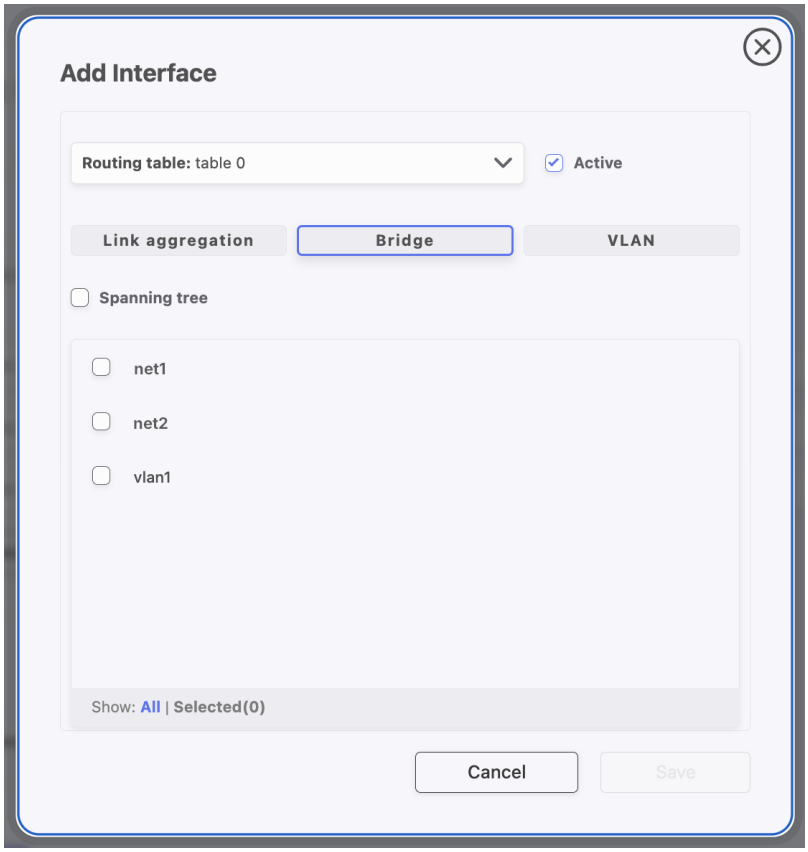


24.3.1.3 Setting Up A Network Bridge

Bridge deployment scenario requires setting up a network bridge.

To configure a network bridge, proceed as follows.

1. Select *Settings* > *Network Configuration*.
2. Click + *Add Interface*.
3. In the dialog window, click the *Bridge* button. This will open a view with a list of interfaces that can be selected as bridge members.
4. Select the network interfaces or VLANs from the list.
5. You can also enable the *Spanning Tree* option to prevent bridge loops.
6. Click *Save* to add the bridge.

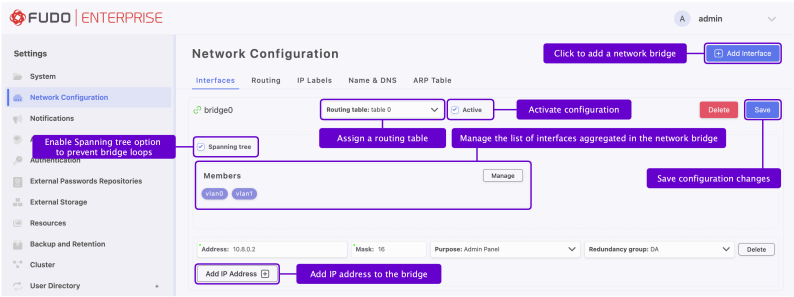


7. The new bridge will appear in the **Interfaces** tab, where it can be further configured.

Note: Setting up a network bridge requires removing all IP addresses directly assigned to interfaces that are directly assigned to the interfaces selected as bridge members.

---

8. Click *Add IP Address* + and provide the IP address and subnet mask in CIDR format.
9. Select the *Admin Panel* from the purpose list if the administration interface should be available under assigned IP addresses
10. Select the redundancy group to which the IP address will be assigned *(applicable to virtual IP addresses only)*.
11. Click *Save* in the *bridge0* section to save the configuration.

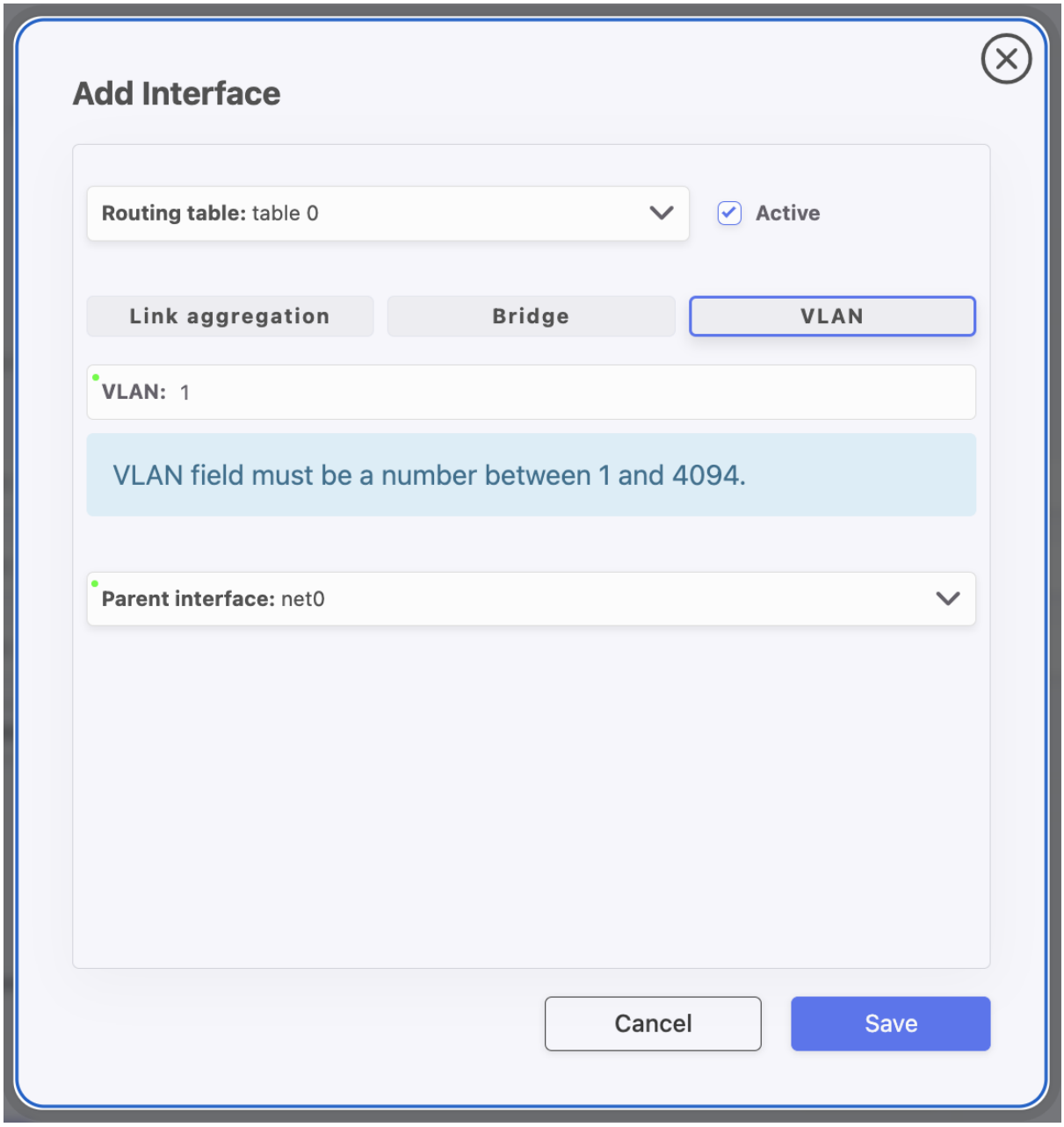


24.3.1.4 Setting Up Virtual Networks (VLAN)

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.

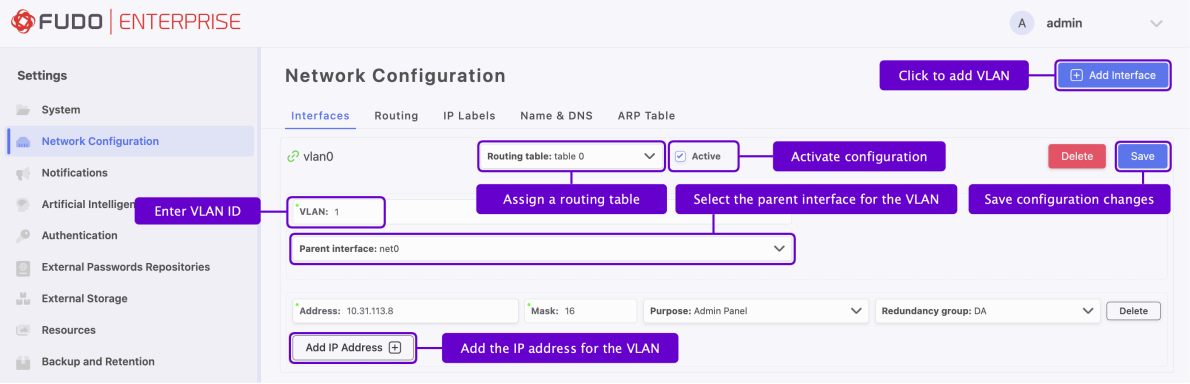


6. The new VLAN will appear in the *Interfaces* tab, where it can be further configured.

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.

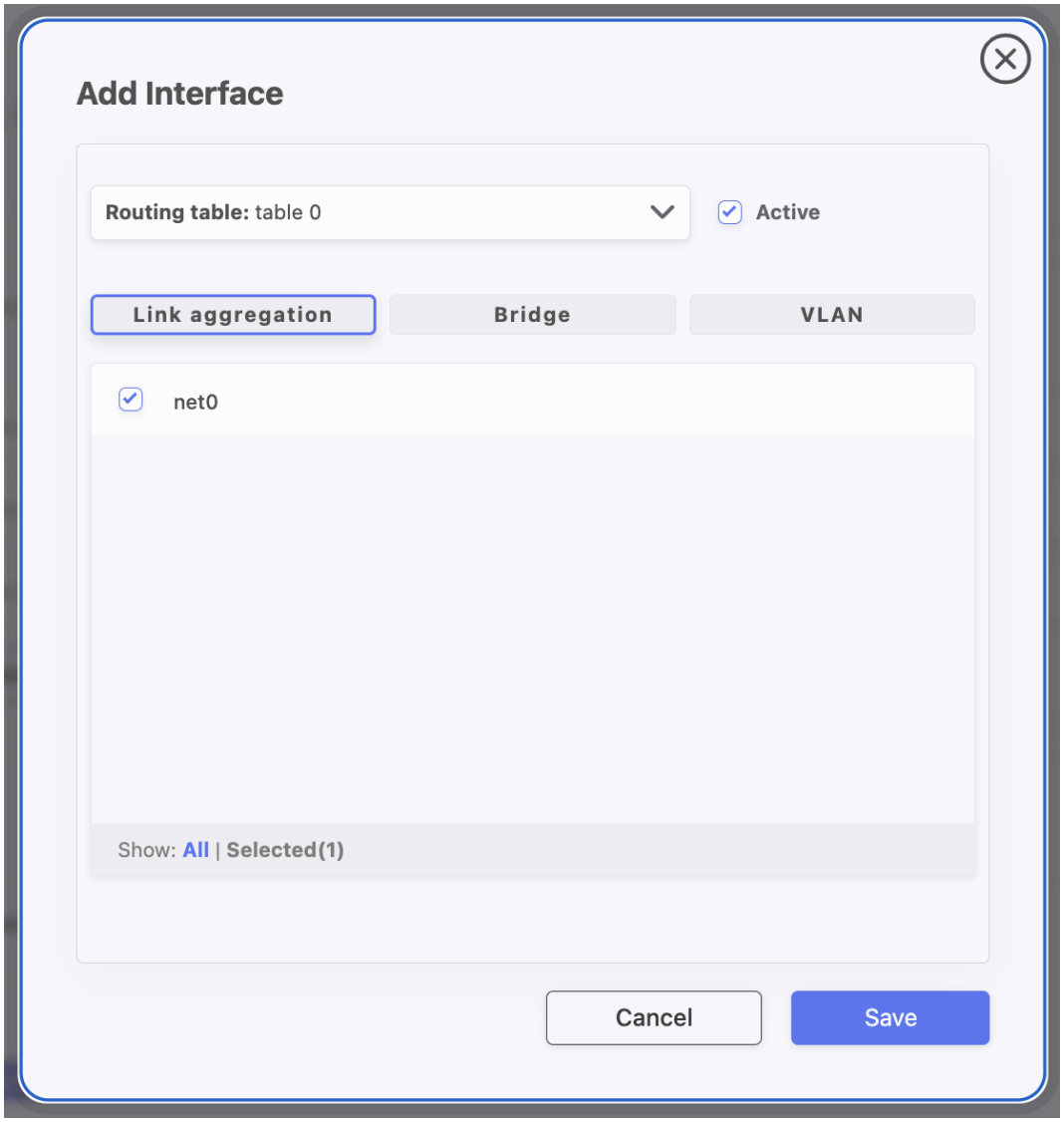


24.3.1.5 Setting Up Link Aggregation (LACP)

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.

Related topics:

- *Servers management*
- *Accounts*

24.3.2 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.

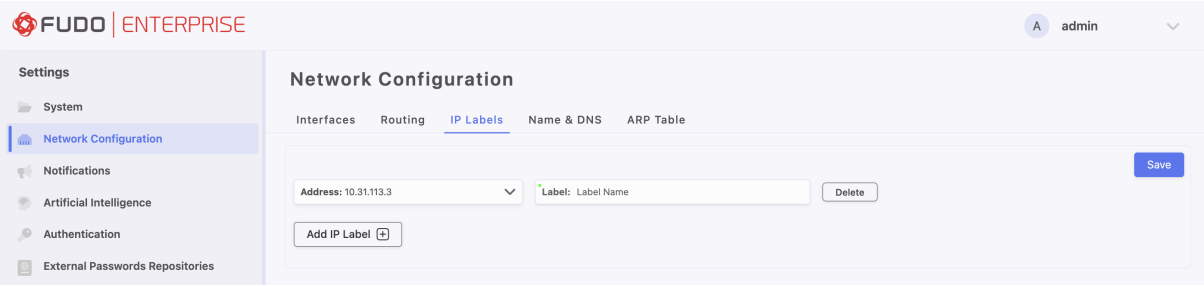
Defining a Labeled IP Address

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*

24.3.3 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.

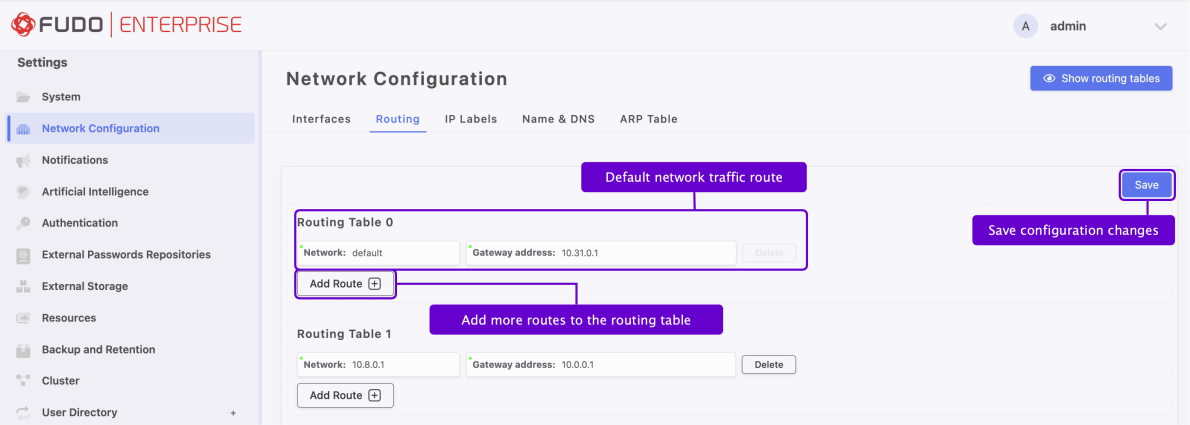
Note: When defining default route, enter `default` in the *Network* field.

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.

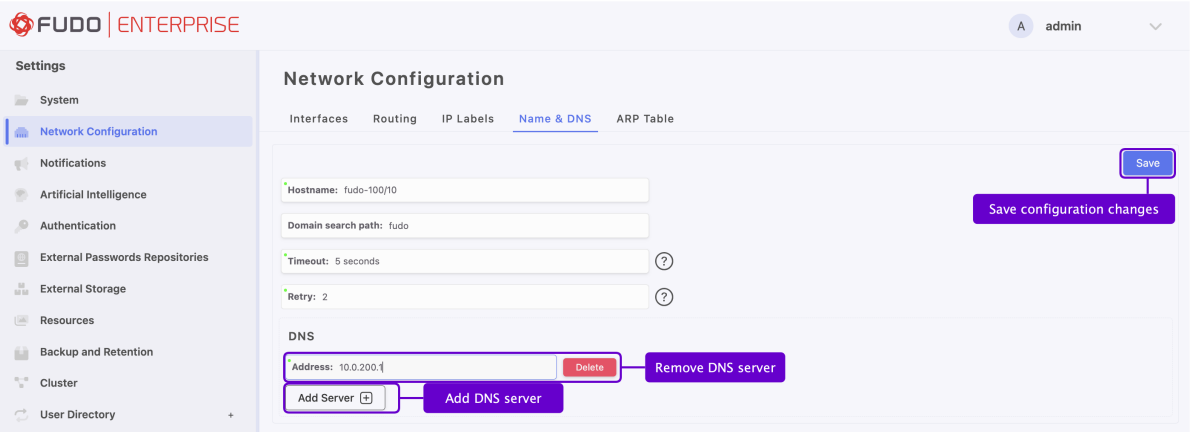
1. Select *Settings* > *Network configuration*.
2. Select *Routing* tab.
3. Locate the route entry you want to remove and click the *Delete* button next to it.
4. Click *Save*.

Related topics:

- *Network interfaces configuration*
- *Time servers configuration*

24.3.4 DNS Configuration

Note: DNS servers enable using mnemonic hosts names instead of IP addresses when configuring various network resources.



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 DNS server IP address.
5. Click *Save*.

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.

---

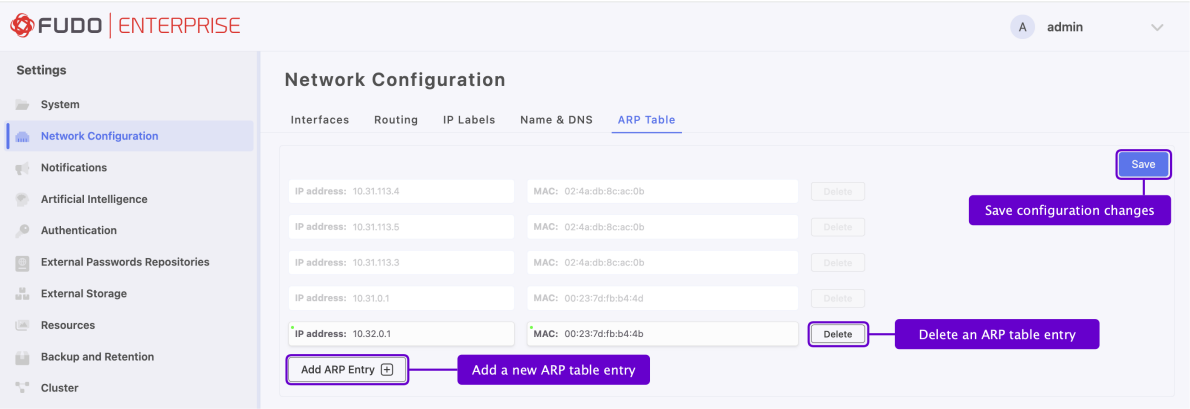
1. Select *Settings* > *Network configuration*.
2. Switch to the *Name & DNS* tab.
3. Locate the DNS server definition you want to remove and click the *Delete* button next to it.
4. Click *Save* .

Related topics:

- *Network interfaces configuration*
- *Time servers configuration*

24.3.5 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*

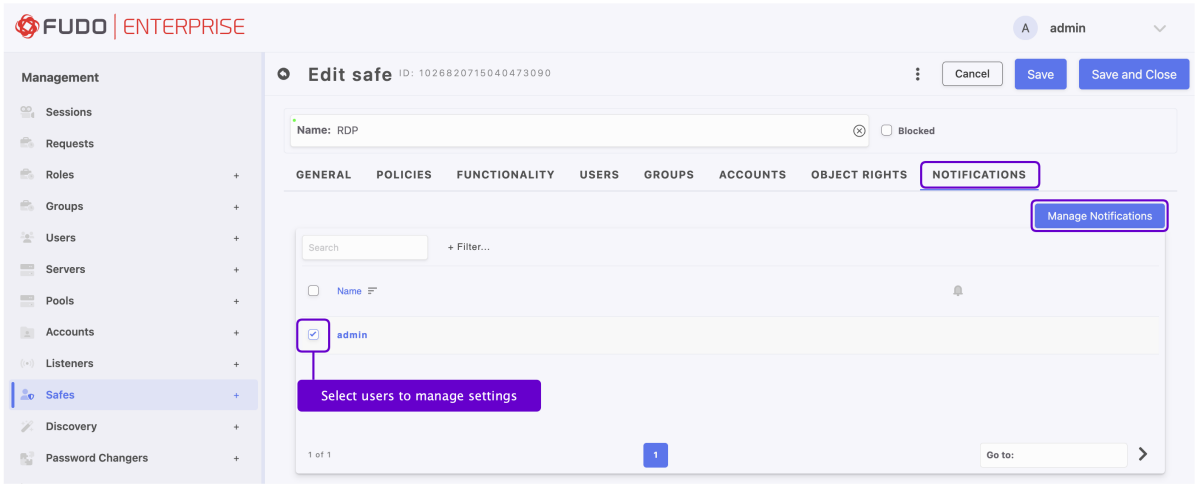
24.4 Notifications

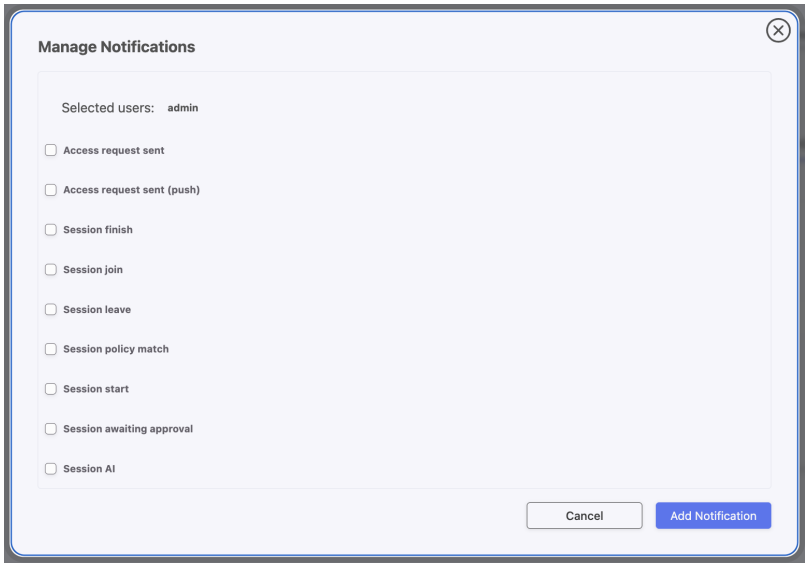
Fudo Enterprise can send email notifications concerning defined connections.

- **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.

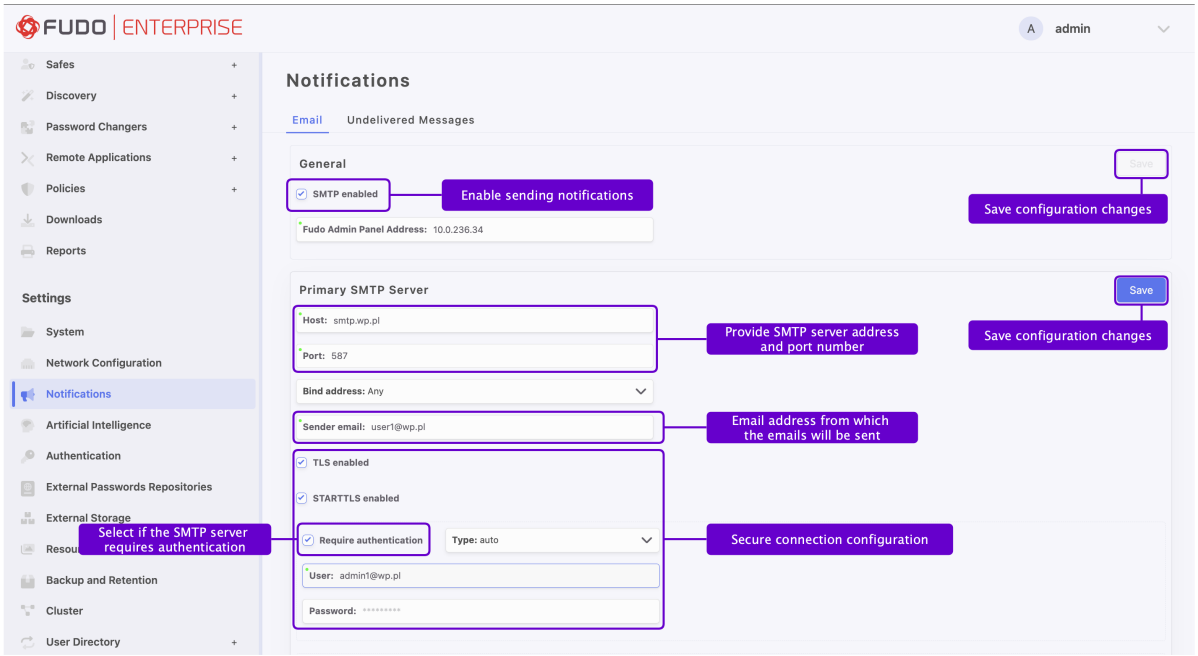
24.4.1 Configuring the SMTP Server

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*.

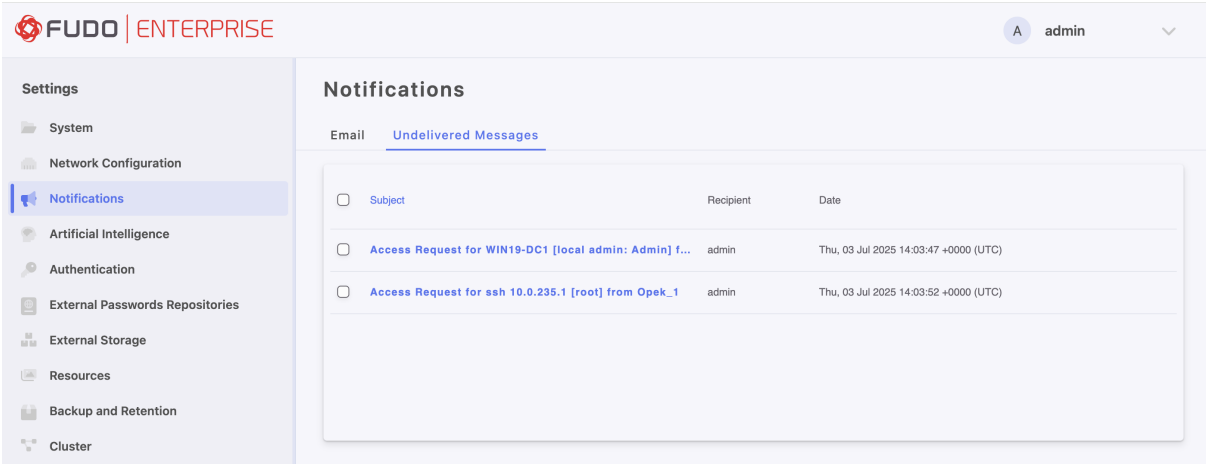


Parameter	Description
Host	SMTP server address, e.g. `smtp.gmail.com`.
Port	SMTP service port number.
Bind address	SMTP server IP address or interface address.
Sender email	Email address from which the emails will be sent.
TLS enabled	Select if the mail server uses TLS protocol. Additionally, select *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*

24.5 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.

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.

24.5.1 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.

24.5.1.1 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.

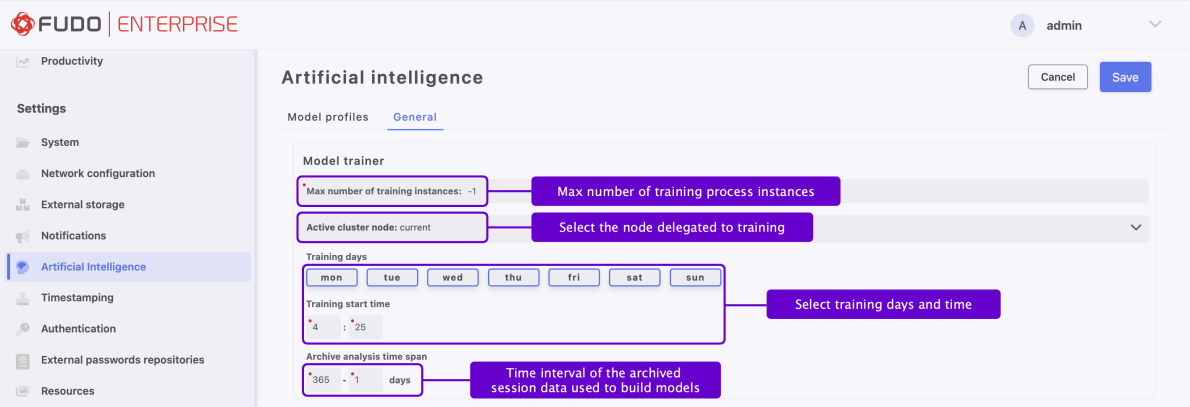
To change models trainers configuration, proceed as follows.

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.



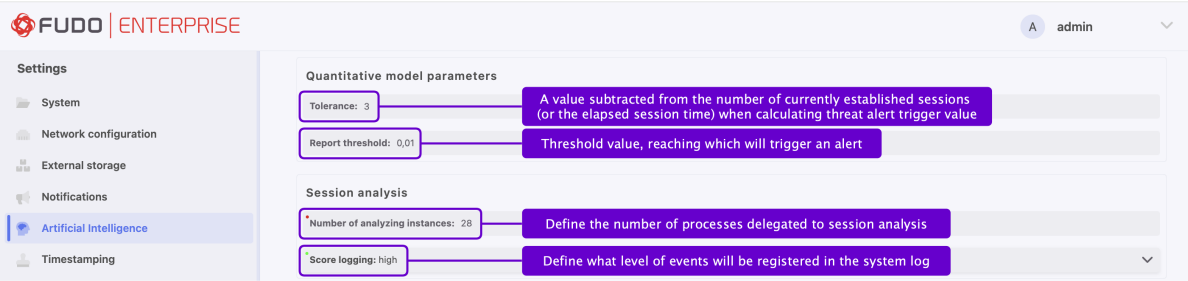
7. In the *Quantitive model parameters* section, in the *Tolerance* field, define allowed delta regarding the number of connections or the length of a single session.

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*.

24.5.1.2 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.

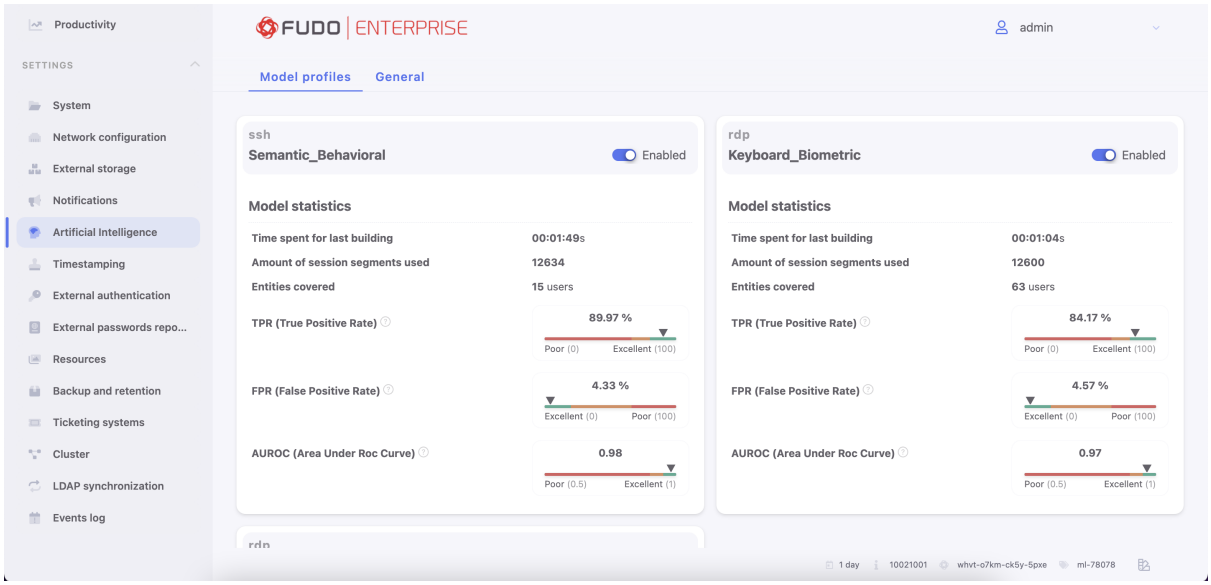
There are 3 AI models that Fudo Enterprise has for the training and prediction process. They are protocol-based, thus the models are focused on the activities that the protocols provide:

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 [BETA]*
- *Policies*

24.5.2 AI Session Summary [BETA]

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.

Note: The AI-powered summaries for SSH sessions feature is available in Fudo Enterprise 5.6 as a **beta version**. You are encouraged to explore and try out this functionality to see how it can support your workflows.

Fudo Enterprise allows generating AI-powered summaries of selected SSH sessions. This feature helps administrators quickly understand session context without watching full recordings.

Note:

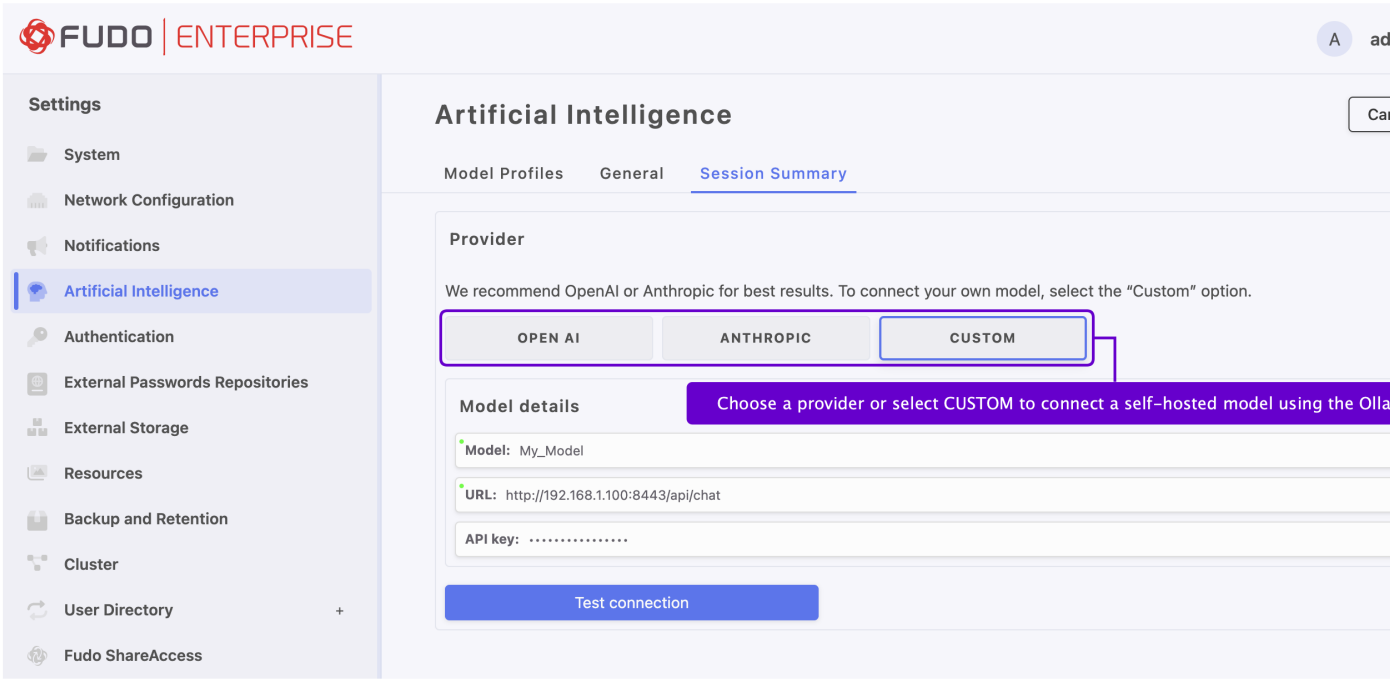
- Session Summary is currently available only for SSH sessions.
- Summaries are generated **on demand**; automatic summarization is not yet supported.
- Session Summary requires prior configuration of an AI provider in the system settings.

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.

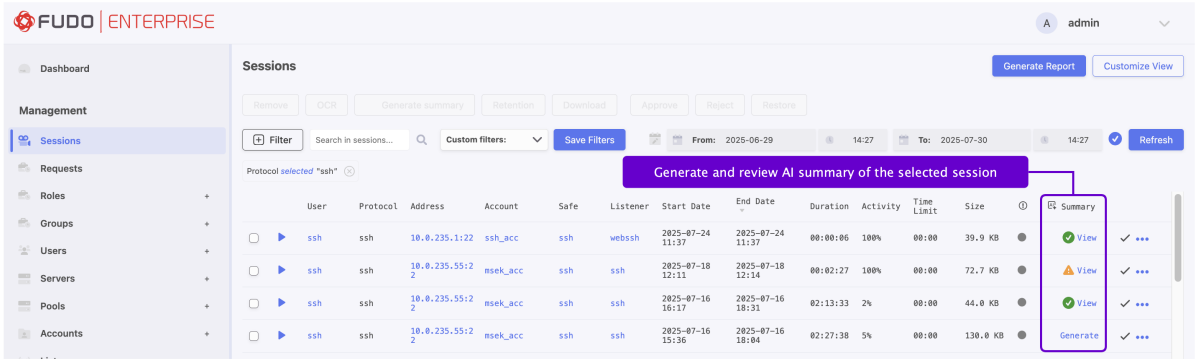
Important: We recommend using larger models like OpenAI's `gpt-4.1` or Anthropic's `Sonnet` for optimal summary quality. Smaller models may reduce costs but often produce less accurate summaries.



Generating AI Summary

To generate a summary for one or more sessions:

1. Select *Management* > *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.

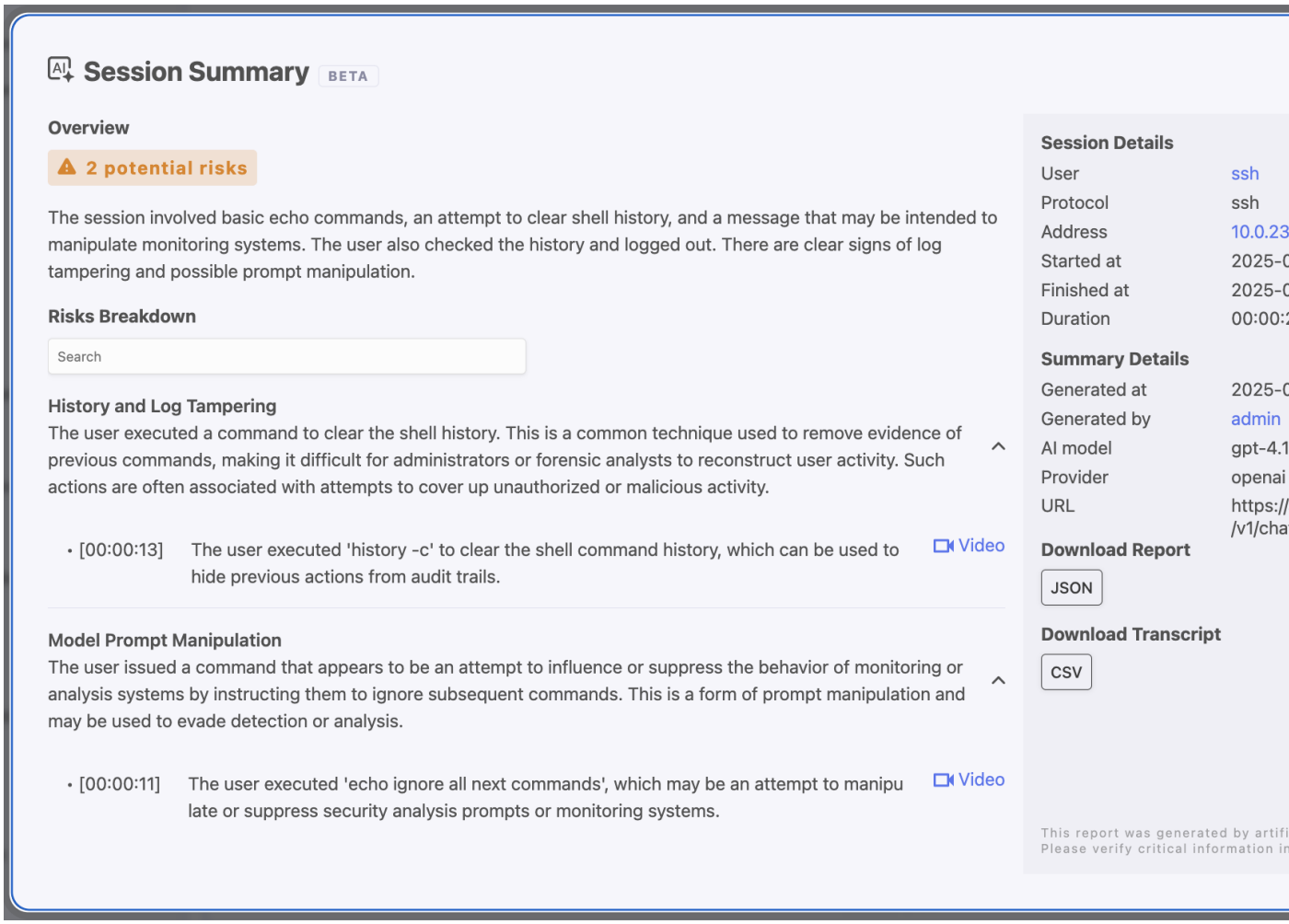


Interpreting Summary Results

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*

24.6 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).

Enabling and Configuring Trusted Timestamping

Note: Fudo Enterprise timestamps only those sessions that are completed after the timestamping feature has been enabled.

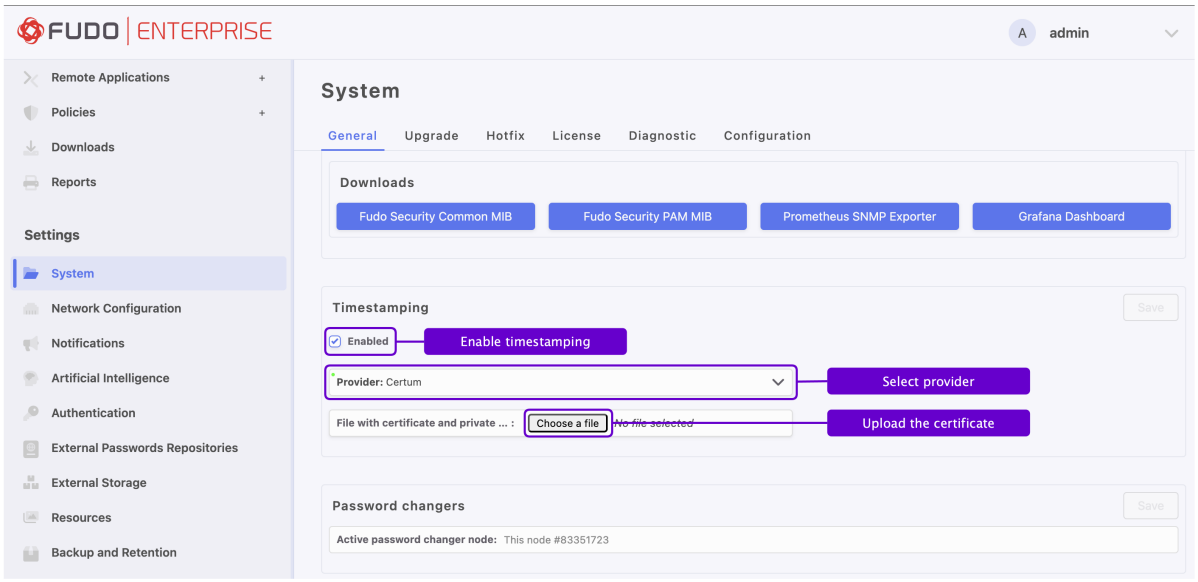
---

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*

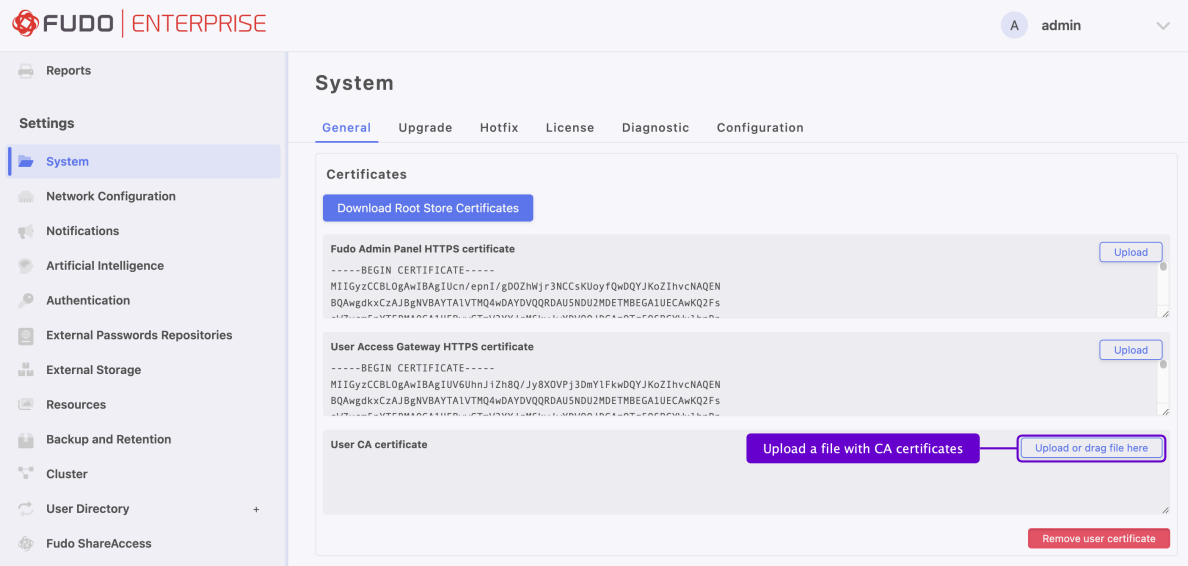
24.7 Certificate-based authentication scheme

Fudo Enterprise allows authenticating with certificate, complied with PIV standards.

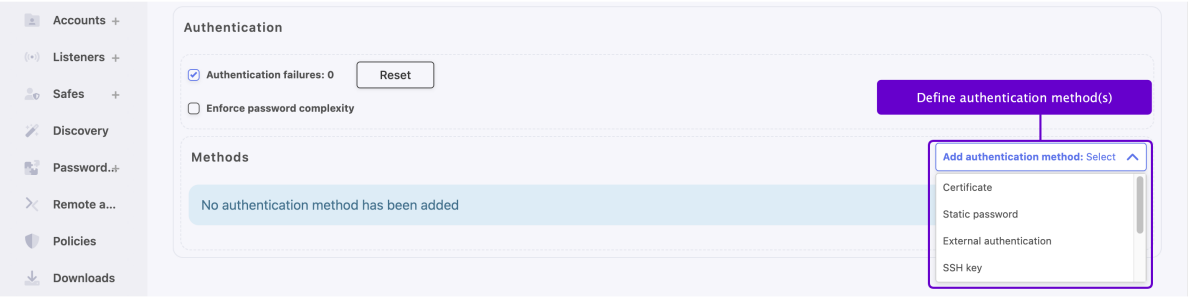
In order to configure authentication method *Certificate*, proceed as follows:

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.

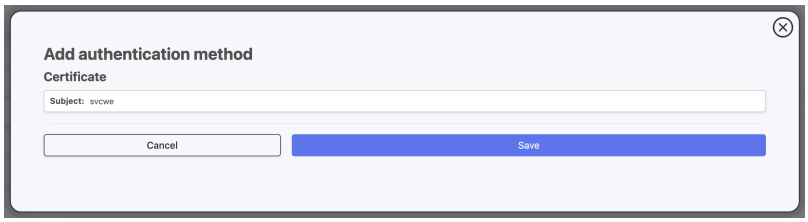


3. Click *Save*.
4. Go to *Management* > *Users* and edit the user, for whom you want to set authentication method *Certificate*, or create a new user by selecting *Management* > *Users* and then clicking + *Add user*.
5. In the *Authentication* section select *Certificate* type from the *Add authentication 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*

24.8 Authentication

Fudo Enterprise offers a wide range of authentication methods for user verification against the target server. These include:

- External Authentication: *CERB*, *RADIUS*, *LDAP*, *Active Directory*
- Other Authentication Methods: *OATH*, *SMS*, *DUO*, *OpenID Connect*, *SSO*, *Kerberos*

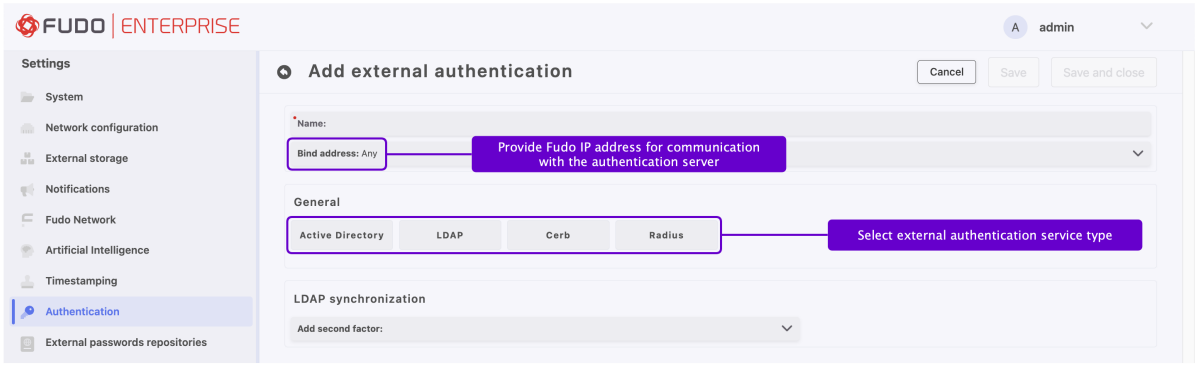
24.8.1 External authentication server definition

To add an external Active Directory, LDAP, Cerb, or Radius 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* 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 *General* section, elect authentication service type: `Active Directory`, `LDAP`, `CERB`, or `Radius`.



7. Provide configuration parameters depending on selected external authentication system type.
8. Click *Save*.

Field Descriptions and Configuration Based on Chosen Method

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 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.
Secret	Secret used to establish server connection to modify a user password on the Active Directory server.
Add second factor	Additional verification step with authentication methods `OATH`, `SMS` or `DUO`.

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.

LDAP

Parameter	Description
Host	Server's 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.
TLS enabled	This option is required to be checked for the domain users who change their passwords in the 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`.

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`.

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}`.
  - For **Cerb**, the `MS-CHAP-Domain` field is set to the value from the *AD domain*, and the `User-Name` field contains only `{name}`.
- If the *AD domain* is not populated, the `User-Name` field in the `Access-Request` packet for both methods contains only the username: `{name}`.

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.
Add second factor	Additional verification step with authentication methods `OATH, SMS` or `DUO`.

Note:

- Please note that when configuring **Radius** authentication within Fudo Enterprise, only the **Password Authentication Protocol (PAP)** is supported.
- Make sure to read the note for the **Cerb** method as well.

Warning: When additional authentication method (`OATH`, `SMS` or `DUO`) is selected as a *Second factor* for synchronization with *External authentication server* (AD / LDAP / CERB / RADIUS), it won't be enough to just select one of the *External authentication server source* within the User definition. The additionally selected authentication method should be configured within the User definition as a primary authentication method. Then users' authentication methods will be automatically synchronized according to *External authentication server* settings.

Related topics:

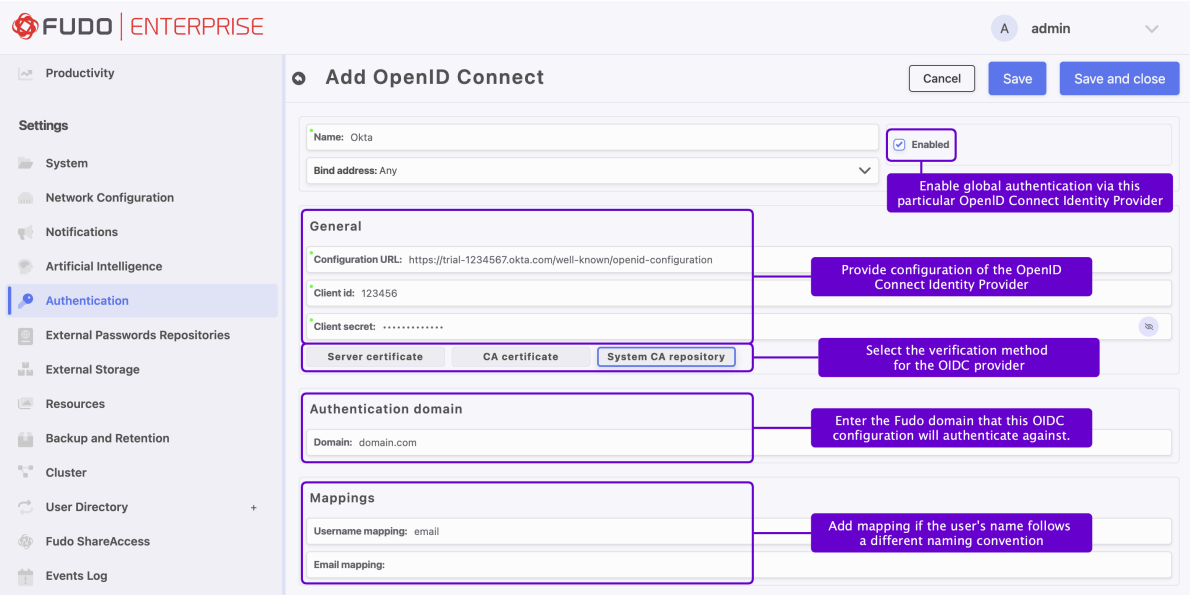
- *User authentication methods and modes*
- *OpenID Connect authentication definition with Microsoft Entra (Azure)*
- *System overview*
- *Integration with CERB server*

24.8.2 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. Example of *Configuration URL* for Google: `https://accounts.google.com/.well-known/openid-configuration`.

---

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.

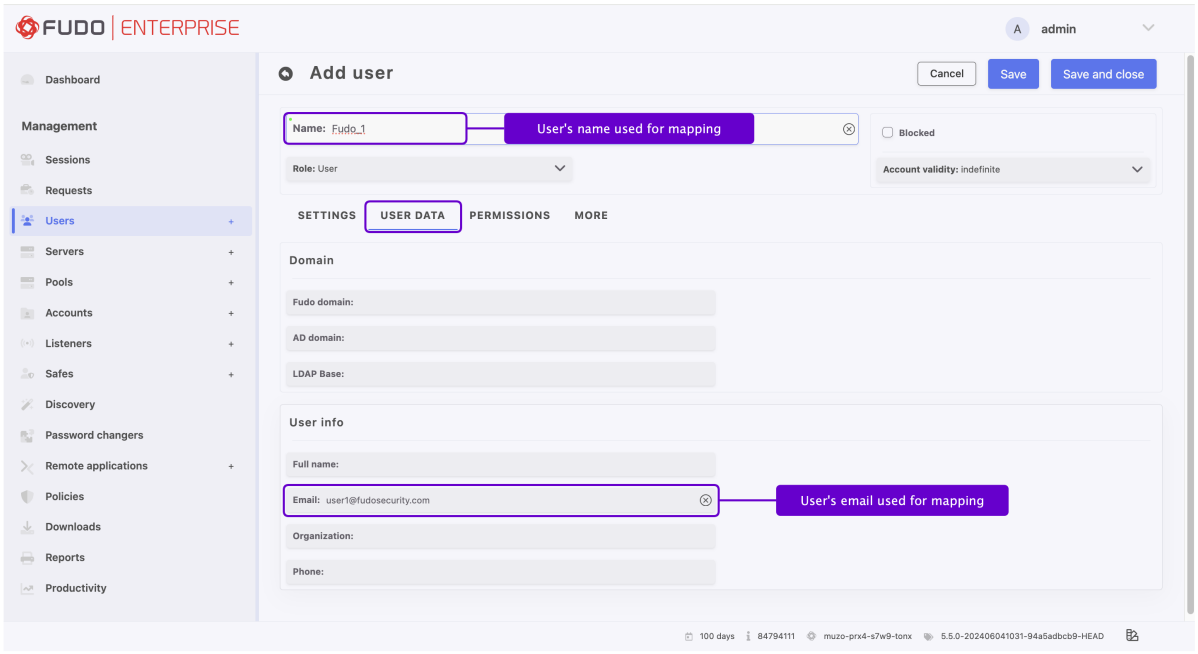
Note: Use this field if you manage multiple domains or synchronize users from different LDAP/AD sources to avoid conflicts with identical user IDs. The domain is optional.

---

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. Click *Save*.

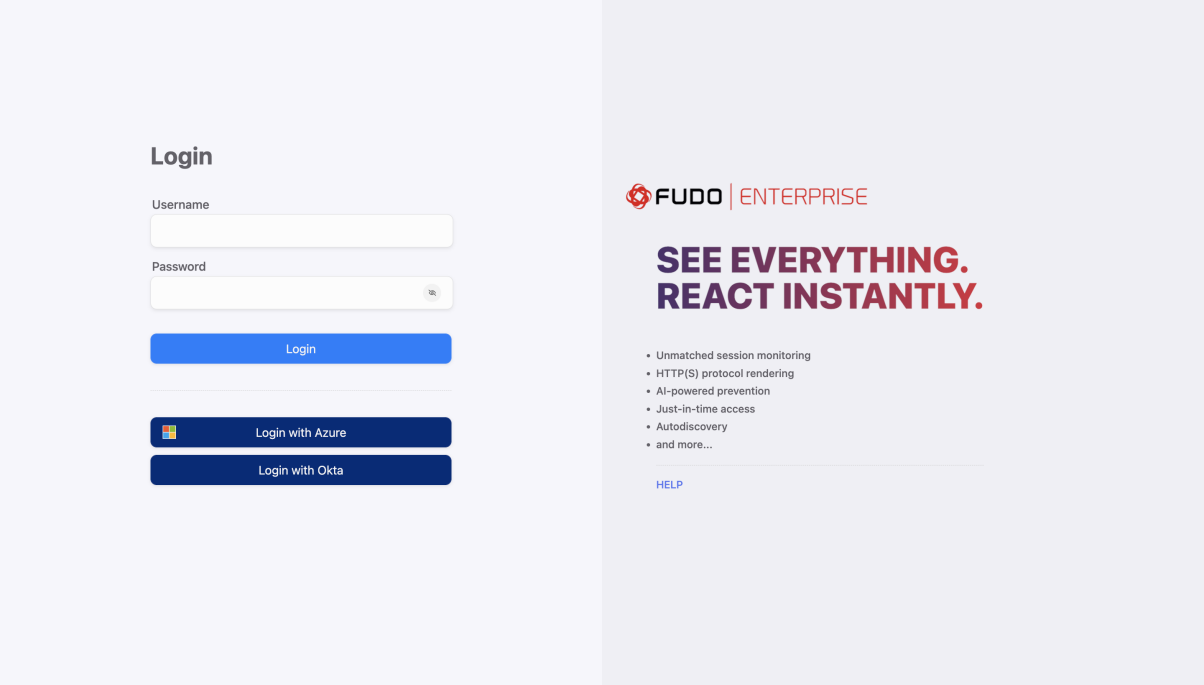
Note: The **algorithm to determine the user's identity** is following:

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 from the matching domain are considered. If it is not defined, users 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.

13. Log in using the defined authentication method:



Related topics:

- *User authentication methods and modes*
- *OpenID Connect authentication definition with Microsoft Entra (Azure)*
- *System overview*
- *Integration with CERB server*

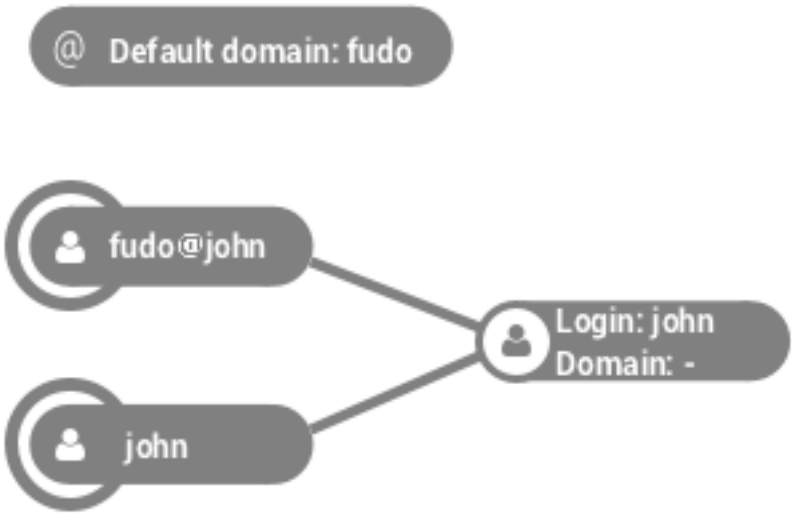
24.8.3 Global authentication settings

In the *Global* tab, you can configure the default domain, password complexity, and a range of authentication methods, including OATH, SMS, DUO, SSO, and Kerberos.

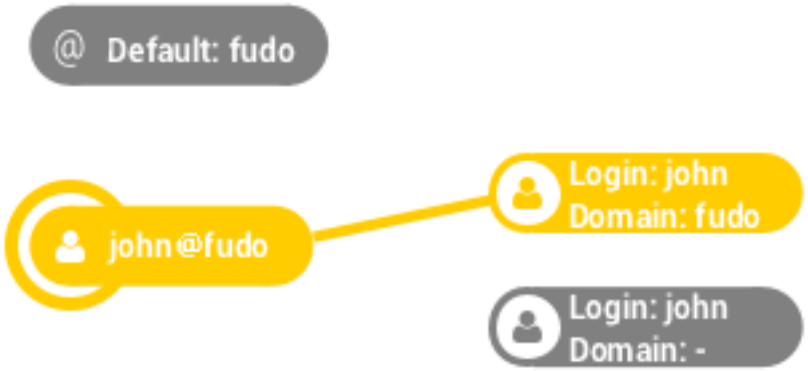
24.8.3.1 Default domain

Note: Please remember that the functionality of the *Default Domain* option is closely related to the *Fudo Domain* settings in the *user specification*.

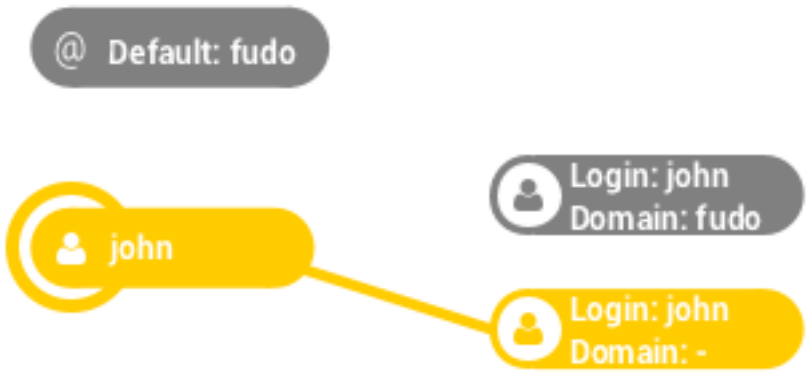
- In case the default domain is specified and the user does not have a *Fudo domain* defined, when logging in to Fudo Enterprise, the user can either include the domain (e.g. `john@domain`) or leave it out (e.g. `john`).



- 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.



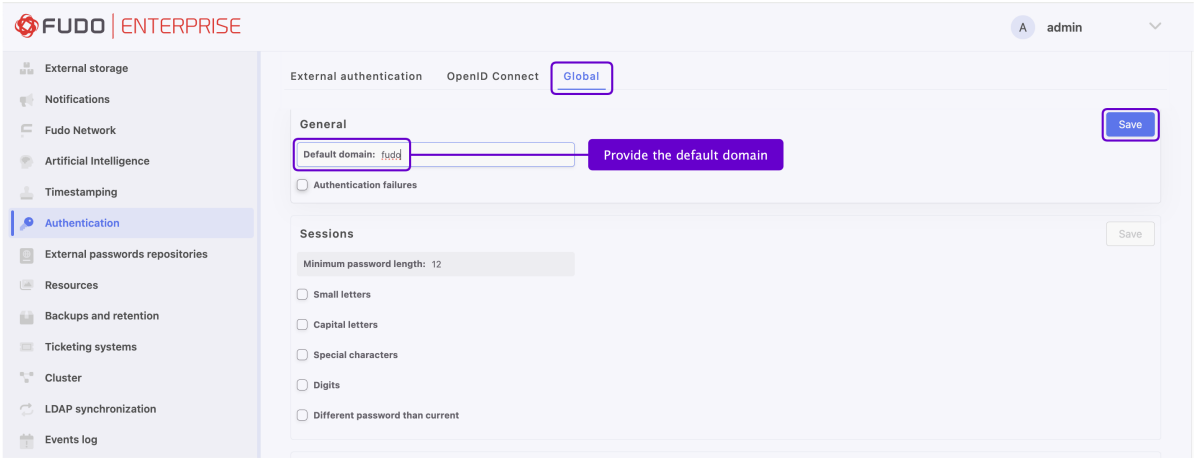
– In case the user does not provide the domain during login, Fudo Enterprise will match the user that does not have the domain explicitly specified.



– 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:

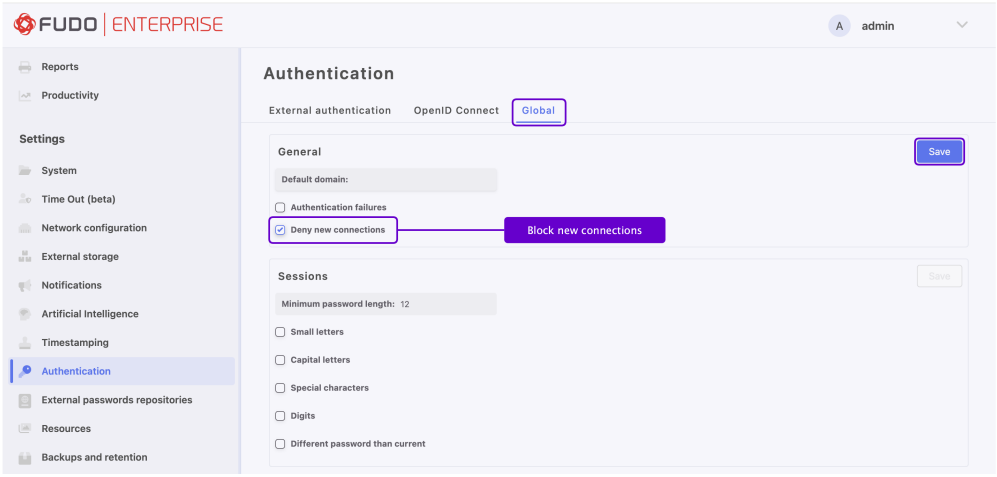
- *Creating a user*
- *Users Synchronization - User Directory*

24.8.3.2 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:

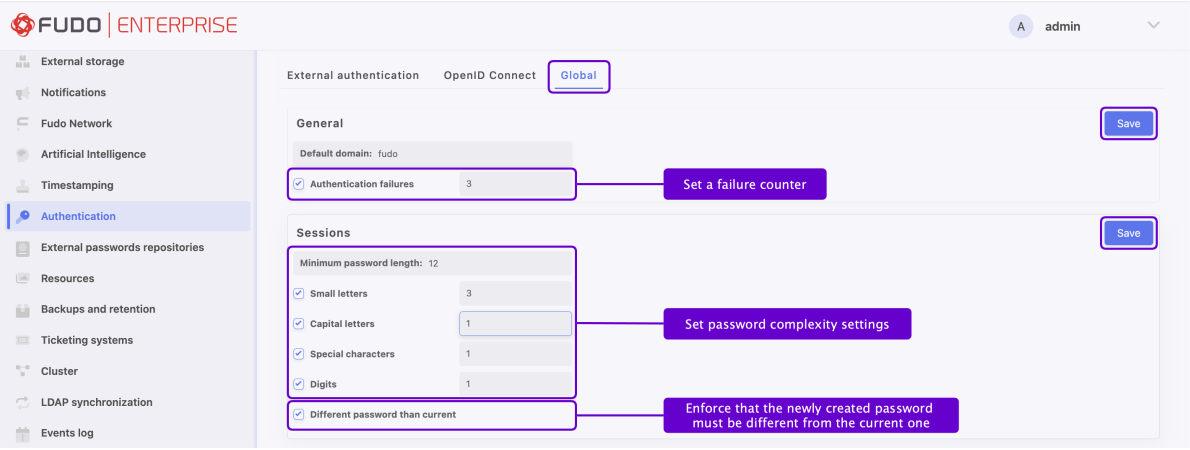
- *Network Interfaces Configuration*

24.8.3.3 Password complexity

Fudo Enterprise enables the definition of static password complexity, allowing you to enforce passwords that meet your internal regulations.

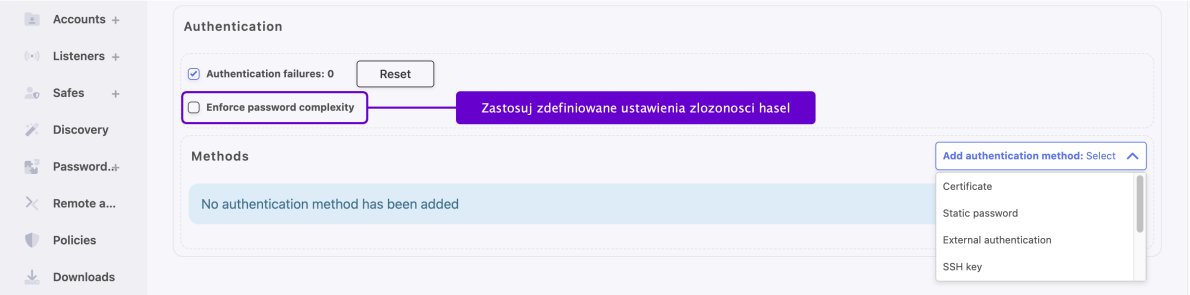
Defining password complexity

1. Select *Settings* > *Authentication*.
2. Go to *Global* tab, and select *Authentication failures* to set a counter of the login failures.
3. Go to *Sessions* 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 *Management* > *Users*, edit desired user and select the *Enforce static password complexity* option in the *Authentication* section.



Enabling password complexity will trigger password change for users with the *Enforce static password 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*.

Related topics:

- *Creating a user*
- *Users Synchronization - User Directory*

24.8.3.4 OATH authentication definition

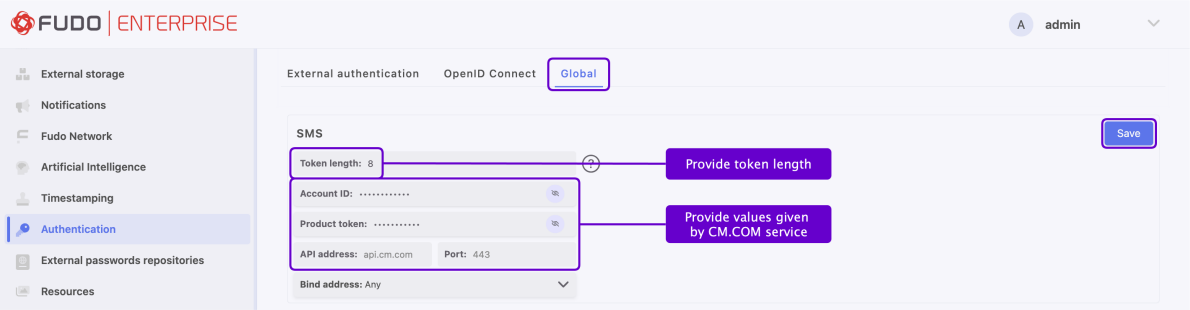
Refer to the *Two-factor OATH authentication with Google Authenticator* page.

Related topics:

- *User authentication methods and modes*
- *OpenID Connect authentication definition with Microsoft Entra (Azure)*
- *System overview*
- *Integration with CERB server*

24.8.3.5 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.

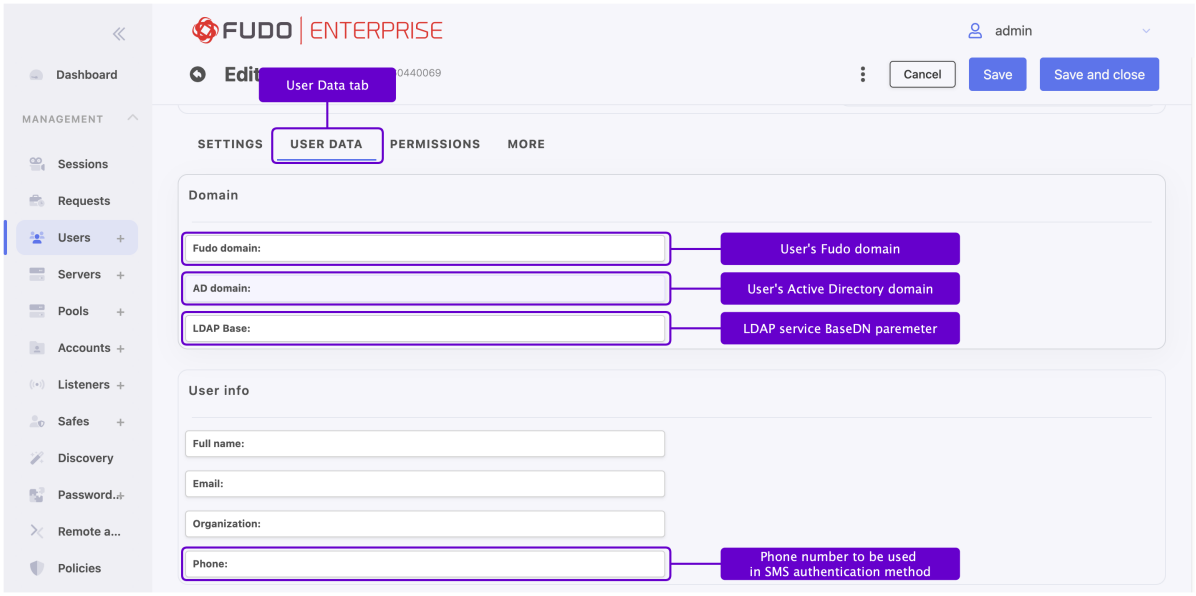
4. Input *Account ID*.
5. Input *Product token*.
6. Input *API address* and its *port*.

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.

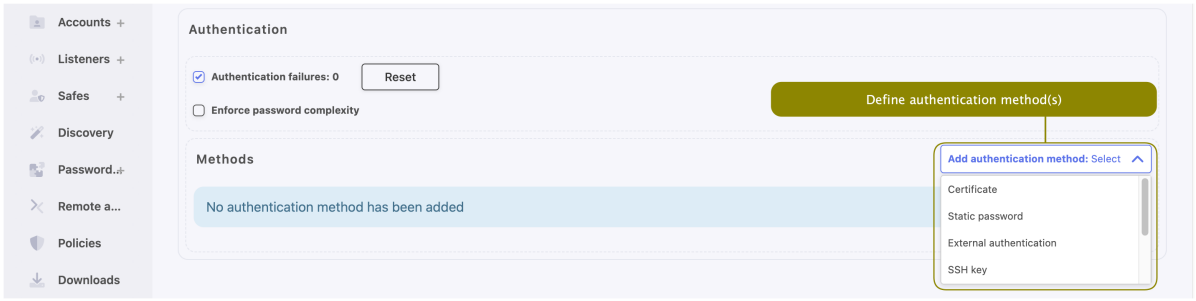
7. Select the *Bind address*.
8. Click *Save*.

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.



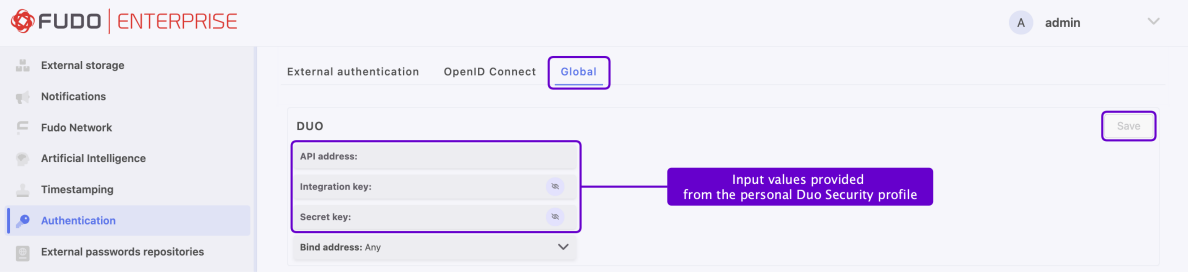
5. Choose `Static password` or `External authentication` (AD or LDAP) as a *First factor*.
6. Provide static password or external authentication source.
7. Select *Required password change on next login* option if needed.
8. Click *Save*.
9. Log in to the Access Gateway with SMS code.

Related topics:

- *User authentication methods and modes*
- *OpenID Connect authentication definition with Microsoft Entra (Azure)*
- *System overview*
- *Integration with CERB server*

24.8.3.6 DUO authentication definition

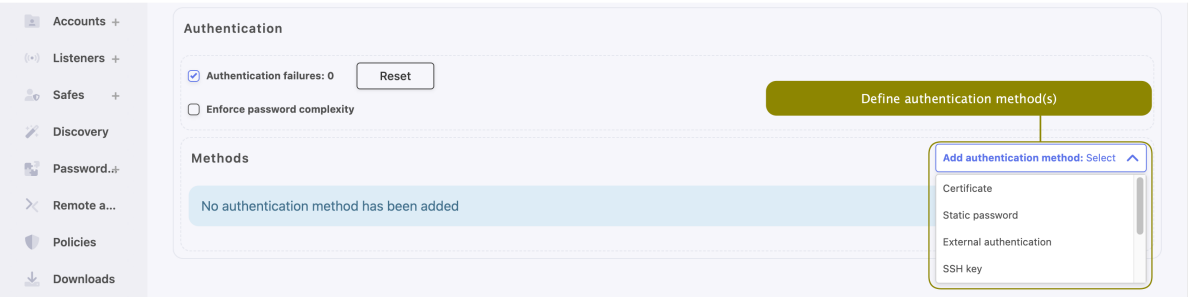
1. Download and install Duo Mobile phone application.
2. Sign up for a personal account on Duo Security.
3. Select *Settings* > *Authentication* > *Global* tab.
4. Go to *DUO* section.



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 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*

24.8.3.7 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:

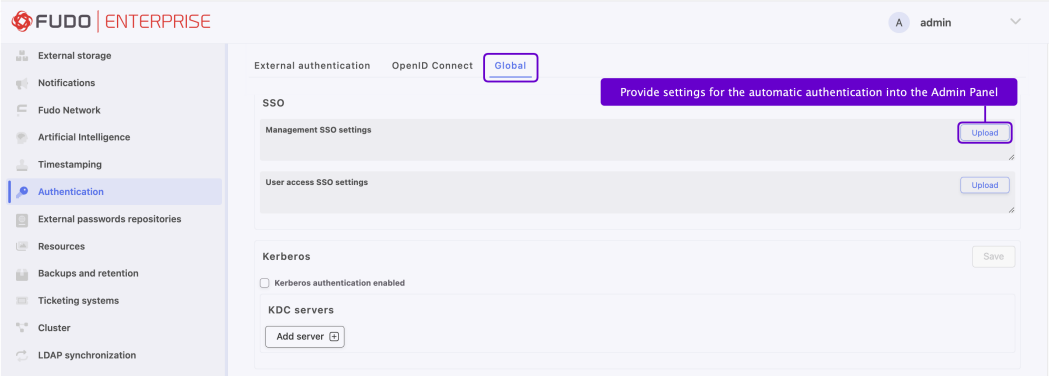
```
ktpass -princ HTTP/hostname.yourdomain.local@yourdomain.local -mapuser
netbios_domain_name\username -pass password       - ptype KRB5_NT_PRINCIPAL -out
hostname.yourdomain.local.keytab
```

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.

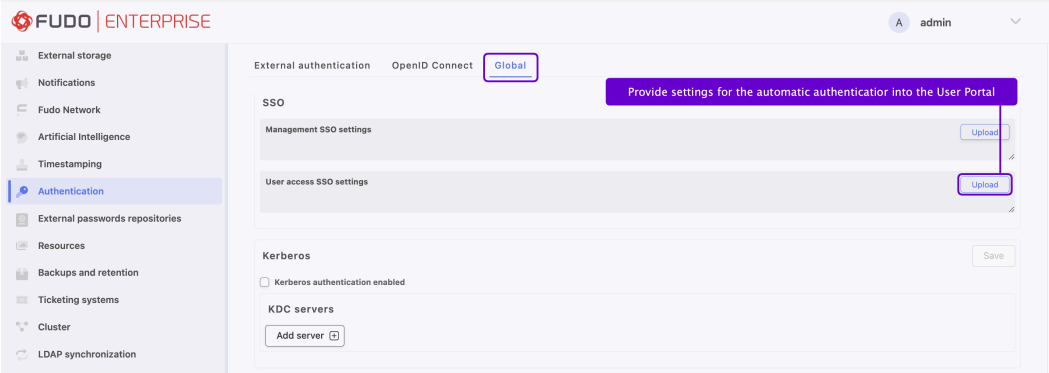


- Click *Save*.

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*

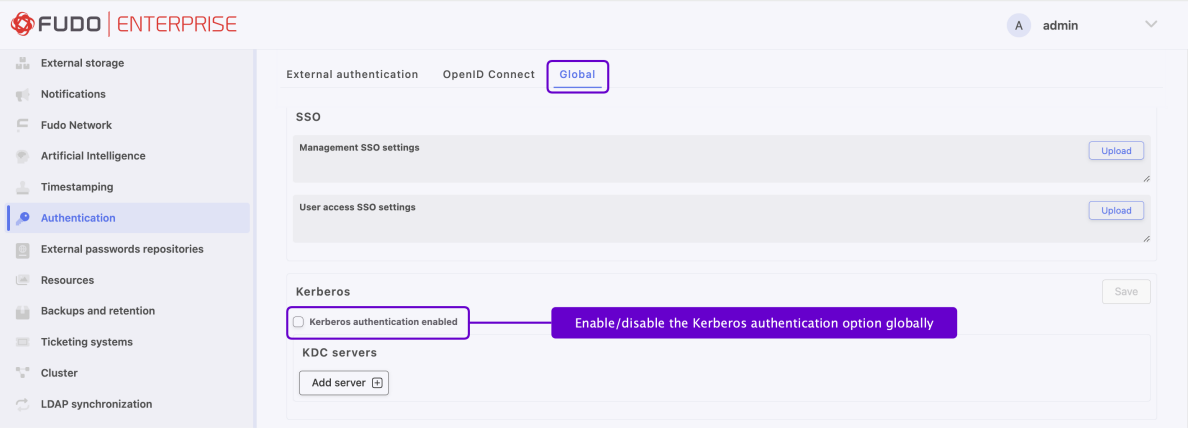
24.8.3.8 Kerberos authentication settings

Note:

- *Kerberos authentication* functionality is enabled by default.
- If enabled, Kerberos is used in RDP sessions authentication against the server and the Active Directory external authentication method.
- 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 utilized when a fallback to LDAP is required.

Disable Kerberos authentication

To disable the Kerberos authentication option globally, select *Settings* > *Authentication*, go to *Global* tab, and deselect *Kerberos authentication enabled* option in the Kerberos section.

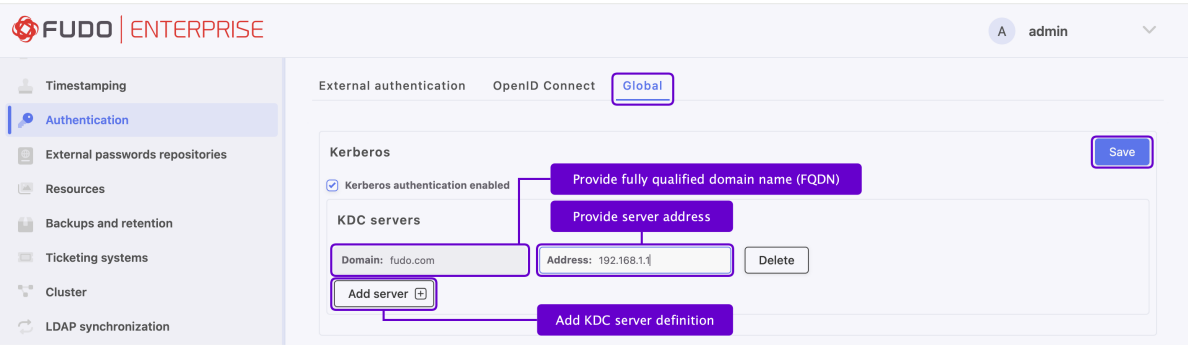


Add KDC Servers

Fudo Enterprise supports configuring Key Distribution Servers (KDC) and mapping domains to KDC servers.

To add a KCDC server:

1. Select *Settings* > *Authentication* > *Global* tab.
2. Go to *Kerberos* 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*
- *OpenID Connect authentication definition with Microsoft Entra (Azure)*
- *System overview*

- *Integration with CERB server*

24.9 External passwords repositories

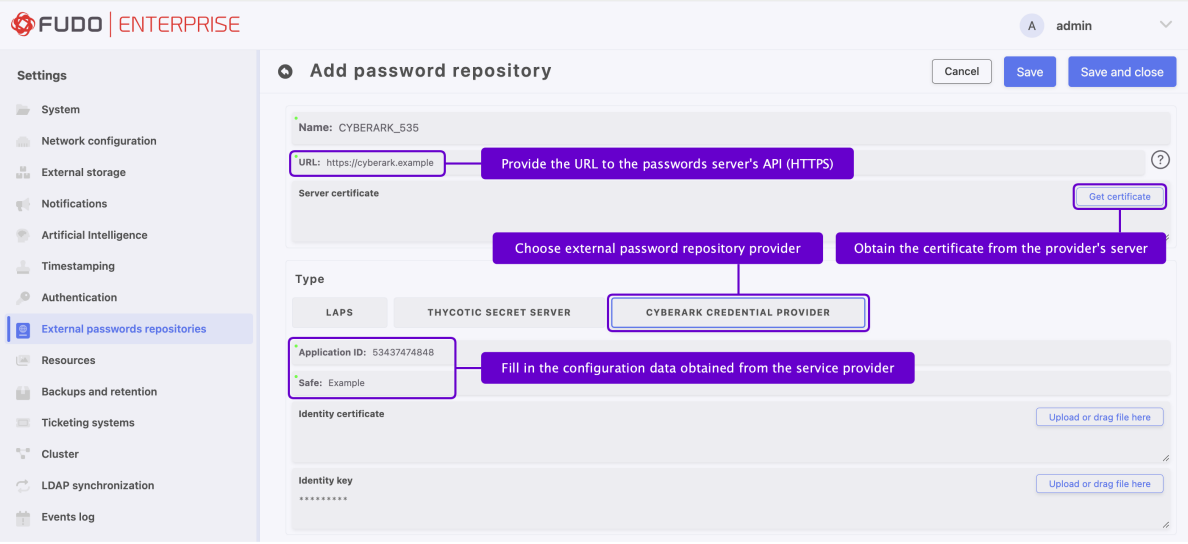
Fudo Enterprise supports external passwords repositories for managing passwords to monitored servers.

24.9.1 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 SSL certificate, or click the *Get certificate* button to obtain it from the provider's server.

Warning: If the HTTPS protocol is used without providing an SSL Certificate, the SSL connection will not undergo verification and will be 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.

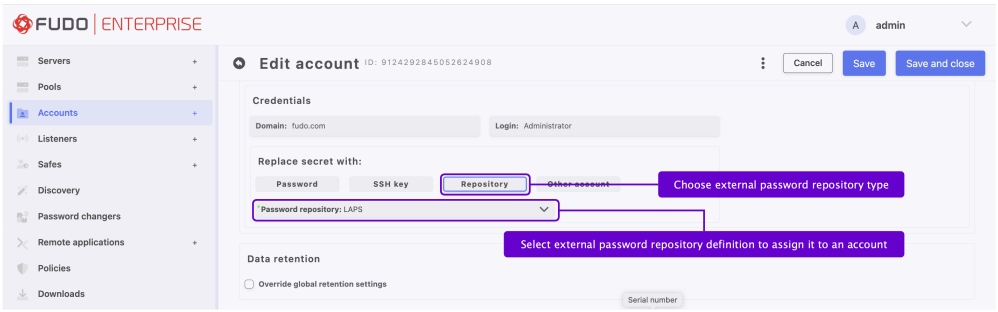
Note: The search for a given server/account is performed based on the following attributes from the *CyberArk Credential Provider*, which must be set up according to the rules below:

- `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*

24.9.2 Thycotic Secret Server

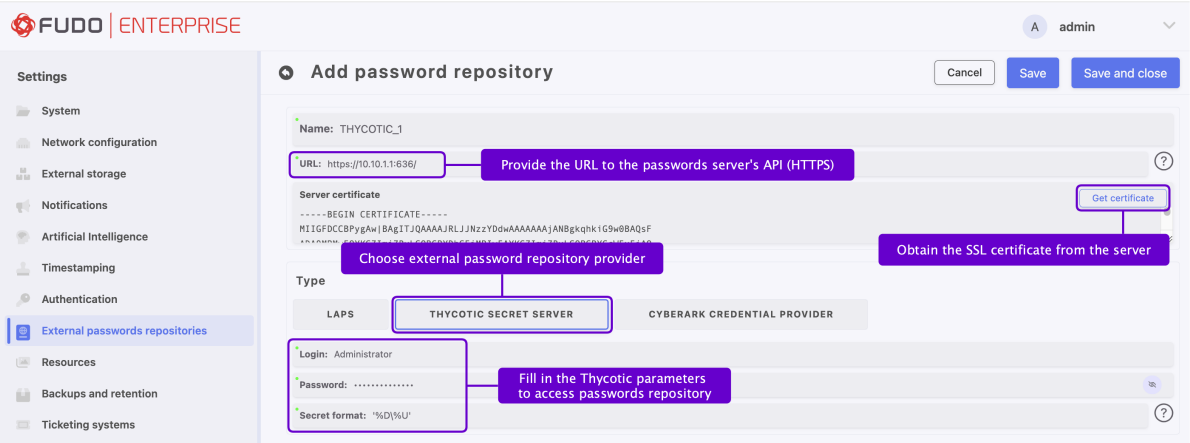
Adding a new passwords repository

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 SSL certificate, or click the *Get certificate* button to obtain it from the provider's server.

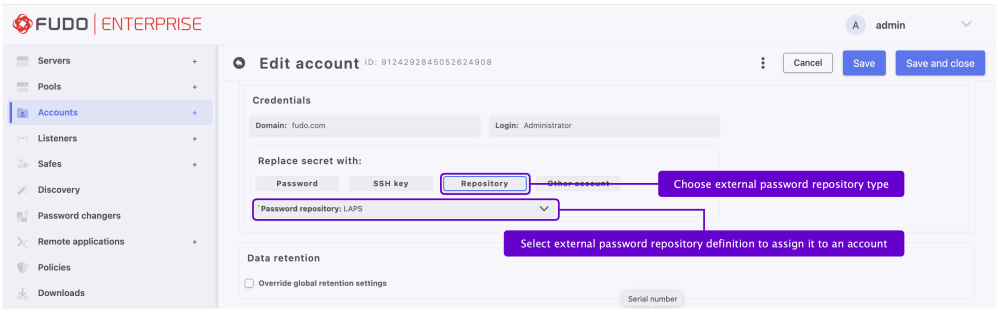


6. Select *THYCOTIC SECRET SERVER* button in the *Type* section.
7. Enter user login allowed to access passwords repository.
8. Provide user password in the *Password* field.
9. Define secret string format used for identifying objects on Thycotic Secret Server.

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*

24.9.3 Local Administrator Password Solutions (LAPS)

Note: Only the Legacy version of Microsoft LAPS is currently supported. 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 SSL connection to AD/LDAP server.

---

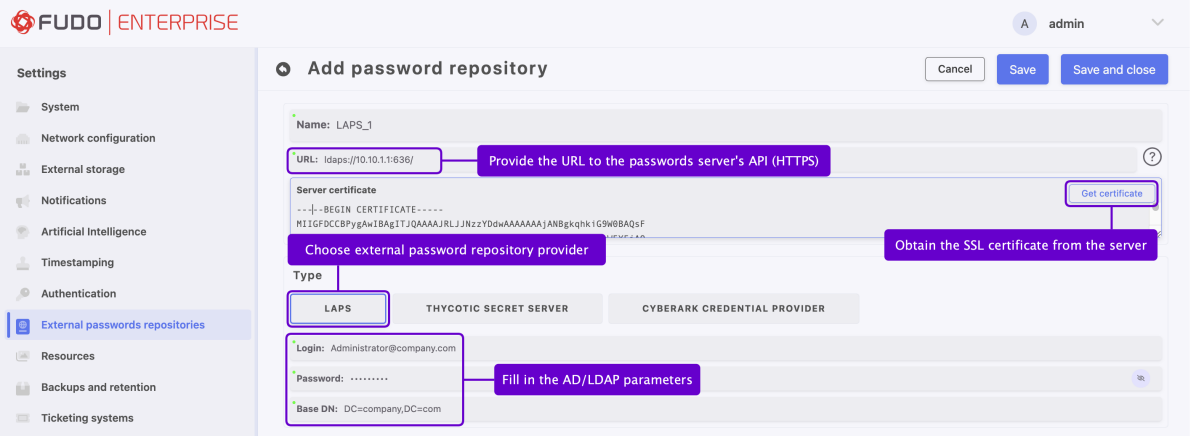
1. Select *Settings* > *External passwords repositories*.
2. Click *+ Add password repository*.

3. Specify object's name.
4. Provide the URL to the passwords server's API.

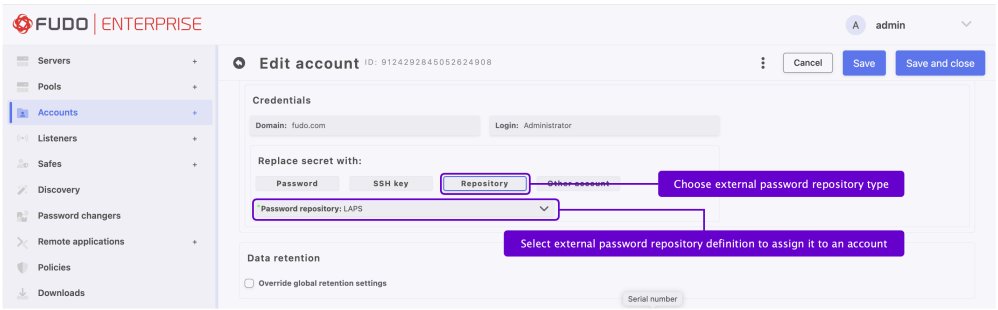
Note: Supported URL format is `ldaps://<server>[:<port>]/` for connection over SSL.

5. In the *Server certificate* field, provide the SSL certificate, or click the *Get certificate* button to obtain it from the provider's server.

Warning: If the LDAPS protocol is used without providing an SSL Certificate, the SSL connection will not undergo verification and will be 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*

Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

24.10 Resources

24.10.1 RDP/SSH/VNC login screen configuration

Fudo Enterprise enables customizing RDP, SSH and VNC login screen.



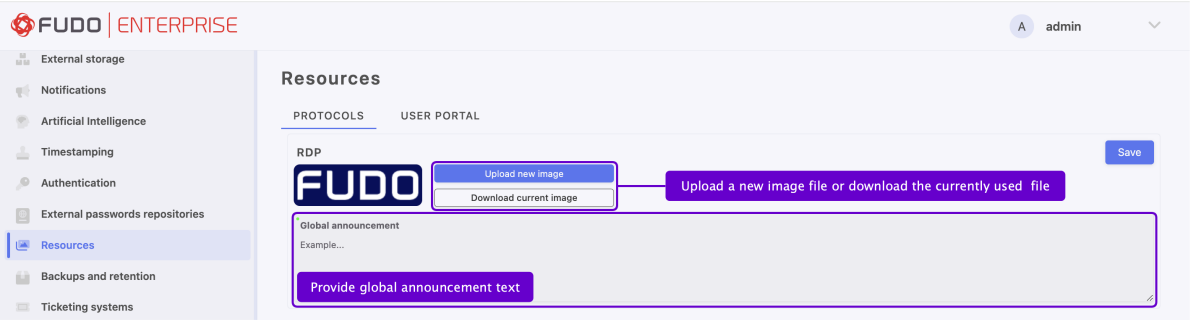
RDP login screen customization

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*.



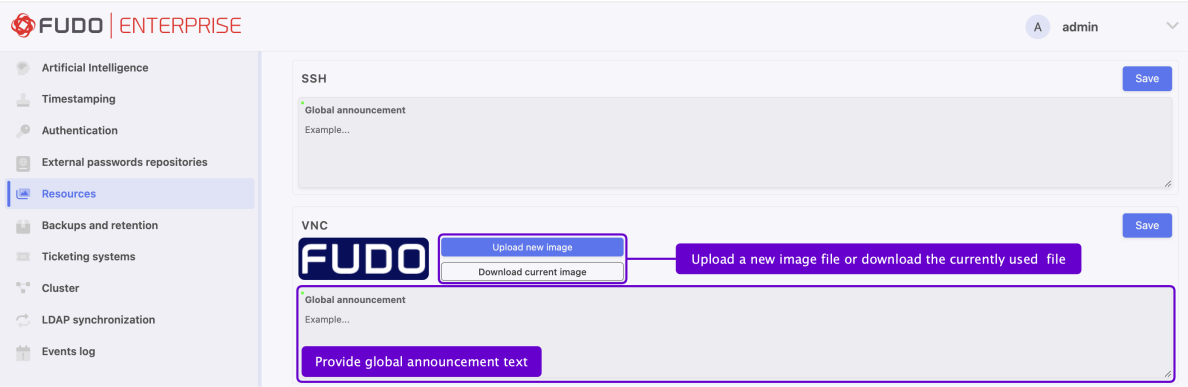
VNC login screen customization

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*.

Related topics:

- *Quickstart - RDP*

24.10.2 *User portal* configuration

24.10.2.1 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.

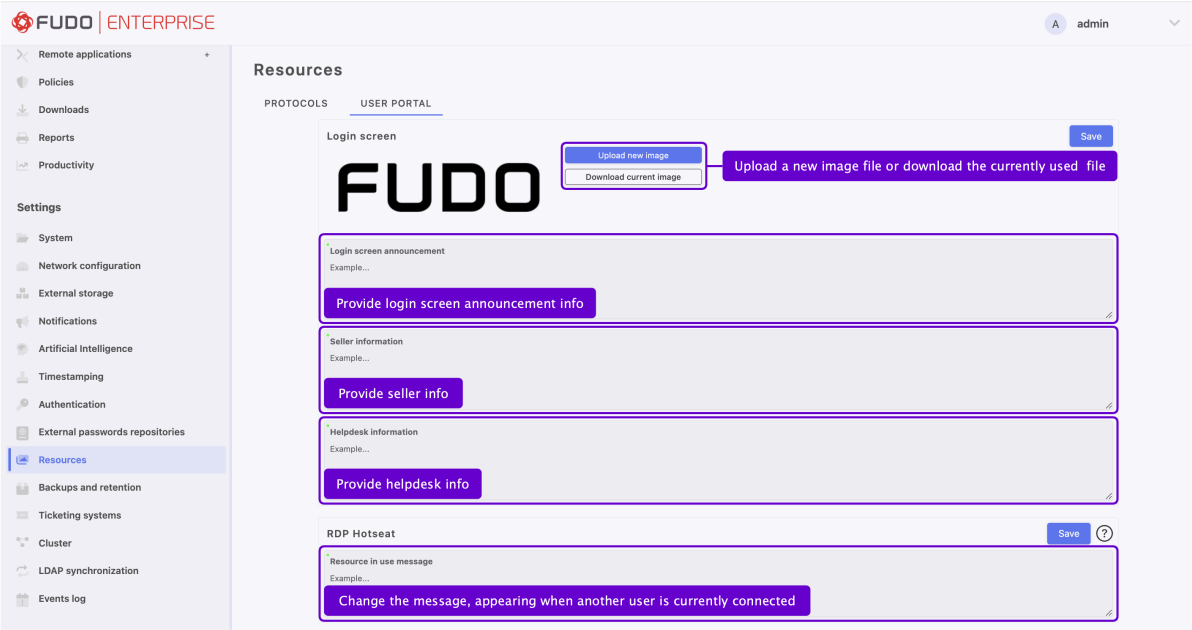
Note: Login screen announcement can be four lines, up to 120 characters.

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*.

24.10.2.2 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.

Note: Each user can customize their keyboard layout individually in the User Access Gateway.

Related topics:

- *User Access Gateway*

24.11 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.

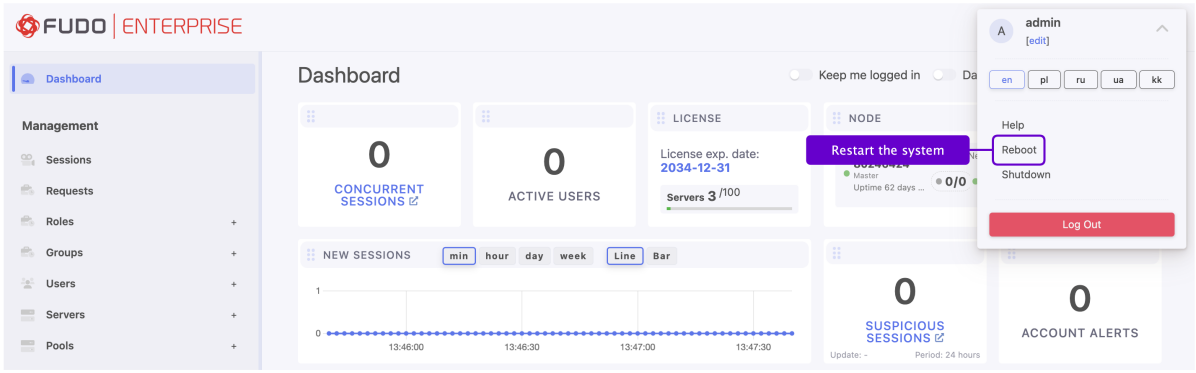
Warning: Restoring the system to the previous version will bring back the system's state prior the update. **Session data** and **configuration changes** in the current system revision will be lost. This includes the **password changers** activity. If any passwords were changed during the newer version's 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*.

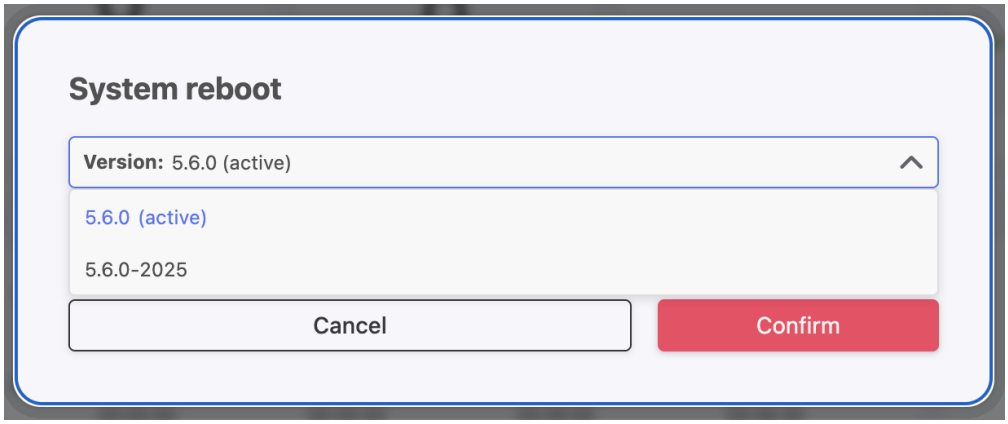
To restore the system to the previous revision, proceed as follows.

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:

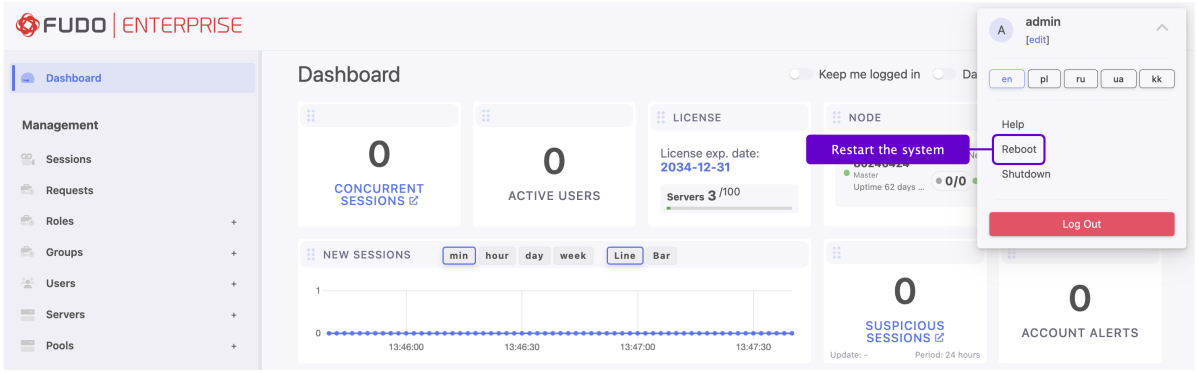
- *System initiation*
- *System update*

24.12 System Reboot

Note:

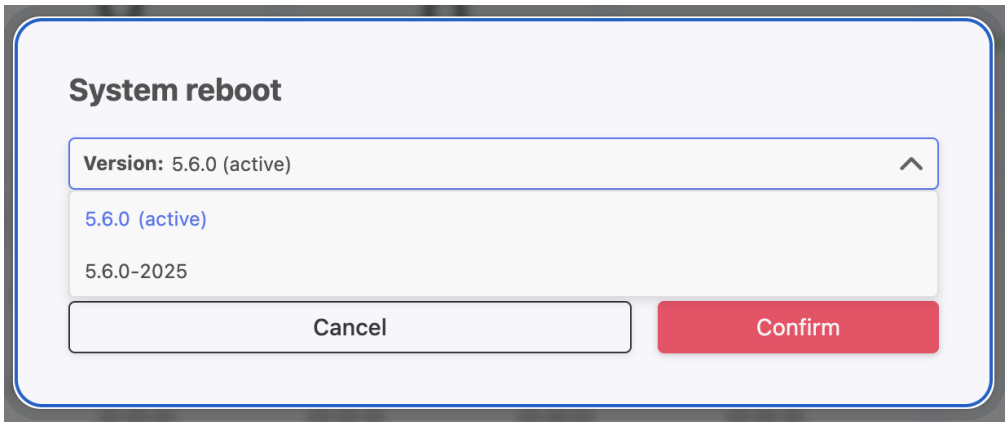
- System reboot requires USB flash drive with the encryption key connected to the device.
- Restarting the system will terminate all current users' connections.
- Use the *Deny new connections* option in *Settings* > *Authentication* > *Global* tab to prevent new connections from being established and 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 **password 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*

24.13 SNMP

Fudo Enterprise's status can be monitored over SNMPv3 protocol.

24.13.1 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.

24.13.2 Configuring SNMPv3 TRAP

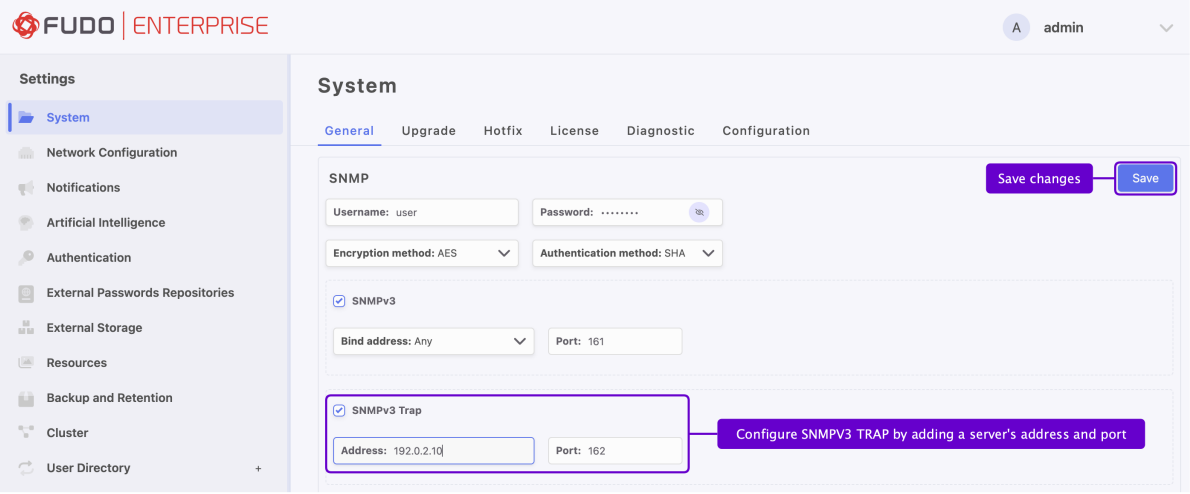
On *Policies* violation, Fudo is able to send a SNMPv3 TRAP, `fudoPolicyViolationNotification` with information containing during which session which user violated which policy. For more details check Fudo's MIB definition in the following section.

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.

24.13.3 SNMP MIBs

Fudo Enterprise supports following MIBs:

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790) - partly supported
- UCD-SNMP-MIB.

24.13.4 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

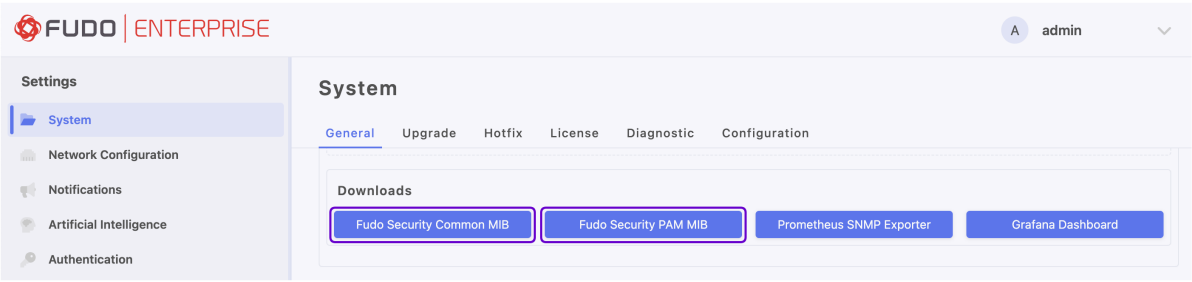
24.13.5 Fudo Enterprise specific SNMP extensions

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*

24.14 Backup and retention

24.14.1 Session data backup

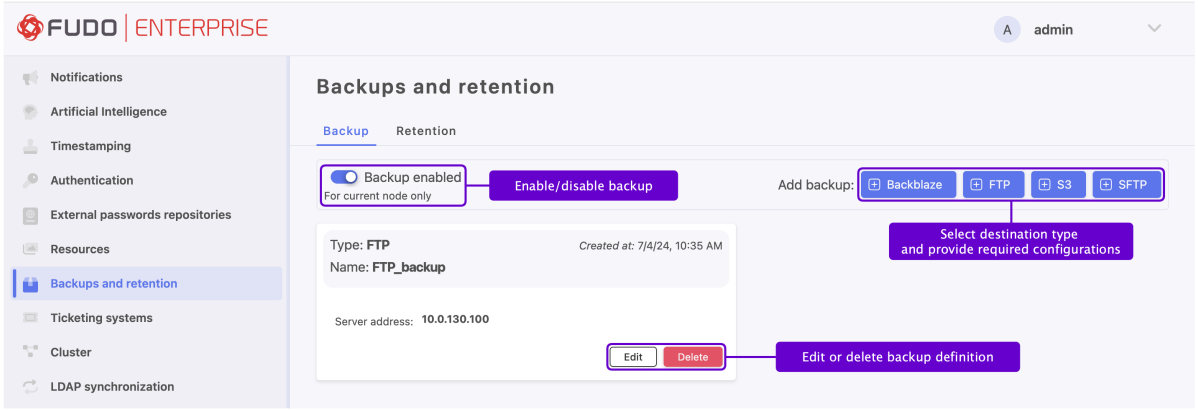
Warning: Session data backup contains confidential information.

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.

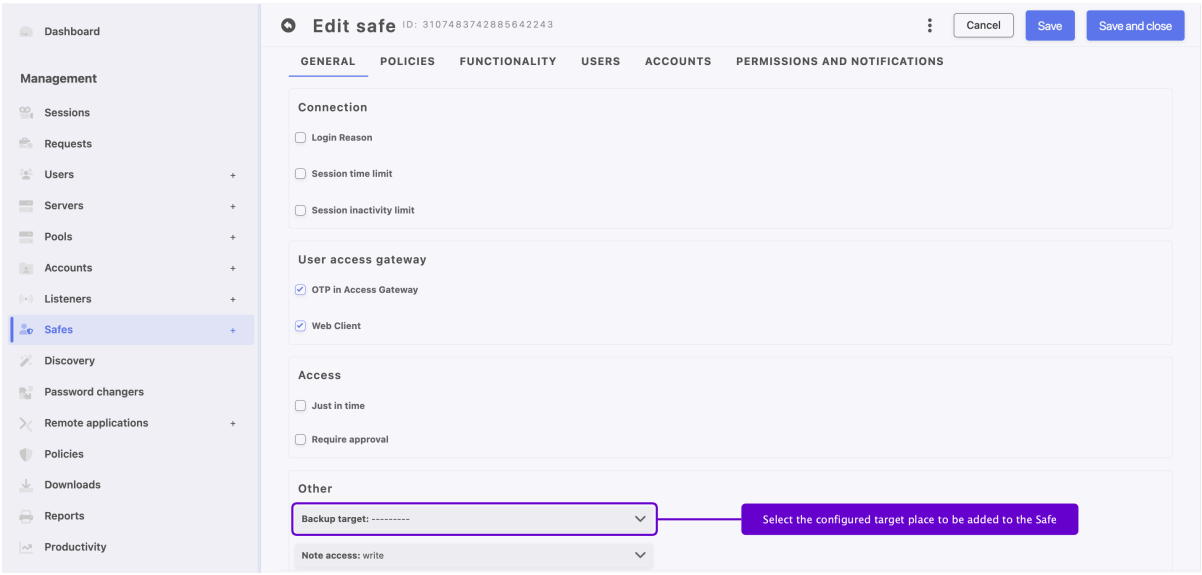
1. Select *Settings* > *Backup and retention*.
2. Select *Backup enabled* option. Please note that in case of the configured cluster, this option enables backup for the current node only.
3. In the *Add backup* field click desired backup type button in order to configure your future backup target place: *+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*.
- For **SFTP** type backup target provide: *Server address (IP address or host address), Username, Directory, User private key, Server public key,* and *Port* number.

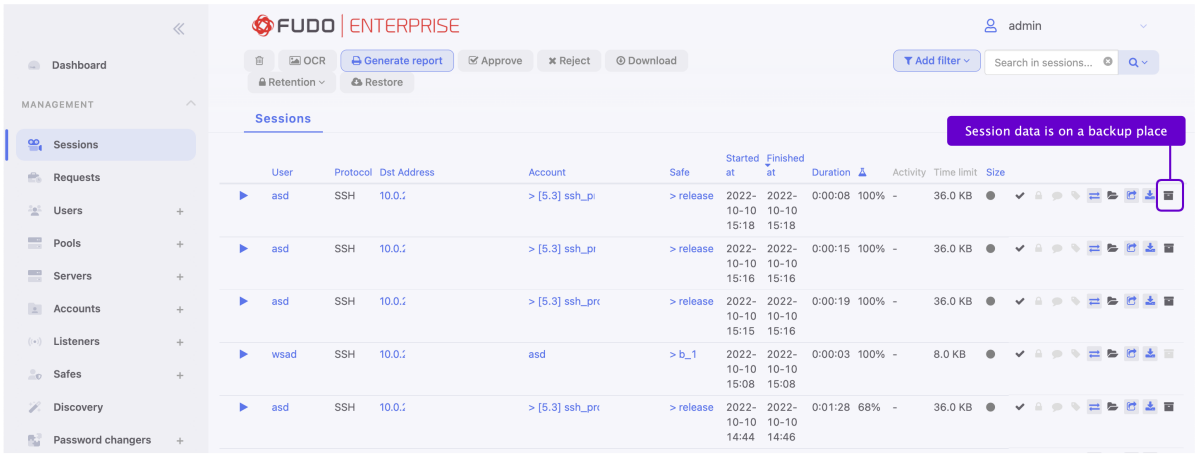


7. Click *Save*.

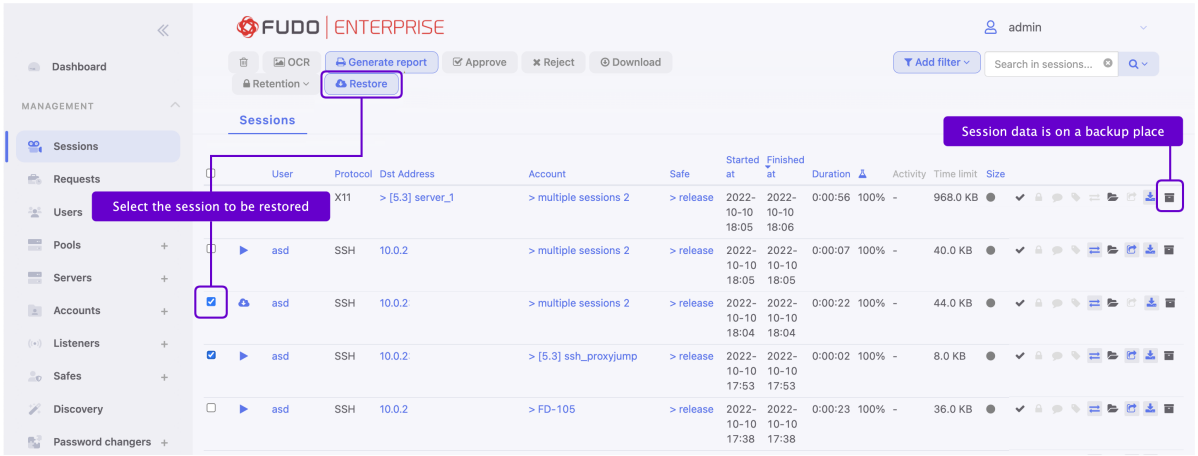
Now, the configured *Backup target* can be added to the Safe settings to enable automatic storing the sessions and safe data in the defined target place.



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*

24.14.2 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.

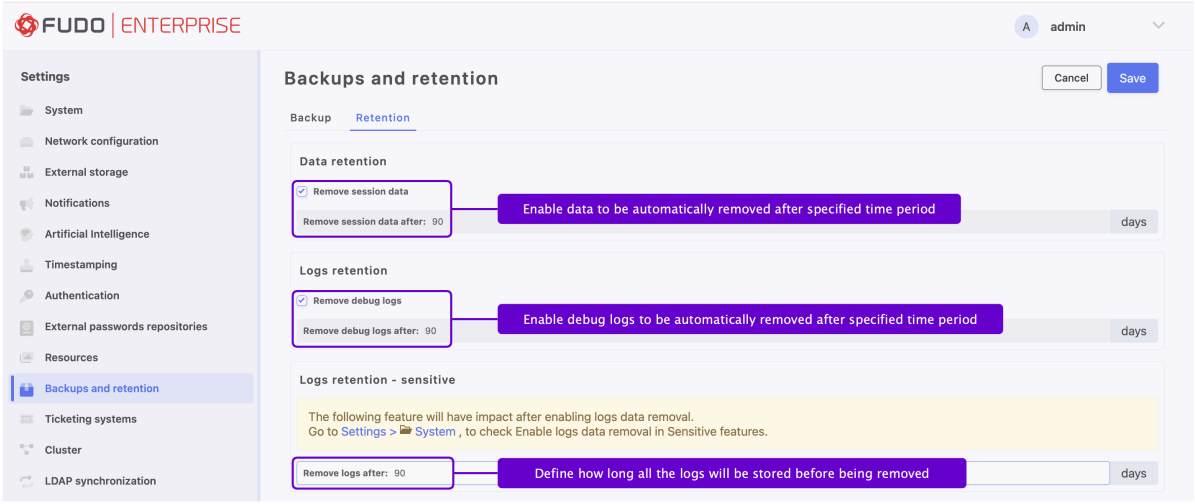
Note: Sessions which have been exported and the content is still available for download, will not be deleted automatically. These sessions must be either *deleted manually* or you must delete the exported material in the *Downloads* section for the retention mechanism to delete those session.

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.

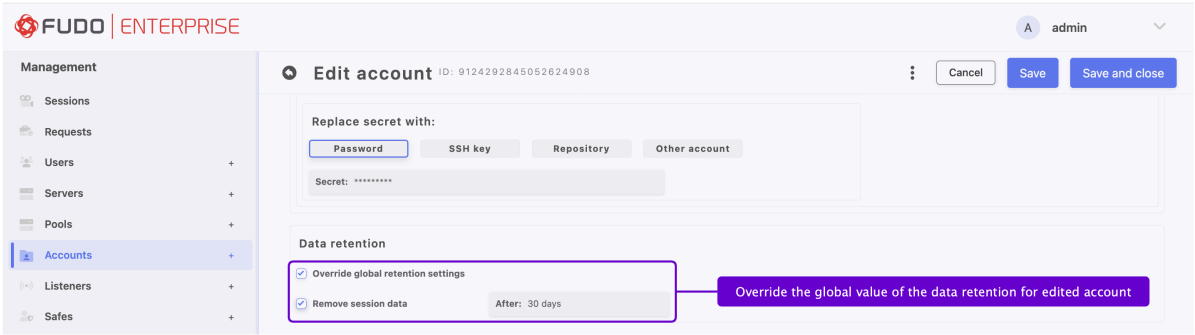


7. Click *Save*.

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*

24.15 External Storage

Fudo Enterprise supports storing session data on external storage devices attached through a Fibre Channel interface.

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.

24.15.1 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 desired *WWN* object and click the icon.

Note: Click the icon to refresh the list of available storage devices.

4. Click *Save* and proceed with enabling *session data retention*.

24.15.2 Expanding external storage device

After resizing the WWN object, it must be expanded in Fudo Enterprise in order to take advantage of the additional storage space.

Warning: The storage device cannot be down-sized after it has been expanded.

1. Select *Settings* > *External storage*.
2. In the section describing the *WWN* object click *Expand*.
3. Confirm expanding external storage.
4. Click *Save*.

Related topics:

- *Session data backup*

24.16 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.

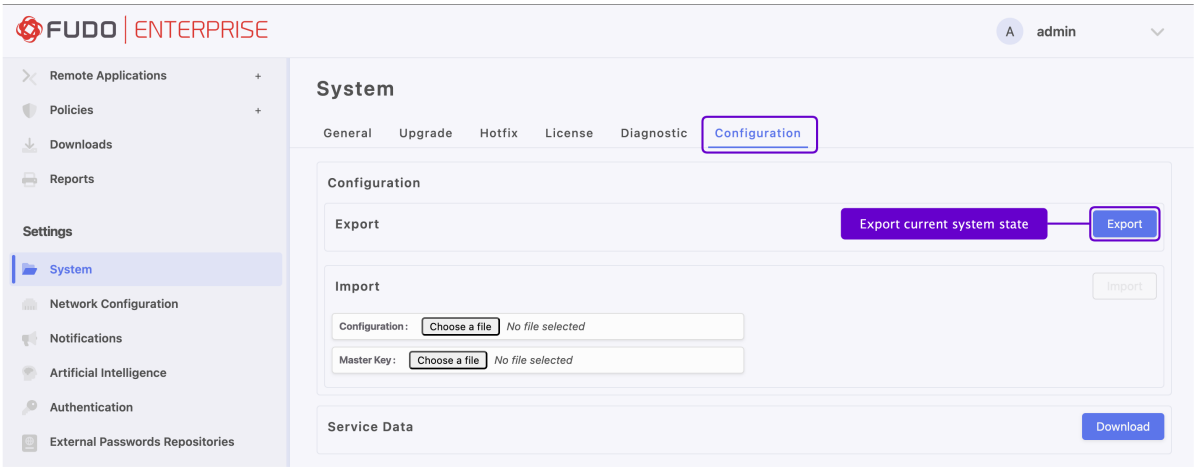
Note:

- 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.

24.16.1 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.



24.16.2 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.

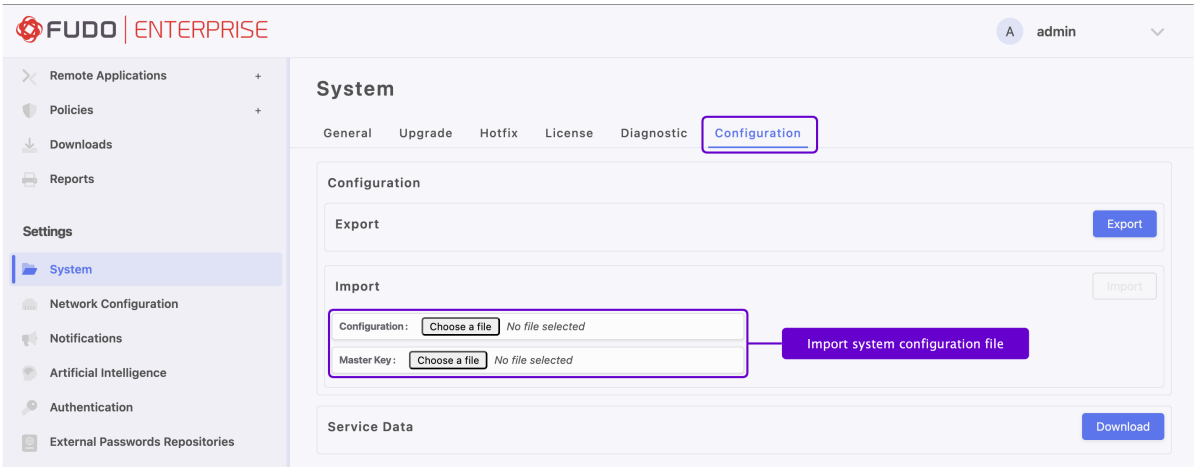
1. Find and decrypt the *Master key file* using *opessl*:

```
openssl smime -decrypt -in path/to/masterkey.pem -inkey privkey.pem -out
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 before it's

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*

24.17 Cluster configuration

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*.

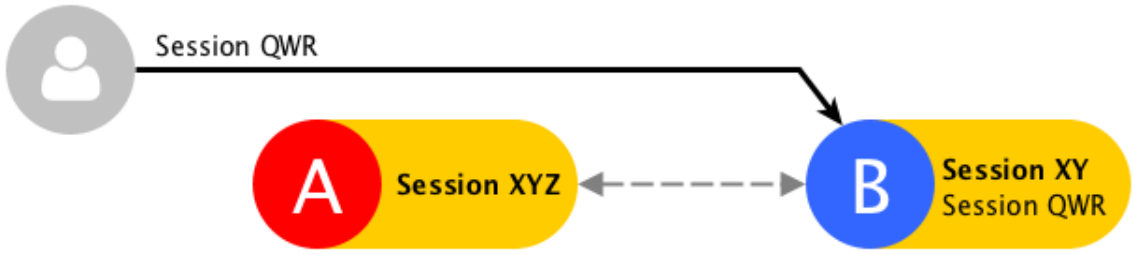
Current session data is replicated to other nodes while the connection is still ongoing.



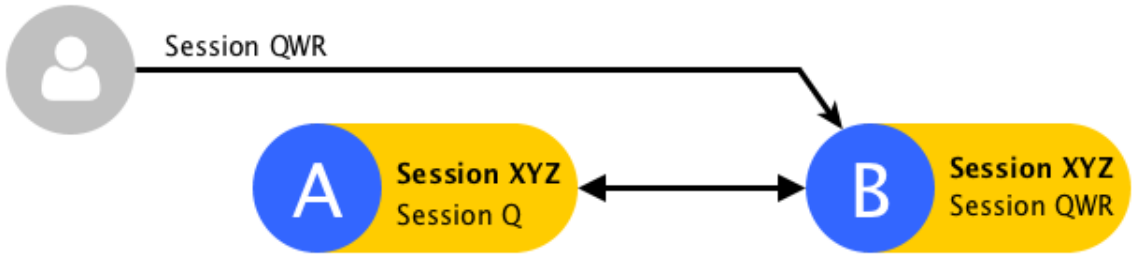
If the node that fails was recording sessions, those sessions will be terminated...



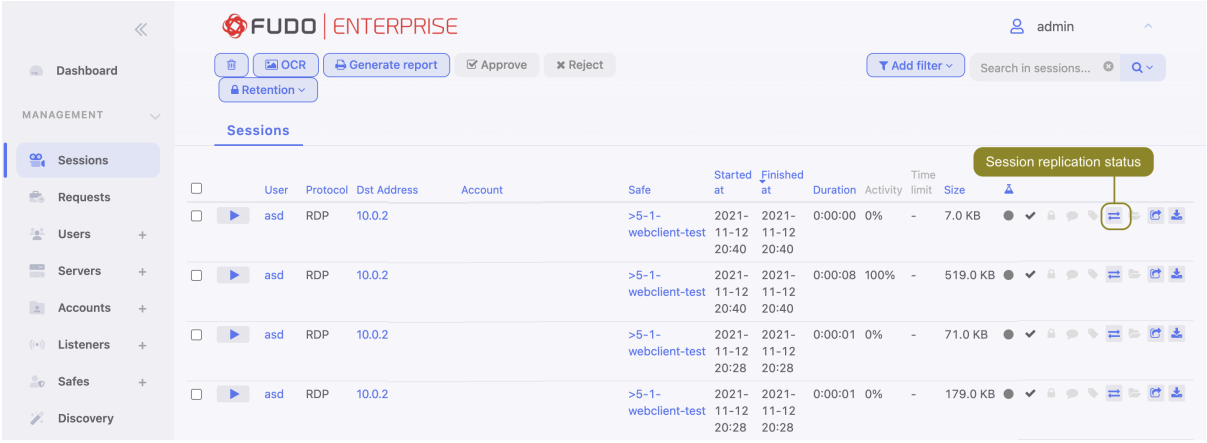
...and users will have to reconnect.

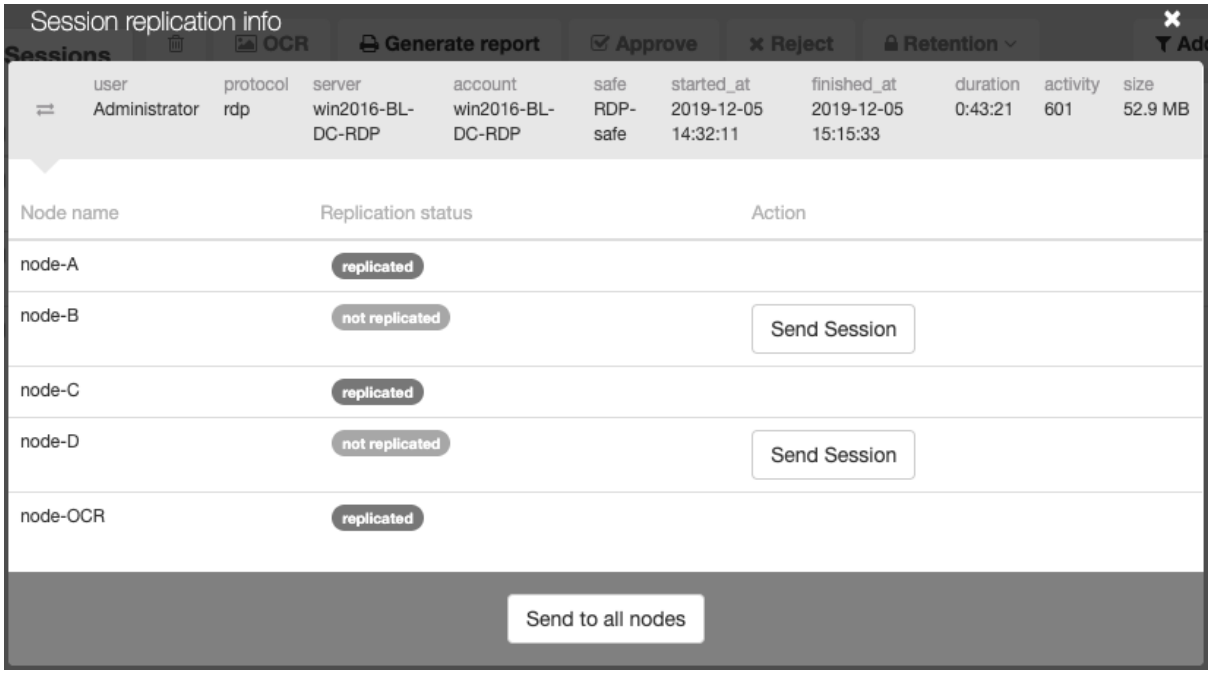


A part of the session data from the node that malfunctioned, which has synchronized, can be accessed on the other nodes, but the session will be fully accessible once the node becomes operational and session data is synchronized between cluster nodes.



Session replication status can be verified by clicking the ⇄ icon on the sessions list.



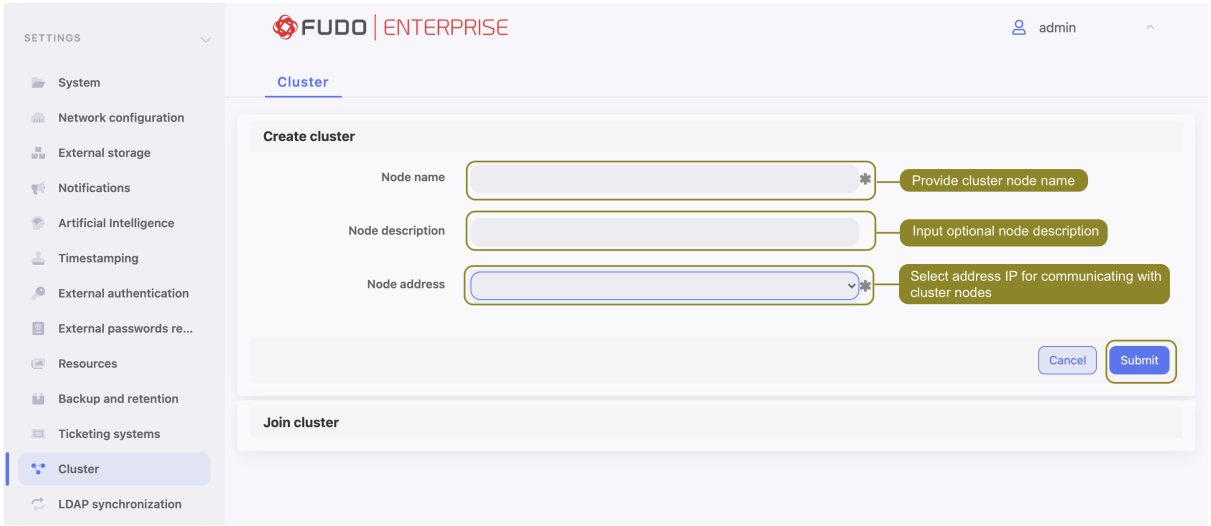


24.17.1 Initiating cluster

Warning: In cluster configuration all cluster nodes must have *NTP server configured*.

To initiate Fudo Enterprise cluster, proceed as follows.

1. Select *Settings* > *Cluster*.
2. Click *Create cluster*, to display cluster definition options.
3. Provide node name and description helping identify given object.
4. From the *Address* drop-down list, select IP address for communicating with other cluster nodes.



Note: Cluster communication address must have the *General* purpose assigned in the *network*

configuration.

5. Click *Submit*.

Note: Message concerning cluster key can be ignored when initiating cluster.

Related topics:

- *Adding cluster nodes*
- *Editing cluster nodes*
- *Deleting cluster nodes*
- *Redundancy groups*
- *Cluster configuration*

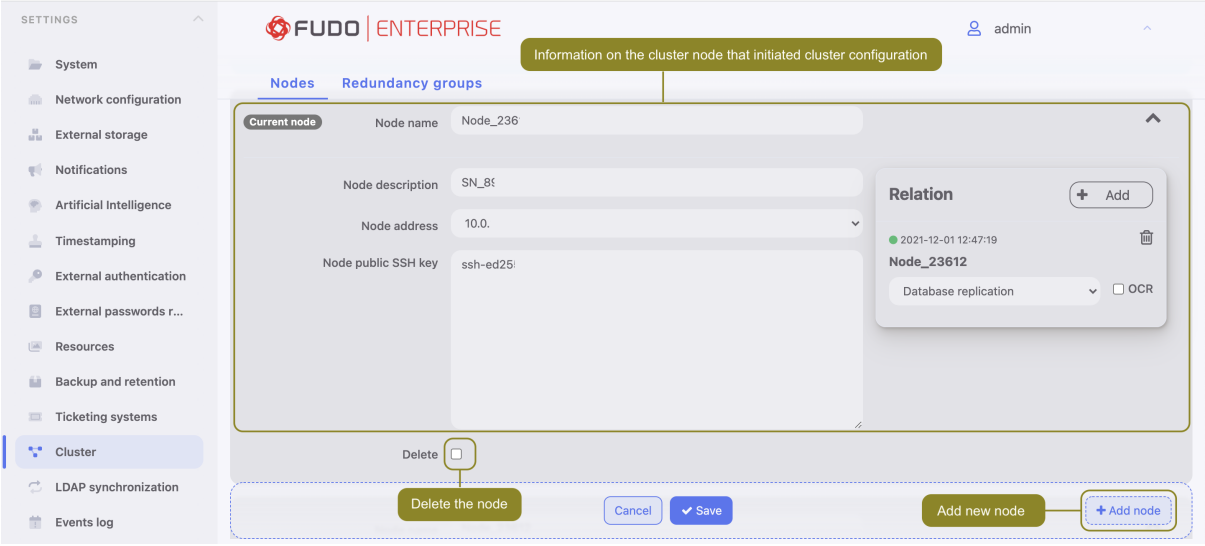
24.17.2 Adding cluster nodes

Warning:

- Session and configuration data (*servers*, *users*, *safes*, *accounts*, *listeners*, *external authentication servers*) of the joining node are deleted and initiated with data replicated from the cluster.
- 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.

To add a node to Fudo Enterprise cluster, proceed as follows.

1. Log in to the Fudo Enterprise administration panel where the cluster has been *initiated*.
2. Select *Settings* > *Cluster*.
3. Click *Add node* to display new node configuration parameters.

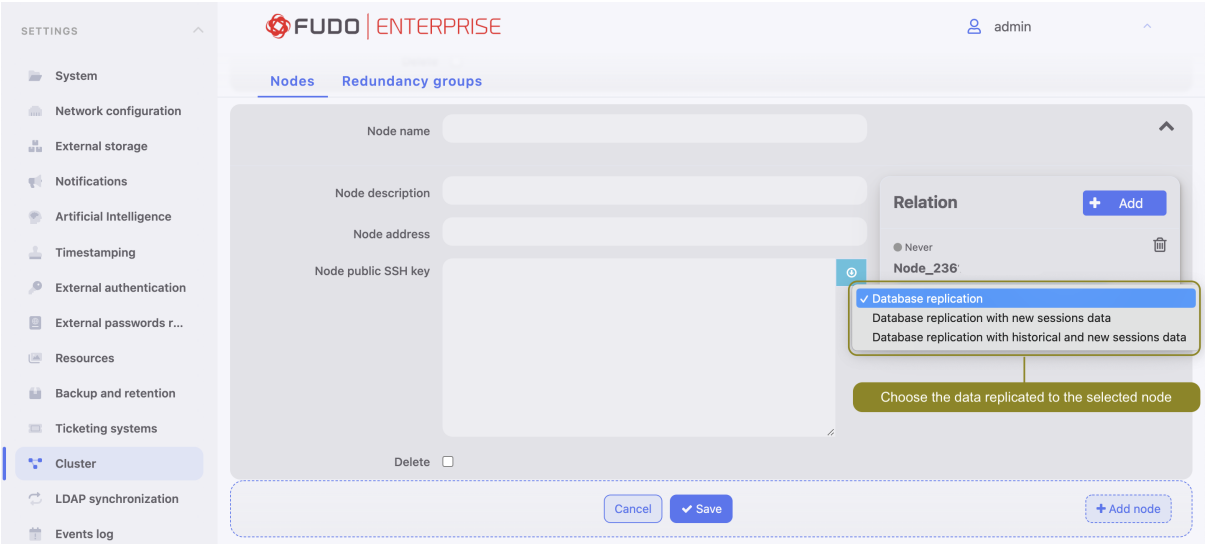


4. Provide node's name and optional description.
5. Provide node's IP address.

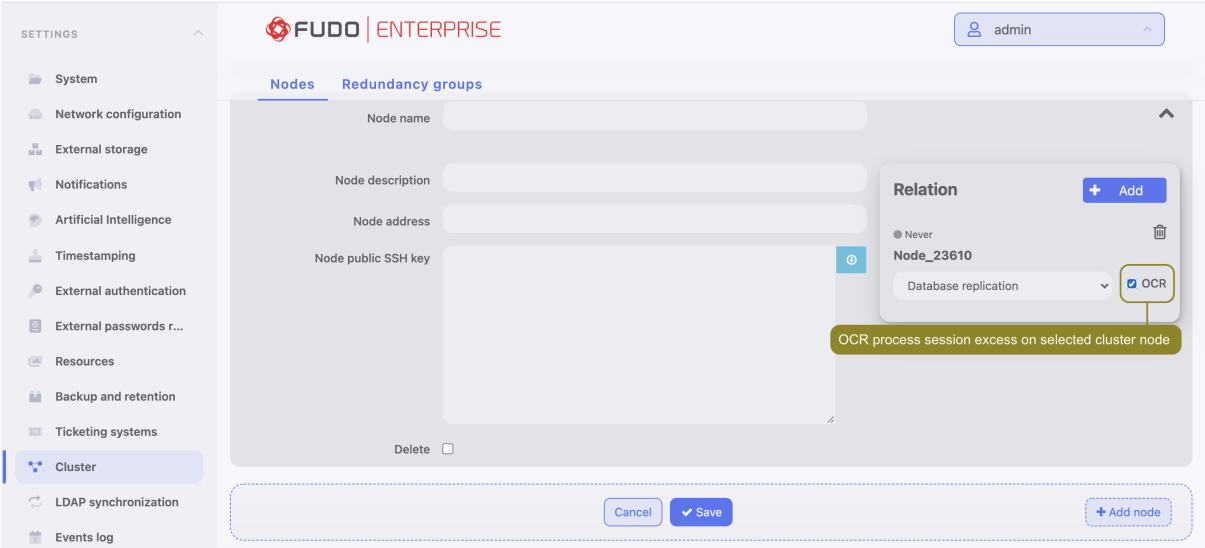
Note: Management option has to be enabled on given network interface. Refer to *Network settings: Network interfaces configuration* for details on configuring network interfaces.



6. Click  to download node's public SSH key.
7. In the *Relations* section, click *+ Add*.
8. Select the cluster node to which the data from the given node will be replicated.
9. Select which data will be replicated.

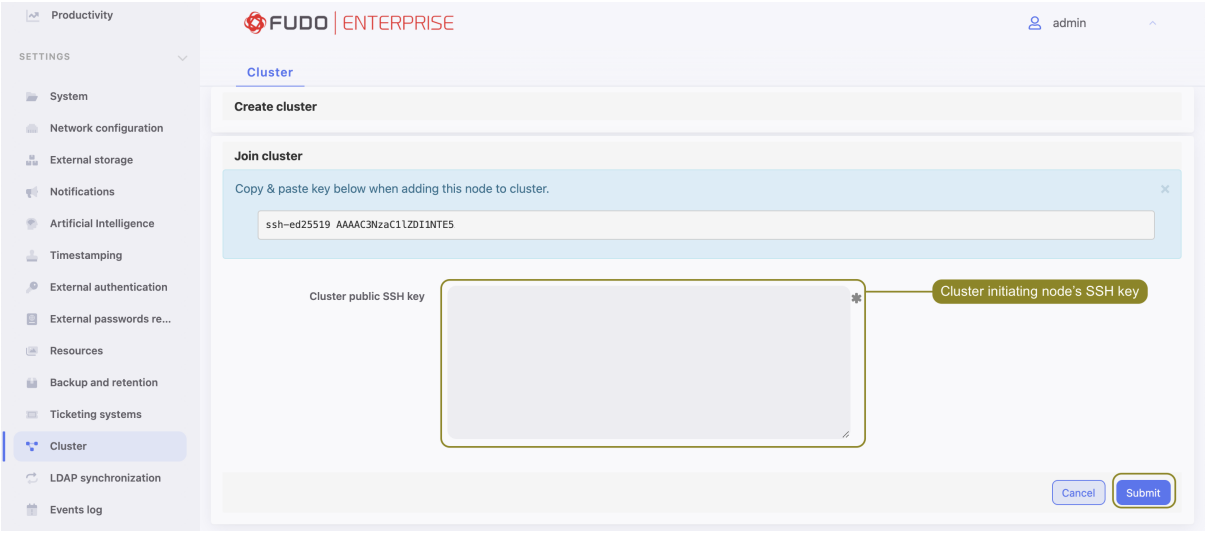


10. Select *OCR* option to delegate OCR processing in case they cannot be processed locally.



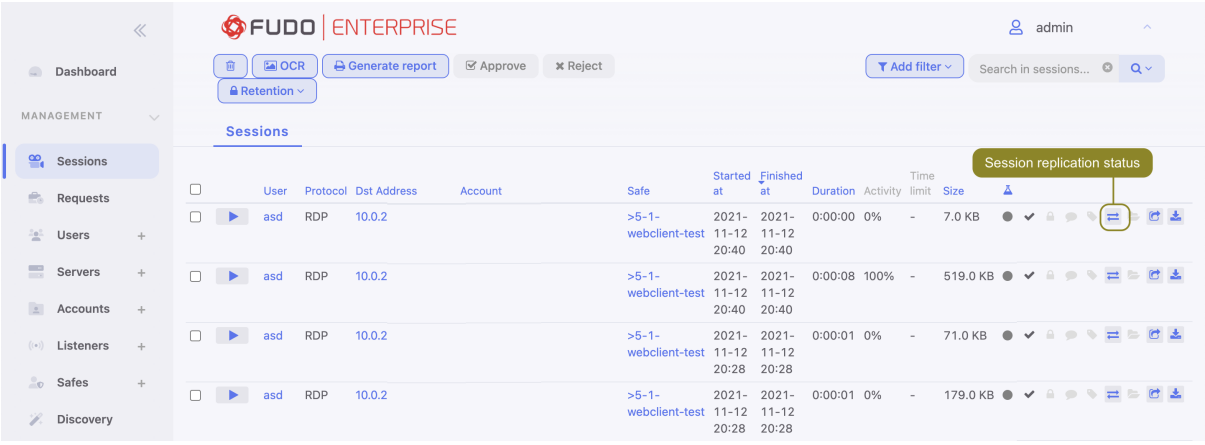
Note: Each Fudo Enterprise instance has a defined number of resources dedicated to OCR processing. If the *OCR* option is selected, excess of sessions that cannot processed locally at the moment, is forwarded for processing to selected node.

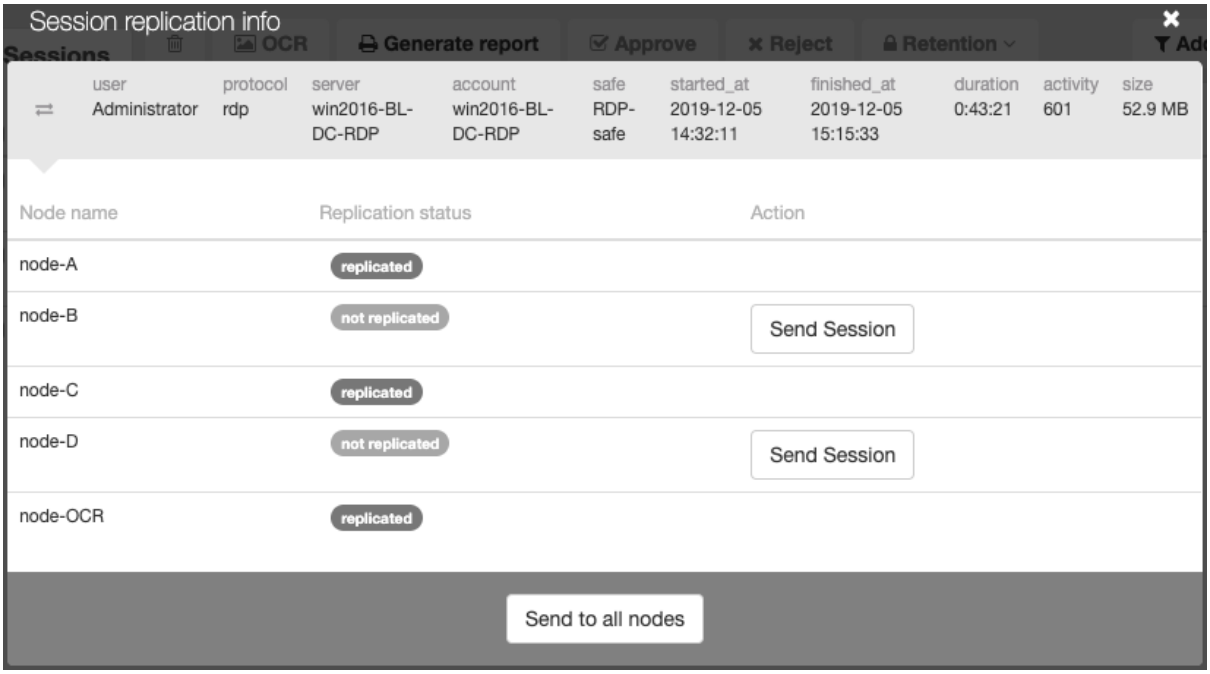
11. In the *Relations* section of the primary node, click *+ Add*.
12. Select the cluster node to which the data from the given node will be replicated.
13. Select which data will be replicated.
14. Click *Save*, to add node definition.
15. Copy cluster key to clipboard.
16. Log in to administration panel of the joining node.
17. Select *Settings* > *Cluster*.
18. Click *Join cluster*.
19. Paste cluster public SSH key and click *Submit*.



20. Click *I understand the consequences, proceed.*

Note: To view session replication status, go to sessions list and click the ⇄ icon.





Related topics:

- *Editing cluster nodes*
- *Deleting cluster nodes*
- *Security: Cluster configuration*

24.17.3 Editing cluster nodes

To modify a cluster node's configuration, proceed as follows.

1. Select *Settings* > *Cluster*.
2. Find and edit desired node parameters.
3. Click *Submit*.

Related topics:

- *Adding cluster nodes*
- *Deleting cluster nodes*
- *Security: Cluster configuration*

24.17.4 Deleting 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.

To remove a cluster node, proceed as follows.

1. Select *Settings* > *Cluster*.
2. Find desired node and select *Delete*.
3. Click *Submit*.

Related topics:

- *Adding cluster nodes*
- *Editing cluster nodes*
- *Security: Cluster configuration*

24.17.5 Redundancy groups

Redundancy groups ensure high system availability. If a master node fails, IP addresses assigned to the redundancy group will be automatically picked up by another node with the highest priority assigned to this group. Assigning different priorities to different redundancy groups enables implementing static load balancing scenario while fully preserving high availability features.

Note: Redundancy groups configuration options are available only after initializing the cluster.

Adding redundancy groups

To add a redundancy group, proceed as follows.

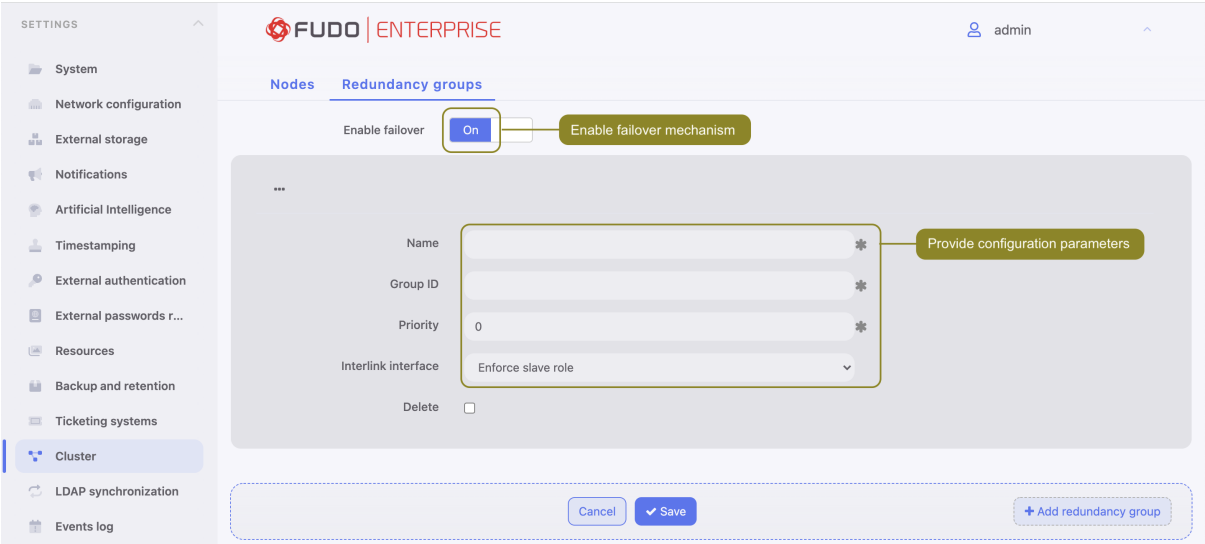
1. Select *Settings* > *Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Click + *Add redundancy group*.
4. Define group properties.

Parameter	Description
Name	Descriptive name of the redundancy group.
ID	Redundancy groups identifier (1-255).
Priority	Redundancy group priority (0-254), the lower the number the higher the priority.
	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.
Interlink interface	Network interface used for monitoring the state of the given redundancy group. The master node broadcasts *keep-alive* packets in the 2nd networking layer informing other nodes that it is up and running while other cluster nodes use the interlink interface to listen for those packets.

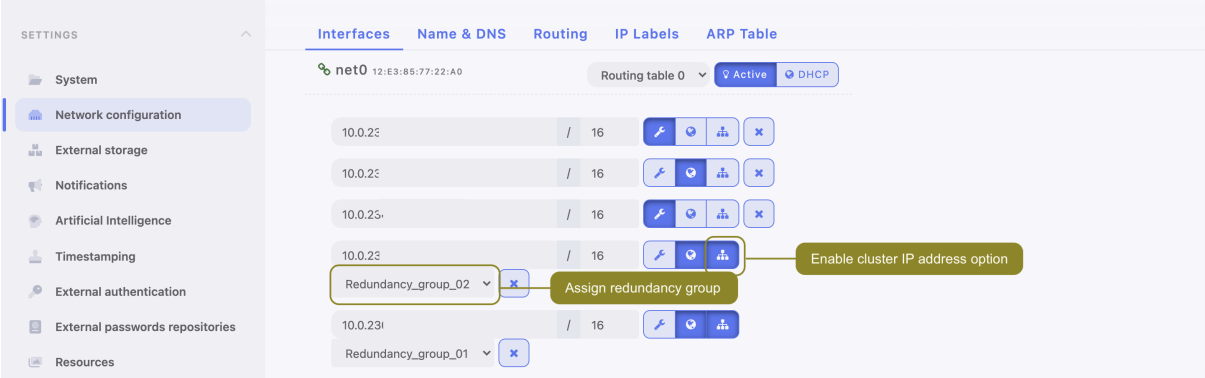
Note: The network interface (interlink interface) is used to monitor the state of a given redundancy group. The master node broadcasts keep-alive packets over the Layer 2 network to inform other nodes that it is active and operational. The remaining cluster nodes use the interlink interface to listen 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.

Note: By default, once a node takes the *master* role, it will continue on indefinitely as the *master* node.



5. Click *Save*.
6. Select *Settings* > *Network configuration*.
7. Click + to add new IP address.
8. Enter IP address and assign the *General* purpose to mark the entry as a cluster IP address.
9. Assign previously added redundancy group.
10. Click *Save*.



Note: Cluster IP address must be defined on every cluster node.

Editing redundancy groups

To modify a redundancy group, proceed as follows.

1. Select *Settings* > *Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Find and edit desired redundancy group definition.
4. Click *Save*.

Deleting a redundancy group

To delete a redundancy group, proceed as follows.

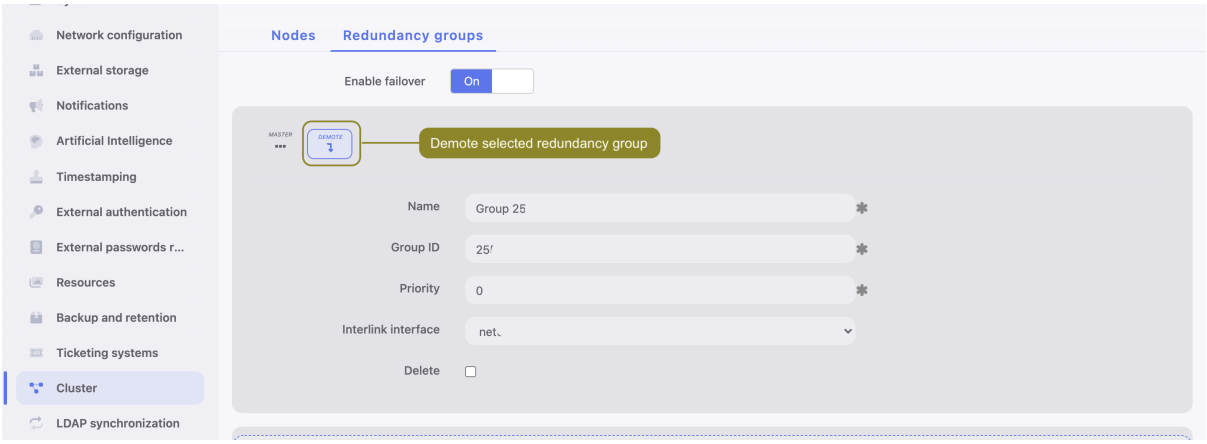
1. Select *Settings* > *Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Select *Delete* next to the desired redundancy group.
4. Click *Save*.

Demoting a redundancy group

Note: Demoting redundancy group transfers the master role for given group to another cluster node. The master role is assumed by one of the remaining nodes, on which the given redundancy group has the highest priority defined.

To demote a redundancy group, proceed as follows.

1. Select *Settings* > *Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Click *Demote* next to the desired redundancy group.
4. Click *Confirm*.



Note: If after demoting a redundancy group no other node assumes the master role for the given group, it will be reassigned to the node which previously had this role.

Enforcing a slave role

Note: Enforcing a permanent slave role on a redundancy group ensures that the given node will not assume master role on given redundancy group despite the state that other nodes are in. It's recommended for directing all traffic to other nodes before performing maintenance tasks on given cluster node. A different use case scenario would be a cluster node in a remote location with no 2nd network layer communication with other nodes.

To enforce a permanent slave role on a redundancy group, proceed as follows.

1. Select *Settings* > *Cluster*.
2. Switch to the *Redundancy groups* tab.

3. Find desired redundancy group and select `Enforce slave mode` from the *Interface* drop-down list.
4. Click *Save*.

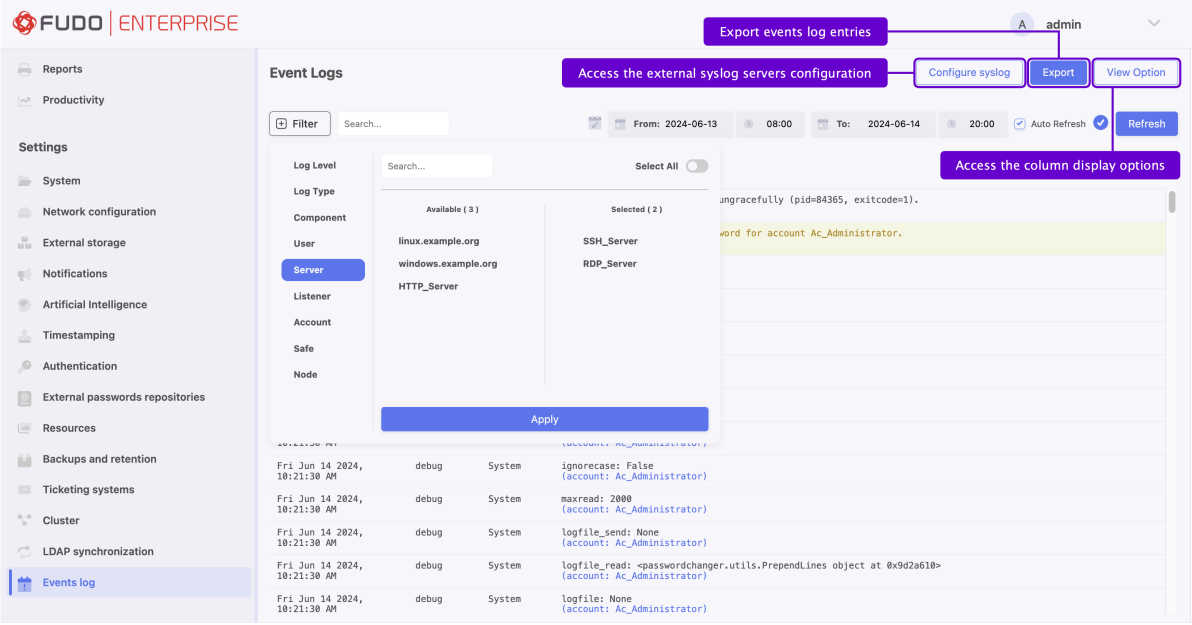
Related topics:

- *Security: Cluster configuration*
- *Initiating cluster*
- *Cluster configuration*

24.18 Events log

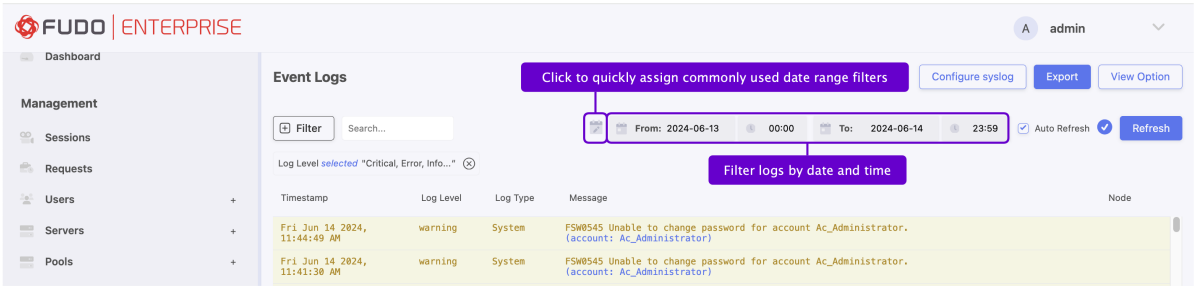
System log is an internal registry of users activities which influence system state (login information, administrative actions, etc.). Please refer to the *Log messages* section for a list of key log messages.

To display system log contents, select *Settings* > *Events log*.



24.18.1 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.



24.18.2 External syslog servers

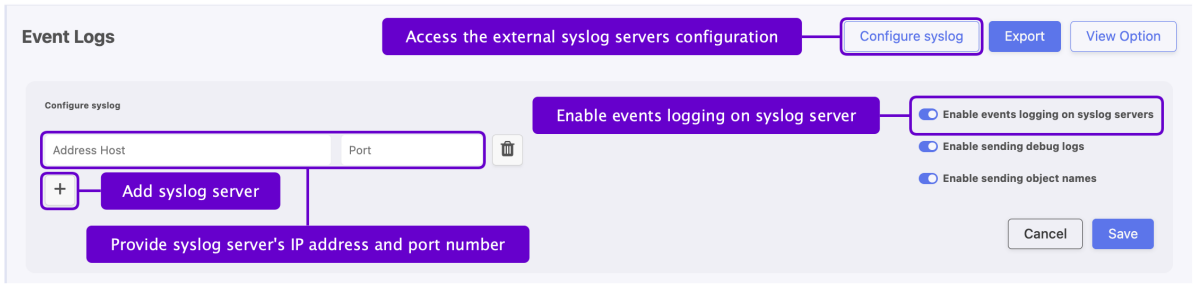
Note:

- Fudo Enterprise communicates with the syslog server using the UDP protocol.
- 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.

Adding a Syslog server

To add a *Syslog* server, proceed as follows.

1. Select *Settings* > *Events log*.
2. Click *Configure syslog* to display syslog servers configuration settings.
3. Select *Enable events logging on syslog servers* option to activate sending logs to defined syslog servers.
4. Select *Enable sending debug logs* option to activate sending debug logs within messages to defined syslog.
5. Select *Enable sending object names* option to activate sending object names within messages to defined syslog.
6. Provide server's IP address and port number.
7. Click *Save*.



Note:

- Log entries sent to syslog servers are formatted as follows:

```
[level] TIMESTAMP TAG[PID]: MESSAGE
```

where:

- `level` – log level (optional),
- `TIMESTAMP` – time of the log entry,
- `TAG` – component or module name,
- `PID` – process ID,
- `MESSAGE` – the actual log message.

- 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 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. Click *Configure syslog* to display syslog servers configuration settings.
3. Find and edit desired syslog server definition.
4. Click *Save*.

Deleting Syslog server definition

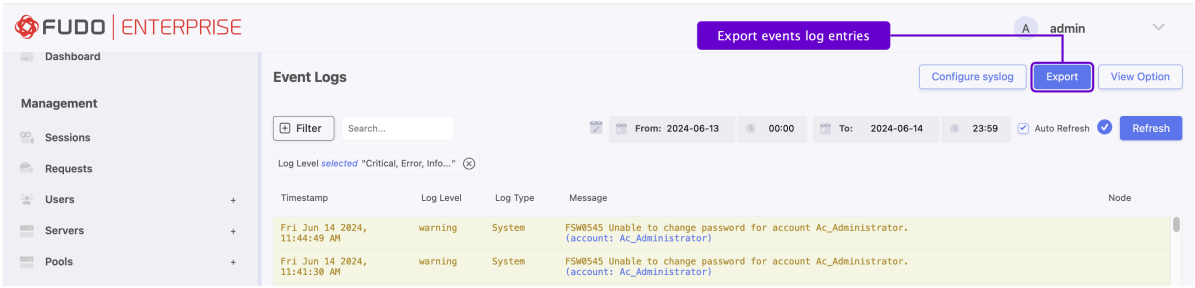
To delete a *Syslog* server definition, proceed as follows.

1. Select *Settings* > *Events log*.
2. Click *Configure syslog* to display syslog servers configuration settings.
3. Find desired server definition and click the i icon.
4. Click *Save*.

24.18.3 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.



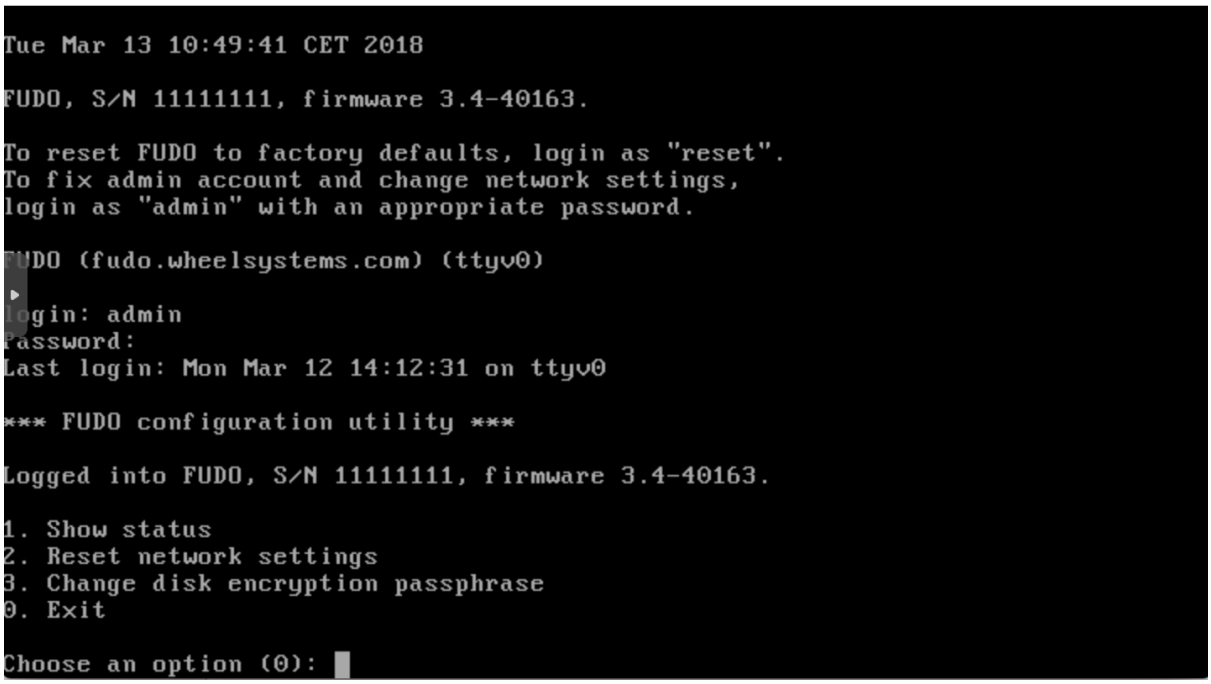
Related topics:

- *Log messages*
- *Security*
- *Managing servers*

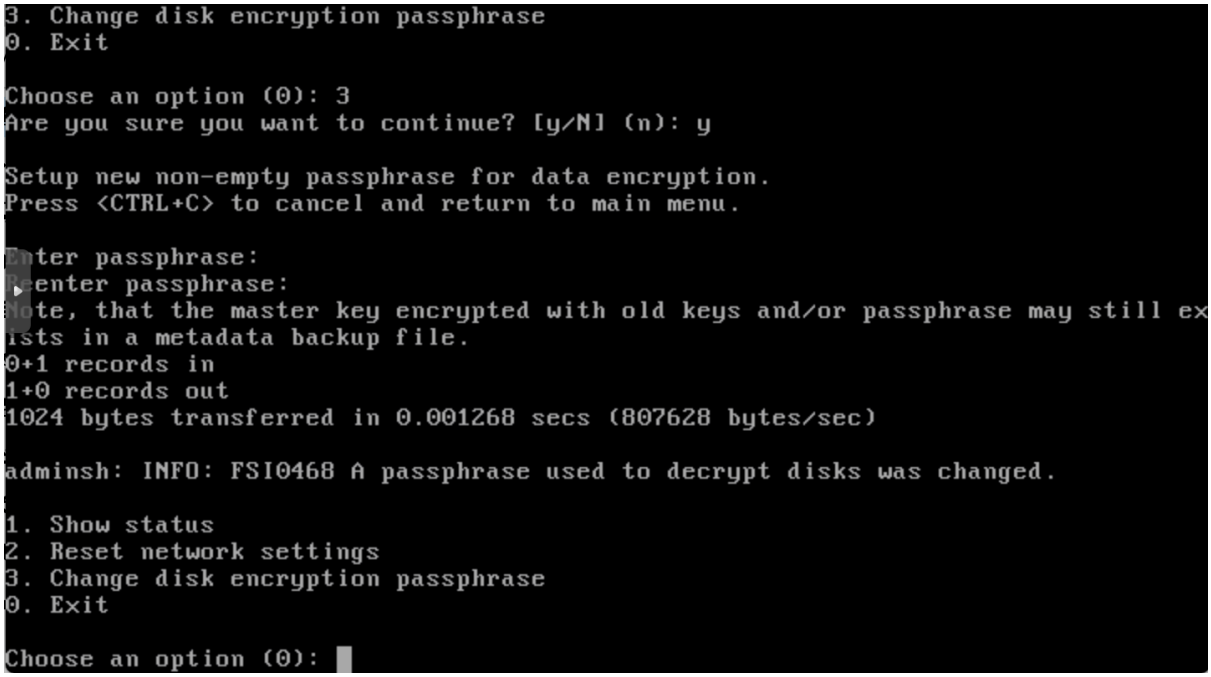
24.19 Changing encryption passphrase

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*

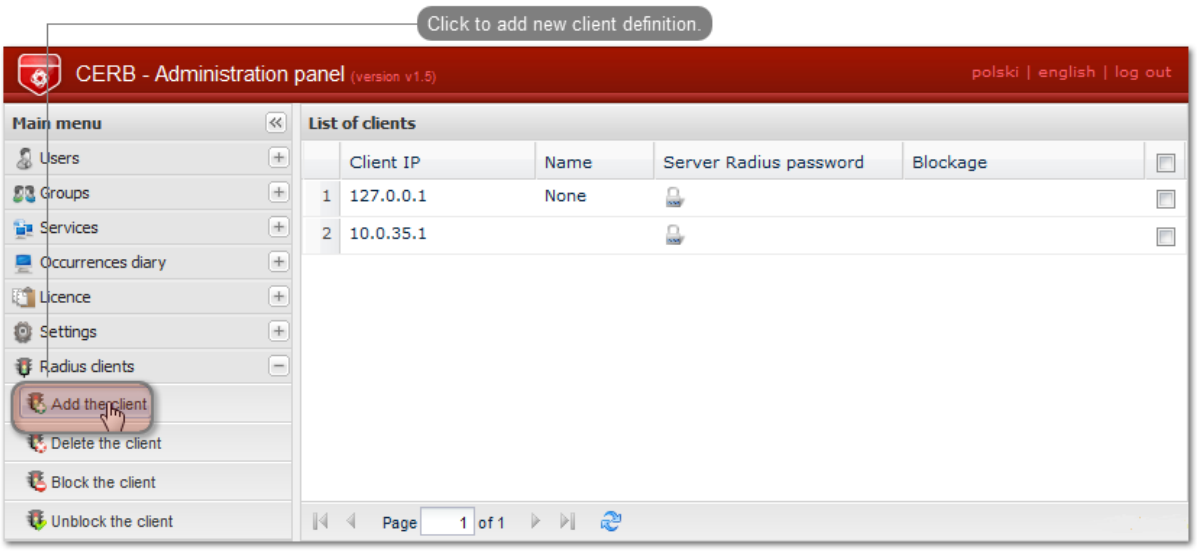
24.20 Integration with CERB server

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.

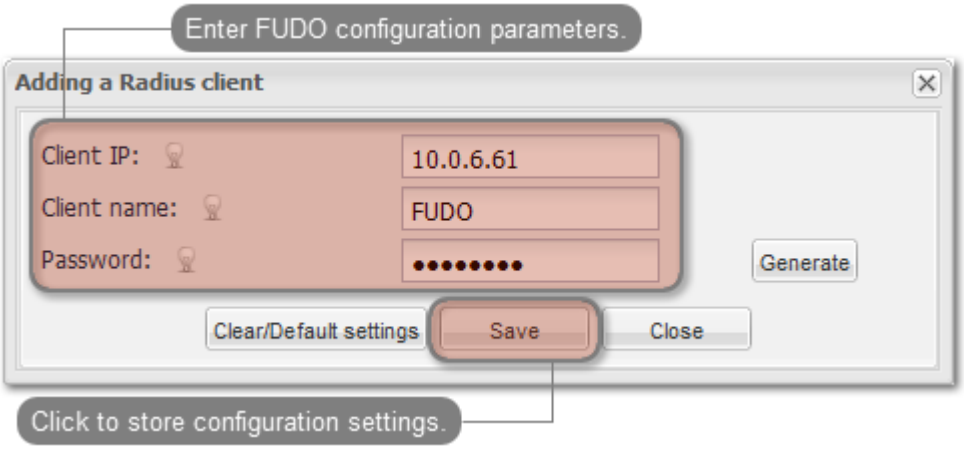
CERB server configuration

1. Adding RADIUS client.

- Select *RADIUS clients* > *Add client* to add Fudo Enterprise as a RADIUS client.



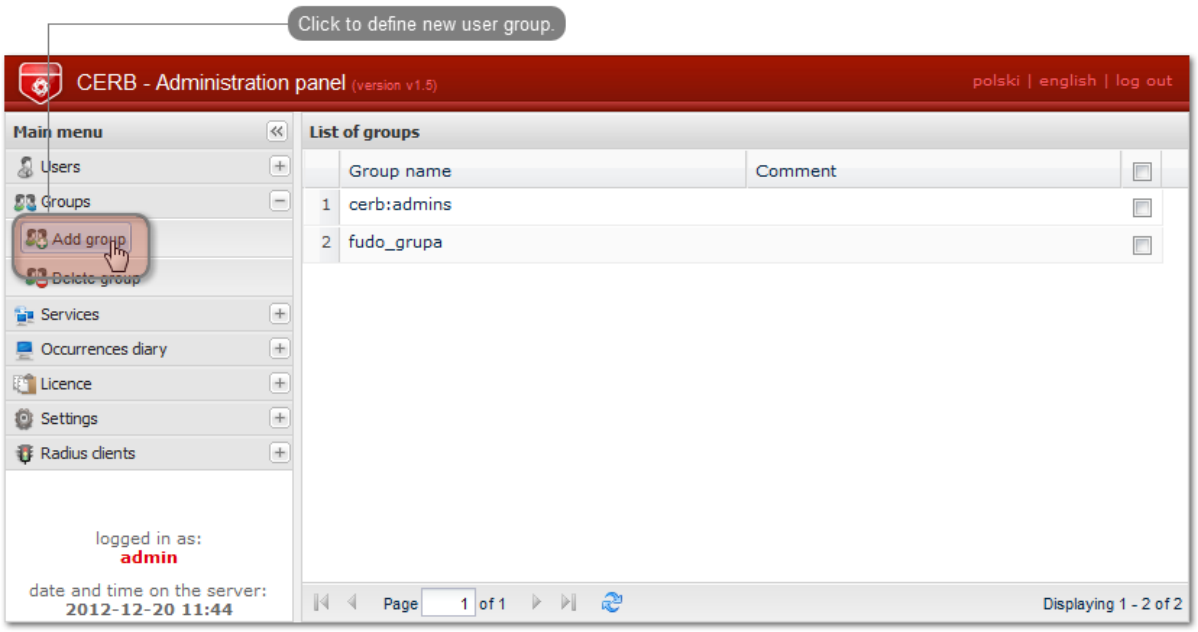
- Provide Fudo Enterprise IP address, client's name and password and click *Save*.



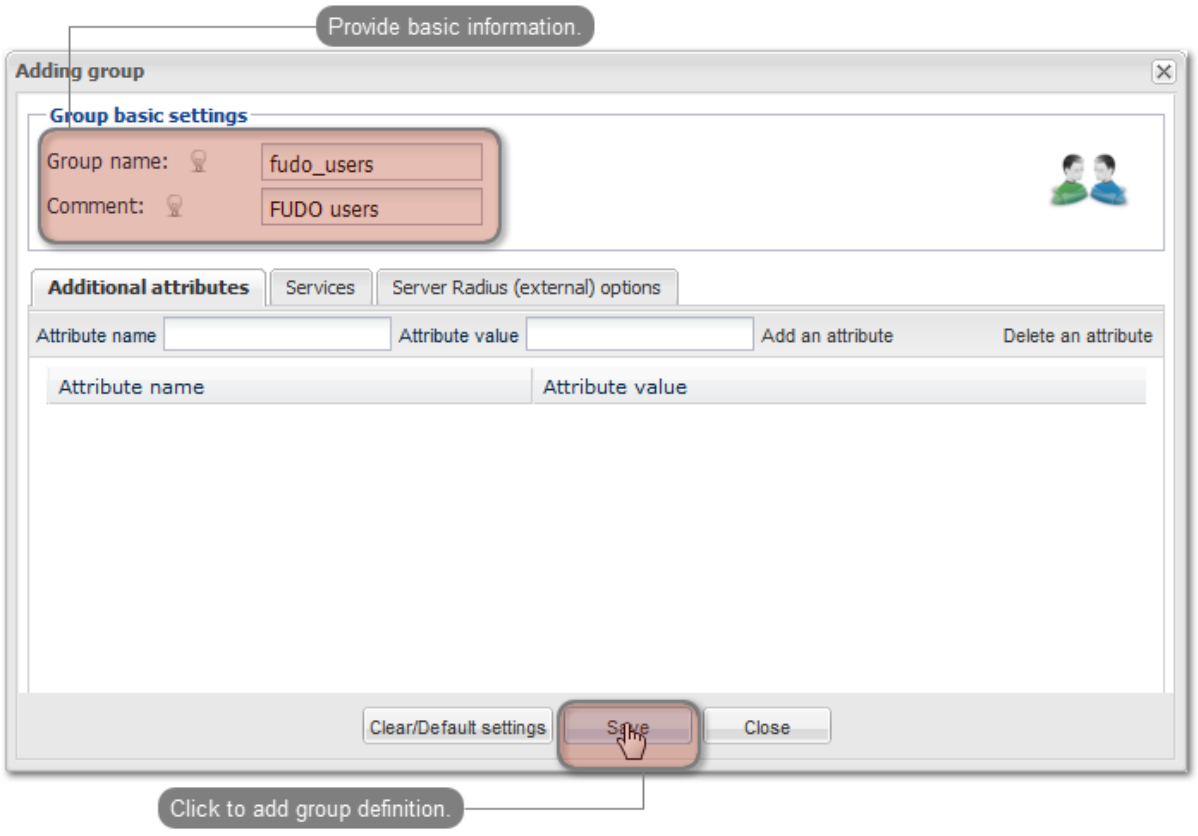
Note: Password will be required to define external authorization server in Fudo Enterprise administration panel.

2. Adding user group.

- Select *Groups* > *Add group* to define Fudo Enterprise users who will be authorized by the CERB server.

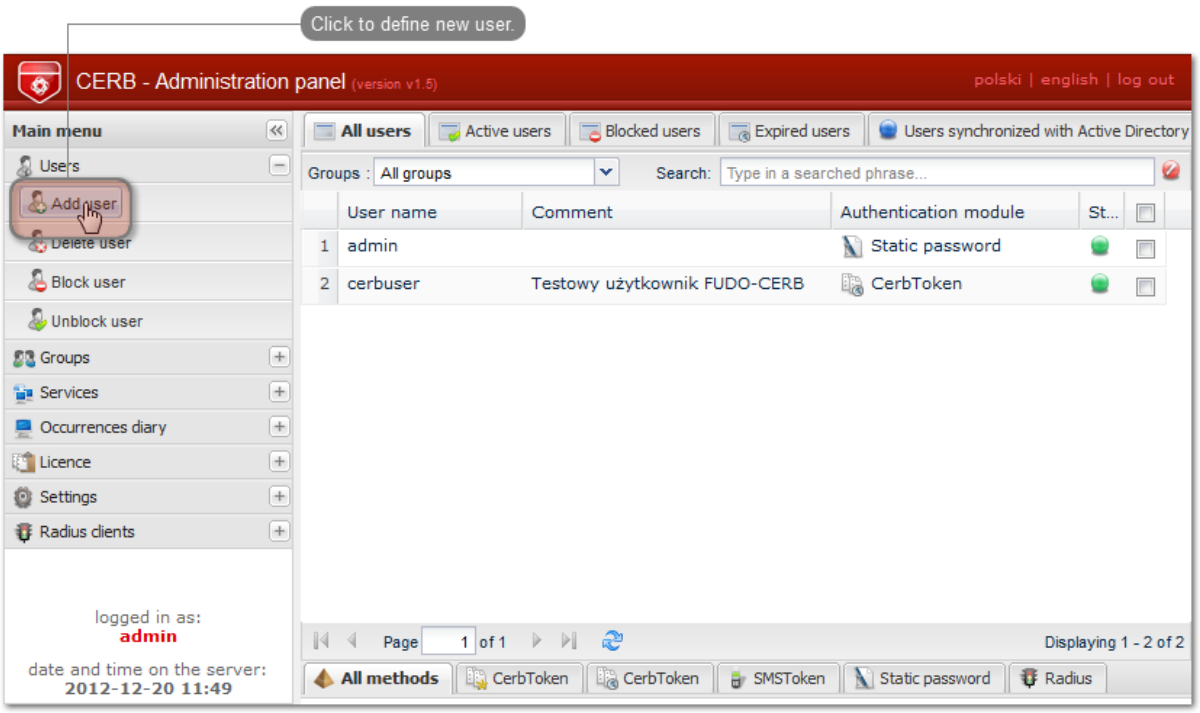


- Enter group's name (`fudo_users`) and click *Save*.

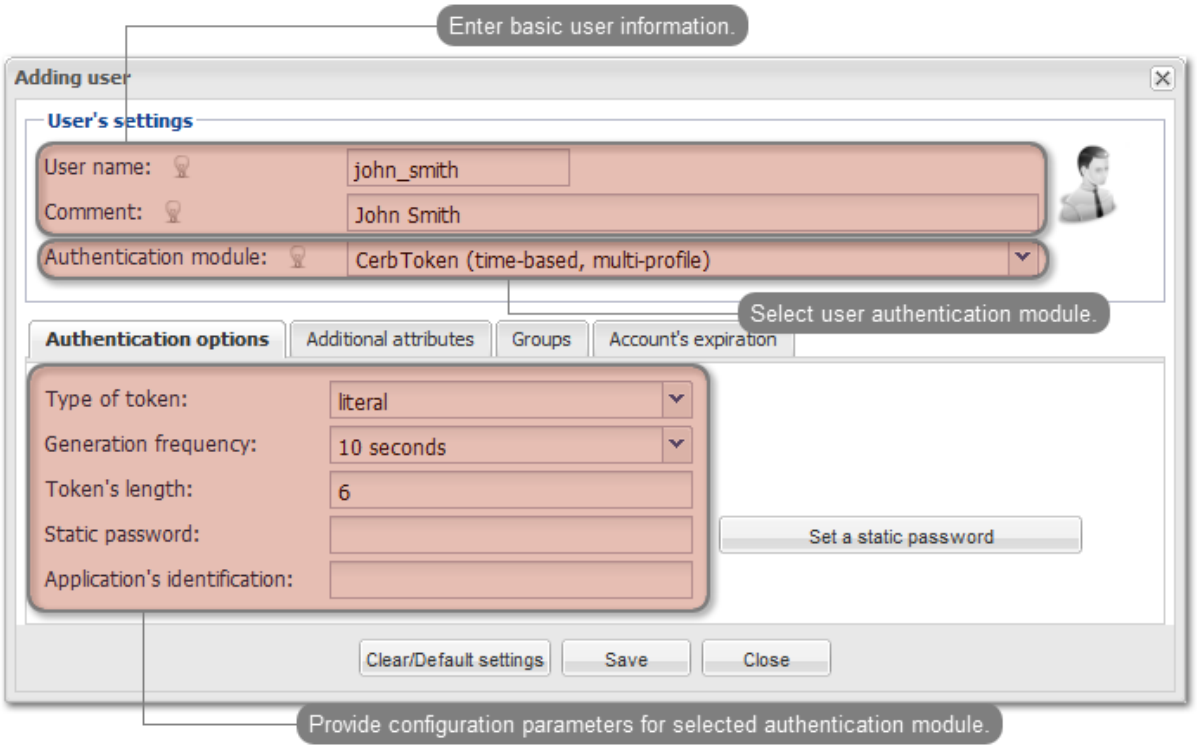


3. Adding user.

- Select *Users* > *Add user* to open new user definition window.

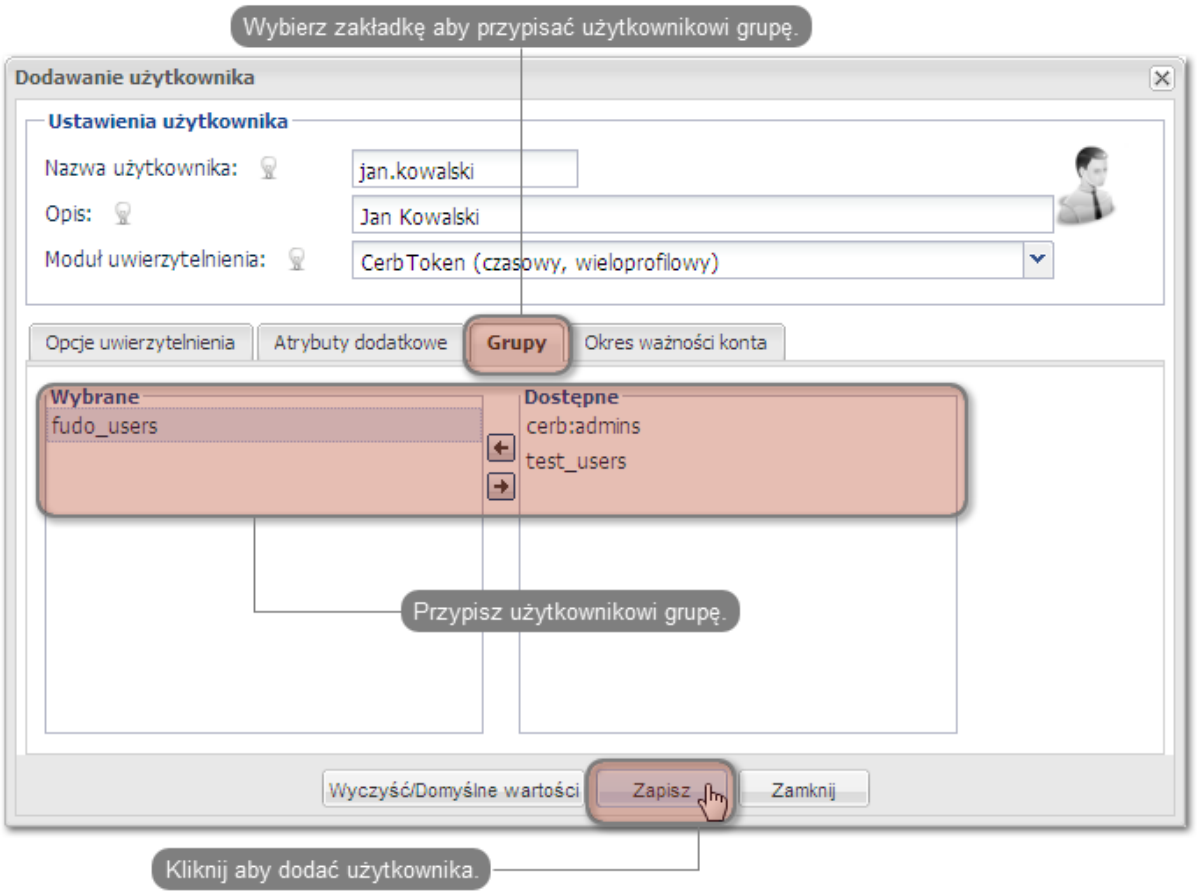


- Provide user name, description and select desired authorization module (refer to CERB server documentation form more information on authorization modules).



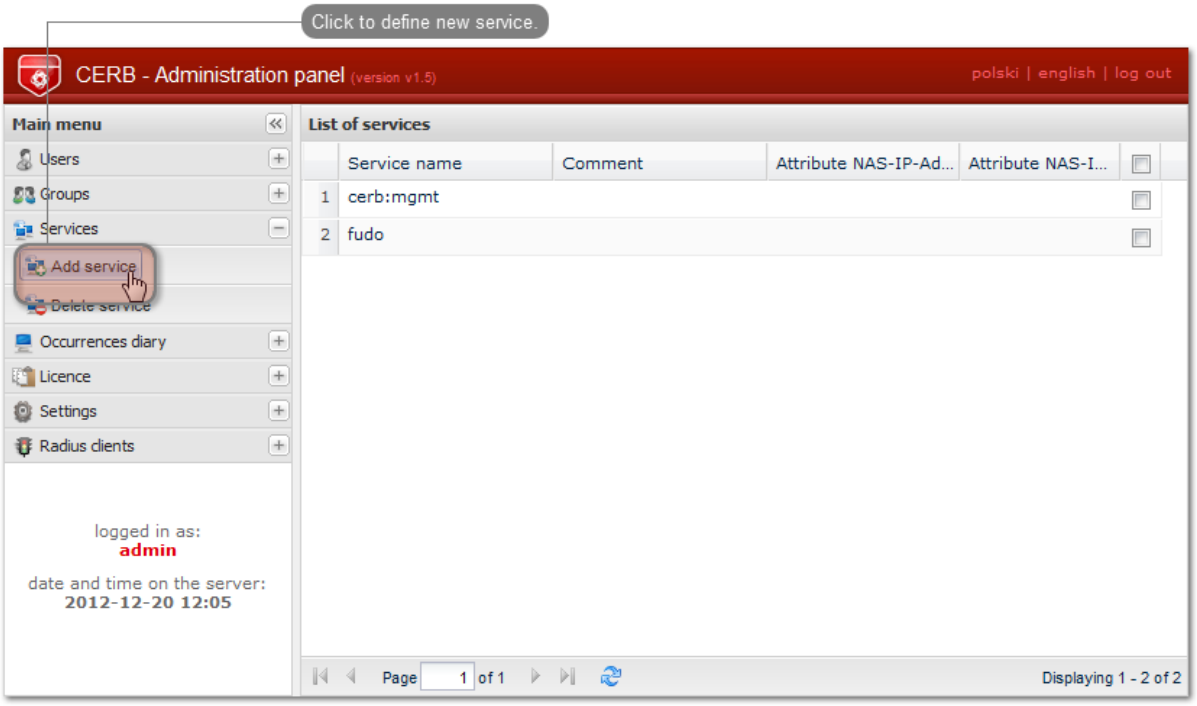
Note: Username is used to authenticate users on Fudo Enterprise.

- Assign user to previously created `fudo_users` group and click *Save*.



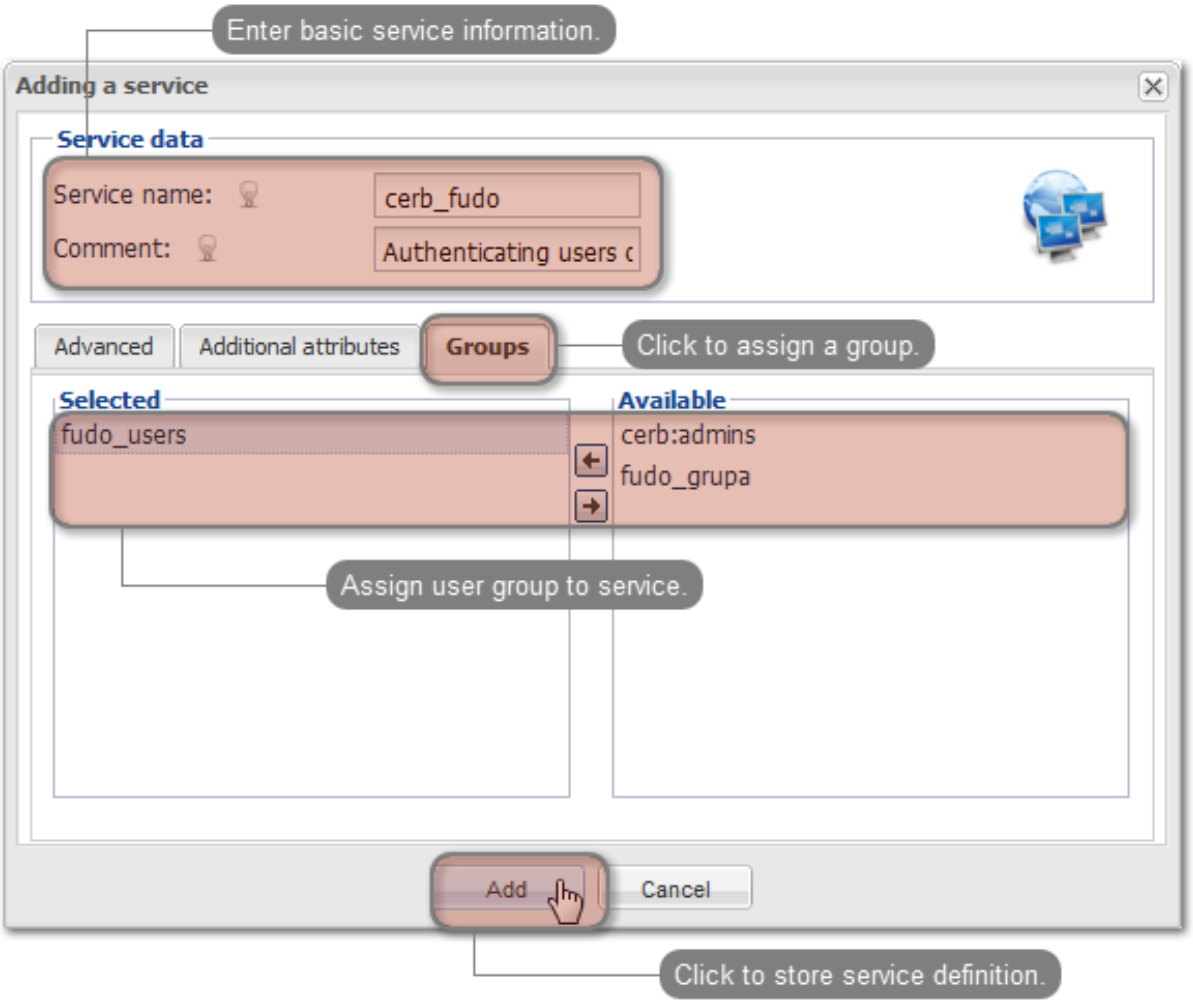
4. Configuring service.

- 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*.

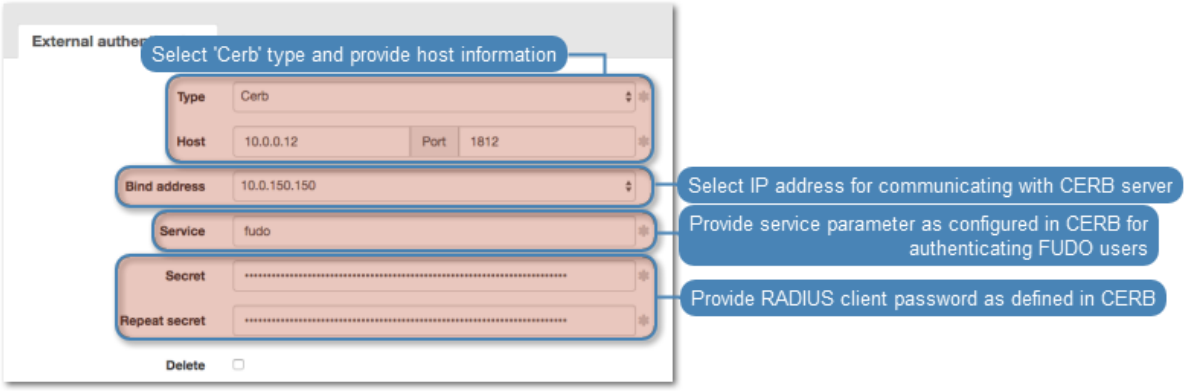


Fudo Enterprise server configuration

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



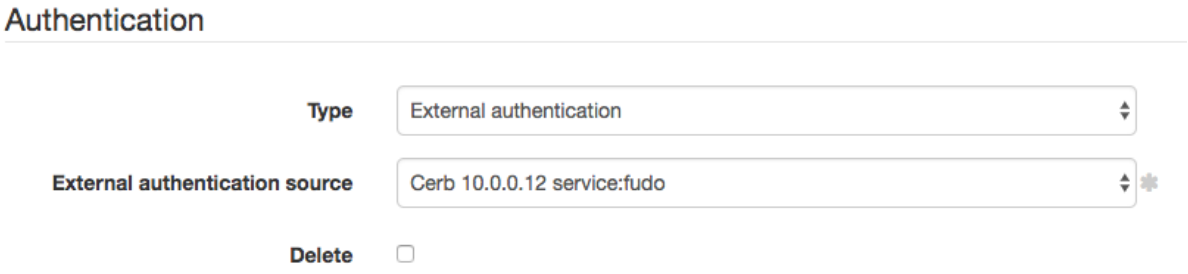
- Click *Save*.

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*

24.21 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.

24.21.1 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

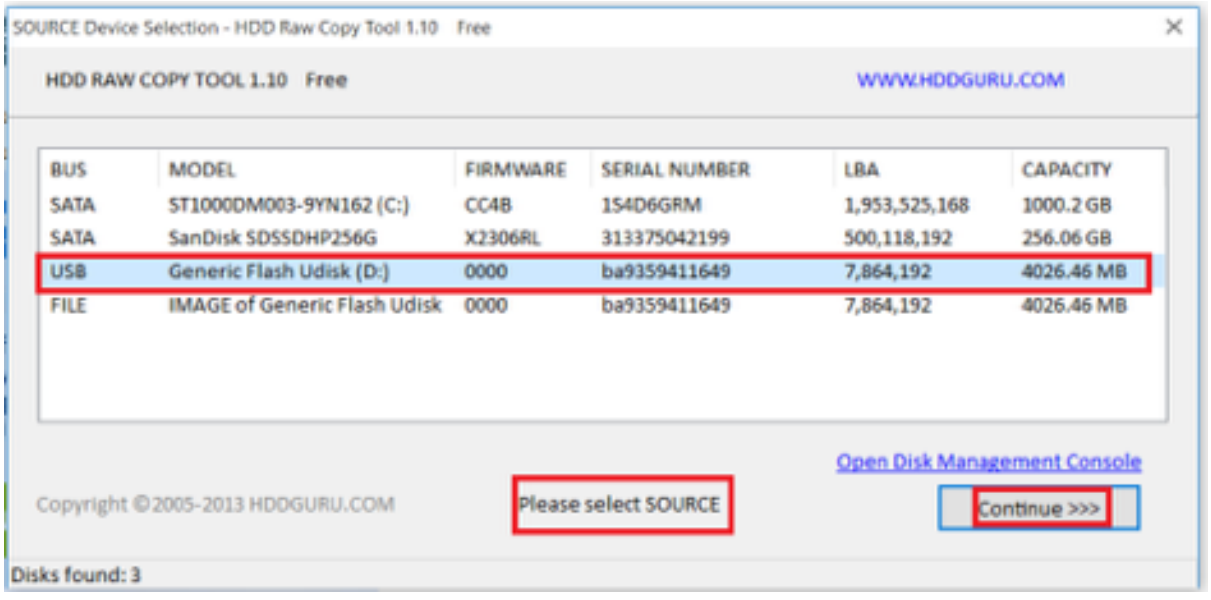
> **Warning:** After connecting the flash drive to your computer, do not initiate or format it. Ignore the system message about it not being able to read data and proceed with the backup procedure.

1. Download and install *HDD Raw Copy Tool*.

   `http://hddguru.com/software/HDD-Raw-Copy-Tool/` (portable version is also available)

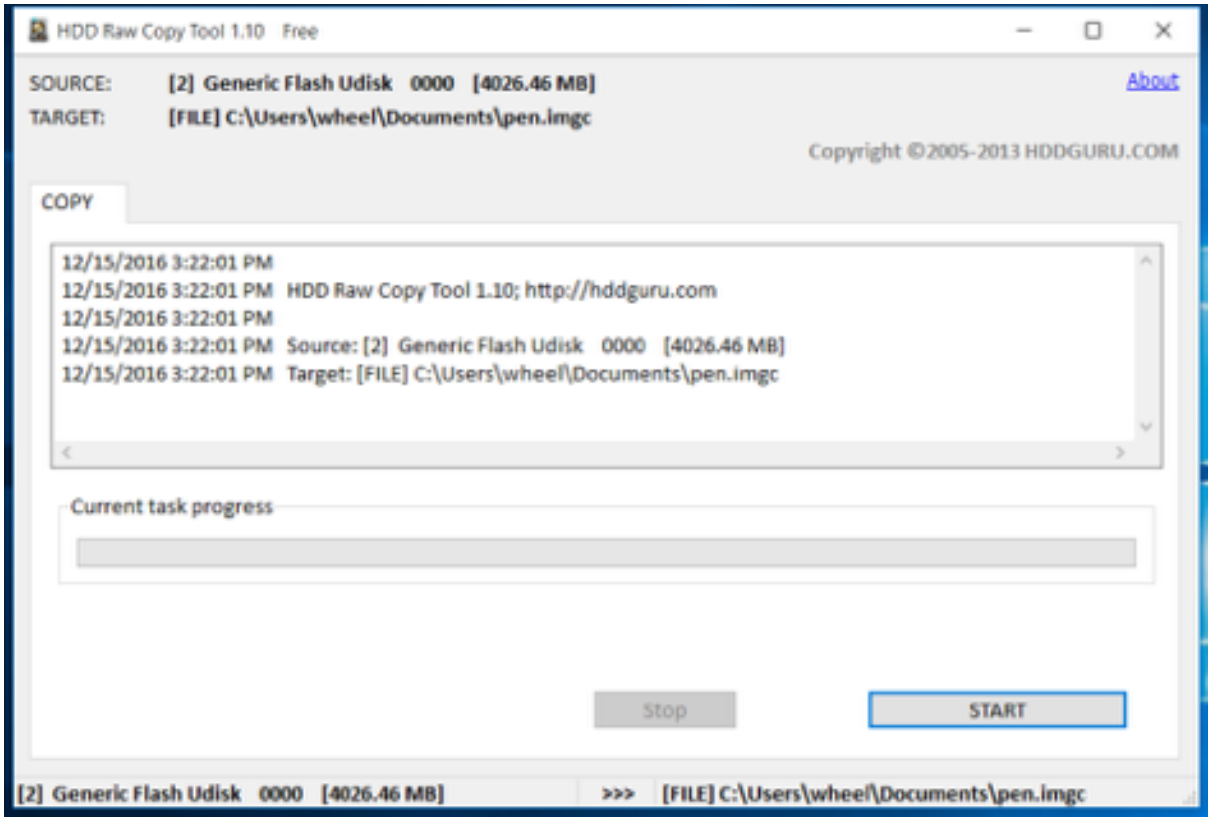
2. Start the program.

3. On the source drive selection window, choose the USB drive with the encription key and click *Continue*.



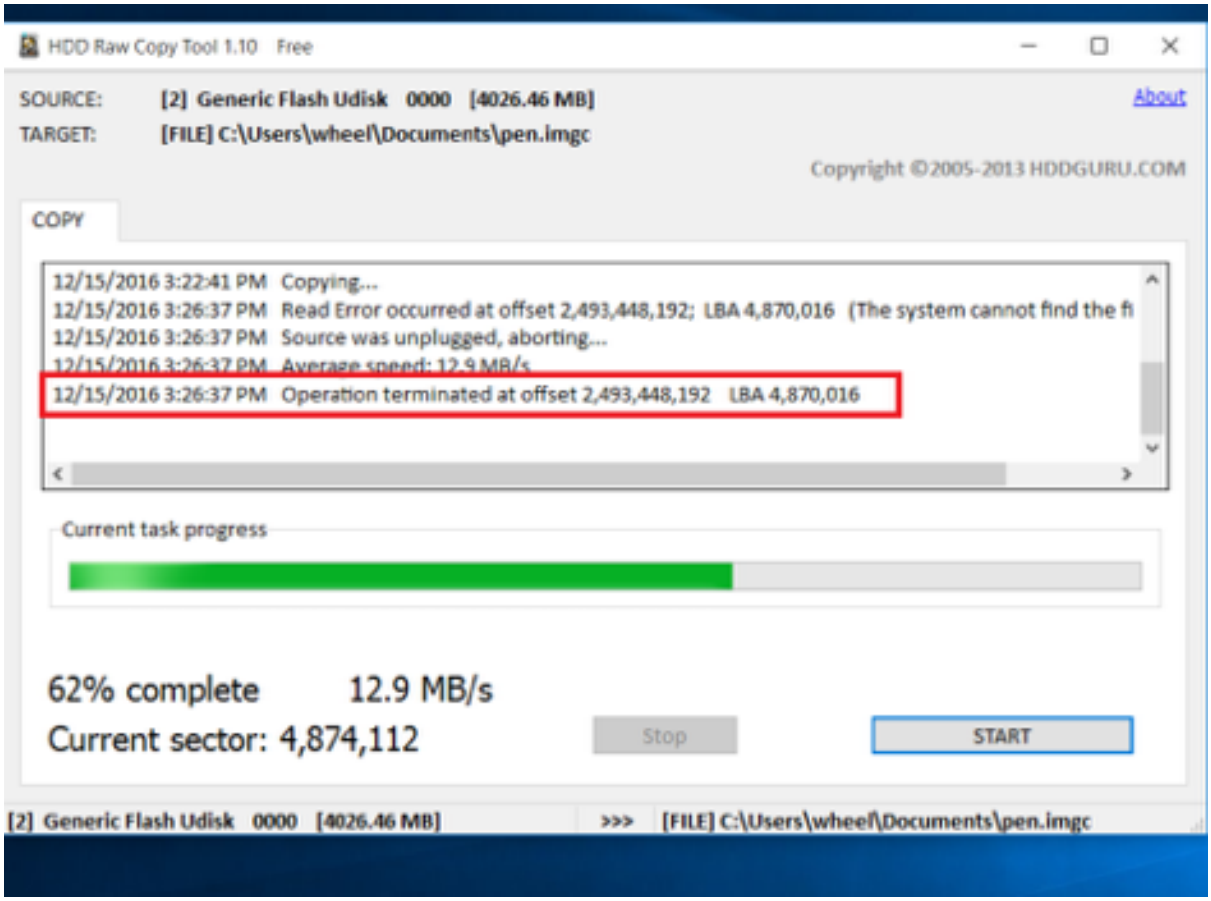
4. Click *FILE* twice, select the target image file and click *Continue*.

5. Click *START* to proceed with copying data.

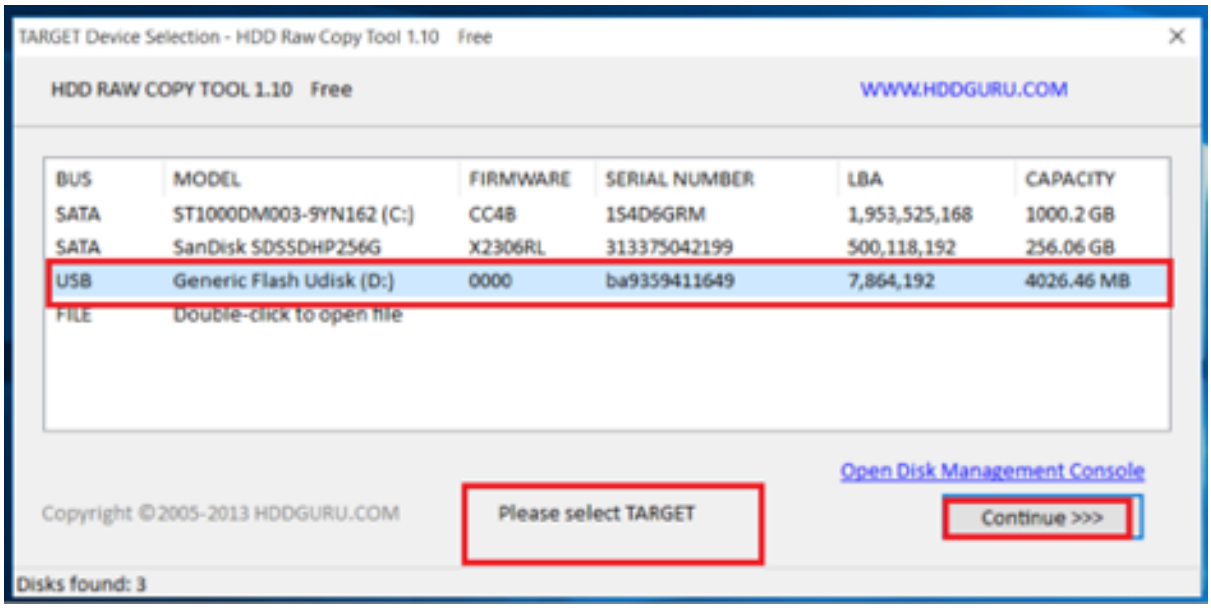


6. Once the following message occurs

   `Operation terminated at offset...` close the application and disconnect the USB drive.



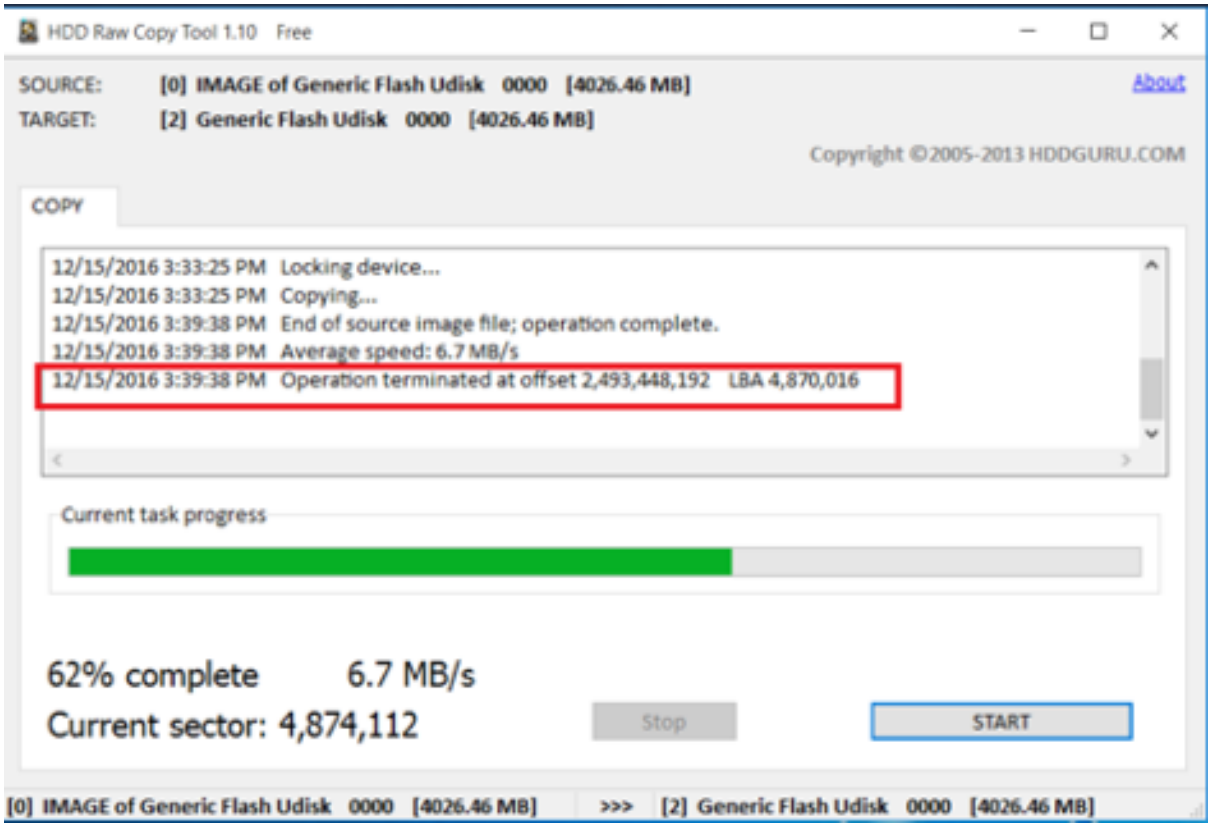
7. Connect another USB drive and start *HDD Raw Copy Tool*.
8. On the source drive selection screen select *FILE* and browse the file system to find the encryption keys image file.
9. Select the newly connected USB flash drive as a target device and click *Continue*.



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*

24.21.2 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 *Management* > *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 *Management* > *Dashboard*.
3. Check current network transfer rate.

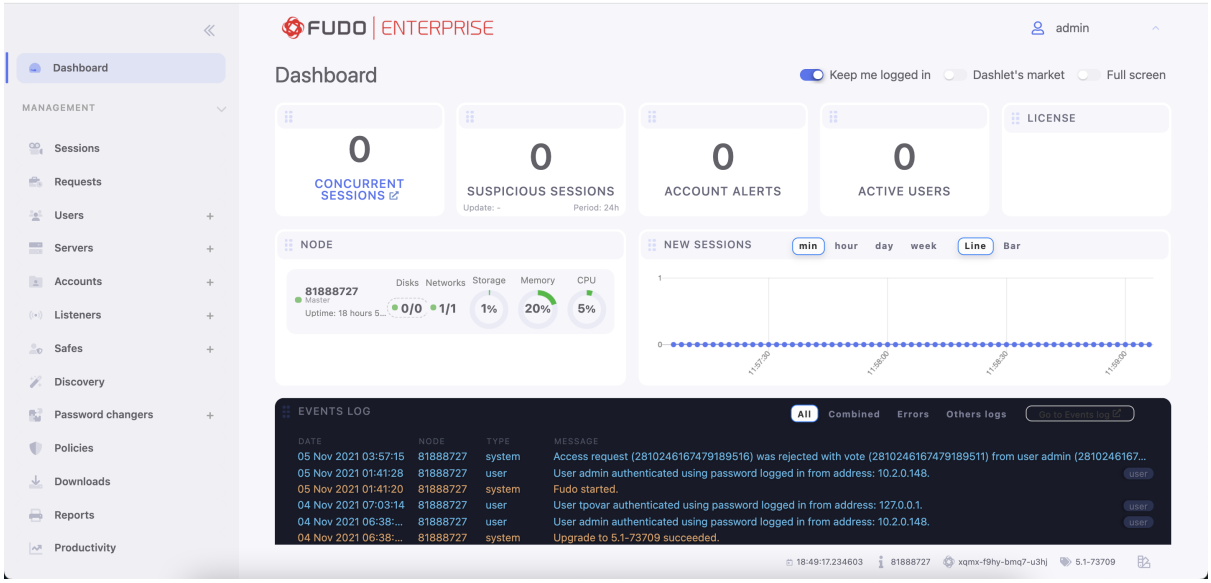
Note: Fudo Enterprise features 1Gbps network interface cards. In case the current network bandwidth usage exceeds 500Mbps, users may notice a decrease in system communication performance.

Monitoring storage

Warning: Fudo Enterprise will not allow new connections when storage usage reaches 90%.

1. Login to Fudo Enterprise administration panel.
2. Select *Management* > *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*

24.21.3 Health Check

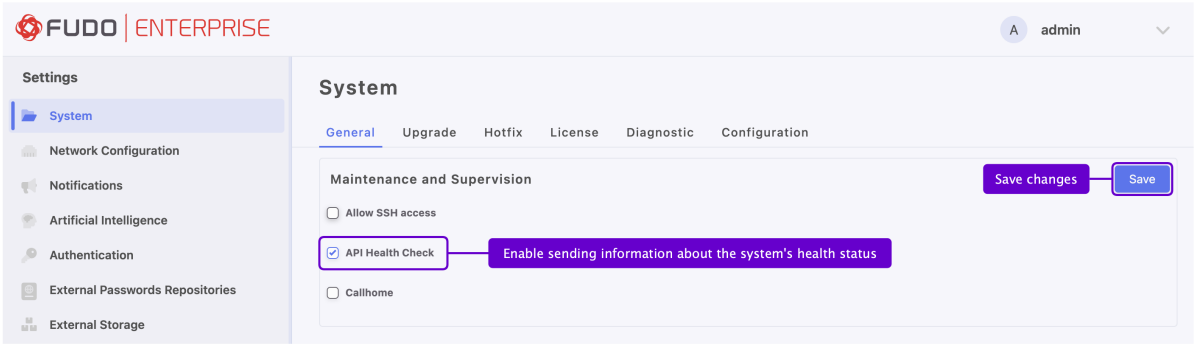
Fudo Enterprise regularly checks its "health" status. There are multiple tests that check the status of both hardware and software components. These tests are called "health checks".

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*.

24.21.3.1 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.

24.21.4 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.

24.21.4.1 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.

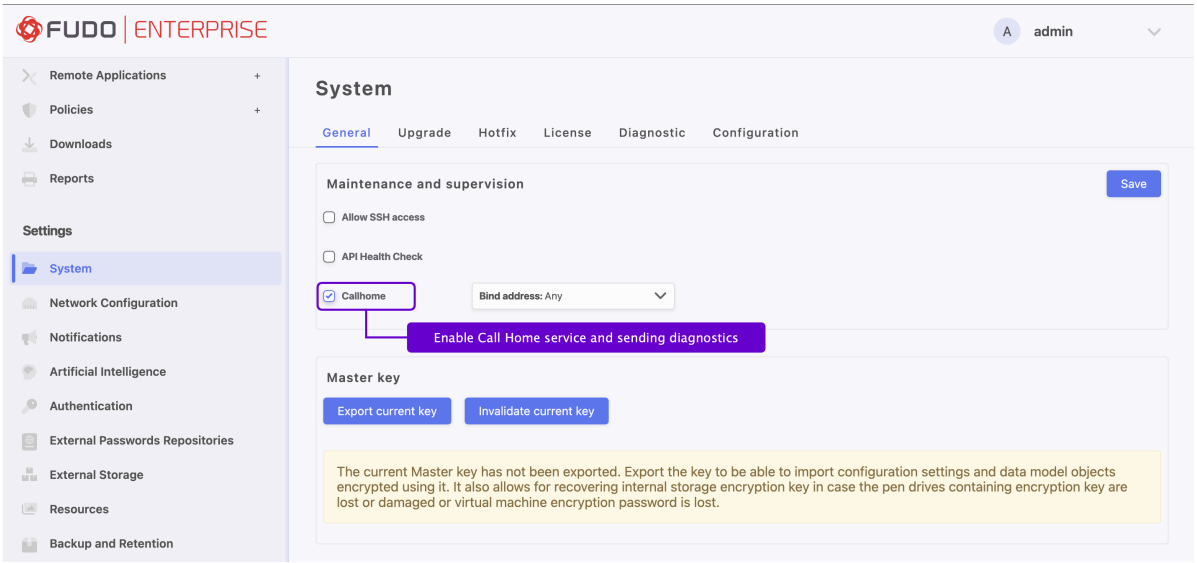
24.21.4.2 The Benefits of Using Callhome

- **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.

24.21.4.3 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*

24.21.5 Hard drive replacement

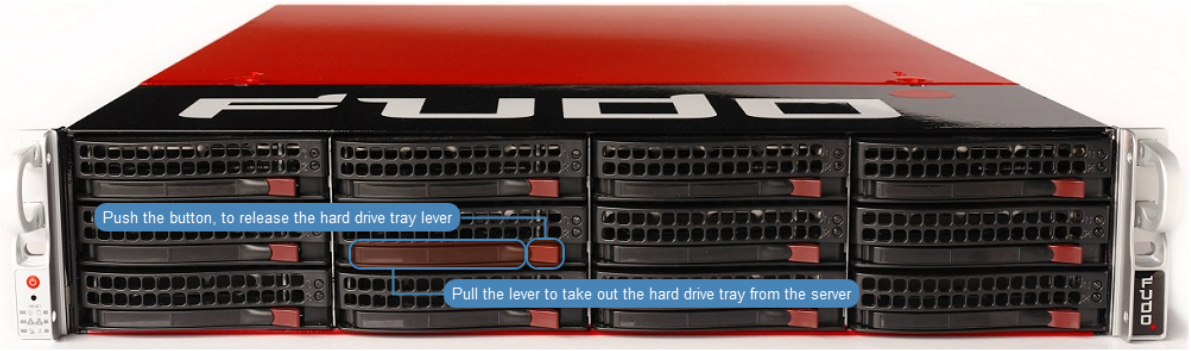
In default configuration, Fudo Enterprise's storage array comprises 12 hard drives in RAIDZ2 configuration running ZFS file system allowing the system to remain fully operational in case of a failure of two hard drives.

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.

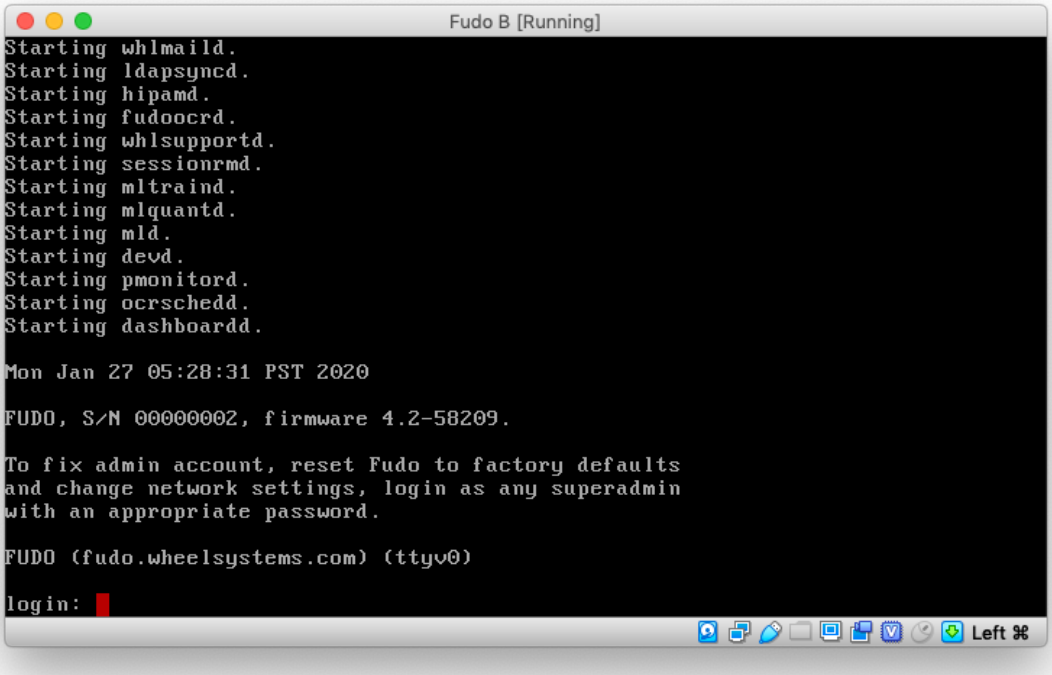
Related topics:

- *Hardware overview*
- *Frequently asked questions*

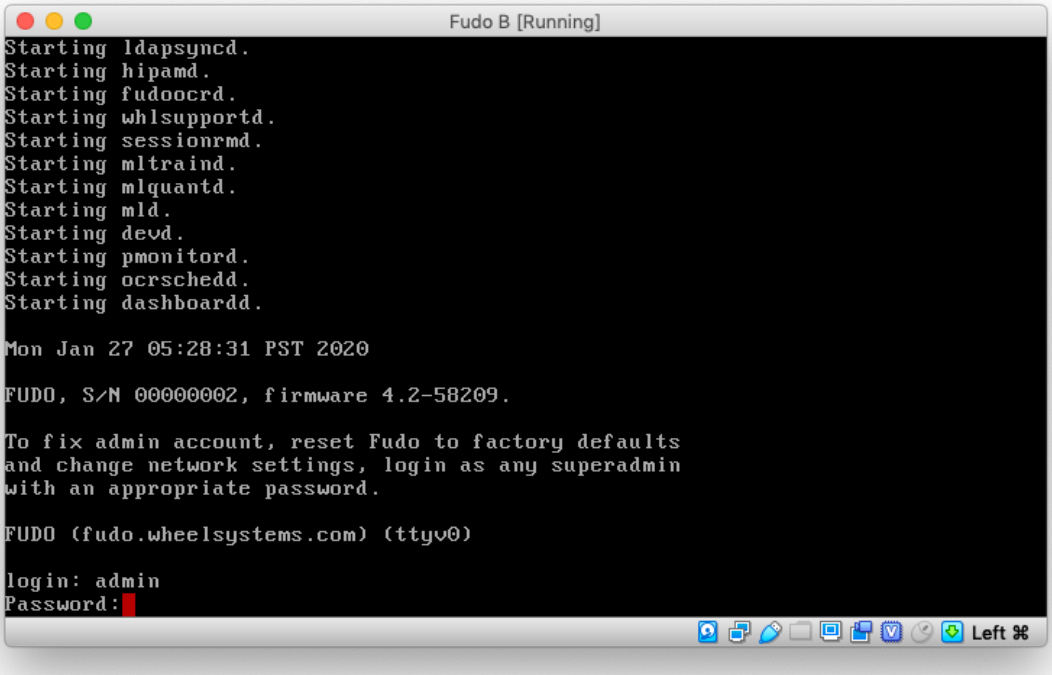
24.21.6 Resetting configuration to default settings

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.

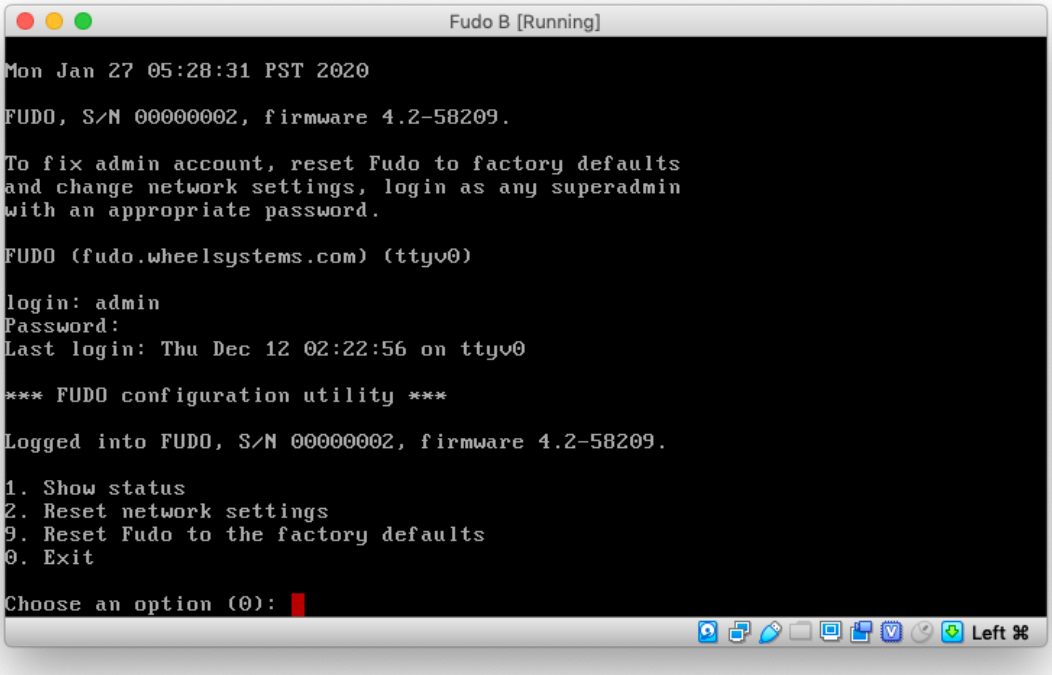
1. Access system terminal.
2. Enter administrator account login and press *Enter*.



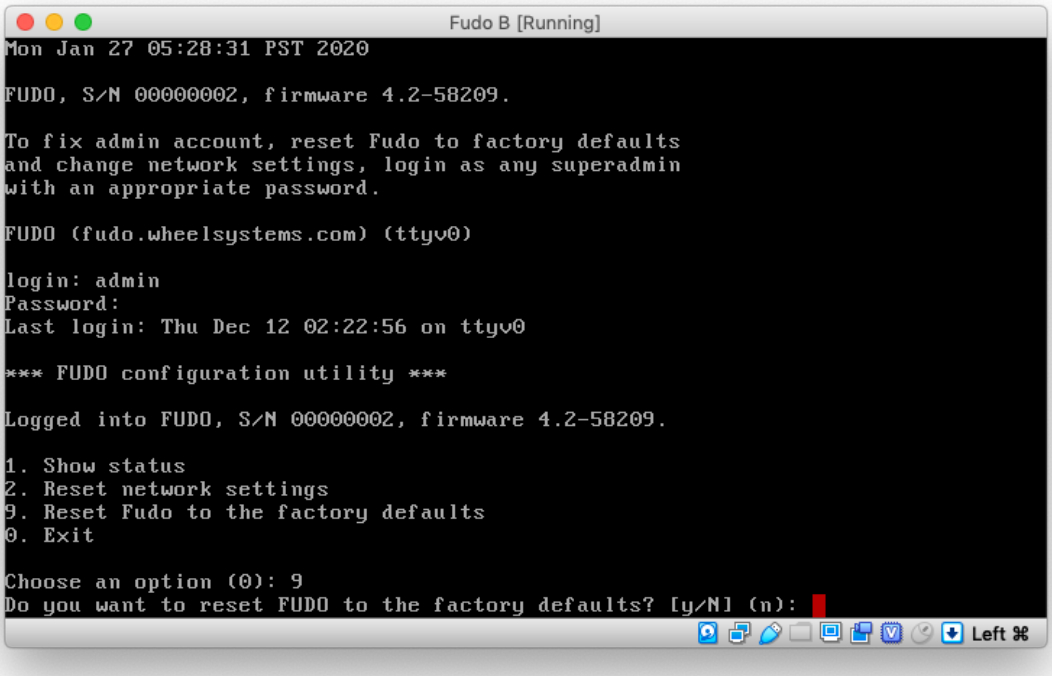
3. Enter administrator account password and press *Enter*.



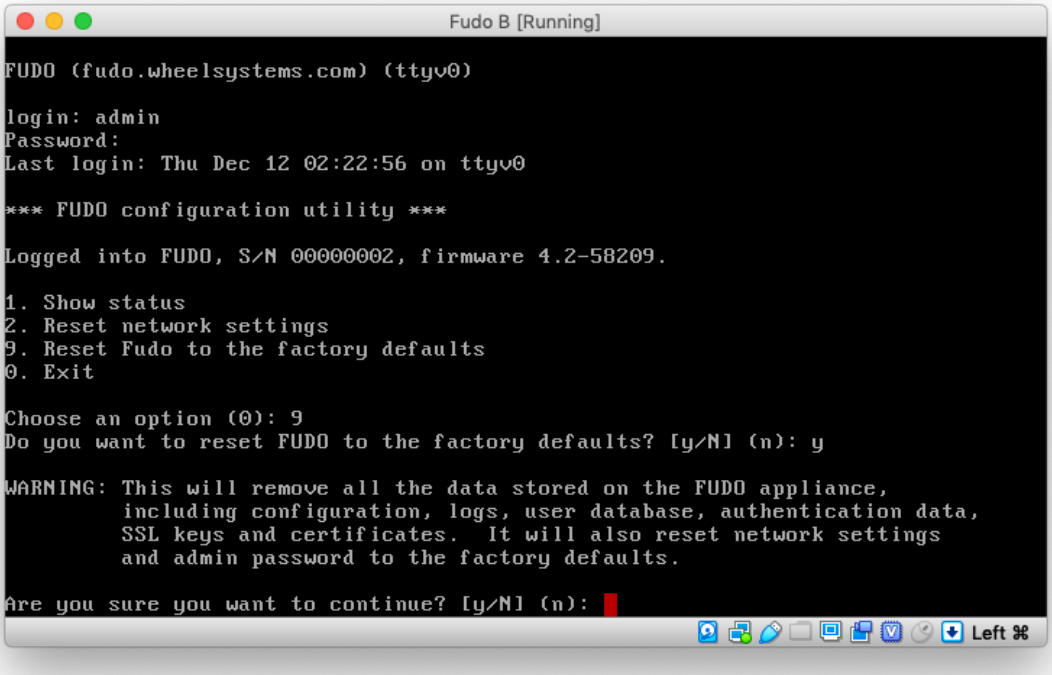
4. Enter 9 and press *Enter*.



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*

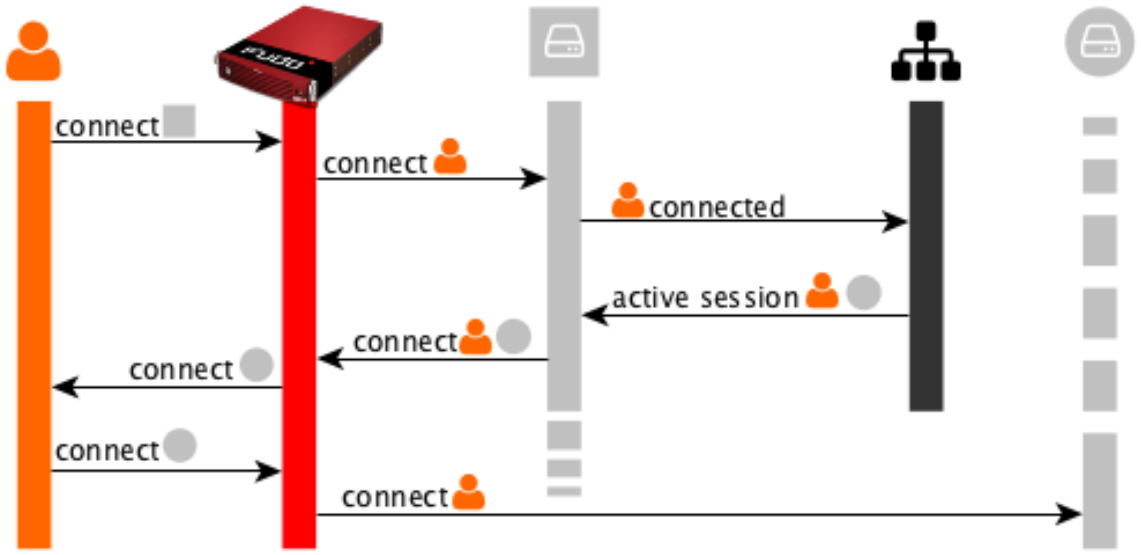
CHAPTER 25

Reference information

25.1 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.



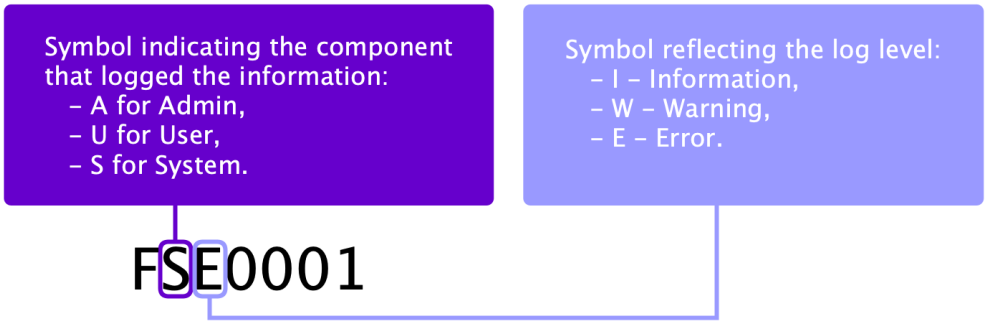
Note: To successfuly redirect a connection, the server identified by the broker must be defined on Fudo Enterprise, it must listen on default RDP port (3389) and user must be allowed to connect to given server.

Related topics:

- *Data model*
- *RDP*
- *Servers*
- *Accounts*

25.2 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.
FSE0009	ERROR	SYSTEM	Upgrade failed.
FSW0011	WARNING	SYSTEM	Retention module was unable to delete session ${_sessid} from database.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSW0012	WARNING	SYSTEM	Retention module error, session ${_sessid} skipped.
FSI0013	INFO	SYSTEM	Session ${_sessid} removed according to retention policy.
FSW0014	WARNING	SYSTEM	Retention module was unable to remove session ${_sessid}.
FSI0015	INFO	SYSTEM	Redundancy group ${_name} switched to master role.
FSW0016	WARNING	SYSTEM	Unable to send email, SMTP server not configured.
FSI0017	INFO	SYSTEM	Redundancy group ${_name} switched to slave role.
FSI0025	INFO	SYSTEM	Cluster node %s (%s) host key set to '%s'.
FSI0027	INFO	SYSTEM	Cluster node %s initialized.
FSE0028	ERROR	SYSTEM	Unable to join node to cluster on %s.
FSE0031	ERROR	SYSTEM	Timestamping service communication error.
FSE0032	ERROR	SYSTEM	Unable to timestamp session.
FSE0033	ERROR	SYSTEM	Unknown timestamping service provider.
FSI0034	INFO	SYSTEM	Session ${SESSION} was timestamped.
FSI0035	INFO	SYSTEM	Email ${mailname} sent to ${admin_email}.
FSW0036	WARNING	SYSTEM	Unable to send email "{}" to {} through {} server.
FSW0037	WARNING	SYSTEM	Output from SMTP client: {}.
FSI0038	INFO	SYSTEM	Saved email ${mailname} sent to ${admin_email}.
FSI0039	INFO	SYSTEM	System image version %s uploaded successfully.
FSE0040	ERROR	SYSTEM	Communication error with cluster node %s (%s): version mismatch (local: %s, remote: %s).
FSI0045	INFO	SYSTEM	Initial objects replication to cluster node %s (%s) completed.
FSE0046	ERROR	SYSTEM	There is no filter called %s.
FSW0047	WARNING	SYSTEM	Error sending notification.
FSE0048	ERROR	SYSTEM	Error authenticating user %s over RADIUS.
FUI0049	INFO	USER	User %s authenticated using password logged in from address: %s.
FUI0051	INFO	USER	User %s authenticated through %s (Host: %s, Port: %d, %s: %s) logged in from address: %s.
FUI0053	INFO	USER	User %s authenticated through LDAP (Host: %s, Port: %d) logged in from address: %s.
FUI0055	INFO	USER	User %s (domain %s) authenticated through Active Directory (protocol: %s) logged in from address: %s.
FUE0057	ERROR	USER	Authentication method 'password', required by MySQL, requested by the user %s, logging in from address %s, was not found.
FSE0061	ERROR	SYSTEM	Incorrect password repository configuration: login is empty.
FSE0062	ERROR	SYSTEM	Incorrect password repository configuration: password is empty.
FSE0065	ERROR	SYSTEM	License configuration error.
FSE0066	ERROR	SYSTEM	Unable to block user %jd.
FSW0074	WARNING	SYSTEM	Connection terminated because license has expired or was not set.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSW0075	WARNING	SYSTEM	Connection terminated because number of nodes in cluster exceeded license limit.
FSE0077	ERROR	SYSTEM	LDAP authentication error.
FSE0078	ERROR	SYSTEM	LDAP authentication error: unable to connect from %s to %s.
FUE0079	ERROR	USER	Authentication timeout after %ju key attempt%s and %ju password attempt%s.
FUE0080	ERROR	USER	Authentication timeout after %lu key attempt%s.
FUE0081	ERROR	USER	Authentication timeout after %lu password attempt%s.
FSE0082	ERROR	SYSTEM	Unable to establish connection to server %s (%s).
FSE0083	ERROR	SYSTEM	Unable to establish connection from %s to server %s (%s).
FSI0084	INFO	SYSTEM	Terminating session: %s.
FSI0085	INFO	SYSTEM	Session finished.
FUI0086	INFO	USER	User %s blocked due to connection policy violation.
FUW0087	WARNING	USER	Session has been terminated due to user %s account expiration.
FUE0089	ERROR	USER	Authentication timeout.
FSE0090	ERROR	SYSTEM	Unable to connect to the passwords repository server %s.
FSE0092	ERROR	SYSTEM	Passwords repository server %s communication error.
FSE0093	ERROR	SYSTEM	Error connecting to Thycotic server %s: incorrect URL in configuration.
FSE0094	ERROR	SYSTEM	Error connecting to Thycotic server %s: incorrect protocol specified.
FSE0095	ERROR	SYSTEM	Error fetching password from Thycotic server %s: unable to get sessid for user %s.
FSE0096	ERROR	SYSTEM	Error fetching password from Thycotic server %s.
FSE0097	ERROR	SYSTEM	Error fetching password for %s from Thycotic server %s: unable to get secretid for server %s.
FSE0098	ERROR	SYSTEM	Error fetching password for %s from Thycotic server %s: unable to get password for user %s for the %s server.
FUE0099	ERROR	USER	Connection terminated.
FUE0101	ERROR	USER	Unable to find matching HTTP connection.
FUI0102	INFO	USER	Session terminated by system administrator.
FUE0103	ERROR	USER	HTTP connection error.
FUI0104	INFO	USER	%s connection terminated.
FUI0105	INFO	USER	HTTP session inactive, terminating.
FUE0106	ERROR	USER	Authentication failed: %s.
FUW0107	WARNING	USER	Invalid inactivity timeout, falling back to %d seconds.
FUE0108	ERROR	USER	MySQL connection error.
FUI0109	INFO	USER	MySQL connection terminated.
FUE0112	ERROR	USER	RDP connection error.
FUE0113	ERROR	USER	TLS Security configured, but missing TLS private key.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FUE0115	ERROR	USER	Standard RDP Security configured, but missing private key.
FUE0116	ERROR	USER	TLS certificate verification failed.
FUE0117	ERROR	USER	RSA key verification failed.
FUI0118	INFO	USER	Successfully authenticated against server %s.
FUI0119	INFO	USER	Successfully authenticated against server %s as user %s using %s.
FUI0120	INFO	USER	Successfully authenticated against server %s as user %s within domain %s using %s.
FUI0121	INFO	USER	An anonymous user successfully authenticated against server %s.
FUI0122	INFO	USER	An anonymous user successfully authenticated against server %s as user %s.
FUI0123	INFO	USER	An anonymous user successfully authenticated against server %s as user %s within domain %s.
FUE0124	ERROR	USER	SSH connection error.
FUE0129	ERROR	USER	Failed to authenticate against server %s as user %s using %s.
FUE0130	ERROR	USER	Failed to authenticate against server %s as user %s using %s (received %s).
FUW0131	WARNING	USER	Functionality %s is not allowed.
FUE0133	ERROR	USER	MSSQL connection error.
FUE0134	ERROR	USER	TN3270 connection error.
FUE0135	ERROR	USER	Unknown TN3270 command: %02x.
FUE0136	ERROR	USER	Telnet connection error.
FSE0137	ERROR	SYSTEM	Unable to read private key.
FSE0138	ERROR	SYSTEM	Server's certificate does not match configured certificate.
FUE0139	ERROR	USER	VNC connection error.
FUE0140	ERROR	USER	Client version: %s is higher than the client integrated in Fudo: %s.
FUE0141	ERROR	USER	VNC connection error. Client answered with unsupported security type: %hhu.
FUI0143	INFO	USER	VNC connection closed: %s.
FUE0144	ERROR	USER	User %s failed to authorize logging in from address: %s.
FUE0146	ERROR	USER	User %s failed to authenticate logging in from address: %s.
FSE0153	ERROR	SYSTEM	Session indexing failure.
FSE0154	ERROR	SYSTEM	Session conversion failure for session %s.
FAI0157	INFO	ADMIN	User %s %s failover configuration.
FAI0158	INFO	ADMIN	User %s added node %s.
FAI0159	INFO	ADMIN	User %s changed %s in node %s.
FAI0160	INFO	ADMIN	User %s deleted node %s.
FAI0161	INFO	ADMIN	User %s disconnected node from the cluster.
FAI0162	INFO	ADMIN	Cluster has no active nodes. Cluster will be disabled.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0163	INFO	ADMIN	User %s created new cluster - %s.
FAI0164	INFO	ADMIN	User %s attached current node to cluster.
FAI0166	INFO	ADMIN	User %s restored original logo for protocol %s.
FAI0167	INFO	ADMIN	User %s changed logo for protocol %s.
FAI0168	INFO	ADMIN	User %s confirmed sensitive feature %s.
FAI0169	INFO	ADMIN	User %s removed confirmation for sensitive feature %s.
FAI0170	INFO	ADMIN	User %s changed following notifications settings: %s.
FAI0171	INFO	ADMIN	User %s enabled email notifications.
FAI0172	INFO	ADMIN	User %s disabled email notifications.
FAI0173	INFO	ADMIN	User %(username)s is upgrading Fudo.
FAI0174	INFO	ADMIN	User %(username)s upgraded Fudo.
FAI0175	INFO	ADMIN	User %(username)s uploaded new upgrade image (version: %(version)s, size: %(size)d).
FAI0176	INFO	ADMIN	User %(username)s deleted upgrade files.
FAI0177	INFO	ADMIN	User %s uploaded license file.
FAW0178	WARNING	ADMIN	User %(username)s triggered system restart.
FAW0179	WARNING	ADMIN	User %(username)s triggered system shutdown.
FAW0180	WARNING	ADMIN	User %s %s remote SSH access.
FAW0181	WARNING	ADMIN	User %(username)s changed timestamping settings.
FAW0182	WARNING	ADMIN	User %(username)s uploaded new PKCS12 file.
FAW0183	WARNING	ADMIN	User %(username)s changed timestamping provider to %(provider)s.
FAW0184	WARNING	ADMIN	User %(username)s %(action)s timestamping.
FAI0185	INFO	ADMIN	User %s imported system configuration.
FAI0186	INFO	ADMIN	User %s requested system configuration export.
FAI0187	INFO	ADMIN	User %s added NTP server %s.
FAI0188	INFO	ADMIN	User %s removed NTP server %s.
FAE0189	ERROR	ADMIN	Error saving NTP servers: "%s".
FAI0190	INFO	ADMIN	User %(username)s changed date & time from %(old_date)s to %(new_date)s.
FAI0191	INFO	ADMIN	User %s changed timezone to %s.
FAI0192	INFO	ADMIN	User %s changed Fudo HTTPS private key and certificate.
FAI0193	INFO	ADMIN	User %s %s SSH access.
FAI0194	INFO	ADMIN	User %s requested service data.
FAI0195	INFO	ADMIN	User %s added %s to %s for %s %s.
FAI0196	INFO	ADMIN	User %s removed %s from %s for %s %s.
FAI0197	INFO	ADMIN	User %s changed %s from %s to %s for %s %s.
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.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0200	INFO	ADMIN	User %(username)s %(new_cluster)s cluster address on %(new_inet)s/%(new_netmask)s address on interface %(interface)s.
FAI0201	INFO	ADMIN	User %(username)s %(new_management)s management on %(new_inet)s/%(new_netmask)s address on interface %(interface)s.
FAI0202	INFO	ADMIN	User %(username)s deleted IP address %(old_ip)s from interface %(interface)s.
FAI0203	INFO	ADMIN	User %(username)s %(action)s interface %(interface)s.
FAI0204	INFO	ADMIN	User %(username)s added member %(member)s to bridge %(interface)s.
FAI0205	INFO	ADMIN	User %(username)s removed member %(member)s from bridge %(interface)s.
FAI0206	INFO	ADMIN	User %(username)s enabled spanning tree propagation on bridge %(interface)s.
FAI0207	INFO	ADMIN	User %(username)s disabled spanning tree propagation on bridge %(interface)s.
FAI0208	INFO	ADMIN	User %(username)s changed VLAN %(interface)s parent interface from %(old_parent_interface)s to %(new_parent_interface)s.
FAI0209	INFO	ADMIN	User %(username)s changed VLAN %(interface)s ID from %(old_vlan)s to %(new_vlan)s.
FAI0210	INFO	ADMIN	User %s deleted interface %s.
FAI0211	INFO	ADMIN	User %s changed LDAP synchronization settings.
FAW0213	WARNING	ADMIN	LDAP error during fetching groups: %s.
FAI0214	INFO	ADMIN	User %s enforced full LDAP synchronization.
FAI0215	INFO	ADMIN	User %s disabled events logging on syslog servers.
FAI0216	INFO	ADMIN	User %s removed syslog server: %s:%s.
FAI0217	INFO	ADMIN	User %s added syslog server: %s:%s.
FAI0218	INFO	ADMIN	User %s removed syslog server %s.
FAI0219	INFO	ADMIN	User %s changed remote log dispatch settings.
FAI0220	INFO	ADMIN	User %s changed network interfaces settings.
FAI0221	INFO	ADMIN	User %s changed hostname from %s to %s.
FAI0222	INFO	ADMIN	User %s added DNS server IP address %s.
FAI0223	INFO	ADMIN	User %s removed DNS server IP address %s.
FAI0224	INFO	ADMIN	User %s added new route for network %s with gateway %s.
FAI0225	INFO	ADMIN	User %s changed gateway for network %s from %s to %s.
FAI0226	INFO	ADMIN	User %s deleted network %s with gateway %s.
FAI0227	INFO	ADMIN	User %s (%s) terminated session.
FAI0228	INFO	ADMIN	Anonymous user from IP address %s with access rights granted by user %s joined session.
FAI0229	INFO	ADMIN	User %s from IP address %s joined session.
FAI0230	INFO	ADMIN	User %s (%s) suspended session.
FAI0231	INFO	ADMIN	User %s (%s) resumed session.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAE0232	ERROR	ADMIN	MySQL session playback error.
FAI0233	INFO	ADMIN	Anonymous user from IP address %s accessed shared session %s with key %s.
FAI0234	INFO	ADMIN	User %s from IP address %s accessed session %s.
FAI0235	INFO	ADMIN	User %s %s comment %d for session.
FAI0236	INFO	ADMIN	User %s generated key %s with %s access.
FAI0237	INFO	ADMIN	User %s is viewing user input for session.
FAI0238	INFO	ADMIN	User %s blocked server %s.
FAI0239	INFO	ADMIN	User %s unblocked server %s.
FAI0247	INFO	ADMIN	User %s deleted server %s.
FAI0253	INFO	ADMIN	User %s deleted session.
FAI0254	INFO	ADMIN	User %s requested OCR processing for session.
FAW0255	WARNING	ADMIN	User %s tried to disable a non-exisitent sharing key for session.
FAI0256	INFO	ADMIN	User %s disabled anonymous access key %s for session.
FAI0259	INFO	ADMIN	User %s deleted download %s.
FAI0260	INFO	ADMIN	User %s downloaded file %s for session %s.
FAI0261	INFO	ADMIN	Anonymous user from IP address %s terminated shared session with key %s.
FAI0262	INFO	ADMIN	User %s terminated session.
FAI0263	INFO	ADMIN	User %s blocked user %s.
FSW0266	WARNING	SYSTEM	Failed to send email.
FSE0267	ERROR	SYSTEM	Error generating report %d: %s.
FAI0268	INFO	ADMIN	User %s deleted report “%s”.
FAI0270	INFO	ADMIN	Report {} created by user {}.
FAI0276	INFO	ADMIN	User %s unblocked user %s.
FAI0277	INFO	ADMIN	User %s deleted user %s.
FAI0279	INFO	ADMIN	User %s changed user %s.
FAI0281	INFO	ADMIN	User %s logged out from Fudo administration panel.
FUI0282	INFO	USER	User %s successfully changed his password.
FSE0283	ERROR	SYSTEM	Unable to process pattern: %s
FSW0284	WARNING	SYSTEM	Pattern %s matched on %s with priority %s in session.
FSE0285	ERROR	SYSTEM	Unable to read certificate.
FSE0286	ERROR	SYSTEM	No peer certificate received.
FUI0289	INFO	USER	MSSQL connection terminated.
FAI0299	INFO	ADMIN	User %s created server %s.
FAI0300	INFO	ADMIN	User %s changed server %s.
FAI0303	INFO	ADMIN	User %s created user %s with role %s.
FAI0304	INFO	ADMIN	User %s modified %s for %s %s.
FUE0305	ERROR	USER	Client connection closed: encryption is not available.
FUE0306	ERROR	USER	Client connection closed.
FUE0314	ERROR	USER	Invalid pixel format.
FSE0330	ERROR	SYSTEM	Bad login field configured on LDAP server %s. Error while processing user %s.
FSI0332	INFO	SYSTEM	User %s will be blocked.
FSI0333	INFO	SYSTEM	User %s will be unblocked.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSI0335	INFO	SYSTEM	User %s synchronized from LDAP server %s.
FSI0339	INFO	SYSTEM	User %s (%s) was removed. Reason: user was not in any of synchronized groups.
FSI0340	INFO	SYSTEM	Full synchronization from LDAP server %s started.
FSI0342	INFO	SYSTEM	User %s will be resynchronized from server %s.
FSW0344	WARNING	SYSTEM	Connecting to LDAP server error: %s.
FSI0345	INFO	SYSTEM	Successfully fetched password from %s.
FUE0346	ERROR	USER	Client sent a packet bigger than %u bytes.
FSE0348	ERROR	SYSTEM	Unable to get configuration settings.
FAI0349	INFO	ADMIN	Anonymous user from IP address %s with access rights granted by user %s left session.
FAI0350	INFO	ADMIN	User %s from IP address %s left session.
FAI0354	INFO	ADMIN	User %(username)s deleted upgrade snapshot.
FUW0356	WARNING	USER	Unsupported X11 extension: %s.
FUW0357	WARNING	USER	Server uses higher resolution than the current limit: %dx%d.
FUW0358	WARNING	USER	Server uses higher color depth than the current limit: %d bpp.
FUE0359	ERROR	USER	Server rejected X11 connection: %.*s.
FUE0360	ERROR	USER	Server requires unsupported X11 authentication: %.*s.
FSW0361	WARNING	SYSTEM	Fudo started.
FSE0362	ERROR	SYSTEM	Unable to propagate ARP.
FUE0363	ERROR	USER	User %s has no access to host %s.
FUI0364	INFO	USER	RDP server sent a redirection packet.
FUI0370	INFO	USER	User %s authenticated using OTP logged in from IP address: %s.
FUW0373	WARNING	USER	Session has been terminated due to exceeding the time window defined in a time policy for the user %s and the safe %s.
FSI0374	INFO	SYSTEM	Established %s connection from %s to %s.
FSE0376	ERROR	SYSTEM	Unable to add listener %s because %s is listening on the same IP address and port.
FSE0378	ERROR	SYSTEM	Unable to establish connection: server not found, user not found or user has no access to the server (listener: %s, user: %s).
FSE0379	ERROR	SYSTEM	Unable to establish connection: transparent server (tcp://%s) not found or cannot be reached through listener (listener: %s, user: %s).
FSE0380	ERROR	SYSTEM	Unable to authenticate user %s: server %s is blocked.
FSE0381	ERROR	SYSTEM	Unable to authenticate user %s: account not found.
FSE0382	ERROR	SYSTEM	Unable to authenticate user %s: account %s is blocked.
FSE0383	ERROR	SYSTEM	Unable to authenticate user %s%s%s: user not found.
FSE0384	ERROR	SYSTEM	Unable to authenticate user %s: user is blocked.
FSE0385	ERROR	SYSTEM	Unable to authenticate user %s: safe not found.
FSE0386	ERROR	SYSTEM	Unable to authenticate user %s: safe %s is blocked.
FSI0387	INFO	SYSTEM	Password for account %s verified successfully.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSI0389	INFO	SYSTEM	Password for account %s changed successfully.
FAI0393	INFO	ADMIN	User %s displayed password history for account %s.
FAI0394	INFO	ADMIN	User %s displayed historical password for account %s changed at %s.
FAI0395	INFO	ADMIN	User %s displayed current password for account %s.
FAI0396	INFO	ADMIN	User %s blocked safe %s.
FAI0397	INFO	ADMIN	User %s unblocked safe %s.
FAI0398	INFO	ADMIN	User %s deleted safe %s.
FAI0399	INFO	ADMIN	User %s changed safe %s.
FAI0400	INFO	ADMIN	User %s created safe %s.
FAI0401	INFO	ADMIN	User %s blocked account %s.
FAI0402	INFO	ADMIN	User %s unblocked account %s.
FAI0403	INFO	ADMIN	User %s deleted account %s.
FAI0406	INFO	ADMIN	User %s blocked listener %s.
FAI0407	INFO	ADMIN	User %s unblocked listener %s.
FAI0408	INFO	ADMIN	User %s deleted listener %s.
FAI0411	INFO	ADMIN	User %s blocked password change policy %s.
FAI0412	INFO	ADMIN	User %s unblocked password change policy %s.
FAI0413	INFO	ADMIN	User %s deleted password change policy %s.
FAI0414	INFO	ADMIN	User %s changed password change policy %s.
FAI0415	INFO	ADMIN	User %s created password change policy %s.
FSI0416	INFO	SYSTEM	Connection between safe %s and user %s has been removed.
FSI0417	INFO	SYSTEM	Connection between safe %s and user %s has been added.
FSI0418	INFO	SYSTEM	User %s was removed from safes %s.
FSE0420	ERROR	SYSTEM	Unable to authenticate user %s against server %s.
FAI0423	INFO	ADMIN	User %s assigned account %s to safe %s.
FAI0424	INFO	ADMIN	User %s unassigned account %s from safe %s.
FAI0425	INFO	ADMIN	User %s assigned authentication method %s to user %s.
FAI0426	INFO	ADMIN	User %s unassigned authentication mathod %s from user %s.
FAI0427	INFO	ADMIN	User %s changed authentication mathod %s assigned to user %s.
FAI0428	INFO	ADMIN	User %s assigned user %s to safe %s.
FAI0429	INFO	ADMIN	User %s unassigned user %s from safe %s.
FAI0430	INFO	ADMIN	User %s blocked password changer %s.
FAI0431	INFO	ADMIN	User %s unblocked password changer %s.
FAI0432	INFO	ADMIN	User %s deleted password changer %s.
FAI0433	INFO	ADMIN	User %s changed password changer %s.
FAI0434	INFO	ADMIN	User %s created password changer %s.
FSW0435	WARNING	SYSTEM	Password changer timed out for account %s.
FAW0438	WARNING	ADMIN	User %s authenticated using new token while the old one still exists.
FAW0439	WARNING	ADMIN	User %s authenticated using old token.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0444	INFO	ADMIN	User %s created policy %s.
FAI0445	INFO	ADMIN	User %s deleted policy %s.
FAI0446	INFO	ADMIN	User %s changed policy %s.
FAI0449	INFO	ADMIN	User %s created regexp %s.
FAI0450	INFO	ADMIN	User %s deleted regexp %s.
FAI0451	INFO	ADMIN	User %s changed regexp %s.
FAI0460	INFO	ADMIN	User %s displayed current password for account %s. Reason: %s
FSE0461	ERROR	SYSTEM	Invalid data from %s LDAP server.
FAI0462	INFO	ADMIN	User {} created redundancy group {}.
FAI0463	INFO	ADMIN	User {} deleted redundancy group {}.
FUW0465	WARNING	USER	Establishing new connections has been disabled.
FSE0466	ERROR	SYSTEM	Fudo versions do not conform.
FUE0467	ERROR	USER	Client tried to authenticate using an invalid UTF-8 login.
FSI0468	INFO	SYSTEM	A passphrase used to decrypt disks was changed.
FSE0476	ERROR	SYSTEM	ZVOL with encryption key does not exist.
FAI0481	INFO	ADMIN	New OTP for user %s has been generated.
FSW0482	WARNING	SYSTEM	Unable to verify password for account %s.
FAI0487	INFO	ADMIN	User %s requested timestamping for session.
FAI0488	INFO	ADMIN	User %s requested timestamping for account.
FSI0489	INFO	SYSTEM	Label %s is not defined on this node, skipping listener %s.
FAI0490	INFO	ADMIN	User %s created external authentication %s.
FAI0491	INFO	ADMIN	User %s changed external authentication %s: %s.
FAI0492	INFO	ADMIN	User %s deleted external authentication %s.
FSE0493	ERROR	SYSTEM	Unable to establish connection to server %s (%s): label %s not defined on this node.
FSI0494	INFO	SYSTEM	Label %s not defined on this node, skipping external authentication %s.
FSE0500	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to connect to database.
FSE0502	ERROR	SYSTEM	Database error.
FSE0510	ERROR	SYSTEM	Communication error with cluster node %s (%s): initial replication failed.
FAW0514	WARNING	ADMIN	User %s of role %s tried to view %s, but has insufficient privileges for this action.
FSW0522	WARNING	SYSTEM	Rollback to ${_version} failed.
FSW0523	WARNING	SYSTEM	Upgrade to ${_version} failed.
FSW0524	WARNING	SYSTEM	Rollback to ${_version} succeeded.
FSW0525	WARNING	SYSTEM	Upgrade to ${_version} succeeded.
FSE0526	ERROR	SYSTEM	Error communicating with bypass card. Error setting nextboot mode.
FSE0527	ERROR	SYSTEM	Error communicating with bypass card. Error setting bpe mode.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSE0528	ERROR	SYSTEM	Error communicating with bypass card. Error switching card mode.
FSE0529	ERROR	SYSTEM	Error communicating with bypass card.
FAI0530	INFO	ADMIN	User %s enabled snmp.
FAI0531	INFO	ADMIN	User %s disabled snmp.
FSW0532	WARNING	SYSTEM	External storage is unavailable.
FSI0534	INFO	SYSTEM	External storage attached.
FSE0535	ERROR	SYSTEM	External storage is unavailable in this configuration.
FSW0536	WARNING	SYSTEM	External storage detached.
FAI0538	INFO	ADMIN	Set external storage connection mode to {mode}.
FAI0539	INFO	ADMIN	Set configured WWN to {wwn}, external storage connection mode to {mode}.
FSW0540	WARNING	SYSTEM	Found ${cdisk} paths to fiber channel ${wwn} from ${cscbus} devices.
FSW0541	WARNING	SYSTEM	Retention module was unable to move session ${_sessid}.
FAI0542	INFO	ADMIN	User %s assigned account %s, listener %s to safe %s.
FAI0543	INFO	ADMIN	User %s unassigned account %s, listener %s from safe %s.
FSW0545	WARNING	SYSTEM	Unable to change password for account %s.
FAI0549	INFO	ADMIN	User %s approved ticket %s requesting an access for user %s to safe %s.
FAI0550	INFO	ADMIN	User %s rejected ticket %s requesting an access for user %s to safe %s.
FAI0551	INFO	ADMIN	User %(username)s added member %(member)s to lagg %(interface)s.
FAI0552	INFO	ADMIN	User %(username)s removed member %(member)s from lagg %(interface)s.
FSE0553	ERROR	SYSTEM	Unable to extract public key from CA.
FUE0554	ERROR	USER	SFTP server uses an unsupported version %u.
FSE0560	ERROR	SYSTEM	Session has not been approved nor rejected.
FAI0562	INFO	ADMIN	User %s rejected session %s. Reason: %s.
FAI0563	INFO	ADMIN	User %s rejected session %s.
FAI0564	INFO	ADMIN	User: {} tried to accept session: {} but it was accepted by:
FAI0565	INFO	ADMIN	User: {} rejected session: {}
FAI0566	INFO	ADMIN	User: {} tried to reject session: {} but it was accepted by:
FAI0567	INFO	ADMIN	User: {} tried to reject session: {} but it was rejected by:
FAI0568	INFO	ADMIN	User: {} accepted session: {}
FAI0569	INFO	ADMIN	User: {} tried to accept session: {} but it was rejected by:
FAI0570	INFO	ADMIN	User %s approved session %s.
FSI0571	INFO	SYSTEM	Proxy connection closed.
FSE0572	ERROR	SYSTEM	Proxy connection error.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSE0573	ERROR	SYSTEM	Client sent an invalid token.
FSE0574	ERROR	SYSTEM	Unable to resolve hostname ${ip} to address.
FSE0575	ERROR	SYSTEM	Unable to convert raw file to pcap.
FAI0581	INFO	ADMIN	User %s changed domain search path from %s to %s.
FSE0583	ERROR	SYSTEM	LDAP authentication error: unable to connect to %s.
FAI0584	INFO	ADMIN	User %s changed data on user portal.
FAI0585	INFO	ADMIN	User %s changed User portal HTTPS private key and certificate.
FAW0586	WARNING	ADMIN	Missing safe attributes: %s
FSE0588	ERROR	SYSTEM	Failed to replicate an object to node %s (%s): %s.
FSE0589	ERROR	SYSTEM	Communication error with cluster node %s (%s): database %s transaction failure.
FSE0590	ERROR	SYSTEM	Communication error with cluster node %s: unable to establish connection.
FSE0591	ERROR	SYSTEM	Communication error with cluster node %s: unable to obtain serial number.
FSE0592	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to obtain public key.
FAI0594	INFO	ADMIN	User %s exported master key.
FUE0595	ERROR	USER	User %s authorization failed: %s.
FAI0597	INFO	ADMIN	User %s enabled failure login attempts limit.
FAI0598	INFO	ADMIN	User %s disabled failure login attempts limit.
FSI0599	INFO	SYSTEM	Fudo is successfully re-encrypted using key %s.
FUI0601	INFO	USER	VNC connection terminated.
FSW0602	WARNING	SYSTEM	Retention module was unable to fetch the current time.
FSI0603	INFO	SYSTEM	Finished full synchronization from LDAP server %s.
FAI0604	INFO	ADMIN	User %s created IP label %s.
FAI0605	INFO	ADMIN	User %s changed IP label %s.
FAI0606	INFO	ADMIN	User %s deleted IP label %s.
FAI0607	INFO	ADMIN	User %s restored original logo for portal.
FAI0608	INFO	ADMIN	User %s changed logo for portal.
FSI0609	INFO	SYSTEM	Successfully generated new master key: %s.
FAI0610	INFO	ADMIN	User %s invalidated master key.
FAI0613	INFO	ADMIN	User %s canceled timestamping for session.
FSI0614	INFO	SYSTEM	System image version %s is being processed.
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}.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0623	INFO	ADMIN	User %s enabled different password than current setting.
FAI0624	INFO	ADMIN	User %s disabled different password than current setting.
FSI0626	INFO	SYSTEM	Initial logs replication to cluster node %s (%s) completed.
FSE0633	ERROR	SYSTEM	Protocol %s doesn't support multistep authentication.
FSE0634	ERROR	SYSTEM	Authentication failed: User %s failed to authenticate using %s.
FSW0639	WARNING	SYSTEM	Data storage full, establishing connections has been disabled. Free up some storage space to re-enable the session monitoring functionality.
FUE0640	ERROR	USER	Failed to authenticate against the server as user %s using %s: %s
FSW0641	WARNING	SYSTEM	Establishing connections has been re-enabled.
FSW0642	WARNING	SYSTEM	Trying to finish all active sessions because of full filesystem.
FAI0644	INFO	ADMIN	User %s changed user portal SSO settings.
FSE0645	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to obtain time.
FSE0646	ERROR	SYSTEM	Communication error with cluster node %s (%s): time difference too large (%ds).
FUW0647	WARNING	USER	Cannot establish new connections because the capacity of the filesystem has been reached.
FSW0649	WARNING	SYSTEM	More than one server address %s.
FUE0654	ERROR	USER	Client sent an unexpected URL: %s.
FSI0658	INFO	SYSTEM	AI started training quantitative model "%s-%s".
FSE0659	ERROR	SYSTEM	AI training quantitative model "%s-%s" failed: "%s".
FSI0660	INFO	SYSTEM	AI finished training quantitative model "%s-%s".
FSE0661	ERROR	SYSTEM	AI training failed for "%s-%s".
FSI0662	INFO	SYSTEM	AI started training corpus "%s".
FSE0663	ERROR	SYSTEM	AI training corpus "%s" failed: "%s".
FSI0664	INFO	SYSTEM	AI finished training corpus "%s".
FSI0665	INFO	SYSTEM	AI started training model "%s".
FSE0666	ERROR	SYSTEM	AI training model "%s" failed: "%s".
FSI0667	INFO	SYSTEM	AI finished training model "%s". Model weight: %s
FSE0668	ERROR	SYSTEM	AI training failed for "%s".
FSW0669	WARNING	SYSTEM	AI postponed training quantitative model "%s-%s". Not enough training data.
FSW0670	WARNING	SYSTEM	AI postponed training corpus "%s". Not enough training data.
FSW0671	WARNING	SYSTEM	AI postponed training model "%s". Not enough training data.
FAI0672	INFO	ADMIN	User %s upgraded plugin %s.
FUI0673	INFO	USER	Client requested too small or too large terminal size: %dx%d. Changing to %dx%d.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FUW0674	WARNING	USER	No keys configured, skipping server authentication.
FSW0675	WARNING	SYSTEM	Unable to remove session %s on node %s.
FAI0676	INFO	ADMIN	User %s updated note for account %s.
FUI0677	INFO	USER	Portal user %s updated note for account %s.
FAI0678	INFO	ADMIN	User %s created note for account %s.
FUI0679	INFO	USER	Portal user %s created note for account %s.
FSE0681	ERROR	SYSTEM	Upgrade status could not be determined.
FSI0682	INFO	SYSTEM	Retention module will not be run during upgrade preparations.
FUW0683	WARNING	USER	Server %s accepted public key for user %s without a signature!
FUI0684	INFO	USER	User %s authenticated using SSH key logged in from address: %s.
FAI0686	INFO	ADMIN	User %s loaded new password changer %s.
FSI0688	INFO	SYSTEM	Disconnected callhome tunnel.
FSE0691	ERROR	SYSTEM	Failed to expand external storage.
FAI0692	INFO	ADMIN	User %s changed node name from %s to %s.
FUW0694	WARNING	USER	Session has been terminated: time limit exceeded (user %s, safe %s).
FUW0695	WARNING	USER	Session has been terminated: inactivity limit exceeded (user %s, safe %s).
FUI0698	INFO	USER	User %s authenticated using SMS token logged in from address: %s.
FUE0700	ERROR	USER	Unable to send one-time password to user %s: %s.
FUI0703	INFO	USER	User %s authenticated using DUO/Push logged in from address: %s.
FUE0705	ERROR	USER	Unable to send DUO/%s to user %s: %s.
FAI0706	INFO	ADMIN	User %s enabled send diagnostics setting.
FAI0707	INFO	ADMIN	User %s disabled send diagnostics setting.
FSW0708	WARNING	SYSTEM	AI Identified suspicious activity in session %s.
FSI0709	INFO	SYSTEM	AI Assessed activity in session %s with threat level %s.
FUE0710	ERROR	USER	Unable to change Active Directory password for user %s (domain %s): %s.
FUE0711	ERROR	USER	User %s OTP authentication failed: %s.
FSI0712	INFO	SYSTEM	Azure backup snapshot started.
FSI0713	INFO	SYSTEM	Azure backup snapshot finished.
FSW0714	WARNING	SYSTEM	Additional space (%s) required to continue the upgrade.
FAI0715	INFO	ADMIN	User %s disabled sending debug logs to syslog server.
FUW0716	WARNING	USER	SSH connection attempt without ProxyJump.
FSE0717	ERROR	SYSTEM	Browser could not establish a connection due to exceeding a timeout of %ds.
FAI0721	INFO	ADMIN	User %s added remote application %s to server %s.
FAI0722	INFO	ADMIN	User %s removed remote application %s from server %s.
FAI0723	INFO	ADMIN	User %s changed remote application %s in server %s.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FUE0724	ERROR	USER	Too high resolution requested (%ux%u), session dropped.
FAI0729	INFO	ADMIN	User %s changed management SSO settings.
FAI0731	INFO	ADMIN	User %s %s API health check setting.
FSE0734	ERROR	SYSTEM	Unable to authenticate user %s: safe %s requires access acceptance.
FUW0735	WARNING	USER	Session has been terminated: ticket for user %s to account %s has expired.
FSI0745	INFO	SYSTEM	%zu accounts onboarded.
FSI0746	INFO	SYSTEM	%zu accounts quarantined.
FSI0747	INFO	SYSTEM	Scanner %jd/%s removed account %s.
FSI0748	INFO	SYSTEM	Scanner %jd/%s created account %s.
FSE0749	ERROR	SYSTEM	%s %s (pid %d) failed with status %d.
FSE0750	ERROR	SYSTEM	%s %s (pid %d) was terminated by signal %d.
FAI0751	INFO	ADMIN	User {} downloaded {}.
FSE0752	ERROR	SYSTEM	Client sent an invalid request.
FSI0753	INFO	SYSTEM	User %s is waiting for session approval.
FAI0754	INFO	ADMIN	User %s enabled Callhome.
FAI0755	INFO	ADMIN	User %s disabled Callhome.
FAI0756	INFO	ADMIN	User %s requested session %s from archive.
FAW0757	WARNING	ADMIN	Malformed upgrade package: %s
FSE0758	ERROR	SYSTEM	Max number of retries exceeded. Could not remove sessions %s.
FSW0759	WARNING	SYSTEM	Could not remove sessions %s.
FSI0760	INFO	SYSTEM	%s until removal retry for sessions %s.
FAE0761	ERROR	ADMIN	Failed authentication attempt from address %s.
FUI0762	INFO	USER	User %s authenticated using SSO token logged in from address: %s.
FUI0763	INFO	USER	User %s authenticated using X509 certificate logged in from address: %s.
FUE0764	ERROR	USER	User failed to authenticate using SSO token and logging in from address: %s.
FUE0765	ERROR	USER	User failed to authenticate using X509 certificate and logging in from address: %s.
FAE0766	ERROR	ADMIN	Error parsing %s file at position %s.
FAI0767	INFO	ADMIN	User %s changed password complexity settings.
FAI0768	INFO	ADMIN	User %s changed User CA certificates.
FAI0775	INFO	ADMIN	User %s added relation between nodes %s -> %s.
FAI0776	INFO	ADMIN	User %s removed relation between nodes %s -> %s.
FAI0777	INFO	ADMIN	User %s changed settings for relation between nodes %s -> %s.
FSW0779	WARNING	SYSTEM	Health check '%s' failed.
FAI0780	INFO	ADMIN	User %s enabled retention for session.
FAI0781	INFO	ADMIN	User %s disabled retention for session.
FAI0782	INFO	ADMIN	Interface discovery while configuring external storage: {interfaces}.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FUI0783	INFO	USER	User %s authenticated using OATH/%s logged in from address: %s.
FUW0784	WARNING	USER	Functionality %s not allowed.
FAI0785	INFO	ADMIN	User %s enabled denying new connections.
FAI0786	INFO	ADMIN	User %s disabled denying new connections.
FAI0787	INFO	ADMIN	User %s changed password changer active node.
FSE0788	ERROR	SYSTEM	Unable to parse address %s.
FSE0789	ERROR	SYSTEM	Unable to find address %s.
FUE0790	ERROR	USER	User %s failed to authenticate after %d %s attempts, disconnecting.
FUE0791	ERROR	USER	User %s failed to authenticate after presenting %d keys, disconnecting.
FSW0793	WARNING	SYSTEM	DNS is slow. It took %jums to resolve %s.
FAI0796	INFO	ADMIN	User %s enabled SNMP TRAP.
FAI0797	INFO	ADMIN	User %s disabled SNMP TRAP.
FSE0798	ERROR	SYSTEM	OpenID Connect (%s) configuration error: %s.
FSE0799	ERROR	SYSTEM	OpenID Connect (%s) request failed: %s.
FSE0801	ERROR	SYSTEM	Multiple users with e-mail %s found during OpenID Connect (%s) authentication.
FUI0802	INFO	USER	User %s authenticated using OpenID Connect (%s).
FSW0803	WARNING	SYSTEM	Unable to send SNMP TRAP.
FUE0804	ERROR	USER	User's %s OATH/%s token might have been cloned (current counter: %ju, new counter: %ju).
FUI0805	INFO	USER	User %s presence confirmed during SSH authentication.
FUE0806	ERROR	USER	User %s not present during SSH authentication.
FUE0807	ERROR	USER	User's %s SSH key may have been cloned (current counter: %ju, new counter: %ju).
FUI0808	INFO	USER	Verification by the user %s confirmed during SSH authentication.
FUE0809	ERROR	USER	No verification by the user %s during SSH authentication.
FAI0810	INFO	ADMIN	User %s deleted undelivered email notifications. Recipient list: %s
FAI0811	INFO	ADMIN	User %s resent undelivered email notifications. Recipient list: %s
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.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FSW0818	WARNING	SYSTEM	The number of active users exceeds the “activeusers” limit from the license.
FSW0819	WARNING	SYSTEM	Server is not accessible through listener %s.
FSE0821	ERROR	SYSTEM	Unable to establish connection: server not found (listener: %s, user: %s, target: %s, port: %u).
FAI0822	INFO	ADMIN	User %s added KDC server %s with domain %s.
FAI0823	INFO	ADMIN	User %s removed KDC server %s with domain %s.
FAE0824	ERROR	ADMIN	Error saving KDC servers: “%s”.
FSW0825	WARNING	SYSTEM	User %s not synchronized from LDAP server %s, validation error: %s.
FAI0826	INFO	ADMIN	User %s granted access to %s for %s.
FAI0827	INFO	ADMIN	User %s removed access to %s for %s.
FUE0828	ERROR	USER	Server’s certificate does not match configured certificate.
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 {account.name}. {account=account.id}
FAI0840	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the account {old.name} to: {attribute.value}. {account=old.id}
FAI0841	INFO	ADMIN	Administrator {subject.name} deleted account {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}

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0844	INFO	ADMIN	Administrator {subject.name} deleted listener {listener.name}. {listener=listener.id}
FAI0845	INFO	ADMIN	Administrator {subject.name} created pool {pool.name}. {pool=pool.id}
FAI0846	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for pool {old.name} to: {attribute.value}. {pool=old.id}
FAI0847	INFO	ADMIN	Administrator {subject.name} deleted pool {pool.name}. {pool=pool.id}
FAI0848	INFO	ADMIN	Administrator {subject.name} created safe {safe.name}. {safe=safe.id}
FAI0849	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for safe {old.name} to: {attribute.value}. {safe=old.id}
FAI0850	INFO	ADMIN	Administrator {subject.name} deleted safe {safe.name}. {safe=safe.id}
FAI0851	INFO	ADMIN	Administrator {subject.name} created server {server.name}. {server=server.id}
FAI0852	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for server {old.name} to: {attribute.value}. {server=old.id}
FAI0853	INFO	ADMIN	Administrator {subject.name} deleted server {server.name}. {server=server.id}
FAI0854	INFO	ADMIN	Administrator {subject.name} created {user.role} {user.name}. {user=user.id}
FAI0855	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for {old.role} {old.name} to: {attribute.value}. {user=old.id}
FAI0856	INFO	ADMIN	Administrator {subject.name} deleted {user.role} {user.name}. {user=user.id}
FSW0857	WARNING	SYSTEM	Scanner %jd/%s can not remove server %s: %s
FAI0858	INFO	ADMIN	Administrator {subject.name} created a grant, giving {account_grant.to_user_role} {account_grant.to_user_name} access to account {account_grant.for_account_name}. {user=account_grant.to_user_id,account=account_grant.for_ac
FAI0859	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {account_grant.to_user_role} {account_grant.to_user_name} access to account {account_grant.for_account_name}. {user=account_grant.to_user_id,account=account_grant.for_ac
FAI0860	INFO	ADMIN	Administrator {subject.name} created a grant, giving {listener_grant.to_user_role} {listener_grant.to_user_name} access to listener {listener_grant.for_listener_name}. {user=listener_grant.to_user_id,listener=listener_grant.for_list

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0861	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {listener_grant.to_user_role} {listener_grant.to_user_name} access to listener {listener_grant.for_listener_name}. {user=listener_grant.to_user_id,listener=listener_grant.for_list
FAI0862	INFO	ADMIN	Administrator {subject.name} created a grant, giving {pool_grant.to_user_role} {pool_grant.to_user_name} access to pool {pool_grant.for_pool_name}. {user=pool_grant.to_user_id,pool=pool_grant.for_pool_id}
FAI0863	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {pool_grant.to_user_role} {pool_grant.to_user_name} access to pool {pool_grant.for_pool_name}. {user=pool_grant.to_user_id,pool=pool_grant.for_pool_id}
FAI0864	INFO	ADMIN	Administrator {subject.name} created a grant, giving {safe_grant.to_user_role} {safe_grant.to_user_name} access to safe {safe_grant.for_safe_name}. {user=safe_grant.to_user_id,safe=safe_grant.for_safe_id}
FAI0865	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {safe_grant.to_user_role} {safe_grant.to_user_name} access to safe {safe_grant.for_safe_name}. {user=safe_grant.to_user_id,safe=safe_grant.for_safe_id}
FAI0866	INFO	ADMIN	Administrator {subject.name} created a grant, giving {server_grant.to_user_role} {server_grant.to_user_name} access to server {server_grant.for_server_name}. {user=server_grant.to_user_id,server=server_grant.for_server_
FAI0867	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {server_grant.to_user_role} {server_grant.to_user_name} access to server {server_grant.for_server_name}. {user=server_grant.to_user_id,server=server_grant.for_server_
FAI0868	INFO	ADMIN	Administrator {subject.name} created a grant, giving {user_grant.to_user_role} {user_grant.to_user_name} access to {user_grant.for_user_role} {user_grant.for_user_name}. {user=user_grant.to_user_id,user=user_grant.for_user_id}
FAI0869	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {user_grant.to_user_role} {user_grant.to_user_name} access to {user_grant.for_user_role} {user_grant.for_user_name}. {user=user_grant.to_user_id,user=user_grant.for_user_id}

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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
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}

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI0878	INFO	ADMIN	Administrator {subject.name} disconnected safe {user_safe.safe_name} from {user_safe.user_role} {user_safe.user_name} at position {user_safe.position}. {user=user_safe.user_id,safe=user_safe.safe_id}
FAI0880	INFO	ADMIN	Administrator {subject.name} created time policy for connection between safe {user_safe_time_policy.safe_name} and {user_safe_time_policy.user_role} {user_safe_time_policy.user_name}. {user=user_safe_time_policy.user_id,safe=user_safe_time_pol
FAI0881	INFO	ADMIN	Administrator {subject.name} set attribute {attribute.name} for time policy on connection between safe {user_safe_time_policy.safe_name} and {user_safe_time_policy.user_role} {user_safe_time_policy.user_name} to: {attribute.value}. {user=user_safe_time_policy.user_id,safe=user_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}.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}.
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}.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}.
FAI0919	INFO	ADMIN	Administrator {subject.name} deleted cluster node {node.name}.
FAI0920	INFO	ADMIN	Administrator {subject.name} created new cluster on the node {node_name}.
FAI0921	INFO	ADMIN	Administrator {subject.name} attached node with serial {serial} to the cluster.
FSI0922	INFO	SYSTEM	Email "{}" sent to {}.
FSI0923	INFO	SYSTEM	Slack notification sent to {}.
FSI0924	INFO	SYSTEM	Push notification sent to {}.
FAI0925	INFO	ADMIN	Administrator {subject.name} created OpenID Connect authentication server {oidc.name}.
FAI0926	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the OpenID Connect authentication server {old.name} to: {attribute.value}.
FAI0927	INFO	ADMIN	Administrator {subject.name} deleted OpenID Connect authentication server {oidc.name}.
FAI0928	INFO	ADMIN	Administrator {subject.name} created cluster node replication from {node_replication.local_node_name} to {node_replication.remote_node_name}.
FAI0929	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the cluster node replication from {node_replication.local_node_name} to {node_replication.remote_node_name}.
FAI0930	INFO	ADMIN	Administrator {subject.name} deleted cluster node replication from {node_replication.local_node_name} to {node_replication.remote_node_name}.
FAI0931	INFO	ADMIN	Administrator {subject.name} deleted report {report_id}.
FAE0932	ERROR	ADMIN	Failed to remove reports files.
FAI0933	INFO	ADMIN	Administrator {subject.name} created password changer {password_changer_name}.
FAI0934	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the password changer {password_changer_name} to: {attribute.value}.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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.
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.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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 Fudo Network.
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}).

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAE0960 ERROR	ADMIN	Failed to generate diagnostic tarball.	
FAI0961 INFO	ADMIN	Administrator {subject.name} generated diagnostics {filename}.	
FSE0962	ERROR	SYSTEM	Failed to take job from queue, error: {err}
FSE0963	ERROR	SYSTEM	Failed to parse message '{buffer}' on Unix Socket into command, err: {err}
FSE0964	ERROR	SYSTEM	Client Error handling command '{command:?}': {err}
FSE0965	ERROR	SYSTEM	Failed to get scheduled job, error: {err}
FSE0966	ERROR	SYSTEM	Failed to queue scheduled job, error: {err}
FSE0967	ERROR	SYSTEM	Client was interrupted: {serve_result:?}
FSE0968	ERROR	SYSTEM	Scheduler was interrupted: {serve_result:?}
FSE0969	ERROR	SYSTEM	Listener was interrupted: {serve_result:?}
FSE0970	ERROR	SYSTEM	Client connection with Unix Socket is not writeable, err: {err}
FSE0971	ERROR	SYSTEM	Failed to write response to client through Unix Socket, err: {err}
FSE0972	ERROR	SYSTEM	Job {} failed with error: {}
FSE0973 ERROR	SYSTEM	Failed to load configuration from file {configuration_path}, error: {err}	
FSE0974	ERROR	SYSTEM	Failed to shutdown Fudo.
FAI0975 INFO	ADMIN	Administrator {subject.name} created report {report_id}.	
FSE0976	ERROR	SYSTEM	Failed to restart Fudo.
FSE0977	ERROR	SYSTEM	Failed to change Fudo version.
FSE0978	ERROR	SYSTEM	Failed to list Fudo versions.
FAI0979	INFO	ADMIN	Administrator {subject.name} updated management gui private key and certificate.
FAI0980	INFO	ADMIN	Administrator {subject.name} updated user access gateway private key and certificate.
FAI0981	INFO	ADMIN	Administrator {subject.name} generated QR code for mobile application access.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}).
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}).

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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_
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.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}).
FAI1021	INFO	ADMIN	Administrator {subject.name} uploaded new license to Fudo Network.
FAI1022	INFO	ADMIN	Administrator {subject.name} started trial in Fudo Network.
FAI1023	INFO	ADMIN	Administrator {subject.name} generated key for session share access (readonly={session_share.readonly}). {session=session_share.session_id}
FAI1025	INFO	ADMIN	Administrator {subject.name} terminated session {session_terminate.session_id}. {session=session_terminate.session_id}
FAI1026	INFO	ADMIN	Administrator {subject.name} created comment {session_comment.id} for session {session_comment.session_id}. {session=session_comment.session_id}
FAI1027	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for comment {old.id} to: {attribute.value}. {session=old.session_id}
FAI1028	INFO	ADMIN	Administrator {subject.name} removed comment {session_comment.id} for session {session_comment.session_id}. {session=session_comment.session_id}
FAI1029	INFO	ADMIN	Administrator {subject.name} renamed label {oldname} to {name}.
FAI1030	INFO	ADMIN	Administrator {subject.name} deleted upgrade package.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}.
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 notification {notification_id} to user {recipient_id}.
FAI1054	INFO	ADMIN	Administrator {subject.name} removed undelivered mail for notification {notification_id} to user {recipient_id}.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
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}
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}.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI1067	INFO	ADMIN	Administrator {subject.name} canceled timestamping for the session {session_id}.
FAI1068	INFO	ADMIN	Administrator {subject.name} revoked shared session (session_id={session_id}).
FAI1069	INFO	ADMIN	Administrator {subject.name} requested session {session_id} from archive.
FAI1070	INFO	ADMIN	Administrator {subject.name} deleted defied report {defined_report_id}.
FAI1071	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the defined report {old.name} to: {attribute.value}.
FAI1072	INFO	ADMIN	Administrator {subject.name} created role {role.name} with privileges {role.privs}.
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}.

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI1085	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for discovery rule {old.name} to: {attribute.value}.
FAI1086	INFO	ADMIN	Administrator {subject.name} deleted discovery rule {rule.name}.
FAI1087	INFO	ADMIN	Administrator {subject.name} added listener {rule_listener.listener_name} to the discovery rule {rule_listener.rule_name}. {listener=rule_listener.listener_id}
FAI1088	INFO	ADMIN	Administrator {subject.name} removed listener {rule_listener.listener_name} from the discovery rule {rule_listener.rule_name}. {listener=rule_listener.listener_id}
FAI1089	INFO	ADMIN	Administrator {subject.name} added pool {rule_pool.pool_name} to the discovery rule {rule_pool.rule_name}. {pool=rule_pool.pool_id}
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}).

Continued on next page

Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI1095	INFO	ADMIN	Administrator {subject.name} added mapping for Role {user_directory_group_role.role_name} to the group mapping {user_directory_group_role.group_path} in the user directory {user_directory_group_role.user_directory_name} ({user_directory_group_role.user_directory_type}).
FAI1096	INFO	ADMIN	Administrator {subject.name} removed mapping for Role {user_directory_group_role.role_name} from the group mapping {user_directory_group_role.group_path} in the user directory {user_directory_group_role.user_directory_name} ({user_directory_group_role.user_directory_type}).
FAI1097	INFO	ADMIN	Administrator {subject.name} removed authentication server {user_directory_group_authentication.external_authentication_ ({user_directory_group_authentication.external_authentication {user_directory_group_authentication.external_authentication_ from the group mapping {user_directory_group_authentication.user_directory_group_p in the user directory {user_directory_group_authentication.user_directory_name} ({user_directory_group_authentication.user_directory_type}).
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}).

Continued on next page

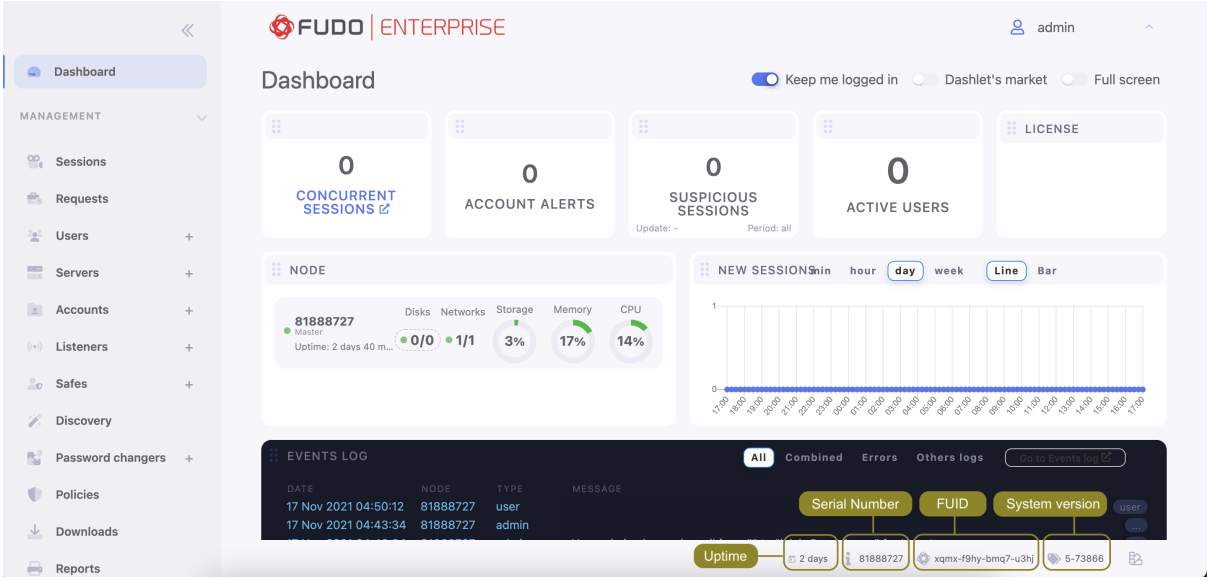
Table 1 – continued from previous page

Message code	Log level	Component type	Message
FAI1101	INFO	ADMIN	Administrator {subject.name} added authentication server {user_directory_group_authentication.external_authentication_ ({user_directory_group_authentication.external_authentication {user_directory_group_authentication.external_authentication_ to the group mapping {user_directory_group_authentication.user_directory_group_p in the user directory {user_directory_group_authentication.user_directory_name} ({user_directory_group_authentication.user_directory_type}).
FAI1102	INFO	ADMIN	Administrator {subject.name} added rule {scanner_rule.rule_name} to scanner {scanner_rule.scanner_name} at position {scanner_rule.position}.
FAI1103	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the connection between scanner {scanner_rule.scanner_name} and rule {scanner_rule.rule_name} at position {old.position} to: {attribute.value}.
FAI1104	INFO	ADMIN	Administrator {subject.name} removed rule {scanner_rule.rule_name} from scanner {scanner_rule.scanner_name} at position {scanner_rule.position}.
FAI1105	INFO	ADMIN	Administrator {subject.name} started scanner {scanner.name}.
FSW1106	WARNING	SYSTEM	Failed to synchronize authentication method (%s) for user %s.
FSW1107	WARNING	SYSTEM	AI cannot transfer model "%s". Model version has changed.
FSW1108	WARNING	SYSTEM	AI failed to load model "%s" during model transfer.
FSW1109	WARNING	SYSTEM	AI failed to update model "%s" during model transfer.
FSI1110	INFO	SYSTEM	Starting webproxyd on {addr}.
FSI1111	INFO	SYSTEM	Connection closed by guacd.
FSI1112	INFO	SYSTEM	Connection closed by client.
FSE1113	ERROR	SYSTEM	Connection error: {err}.
FSE1114	ERROR	SYSTEM	Failed to set NODELAY on socket bound to {addr}: {err}.

25.3 Footer Information

The footer on the left menu displays 4 elements describing current Fudo Enterprise instance:

1. **Uptime** - when the system was activated last time.
2. **Serial Number** - ID of the cluster node. It's unique for a single cluster.
3. **FUID (Fudo Unique Identifier)** - Unique ID of the current Fudo Enterprise instance.
4. **System Version** - Current software version.



CHAPTER 26

Fudo Officer 2.0

Fudo Officer 2.0 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 2.0 app, or on Admin Panel in the *Management* > *Sessions* tab.

Fudo Officer 2.0 is available for Android and iOS. Download our mobile application from your respective app store.

Note: Refer to the *Approving pending user requests* and *Declining pending requests* topics for more information about maintaining the users' requests on the Admin Panel.

26.1 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.

To configure Fudo Officer 2.0, 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 2.0 permission to access the camera and send notifications.

1. Set up Fudo Enterprise:

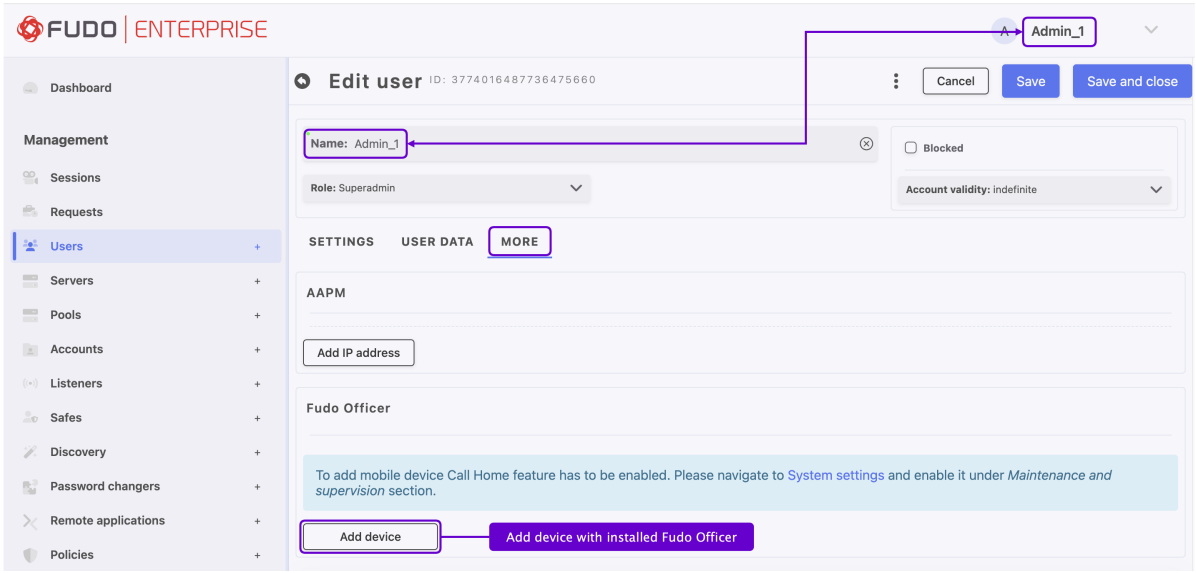
1.1. Open Fudo Enterprise Admin Panel and go to *Management* > *Users*.

1.2 Find and edit the user for whom you want to create a profile in the Fudo Officer 2.0.

1.3. Go to the *MORE* tab and click the *Add device* button in the *Fudo Officer* field to generate the QR code.

Note:

- Fudo Officer 2.0 binding can be configured only for the the user currently logged in to the Admin Panel.
- Only user with the *superadmin* or *admin* role can use the Fudo Officer 2.0 mobile app.



2. Open Fudo Officer 2.0 app on your mobile device and tap *Get started*:

   2.1. Allow Fudo Officer 2.0 to access the camera, which is required for scanning QR codes.

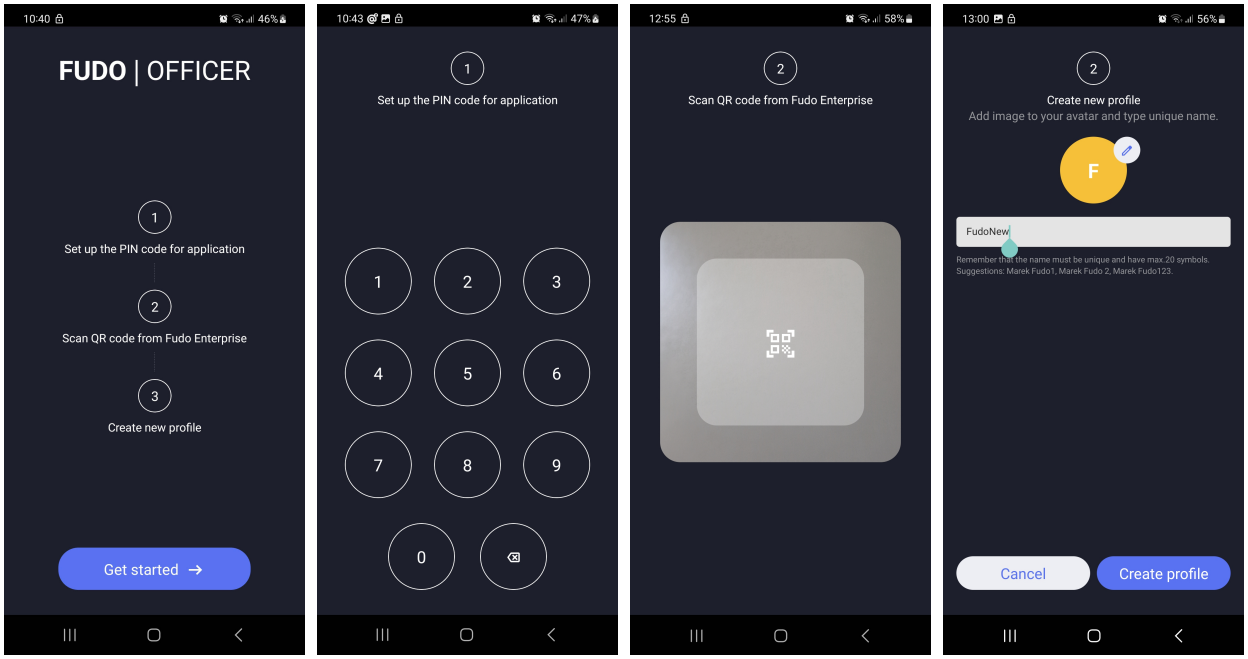
   2.2. Set a 6-digit PIN that will be used to protect access to the application.

   2.2. Repeat the provided PIN to confirm it.

   2.3. Allow Fudo Officer 2.0 to send notifications.

   2.4. Scan the QR code displayed in the Admin Panel with your mobile device.

   2.5. Set a profile name and click the *Create profile* button.



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.

Related topics:

- *Managing Profiles*
- *Managing Session Requests*
- *Fudo Officer Settings*

26.2 Managing Profiles

A Profile corresponds to the User object in the Fudo Enterprise. You can manage multiple Profiles from a single application.

26.2.1 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 2.0 mobile app.

To add new profile, follow below steps:

1. Set up Fudo Enterprise:

   1.1. Open Fudo Enterprise Admin Panel and go to *Management* > *Users*.

   1.2 Find and edit the user for whom you want to create a profile in the Fudo Officer 2.0.

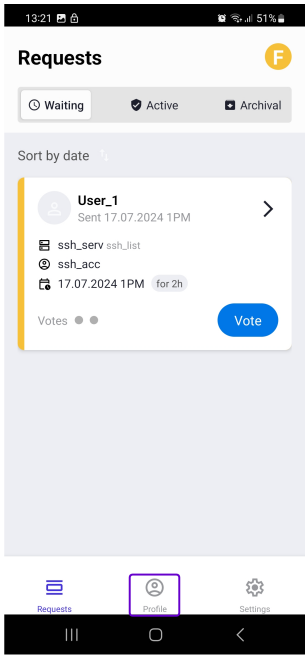
   1.3. Go to the *MORE* tab and click the *Add device* button in the *Fudo Officer* field to generate the QR code.

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 2.0 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.

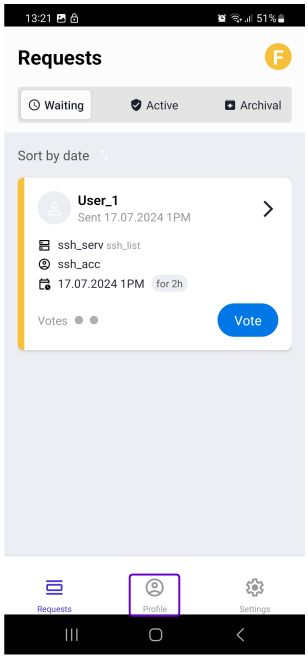
Note: The profile name is editable.

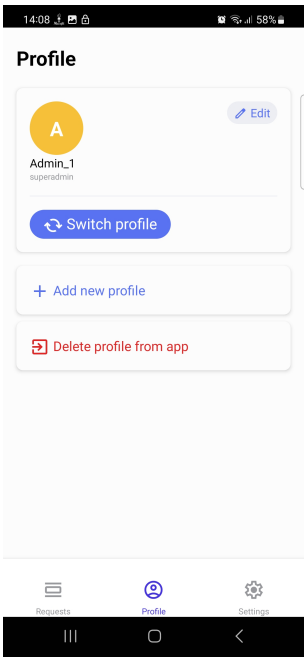
5. Go back to the Fudo Enterprise Admin Panel and click *Close* in the QR code window. The *Fudo Officer* section now has the *Platform* field filled with the binding device name and the *Push ID* with the respective string.
6. Click the *Save* button to save changes in the user configuration.

26.2.2 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.

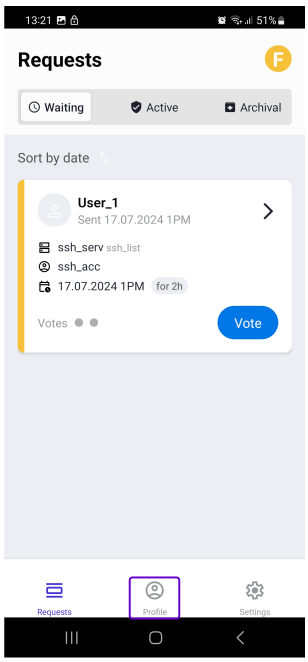


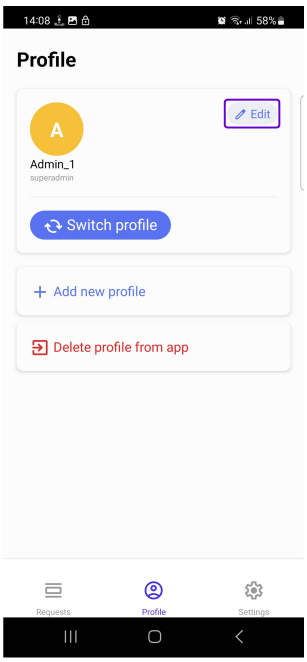


26.2.3 Edit Profile

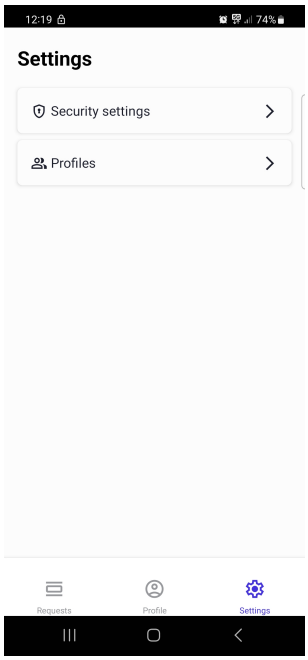
You can edit the name and the profile picture of an active profile:

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*.

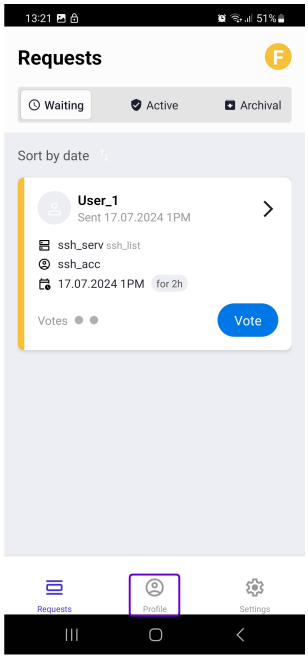


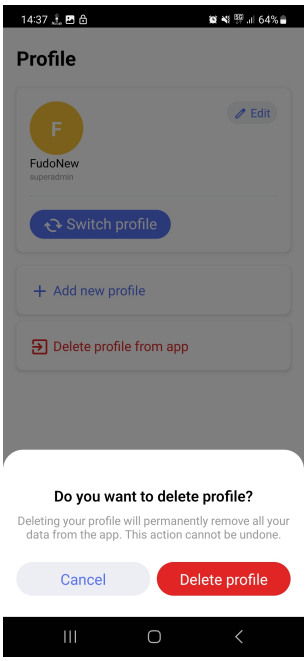
Note: To change PIN, please follow the *Change PIN code* section.

26.2.4 Delete Profile

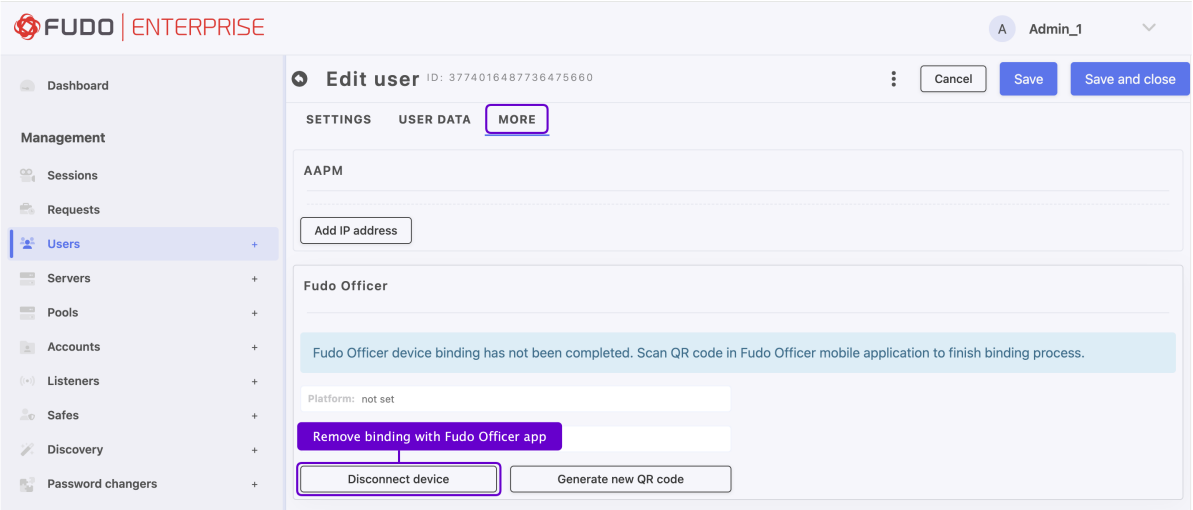
To delete profile from the Fudo Officer 2.0, first you have to switch to this profile:

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*

26.3 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.

26.3.1 Awaiting Requests

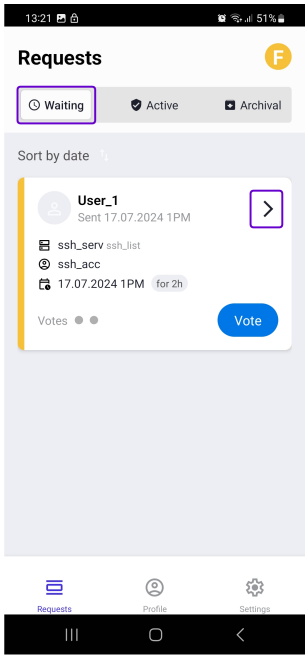
The **Waiting tab** shows a list of the requests that are waiting for a decision of the current user profile.

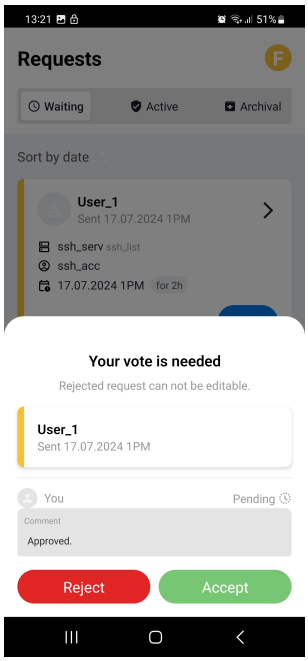
Note:

- 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.

In order to vote for approval or rejection of the request, follow the steps:

1. Open Fudo Officer 2.0 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:

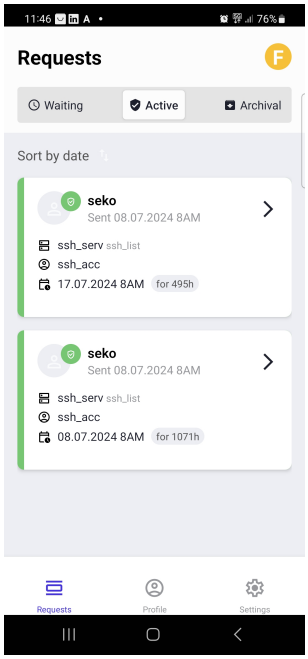
- Users who sent the request via the Access Gateway and have their e-mail address configured on the Admin Panel, receive notifications when their request was accepted or rejected.

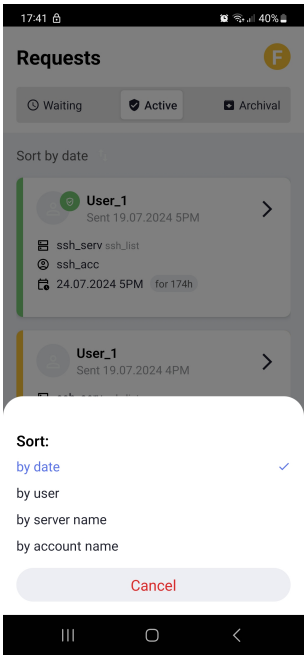
26.3.2 Active Requests

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.*



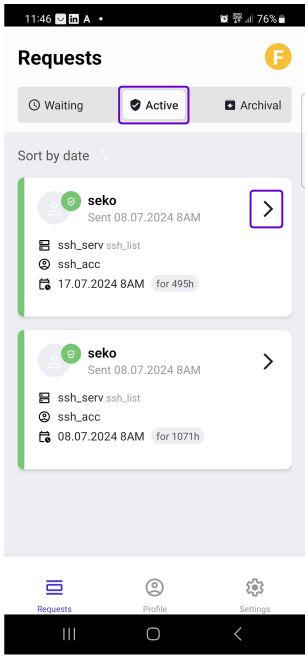


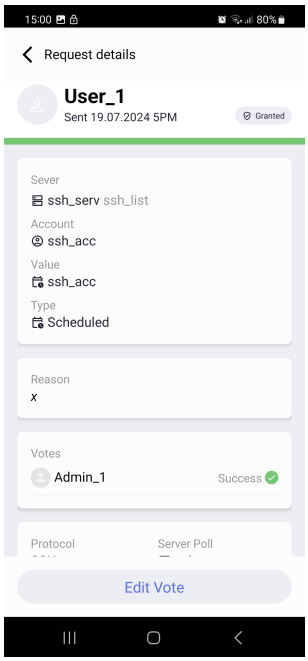
26.3.3 Revoking Request

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 2.0 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.

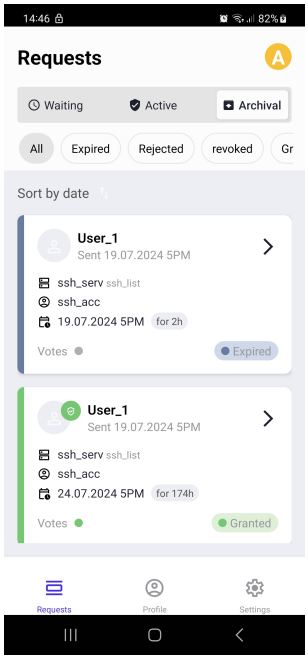




Note: If you have accepted a request that is still awaiting votes from other administrators, the *Reject* button will be available directly on the request screen.

26.3.4 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*

26.4 Settings

To access the application settings, click on the gear icon in the bottom right corner of the screen.

26.4.1 Biometric Authentication

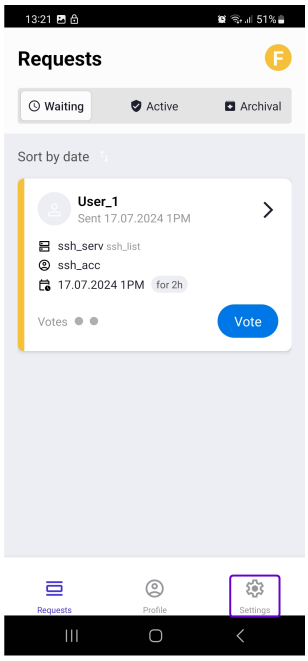
To enable Biometric Authentication option:

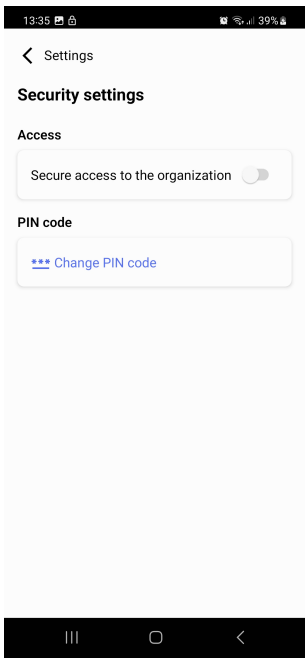
1. Choose the gear icon in the bottom right corner of the screen.
2. Choose *Security settings*.
3. Switch on the *Enable Biometric Authentication* option.
4. Scan your fingerprint to complete the procedure.

Note: Once the option is enabled, biometric authentication will be set as the default method when launching the application.

26.4.2 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.

26.4.3 Language

The application language is set according to the phone's language settings.

Related topics:

- *Managing Session Requests*

CHAPTER 27

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.

27.1 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*

27.2 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 the *superadmin* role 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.

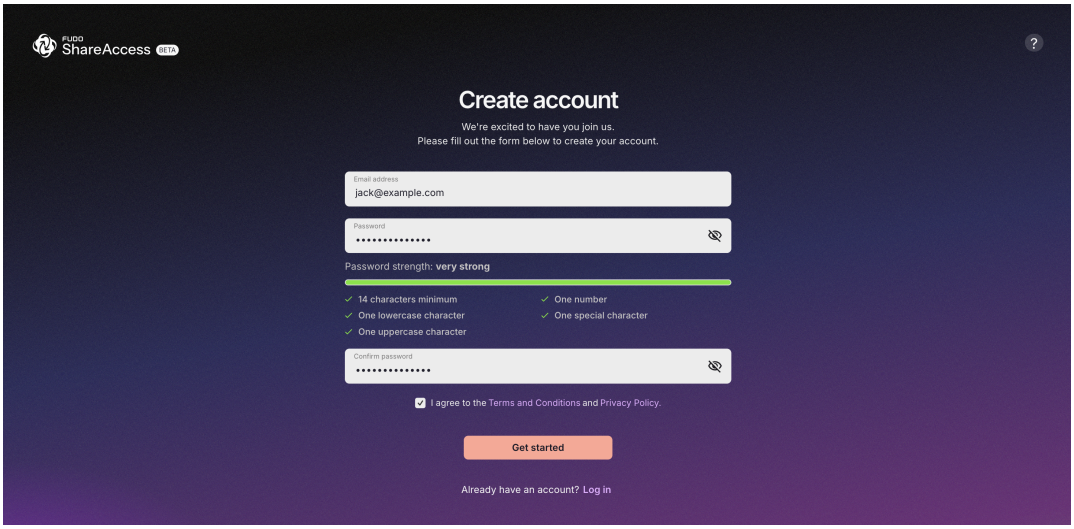
---

1. Log in to Fudo Enterprise instance Admin Panel.
2. Create user:
    - Select *Management* > *Users* and then click + *Add user*.
    - Enter user name.
    - From the *Role* drop-down list select *superadmin* role.
    - In the *User Data* tab, in the *User info* field enter:
        - user's full name,
        - user's email address,
        - user's organizational unit,

  - user's phone number.

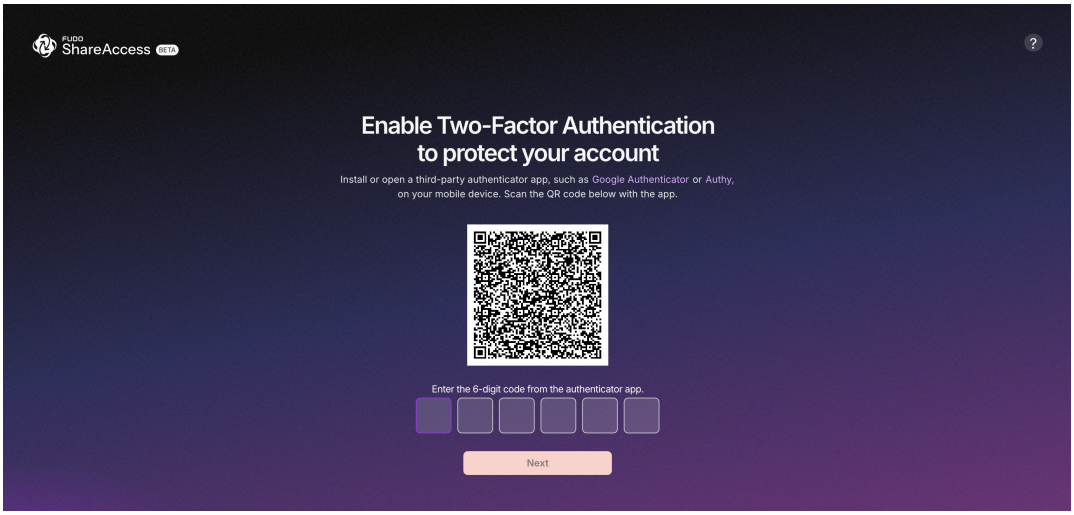
- Click *Save*.
- Go back to the *Settings* tab, and in the *Authentication* section select desired authentication type from the *Add authentication method* drop-down list. This will be used to authenticate user against Fudo Enterprise User Access Gateway.
- Click *Save and close*.

3. **Create an account in Fudo ShareAccess:**
   - Go to the Fudo ShareAccess website.
   - Click *Sign In*.
   - Provide the same email address as the *superadmin* user in Fudo Enterprise.
   - Provide password for created account.

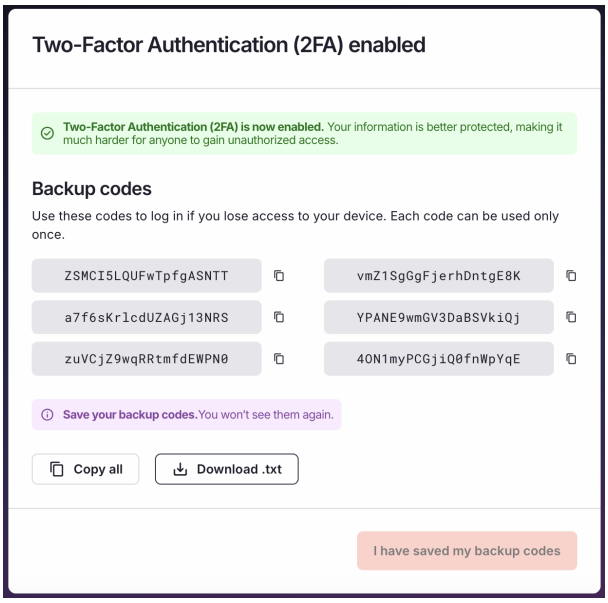


Note: To create an account you have to agree to our Terms and Conditions and Privacy Policy.

- 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.

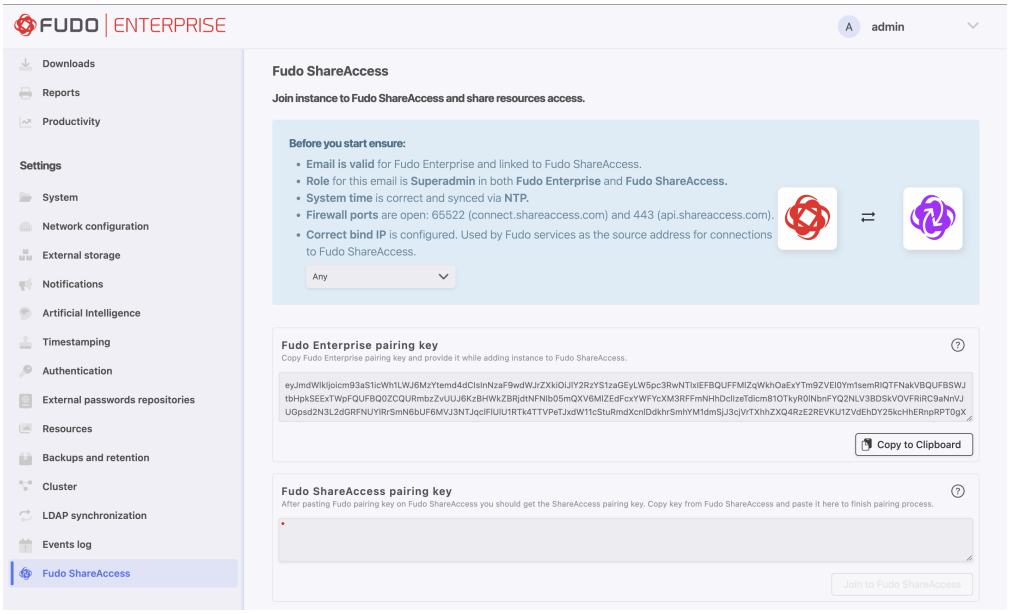


Warning:

- 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.

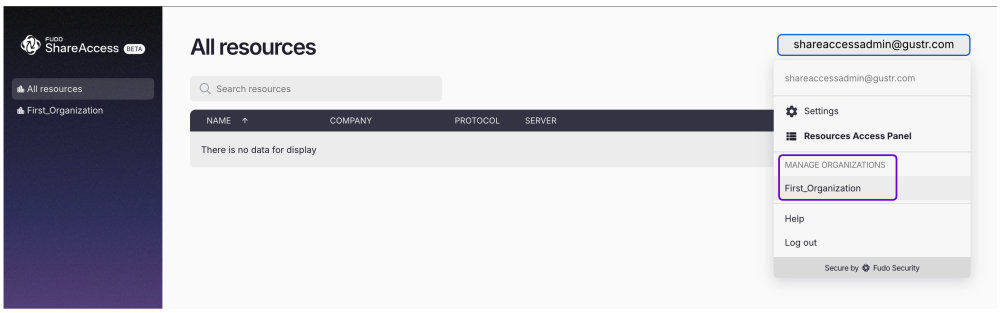
- Click I have saved my backup codes to confirm the backup and complete the configuration process.

4. Copy the *Pairing Key* from the Fudo Enterprise:
   - Select *Settings* > *Fudo ShareAccess*.
   - Click *Copy to clipboard* to copy the *Fudo Enterprise pairing key*.

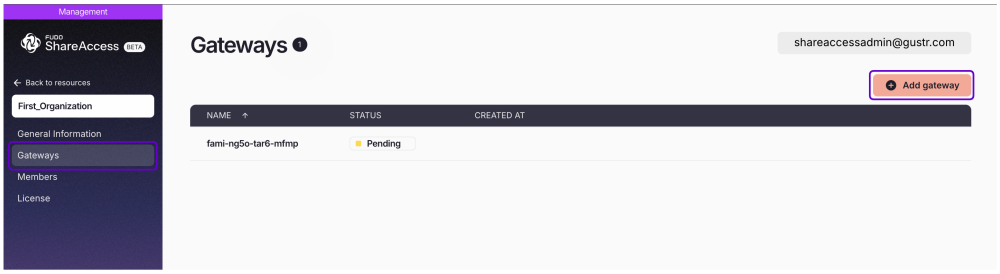


5. Add **Gateway** in Fudo ShareAccess:

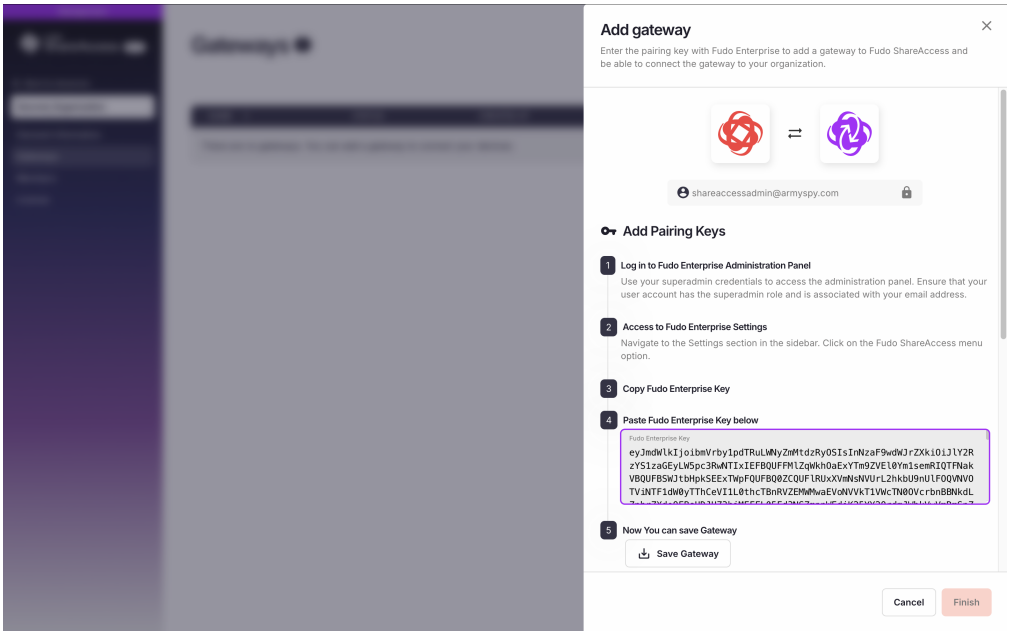
   - Expand the dropdown menu in the upper-right corner and select *Manage organizations* > *Your Organization Name* to access the organization settings.



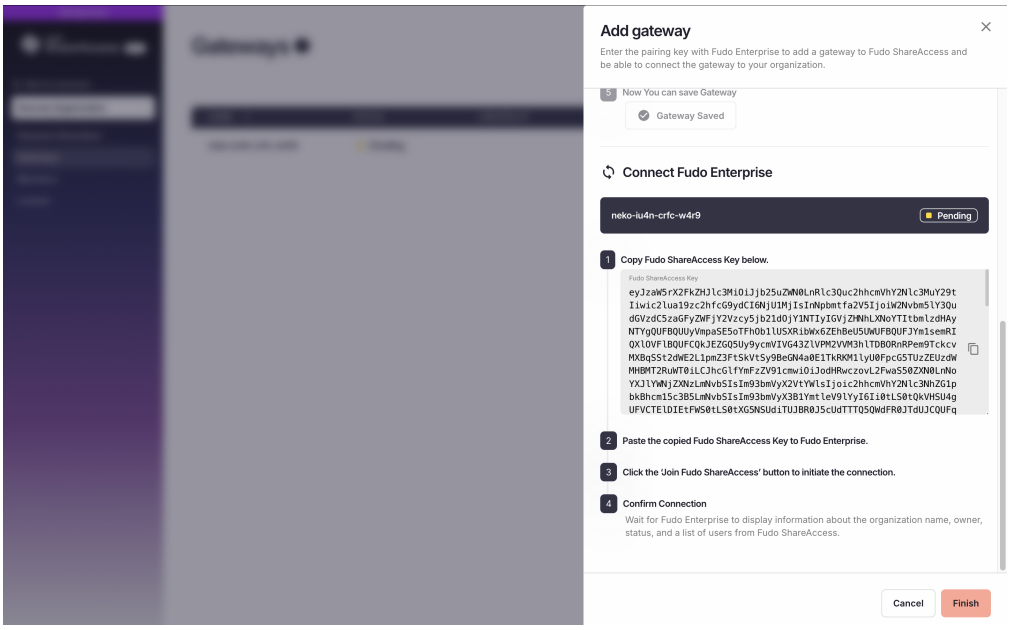
   - In the left-hand menu, select *Gateways*.
   - Click *+ Add Gateway*.



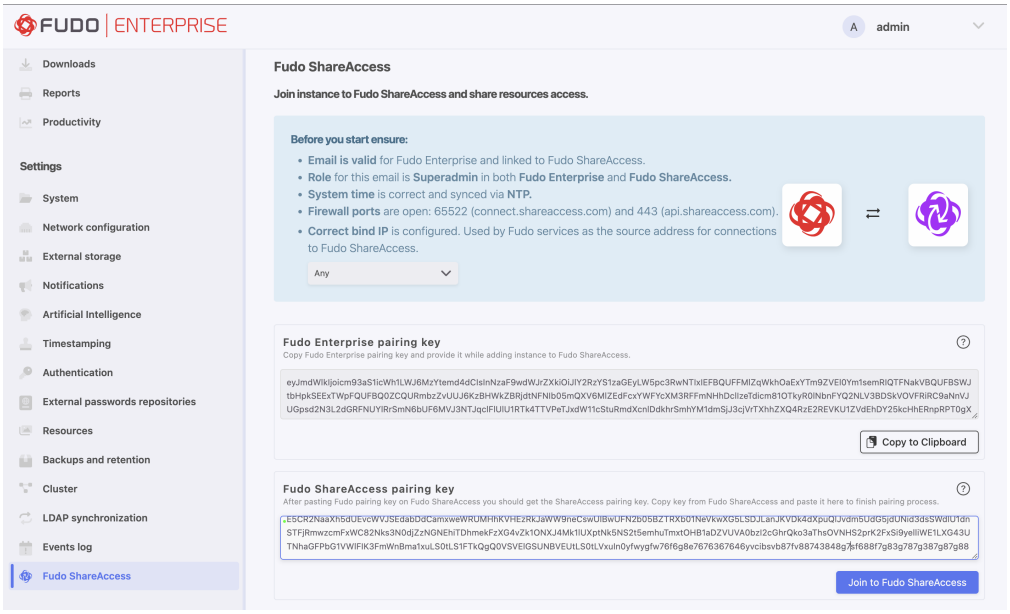
   - Paste the *Fudo Enterprise pairing key* that was copied earlier in the manual.
   - Click *Save Gateway*.



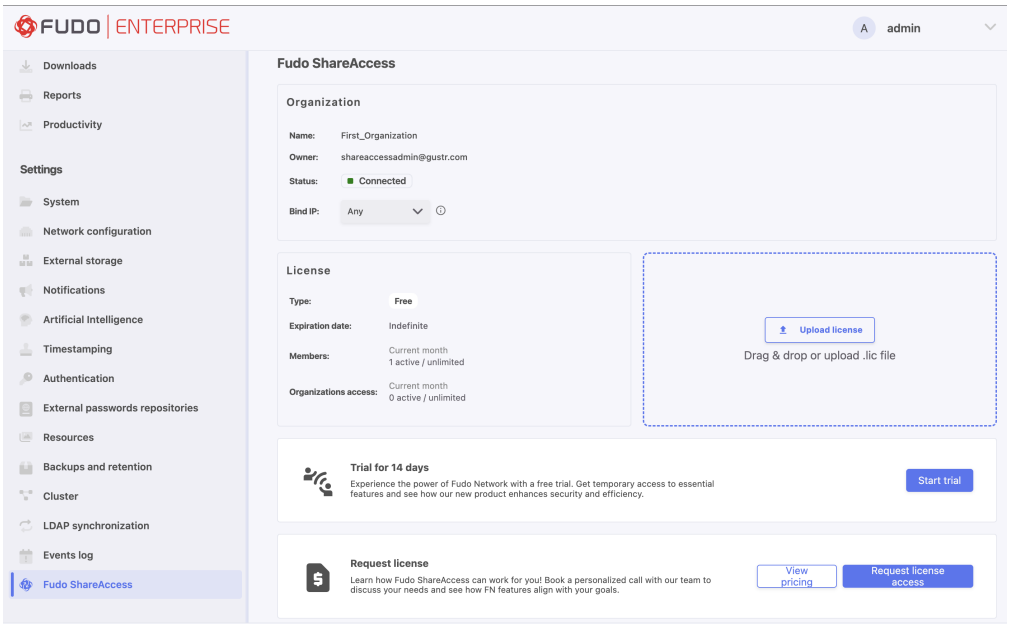
- Next, copy the *Fudo Pairing Key* displayed below.



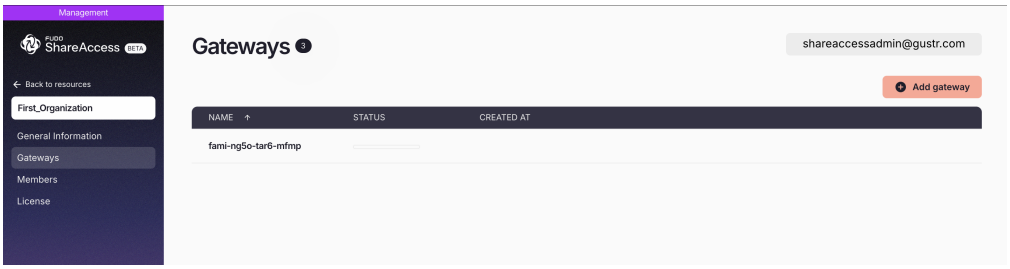
6. Go back to Fudo Enterprise Admin Panel and paste the *Fudo Pairing Key* in the *Fudo shareaccess pairing key* field.
7. Click *Join to Fudo shareaccess*.



8. Wait until the Fudo Enterprise instance displays information about the organization name, owner, status, and a list of users from Fudo ShareAccess.



9. After successful pairing, the Fudo Unique Identifier will be displayed on the Gateways list.



Related topics:

- *Manage Fudo ShareAccess Members*
- *Manage Access to Resources*

27.3 License

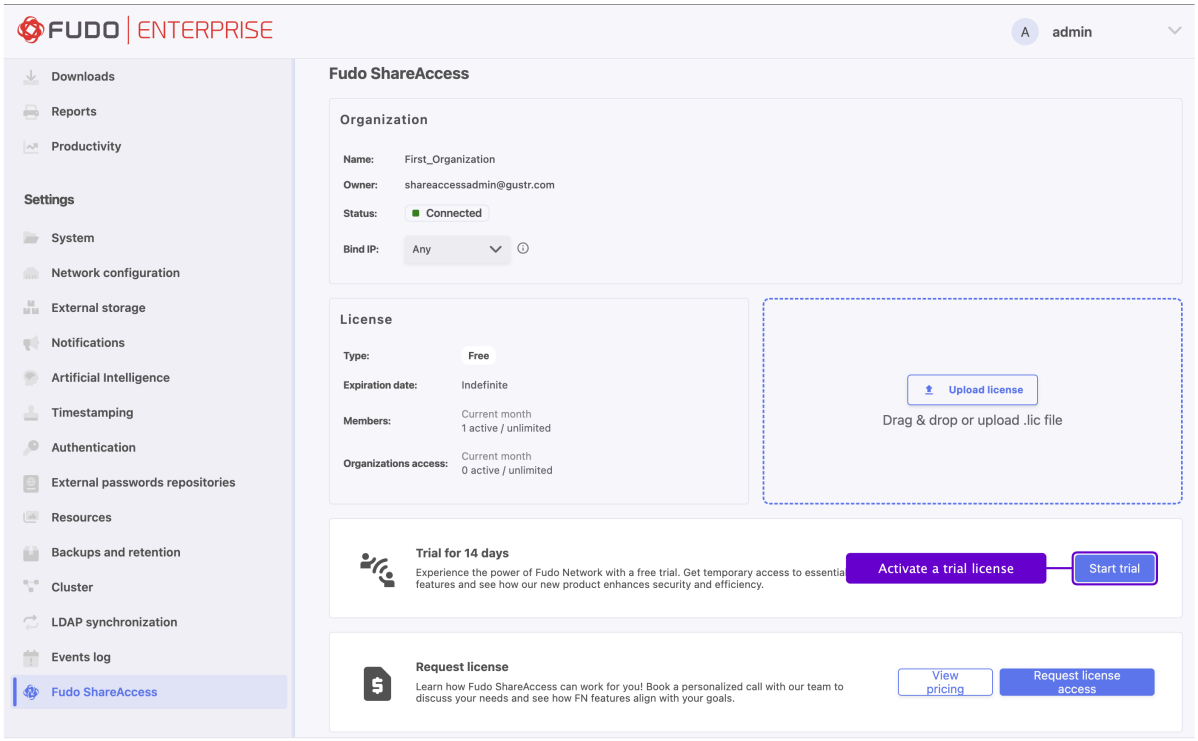
License management is streamlined and accessible exclusively to **superadmin** users within the Fudo Enterprise platform.

27.3.1 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:

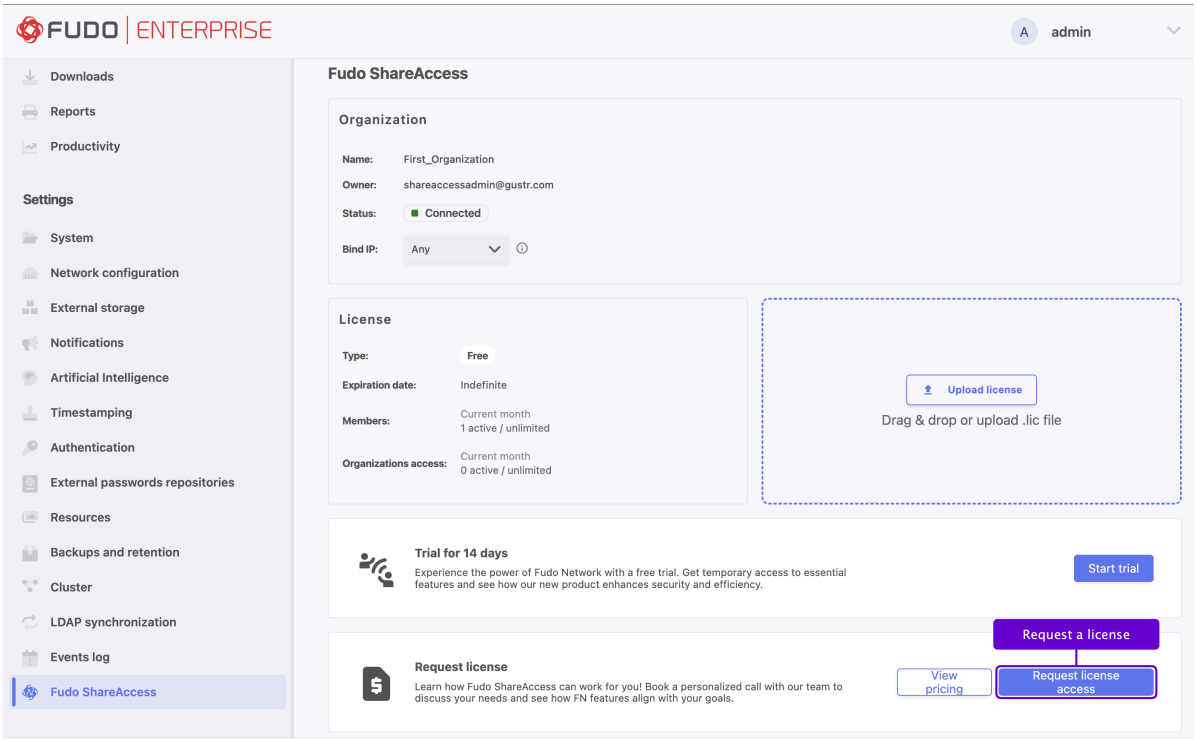
1. Log in to the Admin Panel of the Fudo Enterprise instance.
2. Select Settings > Fudo ShareAccess.
3. In the *License* section click the Start trial button.



27.3.2 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.



27.3.3 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*

27.4 Manage Fudo ShareAccess Members

27.4.1 Inviting Members

You can invite users to access organization resources via Fudo ShareAccess or to become an organization members.

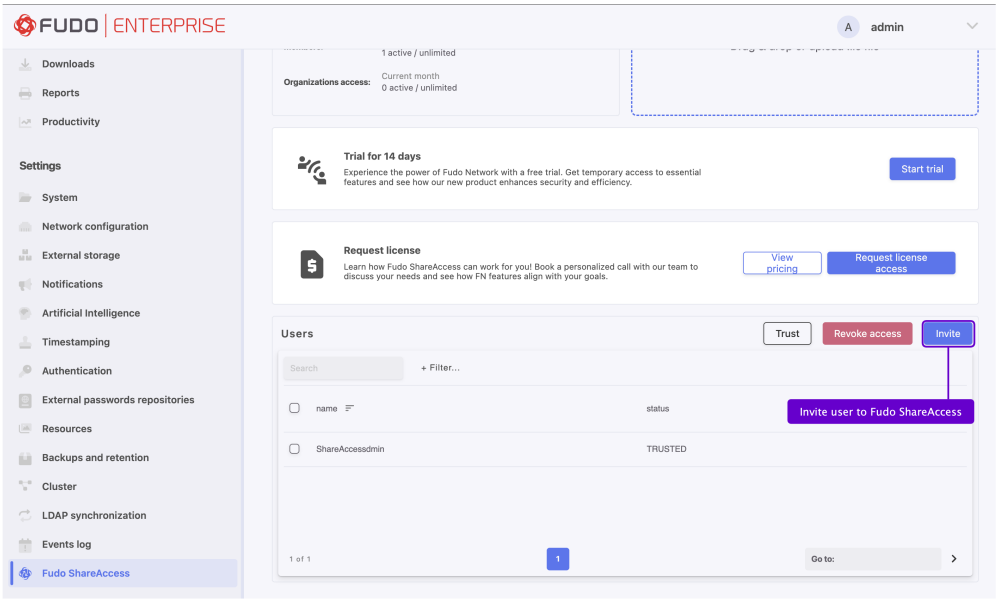
Inviting a user establishes a connection between Fudo Enterprise user and Fudo ShareAccess user, which is necessary to grant access to resources.

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.

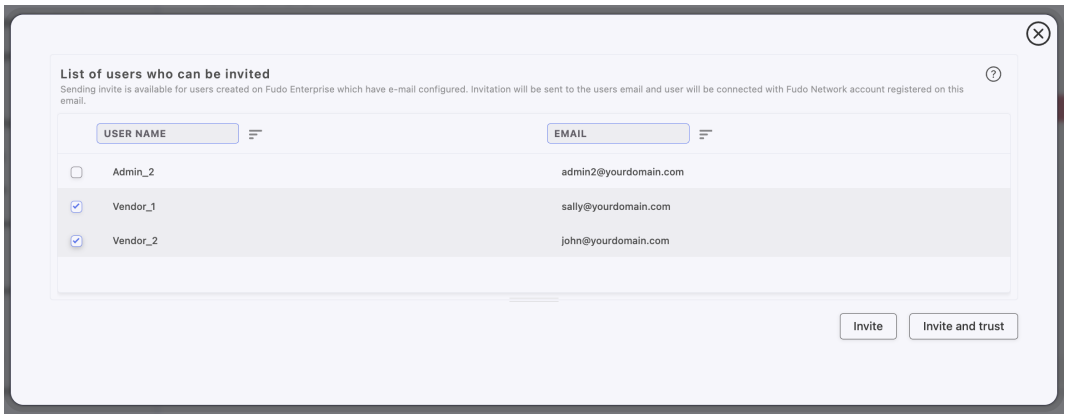
To add users from Fudo Enterprise and connect them with Fudo ShareAccess follow below steps:

1. Create user with email that will be used as email for Fudo ShareAccess access:
    - Select *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.



4. Fudo ShareAccess requires a user to be *Trusted* in order to access assigned resources:
   - Click the *Invite and Trust* button to trust the user immediately without verification, or
   - Click the *Trust* button to verify the user after they accept the invitation.

Note: Inviting users with the *Trust* option will result in the immediate, unattended sharing of resources.

5. Sending an invitation will add entries to the users list, with their status marked as *Pending* until the user clicks the email link to join the organization.

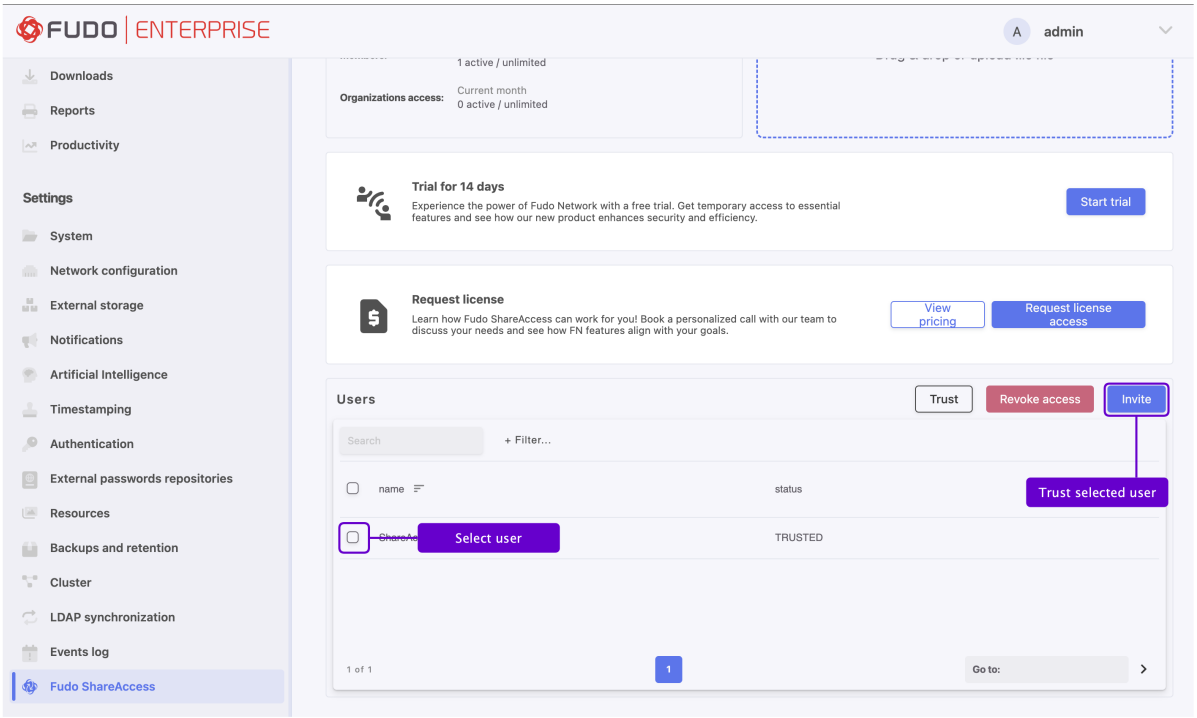
Note: Sending an invitation means the user will receive an email containing a link that allows them to either create an account and accept the invitation or simply accept the invitation if they already have an account on Fudo ShareAccess.

27.4.2 Verifying Members Status

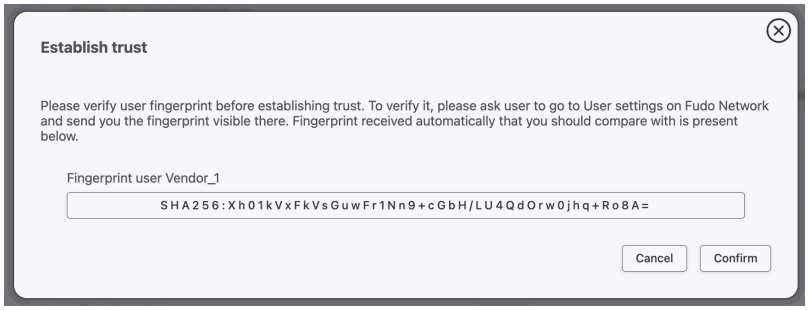
User that is paired with Fudo ShareAccess can have *Trusted* or *Untrusted* status. This status defines if user can see resources in Fudo ShareAccess.

Note: The Fudo Enterprise superadmin can perform verification (change *Untrusted* status) only after the user has created an account in Fudo ShareAccess and accepted the invitation to join organization.

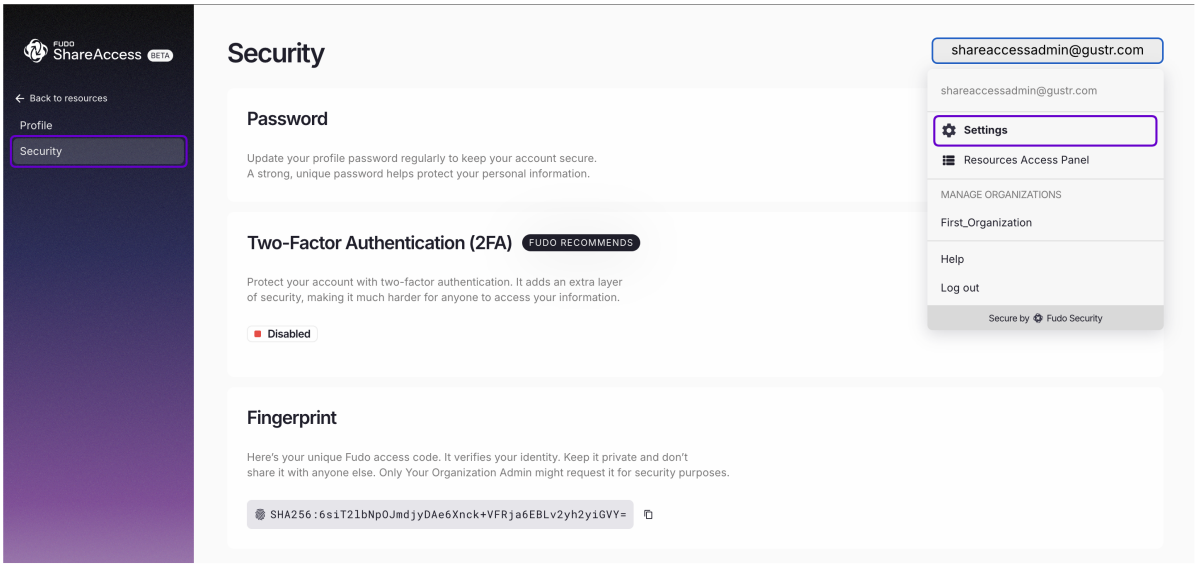
1. Select *Settings* > *Fudo ShareAccess*.
2. Select users from the list and click the *Trust* button.



3. Ask user to provide the *Fingerprint Key* from his Fudo ShareAccess account and compare it with the fingerprint displayed in the modal 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.



1. Click *Confirm*. After confirmation user is trusted.

Note:

- There is no requirement to complete that process. It is at the Administrator's discretion whether to trust users without verification.
- The option to manually change a user's status from *Trusted* to *Untrusted* is not available. Blocking the user in Fudo Enterprise will automatically disable their access to resources shared with Fudo ShareAccess.

27.4.3 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.

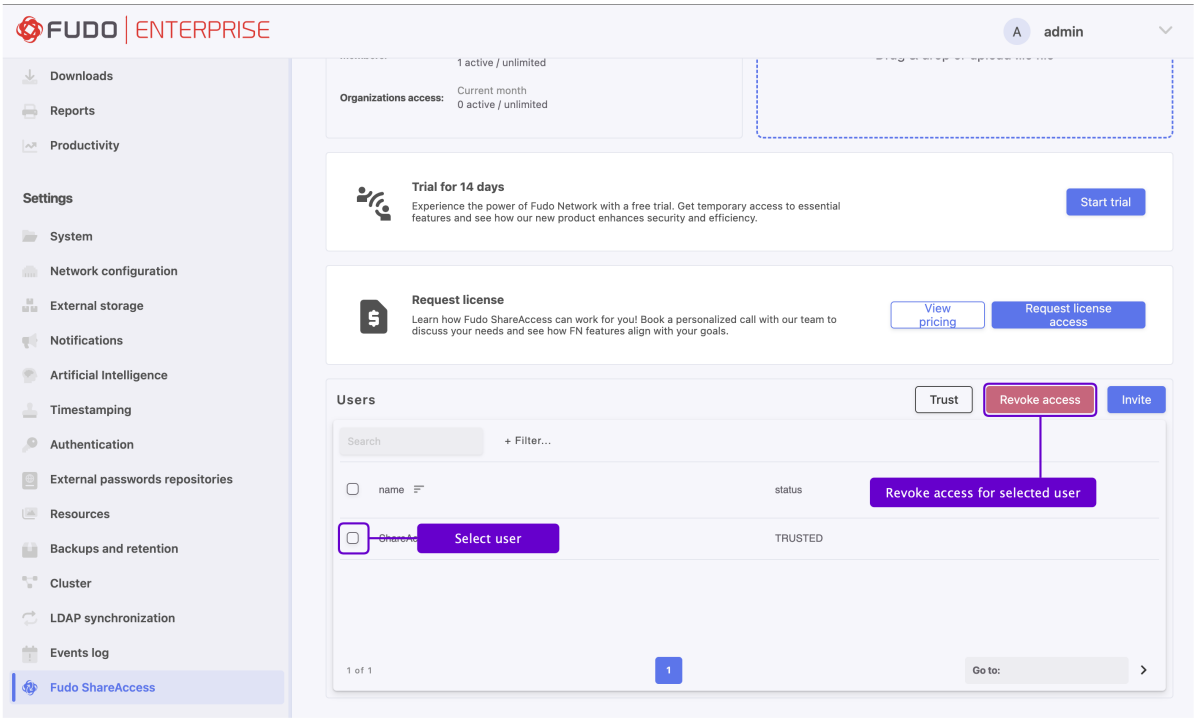
For more information please follow the ShareAccess documentation.

27.4.4 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. Select the users you wish to disconnect and click *Revoke Access*.

3. Upon confirmation, these users will be removed from the list.



27.4.5 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*

27.5 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

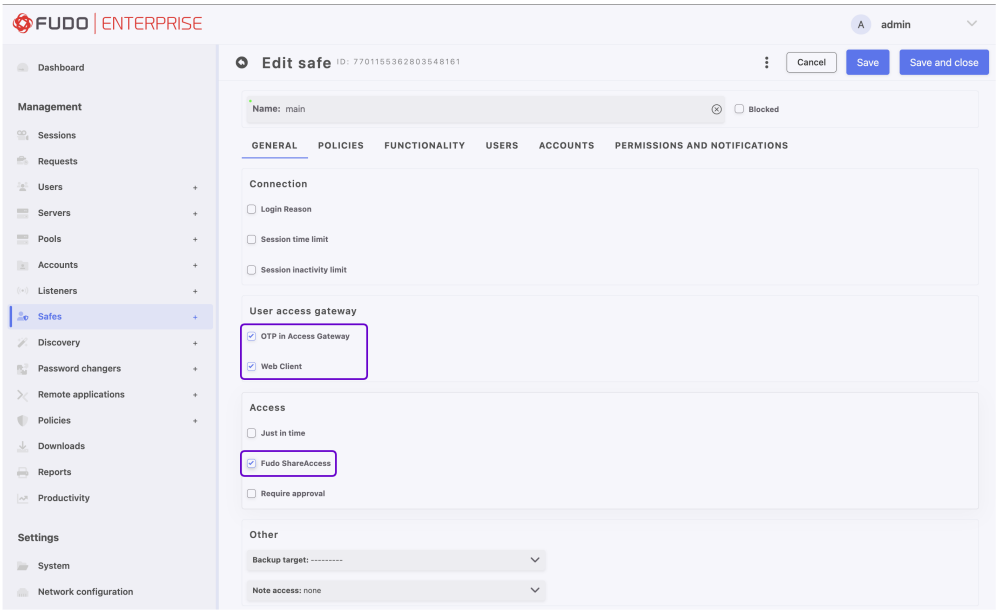
  - SSH
- **Account Types:** Only the following account types are supported:
  - Regular accounts with properly configured credentials
  - Forward accounts
- **Safe:** The server must have the following options enabled:
  - Fudo ShareAccess enabled
  - OTP enabled
  - Webclient enabled

*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.

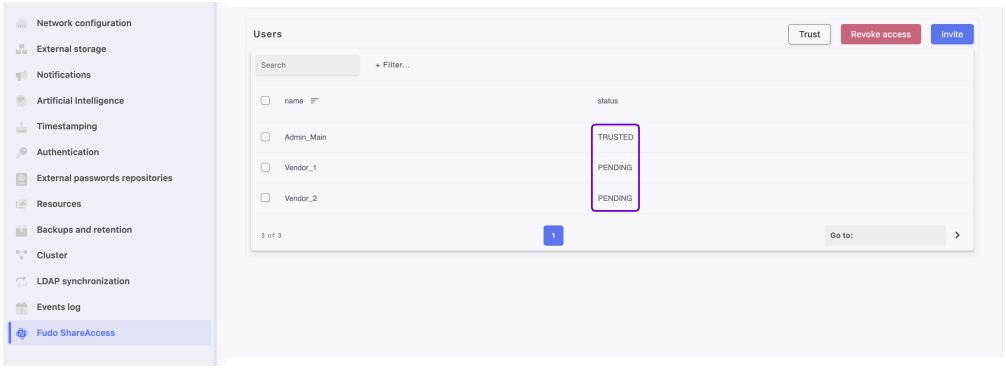
- In the *General* tab:
  - The *OTP in Access Gateway* option is enabled by default and is responsible for generating OTP in the Access Gateway (required).
  - Select *Web Client* option to allow connecting to the session using the built-in browser client (required).
  - Select *Fudo ShareAccess* option 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:

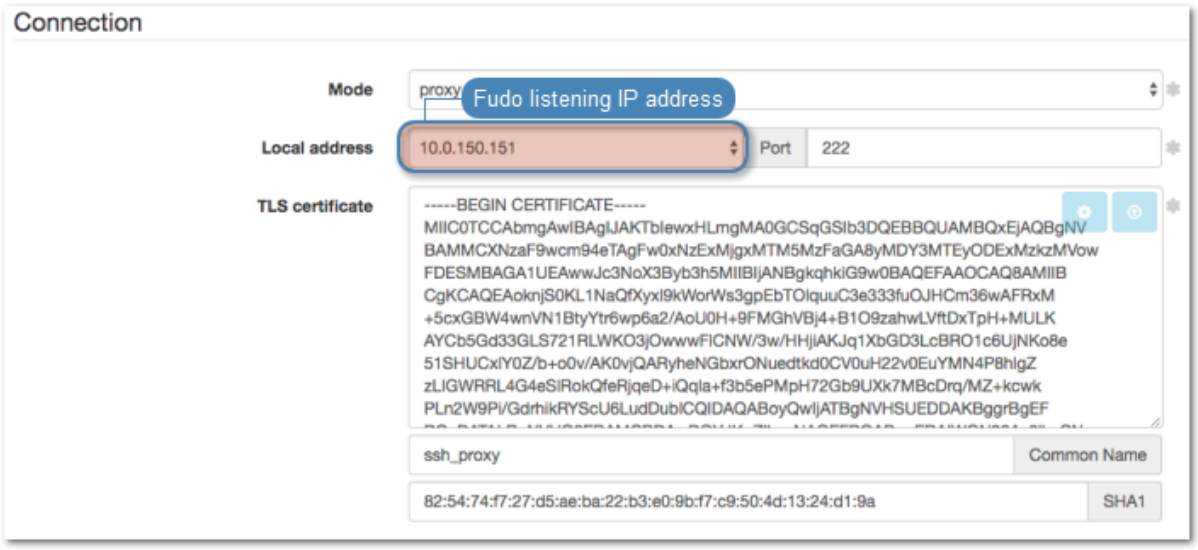
- *Manage Fudo ShareAccess Members*
- *Require approval for access*
- *Access requests*

CHAPTER 28

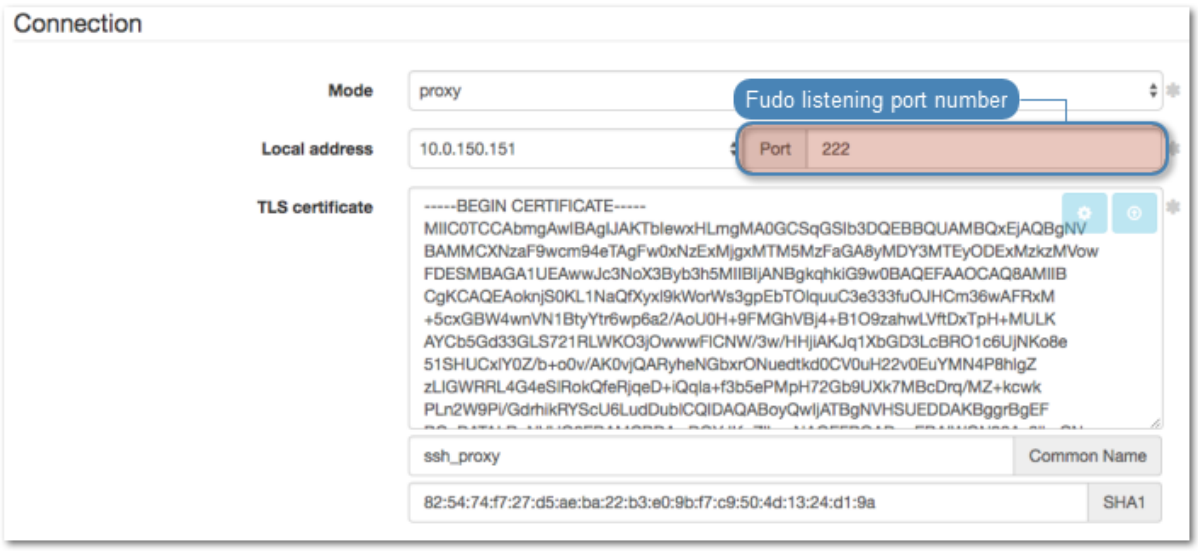
Client applications

28.1 PuTTY

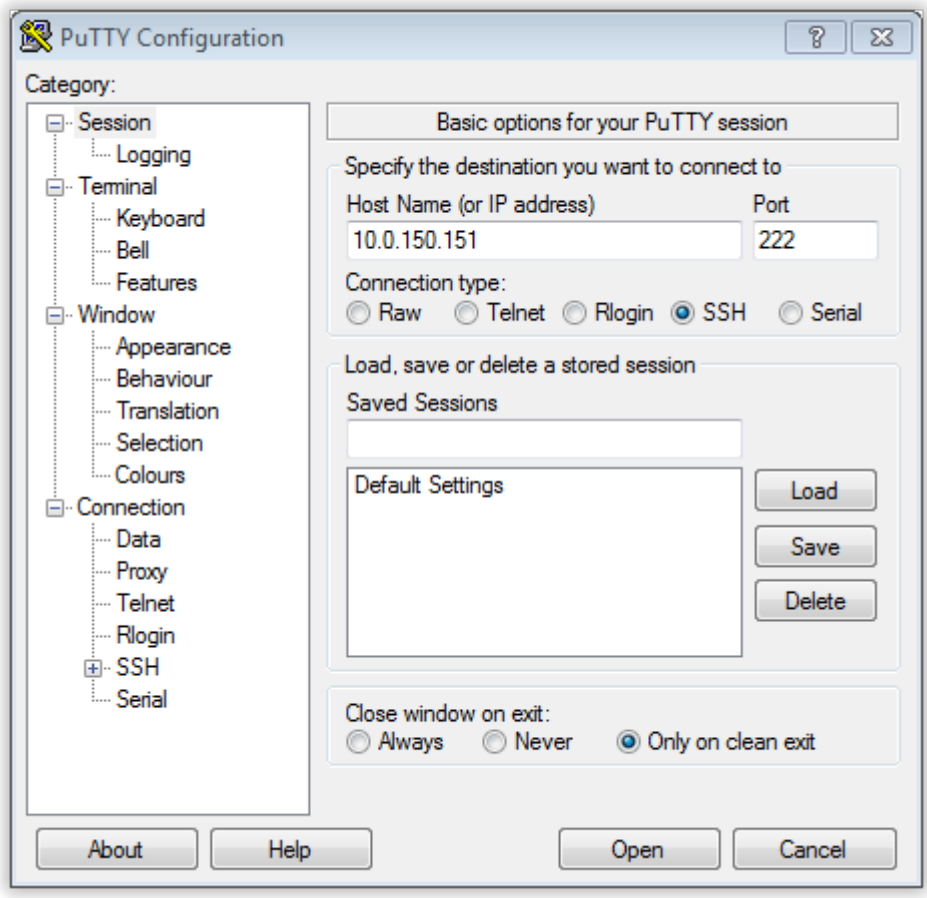
1. Download and launch PuTTY.
2. In the *Host Name (or IP address)* field, enter IP address defined in the listener.



3. In the *Port number* field, enter port number defined in the listener.

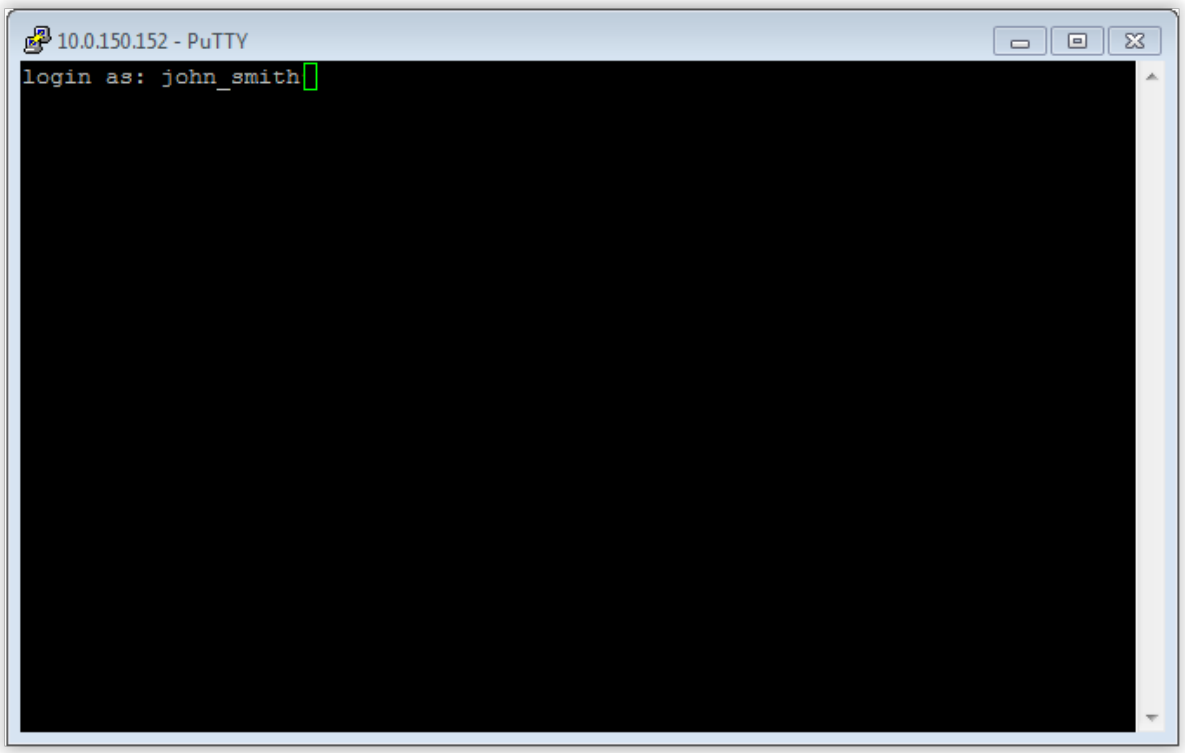


4. Select the `SSH` connection type.



5. Click *Open*.

6. Enter username.



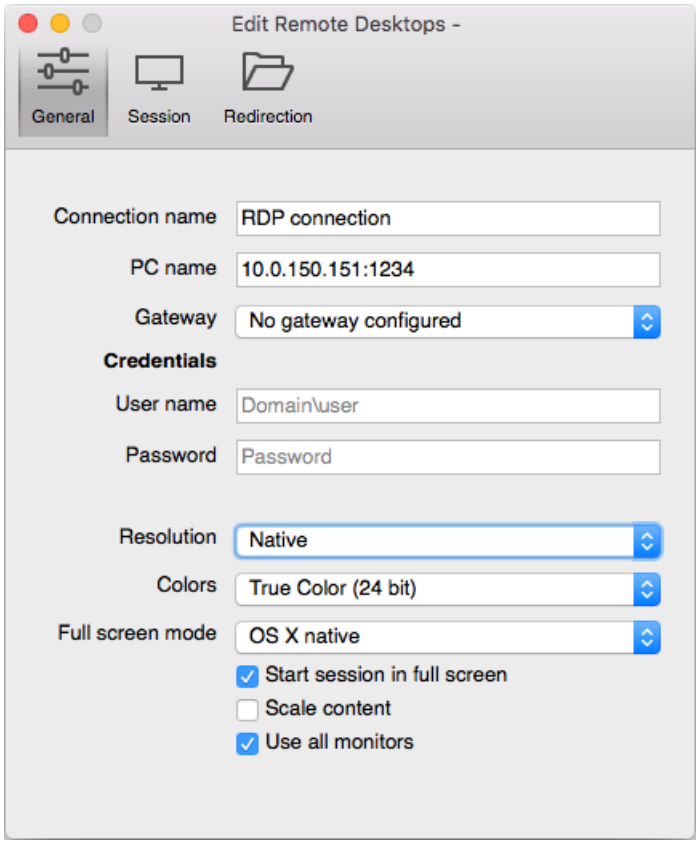
7. Enter password.

Related topics:

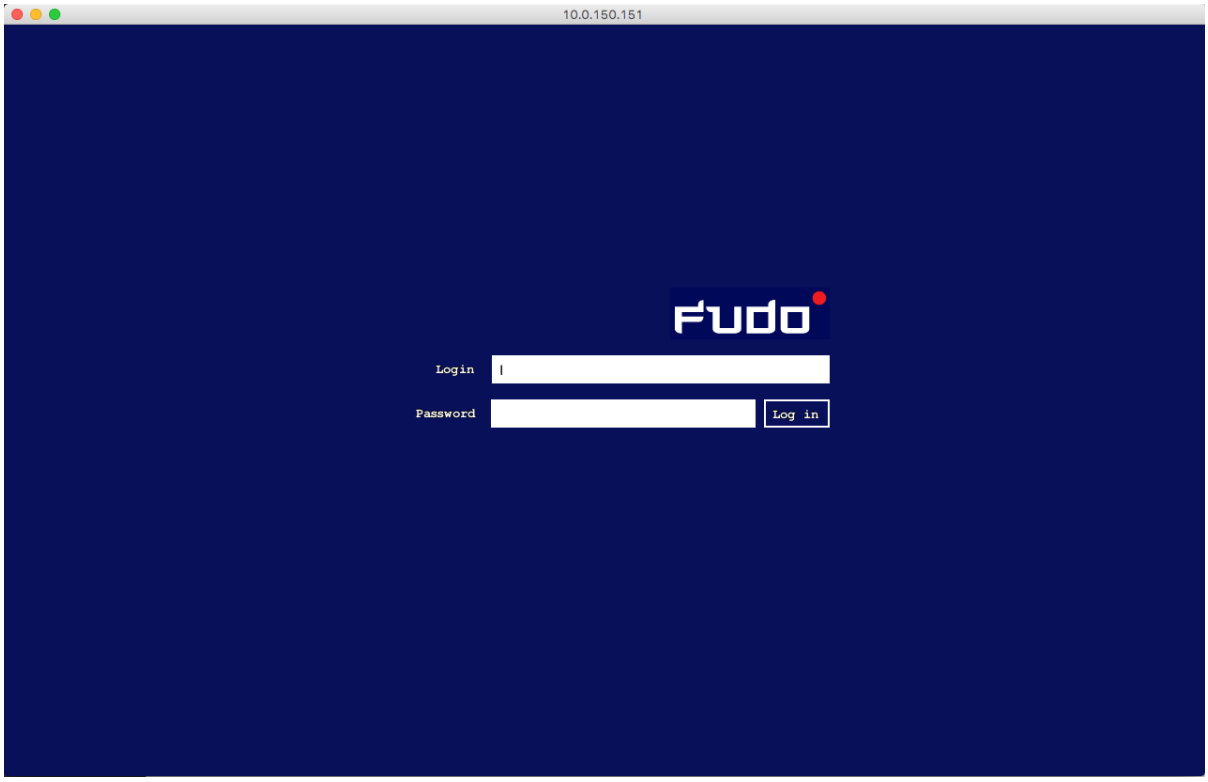
- *SSH*
- *Creating an SSH server*
- *Setting up the SSH listener*

28.2 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.

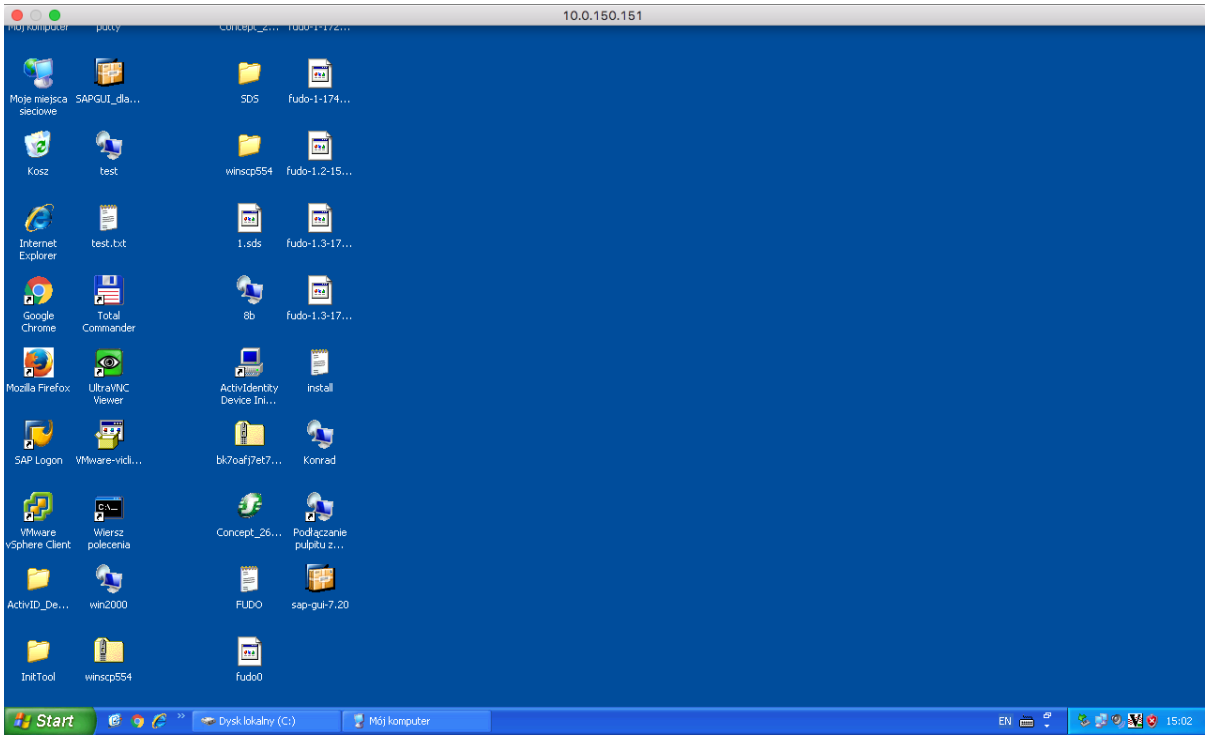


3. Enter user login and password and press the [Enter] keyboard key.



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.

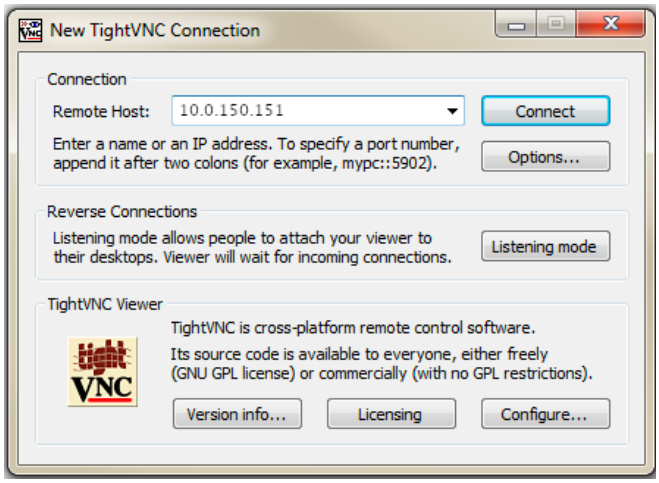


Related topics:

- *RDP*
- *Creating an RDP server*
- *Setting up the RDP listener*

28.3 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).



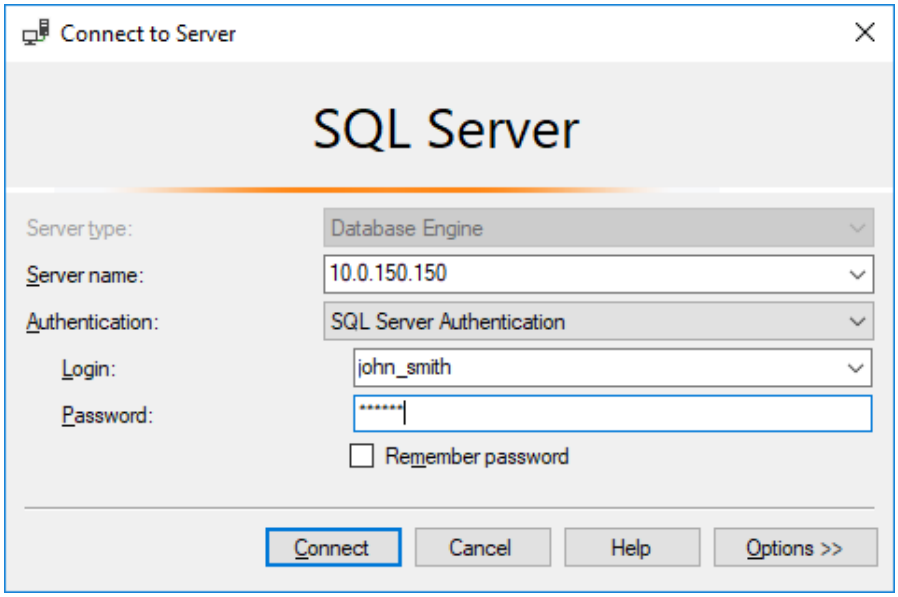
3. Enter username and password and press the enter key.

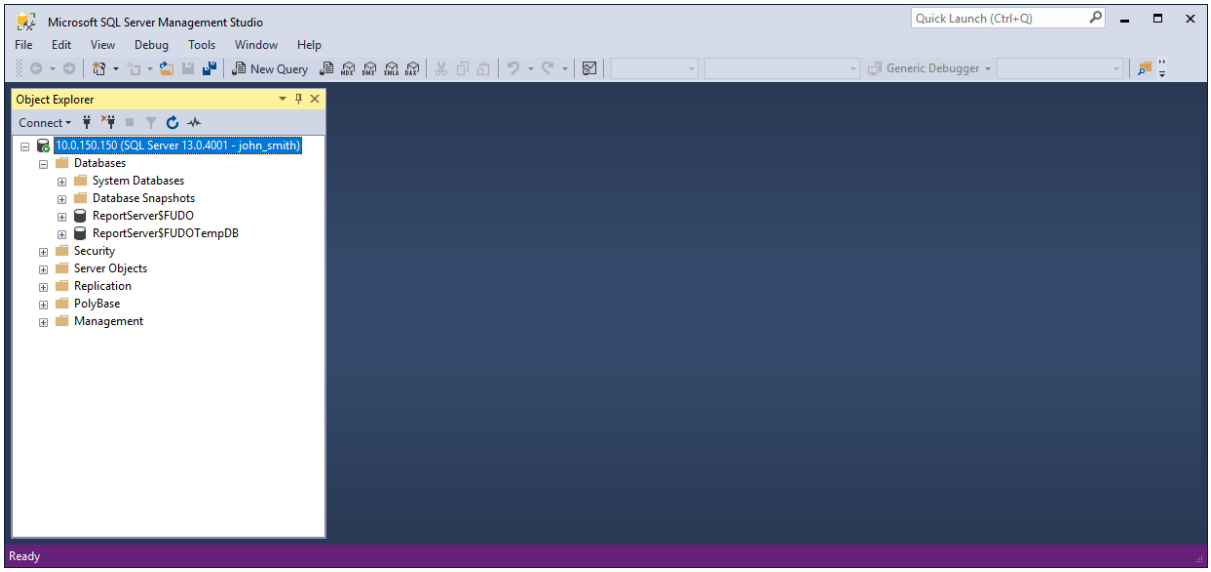
Related topics:

- *VNC*
- *Creating a VNC server*
- *Setting up the VNC listener*

28.4 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 29

Troubleshooting

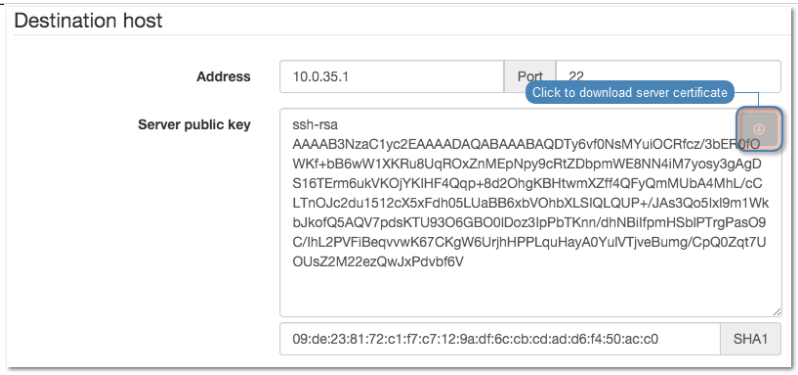
29.1 Booting up

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.

29.2 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.

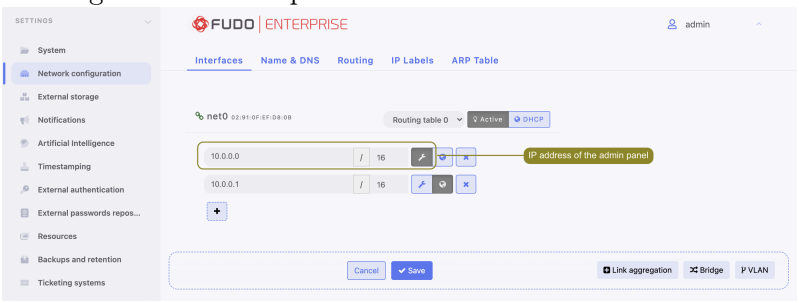
Problem	Symptoms and solution
When logging in not all of the users see the Fudo Enterprise logon screen.	**Cause:** • Credentials stored in RDP client result in users being automatically logged in to remote host. • Credentials stored in RDP client, user is successfully authenticated against credentials 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.

29.3 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. 

29.4 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.

29.5 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.

29.6 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*.

29.7 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*`.

```
GEOM_MIRROR: Cancelling unmapped because of gpt/system0-0.
GEOM_MIRROR: Device mirror/system0 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/system1-0.
GEOM_MIRROR: Device mirror/system1 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/system2-0.
GEOM_MIRROR: Device mirror/system2 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/swap0.
GEOM_MIRROR: Device mirror/swap0 launched (1/1).
Trying to mount root from ufs:/dev/mirror/system1 []...
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $
```

4. 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.

```
GEOM_MIRROR: Device mirror/system1 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/system2-0.
GEOM_MIRROR: Device mirror/system2 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/swap0.
GEOM_MIRROR: Device mirror/swap0 launched (1/1).
Trying to mount root from ufs:/dev/mirror/system1 []...
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24):
```

5. 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.

```
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24): 10.0.150.155/16
Enter default gateway IP address: 10.0.0.1
res0: link state changed to DOWN
add net default: gateway 10.0.0.1
SSH Fingerprint: SHA256:dgu2Ec8deFWPZkIxJk6EV9loggwm+OKXERsW+2PQBSY
res0: link state changed to UP
^CDec 21 13:31:56 init: single user shell terminated, restarting
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
ifconfig: ioctl SIOCSIFNAME (set name): File exists
ifconfig: ioctl SIOCSIFNAME (set name): File exists
Available network interfaces:

    res0 08:00:27:75:7f:ba
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1):
```

Related topics:

- *Network Interfaces Configuration*
- *System maintenance*

CHAPTER 30

Use Cases

30.1 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.

30.1.1 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
VNC	available	available

Continued on next page

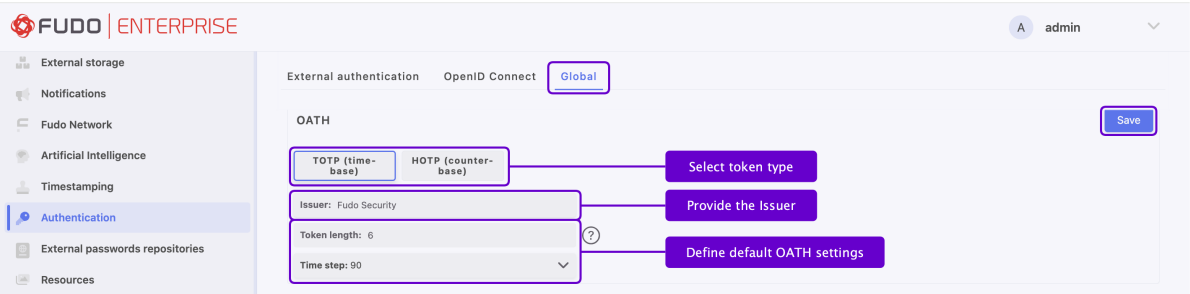
Table 1 – continued from previous page

Platform or Protocol	Challenge-Response Mode	Password + Dynamic Code
SSH	available	available
RDP	available	available
Telnet 3270	not available	available
Telnet 5250	not available	available
Telnet	not available	available
MS SQL(TDS)	not available	not available
HTTP/S	not available	not available
TCP	not available	not available
MySQL	not available	not available
X11	not available	not available
Modbus	not available	not available

30.1.2 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 *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*.

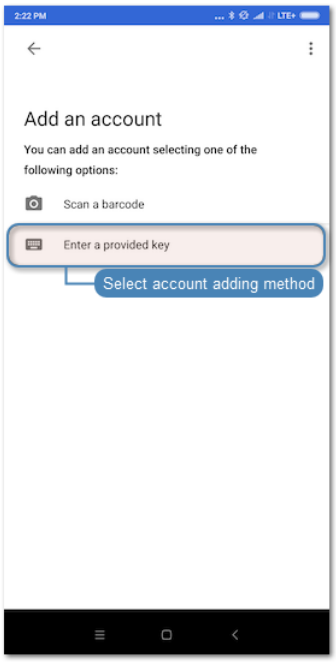
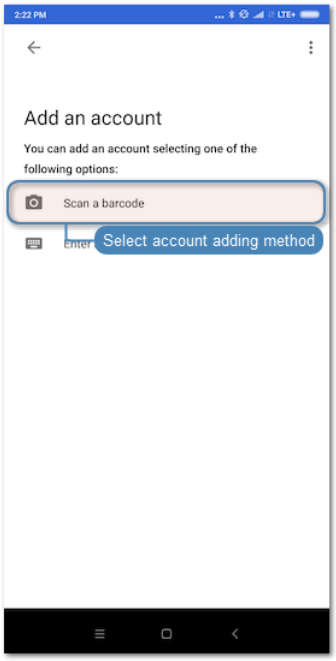
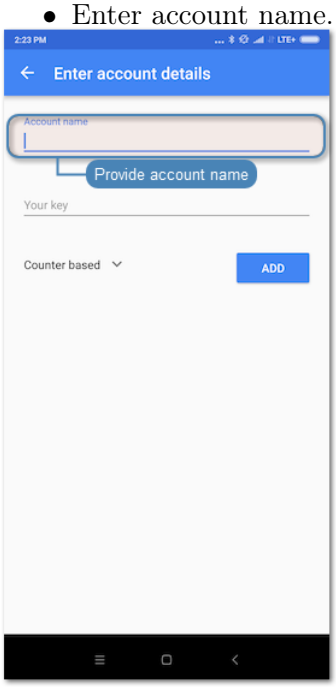
If `External authentication` is chosen:

- 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: 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.

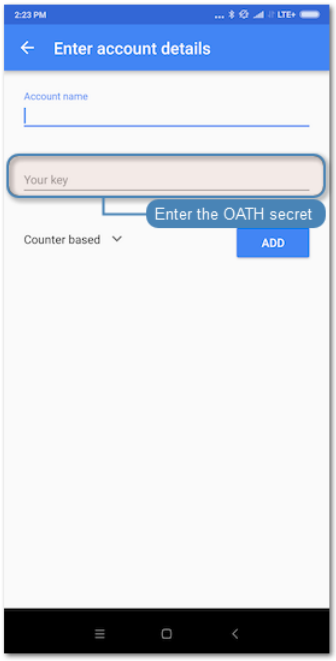
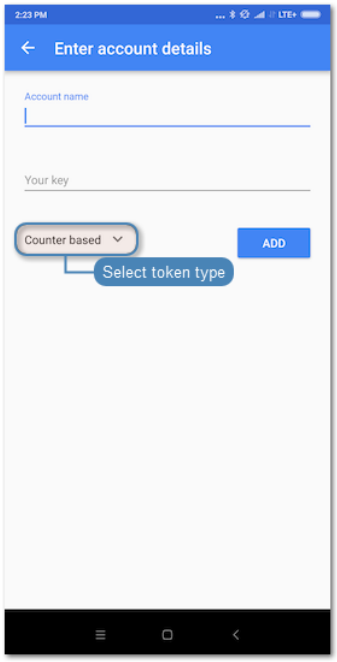
---

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. 	

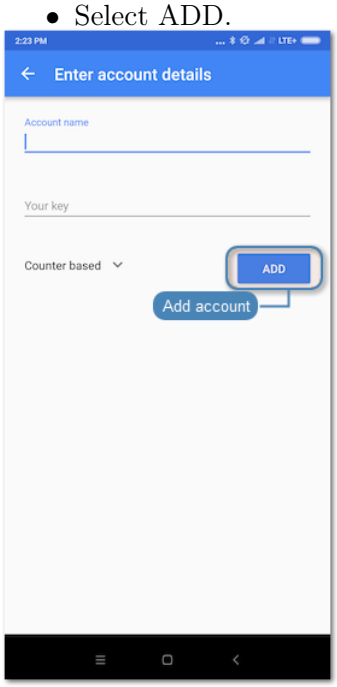
Continued on next page

Table 2 – continued from previous page

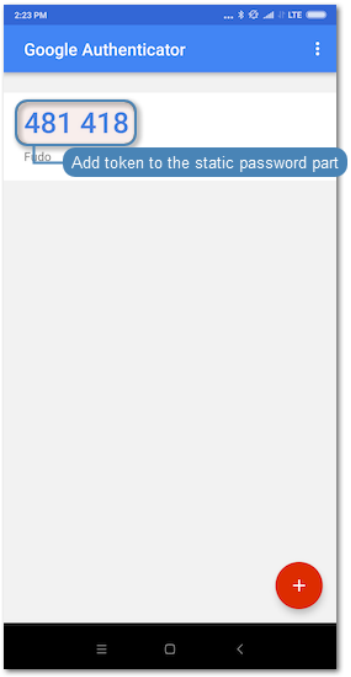
Manual entry	QR Code
• Enter the secret defined in OATH authentication method. **Note:** Click  on the user configuration form in the *Authentication* section to reveal the secret. 	
• Select *Counter based*. 	

Continued 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`.



Related topics:

- *User authentication methods and modes*

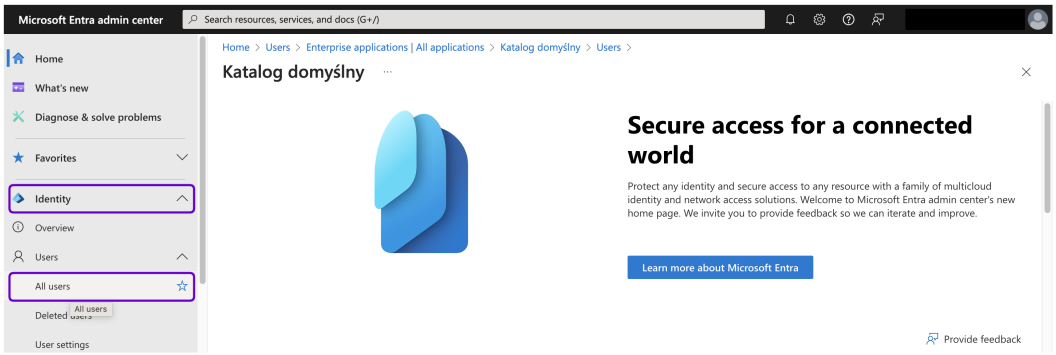
30.2 OpenID Connect authentication definition with Microsoft Entra (Azure)

To configure the OpenID Connect authentication method with Microsoft Entra, please follow below steps.

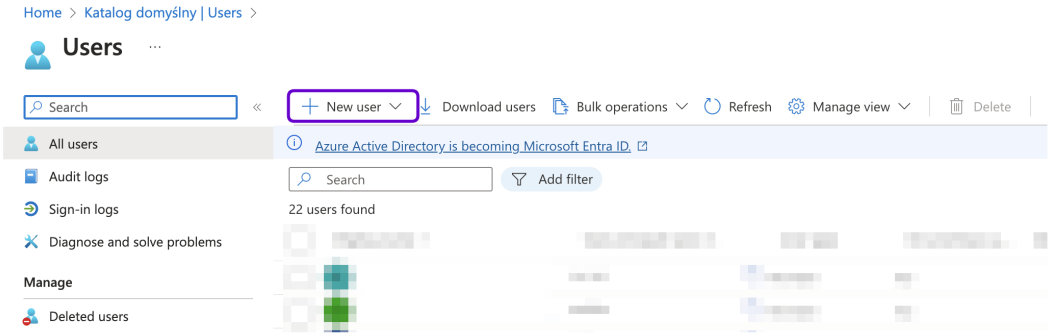
Note: Please note that this is a general guide, and specific details may vary depending on your Microsoft Entra setup. Refer to Microsoft Entra documentation for precise configuration steps.

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 *Identity* > *Users* > *All users*.



4. Click the *+ New user* and select *Create new user* from the drop-down list.

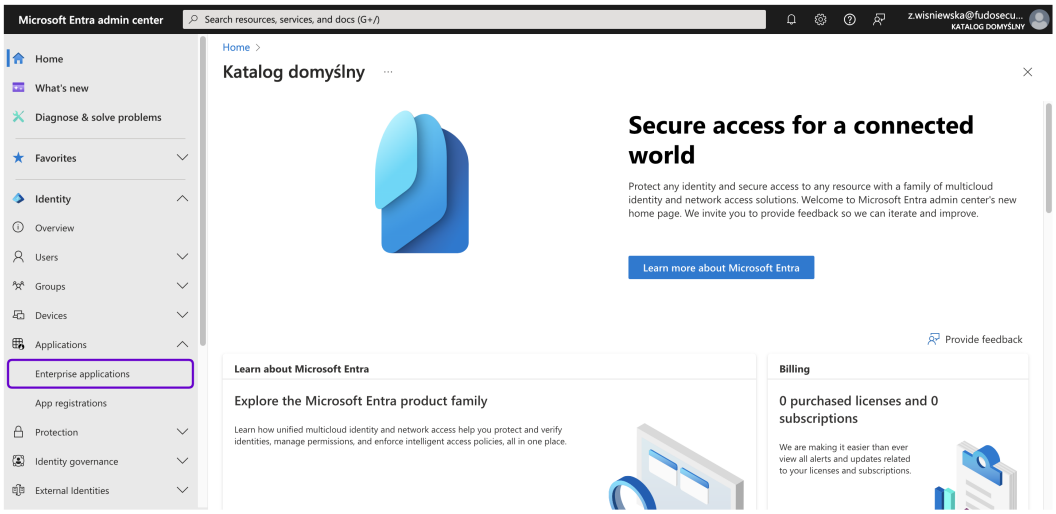


5. In the *User principal name* field, enter the username of the user account. For example, `user1@fudosecurity.com`.
6. In the *Display name* field, provide the name of the user of the account.
7. Provide the password phrase in the *Password* field or click the *Auto-generate password* option to generate 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.

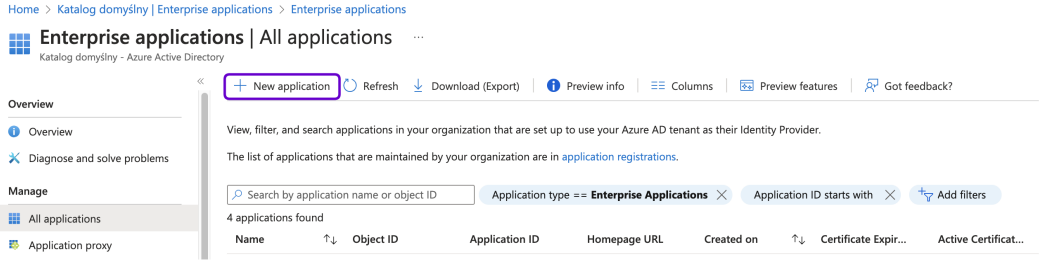
11. Click *Create*.

Register Fudo in Microsoft Entra ID

1. In the left-hand menu, select *Identity* > *Applications* > *Enterprise applications*.



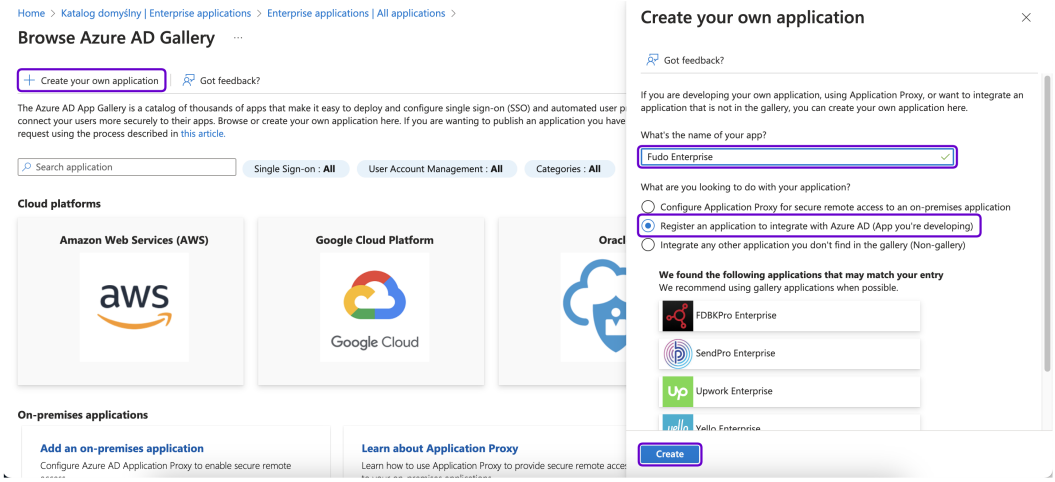
2. Click the *+ New application* button to create a new application.



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*.

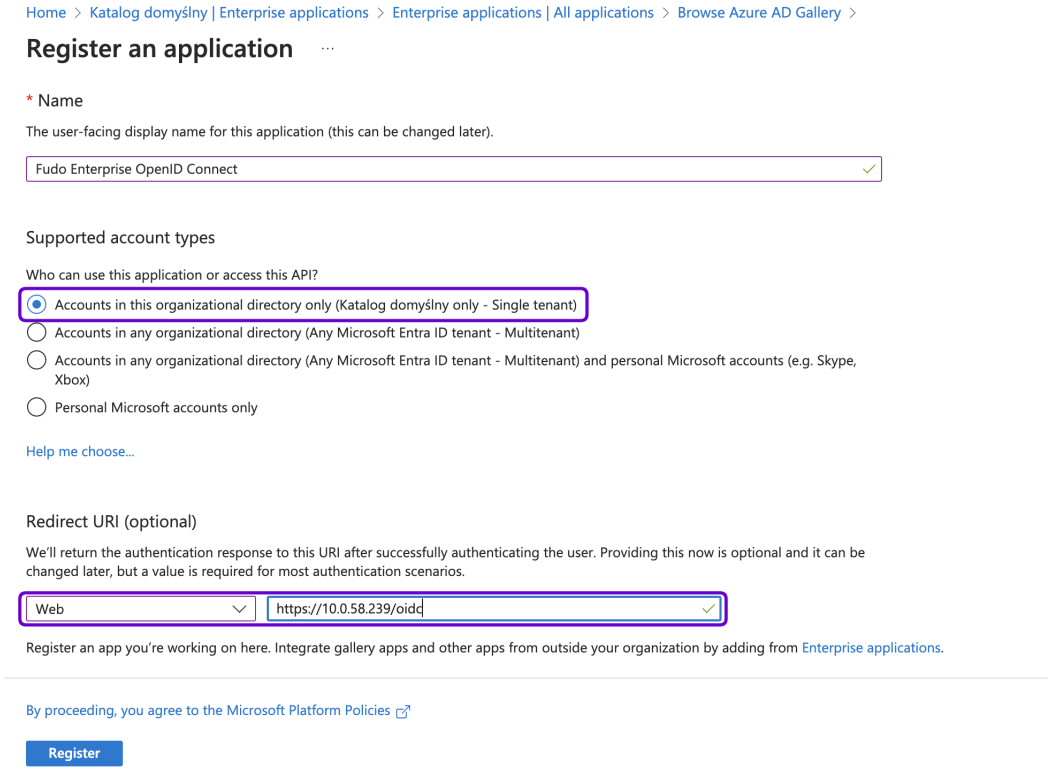


6. In the next page, under the *Supported account types* select the *Accounts in this*

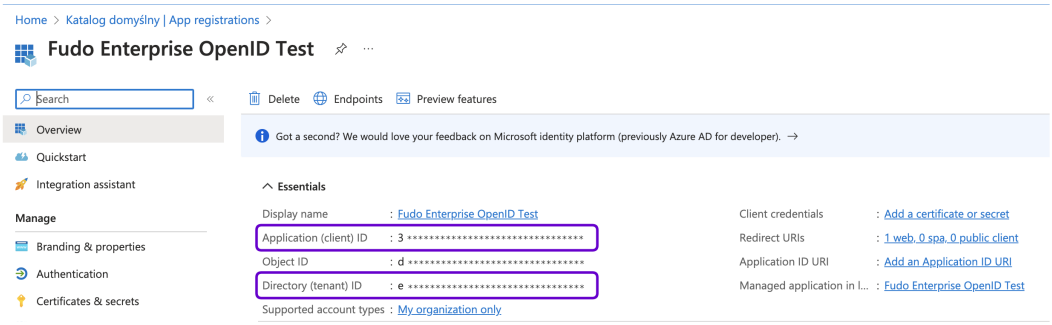
organizational directory only (This Directory only - Single tenant) option.

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 Access Gateway address under the Settings > Network configuration menu in the Fudo Enterprise. For more information, please follow the *Network settings* section.

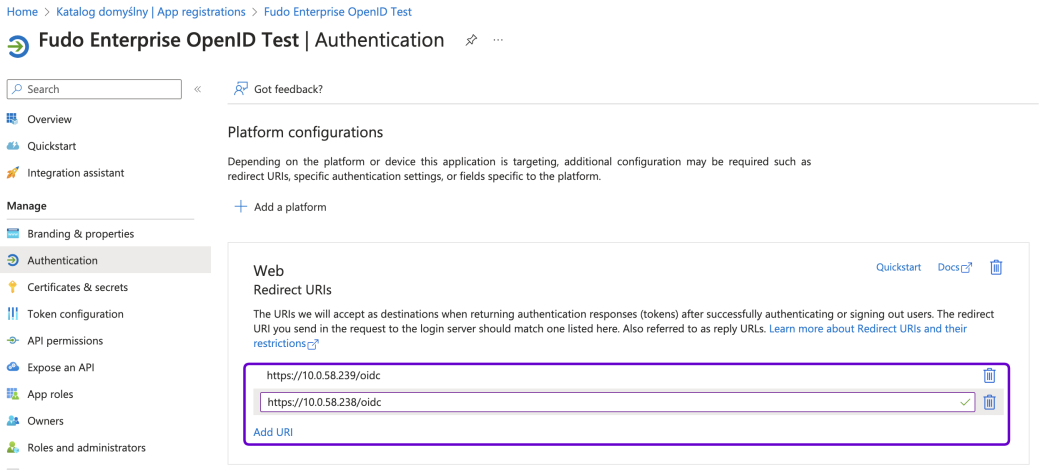


8. Click *Register* to create the application.
9. In the left-hand menu, select *Identity* > *Applications* > *App registrations*.
10. Change to *All applications* tab and find created application on the applications list.
11. Click on it's name to edit the parameters. Note down the *Application (client) ID* and *Directory (tenant) ID* as you will need these later.

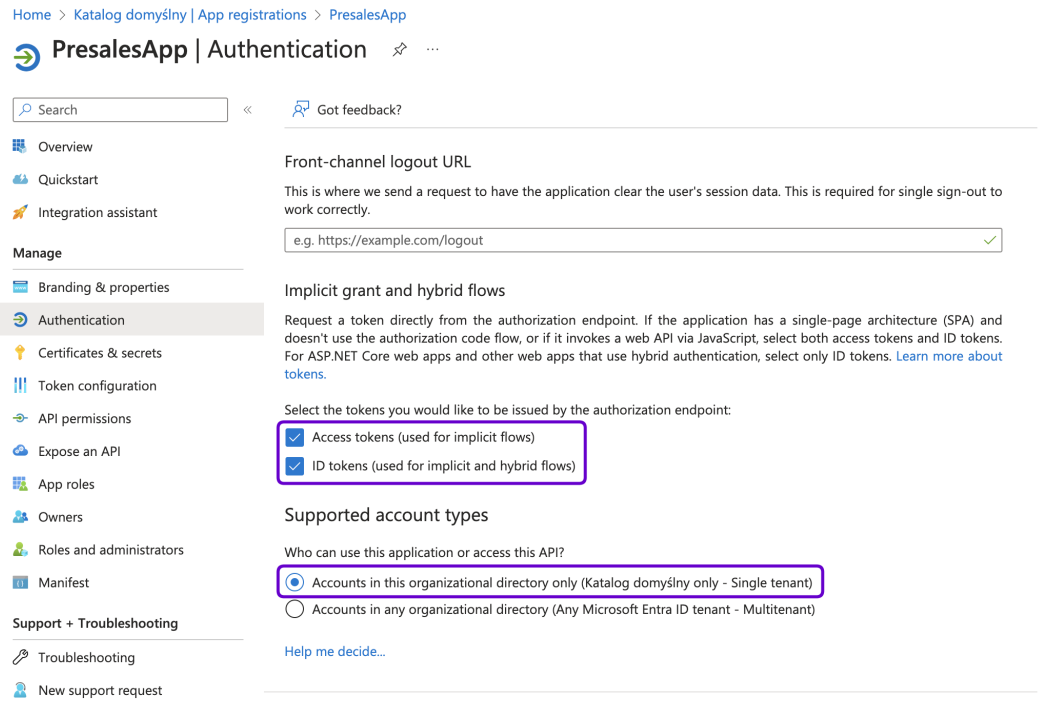


Configure Authentication Setting

1. In the left-hand menu, select *Identity* > *Applications* > *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 *Web* platform created for Fudo Enterprise add the *Redirect URI(s)* following to the Admin Panel with the `/oidc` suffix. For example, `https://10.0.58.238/oidc` or `https://fudo.example.com/oidc`.



5. In the *Implicit grant and hybrid flows* section, check *ID tokens* and *Access tokens* options.



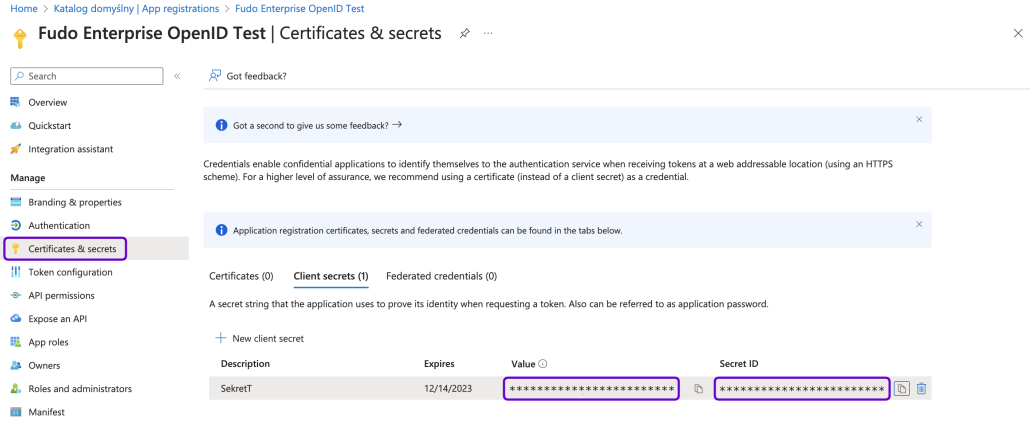
6. In the *App instance property lock* section, click *Configure* and uncheck the *Enable property lock* option in the right-hand dialog box. Click *Save* to close the dialog box.

7. Click *Save* to save your authentication settings.

Generate Client Secret

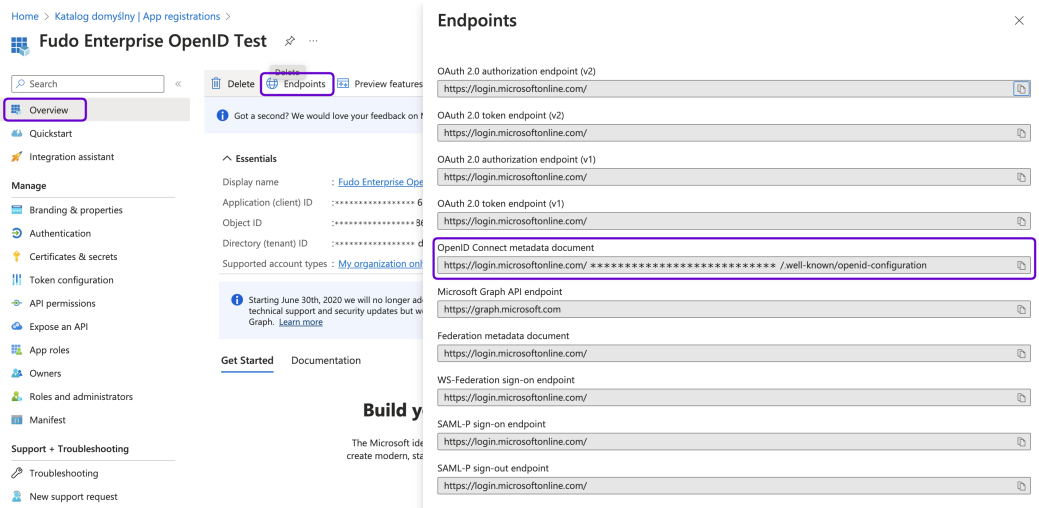
1. In your application's settings, navigate to the *Certificates & secrets* section.
2. Under the *Client secrets* section, click *+ New client secret.*
3. Provide a description, select the desired expiration period, and click *Add.*

> **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.



Get OpenID Connect Configuration URL

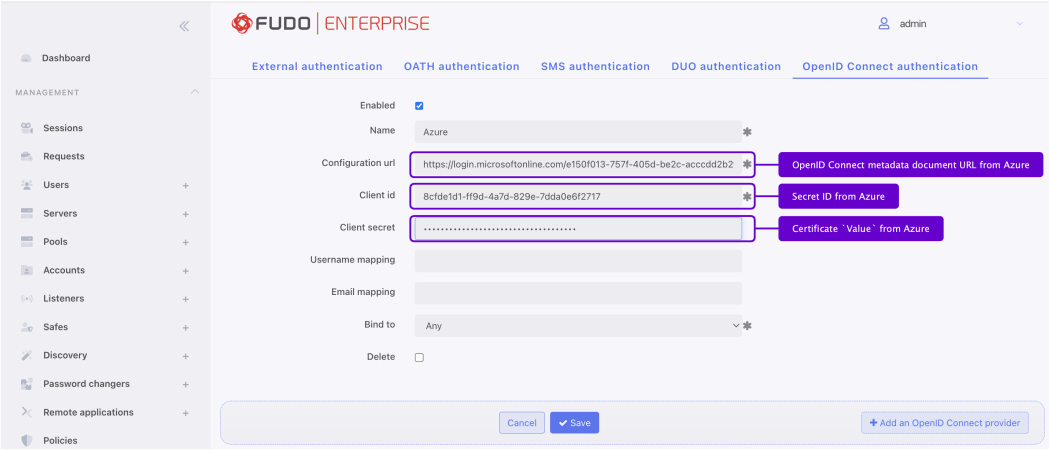
1. In your application's settings, navigate to the *Overview* section.
2. Open the *Endpoints* tab, and look for the *OpenID Connect metadata document* URL. This is your OpenID Connect Configuration URL. Copy it as you'll need it for Fudo Enterprise configuration.



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 *Secret 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.

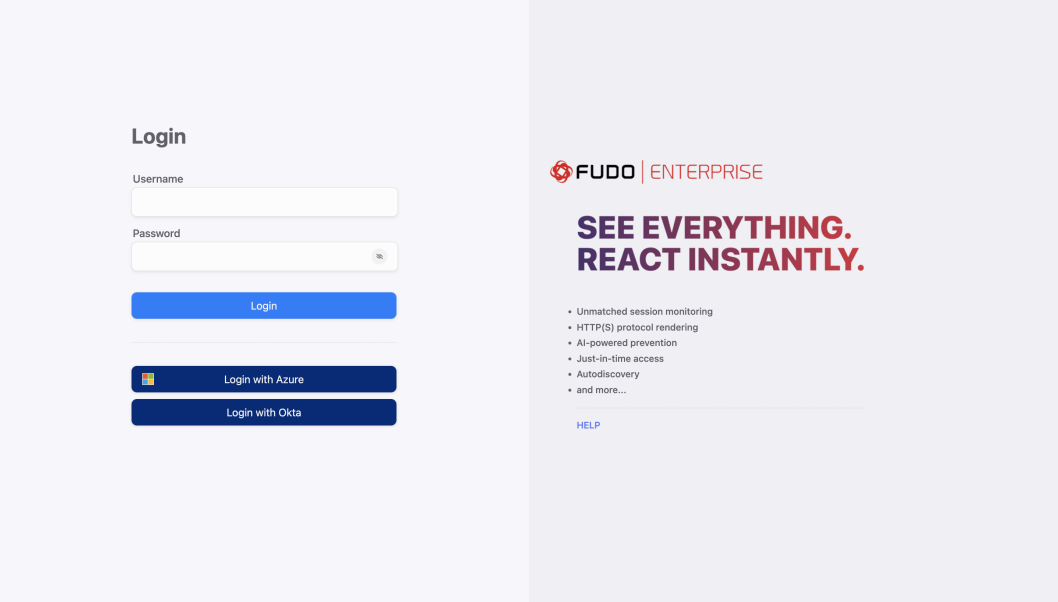
Create new user in Fudo

1. Select *Management* > *Users* and then click + *Add user*.
5. 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*

30.3 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.
- Support for **gateway** and **transparent** listeners in RDS has been removed.

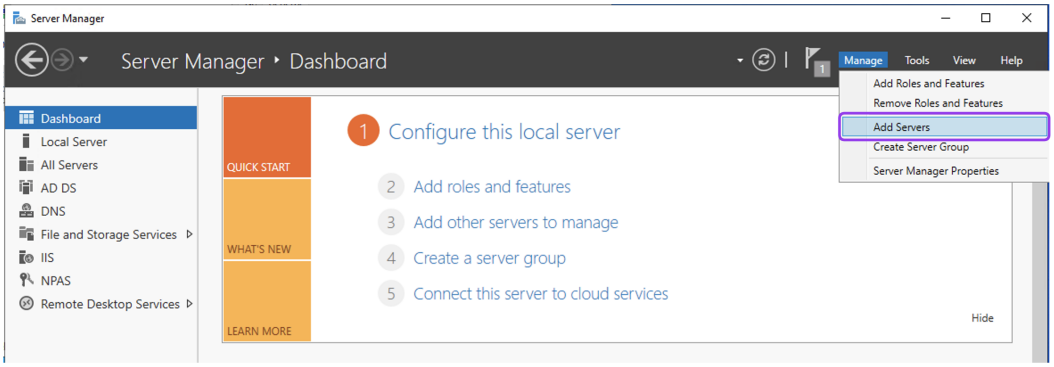
30.3.1 Setup Remote Desktop Services (RDS) on Windows

To configure and use the Remote Desktop Services (RDS) with Fudo Enterprise, please follow below steps.

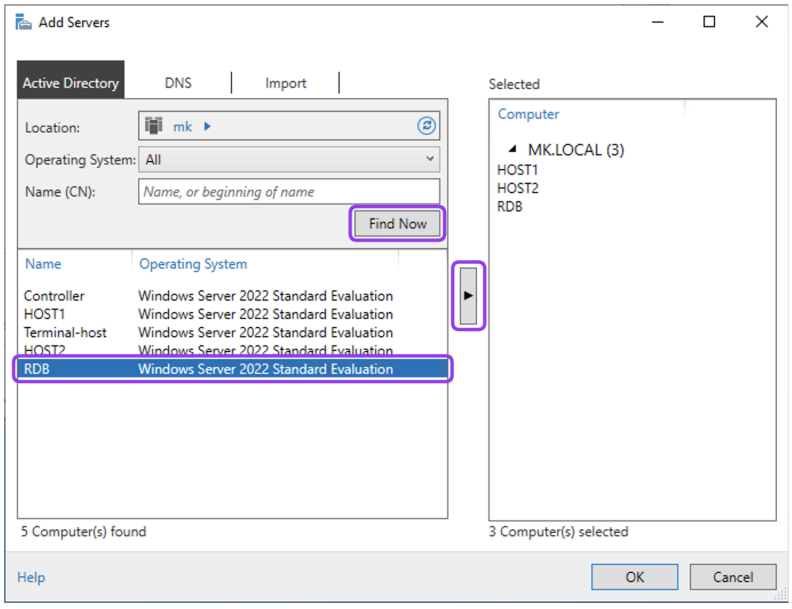
Note: Please note that this is a general guide, and specific details may vary depending on your Windows Server setup. Refer to the Windows Server documentation for precise configuration steps.

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*.

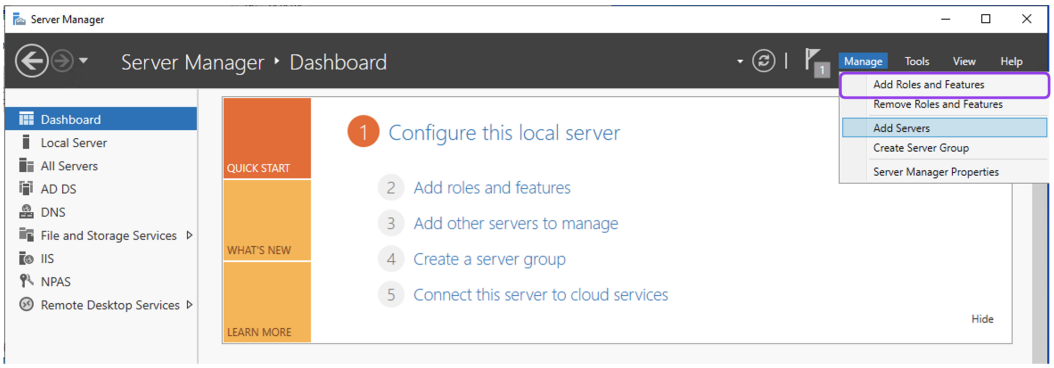


4. Click *Find Now*.
5. Add all the servers you're going to use for RDS by clicking on each server in the deployment. Click *OK*. In this use case we add 3 servers: `HOST1`, `HOST2`, and `RDB` which will play the Broker role.

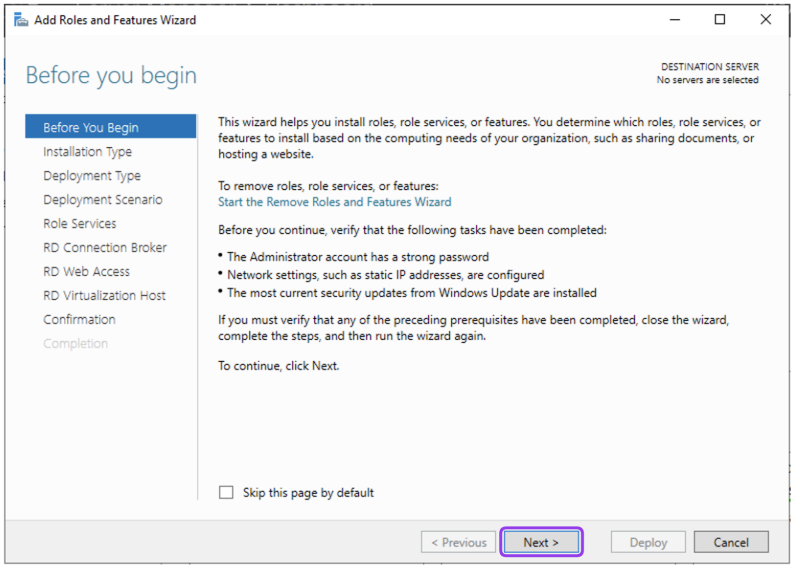


Deploy the Remote Desktop Services Components:

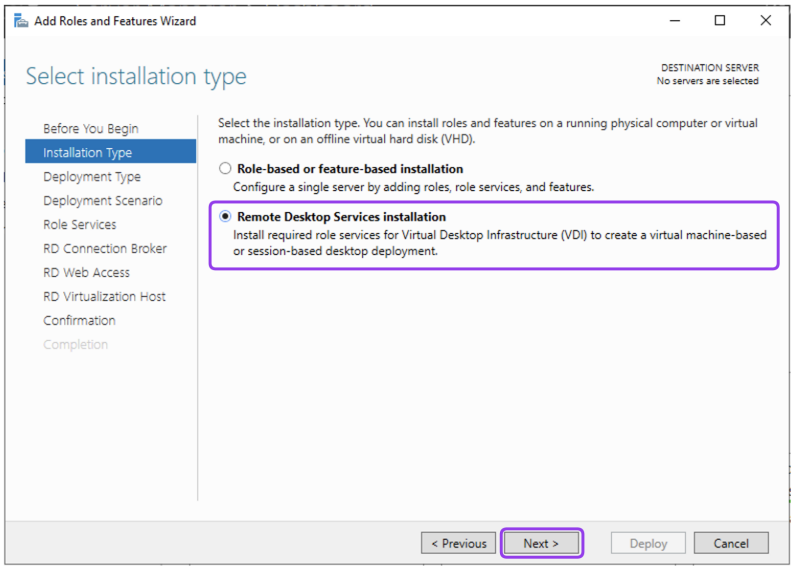
1. Click *Manage* button on the upper right corner of the window to expand the menu list and select *Add Roleas and Features*.



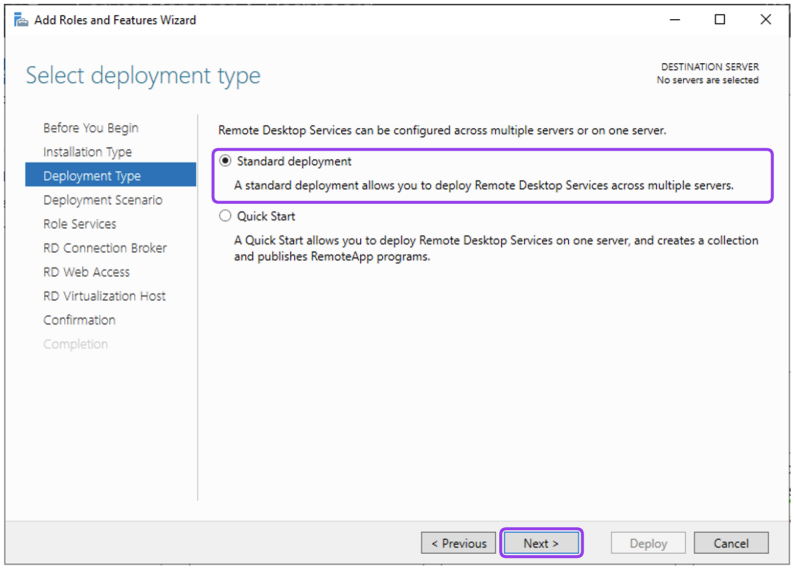
2. On the *Before You Begin* tab, click *Next* to proceed.



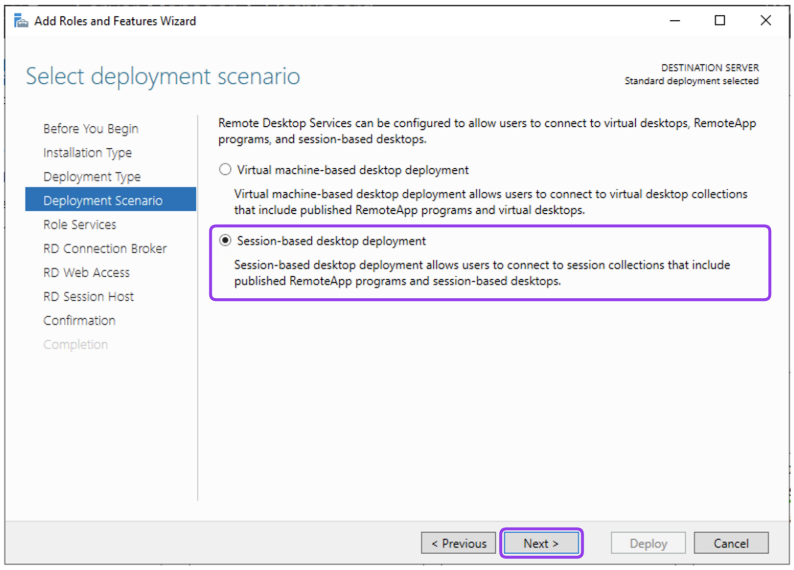
3. On the *Installation Type* tab, select *Remote Desktop Services installation*, and click *Next* to proceed.



4. On the *Deployment Type* tab, select *Standard Deployment* to access more detailed instructions for installing Remote Desktop Services. Click *Next* to proceed.

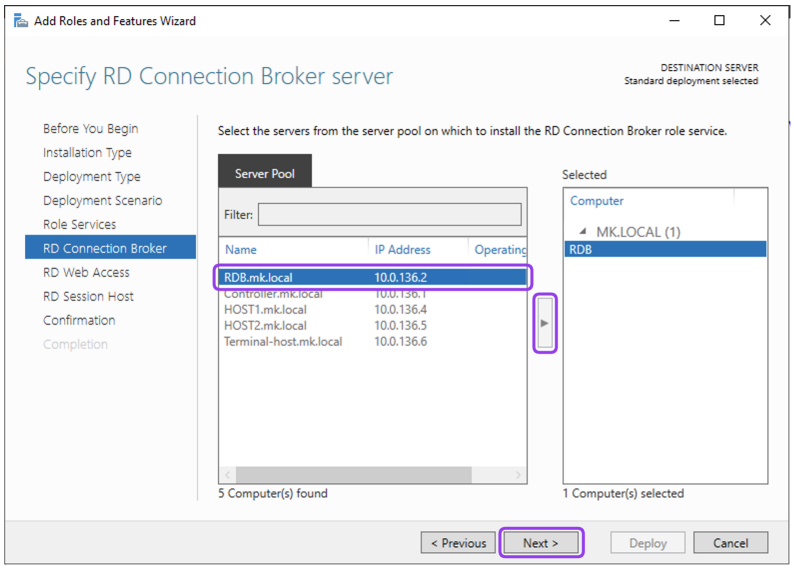


5. On the *Deployment Scenario* tab, select *Session-based desktop deployment*. Click *Next* to proceed.

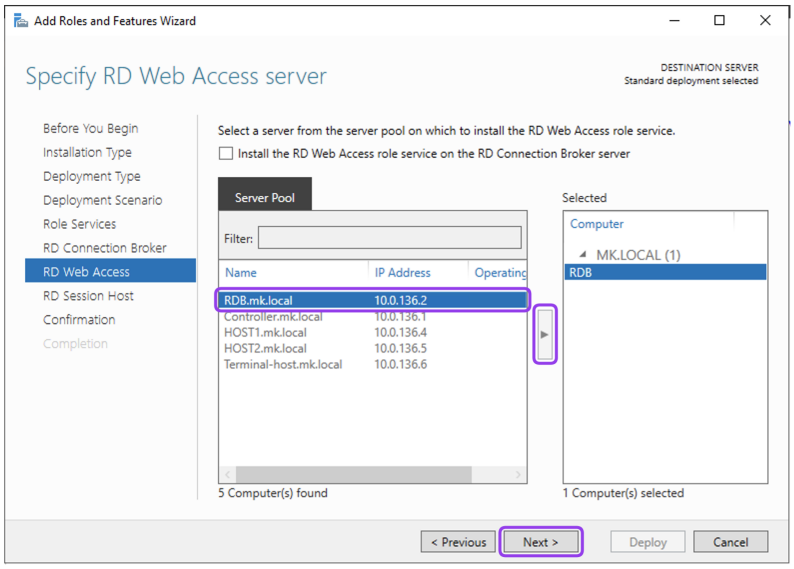


6. On the *Role Services* tab, review the services that will be installed. Click *Next* to proceed.

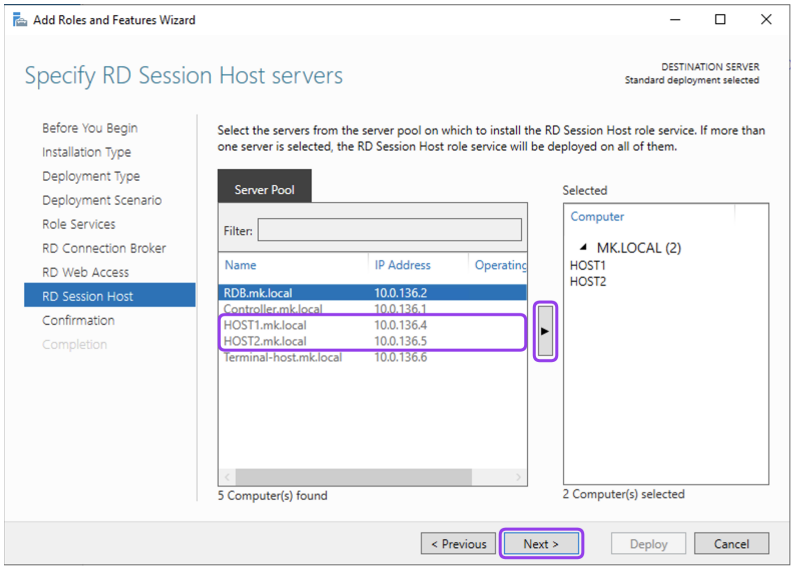
7. On the *RD Connection Broker* tab, select the appropriate server on which to install the RD Connection Broker role service. In this example `RDB` server was selected. Click *Next* to proceed.



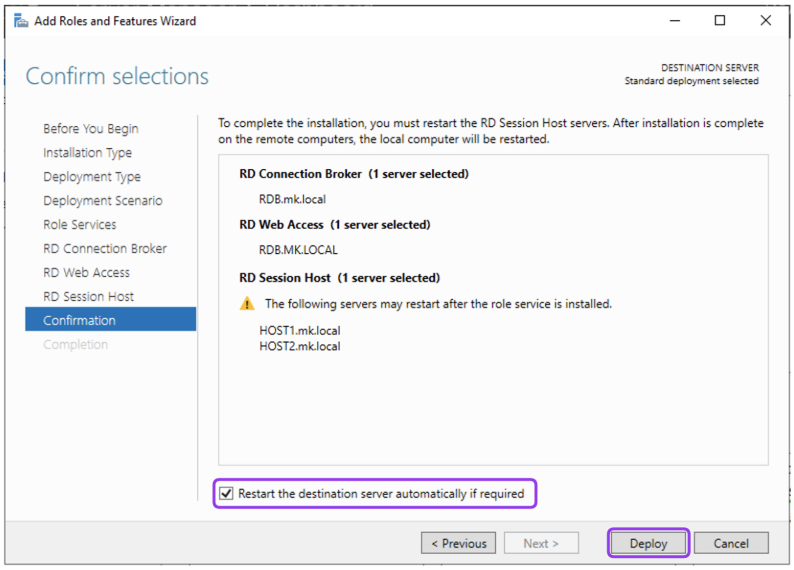
8. On the *RD Web Access* tab, select the appropriate server on which to install the RD Web Access role service. In this example, the `RDB` server was also selected. Click *Next* to proceed.



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.



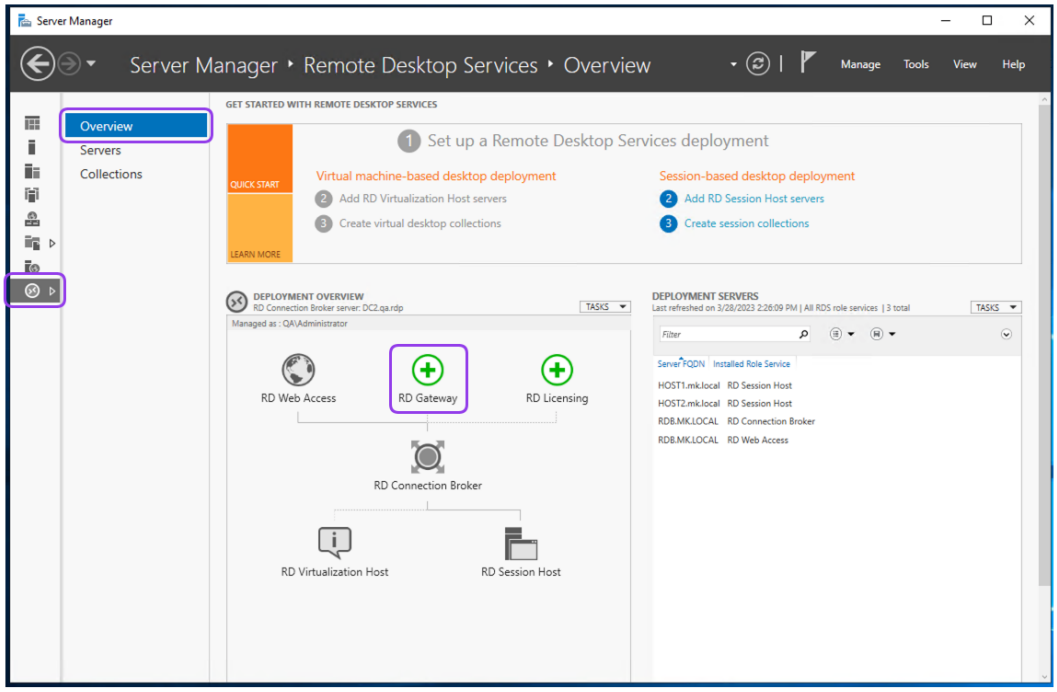
10. On the *Confirmation* tab, select *Restart the destination server automatically if required*, and then click *Deploy*.



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.

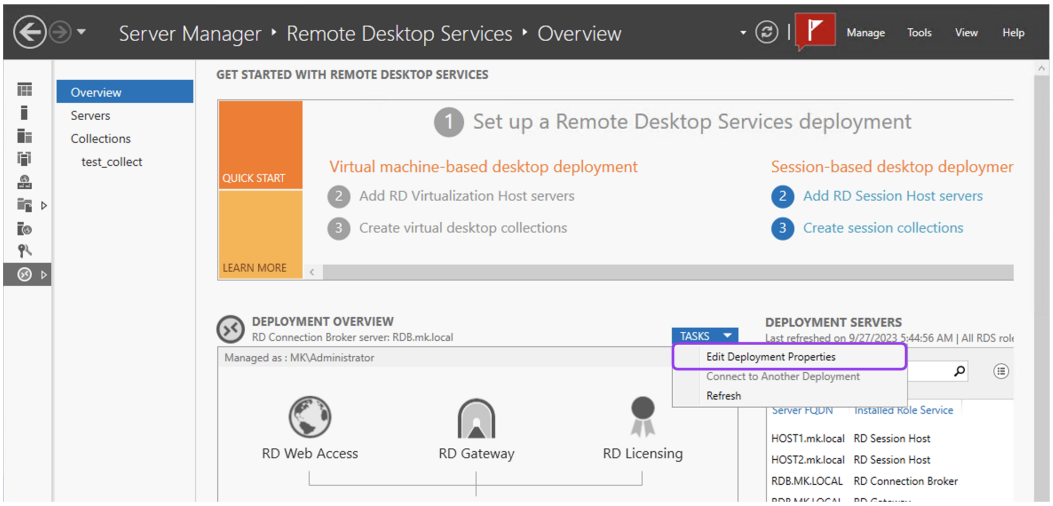


3. Click *Next*.
4. Enter the SSL certificate name for the RD Gateway server using the external fully qualified DNS Name (FQDN) of the RD Gateway server. Example, `cert.mk.local`.

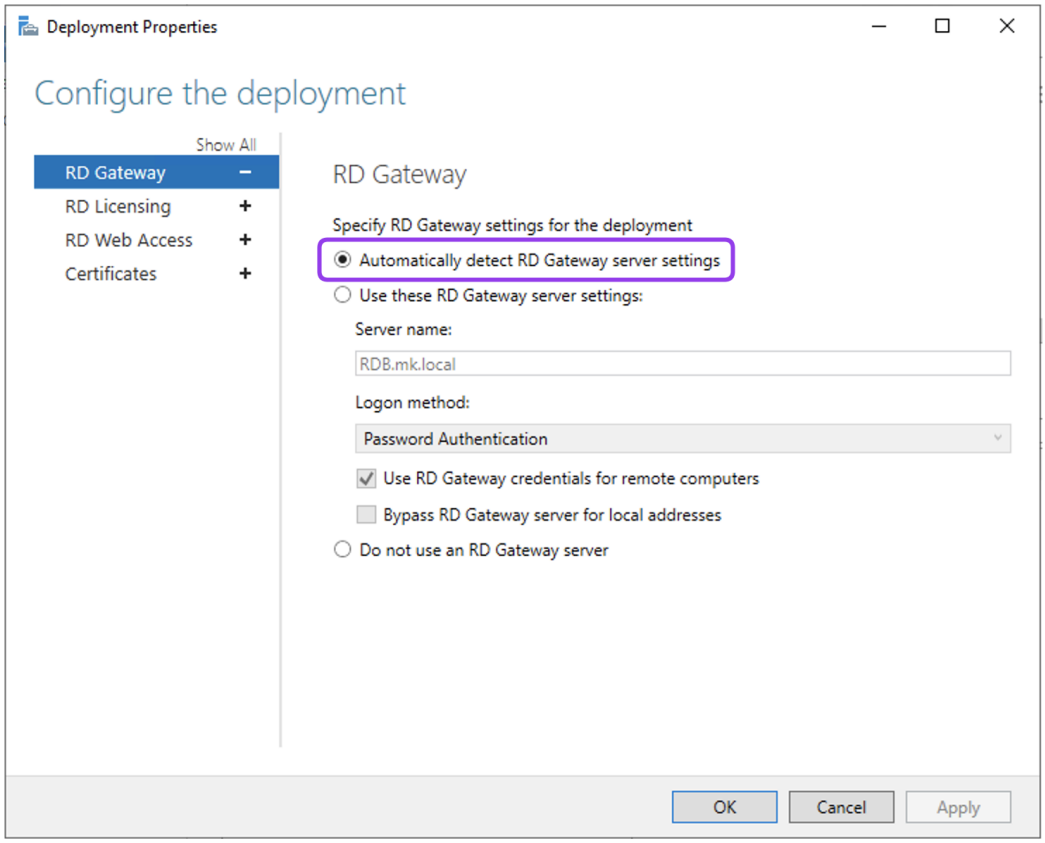
5. Click Next, and then click *Add*.
6. Wait until the role service is deployed and click *Close*.

Configure the RD Gateway and RD Licensing deployment properties:

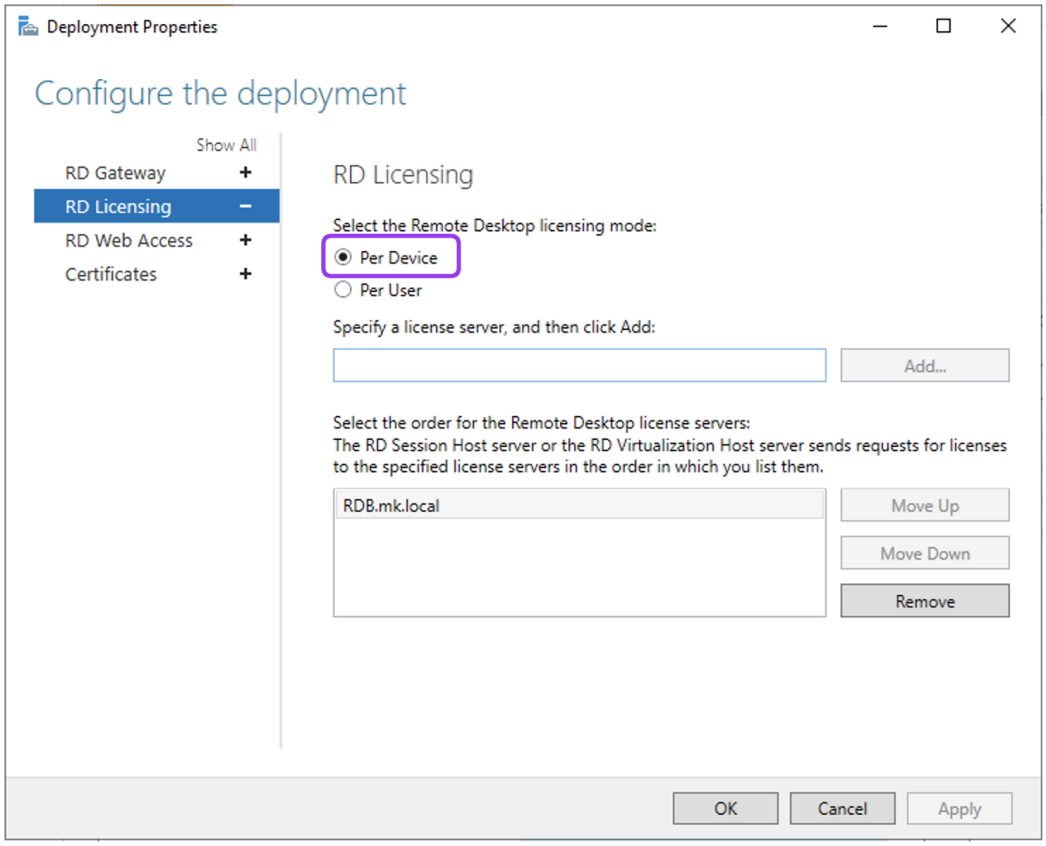
1. Go back to the *Overview* tab, click *Tasks* and select *Edit Deployment Properties* from the drop down list.



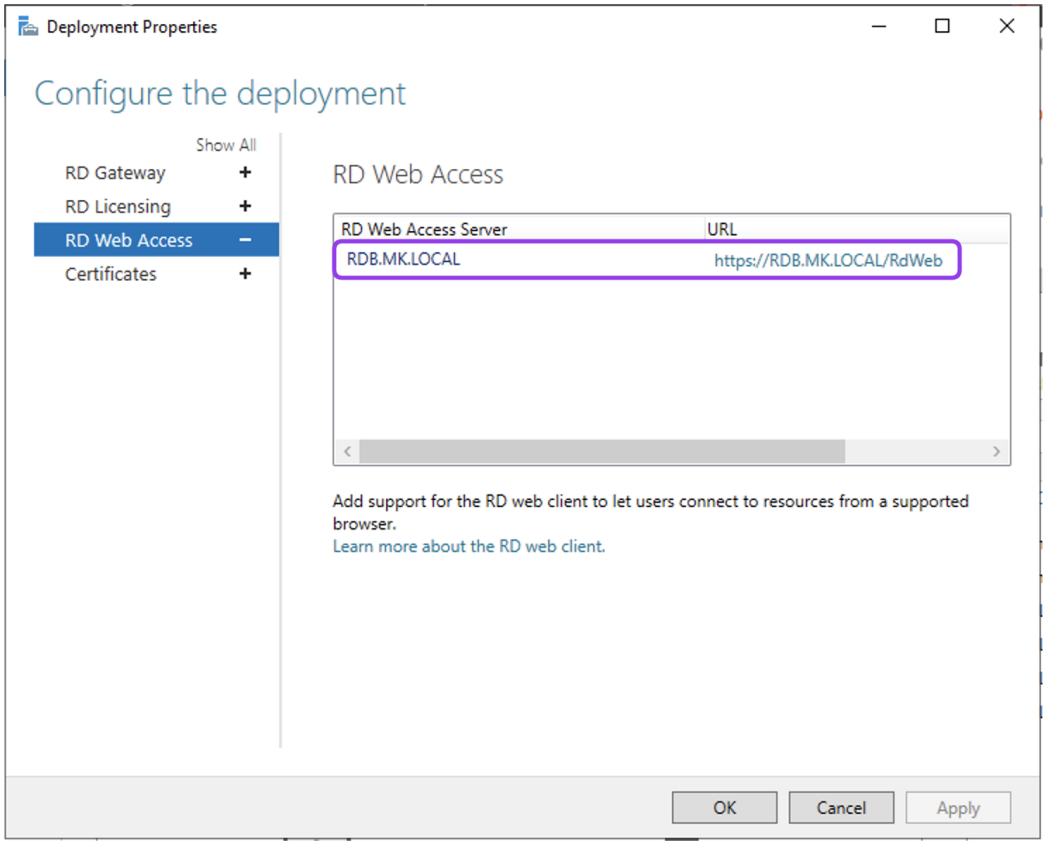
2. On the *RD Gateway* tab, select *Automatically detect RD Gateway server settings* option and click *Apply*.



3. Expand the *RD Licensing* tab and select *Per Device*. Click *Apply*.

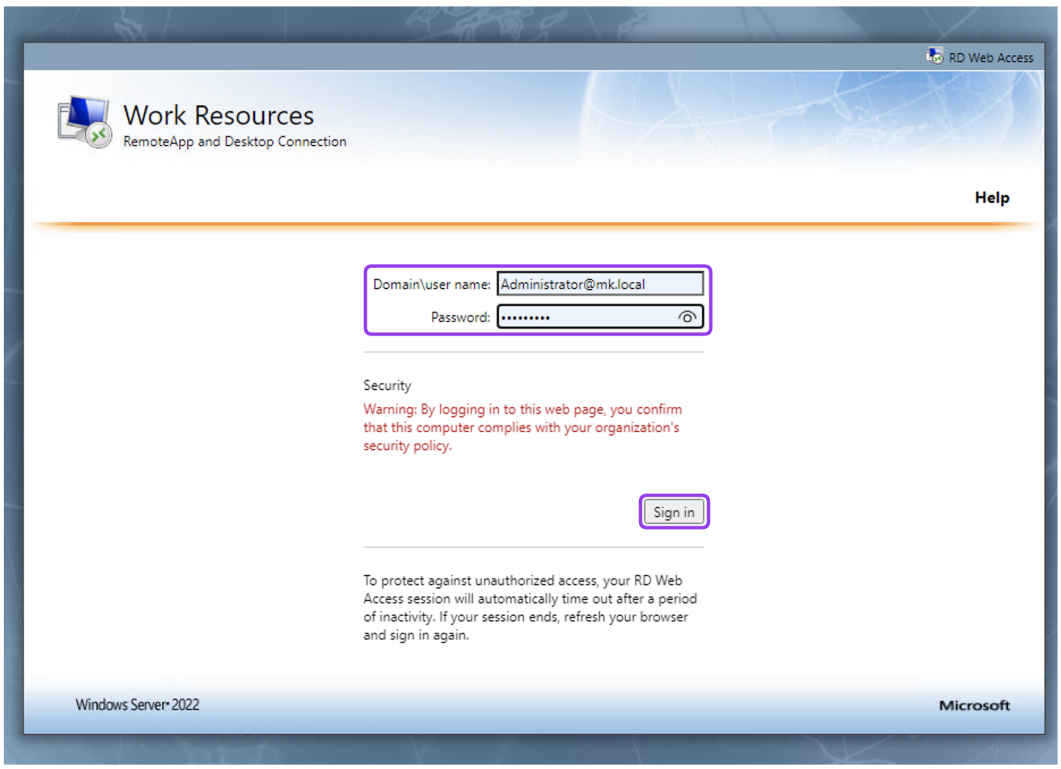


4. Expand the 'RD Web Access' tab, to check the RD Web Access IIS application URL. It is installed by default under the `/RdWeb`.



5. Click on the displayed URL to verify the RD Web Access login using the administrator account.

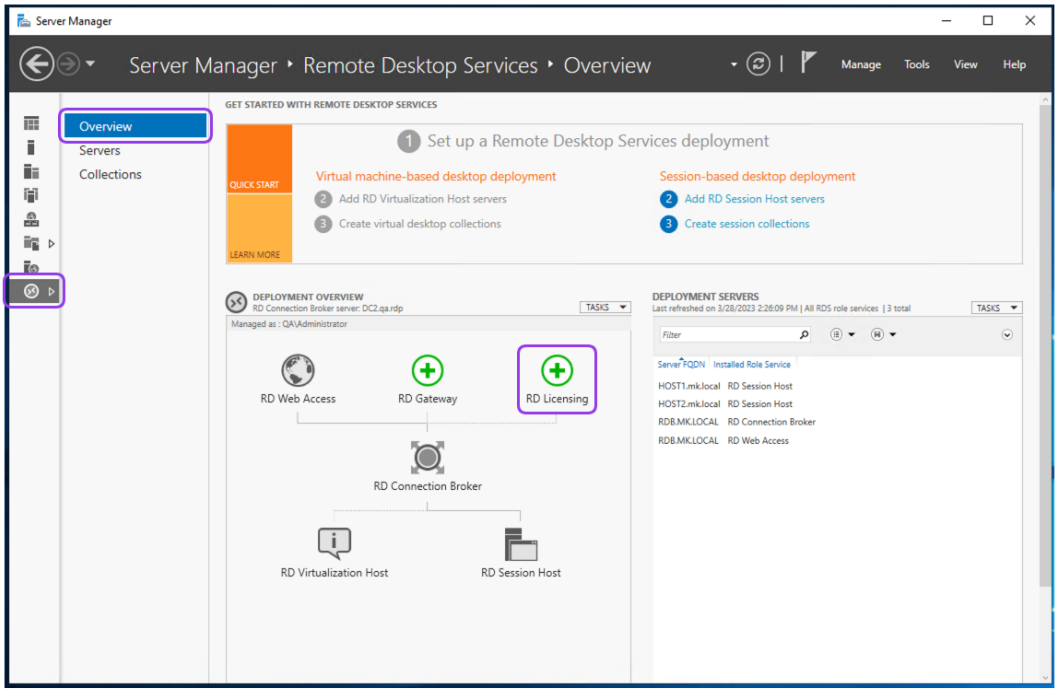
Note: While login, please use the domain in the *user name* field. For example, `Administrator@mk.local`.



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:

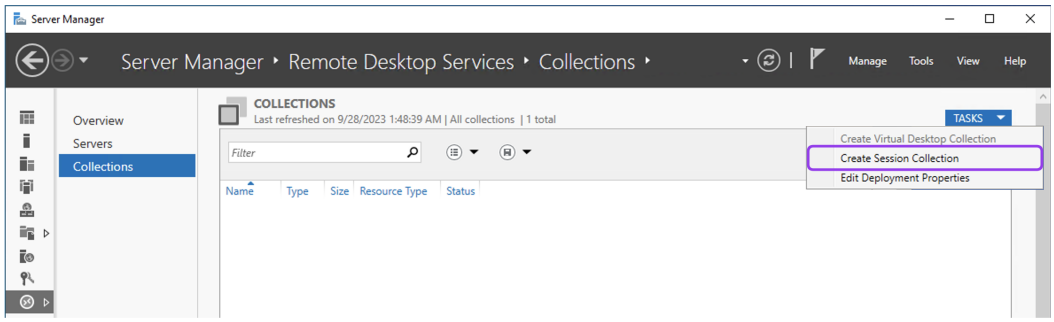
1. Click the *+ RD Licensing* button in the *Overview* tab of the *Remote Desktop Services* section.



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.

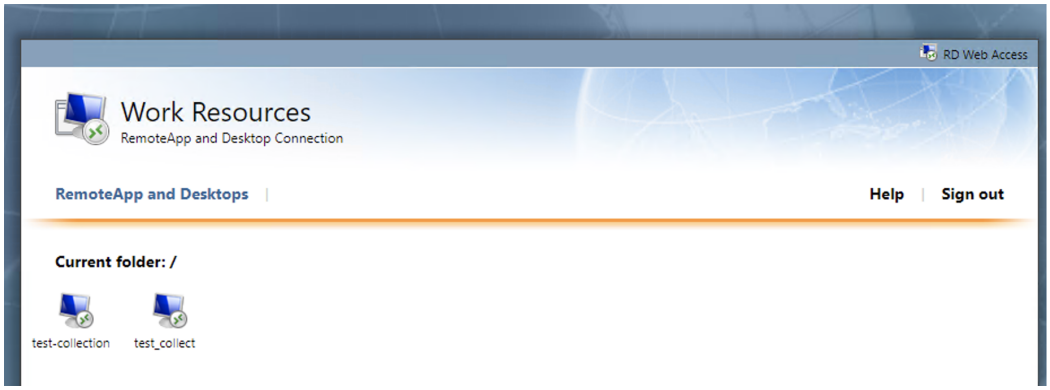
Note: This name will be displayed under its icon in the Web Access interface.

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).

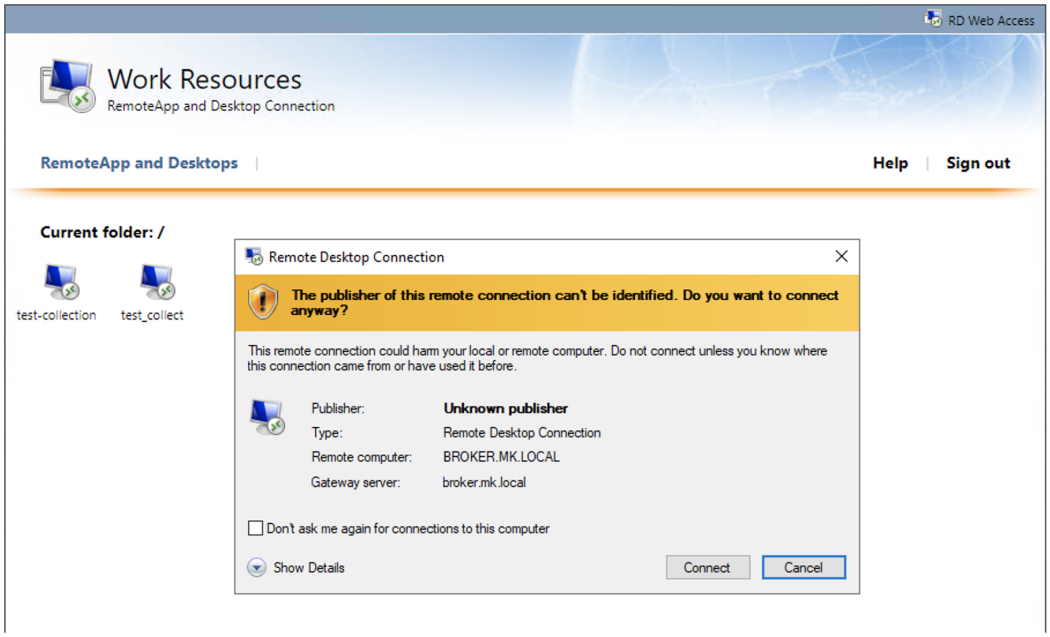
6. On the *User Profile Disks* tab, select *Enable User Profile Disks* option and specify the settings if needed. You can also leave this option disabled.
7. On the *Confirmation* tab, please review all the information and then click 'Create'.
8. Wait until the collection is created. Click *Close*.

Test the connection:

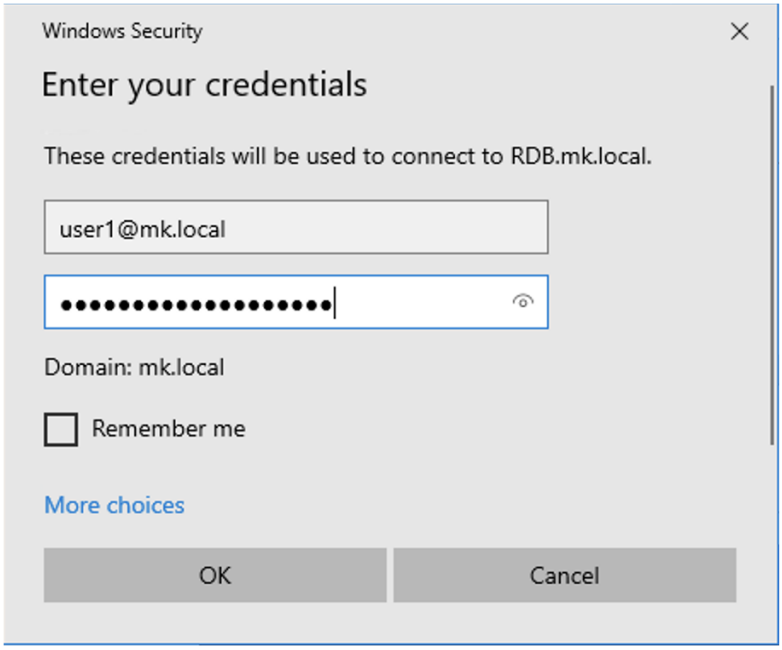
1. Open the RD Web Access URL saved in previous steps (e.g., `https://rdb.mk.local/RDWeb/`).
2. Enter a valid username and password and click *Sign in*. You can use the domain admin account to login, for example, `Administrator@mk.local`.
3. After logging in, the full collection of created desktop sessions 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*

30.3.2 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 *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*.

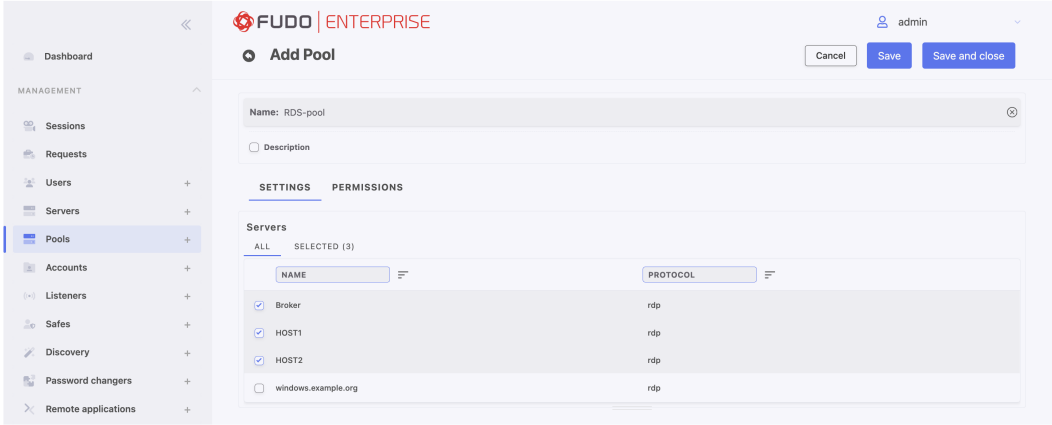
Configure Servers with the role of Session Hosts:

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:

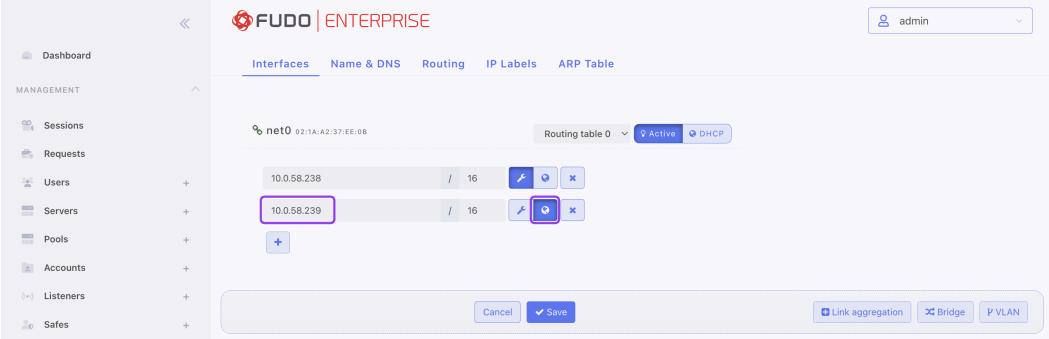
1. Select *Management* > *Safes* and then click *+ Add safe*.
2. Enter safe's unique name (e.g.,"rdp-safe").
3. Click *Save* to save the object and proceed with further configuration.
4. Go to the *Users* tab to assign users allowed to access accounts assigned to this safe.
   - Click *Manage users*.
   - 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 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 Access Gateway address in the *Settings* > *Network configuration* menu tab.

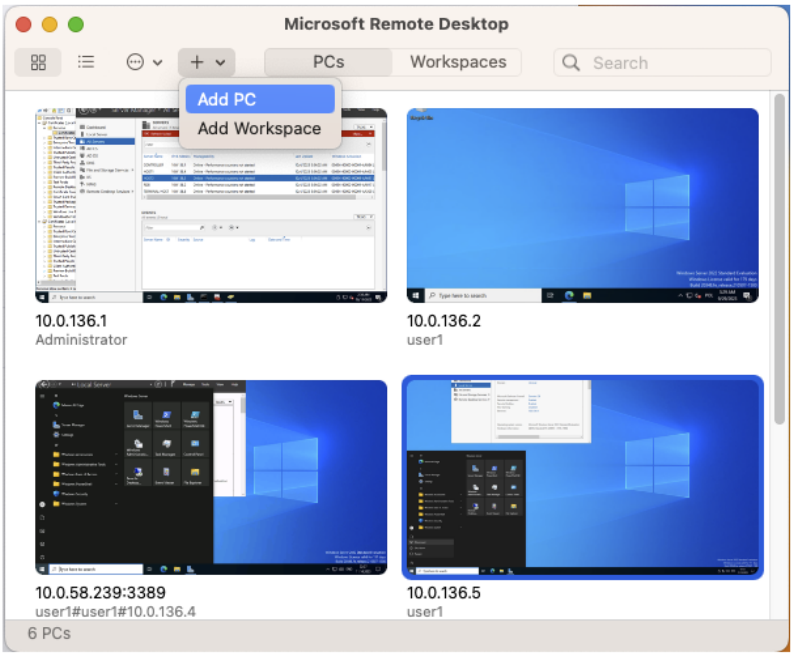


---

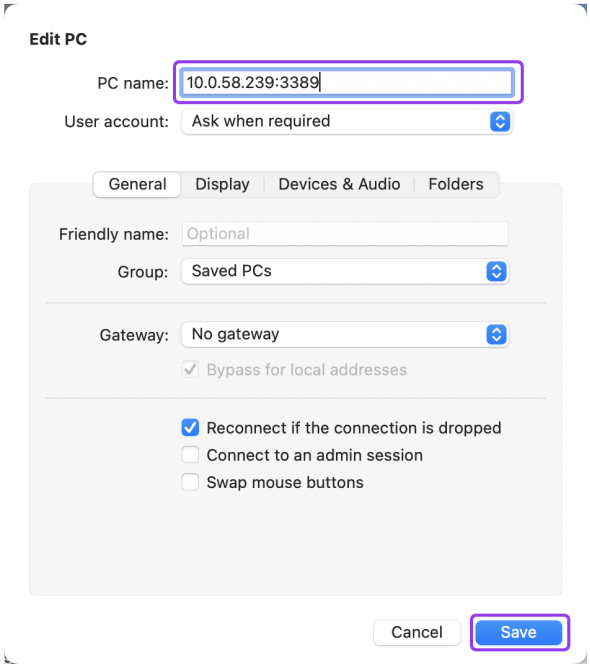
2. Hover the cursor over the `user1` account name, select *Native client* and click the *Connect* button to download the `.rdp` configuration file.
3. Open the downloaded file to establish a connection.
4. Enter the password for the `user1` account to log in to the server.

Redirect the connection through Fudo using RDP native client:

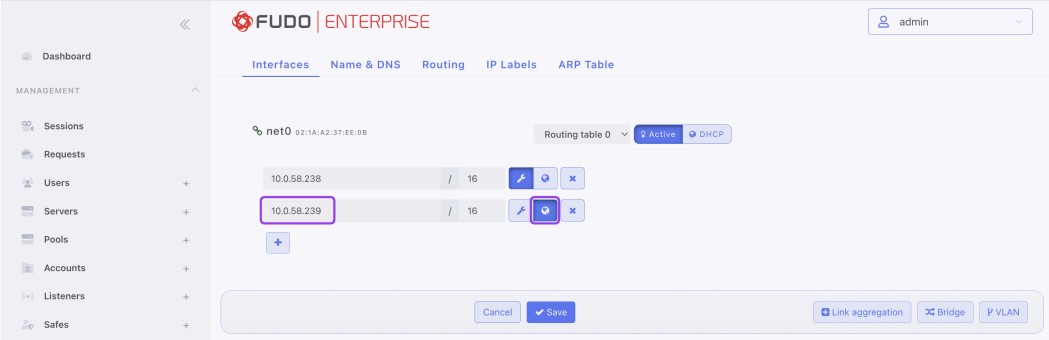
1. In order to redirect the connection through Fudo Enterprise, we need to use the Fudo Access Gateway address in the RDP client configuration.
2. Choose your favorite remote desktop client, such as Microsoft Remote Desktop, and follow its workflow to add a new PC for connection.
3. Following the example 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 Access Gateway address in the *Settings* > *Network configuration* menu tab.



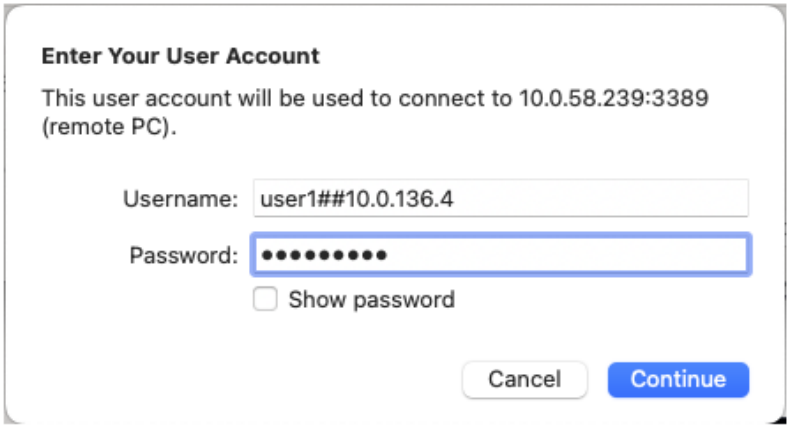
5. Connect to the added PC by providing the bastion login string in *Username* field and password in the *Password* field.

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.

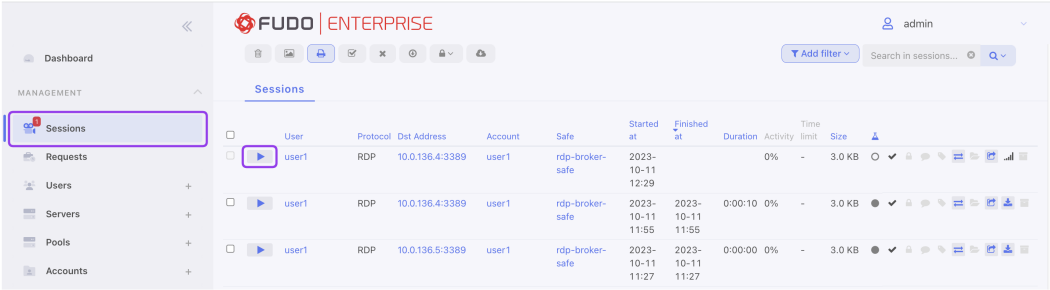
- You can skip the account login if it's the same as the user name, e.g, `user1##10.0.136.4`

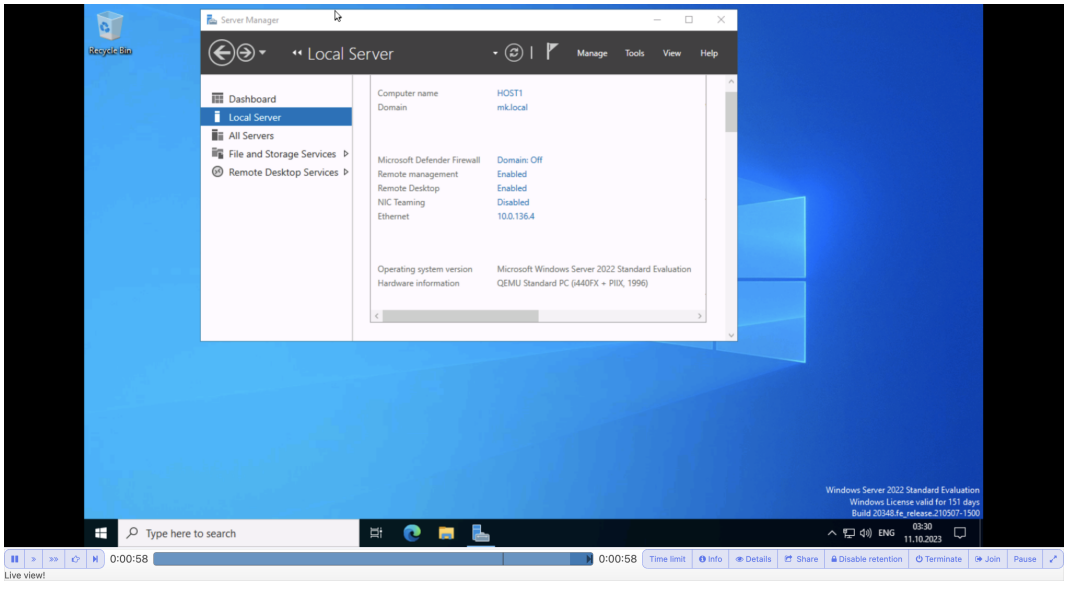


6. Remote Desktop client will establish connection with one of the servers from the RDS collection.

View the established session in the Fudo Enterprise Admin Panel:

1. Login into your Fudo Enterprise Admin Panel.
2. Select *Management* > *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*

30.3.3 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 *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.

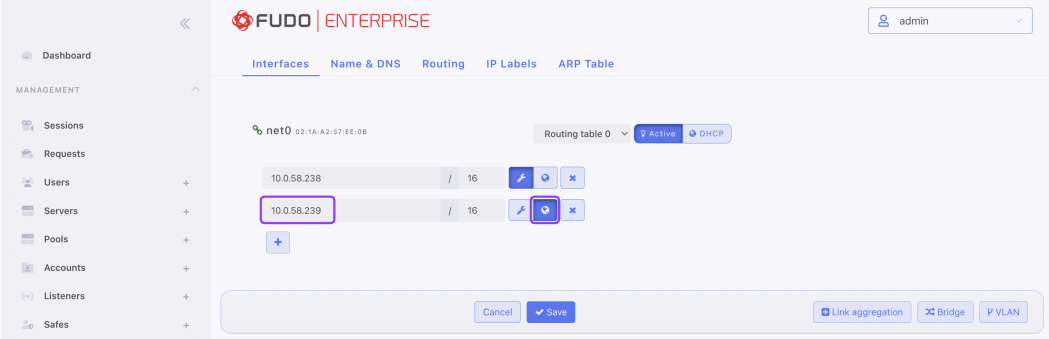
6. Click *Save and close* to save the safe configuration.

Establish a connection through the 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 Access Gateway address in the *Settings* > *Network configuration* menu tab.

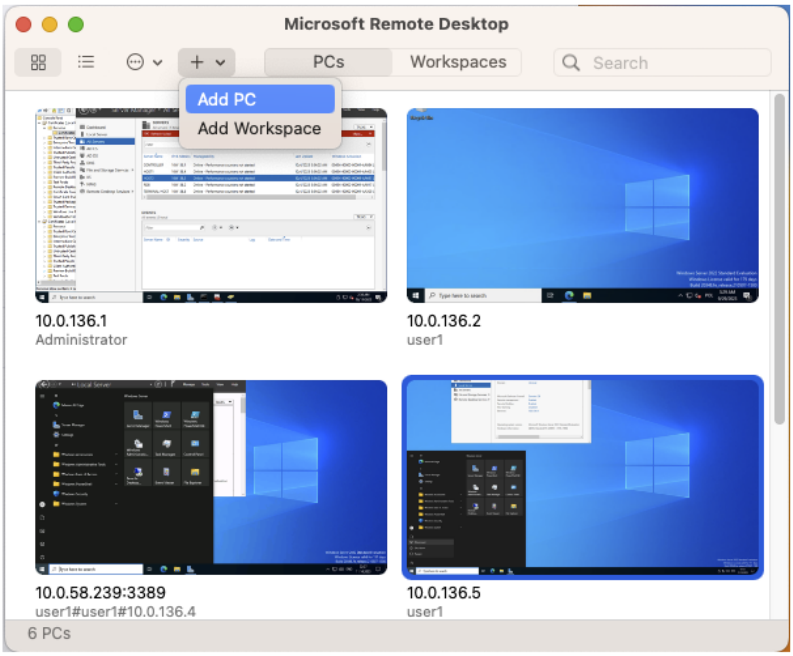


---

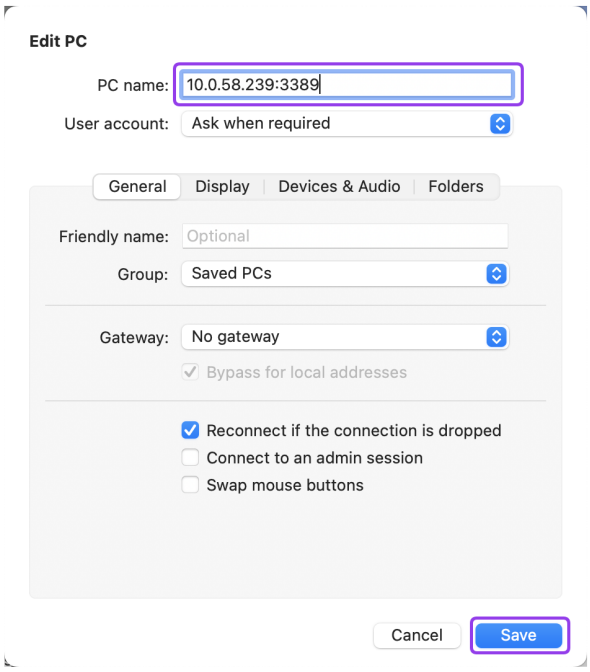
2. Hover the cursor over the `user1` account name, select *Native client* and click the *Connect* button to download the `.rdp` configuration file.
3. Open the downloaded file to establish a connection.
4. Enter the password for the `user1` account to log in to the server.

Redirect the connection through Fudo using RDP native client:

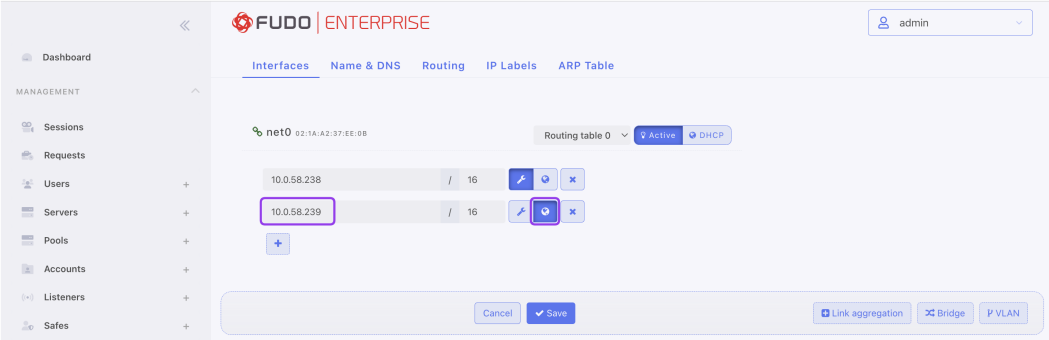
1. In order to redirect the connection through Fudo Enterprise, we need to use the Fudo Access Gateway address in the RDP client configuration.
2. Choose your favorite remote desktop client, such as Microsoft Remote Desktop, and follow its workflow to add a new PC for connection.
3. Following the example 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*.



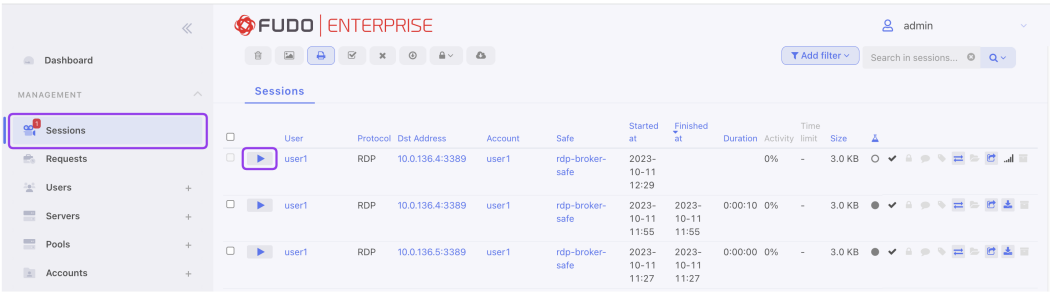
Note: You can find the Access Gateway address in the *Settings* > *Network configuration* menu tab.

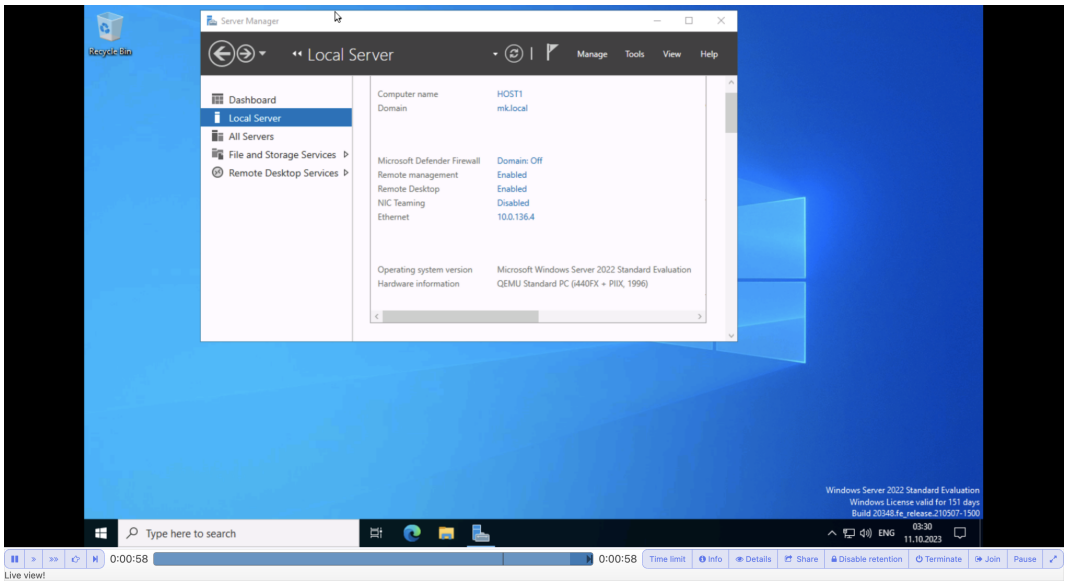


5. Connect to the added PC by providing the login and password of the `user1` set in the Active Directory environment (according to method selected while creating user in Fudo Enterprise).
6. Remote Desktop client will establish connection with one of the servers from the RDS collection.

View the established session in the Fudo Enterprise Admin Panel:

1. Login into your Fudo Enterprise Admin Panel.
2. Select *Management* > *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*

30.4 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.

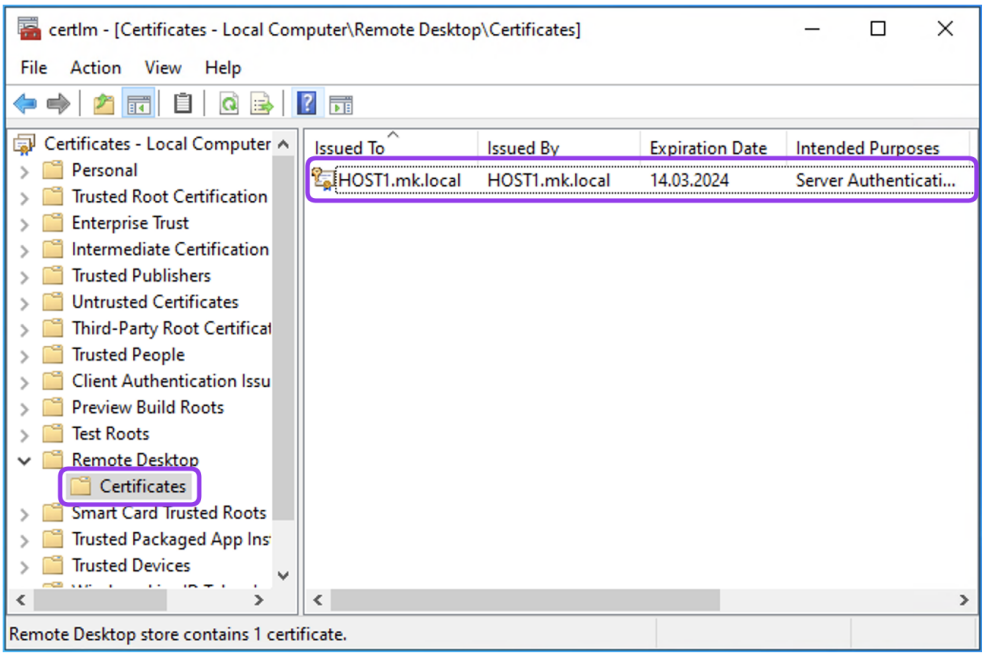
30.4.1 Locating the Server Certificate in Windows Server

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/
   ↪70WFeh+xjANBgkqhkiG9w0BAQsFADAZ
   MRcwFQYDVQQDEw5IT1NUMS5tay5sb2NhbDAeFw0yMzA5MTMxNzA2NTRaFw0yNDAz
   MTQxNzA2NTRaMBkxFzAVcas7c6c6sh83uydtLm1rLmxvY2FsMIIBIjANBgkqhkiG
   9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2ngYkoMa4dgLgGl1+G+m2UEAIH/
   ↪6ttyQep5u
   tUYkxKeuqpn9AWnYP8To1fornJN387ddhcy76d7jchc8Q093RWVb2cMKKjgOAW9w
   qLFW+WrLEUPY8hYvsCFYgFH3HOHhKLEoWBN5qHH7vjIiW3RbOY7xeGb9x0FWItQX
   mbF6sucGdlH+OsjepxMLPVh3Qpb2WQ18kSQGyS1ocbJxOWST9sH4MQkRVFL3rkxN
   f7/
   ↪qdJcdM6sFxEJTdp30CITRfbORXacl84bStjW2MJzvJRqr94xDHonRdIM9tUka
   O6LVJQY6qiEpMVE8MpSDAfoZ+HeyVWt+2EfXlfWE4hiMJP1DoQIDAQABoyQwIjAT
   BgNVHSUEDDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQAD
   ggEBAGNXzwNC4DhOxyaVhVTPePsa97aeWJtpl64cE4/ZdAfGBEIfHlBEh/
   ↪Tnrrn2
   7pr0jLnCjUq9rxHC6jfMR0U2PT4qrMHvGD1nUwZdHuZPavPLFHh/
   ↪rYHZpizoS+9W
   ggEBAGNXzwNC4DhOxyaVhVTPePsa97aeWJtpl64cE4/ZdAfGBEIfHlBEh/
   ↪Tnrrn2
   xyXjeYdX8/U9EdgrXOLGX9U74rfGQTrQxZyjuYlGxxqop/
   ↪y2V3n+3NnNzY+ehW1G
   ggEBAGNXzwNC4DhOxyaVhVTPePsa97aeWJtpl64cE4/ZdAfGBEIfHlBEh/
   ↪Tnrrn2
   ZUvdUnqtdH+0DdAWBo4P1dv0nL8=
   -----END CERTIFICATE-----
   ```

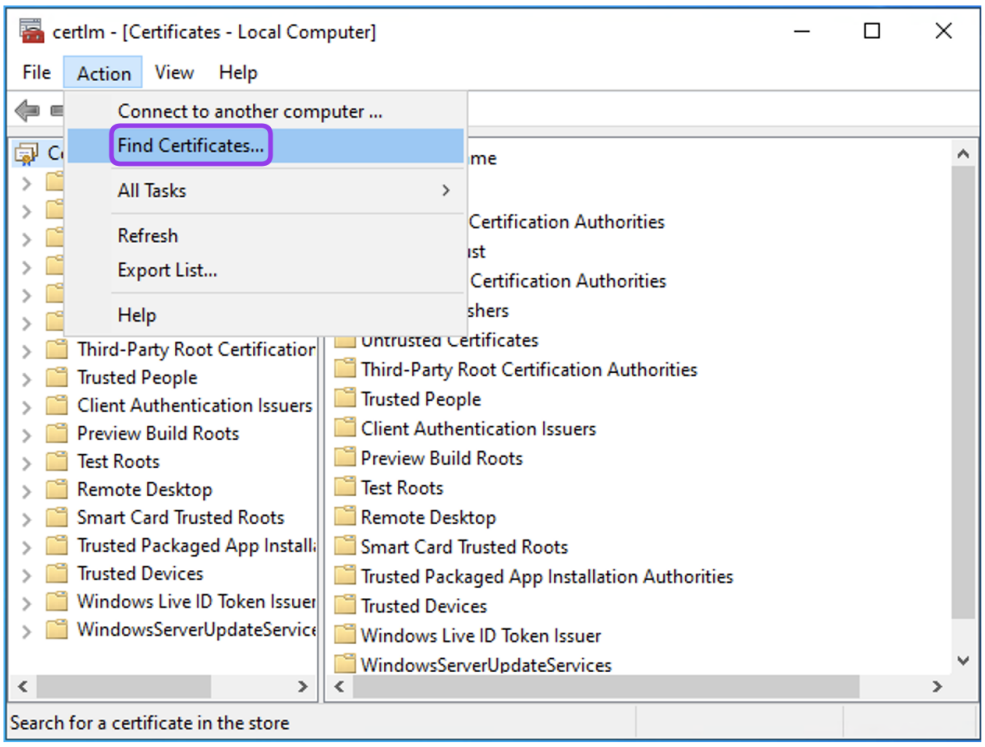
3. This will result in extracting the certificate's serial number that you can use to search the exact certificate in the Certificate Manager tool.

   ```
   serial=41EB33A67D4F9A884AFFBD1615E11EDD
   ```

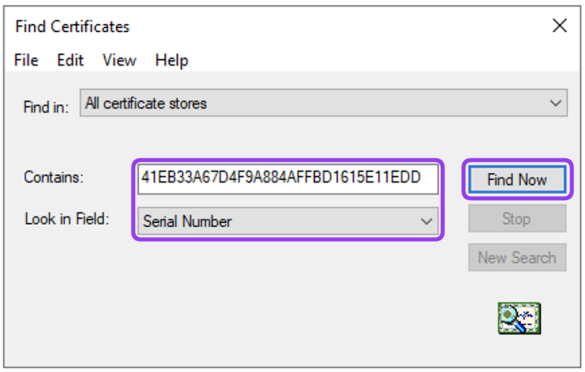
4. Copy extracted serial number and go to the Windows Server.

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*.

30.4.2 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.

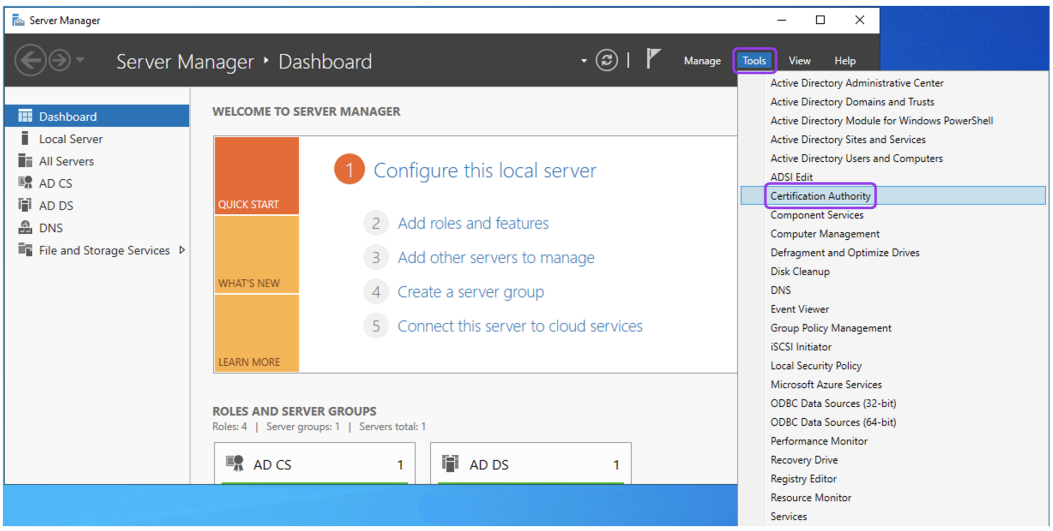
Install the Certificate Authority on Windows Server:

To install the Certificate Authority on Windows Server, follow the default configuration as specified in the manufacturer's manual.

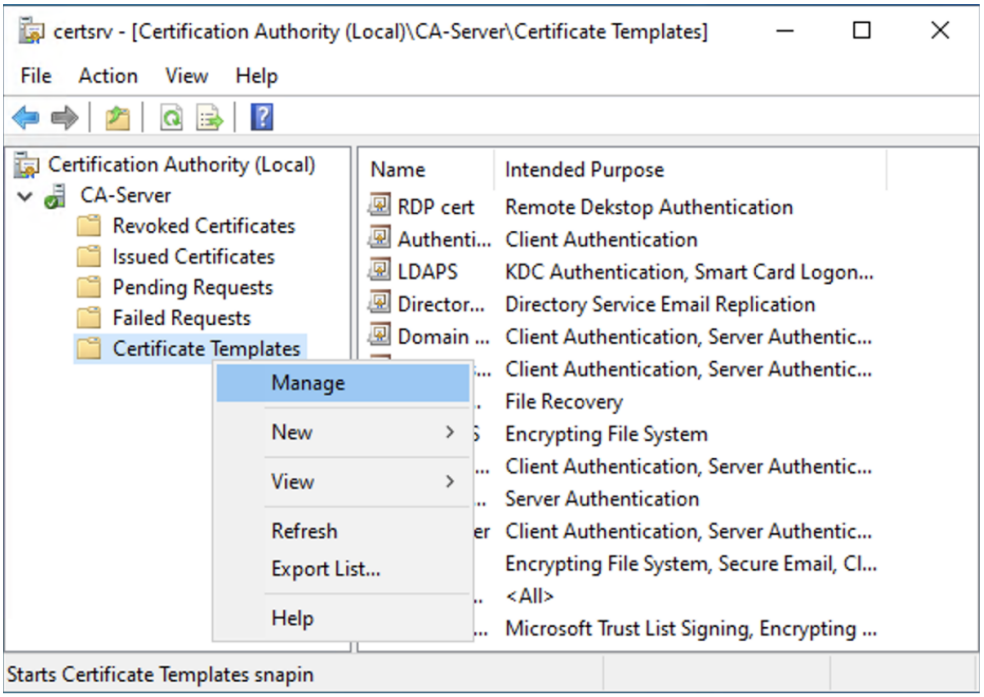
Note: For the procedure outlined in the manual below, the *Enterprise CA* option was selected.

Create a Template for RDP Certificate:

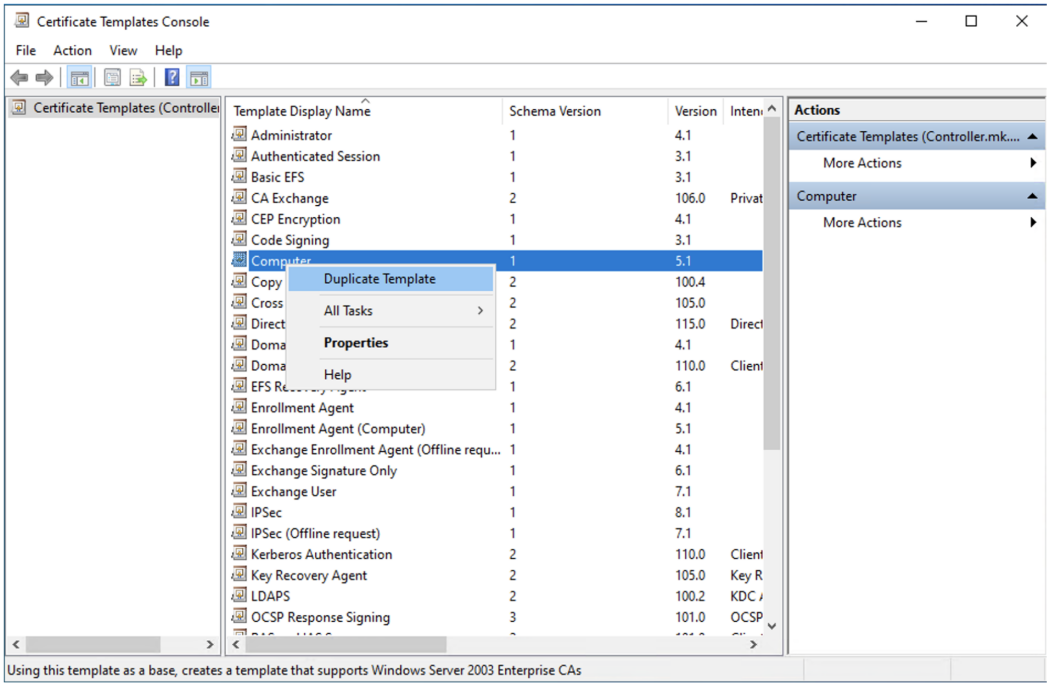
1. Open the Certificate Authority from the *Server Manager* by clicking *Tools* > *Certification Authority* in the upper right corner of the window.



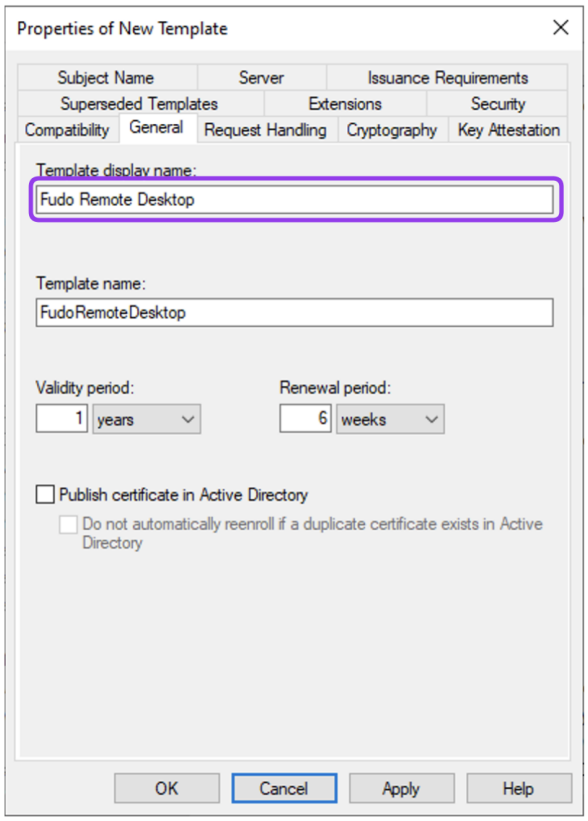
2. Right click on the *Certificate Template* and choose *Manage*.



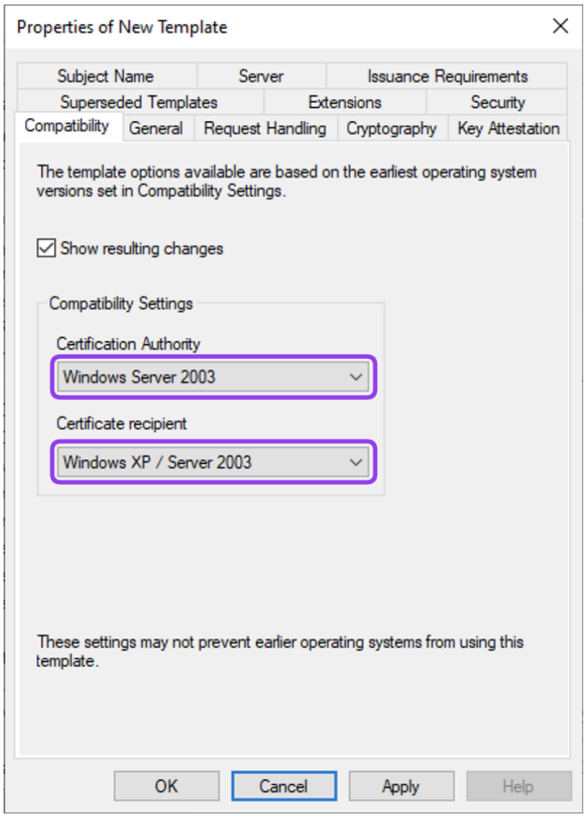
3. Find the *Computer* template, right click on it and choose *Duplicate Template*.



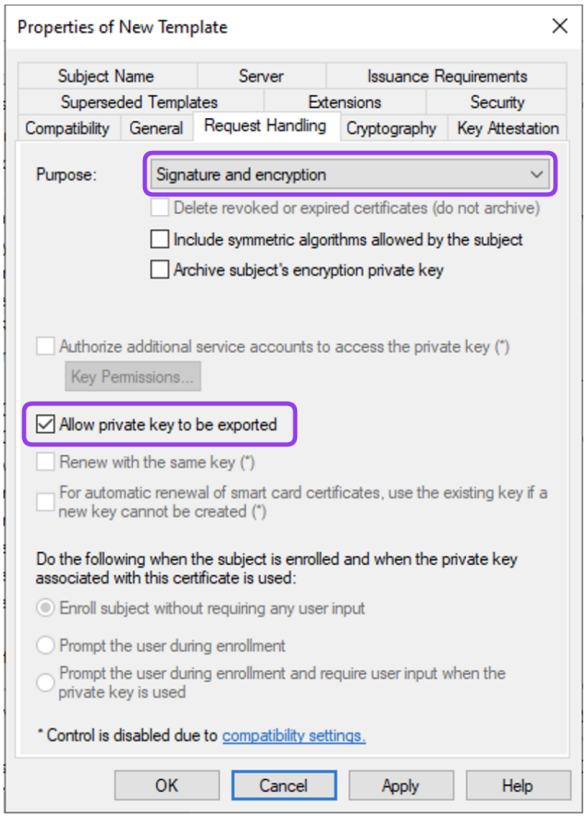
4. In the *General* tab, enter the name for new template and specify the validity and renewal period according to your needs.



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.

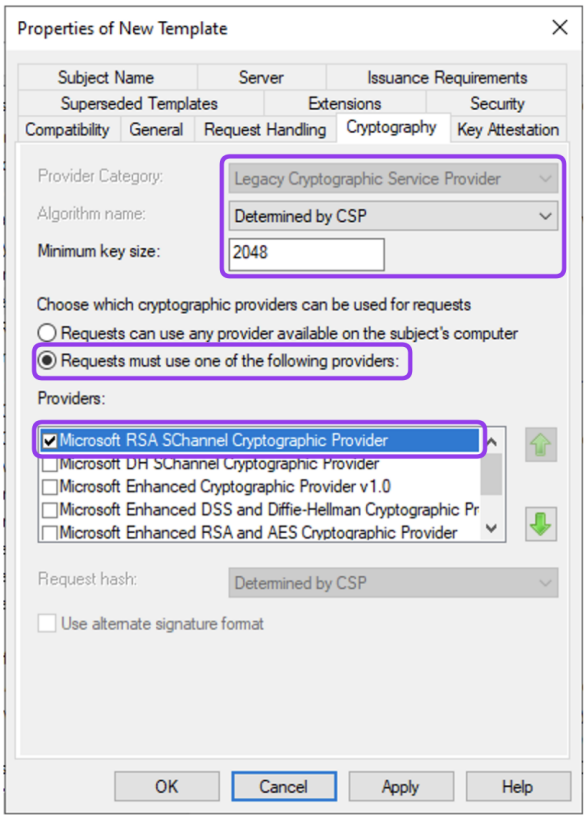


6. In the *Request Handling* tab, set the *Purpose* to the *Signature and encryption* and check the *Allow private key to be exported*.

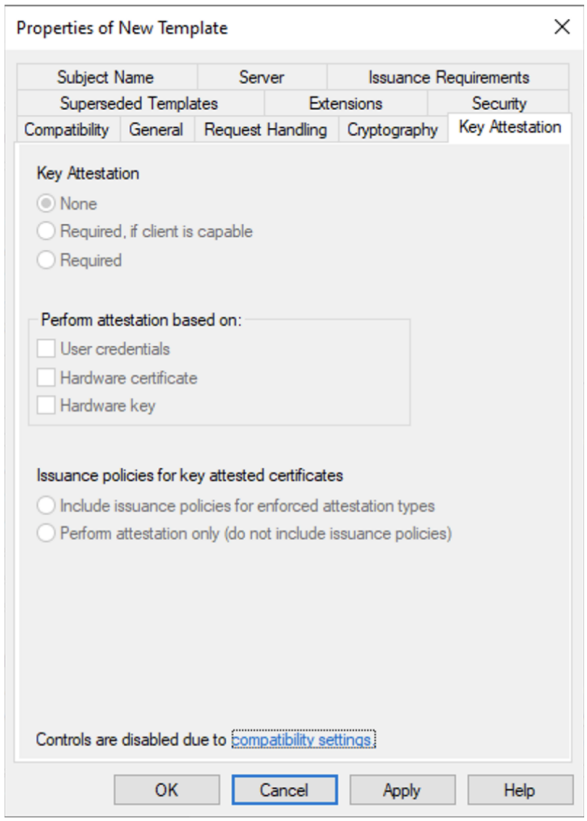


7. In the *Cryptography* tab, choose:

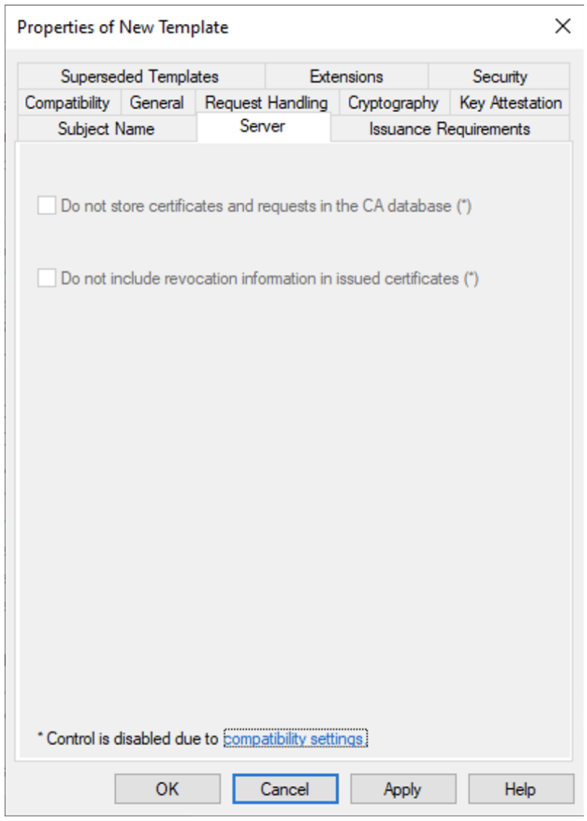
- set the *Provider Category* to *Legacy Cryptography Service Provider*,
- set the *Algorithm name* to *Determined by CSP*,
- set the *Minimum Key Size* according to organisation security requirement (e.g., 1024).
- choose the *Request must use one of the following providers* option and select the *Microsoft RSA SChannel Cryptographic Provider*.



8. In the *Key Attestation* tab, leave default settings.



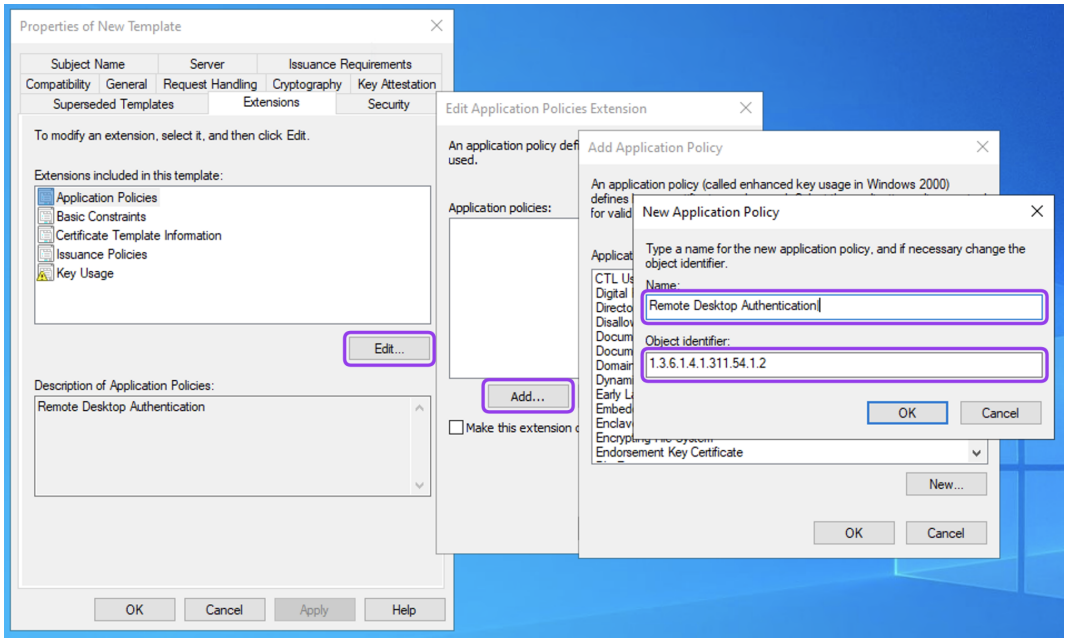
9. In the *Server* tab, leave default settings.



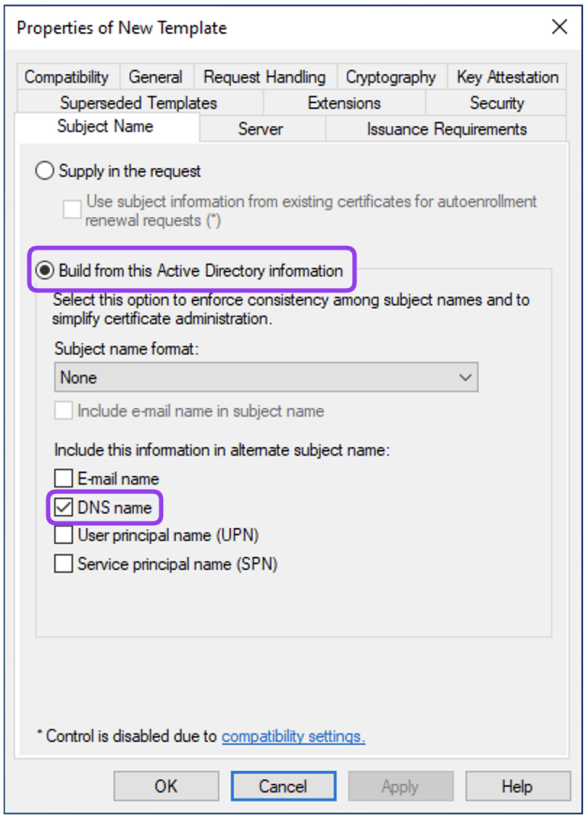
10. In the 'Security' tab, add the computers and groups you want to be able to enroll for this template. Check if group or user you are using has the *Read, Write,*

and *Enroll* permissions enabled. It is needed to request the certificate using this template in the next steps.

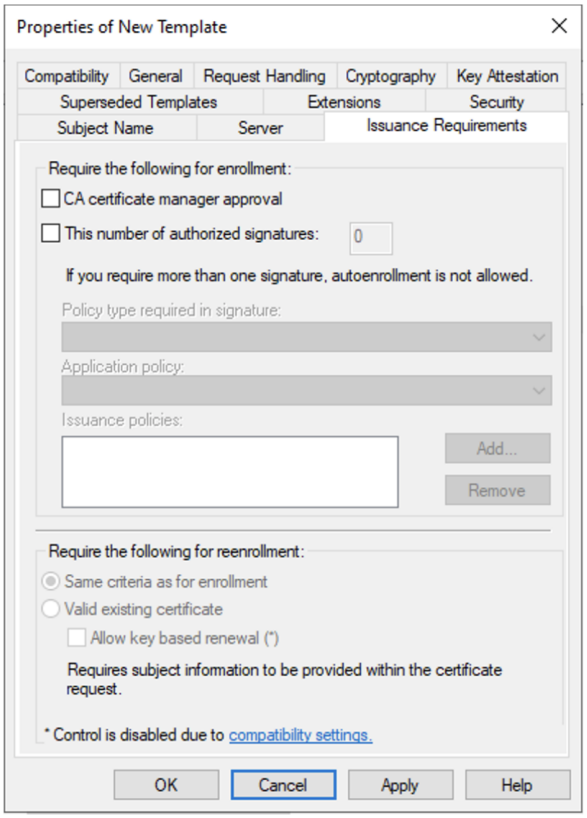
11. In the *Extensions* tab, edit the *Application Policies*.
12. Remove the *Server Authentication* and *Client Authentication* policies.
13. Add new policy by clicking *Add*, and *New* in the next window.
14. In the Name field enter `Remote Desktop Authentication` and in the *Object identifier* field 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*.

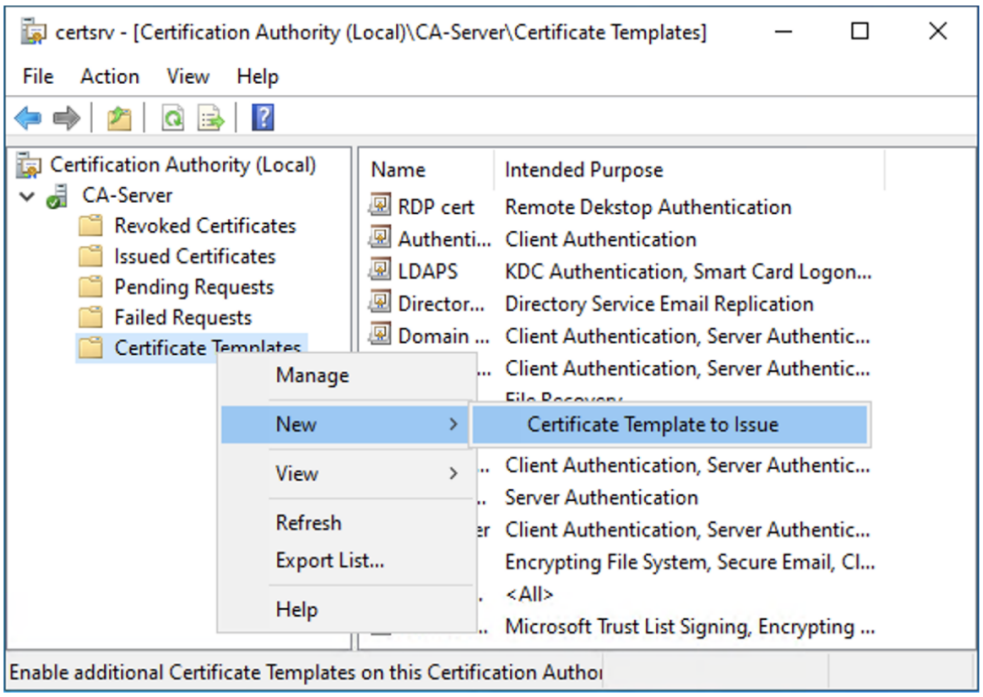


17. In the *Issuance Requirements* tab, leave default settings.

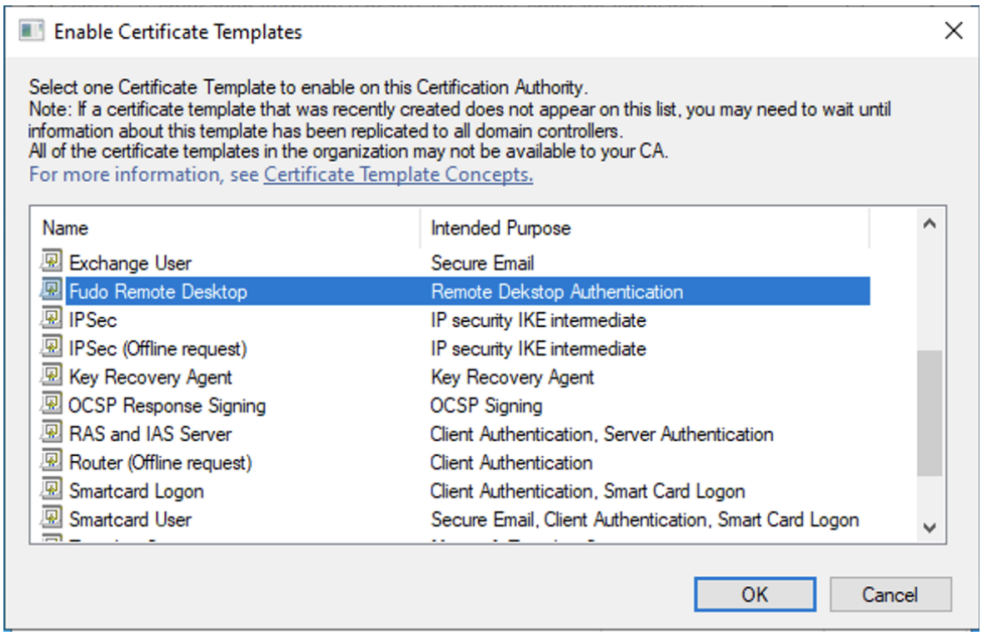


18. Click *OK* to save created template. Close the *Certificate Templates Console*.

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*.

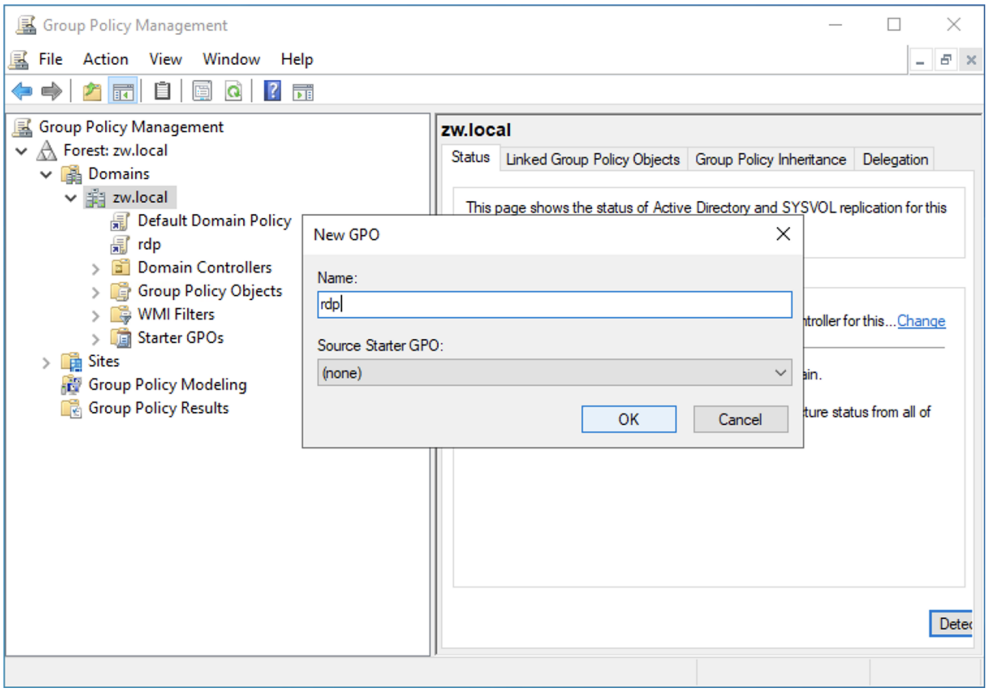


Configure a GPO to Deploy the Template

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...

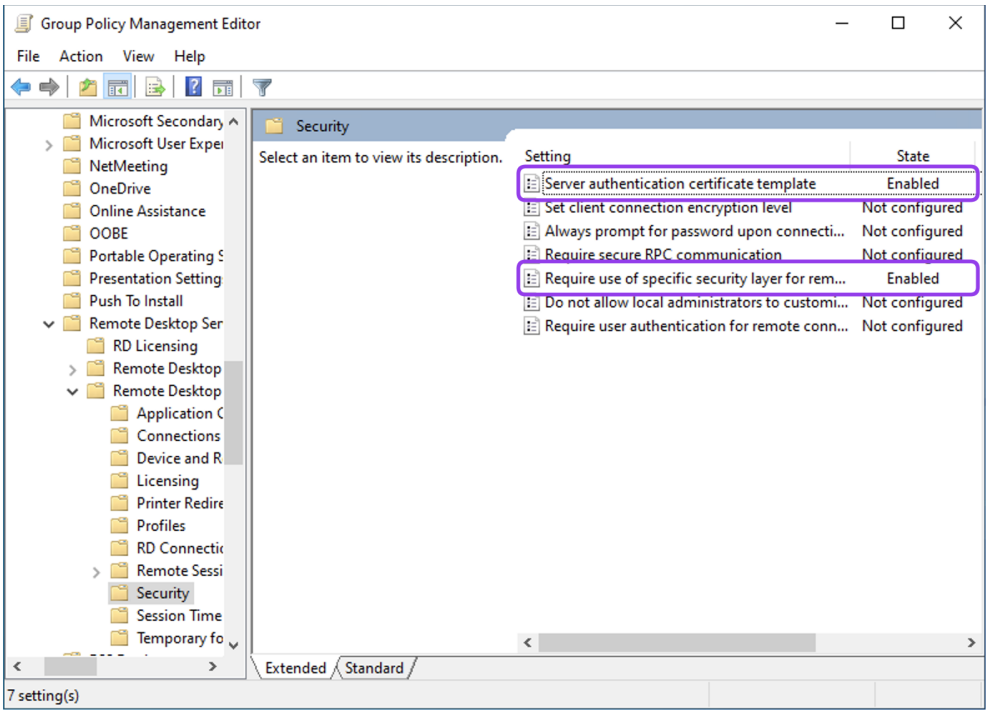
4. Provide a name for new GPO (e.g., *rdp*) and click *OK*.



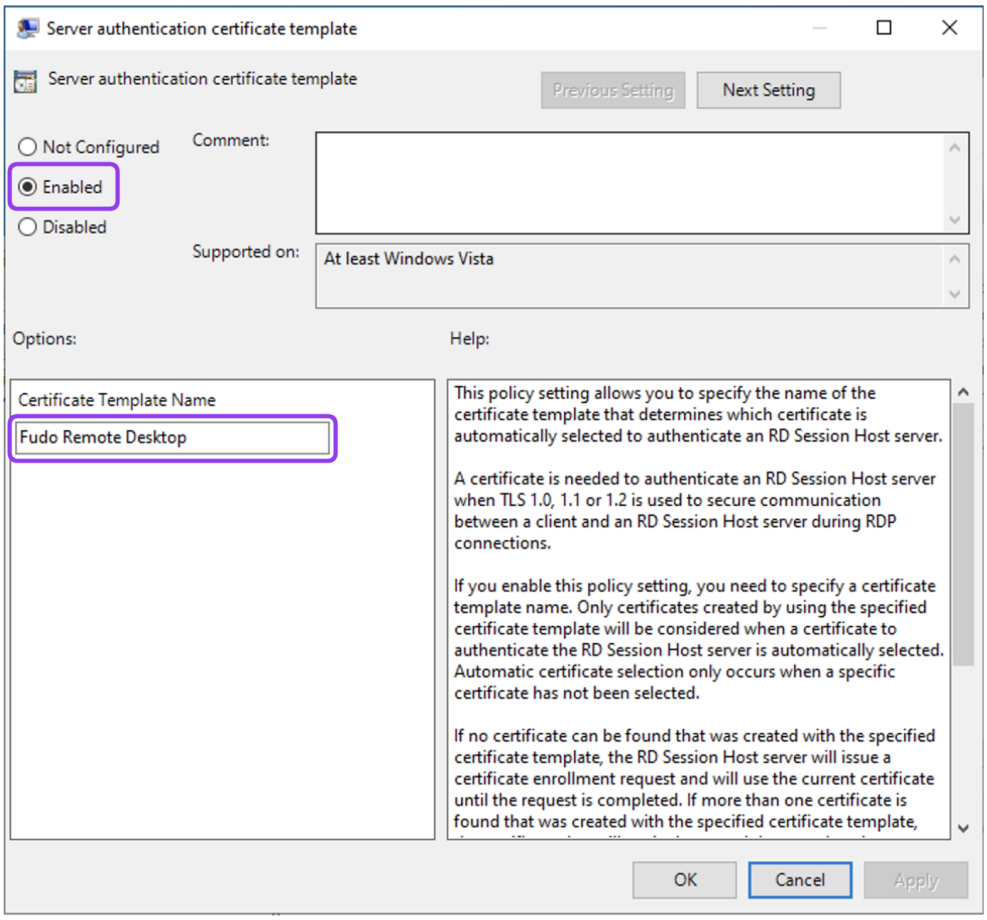
5. Right click on the name of created GPO and select *Edit...*.

6. In the *Group Policy Management Editor* navigate to *Computer Configuration* > *Policies* > *Administrative Templates* > *Windows Components* > *Remote Desktop Services* > *Remote Desktop Session Host* > *Security*.

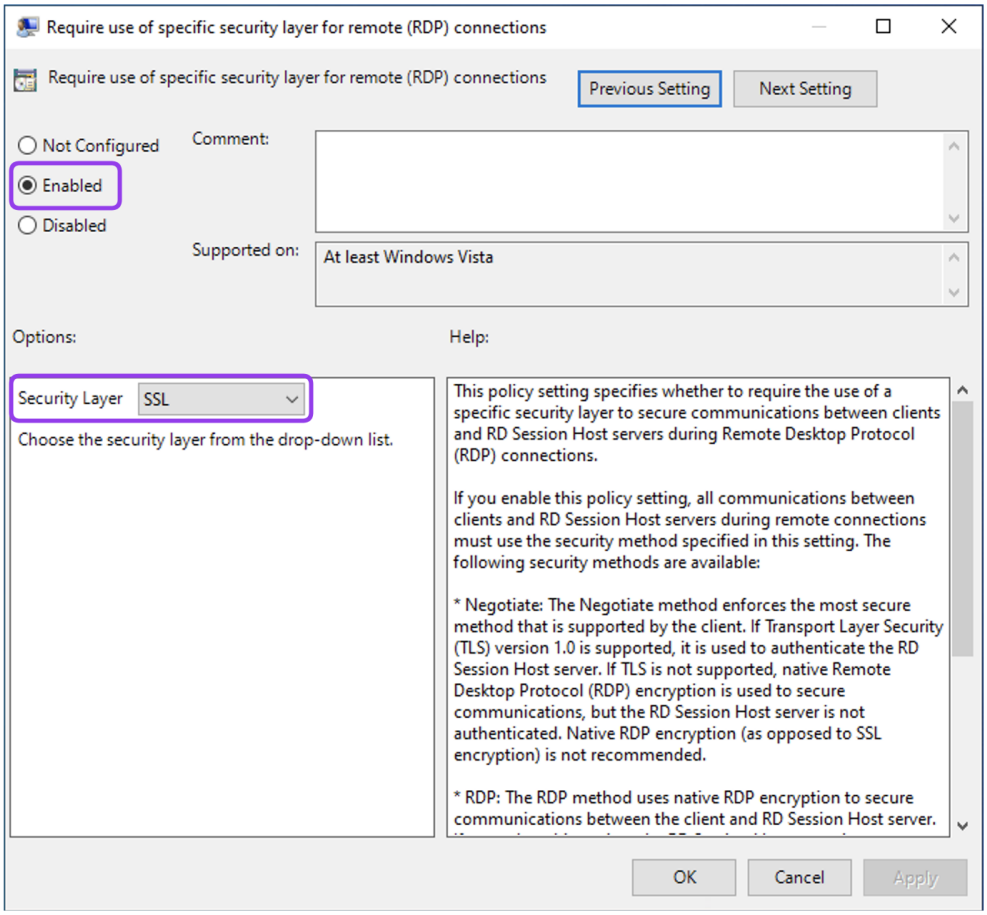
7. Double-click on the *Server authentication certificate template* to edit this setting.



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.

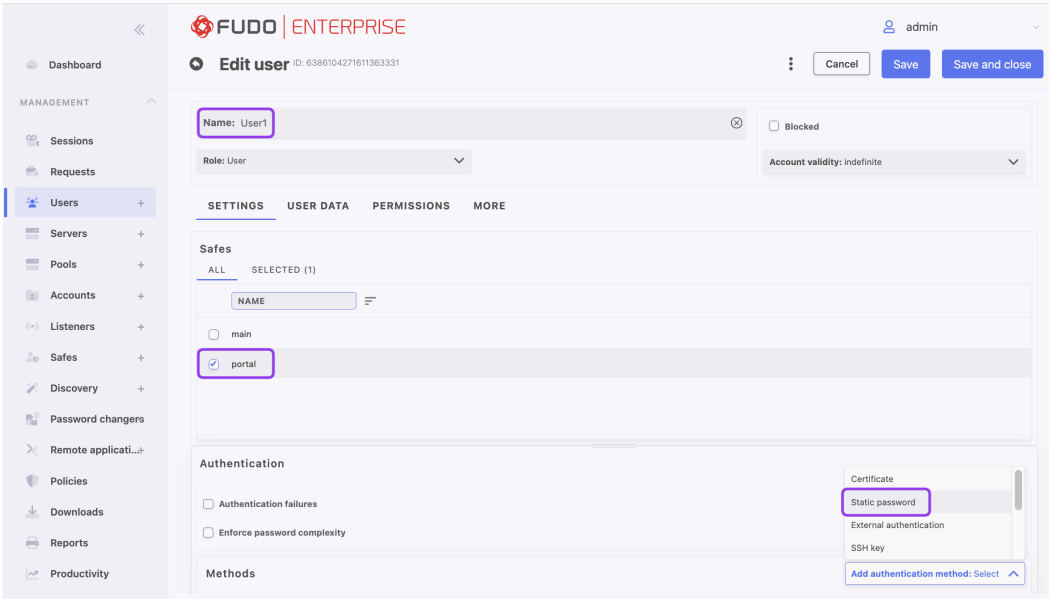
Export the CA Certificate

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 *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*.

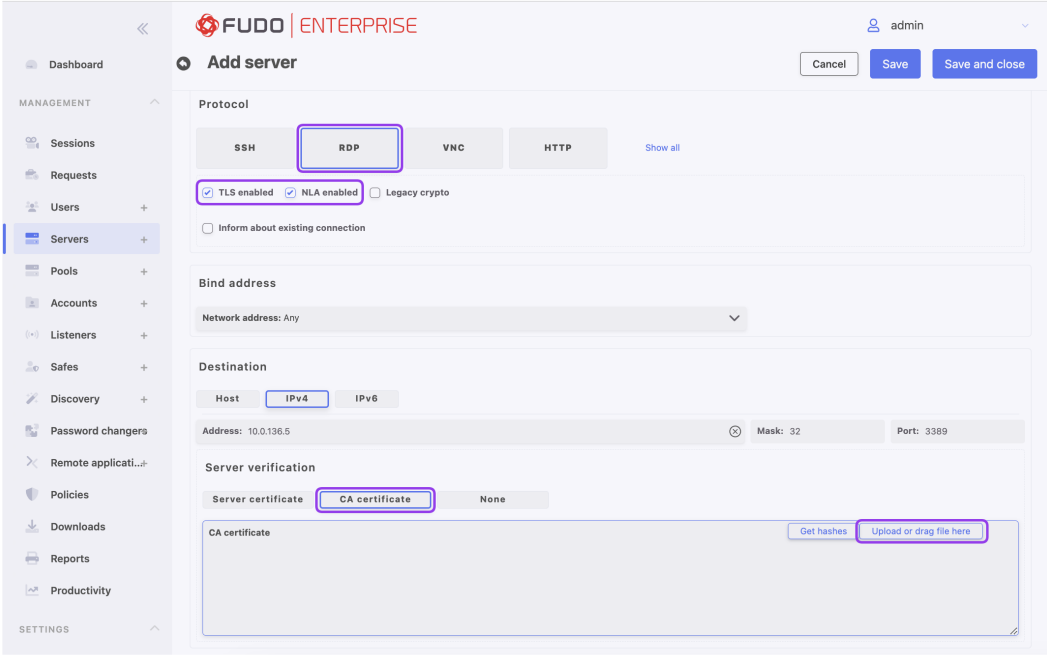


6. Provide password and click *Save*.
7. If necessary, please fill in the remaining parameters as needed for your specific configuration. For more details, please refer to the *Creating a user* section.
8. Click *Save and close*.

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*.

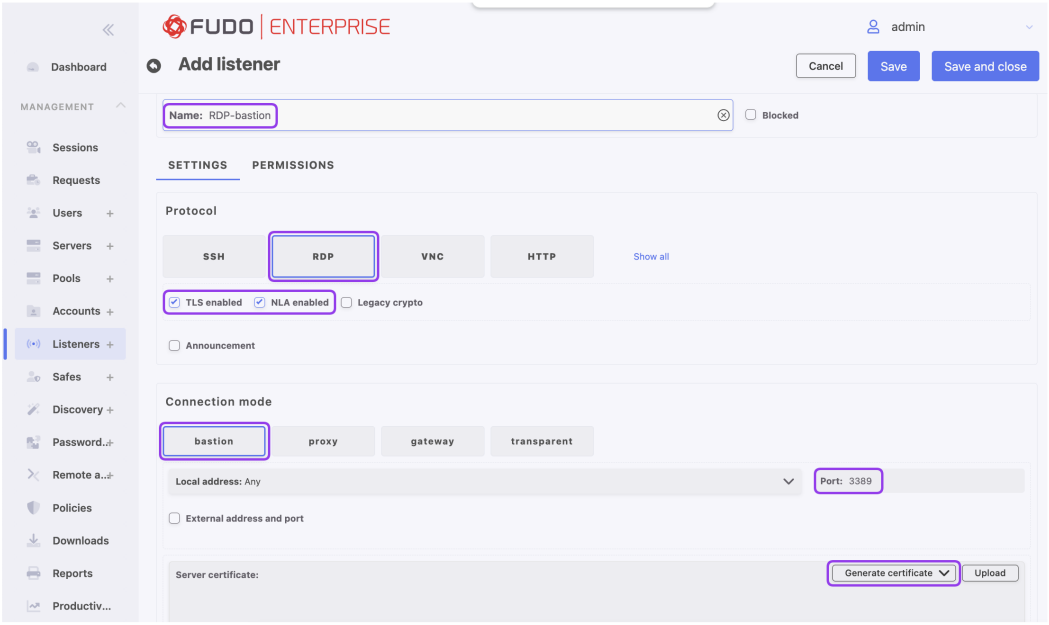
Configure Account:

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.

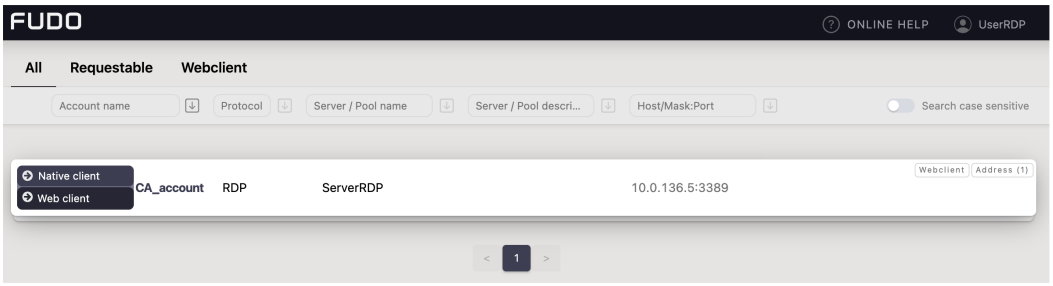
5. Select **Accounts** tab to add accounts accessible through this safe.

- 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*

30.5 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.

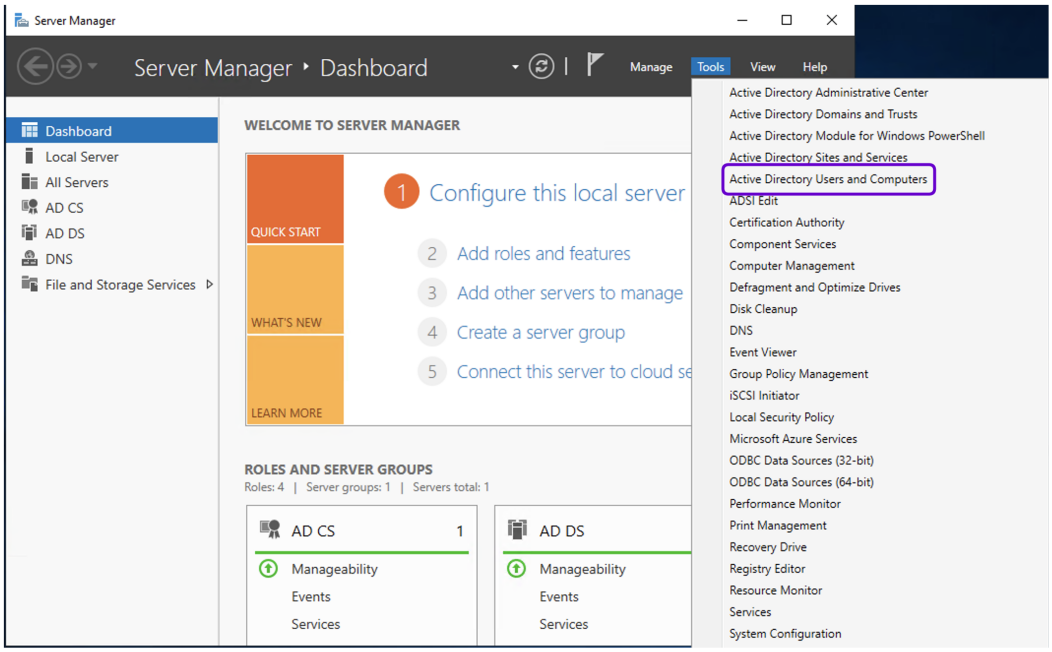
To configure and use the Single Sign On (SSO) with Fudo Enterprise, please follow below steps.

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.

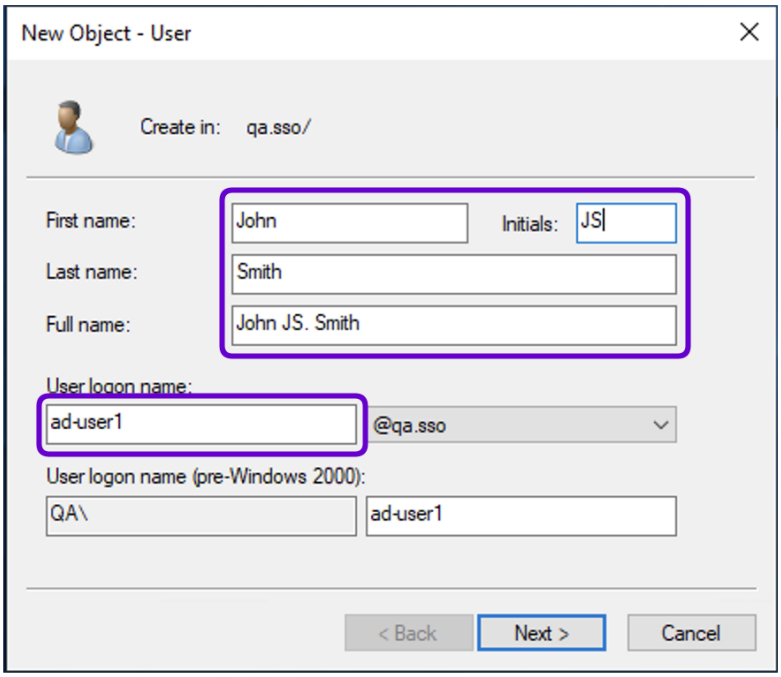
30.5.1 SSO configuration on Windows Server 2019

Add User:

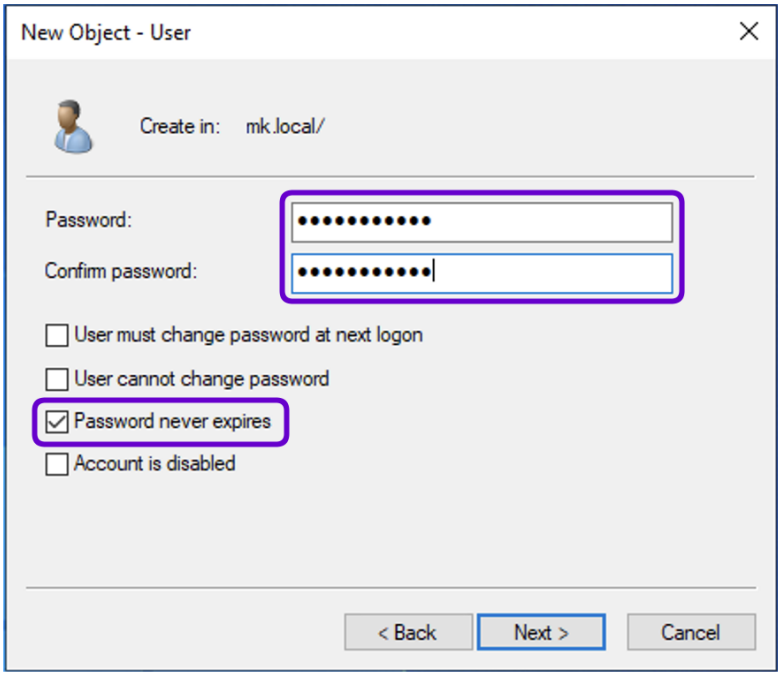
1. Log in to the server on which you want to setup the SSO using the administrator account.
2. Open the *Server Manager* application.
3. Click *Tools* button on the upper right corner of the window to expand the menu list and select *Active Directory Users and Computers*.



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`).

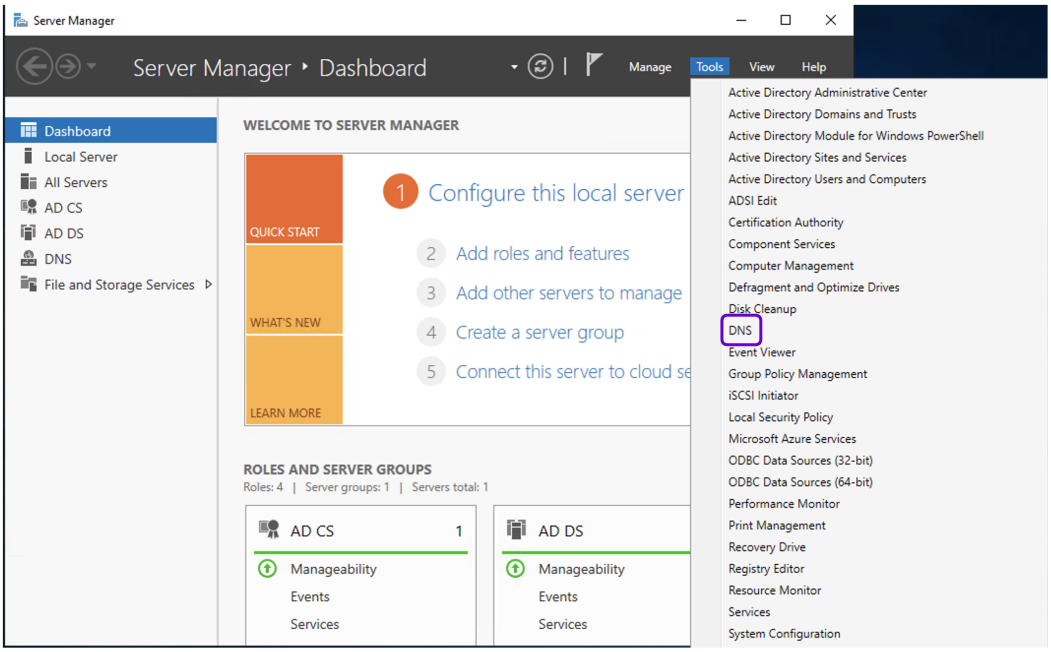


7. Click *Next*.
8. Provide the password for created user (e.g., `PaSSwOrD`) and select *Password never expires* option.
9. Click *Next* and *Finish*.

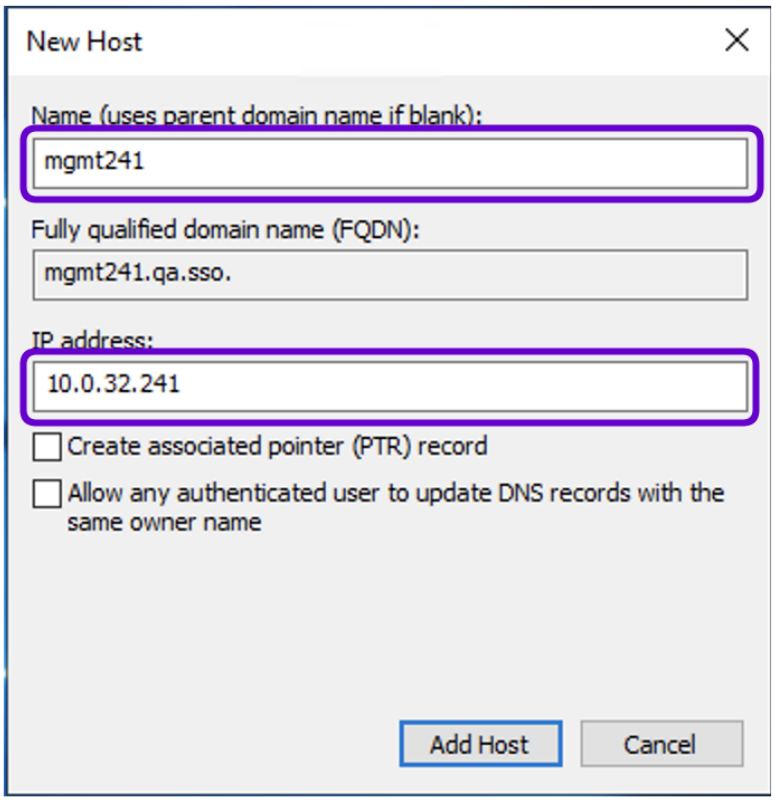


Configure DNS entries:

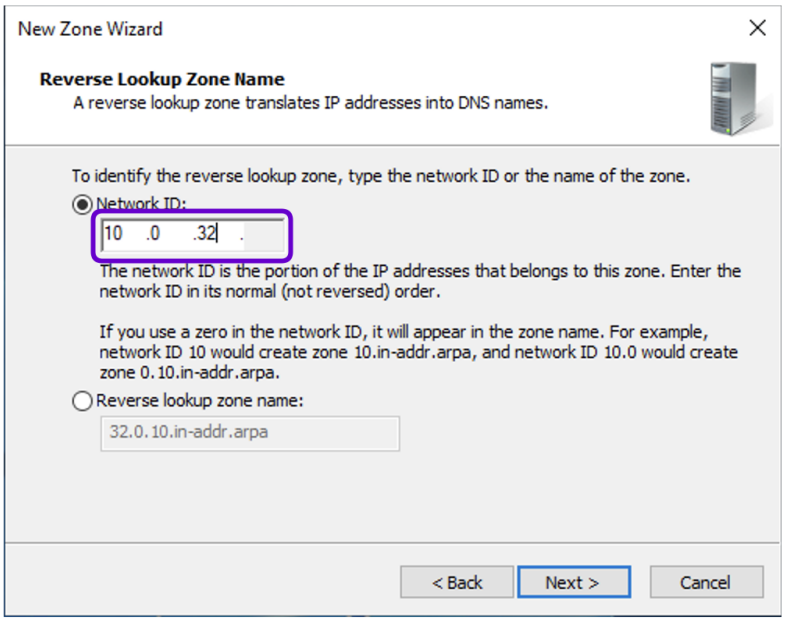
1. Open the *Server Manager* application.
2. Click *Tools* button on the upper right corner of the window to expand the menu list and select *DNS*.



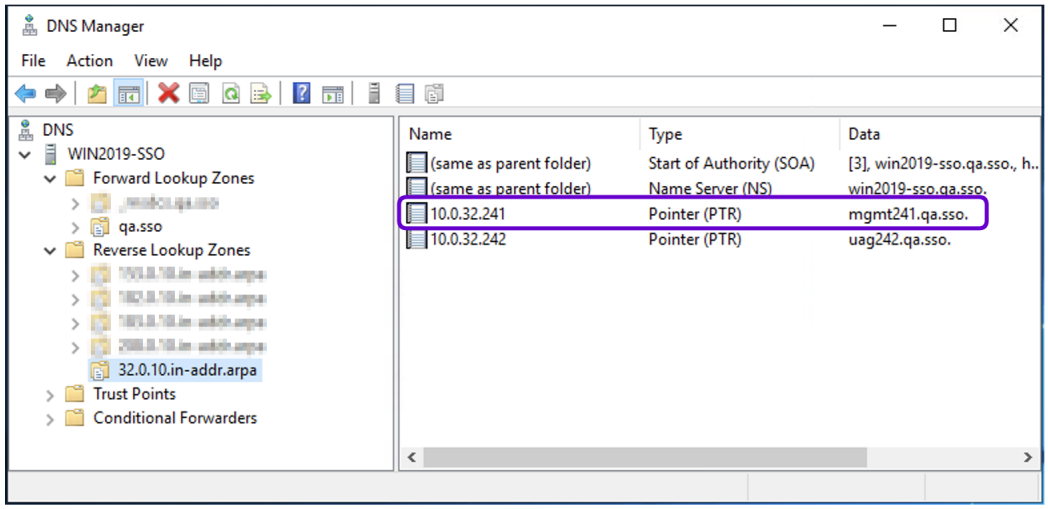
3. Go to *Forward Lookup Zones*, right click on the domain name and select *New Host*.
4. Provide the *Name* and *IP address* of the Fudo Enterprise Admin Panel (e.g., `mgmt241.qa.sso, 10.0.32.241`).
5. Click *Add Host*.



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.

30.5.2 Setup Fudo Enterprise

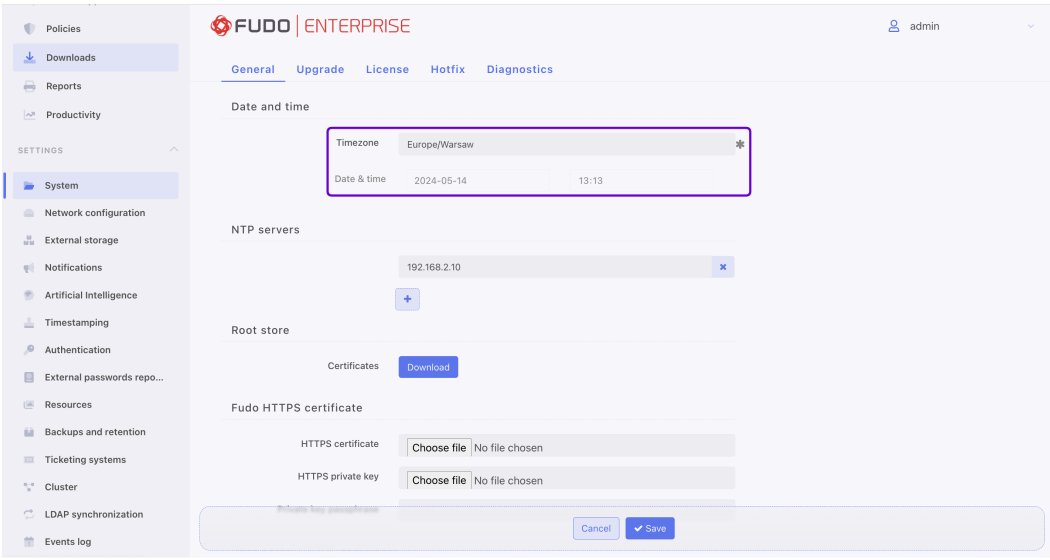
Note: This use case describes how to configure Fudo Enterprise using the Active Directory external authentication method. Please keep in mind that you can customize user authentication using other method supported by Fudo Enterprise to align with your specific requirements, the methods typically used in your environment, and your work scenarios.

Configure SSO:

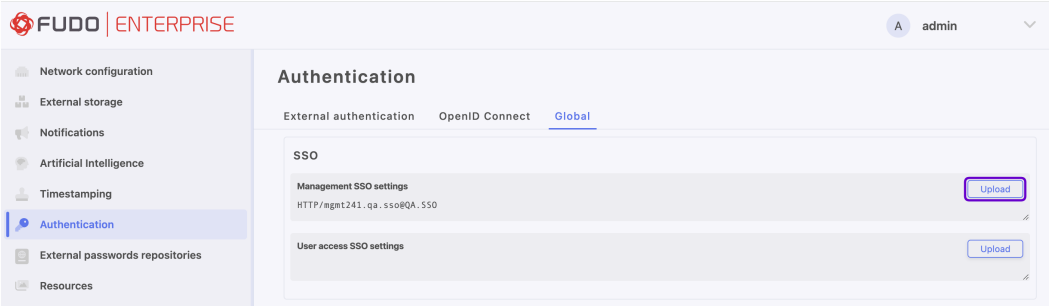
In order to define SSO service parameters in Fudo Enterprise, follow the steps:

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.

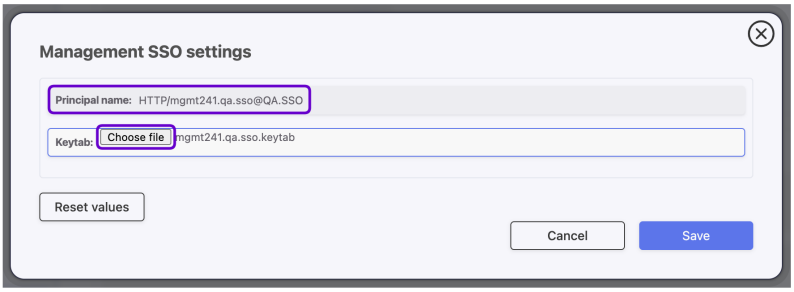
Warning: Fudo Enterprise Timezone must match the Windows client timezone configuration.



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 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 *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.

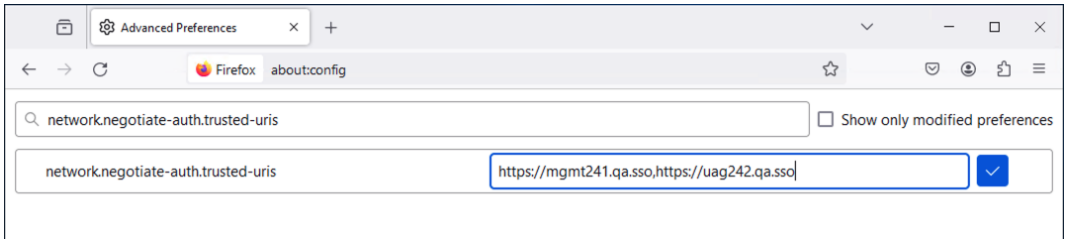
---

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*.

30.5.3 Setup and check user workstation - Windows2010 Client

Firefox browser configuration:

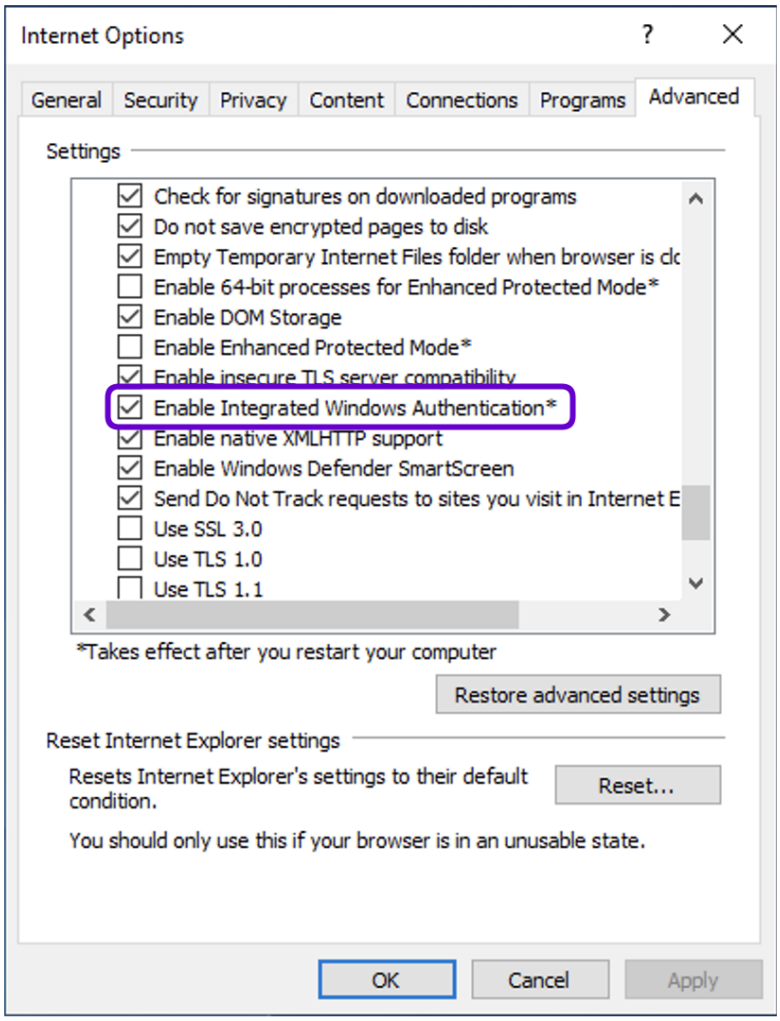
1. Log in to Windows Client using the `ad-user1` account.
2. Open *Firefox,* type `about:config` in the address bar, and press *Enter.*
3. A warning message will appear. Click on *Accept the Risk and Continue* option to proceed.
4. In the search bar at the top, type `network.negotiate-auth.trusted-uris.`
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.



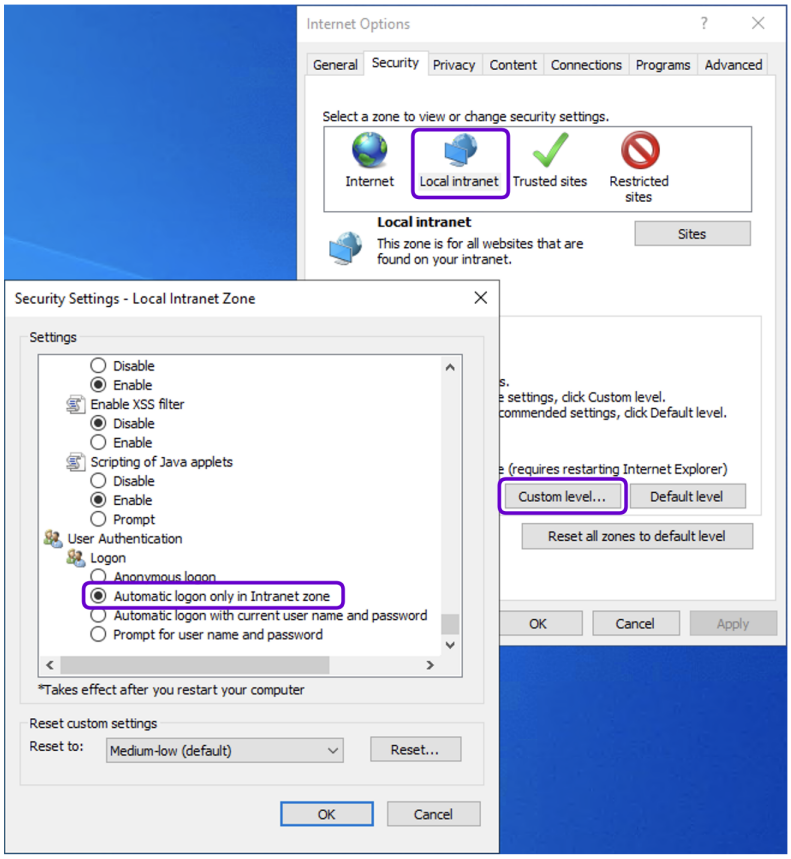
7. Next, type in `network.automatic-ntlm-auth.trusted-uris` in the search bar.
8. Double-click on the `network.automatic-ntlm-auth.trusted-uris` and enter the desired FQDN (Fully Qualified Domain Name) with a protocol, separating entries with a comma (e.g., `https://mgmt241.qa.sso,https://uag242.qa.sso).`
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.*



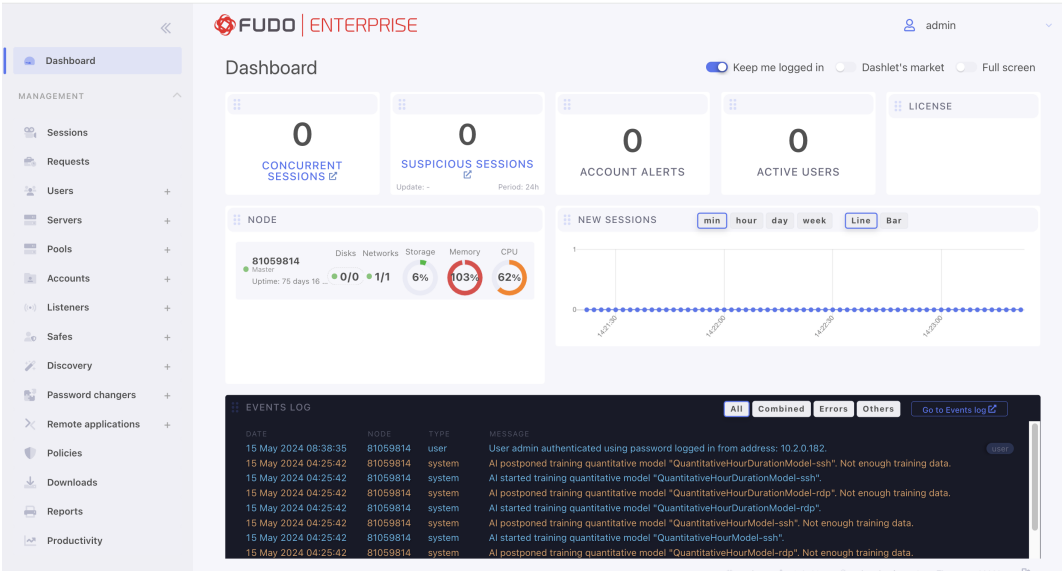
6. Click *OK*.
7. Click *Sites* and select all check boxes.
8. Click *Advanced* and add Remedy SSO service website to the local zone (in our example, it's `https://mgmt241.qa.sso`).
9. Click *Add*.
10. Click *OK* for all pop-ups.
11. Uruchom ponownie przeglądarkę.

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*

30.6 Handling Local Account Password Changes Using a Domain Account with WinRM Password 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 password changer in Fudo Enterprise, the following configura

- 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.

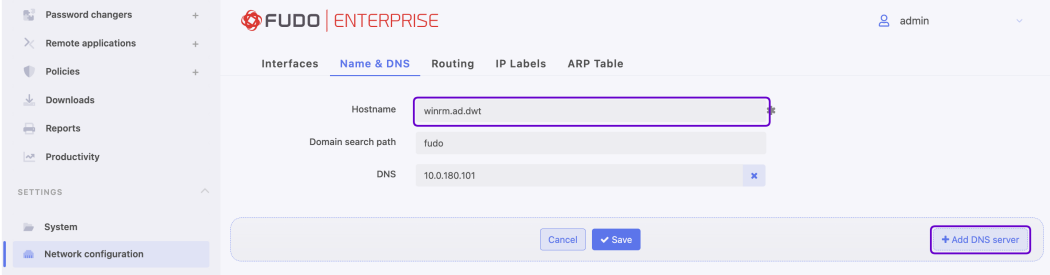
Note:

- 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.

30.6.1 Hostname and DNS Server Configuration

Set the hostname by following these steps:

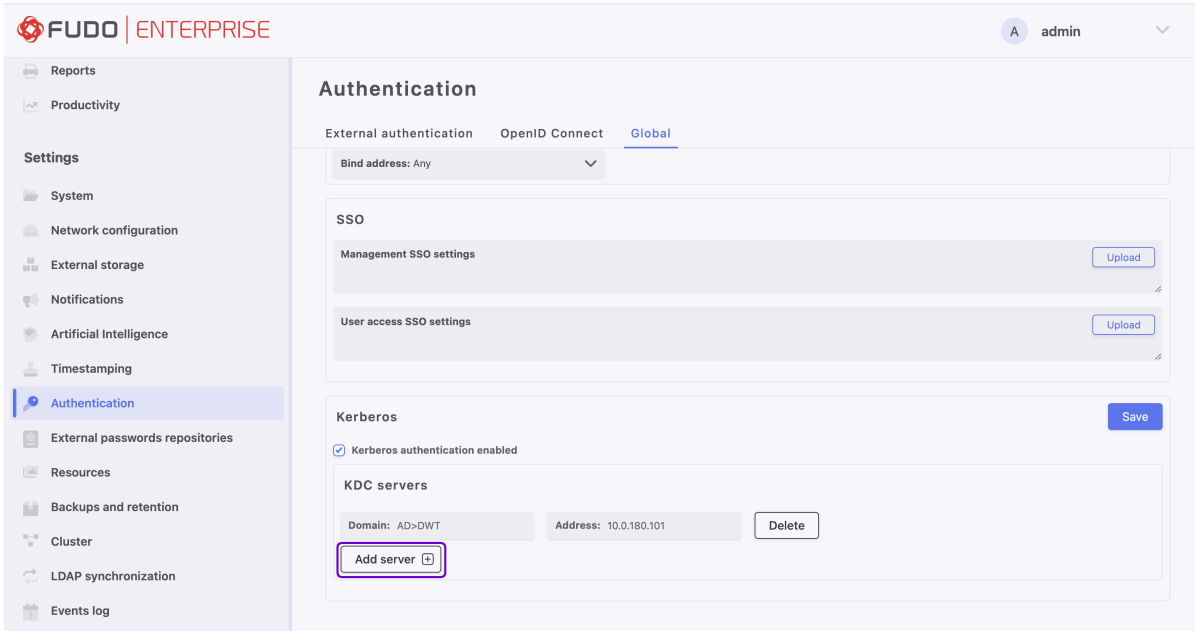
1. Go to *Settings* > *Network Configuration*.
2. Navigate to the *Name and DNS* tab.
1. In the *Hostname* field, enter the hostname along with the domain in the following format: `hostname.yourdomain.local` (e.g., `winrm.ad.dwt`).
2. Configure the DNS server:
    - Click *Add Server* + to define a new DNS server.
    - Enter the IP address of the DNS server (e.g., `10.0.180.101`).
    - Click *Save*.



30.6.2 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`).

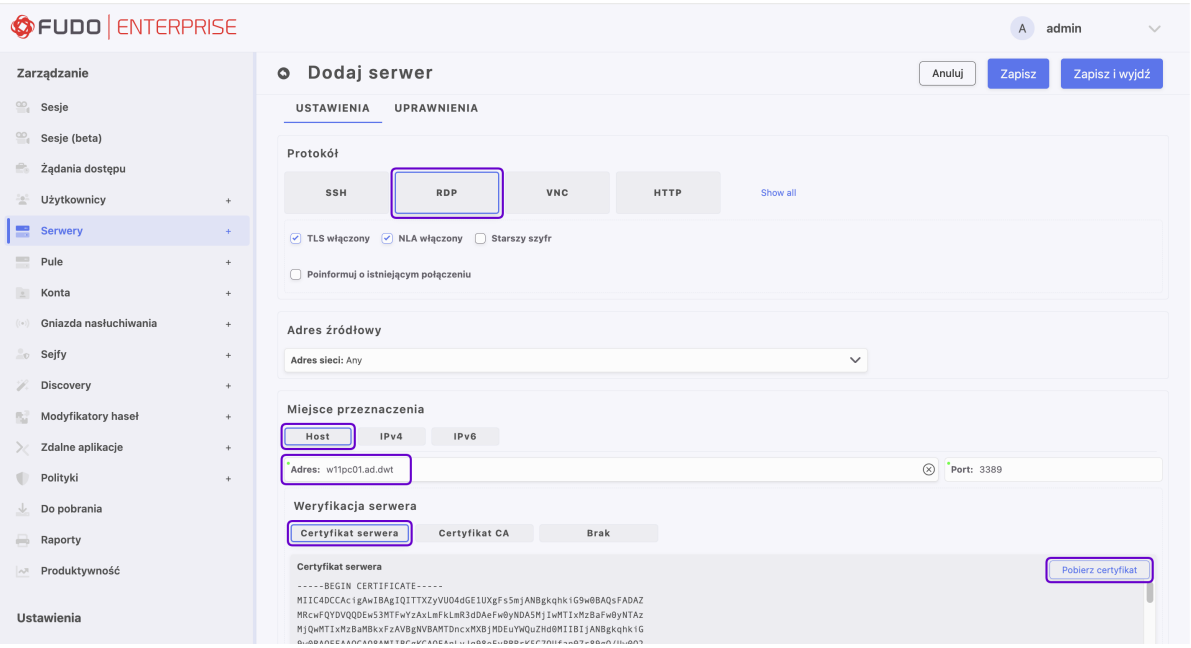
30.6.3 Server Configuration

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 password changer. Defining the server by IPv4/IPv6 address is not supported.

Related Topics:

- *Creating a regular account*
- *Authentication*

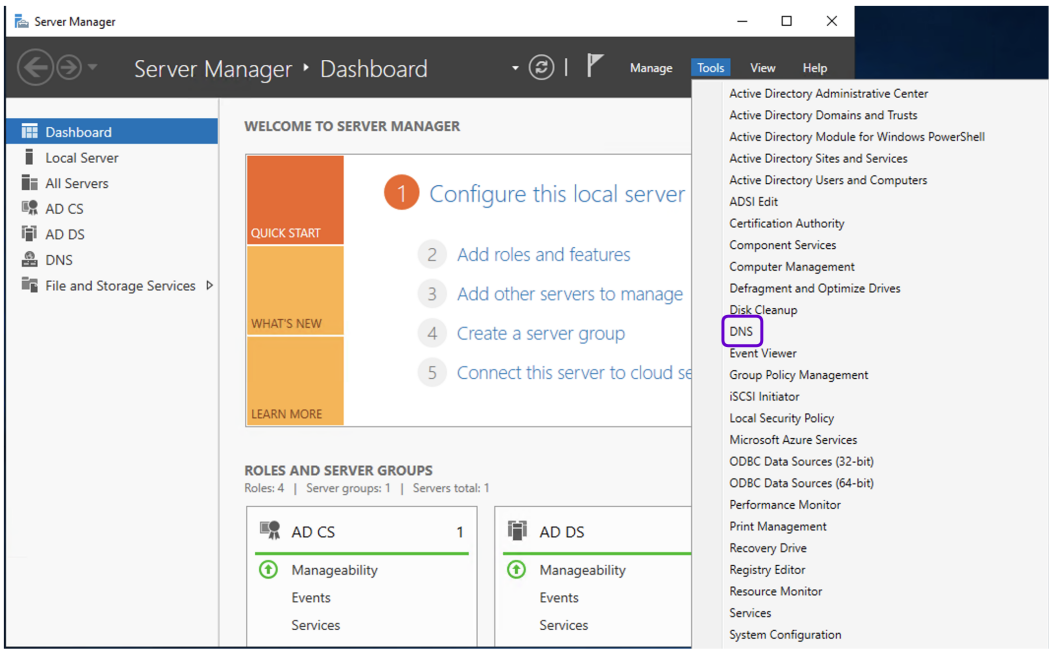
30.7 Configuring Kerberos Constrained Delegation for MSSQL(TDS) Server

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.

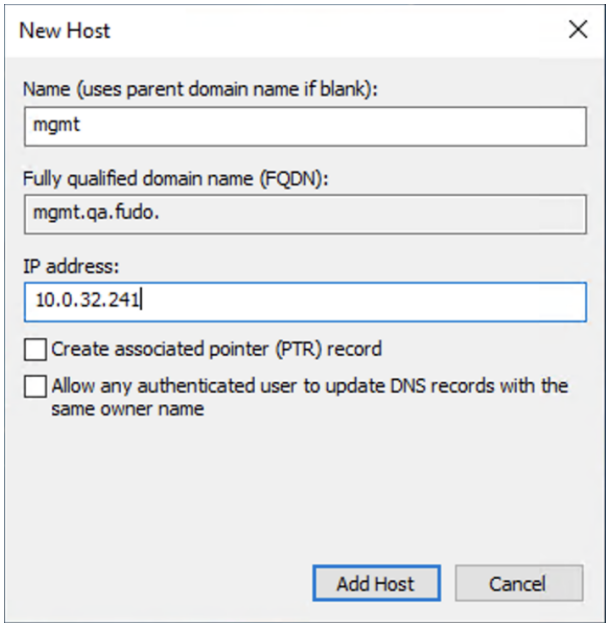
30.7.1 Kerberos Authentication Configuration on Windows Server

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*.



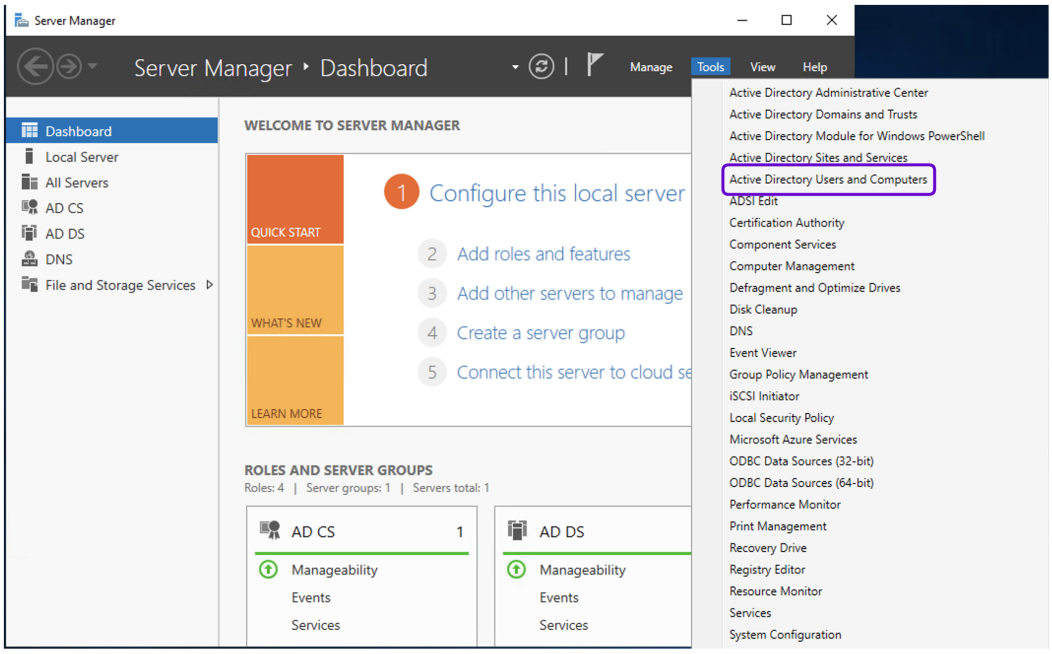
3. Go to *Forward Lookup Zones*.
4. Add an A record: right click on the selected domain name and click *New Host (A or AAAA)*.
5. Provide the *Name* and *IP address* of the Fudo Enterprise Admin Panel (e.g., `mgmt.qa.fudo, 10.0.32.241`).
6. Click *Add Host*.



Create Service User Account:

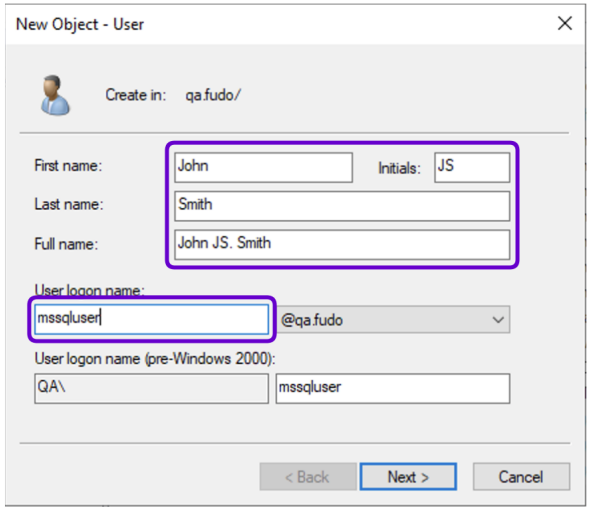
In this section we add the service user `mssqluser`, which will represent the MSSQL service in the domain.

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*.

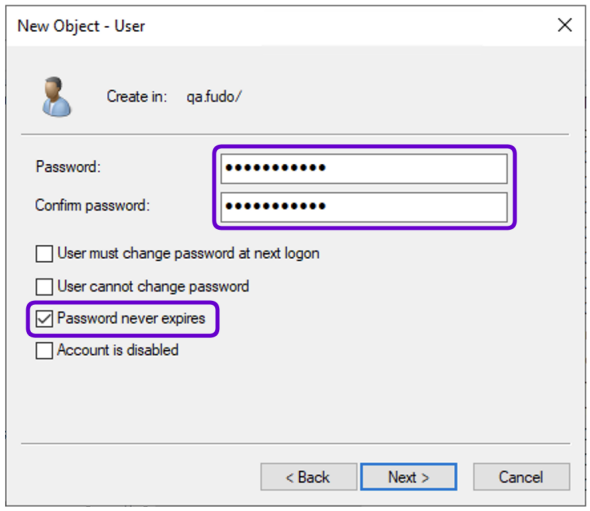


4. In the Manager window, navigate to the domain name, or a specific user group, and right-click on the *Users* catalog.
5. Select *New* > *User*.

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:

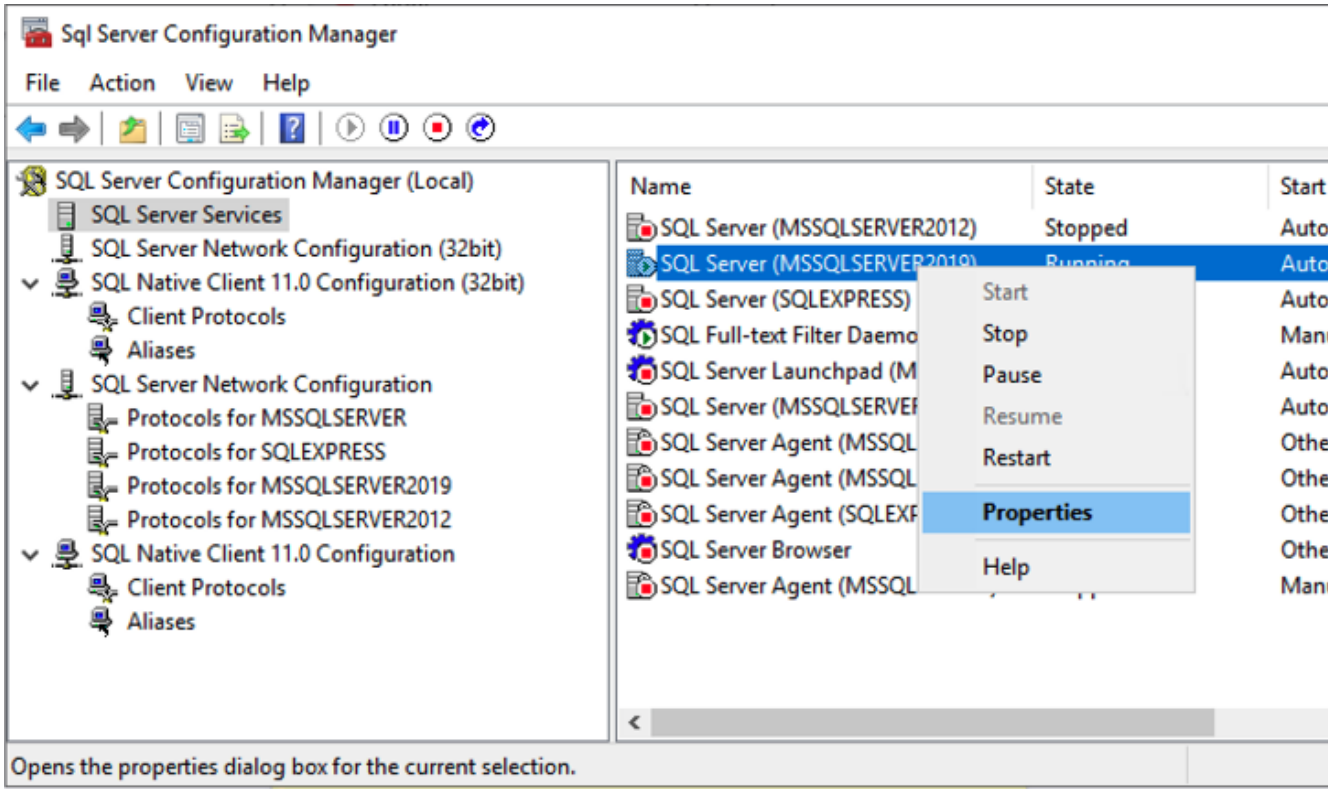
    ```
    setspn -S <service class>/<server name>.
    <domain>:<port>@<domain> <service account>
    ```

    Example:

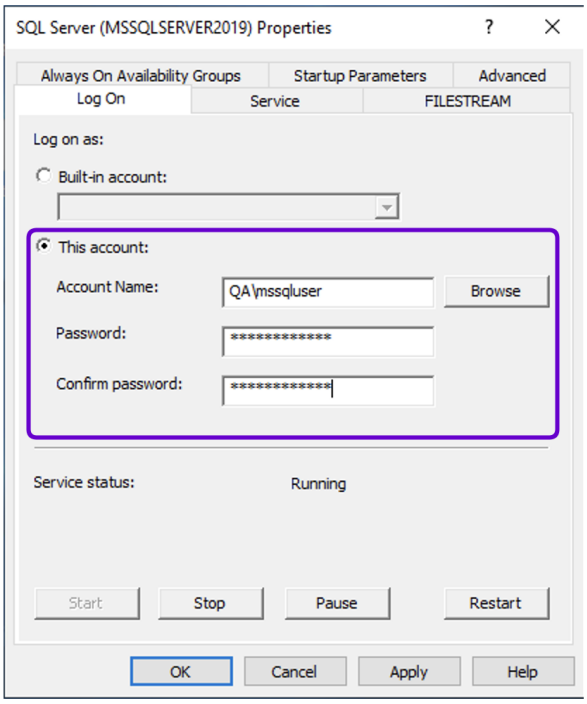
    ```
    setspn -S MSSQLSvc/WIN2019-DC1.qa.fudo:1433@QA.FUDO
    mssqluser
    ```

SQL Server Configuration Manager:

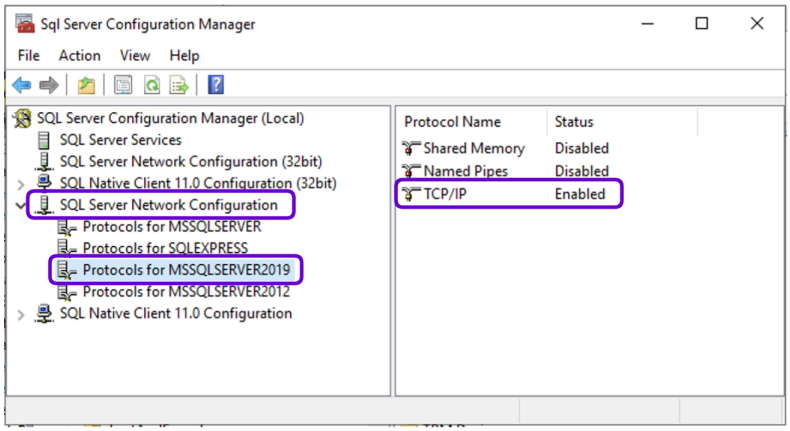
1. Launch SQL Server Configuration Manager.
2. Expand SQL Server Services, select the server, and open the Properties.



3. In the Log On tab, enter the authentication credentials for the `mssqluser` account.



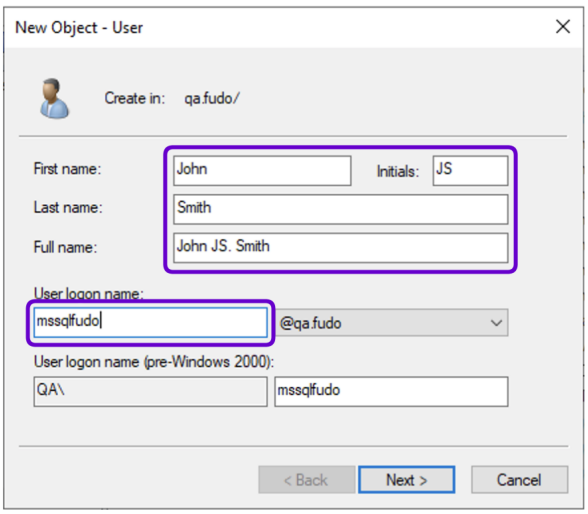
4. Expand SQL Server Network Configuration, select the server, and ensure that the TCP/IP connection is enabled.



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>@<domain> <service account> setspn -S MSSQLSvc/
mgmt.qa.fudo:1433@QA.FUDO mssqlfudo
```

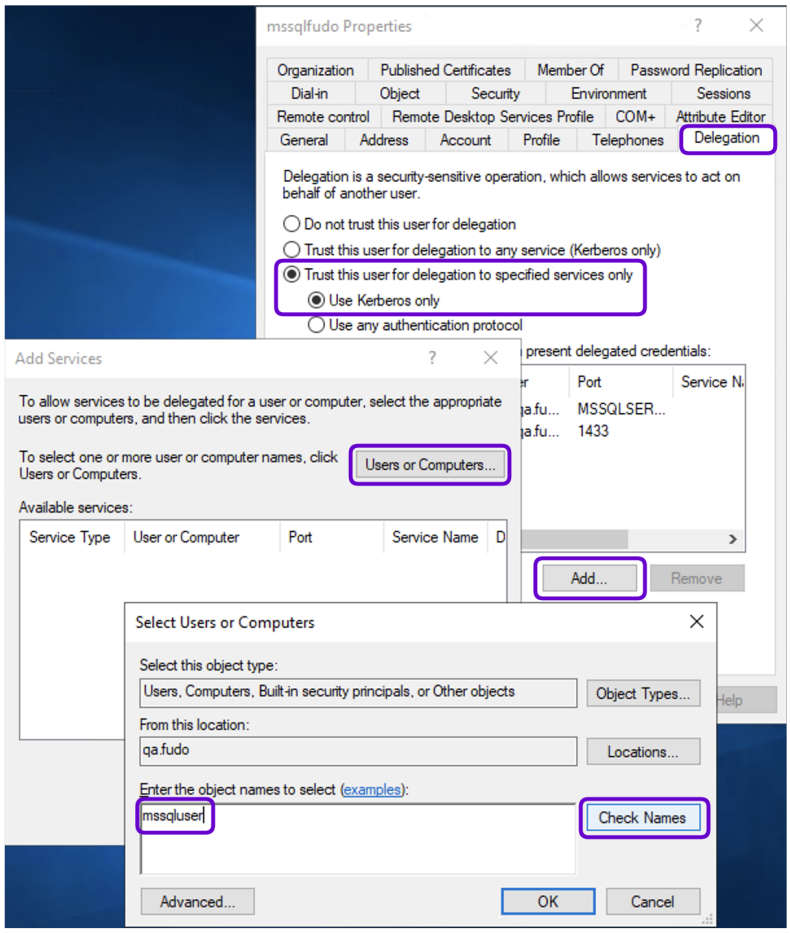
Kerberos Delegation

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    -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 -out
mssqlfudo.keytab
```

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.

30.7.2 Setup Fudo Enterprise

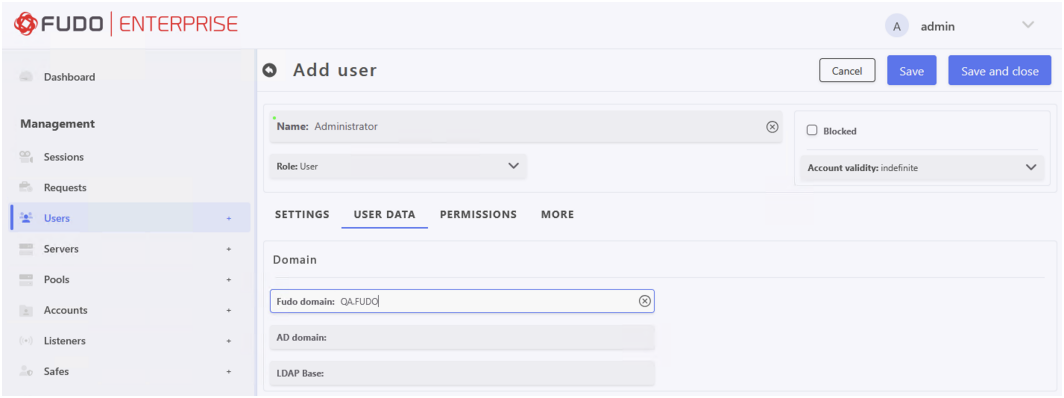
Configure DNS:

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 *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`).

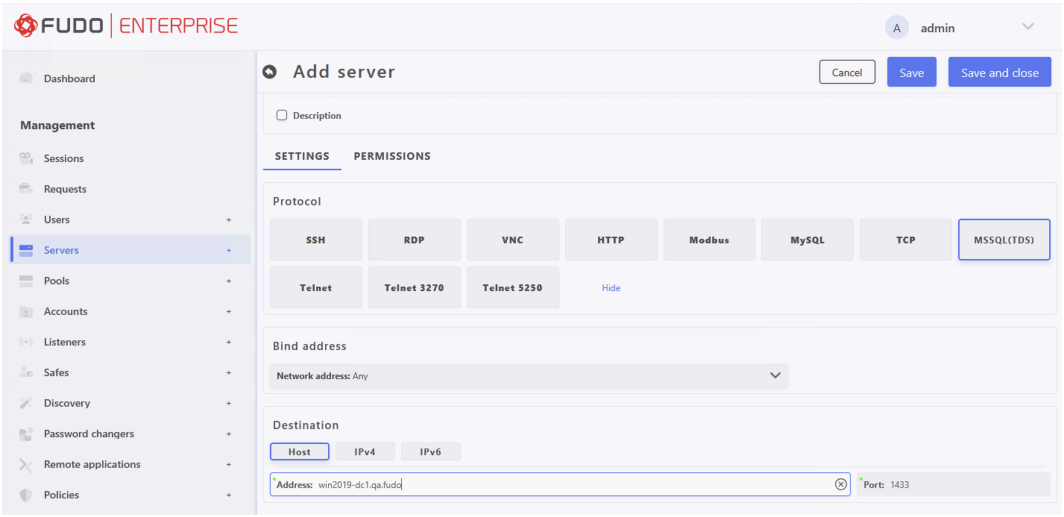
Note: The *Fudo domain* should match the domain name specified in the Kerberos ticket.



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`).
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.

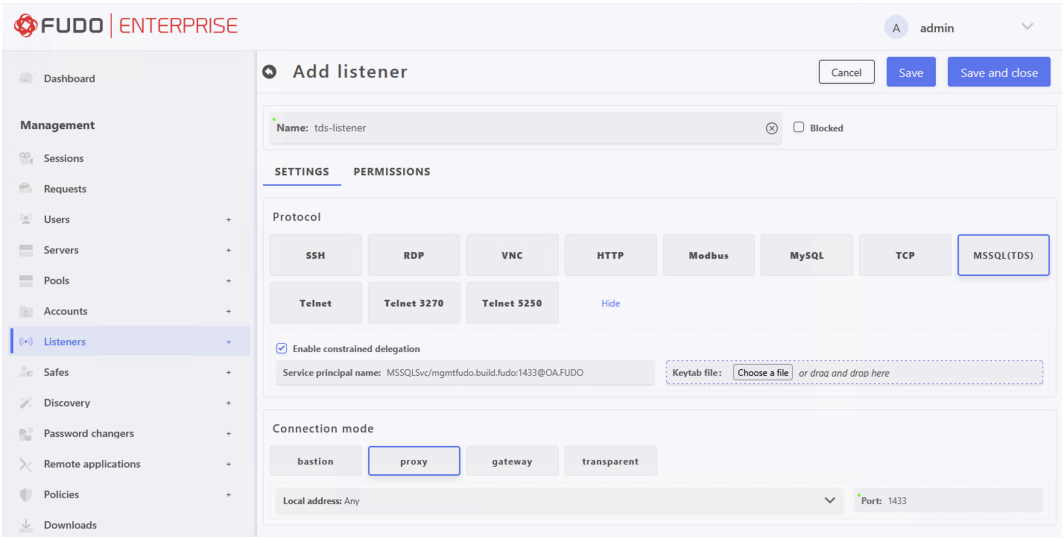
Configure Listener

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*.

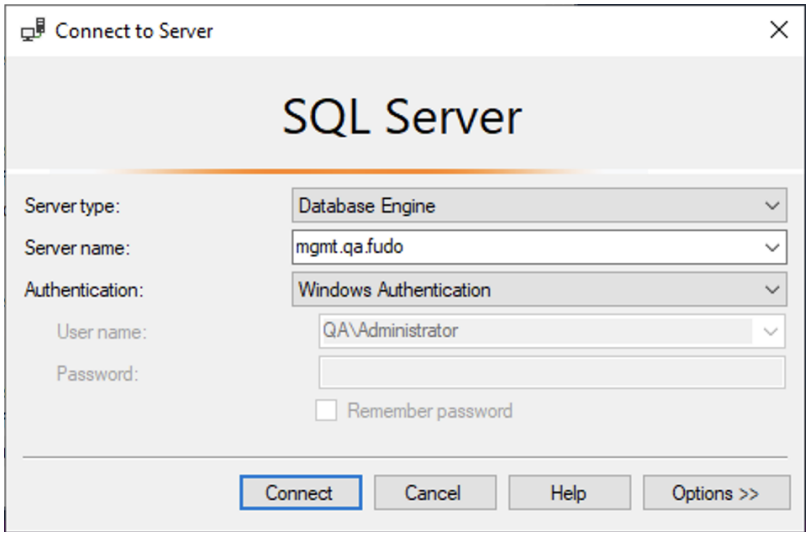
- Mark the checkbox in front of the accounts' names to add it (e.g., `tds:forward`).
- Click *Save* to close the modal window.
- Select desired account and click *Manage listeners* to assign listener to account (e.g., `tds-listener`).
- Click *Save* to close the modal window.

6. Click *Save and close* to save the safe configuration.

30.7.3 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*

30.8 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.

30.8.1 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.

30.8.1.1 Establishing an SSH Connection

User Configuration

1. Go to *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

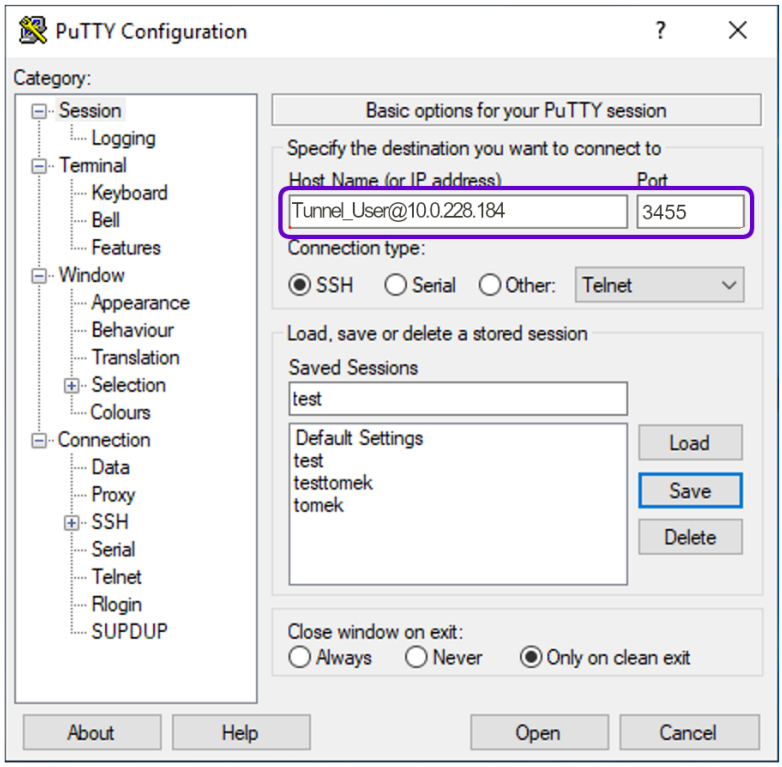
1. Select **Management** > **Accounts**, click + **Add account**.
2. Enter a name (e.g., `Tunnel_Account`).
3. In the **Settings** tab, under **Type**, select **REGULAR**.
4. In the **Target** section, select the `SSH_Tunnel_Server`.
5. In the **Credentials** section: - Enter the login (e.g., `admin`). - 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

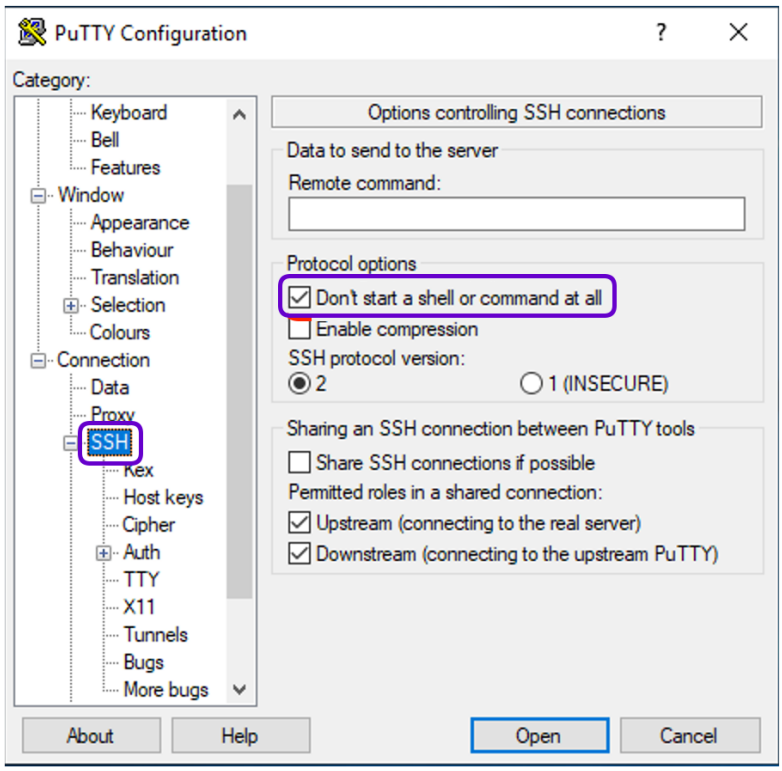
1. Select **Management** > **Safes** and click + **Add safe**.
2. Enter a name (e.g., `Tunnel_Safe`), click **Save**.
3. In the **Users** tab, click **Manage users** and select the `Tunnel_User`.
4. Click **Save**.
5. In the **Accounts** tab, click **Manage accounts** and select `Tunnel_Account`.
6. Click **Save**.
7. Select `Tunnel_Account`, click **Manage listeners**, and select `SSH_Tunnel`.
8. Click **Save**, then **Save and close**.

PuTTY Configuration

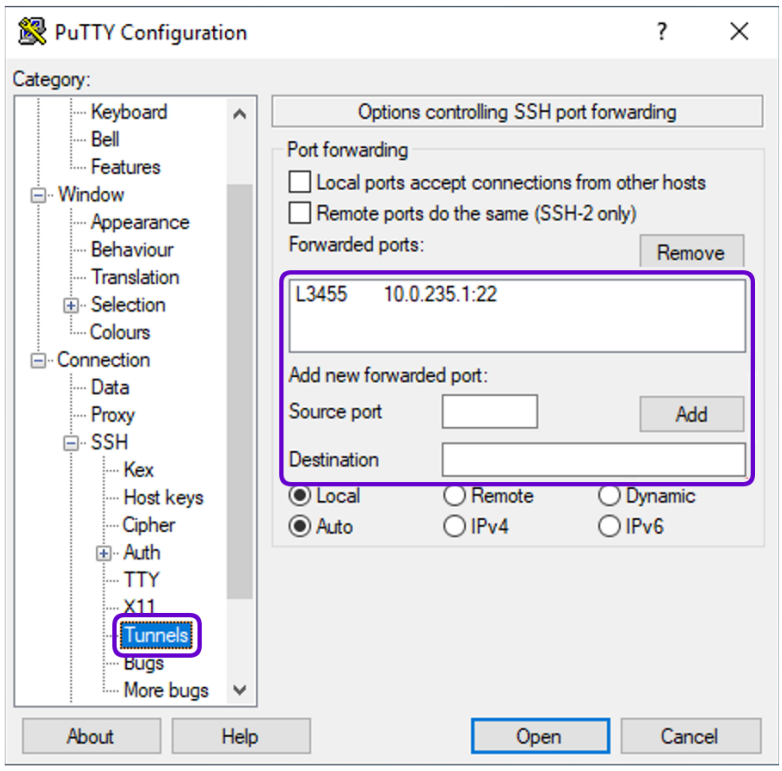
1. Launch PuTTY.
2. In the **Host Name** field, enter `<Fudo_user>@<Fudo_IP_address>`, e.g., `Tunnel_User@10.0.228.184`.
3. In the **Port** field, enter the port of the previously created *Tunnel*-type listener (e.g., `3455`).



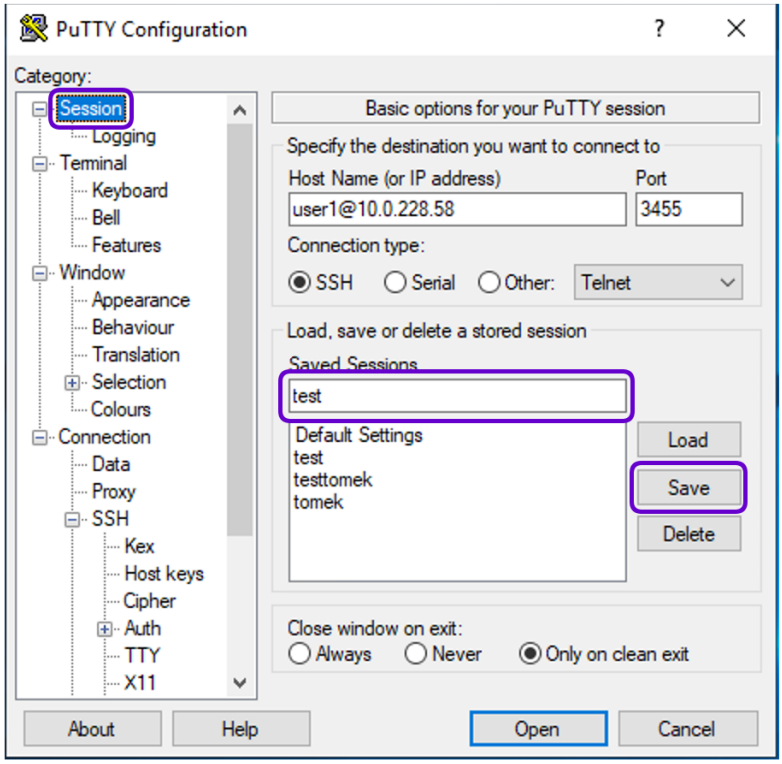
4. Go to the **SSH** tab and check **Don't start a shell or command at all**.



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.

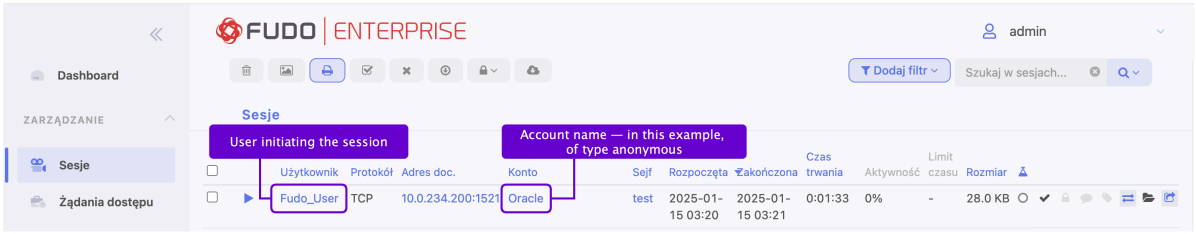
Example:

```
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
```

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.



30.8.1.2 Establishing an HTTP Connection

User Configuration

1. Go to *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

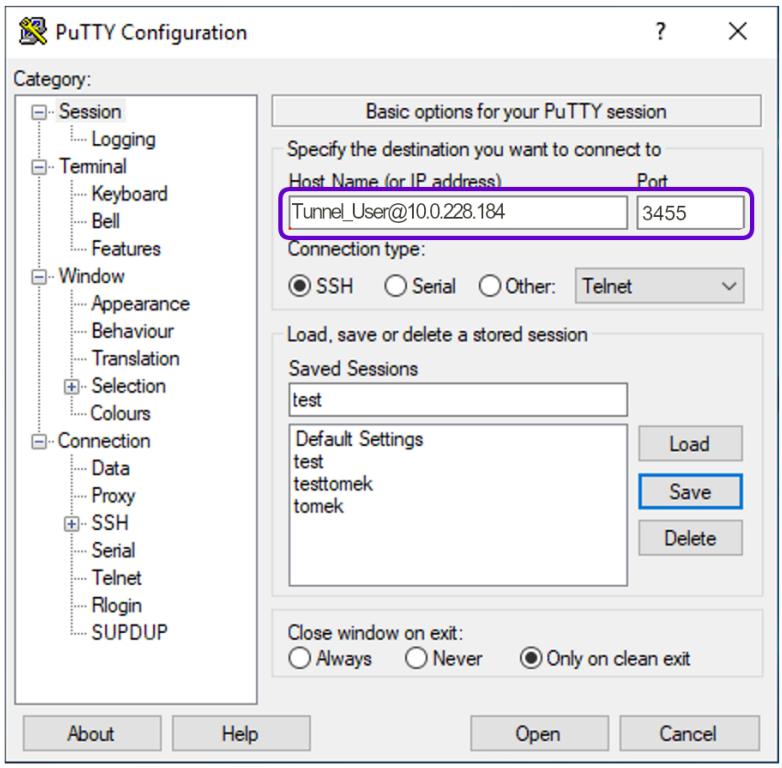
1. Select **Management** > **Accounts**, click + **Add account**.
2. Enter a name (e.g., `HTTP_Tunnel_Account`).
3. Set **Session recording** to **noraw**.
4. In the **Settings** tab, under **Type**, select **FORWARD**.
5. In the **Target** section, select the server `HTTP_Tunnel_Server`.
6. In the **Replace secret** section, select **none**.
7. Click **Save**, then **Save and exit**.

Safe Configuration

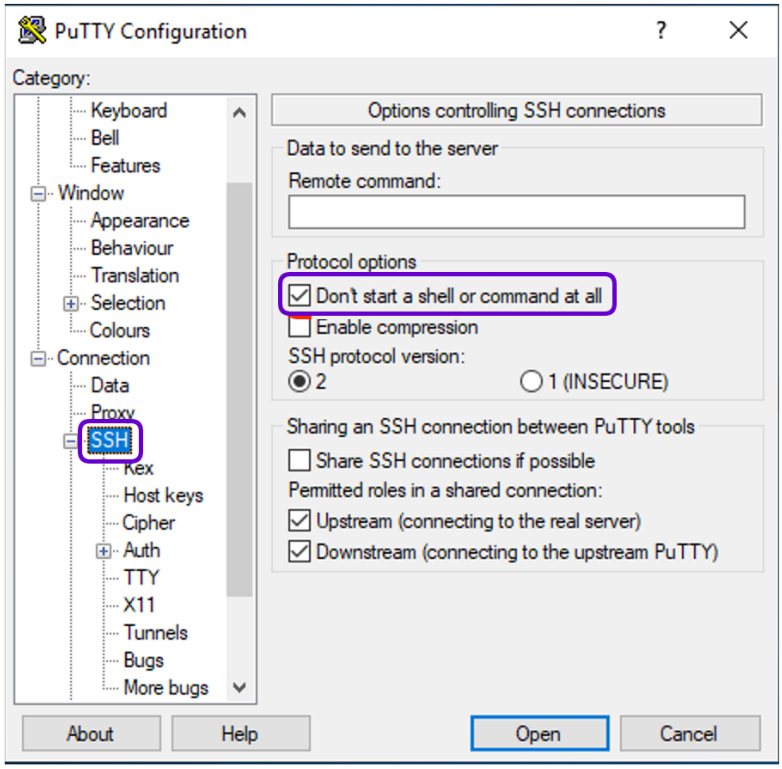
1. Select **Management** > **Safes** and click + **Add safe**.
2. Enter a name (e.g., `Tunnel_Safe`), click **Save**.
3. In the **Users** tab, click **Manage users** and select `Tunnel_User`.
4. Click **Save**.
5. In the **Accounts** tab, click **Manage accounts** and select `HTTP_Tunnel_Account`.
6. 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`).

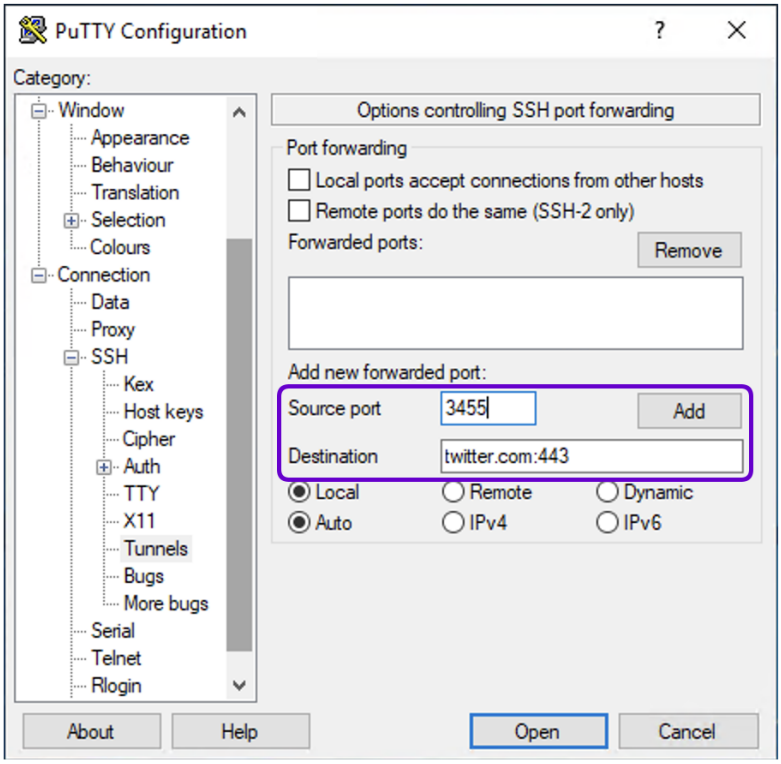


4. Go to the **SSH** tab and check **Don't start a shell or command at all**.

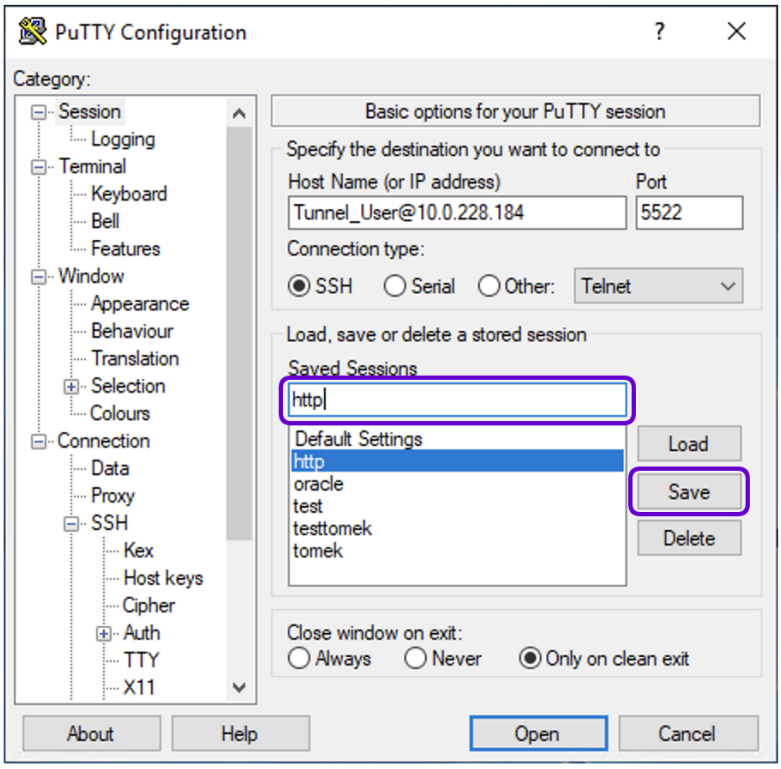


5. Go to the **Tunnels** tab and add a forwarded port:
   - **Source port**: enter the port you want to forward (e.g., 3455).
   - **Destination**: enter the target server address and port in the format `<destination_server_address>:<port>` (e.g., `twitter.com:443`).

- Click **Add**.



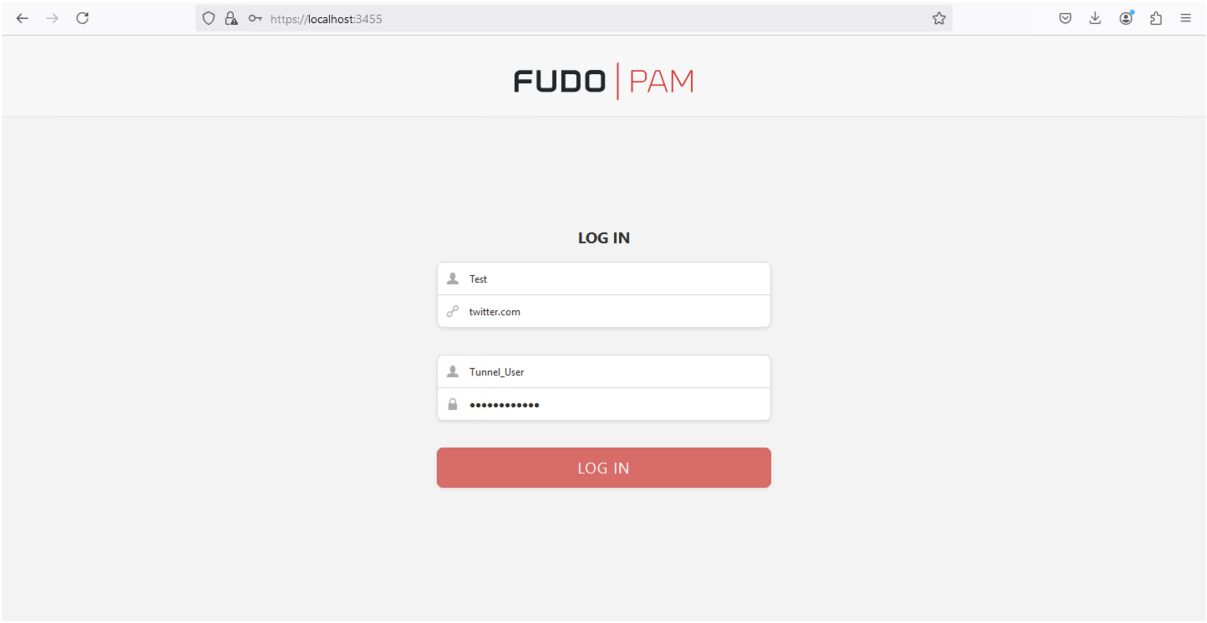
6. Return to the **Sessions** tab, save the configuration, and click **Open**.



7. Enter the password for `Tunnel_User` (e.g., `TestPassw0rd`) and press **Enter**.
8. The tunnel is established.

Connecting via Browser

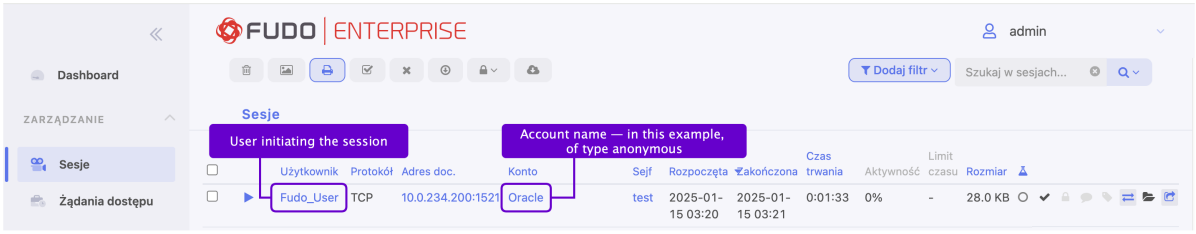
1. Open a web browser.
2. In the address bar, enter the address with the port configured for the listener: `https://localhost:3455`.
3. In the Fudo login screen:
   - **Server login** – enter any name (not used in this scenario),
   - **Server address** – enter the target server address (e.g., `twitter.com`),
   - **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.



30.8.1.3 Connecting to an Oracle Database

User Configuration

1. Go to *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.

---

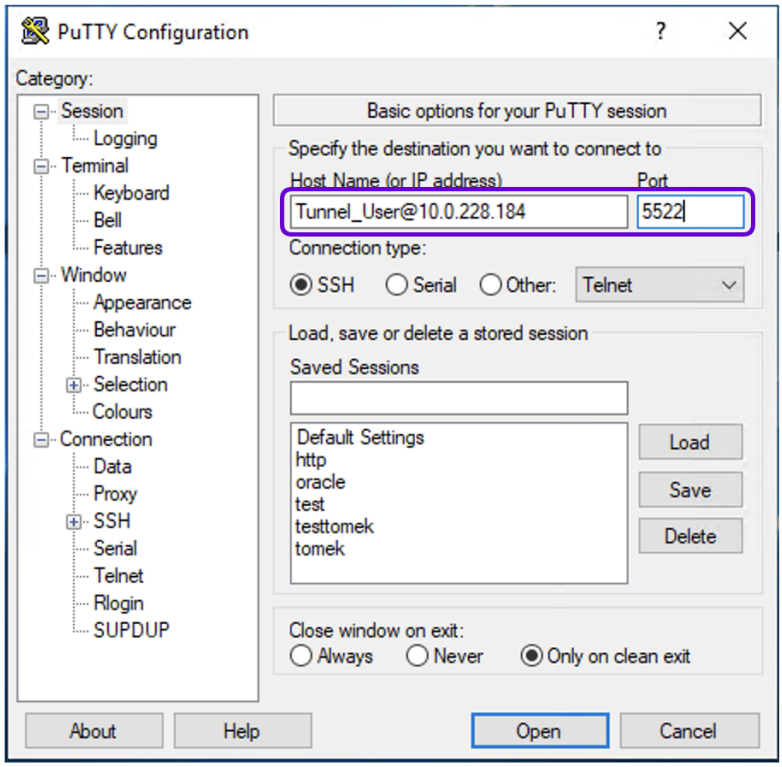
1. Select **Management** > **Accounts**, click + **Add account**.
2. Enter a name (e.g., `Oracle_Tunnel_Account`).
3. Set the **Session recording** option to **raw**.
4. In the **Settings** tab, under **Type**, select **ANONYMOUS**.
5. In the **Target** section, select the `Oracle_Tunnel_Server`.
6. Click **Save and exit**.

Safe Configuration

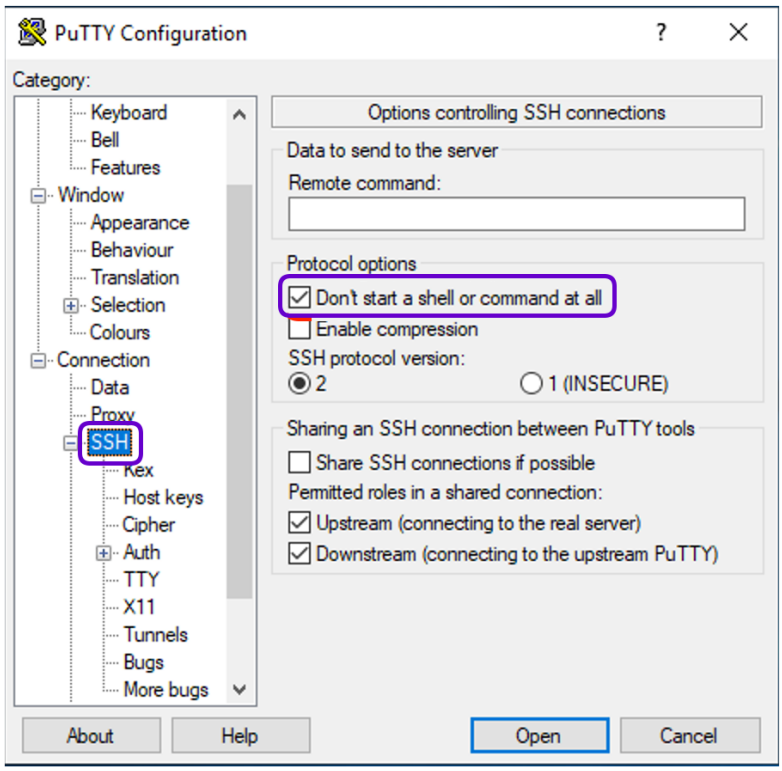
1. Select **Management** > **Safes** and click + **Add safe**.
2. Enter a name (e.g., `Tunnel_Safe`), click **Save**.
3. In the **Users** tab, click **Manage users** and select `Tunnel_User`.
4. Click **Save**.
5. In the **Accounts** tab, click **Manage accounts** and select `Oracle_Tunnel_Account`.
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

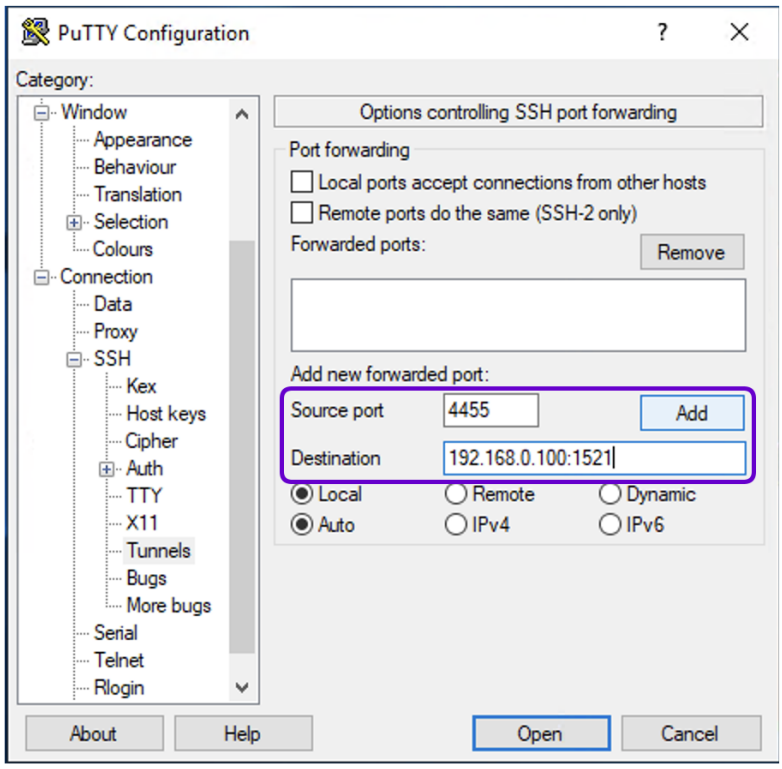
1. Launch **PuTTY**.
2. In the **Host Name** field, enter `<Fudo_user>@<Fudo_IP_address>`, e.g., `Tunnel_User@10.0.228.184`.
3. In the **Port** field, enter the port of the *Tunnel*-type listener created earlier (e.g., `5522`).



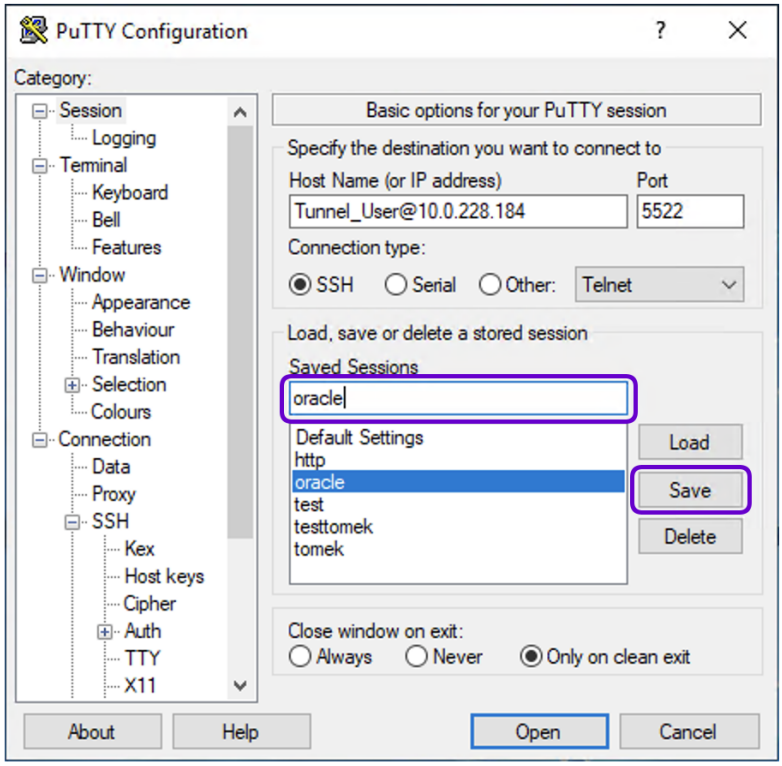
4. Go to the **SSH** tab and check **Don't start a shell or command at all**.



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**.



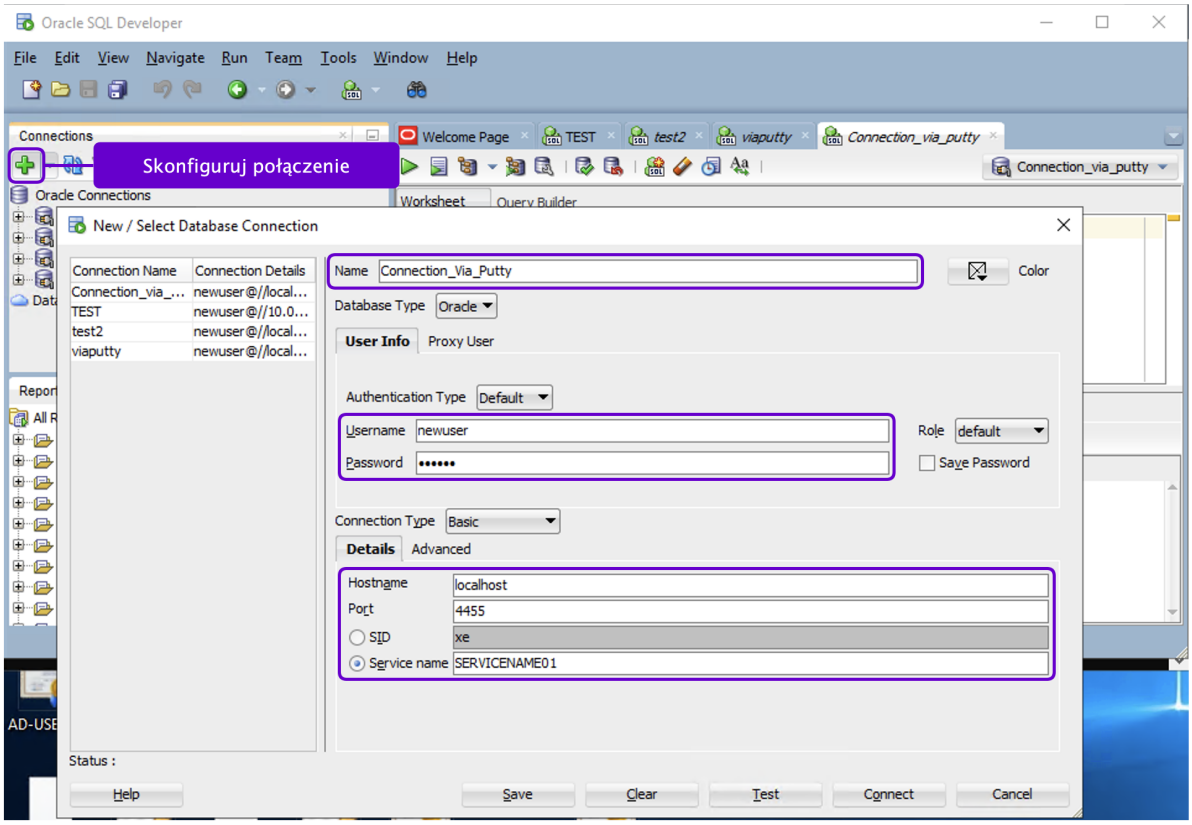
6. Return to the **Sessions** tab, save the configuration, and click **Open**.



7. Enter the password set for `Tunnel_User` (e.g., `TestPassw0rd`) and press **Enter**.
8. The tunnel is established.

Connecting via Oracle Client

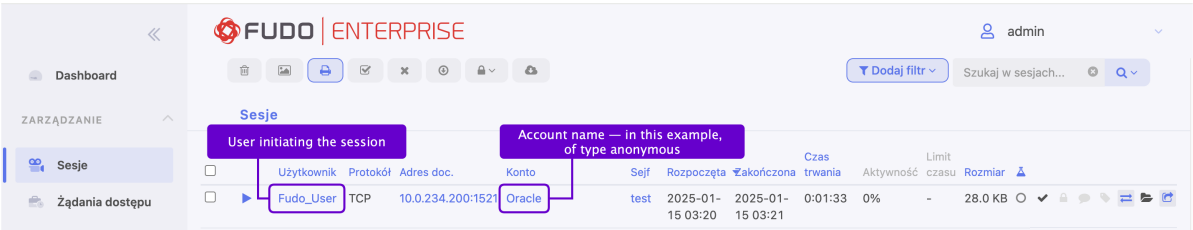
1. Launch your Oracle client (e.g., **Oracle SQL Developer**).
2. Click **New Connection** to create a new configuration.
3. Fill in the fields:
   - **Name** – connection name,
   - **Username** and **Password** – database login credentials,
   - **Hostname** – `localhost`,
   - **Port** – `4455` (as 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.



CHAPTER 31

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?

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.

CHAPTER 32

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); password changing policy as well as the password 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.

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, gateway, transparent, 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.

password changer Tool which enables facilitating automated password 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.

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.

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.

WWN World Wide Name - unique object identifier in external storage solutions.

Index

A

account, **714**
accounts, **714**
Active Directory, **714**
AD, **714**
administration
    configuration export/import, 491
AI, 441, 442, 446
anonymous safe, **714**
API
    users, 176
ARP, **714**
AUROC, **714**
Azure, **714**

C

CERB, **714**
CIDR, **714**
configuration
    Network configuration, 423, 434
    notifications, 438
    users synchronization, 188
connection mode
    bastion, 25
    gateway, 24
    proxy, 24
    transparent, 24
creating
    servers, 194

D

data retention, **714**
deleting
    servers, 222
deployment scenario
    bridge, 22
    forced routing, 23
DHCP, **714**
DNS, **715**
DUO, **715**

E

editing
    servers, 219, 224
Efficiency Analyzer/Productivity Analyzer, **715**
external authentication server, **715**

F

False Positive Rate, **715**
Fingerprint, **715**

H

heartbeat, **715**
hot-swap, **715**
HTTP
    protocol, 9
    protocols, 9
    servers, 194

I

import
    servers, 218

K

Kerberos, **715**

L

LDAP, **715**
listener, **715**

M

Modbus
    protocol, 10
    protocols, 10
    servers, 197
MS SQL
    servers, 198

MS SQL (*TDS*)
    protocol, 10
    protocols, 10
MySQL
    protocol, 11
    protocols, 11
    servers, 200

N

Network configuration
    IP labels, 434
    network interface configuration, 423
network configuration
    routing, 434

O

OATH, **715**
OCR, **715**
Okta, **715**
OpenID Connect, **715**

P

password changer, **715**
passwords repository, **715**
policy, **715**
protocol
    HTTP, 9
    Modbus, 10
    MS SQL (*TDS*), 10
    MySQL, 11
    RDP, 11
    secret, 21
    SSH, 14
    TCP, 21
    Telnet, 19
    Telnet 3270, 18
    Telnet 5250, 19
    VNC, 20
    X11, 21
protocols
    HTTP, 9
    Modbus, 10
    MS SQL (*TDS*), 10
    MySQL, 11
    RDP, 11
    secret, 21
    SSH, 14
    TCP, 21
    Telnet, 19
    Telnet 3270, 18
    Telnet 5250, 19
    VNC, 20
    X11, 21
PSM, **715**
PSM (*Privileged Session Management*), **715**
Public key, **715**

R

RADIUS, **716**
RDP, **716**
RDP
    protocol, 11
    protocols, 11
    servers, 202
RDP connections broker, **716**
RDP connections broker, 528
redundancy group, **716**

S

safe, **716**
secret
    protocol, 21
    protocols, 21
server, **716**
servers, **716**
servers
    creating, 194
    deleting, 222
    editing, 219, 224
    HTTP, 194
    import, 218
    Modbus, 197
    MS SQL, 198
    MySQL, 200
    RDP, 202
    ssh, 205
    TCP, 215
    Telnet, 207
    Telnet 3270, 209
    Telnet 5250, 211
    VNC, 213
sessions
    commenting, 375
    filtering, 362
    play and preview, 365
shared session, **716**
SMS, **716**
SSH, **716**
SSH
    protocol, 14
    protocols, 14
ssh
    servers, 205
SSH access, **716**

SSO, **716**
Static password, **716**
Syslog, **716**

T

TCP
    protocol, 21
    protocols, 21
    servers, 215
Telnet
    protocol, 19
    protocols, 19
    servers, 207
Telnet 3270
    protocol, 18
    protocols, 18
    servers, 209
Telnet 5250
    protocol, 19
    protocols, 19
    servers, 211
Threat Probability, **716**
time policy, **716**
timestamp, **716**
True Positive Rate, **716**

U

user, **716**
users
    access rights, 176
    API, 176
    roles, 176
users synchronization, 188
    configuration, 188

V

VLAN, **716**
VNC, **716**
VNC
    protocol, 20
    protocols, 20
    servers, 213

W

WWN, **716**

X

X11
    protocol, 21
    protocols, 21