# Fudo PAM 3.10 - System Documentation

*Release is not supported*

Fudo Security

January 11, 2022

# Spis treści


**1 General information** **1**
1.1 About documentation . . . 1

**2 System overview** **4**
2.1 PSM . . . 4
2.2 AAPM (Application to Application Password Manager) . . . 5
2.3 Secret manager . . . 5
2.4 Efficiency Analyzer . . . 6
2.5 User portal . . . 6
2.6 Supported protocols . . . 7
2.6.1 Citrix StoreFront (HTTP) . . . 7
2.6.2 HTTP . . . 7
2.6.3 ICA . . . 7
2.6.4 Modbus . . . 8
2.6.5 MS SQL (TDS) . . . 8
2.6.6 MySQL . . . 9
2.6.7 Oracle . . . 9
2.6.8 RDP . . . 10
2.6.9 SSH . . . 11
2.6.10 Telnet 3270 . . . 11
2.6.11 Telnet 5250 . . . 12
2.6.12 Telnet . . . 12
2.6.13 VNC . . . 12
2.6.14 X11 . . . 13
2.6.15 TCP . . . 13
2.7 Data model . . . 14
2.8 Deployment scenarios . . . 15
2.9 Connection modes . . . 16
2.10 User authentication methods and modes . . . 18
2.11 Security measures . . . 21
2.11.1 Data encryption . . . 21
2.11.2 Backups . . . 21
2.11.3 Permissions . . . 21
2.11.4 Sandboxing . . . 21
2.11.5 Reliability . . . 22
2.11.6 Cluster configuration . . . 22

2.12 Dashboard . . . 23

**3 System deployment** **25**
3.1 Requirements . . . 25
3.2 Hardware overview . . . 25
3.3 System initiation . . . 27

**4 Quick start** **33**
4.1 SSH . . . 33
4.1.1 Prerequisites . . . 33
4.1.2 Configuration . . . 33
4.1.3 Establishing connection . . . 38
4.1.4 Viewing user session . . . 39
4.2 SSH in bastion mode . . . 39
4.2.1 Prerequisites . . . 40
4.2.2 Configuration . . . 40
4.2.3 Establishing connection . . . 45
4.2.4 Viewing user session . . . 47
4.3 RDP . . . 48
4.3.1 Prerequisites . . . 48
4.3.2 Configuration . . . 48
4.3.3 Establishing an RDP connection with a remote host . . . 53
4.3.4 Viewing user session . . . 55
4.4 RDP in bastion mode . . . 56
4.4.1 Prerequisites . . . 56
4.4.2 Configuration . . . 56
4.4.3 Establishing an RDP connection with a remote host . . . 61
4.4.4 Viewing user session . . . 63
4.5 Telnet . . . 64
4.5.1 Prerequisites . . . 64
4.5.2 Configuration . . . 65
4.5.3 Establishing a telnet connection with the remote host . . . 69
4.5.4 Viewing user's session . . . 70
4.6 Telnet 5250 . . . 70
4.6.1 Prerequisites . . . 71
4.6.2 Configuration . . . 71
4.6.3 Establishing a telnet connection with the remote host . . . 75
4.6.4 Viewing user's session . . . 77
4.7 MySQL . . . 77
4.7.1 Prerequisites . . . 78
4.7.2 Configuration . . . 78
4.7.3 Establishing connection with a MySQL database . . . 83
4.7.4 Viewing user session . . . 84
4.8 MS SQL . . . 85
4.8.1 Prerequisites . . . 85
4.8.2 Configuration . . . 86
4.8.3 Establishing connection with a MS SQL database . . . 91
4.8.4 Viewing user session . . . 92
4.9 HTTP . . . 93
4.9.1 Prerequisites . . . 94
4.9.2 Configuration . . . 94
4.9.3 Connecting to remote resource . . . 98

4.9.4 Viewing user session . . . 98
4.10 Citrix . . . 99
4.10.1 ICA . . . 100
4.10.1.1 Prerequisites . . . 100
4.10.1.2 Configuration . . . 100
4.10.1.3 Creating `.ica` file with connection parameters . . . 104
4.10.1.4 Connecting to remote resource . . . 105
4.10.1.5 Viewing user session . . . 105
4.10.2 ICA via Citrix StoreFront . . . 105
4.10.2.1 Prerequisites . . . 105
4.10.2.2 Configuration . . . 106
4.10.2.3 Connecting to remote resource . . . 112
4.10.2.4 Viewing user session . . . 113
4.11 VNC . . . 114
4.11.1 Prerequisites . . . 114
4.11.2 Configuration . . . 114
4.11.3 Establishing connection . . . 119
4.11.4 Viewing user session . . . 122
4.12 Oracle over RemoteApp . . . 123
4.12.1 Prerequisites . . . 123
4.12.2 Configuration . . . 124
4.12.3 Changing registry entries on the RDS domain controller . . . 129
4.12.4 Establishing connection . . . 129
4.12.5 Viewing user session . . . 132
4.13 User authentication against external LDAP server . . . 133
4.13.1 Prerequisites . . . 134
4.13.2 Configuration . . . 134

**5 Users** **136**
5.1 Creating a user . . . 137
5.2 Editing a user . . . 143
5.3 Blocking a user . . . 144
5.4 Unblocking a user . . . 145
5.5 Deleting a user . . . 146
5.6 Time access policy . . . 147
5.7 Authentication failures counter . . . 149
5.8 Roles . . . 150
5.9 Users synchronization . . . 151
5.10 Adding a mobile device . . . 155
5.11 Removing paired mobile device . . . 157

**6 Servers** **159**
6.1 Creating a server . . . 159
6.1.1 Static server . . . 159
6.1.1.1 Creating a Citrix server . . . 159
6.1.1.2 Creating an HTTP server . . . 161
6.1.1.3 Creating an ICA server . . . 163
6.1.1.4 Creating a Modbus server . . . 165
6.1.1.5 Creating a MS SQL server . . . 167
6.1.1.6 Creating a MySQL server . . . 168
6.1.1.7 Creating an Oracle server . . . 170
6.1.1.8 Creating an RDP server . . . 171

6.1.1.9 Creating an SSH server . . . 173
6.1.1.10 Creating a Telnet server . . . 175
6.1.1.11 Creating a Telnet 3270 server . . . 177
6.1.1.12 Creating a Telnet 5250 server . . . 179
6.1.1.13 Creating a VNC server . . . 181
6.1.1.14 Creating a TCP server . . . 183
6.1.2 Dynamic server . . . 185
6.1.2.1 Creating a dynamic servers group . . . 185
6.1.2.2 Adding a single host to a servers group . . . 186
6.2 Editing a server . . . 187
6.3 Blocking a server . . . 188
6.4 Unblocking a server . . . 189
6.5 Deleting a server . . . 190
6.5.1 Deleting a static server definition . . . 190
6.5.2 Deleting a dynamically added host . . . 190

**7 Accounts** **192**
7.1 Creating an account . . . 193
7.1.1 Creating an *anonymous* account . . . 193
7.1.2 Creating a *forward* account . . . 194
7.1.3 Creating a *regular* account . . . 197
7.2 Editing an account . . . 201
7.3 Blocking an account . . . 202
7.4 Unblocking an account . . . 203
7.5 Deleting an account . . . 204

**8 Safes** **206**
8.1 Creating a safe . . . 207
8.2 Editing a safe . . . 209
8.3 Blocking a safe . . . 210
8.4 Unblocking a safe . . . 211
8.5 Deleting a safe . . . 212

**9 Listeners** **214**
9.1 Creating a listener . . . 215
9.1.1 Creating a Citrix listener . . . 215
9.1.2 Creating a HTTP listener . . . 217
9.1.3 Creating an ICA listener . . . 218
9.1.4 Creating a Modbus listener . . . 221
9.1.5 Creating a MySQL listener . . . 222
9.1.6 Creating an Oracle listener . . . 224
9.1.7 Creating an RDP listener . . . 225
9.1.8 Creating an SSH listener . . . 228
9.1.9 Creating a MS SQL listener . . . 230
9.1.10 Creating a Telnet listener . . . 231
9.1.11 Creating a Telnet 3270 listener . . . 233
9.1.12 Creating a Telnet 5250 listener . . . 235
9.1.13 Creating a VNC listener . . . 237
9.1.14 Creating a TCP listener . . . 239
9.2 Editing a listener . . . 241
9.3 Blocking a listener . . . 241
9.4 Unblocking a listener . . . 242

9.5 Deleting a listener . . . 243

**10 Password changers** **245**
10.1 Password changer policy . . . 245
10.1.1 Defining a password changer policy . . . 245
10.1.2 Editing a password changer policy . . . 246
10.1.3 Deleting a password changer policy . . . 247
10.2 Custom password changers . . . 247
10.2.1 Defining a custom password changer . . . 247
10.2.2 Editing a custom password changer . . . 248
10.2.3 Deleting a custom password changer . . . 249
10.3 Setting up password changing on a Unix system . . . 249
10.4 Setting up password changing on Michrosoft Windows system . . . 251

**11 Policies** **255**

**12 Sessions** **261**
12.1 Filtering sessions . . . 262
12.1.1 Defining filters . . . 262
12.1.2 Full text search . . . 264
12.1.3 Managing user defined filter definitions . . . 265
12.2 Viewing sessions . . . 266
12.3 Viewing live sessions . . . 269
12.4 Pausing connection . . . 269
12.5 Terminating connection . . . 270
12.6 Joining live session . . . 272
12.7 Sharing sessions . . . 273
12.8 Commenting sessions . . . 275
12.9 Exporting sessions . . . 277
12.10 Deleting sessions . . . 279
12.11 OCR processing sessions . . . 279
12.12 Timestamping selected sessions . . . 281
12.13 Approving pending connections . . . 281
12.13.1 Fudo management interface . . . 281
12.13.2 Fudo Mobile . . . 282
12.14 Declining pending connections . . . 282
12.14.1 Fudo administration interface . . . 282
12.14.2 Fudo Mobile . . . 283

**13 Reports** **285**

**14 Efficiency analyzer** **289**
14.1 Overview . . . 289
14.2 Sessions analysis . . . 290
14.3 Activity comparison . . . 292

**15 Administration** **293**
15.1 System . . . 293
15.1.1 Date and time . . . 293
15.1.2 SSL certificates . . . 296
15.1.3 Deny new connections . . . 298
15.1.4 SSH access . . . 298

15.1.5 Reset account . . . 299
15.1.6 Sensitive features . . . 300
15.1.7 System update . . . 301
15.1.7.1 Updating system . . . 302
15.1.7.2 Deleting upgrade snapshot . . . 303
15.1.8 License . . . 304
15.1.9 Diagnostics . . . 305
15.1.10 Default domain . . . 306
15.1.11 Password complexity . . . 307
15.1.12 Single Sign On in User Portal . . . 308
15.2 Network settings . . . 308
15.2.1 Network interfaces configuration . . . 309
15.2.1.1 Managing physical interfaces . . . 309
15.2.1.2 Defining IP address using system console . . . 312
15.2.1.3 Setting up a network bridge . . . 315
15.2.1.4 Setting up virtual networks (VLANs) . . . 316
15.2.1.5 Setting up LACP link aggregation . . . 317
15.2.2 Labeled IP addresses . . . 318
15.2.3 Bypasses configuration . . . 319
15.2.4 Routing configuration . . . 320
15.2.5 DNS configuration . . . 321
15.2.6 Proxy servers configuration . . . 323
15.2.7 ARP table configuration . . . 325
15.3 Notifications . . . 327
15.4 Trusted time-stamping . . . 330
15.5 External authentication . . . 331
15.6 External passwords repositories . . . 333
15.6.1 CyberArk Enterprise Password Vault . . . 333
15.6.2 Hitachi ID Privileged Access Manager . . . 334
15.6.3 Lieberman Enterprise Random Password Manager . . . 336
15.6.4 Thycotic Secret Server . . . 337
15.7 Resources . . . 339
15.7.1 RDP/VNC login screen configuration . . . 339
15.7.2 *User portal* login screen configuration . . . 341
15.8 System version restore . . . 342
15.9 System restart . . . 343
15.10 SNMP . . . 344
15.10.1 Configuring SNMP . . . 344
15.10.2 SNMP MIBs . . . 345
15.10.3 Getting SNMP readings using `snmpwalk` . . . 345
15.10.4 Wheel Fudo PAM specific SNMP extensions . . . 345
15.11 Backups and retention . . . 353
15.12 External storage . . . 355
15.12.1 Configuring external storage . . . 355
15.12.2 Expanding external storage device . . . 356
15.13 Exporting/importing system configuration . . . 357
15.13.1 Exporting system configuration . . . 357
15.13.2 Importing system configuration . . . 358
15.14 Cluster configuration . . . 358
15.14.1 Initiating cluster . . . 361
15.14.2 Adding cluster nodes . . . 362

15.14.3 Editing cluster nodes . . . 366
15.14.4 Deleting cluster nodes . . . 366
15.14.5 Redundancy groups . . . 367
15.15 Events log . . . 372
15.15.1 External syslog servers . . . 372
15.15.2 Exporting events log . . . 373
15.16 Changing encryption passphrase . . . 374
15.17 Integration with CERB server . . . 375
15.18 System maintenance . . . 383
15.18.1 Backing up encryption keys . . . 383
15.18.2 Monitoring system condition . . . 388
15.18.3 Hard drive replacement . . . 389
15.18.4 Resetting configuration to default settings . . . 390

**16 Reference information** **393**
16.1 RDP connections broker . . . 393
16.2 Log messages . . . 394
16.3 Fudo 2.2 to Fudo 3.0 parameters mapping . . . 407
16.3.1 Connection . . . 408
16.3.2 Server . . . 409
16.4 Data model migration from Wheel Fudo PAM version 2.2 to 3.0 . . . 409
16.4.1 Server . . . 409
16.4.2 Safe (previously *connection*) . . . 409
16.4.3 Account (previously *login credentials*) . . . 410
16.4.4 Listener (previously *bastion* or part of a server) . . . 411
16.4.5 Sessions . . . 411
16.5 ICA configuration file . . . 411
16.5.1 Non-TLS connections ICA file . . . 411
16.5.2 TLS connections ICA file . . . 412

**17 AAPM (Application to Application Password Manager)** **413**
17.1 Compiling *fudopv* tool . . . 413
17.1.1 Python . . . 413
17.1.2 Virtual environment . . . 414
17.1.3 Fetching dependencies . . . 414
17.1.4 Package creation script . . . 415
17.2 Deploying *fudopv* without compiling source files . . . 415
17.3 Using *fudopv* . . . 416
17.4 API interface . . . 422
17.5 Authentication methods . . . 422
17.5.1 Static password . . . 422
17.5.2 Token . . . 423

**18 Service Now** **424**
18.1 Configuration . . . 424
18.2 Requesting access to safe . . . 425
18.3 Granting access . . . 427

**19 Client applications** **429**
19.1 PuTTY . . . 429
19.2 Microsoft Remote Desktop . . . 431
19.3 VNC Viewer . . . 433

19.4 SQL Server Management Studio . . . 436

**20 4-Eyes authentication proxy service** **438**
20.1 Installing proxy service . . . 438
20.2 Initializing configuration using `whlproxyinit` . . . 438
20.3 Managing clusters using `whlproxyctl` . . . 440
20.3.1 Adding a cluster . . . 440
20.3.2 Deleting a cluster . . . 440
20.3.3 Displaying cluster's details . . . 440
20.3.4 Listing clusters . . . 440
20.4 Managing nodes using `whlproxyctl` . . . 441
20.4.1 Adding a node to a cluster . . . 441
20.4.2 Deleting a node . . . 441
20.4.3 Displaying node's details . . . 441
20.4.4 Listing nodes . . . 441

**21 Troubleshooting** **443**
21.1 Booting up . . . 443
21.2 Connecting to servers . . . 444
21.3 Logging to administration panel . . . 448
21.4 Session playback . . . 449
21.5 Cluster configuration . . . 449
21.6 Trusted timestamping . . . 450
21.7 Support mode . . . 450

**22 Frequently asked questions** **454**

**23 Glossary** **457**

**Index** **460**

ROZDZIAŁ 1

# General information

## 1.1 About documentation

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

**Documentation Structure**

*1. General information*

This chapter contains information on documentation.

*2. System overview*

This chapter provides information on Wheel Fudo PAM modules, describes data model, covers deployment scenarios as well as connections models and user authentication methods.

*3. System deployment*

This chapter covers system deployment procedure along with the system initiation.

*4. Quick start*

This chapter contains typical configuration examples.

*5. Users*

This chapter covers users management topics.

*6. Servers*

This chapter covers servers management topics.

*7. Accounts*

This chapter covers accounts management topics.

*8. Safes*

This chapter covers safes management topics.

*9. Listeners*

This chapter covers listeners management topics.

*10. Password changers*

This chapter contains information on automated password changing feature.

*11. Policies*

This chapter contains information on Fudo's proactive monitoring features.

*12. Sessions*

This chapter contains information on stored access sessions.

*13. Reports*

This chapter contains topics related to generating reports.

*14. Efficiency analyzer*

This chapter describes Wheel Fudo PAM's efficiency analyzer module.

*15. Administration*

This chapter contains administration procedures.

*16. Reference information*

This chapter contains reference information which supplement Wheel Fudo PAM administration topics.

*17. AAPM (Application to Application Password Manager)*

This chapter contains information on password management in third party applications.

*18. Service Now*

This chapter covers integration with *Service Now* ticketing system.

*19. Client applications*

This chapter contains client applications configuration instructions for selected protocols.

*20. 4-Eyes authentication proxy service*

This chapter describes proxy service configuration for 4-Eyes authentication scenarios using mobile application.

*21. Troubleshooting*

This chapter contains solutions for potential problems which may occur when using Wheel Fudo PAM.

*22. Frequently asked questions*

This chapter contains frequently requested information about Wheel Fudo PAM.

*23. Glossary*

This chapter contains list of terms used throughout this documentation.

**Conventions and symbols**

This section covers conventions used throughout this documentation.

*italic*

Uster interface elements.

`example`

Example value of a parameter, API method name or code example.

---

**Note:** Note. Additional information closely reletad with described topic, e.g. suggestion concerning given procedure step; additional conditions which have to be met.

---

**Warning:** Warning. 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.

ROZDZIAŁ 2

# System overview

Wheel Fudo PAM is a complete solution for managing remote privileged access.

## 2.1 PSM

PSM module enables facilitating constant monitoring of remote access sessions to IT infrastructure. Wheel Fudo PAM acts as a proxy between users and monitored servers and it registers users' actions, including mouse pointer moves, keystrokes and transferred files.

The PSM module records complete network traffic along with meta data, enabling precise session playback and full-text content search.

Wheel Fudo PAM enables viewing current connections and intervening in a monitored session in case the administrator notices a potential misuse of access rights.

The PSM module supports following system configurations:

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

**Related topics:**

- *Supported protocols*
- *Requirements*
- *Data model*
- *Security measures*

## 2.2 AAPM (Application to Application Password Manager)

AAPM module enables secure passwords exchange between applications.

AAPM supported operating systems:

- Microsoft Windows operating systems,
- Linux family operating systems,
- BSD family operating systems.

**Related topics:**

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

## 2.3 Secret manager

Wheel Fudo PAM can be also set up to automatically manage login credentials on monitored servers and periodically change passwords at specified time intervals (e.g. 1 hour).

Secret manager module supports password changing on following systems:

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

It also enables configuring a custom password changer as a set of commands executed on remote a host.

**Related topics:**

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

## 2.4 Efficiency Analyzer

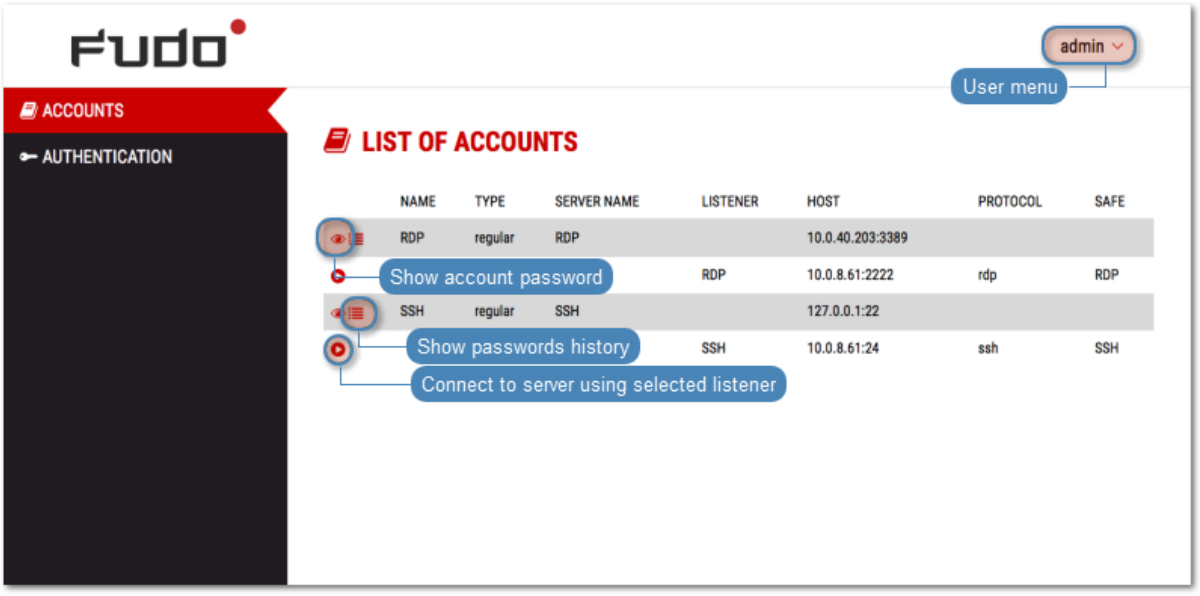
Efficiency Analyzer module tracks users' actions and provides precise information on their activity and idle times.

**Related topics:**

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

## 2.5 User portal

User portal enables browsing available resources and initiating connections with monitored servers using selected listener.




**Related topics:**

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

## 2.6 Supported protocols

### 2.6.1 Citrix StoreFront (HTTP)

Supported connection modes:

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

Notes:

- Session joining is not supported.
- Session player displays raw text without graphical rendering.
- Lack of bastion mode support results from protocol's limitations. Citrix StoreFront itself provides access to a bastion of hosts. When logging to Citrix StoreFront, user can select desired host to connect to over ICA protocol.
- Initiating connections with ICA servers over Citrix StoreFront interface requires *anonymous* or *forward* accounts assigned to those servers.

### 2.6.2 HTTP

Supported connection modes:

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

Notes:

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

### 2.6.3 ICA

Supported connection modes:

- *Bastion* (option to enter account or target server in the ICA file),
- *Gateway*,
- *Proxy*,
- *Transparent*.

Supported client applications:

- Citrix Receiver.

Supported encryption algorithms:

- Basic,
- TLS.

Notes:

- Session joining is not supported.
- ICA connections over *Citrix StoreFront* interface requires using *anonymous* or *forward* type accounts.
- Direct connections to ICA servers (not mediated by *Citrix StoreFront*) requires preparation of an `.ica` configuration file. For more information refer to the *ICA configuration file* topic.

### 2.6.4 Modbus

Supported connection modes:

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

Notes:

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

### 2.6.5 MS SQL (TDS)

Supported connection modes:

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

Supported client applications:

- SQL Server Management Studio,
- sqsh.

Notes:

- Session joining is not supported.

### 2.6.6 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.

**Warning:** Please note that the MySQL server `caching_sha2_password` plugin isn't supported by Fudo PAM. Supportable MySQL plugins by Fudo PAM 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.

### 2.6.7 Oracle

Oracle is a proprietary protocol and its implementation requires reverse engineering. This results in a limited support in development of new features as well as addressing potential issues.

Supported connection modes:

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

Supported client applications:

- SQLDeveloper 4.1.3.20.78,
- SQL*Plus: Release 11.2.0.4.0 Production.

Notes:

- Session joining is not supported.
- Active Directory and other external authentication sources are not supported.
- Session player only displays clients querries (server's responses are not included).
- Oracle 10 and 11 are supported.
- Bastion mode is not supported due to limitations of the protocol.

### 2.6.8 RDP

Supported connection modes:

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

Supported client applications:

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

Supported OCR languages:

- English
- German
- Norwegian
- Polish
- Russian

Notes:

- When authenticating Fudo users against AD (or other external source) the TLS+NLA (Network Level Authentication) is not supported; TLS mode is used instead. NLA mode on server side is supported.
- In case of *Enhanced RDP Security (TLS) + NLA*, Wheel Fudo PAM requires NTLM protocol version 2 or newer. To properly handle NLA authentication connections, enable option to only send NTLMv2 reponse 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*.
- Wheel Fudo PAM 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 Wheel Fudo PAM security restrictions.

To monitor RemoteApp sessions, the connection must be launched through a `*.rdp` configuration file with the Wheel Fudo PAM 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.

### 2.6.9 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,
- 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 - SHA1

Notes:

- SSH keys forwarding is not supported.

### 2.6.10 Telnet 3270

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.

### 2.6.11 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.

### 2.6.12 Telnet

Supported connection modes:

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

Notes:

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

### 2.6.13 VNC

Supported connection modes:

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

Supported client applications:

- TightVNC,

- RealVNC.

Supported OCR languages:

- English,
- German,
- Norwegian,
- Polish,
- Russian.

**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).

### 2.6.14 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.

Notes:

- Session joining is not supported.

### 2.6.15 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.

## 2.7 Data model

Wheel Fudo PAM 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.

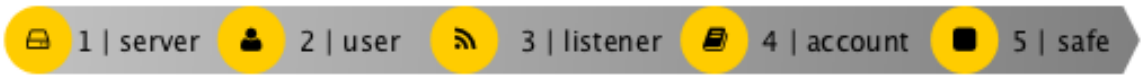
Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

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.

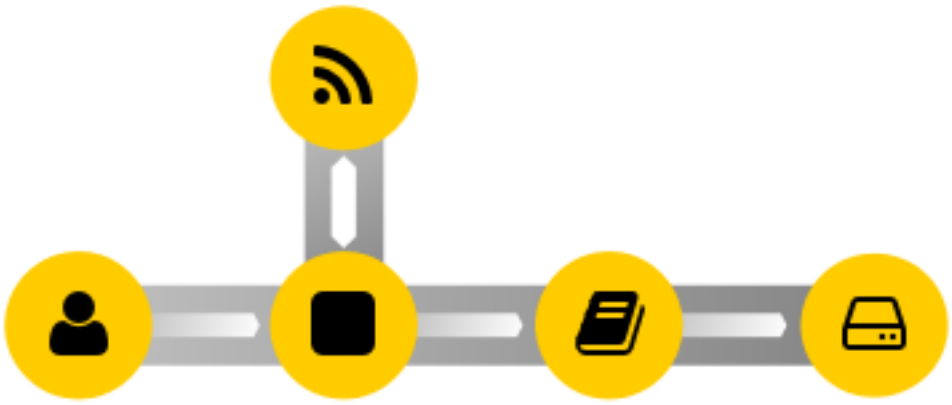
Listener determines server connection mode (proxy, gateway, transparent, bastion) as well as its specifics.

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



**Related topics:**

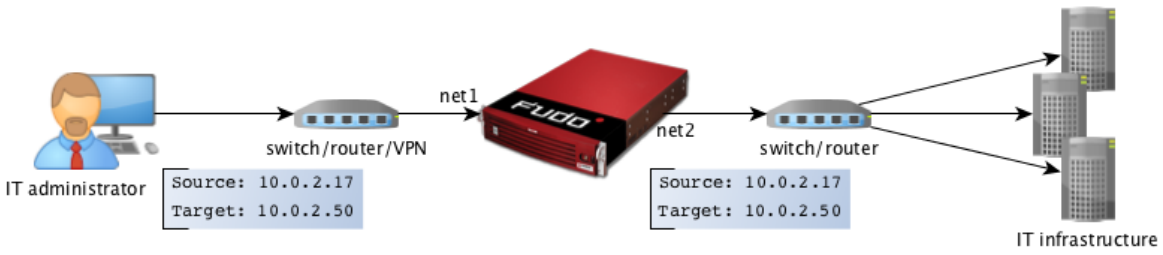
- *System overview*
- *User authorization methods and modes*
- *Quick start*

## 2.8 Deployment scenarios

**Note:** It is advised to deploy the Wheel Fudo PAM 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

In bridge mode Wheel Fudo PAM 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, Wheel Fudo PAM preserves source IP address when forwarding requests to destination servers.

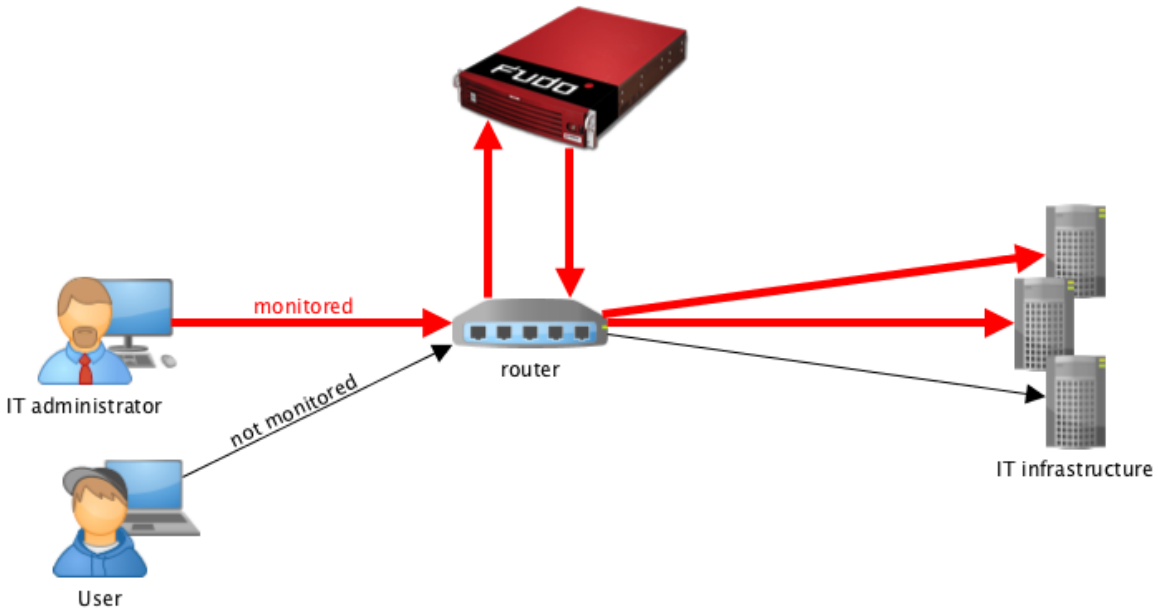
Such solution allows keeping existing rules on firewalls which control access to internal resources.

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 Wheel Fudo PAM 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.

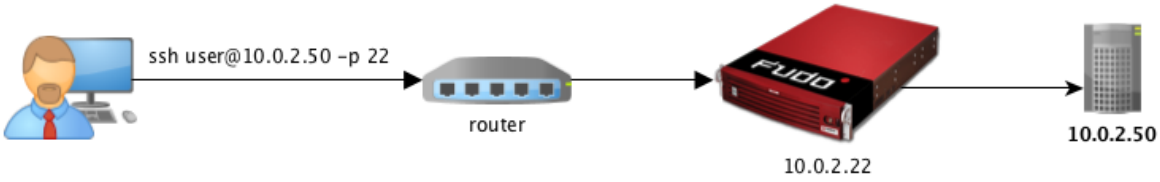
**Related topics:**

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

## 2.9 Connection modes

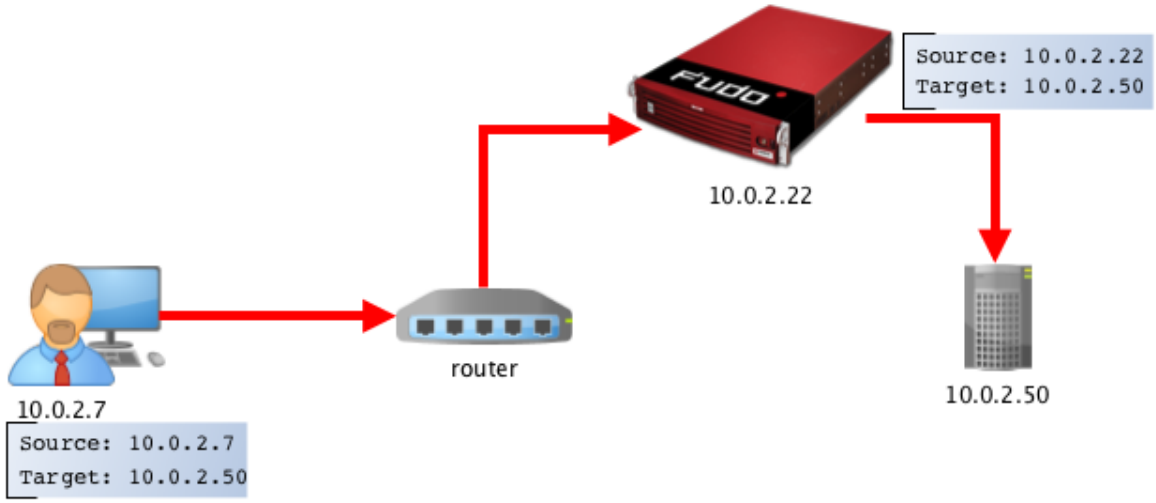
### Transparent

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



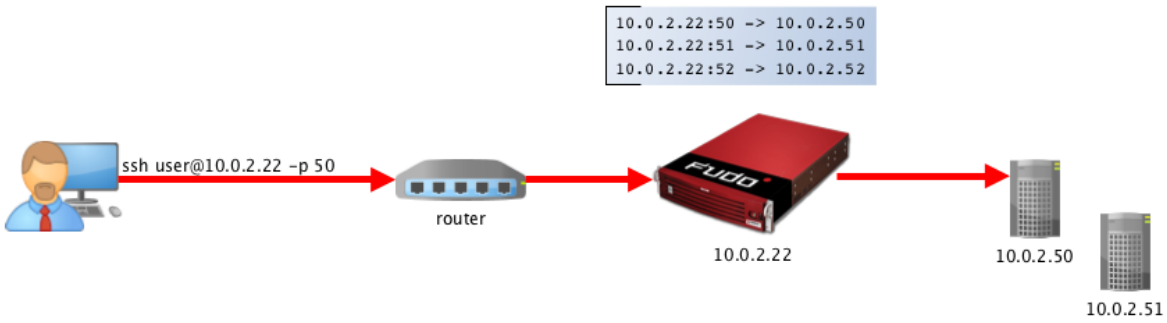

### Gateway

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




### Proxy

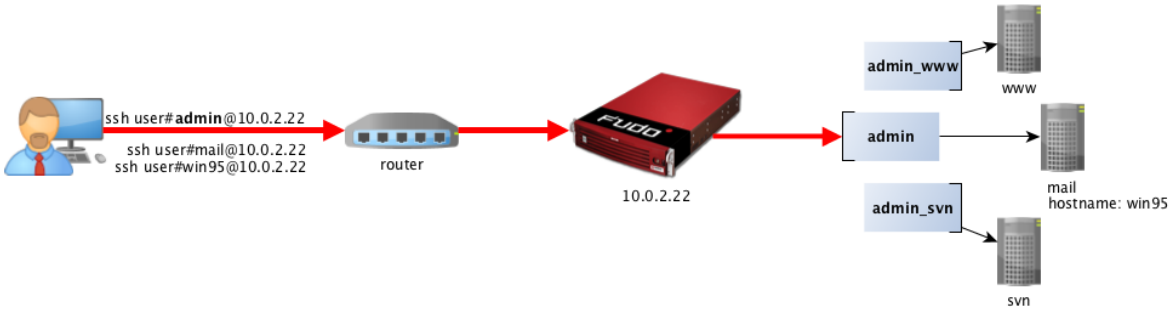
In proxy mode, administrator connects to destination server using combination of Wheel Fudo PAM IP address and unique port number assigned to given server. Uniqueness of this combination enables establishing connection with a particular resource.




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

### Bastion

In bastion mode, the account on the target host, or the host itself, is specified within the string identifying the user, e.g. `ssh john_smith#admin@10.0.2.22`. This enables facilitating access to a group of monitored servers through the same IP address and port number combination.




**Note:**

- The *bastion* mode is supported when connecting over SSH, RDP, VNC, Telnet, Telnet 3270, Telnet 5250, MS SQL and ICA protocols.
- In case the specified account is not found, Wheel Fudo PAM 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.
- The string specifying the target object must unambiguously identify an account or a 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*

## 2.10 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*.

**Note:** External authentication servers CERB, RADIUS, LDAP and Active Directory require configuration. For more information, refer to the *External authentication* topic.

### 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, Wheel Fudo PAM forwards login credentials to the target host, which verifies whether the user is authorized to access it. Verification status is returned to Wheel Fudo PAM, 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*

Wheel Fudo PAM can be configured so each connection to a monitored server will require approval from the administrator using the *Fudo Mobile* application or the administration interface.

- *Adding a mobile device*
- *Removing paired mobile device*
- *Proxy servers configuration*
- *Creating a safe*

- *Approving pending connections*
- *Declining pending connections*

**Related topics:**

- *System overview*
- *External authentication servers configuration*
- *Security measures*

## 2.11 Security measures

### 2.11.1 Data encryption

Data stored on Wheel Fudo PAM 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 Wheel Fudo PAM 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 Wheel Fudo PAM 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 Wheel Fudo PAM, which will allow Wheel Fudo PAM to boot up automatically in case of a power outage or system reboot after software update.

**Virtual machine distribution**

Wheel Fudo PAM'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.

### 2.11.2 Backups

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

### 2.11.3 Permissions

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

For more information on user roles refer to *Roles* topic.

### 2.11.4 Sandboxing

Wheel Fudo PAM takes advantage of CAPSICUM sandboxing mechanism, which separates each connection on Wheel Fudo PAM 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.

### 2.11.5 Reliability

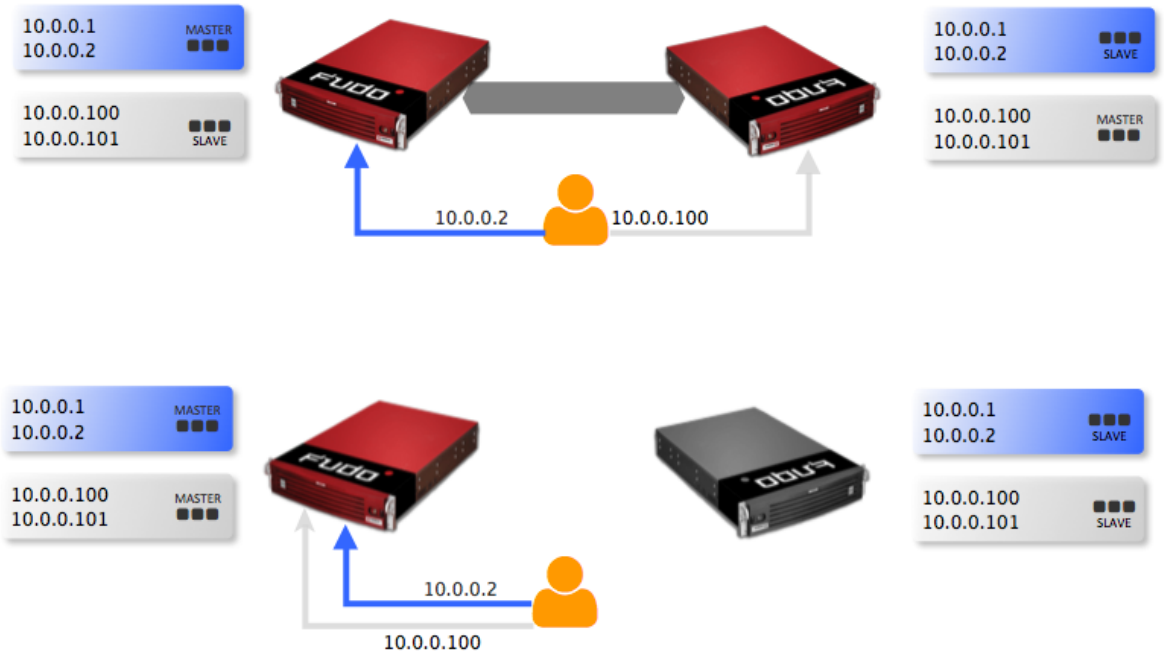
System hardware configuration is optimized to deliver high performance and high availability.

### 2.11.6 Cluster configuration

Wheel Fudo PAM 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:**

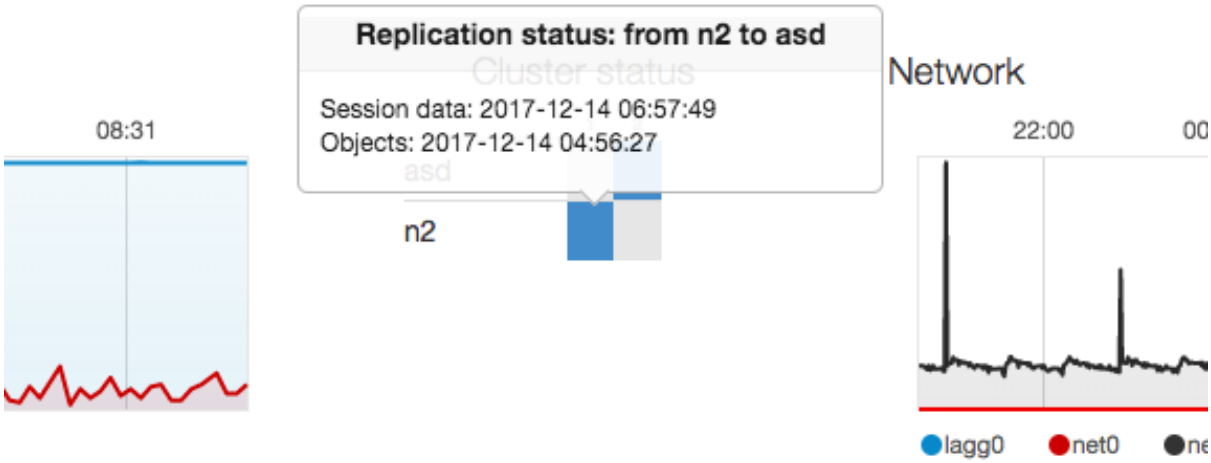
- *User authorization methods and modes*
- *System overview*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*
- *System initiation*

## 2.12 Dashboard

Fudo PAM dashboard page enables quick access to essential status information.

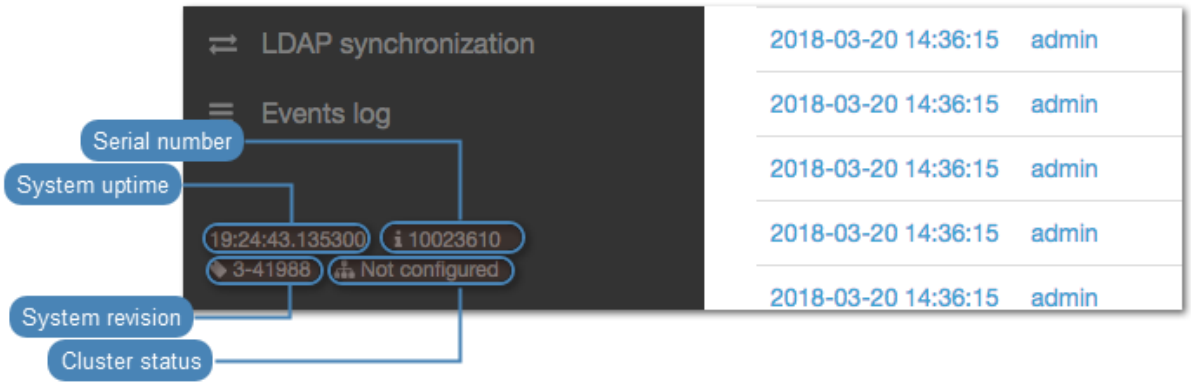
**Note:** Disk usage figures include space taken up by the filesystem's redundancy mechanism. The filesystem reserves a portion of available storage, which results in some of the storage space being reported as used on a newly initiated system.

**Note:** Place the cursor over status indicator for details on data replication between cluster nodes.




- *Session data* - the timestamp of the session data replicated from the given node.
- *Objects* - the timestamp of the replicated data model objects.

### System information




### Hard drives status information

| | |
|---|---|
| ● | 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*

ROZDZIAŁ 3

# System deployment

This topic describes Wheel Fudo PAM appliance and the system initiation procedure.

## 3.1 Requirements

**Administration panel**

System is managed in administration panel available through web browser. Recommended browsers are Google Chrome and Mozilla Firefox.

**Network requirements**

Correct operation requires:

- ability to establish connections to Wheel Fudo PAM on port 443, for administration purposes,
- ability for users to connect to Wheel Fudo PAM and for Wheel Fudo PAM to connect to target systems.

**Hardware requirements** (not applicable to virtual appliance distributions)

Wheel Fudo PAM 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.

**VNC software client requirements**

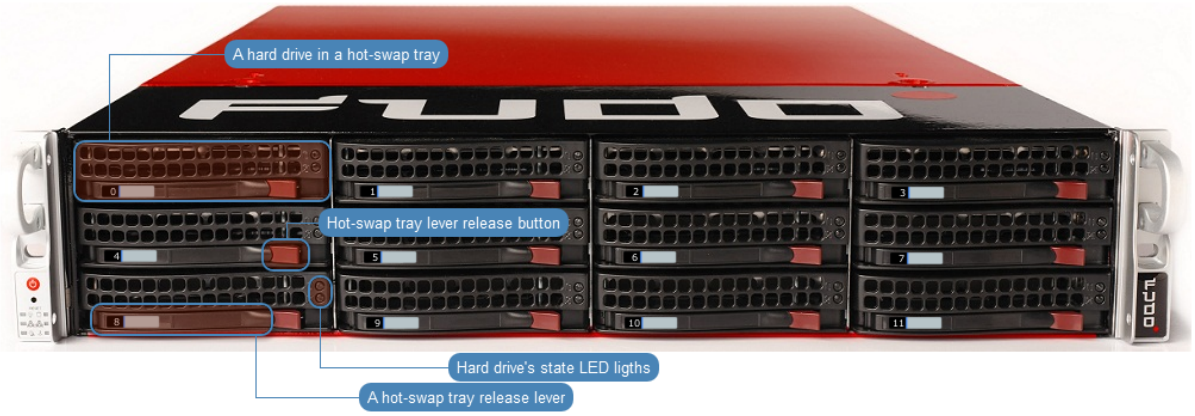
VNC connections require 24-bit (true color) mode.

## 3.2 Hardware overview

Fudo PAM is delivered in a 2U (F1001) or 3U (F3000) 19" rack server case.

**Wheel Fudo PAM F1001**

- Chassis: 19” 2U
- Dimensions: 89 mm (height), 437 mm (width), 647 mm (depth)
- PSU: 2x 500W
- Internal storage: 12x 2TB




### Wheel Fudo PAM F3001

- Chassis: 19” 3U
- Dimensions: 132 mm (height), 437 mm (width), 647 mm (depth)
- PSU: 2x 920W
- Internal storage: 16x 6TB
- External storage controller: 2x Qlogic HBA FC QLE2560 8Gb
- Additional network interfaces: 2x Intel I350AM4 4x RJ45 1GbE

**Related topics:**

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

## 3.3 System initiation

### Appliance

Wheel Fudo PAM is delivered with two uninitiated USB flash drives. During initial boot up, Wheel Fudo PAM 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 Wheel Fudo PAM.

---

**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:**

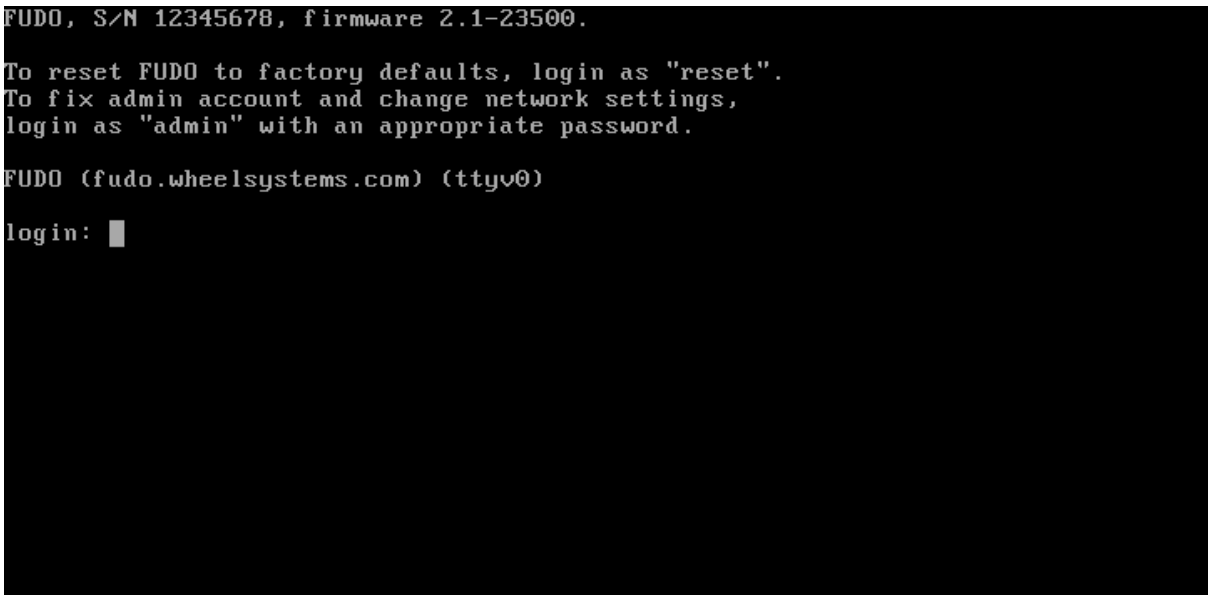
- One of the USB flash drives containing encryption key must be disconnected and placed in a secure location, accessible only to authorized personnel.
- If the USB flash drives with encryption keys are lost, device will not be able to boot up and stored sessions will not be accessible. Manufacturer does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

**Note:**

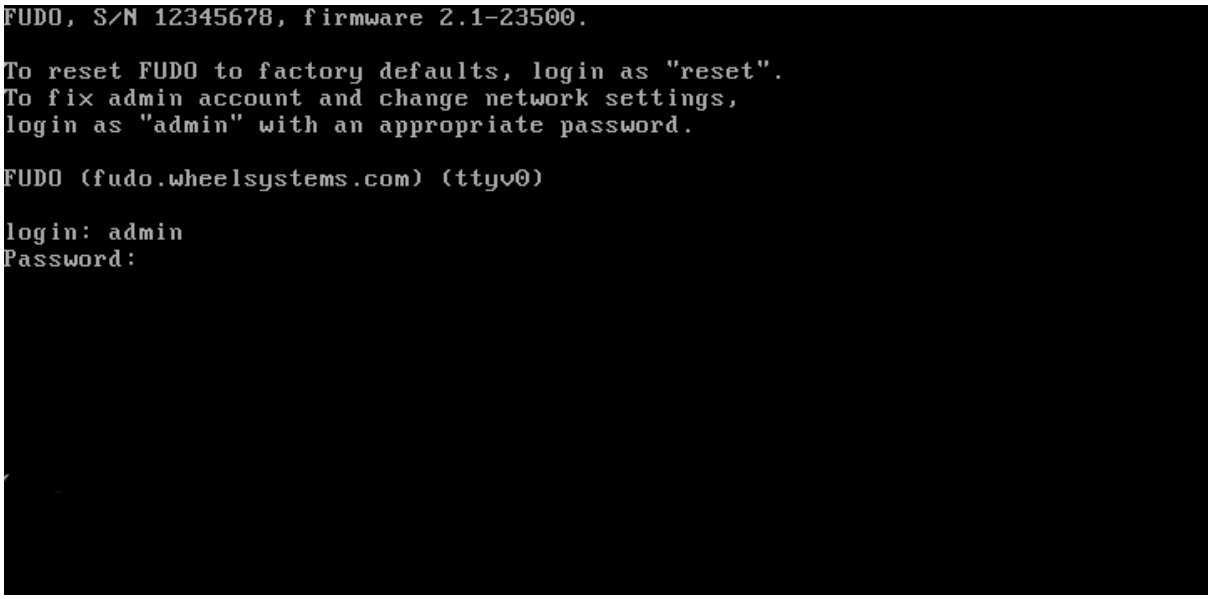
- In daily operation, one encryption key is required to start the system after which it can be disconnected.
- It is advised to make a backup copy of the encryption key.

*Setting IP address using system console*

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




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




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

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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

Choose an option (0):
```

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

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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

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

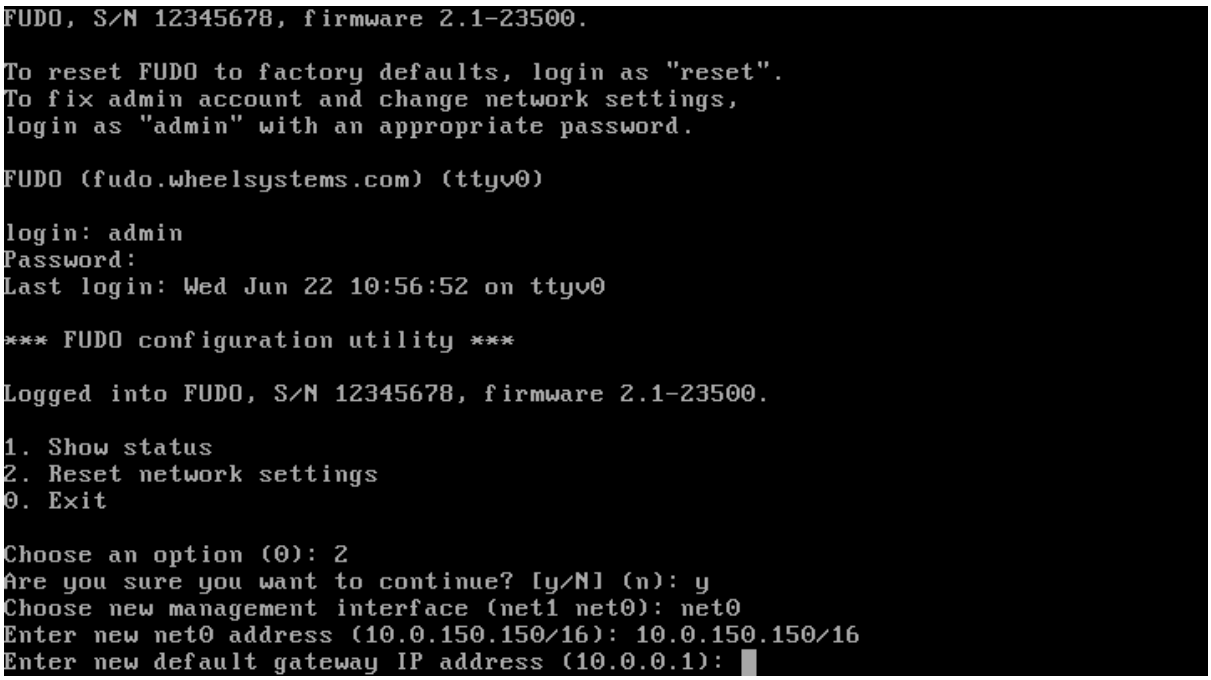
6. Enter the name of the new management interface (Wheel Fudo PAM web interface is accessible through the management interface).

```
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*.




**Related topics:**

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

ROZDZIAŁ 4

# Quick start

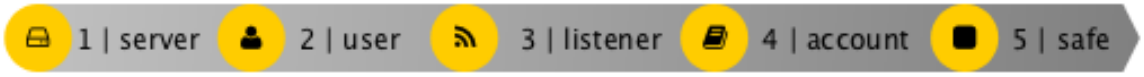
## 4.1 SSH

This chapter contains an example of a basic Wheel Fudo PAM 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 Wheel Fudo PAM using an individual login and password combination (`john_smith`/`john`). When establishing the connection with the remote server, Wheel Fudo PAM substitutes the login and the password with the previously defined values: `root`/`password` (authentication modes are described in the *User authentication modes* section).

### 4.1.1 Prerequisites

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

### 4.1.2 Configuration



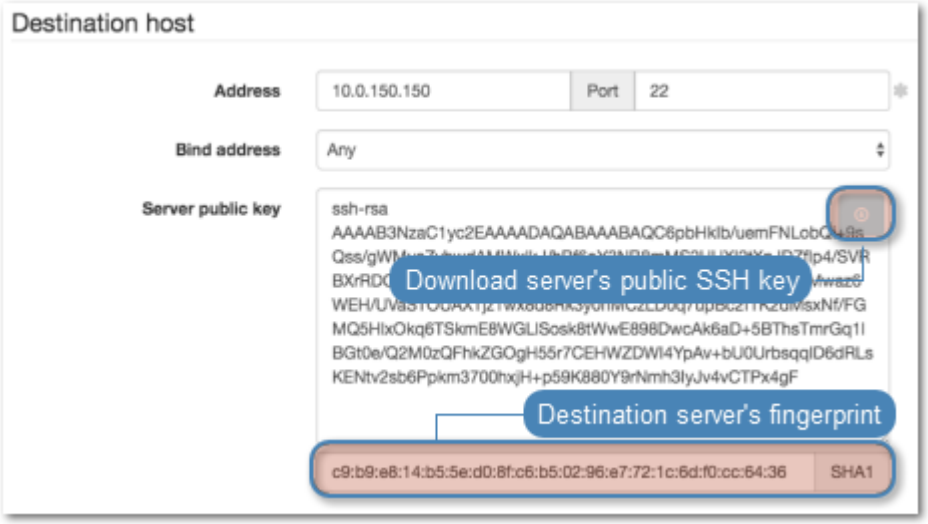

**Adding a server**

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*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `ssh_server` |
| Blocked | ✗ |
| Protocol | `SSH` |
| Description | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Destination host* | |
| Address | `10.0.150.150` |
| Port | 22 |

4. Download or enter target server's public key.




5. Click *Save*.

### 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* | |
| Login | `john_smith` |
| Fudo domain | ✗ |
| Blocked | ✗ |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | ✗ |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | ✗ |
| Phone | ✗ |
| AD Domain | ✗ |
| LDAP Base | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Authentication* | |
| Authentication failures | ✗ |
| Enforce static password complexity | ✗ |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

4. Click *Save*.

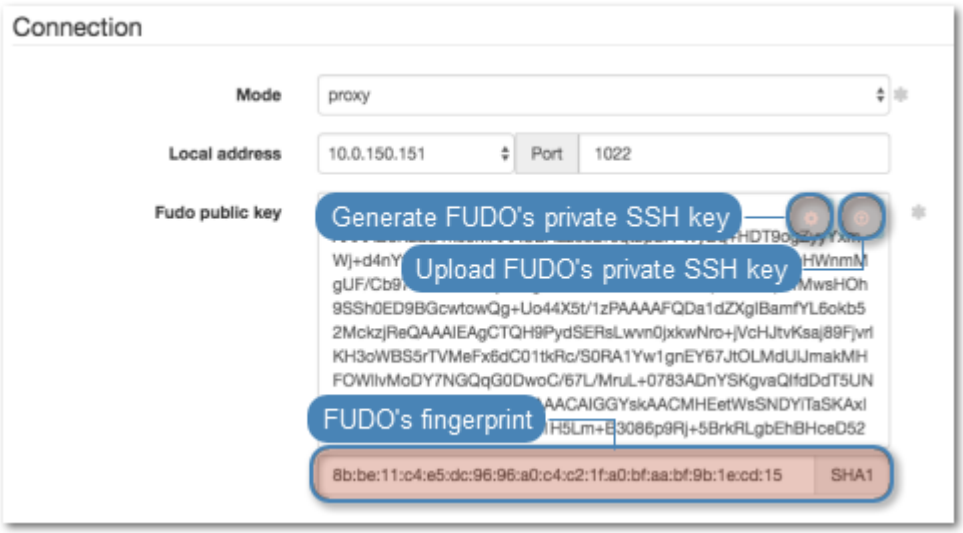
### Adding a listener

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` |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Connection* | |
| Mode | `proxy` |
| Local address | `10.0.150.151` |
| Port | `1022` |

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` |
| Account type | `regular` |
| Session recording | `complete` |
| OCR sessions | |
| 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` |
| Replace secret | |
| | |
| *Password changer* | |
| Password changer | `None` |
| Privileged user | |
| Privileged user password | |

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:

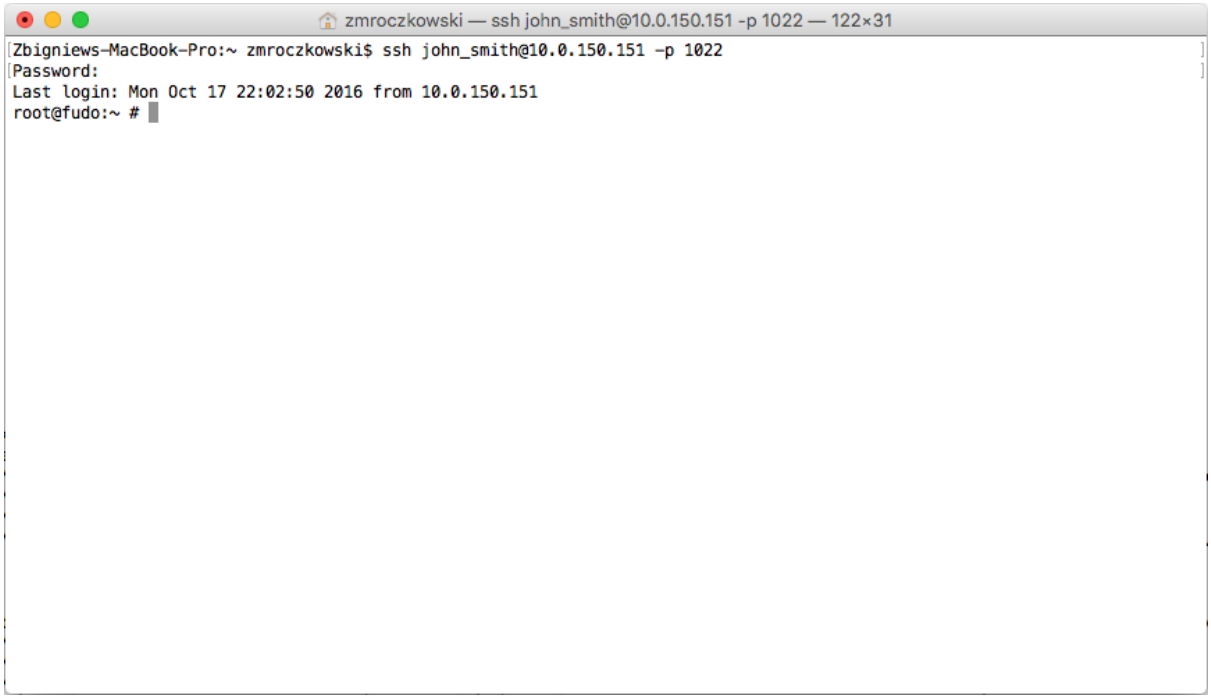
| Parameter | Value |
|---|---|
| *General* | |
| Name | `ssh_safe` |
| Notifications | ✗ |
| Ask for login reason | ✗ |
| Policies | ✗ |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | ✗ |
| SSH | ✓ |
| VNC | ✗ |
| | |
| *Accounts* | |
| `admin_ssh_server` | `ssh_listener` |

4. Click *Save*.

### 4.1.3 Establishing connection

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

Example:

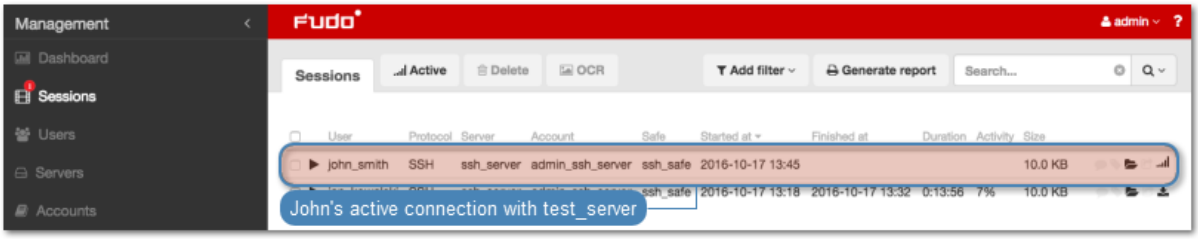



**Note:** Note that the *fingerprint* displayed when connecting to the target host for the first time is the same as was generated during server configuration.

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

### 4.1.4 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 Wheel Fudo PAM administration panel.
3. Select *Management* > *Sessions*.
4. Find *John Smith's* 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*

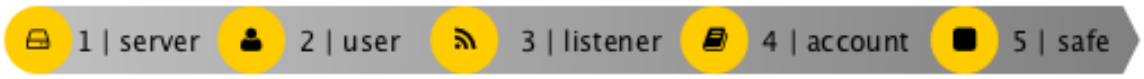
## 4.2 SSH in bastion mode

This chapter contains an example of a basic Wheel Fudo PAM 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 Wheel Fudo PAM using an individual login and password combination (`john_smith`/`john`). The user specifies account on a target server in the login string (`john_smith#admin_ssh_server`) 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).

### 4.2.1 Prerequisites

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

### 4.2.2 Configuration



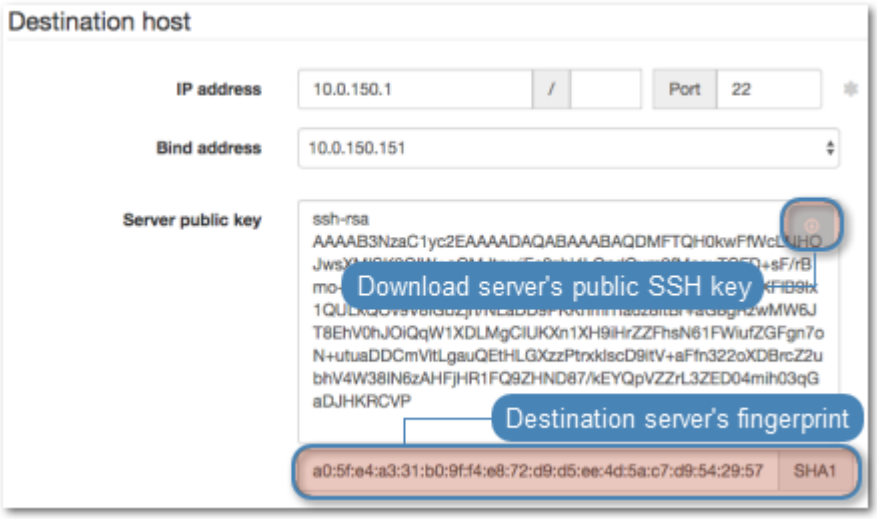

#### Adding a server

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*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `ssh_server` |
| Blocked | ✗ |
| Protocol | `SSH` |
| Description | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Destination host* | |
| Address | `10.0.150.1` |
| Port | `22` |

4. Download or enter target server's public key.




5. Click *Save*.

### 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* | |
| Login | `john_smith` |
| Fudo domain | |
| Blocked | |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | |
| Phone | |
| AD Domain | |
| LDAP Base | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Authentication* | |
| Authentication failures | |
| Enforce static password complexity | |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

4. Click *Save*.

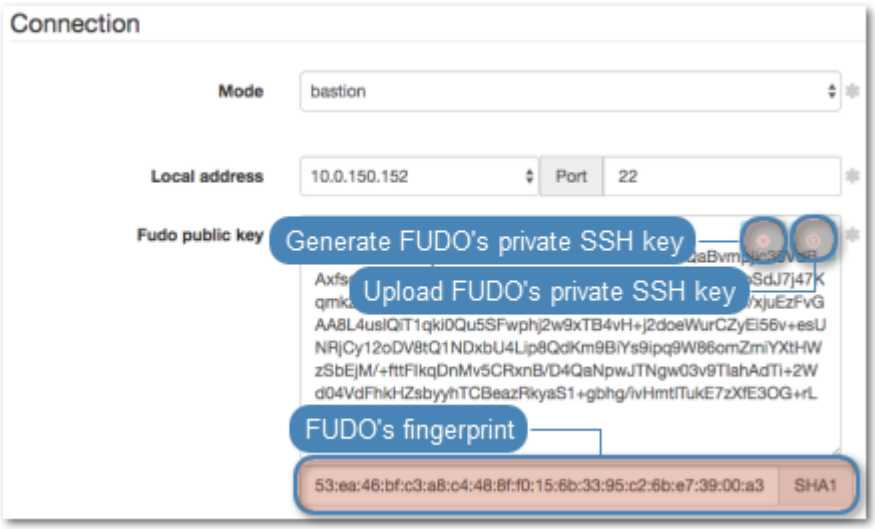
### Adding a listener

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` |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Connection* | |
| Mode | `bastion` |
| Local address | `10.0.150.151` |
| Port | `22` |

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` |
| Account type | `regular` |
| Session recording | `complete` |
| OCR sessions | |
| 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` |
| Replace secret | |
| | |
| *Password changer* | |
| Password changer | `None` |
| Privileged user | |
| Privileged user password | |

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:

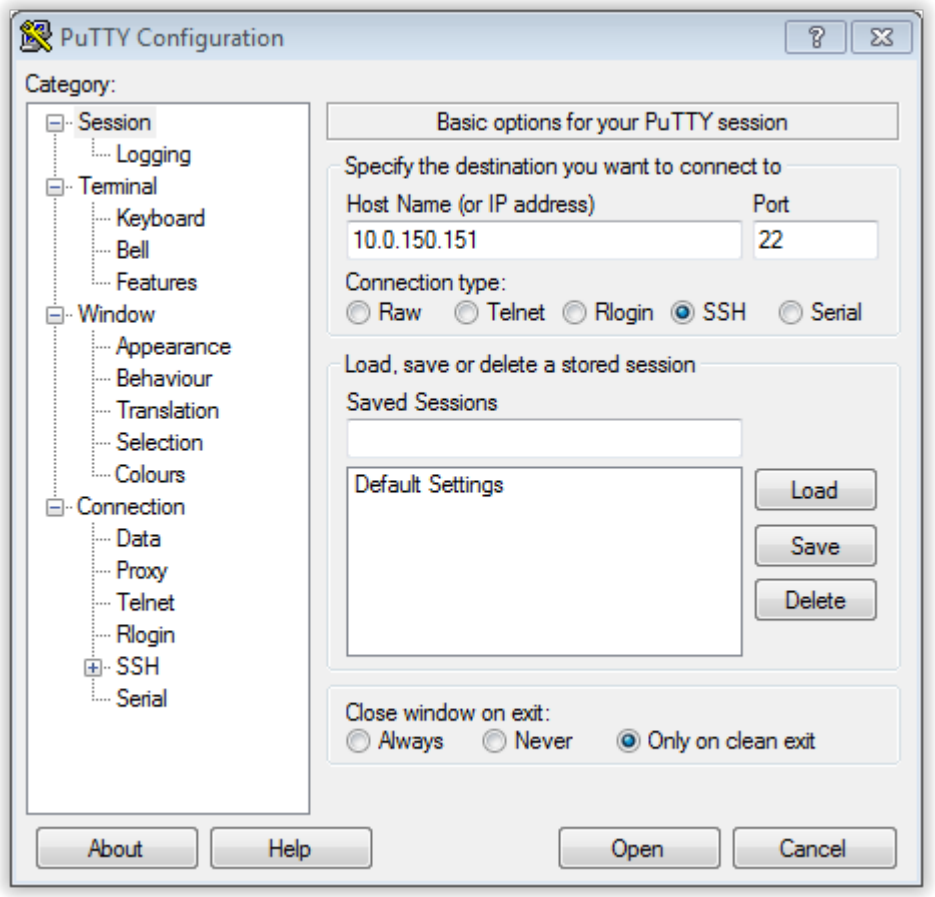
| Parameter | Value |
|---|---|
| *General* | |
| Name | `ssh_safe` |
| Notifications | ✗ |
| Ask for login reason | ✗ |
| Policies | ✗ |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | ✗ |
| SSH | ✓ |
| VNC | ✗ |
| | |
| *Accounts* | |
| `admin_ssh_server` | `ssh_listener` |

4. Click *Save*.

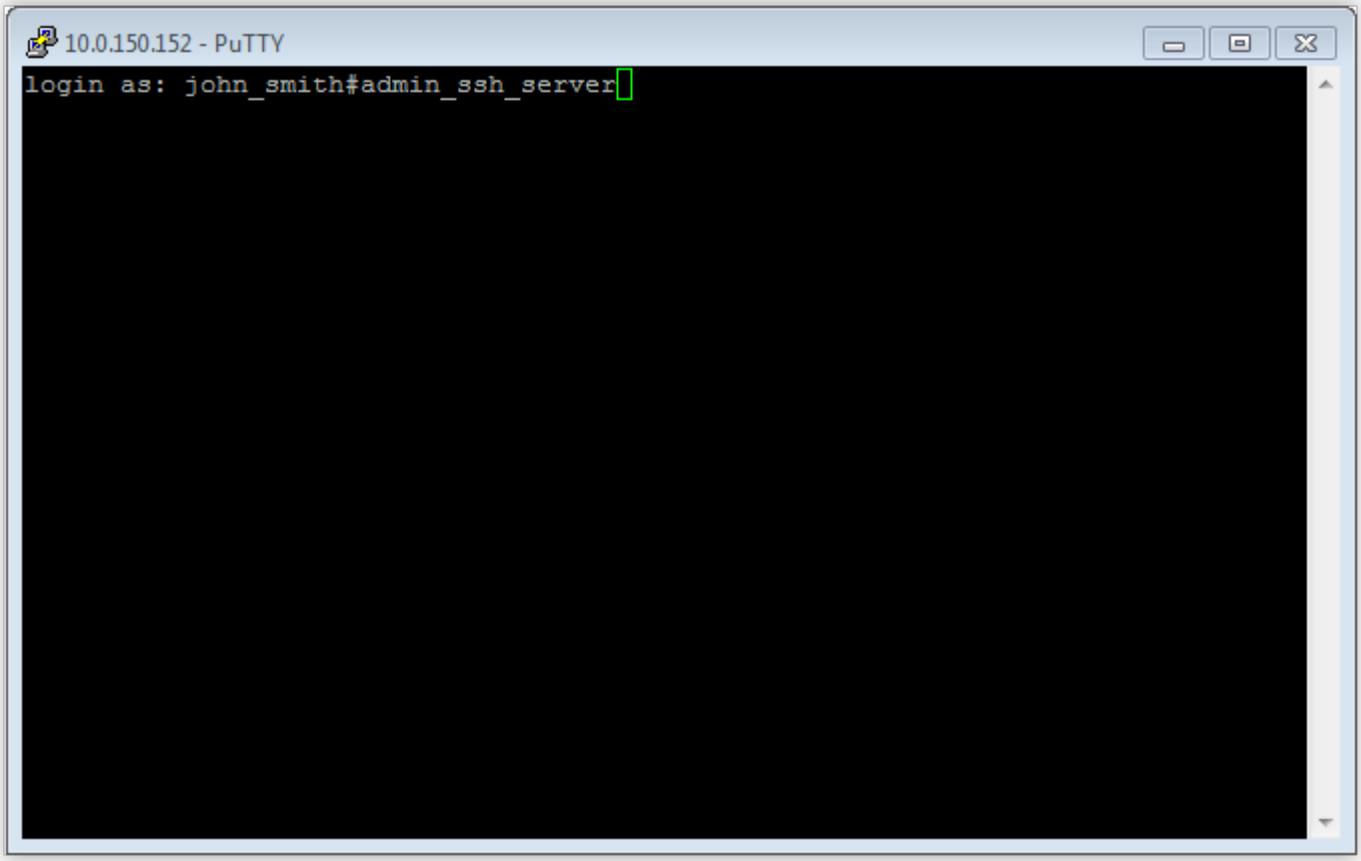
### 4.2.3 Establishing connection

**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 the account name on the target host.




**Note:** Alternatively, instead of the account name, you can specify the server by its name `john_smit#ssh_server`.

6. Enter password.

**Command line interface**

Launch terminal and run ssh command:

```
ssh john_smith#admin_ssh_server@10.0.150.151
```

**Note:** Due to special interpretation of the \ character by different system shells (e.g. bash), user login and domain combination require specific formatting:

- "domain\user"#bsd01@10.0.60.138
- 'domain\user'#bsd01@10.0.60.138
- domain\user#bsd01@10.0.60.138

### 4.2.4 Viewing user session

1. Open a web browser and go to the `10.0.150.150` web address.
2. Enter the login and password to login to the Wheel Fudo PAM 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*

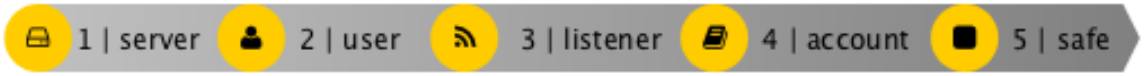
## 4.3 RDP

This chapter contains an example of a basic Wheel Fudo PAM 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 Wheel Fudo PAM using an individual login and password combination (`john_smith`/`john`). When establishing the connection with the remote server, Wheel Fudo PAM 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).

### 4.3.1 Prerequisites

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

### 4.3.2 Configuration




#### Adding a server

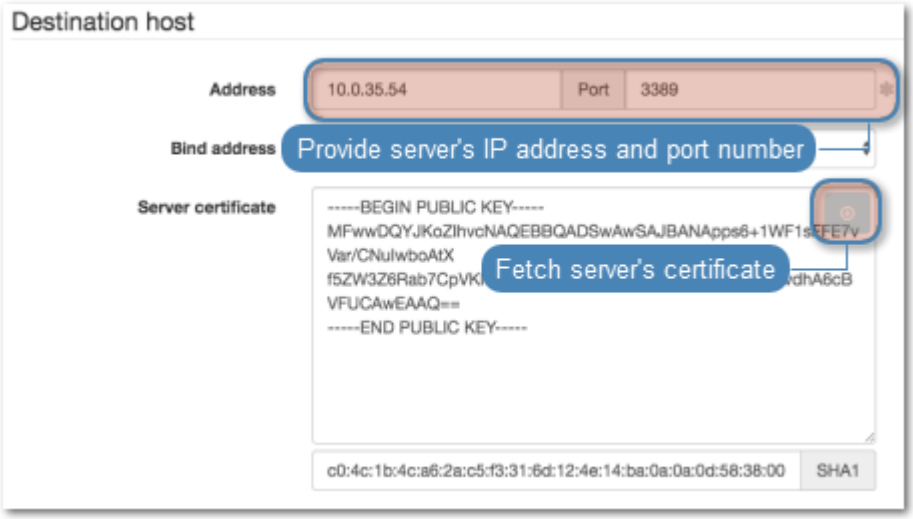
Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

1. Select *Management* > *Servers*.

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

| Parameter | Value |
|---|---|
| Name | `rdp_server` |
| Blocked | ✗ |
| Protocol | `RDP` |
| Description | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Destination host* | |
| Address | `10.0.35.54` |
| Port | `3389` |
| Bind address | `10.0.150.151` |

4. Download or enter target server's public key.




5. Click *Save*.

### 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* | |
| Login | `john_smith` |
| Fudo domain | |
| Blocked | |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | |
| Phone | |
| AD Domain | |
| LDAP Base | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Authentication* | |
| Authentication failures | |
| Enforce static password complexity | |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

4. Click *Save*.

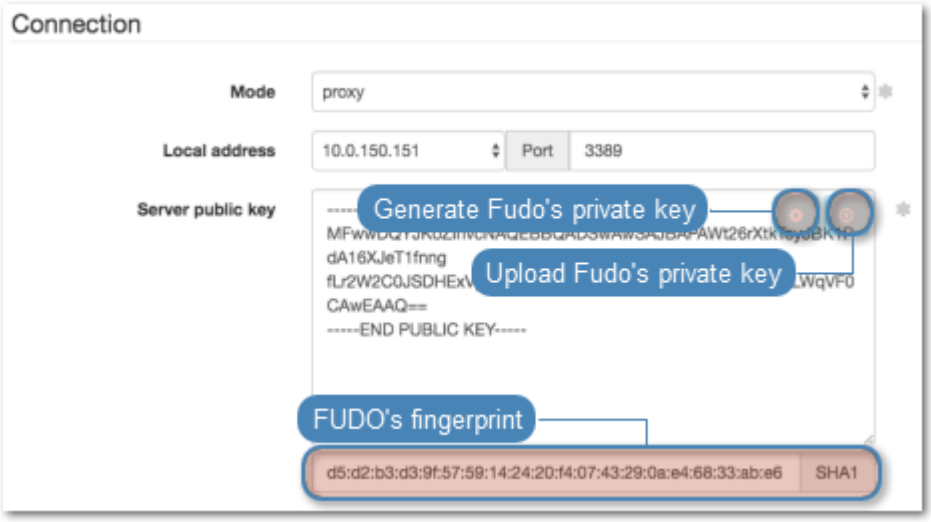
### Adding a listener

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` |

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` |
| 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` |
| | |
| *Password changer* | |
| Password changer | `None` |
| Privileged user | ✗ |
| Privileged user password | ✗ |

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.

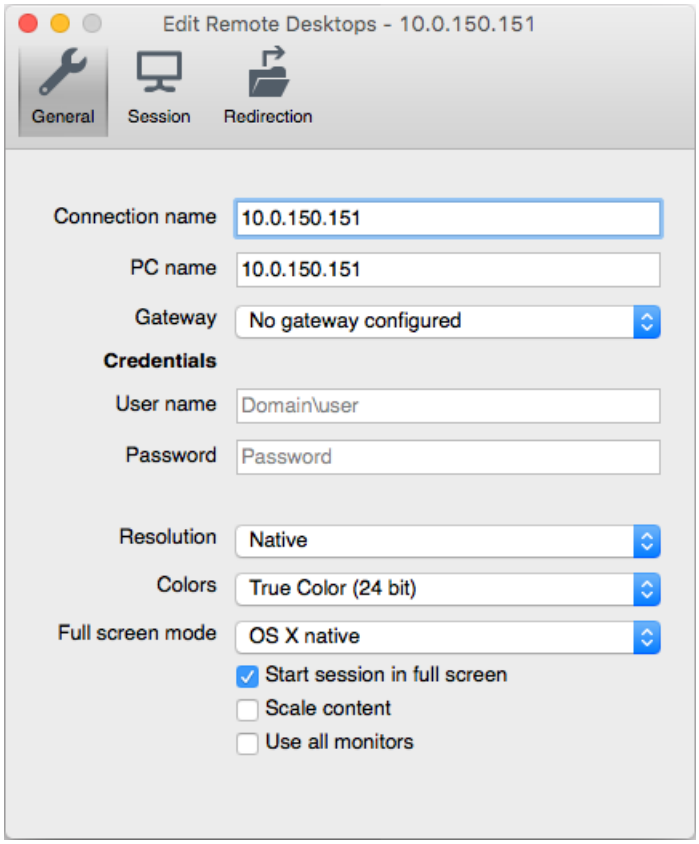
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `rdp_safe` |
| Blocked | |
| Login reason | |
| Notifications | |
| Policies | |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | |
| SSH | |
| VNC | |
| | |
| *Accounts* | |
| `admin_rdp_server` | `rdp_listener` |

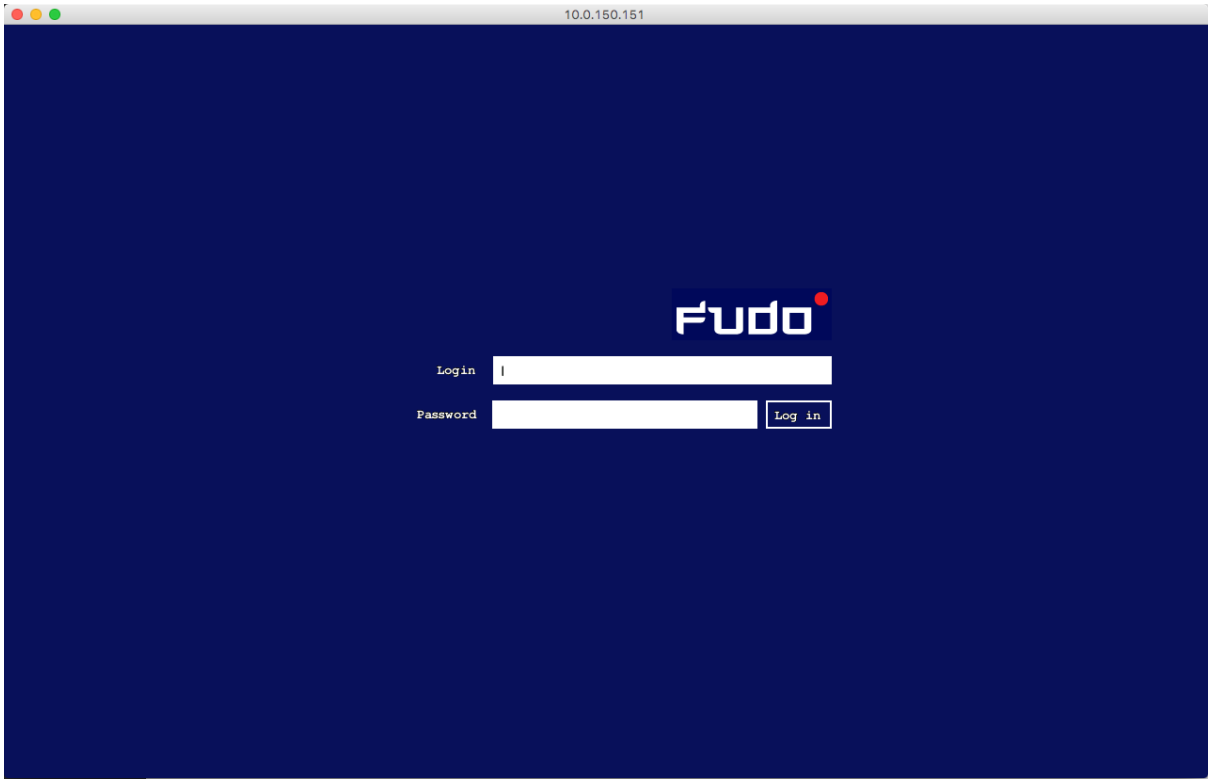
4. Click *Save*.

### 4.3.3 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.

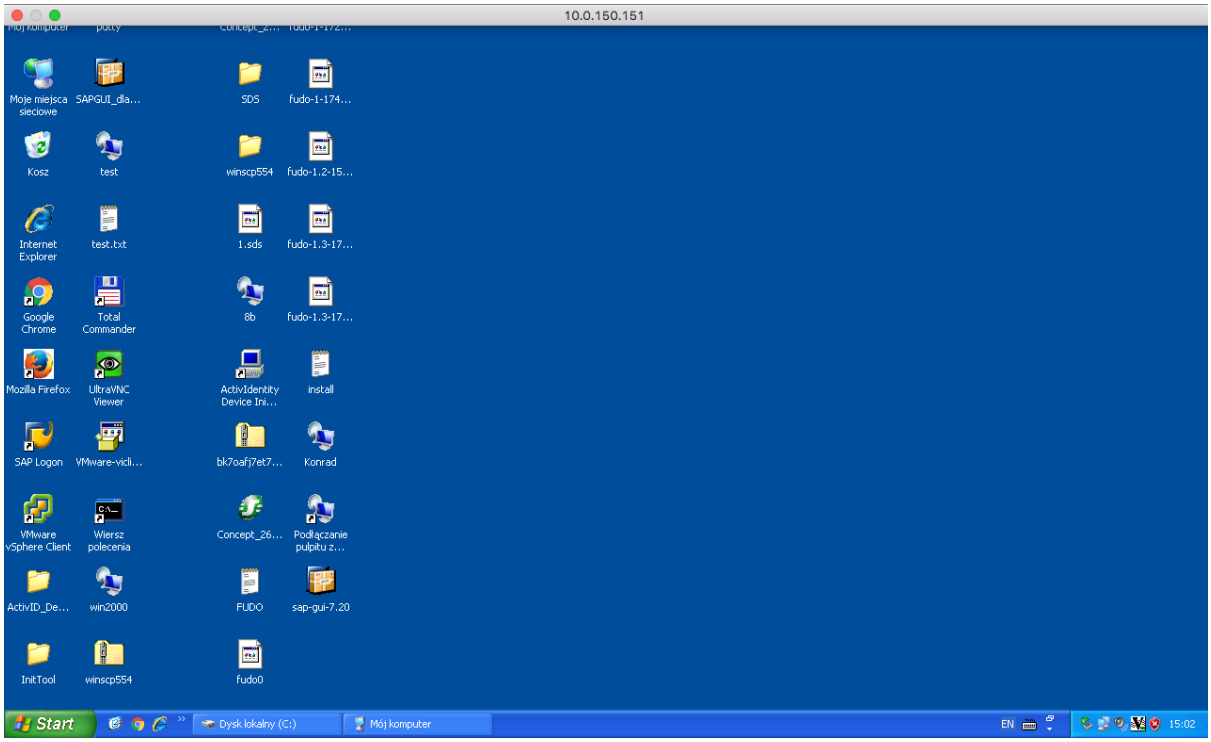



3. Enter user login and password and press the [Enter] keyboard key.




**Note:** Wheel Fudo PAM 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.




### 4.3.4 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 Wheel Fudo PAM 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*

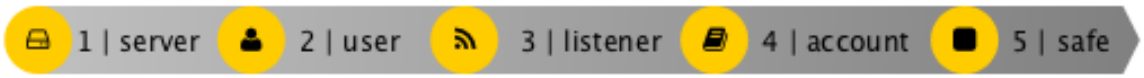
## 4.4 RDP in bastion mode

This chapter contains an example of a basic Wheel Fudo PAM 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 privileged account in the username string. Bastion mode enables facilitating privileged accounts monitoring while preserving default protocols port numbers.

### 4.4.1 Prerequisites

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

### 4.4.2 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*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| Name | `rdp_server` |
| Blocked | |
| Protocol | `RDP` |
| Security | `Standard RDP Security` |
| Description | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Destination host* | |
| IP address | `10.0.234.6/32` |
| Port | `3389` |
| Bind address | `10.0.150.151` |

4. Download or enter target server's public key.
5. Click *Save*.

**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* | |
| Login | `john_smith` |
| Fudo domain | |
| Blocked | |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | |
| Phone | |
| AD Domain | |
| LDAP Base | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Authentication* | |
| Authentication failures | |
| Enforce static password complexity | |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

4. Click *Save*.

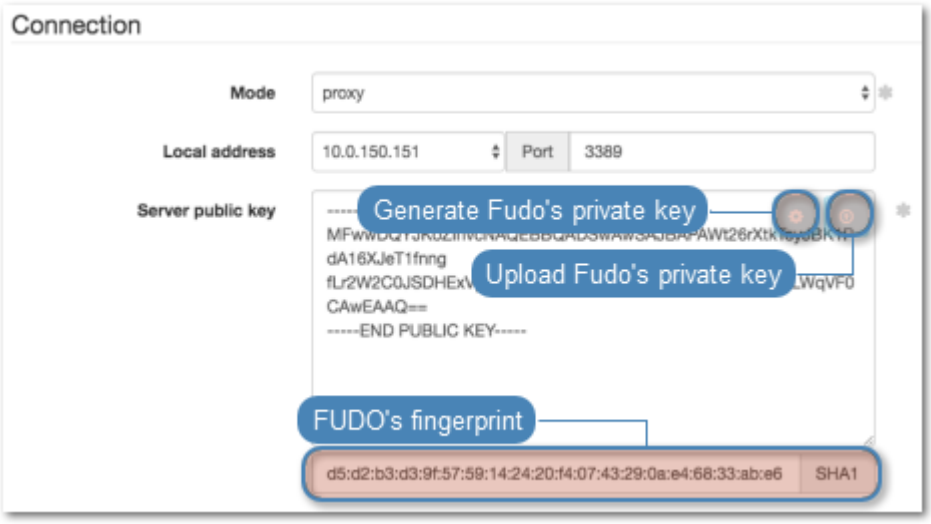
### Adding a listener

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 | ✗ |

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` |
| 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` |
| | |
| *Password changer* | |
| Password changer | `None` |
| Privileged user | ✗ |
| Privileged user password | ✗ |

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.

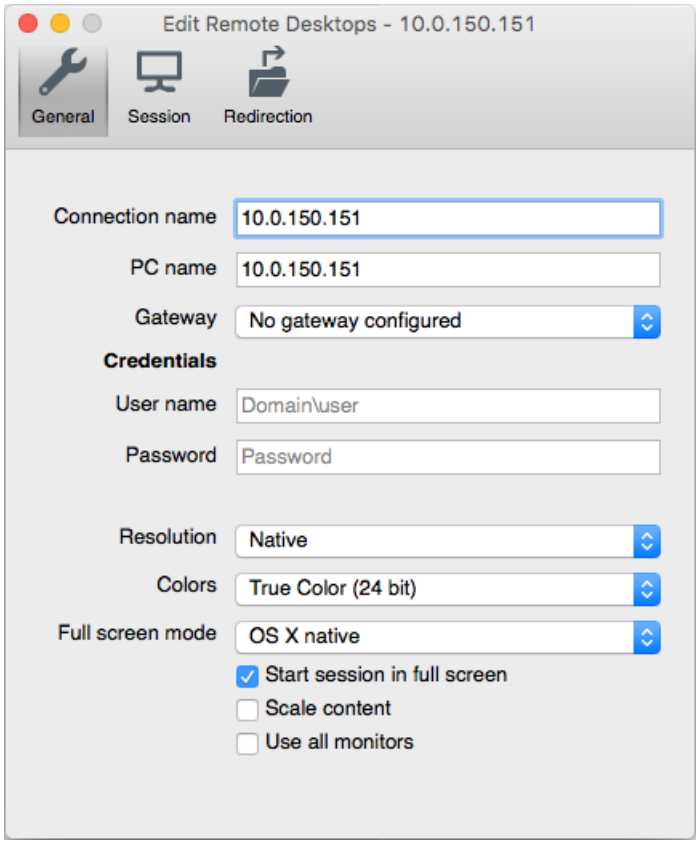
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `rdp_safe` |
| Blocked | ✗ |
| Login reason | ✗ |
| Notifications | ✗ |
| Policies | ✗ |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | ✓ |
| SSH | ✗ |
| VNC | ✗ |
| | |
| *Accounts* | |
| `admin_rdp_server` | `rdp_listener_bastion` |

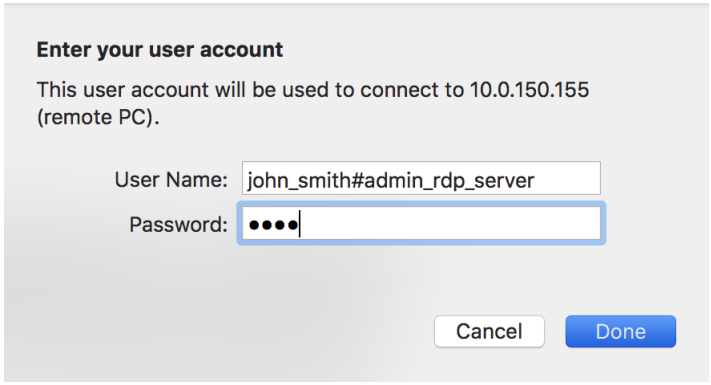
4. Click *Save*.

### 4.4.3 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.

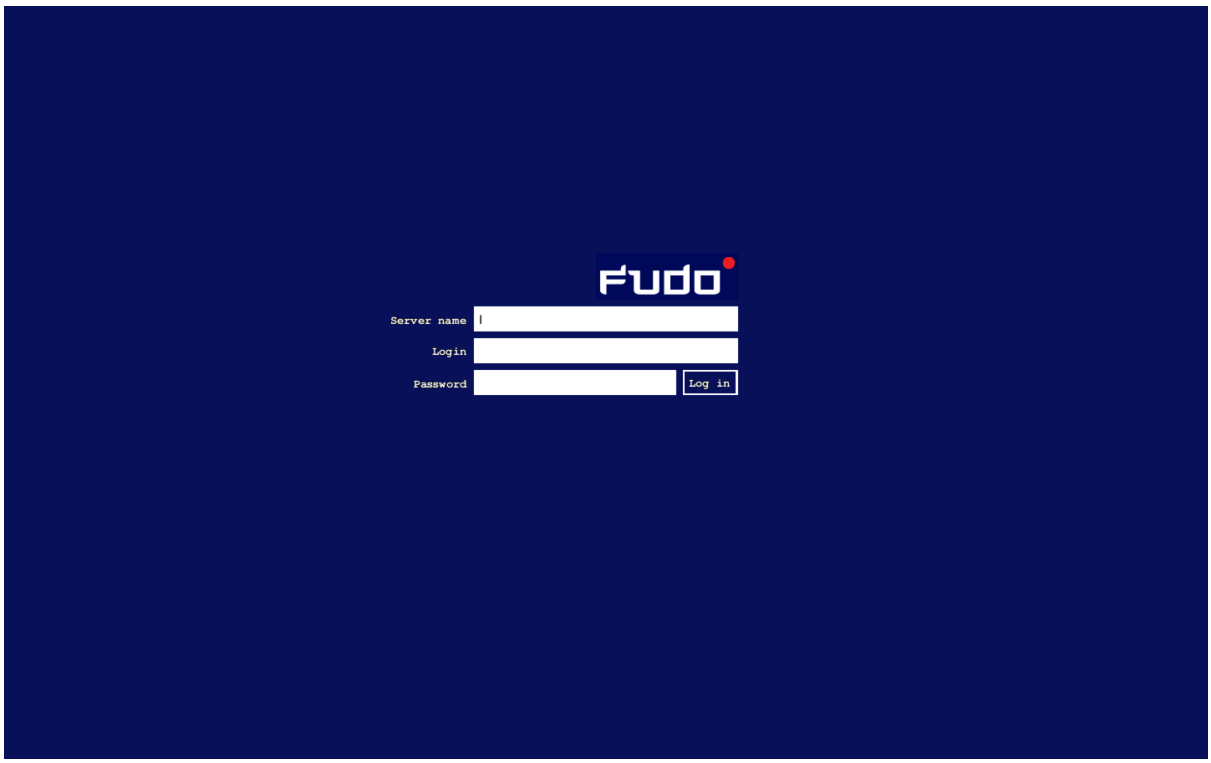



3. Enter user login along with the account name specified in the username string (`john_smith#admin_rdp_server`) and password.

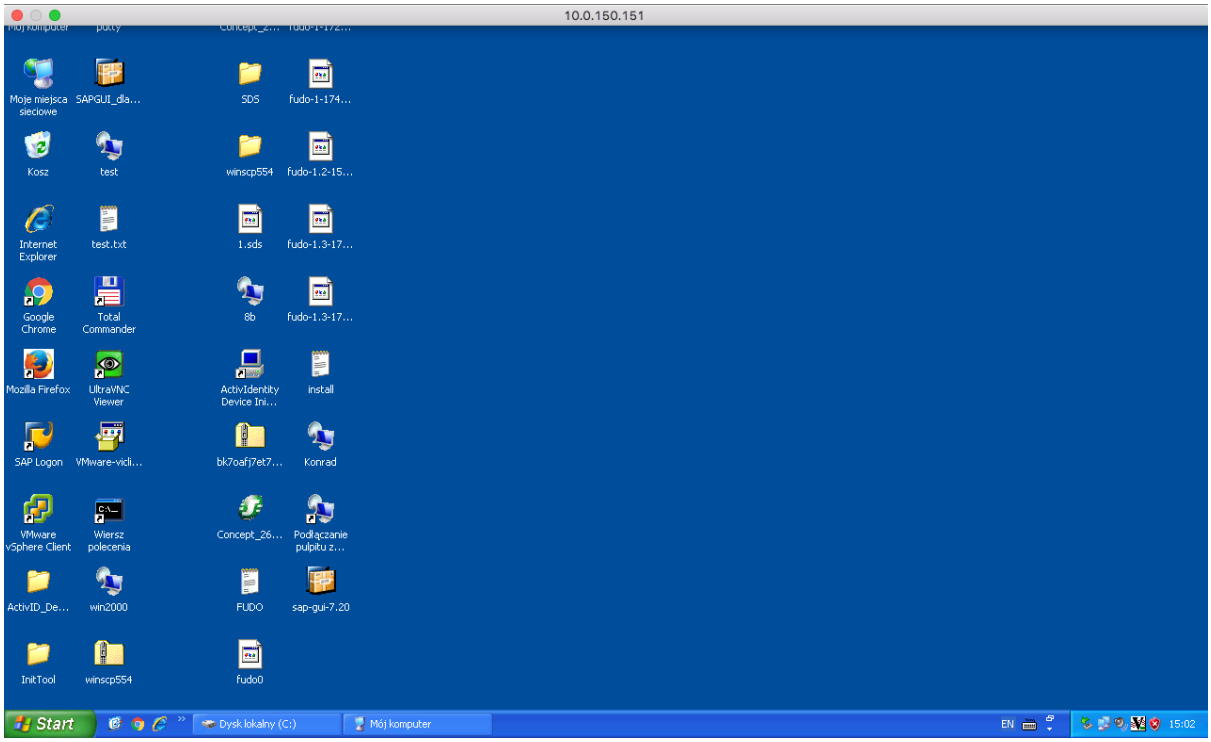



**Note:**

- In case you do not specify login credentials, Fudo will display the internal login screen to enter the account name along with the username and password.



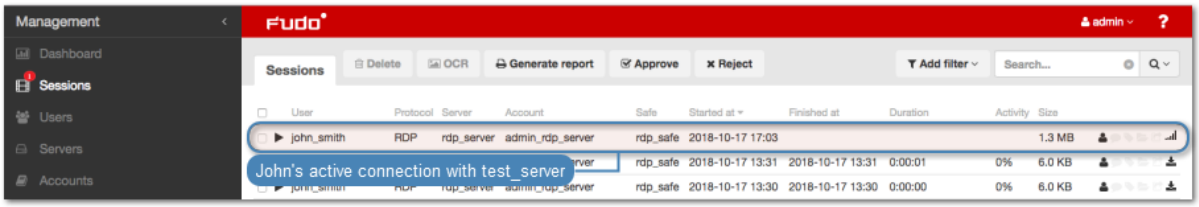

- Wheel Fudo PAM enables using a custom logo on the login screen for RDP and VNC connections. For more information refer to the *Resources* topic.




### 4.4.4 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 Wheel Fudo PAM 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*

## 4.5 Telnet

This chapter contains an example of a basic Wheel Fudo PAM 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. Wheel Fudo PAM authenticates the user against the information stored in the local database, establishes connection with the remote server and starts recording.

---

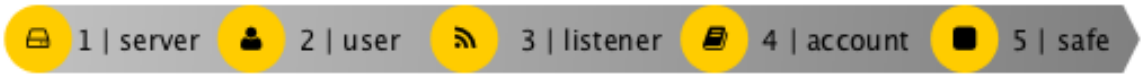
**Note:** Telnet connections do not support login credentials forwarding and login credentials substitution. When connecting to target host over telnet protocol, users are asked to provide their login credentials twice. First time to authenticate against Wheel Fudo PAM and then again, to connect to the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

---

### 4.5.1 Prerequisites

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

### 4.5.2 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 the Add button.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `telnet_server` |
| Blocked | ✗ |
| Protocol | `Telnet` |
| Enable SSLv2 support | ✗ |
| Enable SSLv3 support | ✗ |
| Description | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Destination host* | |
| Address | `10.0.35.137` |
| Port | `23` |

4. Click *Save*.

#### 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* | |
| Login | `john_smith` |
| Fudo domain | |
| Blocked | |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | |
| Phone | |
| AD Domain | |
| LDAP Base | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Authentication* | |
| Authentication failures | |
| Enforce static password complexity | |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

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` |
| Enable SSLv2 support | |
| Enable SSLv3 support | |

| *Permissions* | |
|---|---|
| Granted users | |

| *Connection* | |
|---|---|
| Mode | `proxy` |
| Local address | `10.0.150.151` |
| Port | `23` |

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` |
| OCR sessions | |
| Delete session data after | `61` days |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Server* | |
| Server | `telnet_server` |
| | |
| *Credentials* | |
| Replace secret with | `with password` |
| Password | |
| Repeat password | |

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 | ✗ |
| Login reason | ✗ |
| Notifications | ✗ |
| Policies | ✗ |
| | |
| *Protocol functionality* | |
| RDP | ✗ |
| SSH | ✗ |
| VNC | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Objects relations* | |
| Users | `john_smith` |
| Accounts | `admin_telnet_server` |
| Listeners | `telnet_listener` |

4. Click *Save*.

### 4.5.3 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 Wheel Fudo PAM:

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

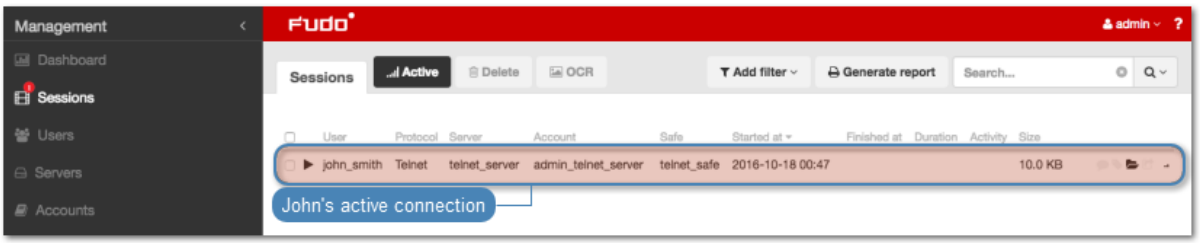
4. Provide user authentication information defined on the target host:

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

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

### 4.5.4 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 Wheel Fudo PAM 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*

## 4.6 Telnet 5250

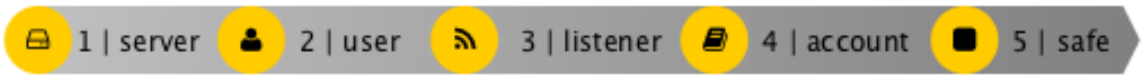
This chapter contains an example of a basic Wheel Fudo PAM configuration, to monitor Telnet 5250 connections to a remote server. In this scenario, the user connects to the remote server using Telnet client and logs in using individual login and password. Wheel Fudo PAM authenticates the user against 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 Wheel Fudo PAM and then again, to connect to the target host.

### 4.6.1 Prerequisites

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

### 4.6.2 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 the Add button.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `telnet_server` |
| Blocked | ✗ |
| Protocol | `Telnet 5250` |
| Enable SSLv2 support | ✗ |
| Enable SSLv3 support | ✗ |
| Description | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Destination host* | |
| Address | `10.0.35.137` |
| Port | `23` |

4. Click *Save*.

#### 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* | |
| Login | `john_smith` |
| Fudo domain | ✗ |
| Blocked | ✗ |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | ✗ |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | ✗ |
| Phone | ✗ |
| AD Domain | ✗ |
| LDAP Base | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Authentication* | |
| Authentication failures | ✗ |
| Enforce static password complexity | ✗ |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

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` |
| Enable SSLv2 support | |
| Enable SSLv3 support | |

| *Permissions* | |
|---|---|
| Granted users | |

| *Connection* | |
|---|---|
| Mode | `proxy` |
| Local address | `10.0.150.151` |
| Port | `23` |

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` |
| OCR sessions | |
| Delete session data after | `61` days |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Server* | |
| Server | `telnet_server` |
| | |
| *Credentials* | |
| Replace secret with | `with password` |
| Password | |
| Repeat password | |

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 | ✗ |
| Login reason | ✗ |
| Notifications | ✗ |
| Policies | ✗ |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | ✗ |
| SSH | ✗ |
| VNC | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Accounts* | |
| `admin_telnet_server` | `telnet_listener` |

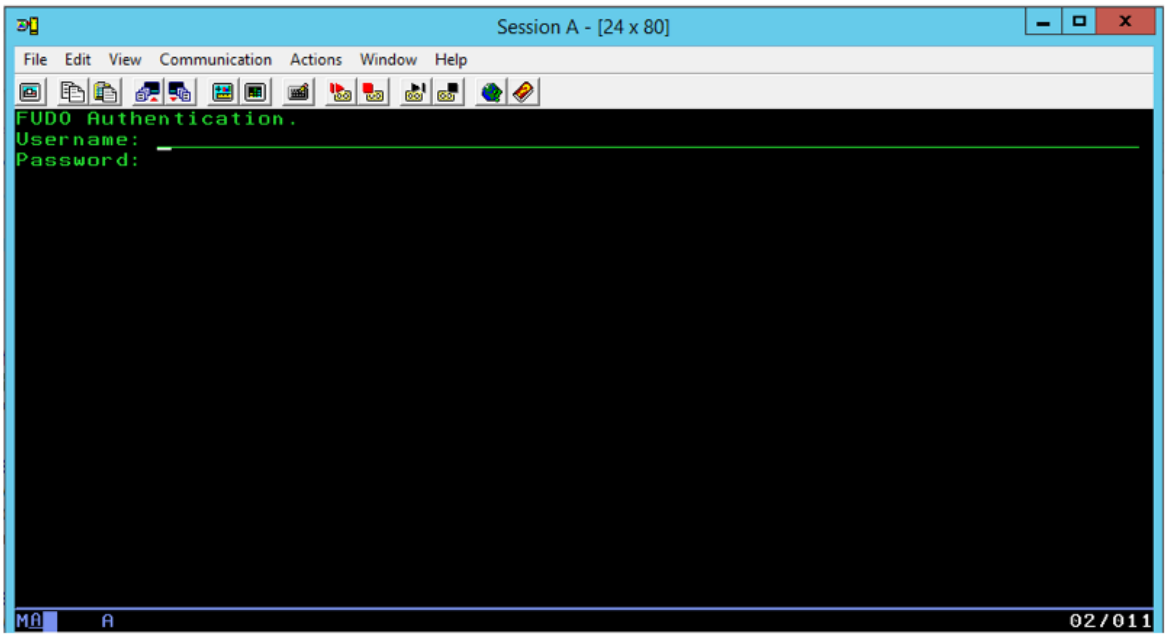
4. Click *Save*.

### 4.6.3 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 '^]'.
```

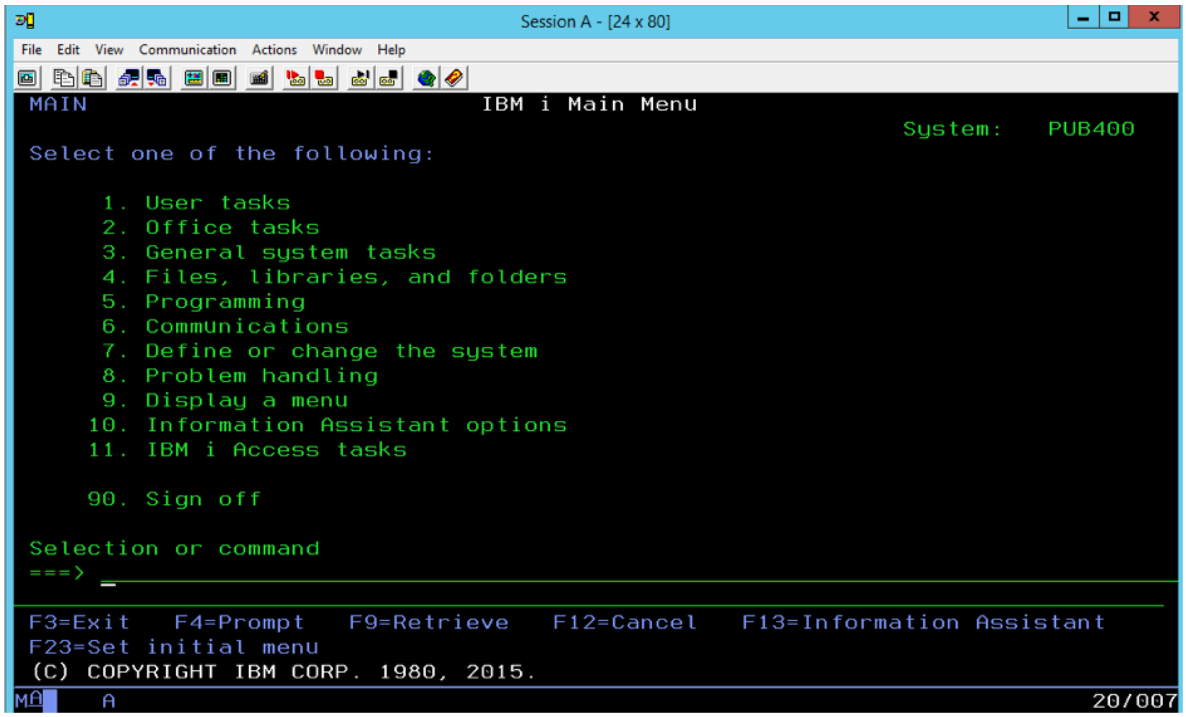
3. Provide user authentication information defined on Wheel Fudo PAM:




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

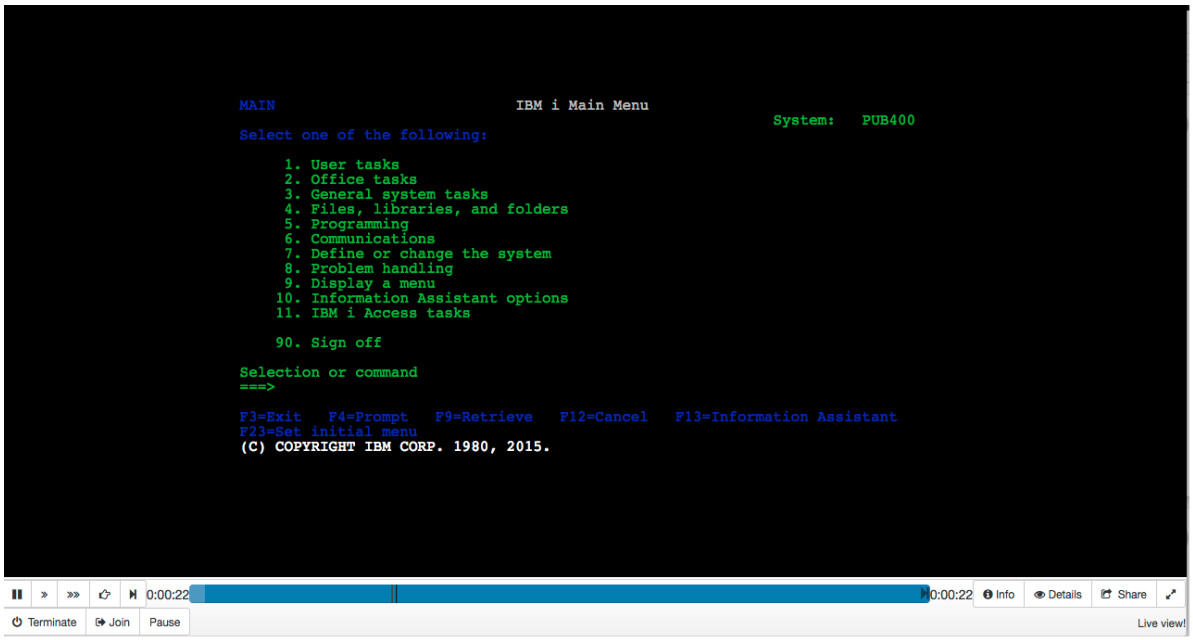
```
FreeBSD/amd83-cerb.whl) (pts/0)
login:
password:
```

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



### 4.6.4 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 Wheel Fudo PAM 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*

## 4.7 MySQL

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

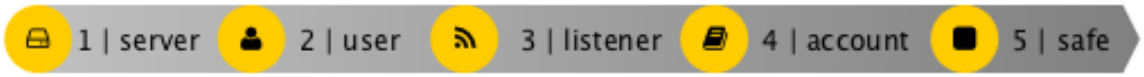
In this scenario, the user connects to a MySQL database using individual login and password. When establishing the connection with the remote server, Wheel Fudo PAM substitutes the login and the password with the previously defined values: `root`/`password` (authorization modes are described in the *User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

**Warning:** Please note that the MySQL server `caching_sha2_password` plugin isn't supported by Fudo PAM. Supportable MySQL plugins by Fudo PAM 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.

### 4.7.1 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.

### 4.7.2 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*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `mysql_server` |
| Blocked | |
| Protocol | `MySQL` |
| Description | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Destination host* | |
| Address | `10.0.1.35` |
| Port | `3306` |
| Bind address | `Any` |

4. Click *Save*.

### 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* | |
| Login | `john_smith` |
| Fudo domain | |
| Blocked | |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | |
| Phone | |
| AD Domain | |
| LDAP Base | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Authentication* | |
| Authentication failures | |
| Enforce static password complexity | |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

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` |
| OCR sessions | ✗ |
| 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` |
| | |
| *Password changer* | |
| Password changer | `None` |
| Privileged user | ✗ |
| Privileged user password | ✗ |

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.

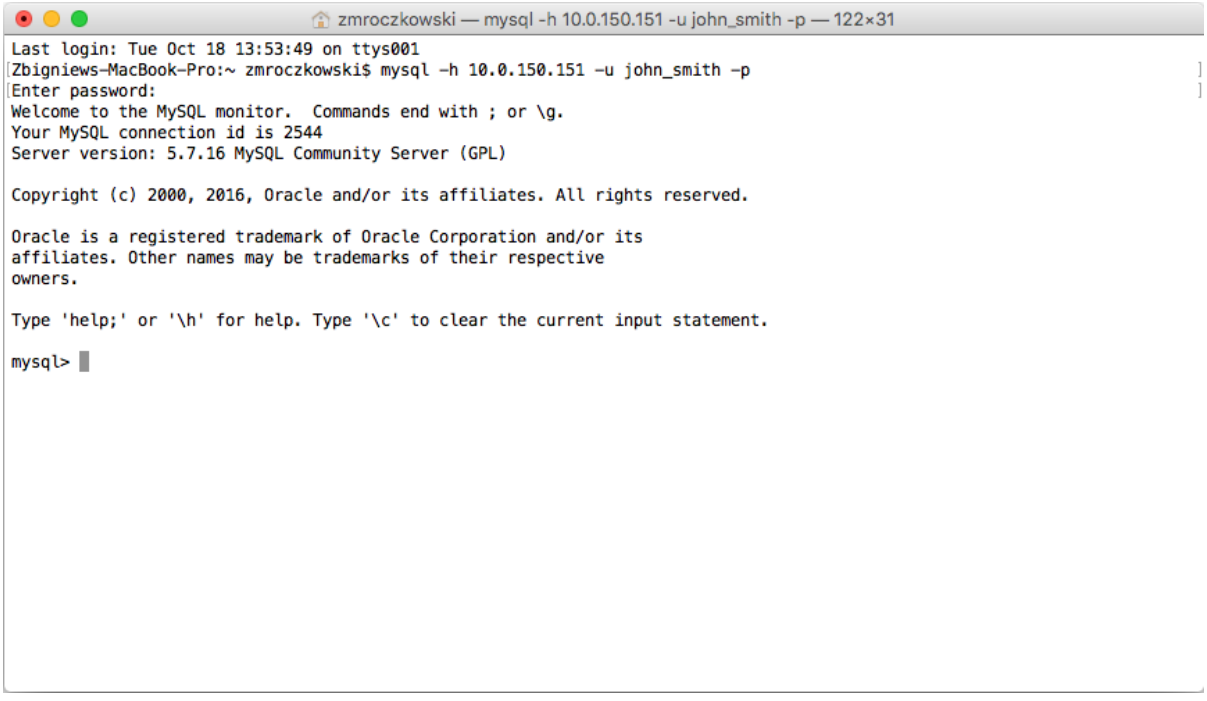
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `mysql_safe` |
| Blocked | ✗ |
| Login reason | ✗ |
| Notifications | ✗ |
| Policies | ✗ |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | ✗ |
| SSH | ✗ |
| VNC | ✗ |
| | |
| *Accounts* | |
| `admin_mysql_server` | `mysql_listener` |

4. Click *Save*.

### 4.7.3 Establishing connection with a MySQL database

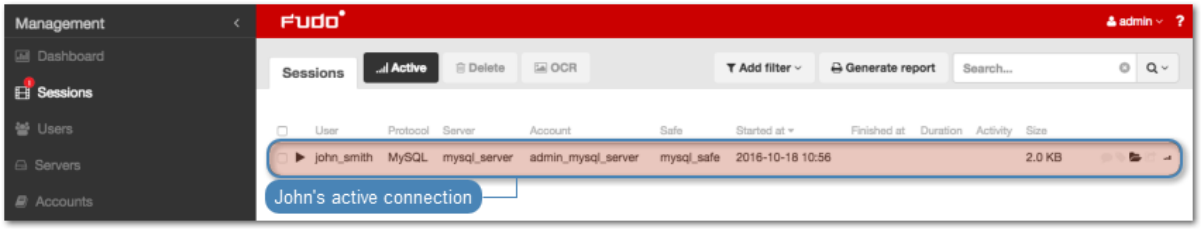
1. Launch a command line interface client.
2. Enter `mysql -h 10.0.150.151 -u john_smith -p`, to connect to the database server.
3. Enter the user's password.




4. Continue browsing the database contents using SQL queries.

### 4.7.4 Viewing user session

1. Open a web browser and go to the Wheel Fudo PAM administration page.
2. Enter user login and password to log in to Wheel Fudo PAM 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*

## 4.8 MS SQL

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

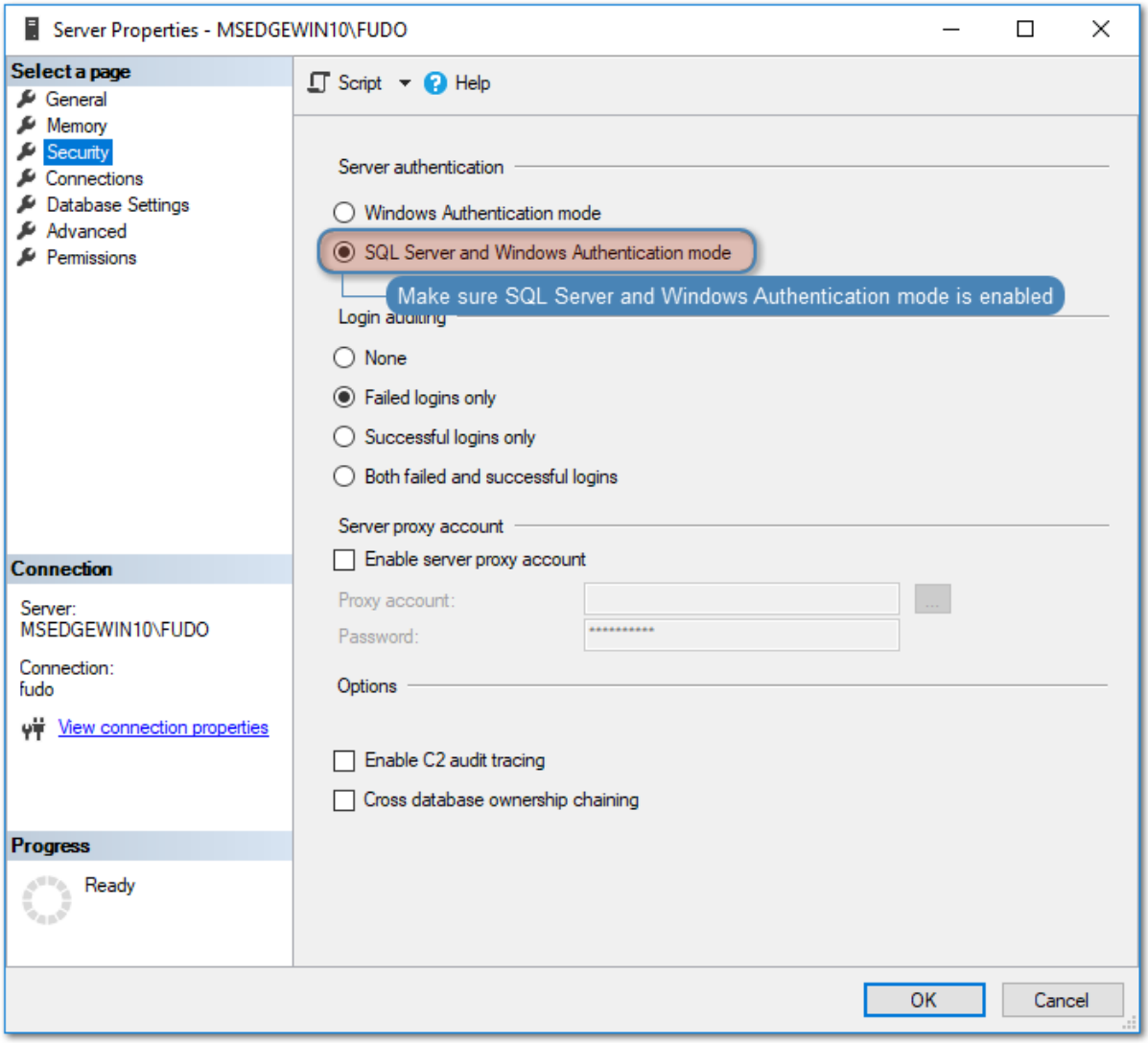
In this scenario, the user connects to a MS SQL database using individual login and password using *SQL Server Management Studio*. When establishing the connection with the remote server, Wheel Fudo PAM substitutes the login and the password with the previously defined values: `fudo`/`password` (authorization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

### 4.8.1 Prerequisites

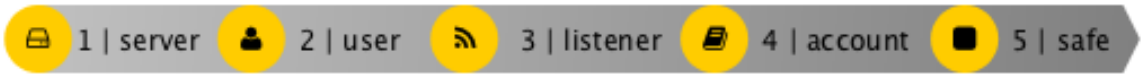
The following description assumes that the system has been already initiated. For more information on the initiation procedure refer to the *System initiation* topic.

---

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




### 4.8.2 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*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `mssql_server` |
| Blocked | |
| Protocol | `MS SQL (TDS)` |
| Description | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Destination host* | |
| Address | `10.0.150.154` |
| Port | `1433` |
| Bind address | `Any` |

4. Click *Save*.

### 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* | |
| Login | `john_smith` |
| Fudo domain | ✗ |
| Blocked | ✗ |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | ✗ |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | ✗ |
| Phone | ✗ |
| AD Domain | ✗ |
| LDAP Base | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Authentication* | |
| Authentication failures | ✗ |
| Enforce static password complexity | ✗ |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

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` |
| OCR sessions | |
| Delete session data after | `61` days |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Server* | |
| Server | `mysql_server` |
| | |
| *Credentials* | |
| Domain | |
| Login | `fudo` |
| Replace secret with | `with password` |
| Password | `password` |
| Repeat password | `password` |
| Password change policy | `Static, without restrictions` |
| | |
| *Password changer* | |
| Password changer | `None` |
| Privileged user | |
| Privileged user password | |

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.

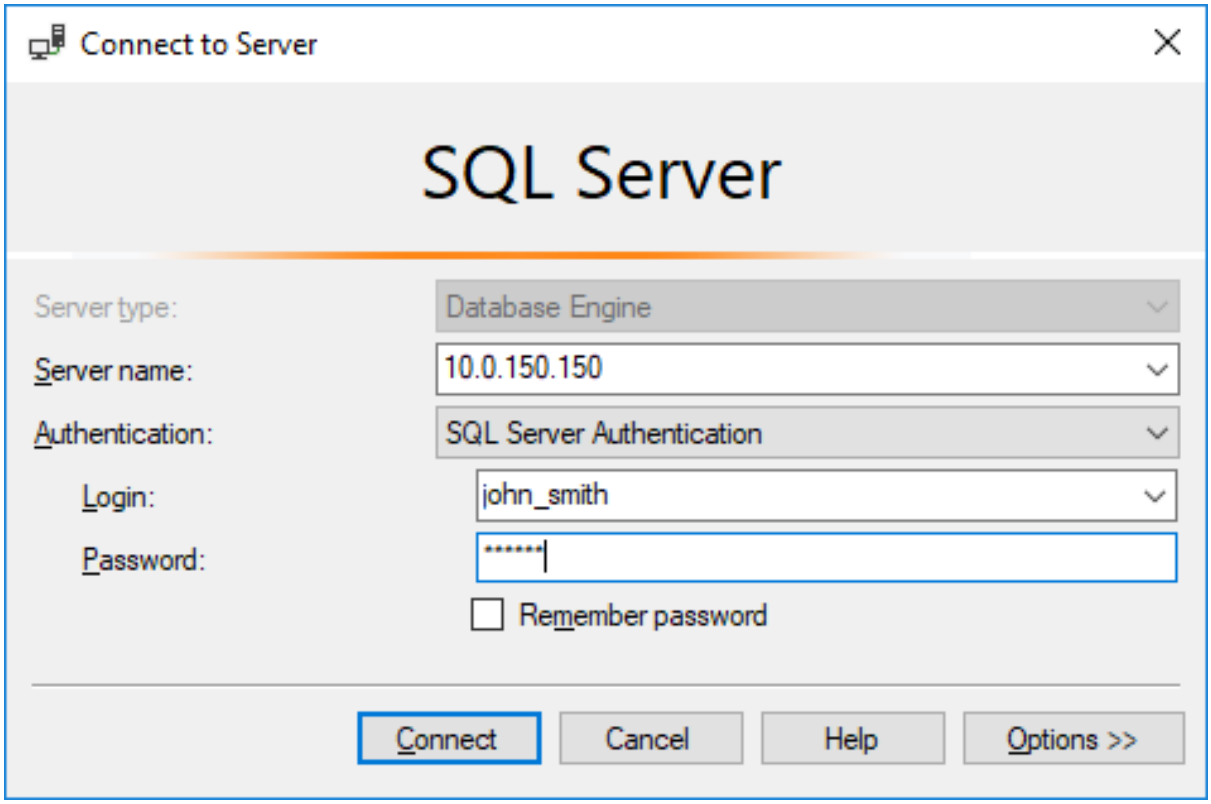
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

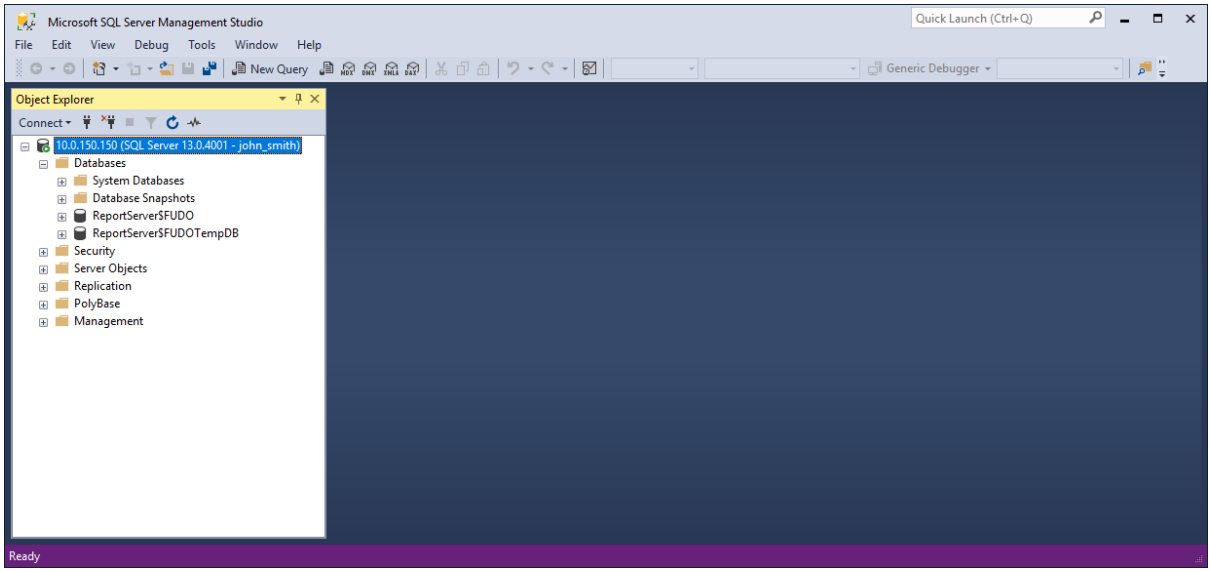
| Parameter | Value |
|---|---|
| *General* | |
| Name | `mssql_safe` |
| Blocked | |
| Login reason | |
| Notifications | |
| Policies | |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | |
| SSH | |
| VNC | |
| | |
| *Accounts* | |
| `admin_mssql_server` | `MSSQL_proxy` |

4. Click *Save*.

### 4.8.3 Establishing connection with a MS SQL database

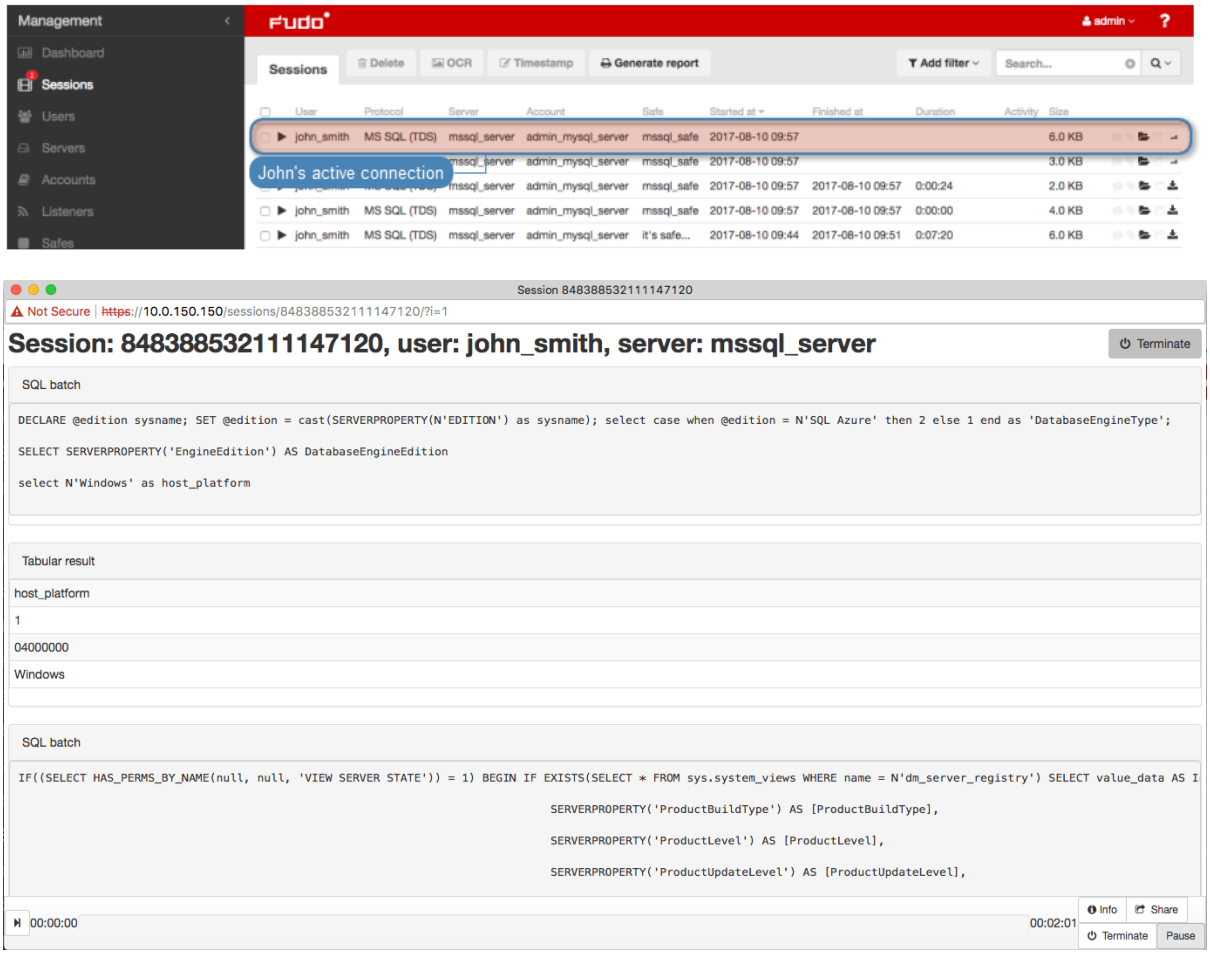
1. Start *SQL Server Management Studio*.
2. Enter previously configured proxy address (10.0.150.150).
3. From the *Authentication* drop-down list, select *SQL Server Authentication*.
4. Enter user login and password.
5. Click *Connect*.




### 4.8.4 Viewing user session

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




**Related topics:**

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

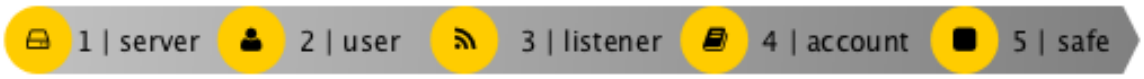
## 4.9 HTTP

This chapter contains an example of a basic Wheel Fudo PAM configuration, to monitor HTTP access to a remote server. In this scenario, the user browses resources of the monitored server using a web browser. The user is authenticated by Wheel Fudo PAM against the local user database. The connection will timeout after 15 minutes (900 seconds) and the user will have to login again to continue browsing the server's contents.

### 4.9.1 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.

### 4.9.2 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*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *Genera* | |
| Name | `http_server` |
| Blocked | ✗ |
| Protocol | `HTTP` |
| HTTP timeout | `900` |
| Enable SSLv2 support | ✗ |
| Enable SSLv3 support | ✗ |
| Description | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Destination host* | |
| Address | `www.wheelsystems.com` |
| Port | `80` |
| HTTP host | ✗ |

4. Click *Save*.

#### 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* | |
| Login | `john_smith` |
| Fudo domain | ✗ |
| Blocked | ✗ |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | ✗ |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | ✗ |
| Phone | ✗ |
| AD Domain | ✗ |
| LDAP Base | ✗ |
| *Permissions* | |
| Granted users | ✗ |
| *Authentication* | |
| Authentication failures | ✗ |
| Enforce static password complexity | ✗ |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

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 | `http_listener` |
| Blocked | |
| Protocol | `HTTP` |
| Enable SSLv2 support | |
| Enable SSLv3 support | |

| *Permissions* | |
|---|---|
| Granted users | |

| *Connection* | |
|---|---|
| Mode | `proxy` |
| Local address | `10.0.150.151` |
| Port | `8080` |
| 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_http_server` |
| Blocked | |
| Type | `forward` |
| Session recording | `all` |
| OCR sessions | |
| Delete session data after | `61` days |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Server* | |
| Server | `http_server` |
| | |
| *Credentials* | |
| Replace secret with | `with password` |
| Password | |
| Repeat password | |

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.

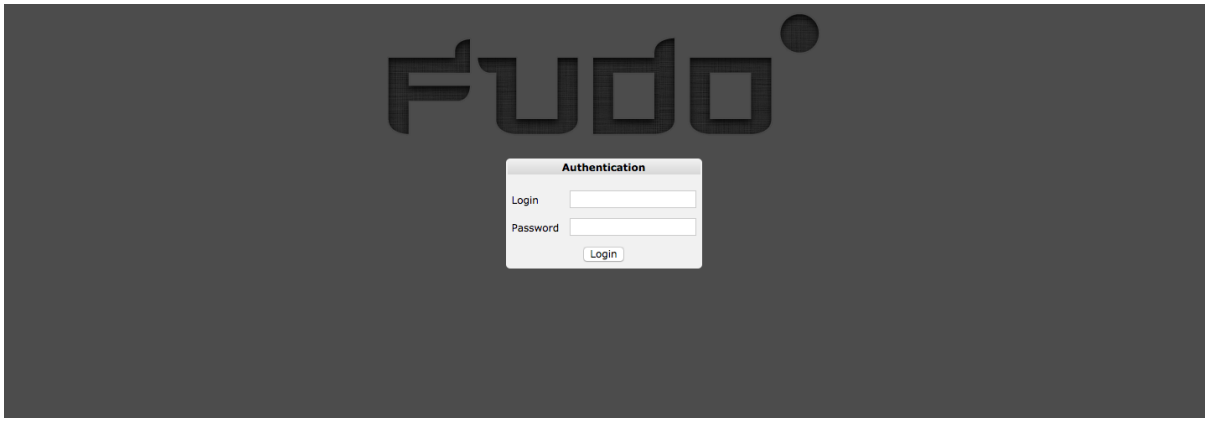
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `http_safe` |
| Blocked | ✗ |
| Login reason | ✗ |
| Notifications | ✗ |
| Policies | ✗ |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | ✗ |
| SSH | ✗ |
| VNC | ✗ |
| | |
| *Accounts* | |
| `admin_http_server` | `http_listener` |

4. Click *Save*.

### 4.9.3 Connecting to remote resource

1. Launch a web browser.
2. Go to the `10.0.150.151:8080` web address.
3. Enter user login and password and press the [Enter] key or click the *Login* button.

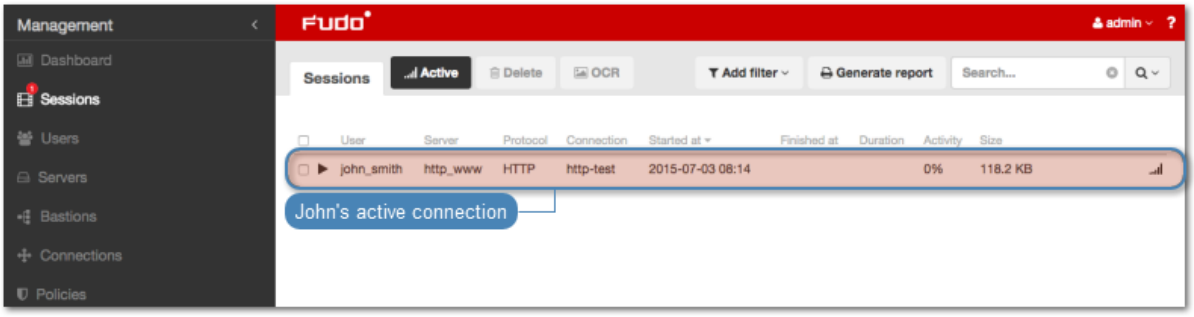


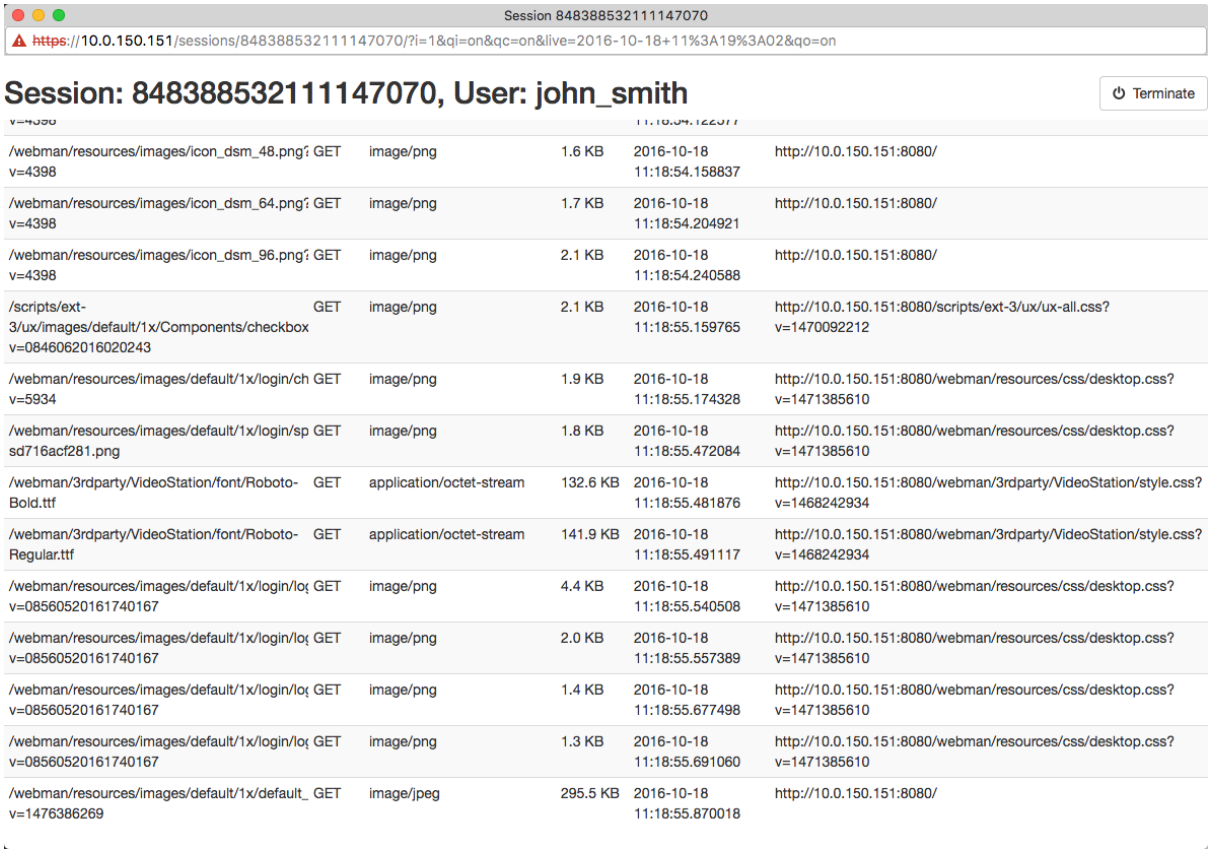

4. Continue browsing the website.

### 4.9.4 Viewing user session

1. Open a web browser and go to the Wheel Fudo PAM administration page.
2. Enter user login and password to log in to Wheel Fudo PAM 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 - MySQL connection configuration*
- *Quick start - Telnet connection configuration*
- *Requirements*
- *Data model*

## 4.10 Citrix

Privileged sessions over ICA protocol cen be established either directly using client software or initiated through Citrix StoreFront interface.

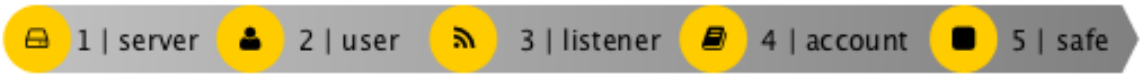
### 4.10.1 ICA

This chapter contains an example of a basic Wheel Fudo PAM configuration, to monitor direct ICA protocol connections.

#### 4.10.1.1 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.

#### 4.10.1.2 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*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `ica_server` |
| Blocked | ✗ |
| Protocol | `ICA` |
| Description | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Destination host* | |
| Address | `10.0.0.21` |
| Port | `1494` |
| Use TLS | ✗ |

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 | `ica_listener` |
| Blocked | ✗ |
| Protocol | `ICA` |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Connection* | |
| Mode | `proxy` |
| Local address | `10.0.150.151` |
| Port | `2494` |
| 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_ica_server` |
| Blocked | |
| Type | `regular` |
| Session recording | `all` |
| OCR sessions | |
| Delete session data after | `61` days |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Server* | |
| Server | `ica_server` |
| | |
| *Credentials* | |
| Domain | |
| Login | `citrixuser` |
| Replace secret with | `password` |
| Password | `password` |
| Repeat password | `password` |
| Password change policy | `Static, without restrictions` |
| | |
| *Password changer* | |
| Password changer | `none` |
| Privileged user | |
| Privileged user password | |

4. Click *Save*.

### 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* | |
| Login | `john_smith` |
| Fudo domain | |
| Blocked | |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | |
| Phone | |
| AD Domain | |
| LDAP Base | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Authentication* | |
| Authentication failures | |
| Enforce static password complexity | |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

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 | `ica_safe` |
| Blocked | ✗ |
| Login reason | ✗ |
| Notifications | ✗ |
| Policies | ✗ |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | ✗ |
| SSH | ✗ |
| VNC | ✗ |
| | |
| *Accounts* | |
| `admin_ica_server` | `ica_listener` |

4. Click *Save*.

**Note:** In case of TLS encrypted connections, Fudo returns an *.ica configuration file* to the Citrix client, which has the *FQDN* server address (*Address*) set to the common name defined in the TLS certificate.

#### 4.10.1.3 Creating `.ica` file with connection parameters

Direct connection with remote server over ICA protocol requires preparing a connection configuration file. This file specifies the listener used to connect to the remote host.

**Note:** Refer to *ICA configuration file* topic for details on the configuration file.

1. Create configuration file containing the following:

```
[ApplicationServers]
ica_connection_example=

[ica_connection_example]
ProxyType=SOCKSV5
ProxyHost=10.0.150.151:2494
ProxyUsername=*
ProxyPassword=*
Address=john_smith
Username=john_smith
ClearPassword=john
TransportDriver=TCP/IP
```

(continues on next page)

(continued from previous page)

```
EncryptionLevelSession=Basic
Compress=Off
```

2. Save the file with `.ica` extension.

#### 4.10.1.4 Connecting to remote resource

1. Double-click the connection configuration file to launch ICA protocol client software.
2. Proceed with using the service.

#### 4.10.1.5 Viewing user session

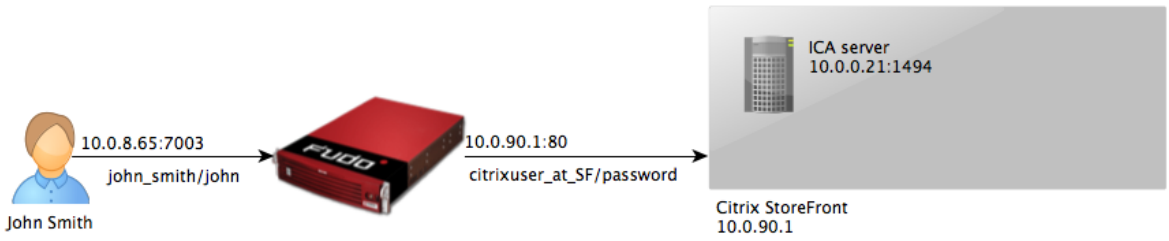
1. Open a web browser and go to the Wheel Fudo PAM administration page.
2. Enter user login and password to log in to Wheel Fudo PAM administration panel.
3. Select *Management* > *Sessions*.
4. Find *John Smith's* session and click the playback icon.

**Related topics:**

- *Data model*
- *Creating an ICA server*
- *Creating an ICA listener*
- *ICA*

### 4.10.2 ICA via Citrix StoreFront

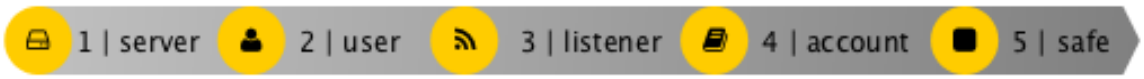
This chapter contains an example of a basic Wheel Fudo PAM configuration, to monitor access to a remote server over ICA protocol with the connection itself being initiated via the Citrix StoreFront.




#### 4.10.2.1 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.

#### 4.10.2.2 Configuration




**Adding an ICA 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*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `ica_server` |
| Blocked | ✗ |
| Protocol | `ICA` |
| Description | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Destination host* | |
| Address | `10.0.0.21` |
| Port | `1494` |
| Use TLS | ✗ |

4. Click *Save*.

**Adding an ICA 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 | `ica_listener` |
| Blocked | ✗ |
| Protocol | `ICA` |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Connection* | |
| Mode | `proxy` |
| Local address | `10.0.150.151` |
| Port | `2494` |
| Use TLS | ✗ |

4. Click *Save*.

### Adding an account for the ICA server

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 | `ICA_forward` |
| Blocked | ✗ |
| Type | `forward` |
| Session recording | `all` |
| OCR sessions | ✗ |
| Delete session data after | `61` days |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Server* | |
| Server | `ica_server` |
| | |
| *Credentials* | |
| Replace secret with | ✗ |
| Forward domain | ✗ |

4. Click *Save*.

### Adding a Citrix StoreFront 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*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `citrix_storefront` |
| Blocked | |
| Protocol | `Citrix StoreFront (HTTP)` |
| HTTP timeout | `900` |
| Description | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Destination host* | |
| Address | `10.0.90.1` |
| Port | `80` |
| Bind address | `Any` |
| URL | `http://10.0.90.1/Citrix/StoreWeb/` |

4. Click *Save*.

### Adding a Citrix StoreFront 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 | `citrix_storefront_listener` |
| Blocked | |
| Protocol | `Citrix StoreFront (HTTP)` |

| *Permissions* | |
|---|---|
| Granted users | |

| *Connection* | |
|---|---|
| Mode | `proxy` |
| Local address | `10.0.8.65` |
| Port | `7003` |
| Use TLS | |

4. Click *Save*.

### Adding an account for the Citrix StoreFront server

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 | `citrixuser_at_SF` |
| Blocked | |
| Type | `regular` |
| Session recording | `all` |
| OCR sessions | |
| Delete session data after | `61` days |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Server* | |
| Server | `citrix_storefront` |
| | |
| *Credentials* | |
| Domain | `tech.whl` |
| Login | `citrixuser` |
| Replace secret with | `password` |
| Password | `password` |
| Repeat password | `password` |
| Password change policy | `Static, without restrictions` |
| | |
| *Password changer* | |
| Password changer | `none` |
| Privileged user | |
| Privileged user password | |

### 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* | |
| Login | `john_smith` |
| Fudo domain | |
| Blocked | |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | |
| Phone | |
| AD Domain | |
| LDAP Base | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Authentication* | |
| Authentication failures | |
| Enforce static password complexity | |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

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.

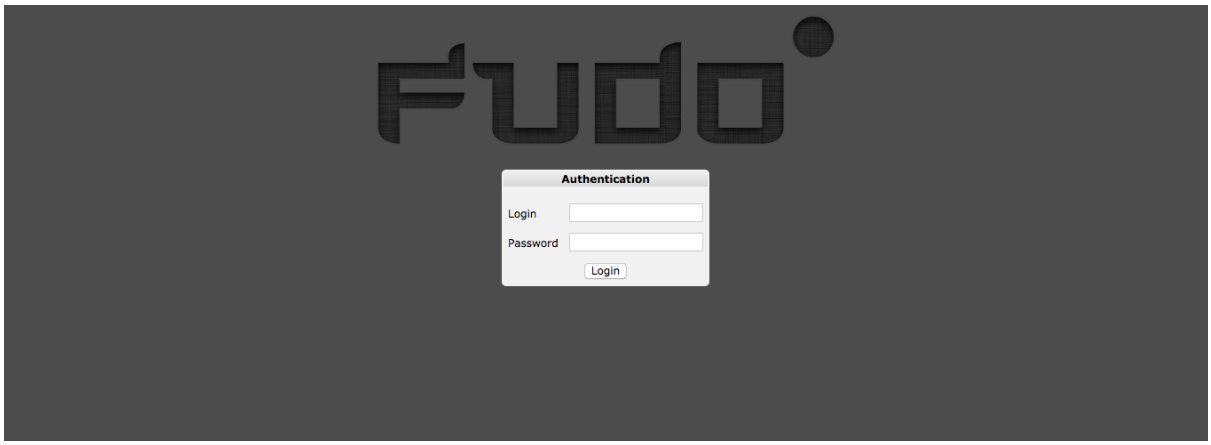
1. Select *Management* > *Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `ica_safe` |
| Blocked | ✗ |
| Login reason | ✗ |
| Notifications | ✗ |
| Policies | ✗ |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | ✗ |
| SSH | ✗ |
| VNC | ✗ |
| | |
| *Accounts* | |
| `citrixuser_at_SF` | `citrix_storefront_listener` |
| `ICA_forward` | `ica_listener` |

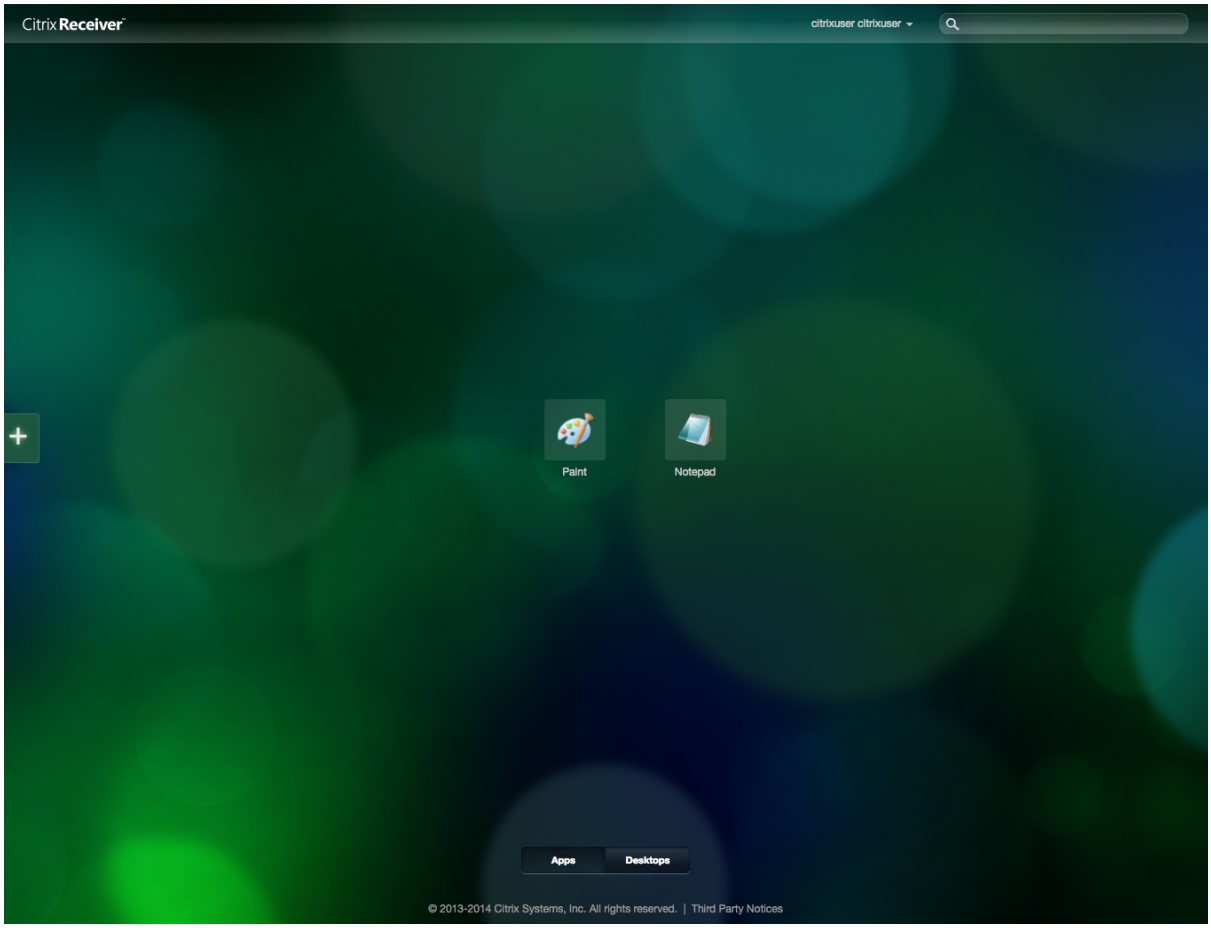
4. Click *Save*.

#### 4.10.2.3 Connecting to remote resource

1. Navigate your web browser to the `10.0.8.65:7003` web address.
2. Enter user login and password to log in into the Citrix StoreFront interface.

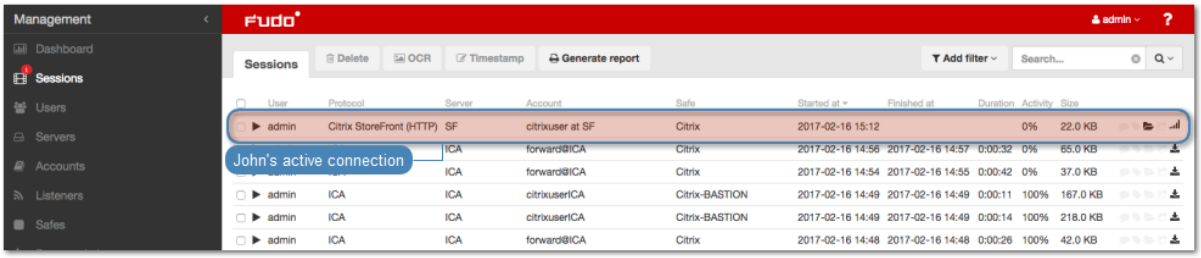



3. Click desired element to establish ICA connection with selected resource.




#### 4.10.2.4 Viewing user session

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




**Related topics:**

- *Data model*
- *ICA*
- *Citrix StoreFront (HTTP)*
- *Creating a Citrix server*
- *Creating a Citrix listener*

## 4.11 VNC

This chapter contains an example of a basic Wheel Fudo PAM 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 Wheel Fudo PAM using an individual login and password combination (`john_smith`/`john`). When establishing the connection with the remote server, Wheel Fudo PAM substitutes the password with the previously defined value: `password` (authentication modes are described in the *User authentication modes* section).

---

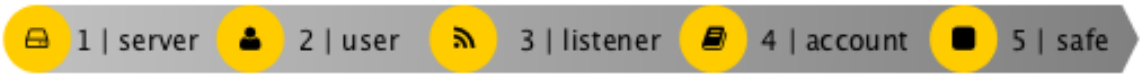
**Note:** Due to specifics of VNC protocol, which authenticates the user using password only, the substitution login string entered in account properties is ignored when establishing a VNC connection.

---

### 4.11.1 Prerequisites

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

### 4.11.2 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*.
3. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| *General* | |
| Name | `vnc_server` |
| Blocked | |
| Protocol | `VNC` |
| Description | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Destination host* | |
| Address | `10.0.40.230` |
| Port | `5900` |

4. Click *Save*.

### 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* | |
| Login | `john_smith` |
| Fudo domain | ✗ |
| Blocked | ✗ |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | ✗ |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | ✗ |
| Phone | ✗ |
| AD Domain | ✗ |
| LDAP Base | ✗ |
| | |
| *Permissions* | |
| Granted users | ✗ |
| | |
| *Authentication* | |
| Authentication failures | ✗ |
| Enforce static password complexity | ✗ |
| Type | `Password` |
| Password | `john` |
| Repeat password | `john` |

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` |

| *Permissions* | |
|---|---|
| Granted users | |

| *Connection* | |
|---|---|
| Mode | `proxy` |
| Local address | `10.0.150.151` |
| Port | `5900` |

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 | `complete` |
| OCR sessions | |
| Delete session data after | `61` days |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Server* | |
| Server | `vnc_server` |
| | |
| *Credentials* | |
| Domain | |
| Login | |
| Replace secret with | `with password` |
| Password | `root` |
| Repeat password | `root` |
| Password change policy | `Static, without restrictions` |
| | |
| *Password changer* | |
| Password changer | `None` |
| Privileged user | |
| Privileged user password | |

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` |
| Notifications | ✗ |
| Ask for login reason | ✗ |
| Policies | ✗ |
| Users | `john_smith` |

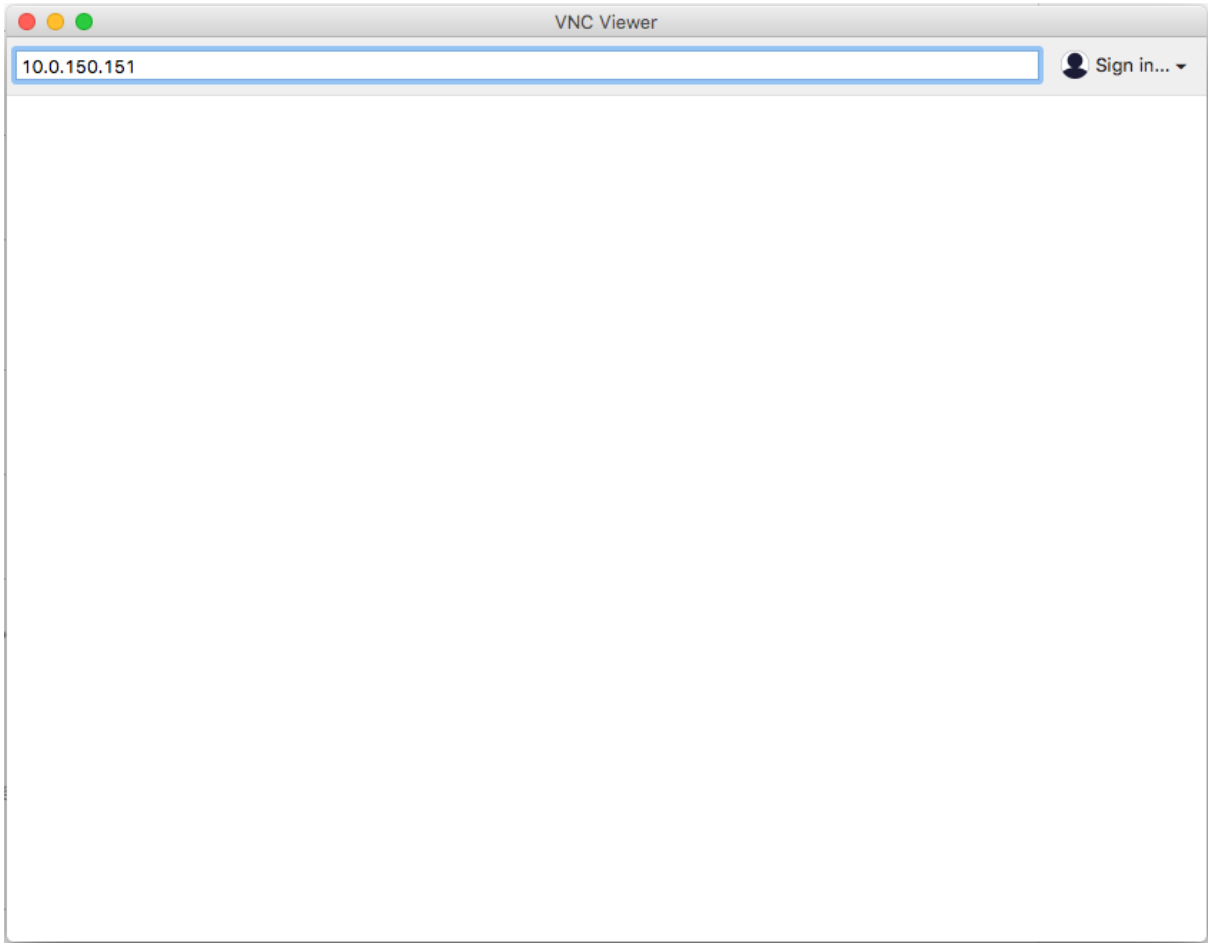
| *Protocol functionality* | |
|---|---|
| RDP | ✗ |
| SSH | ✗ |
| VNC | ✓ |

| *Accounts* | |
|---|---|
| `admin_vnc_server` | `vnc_listener` |

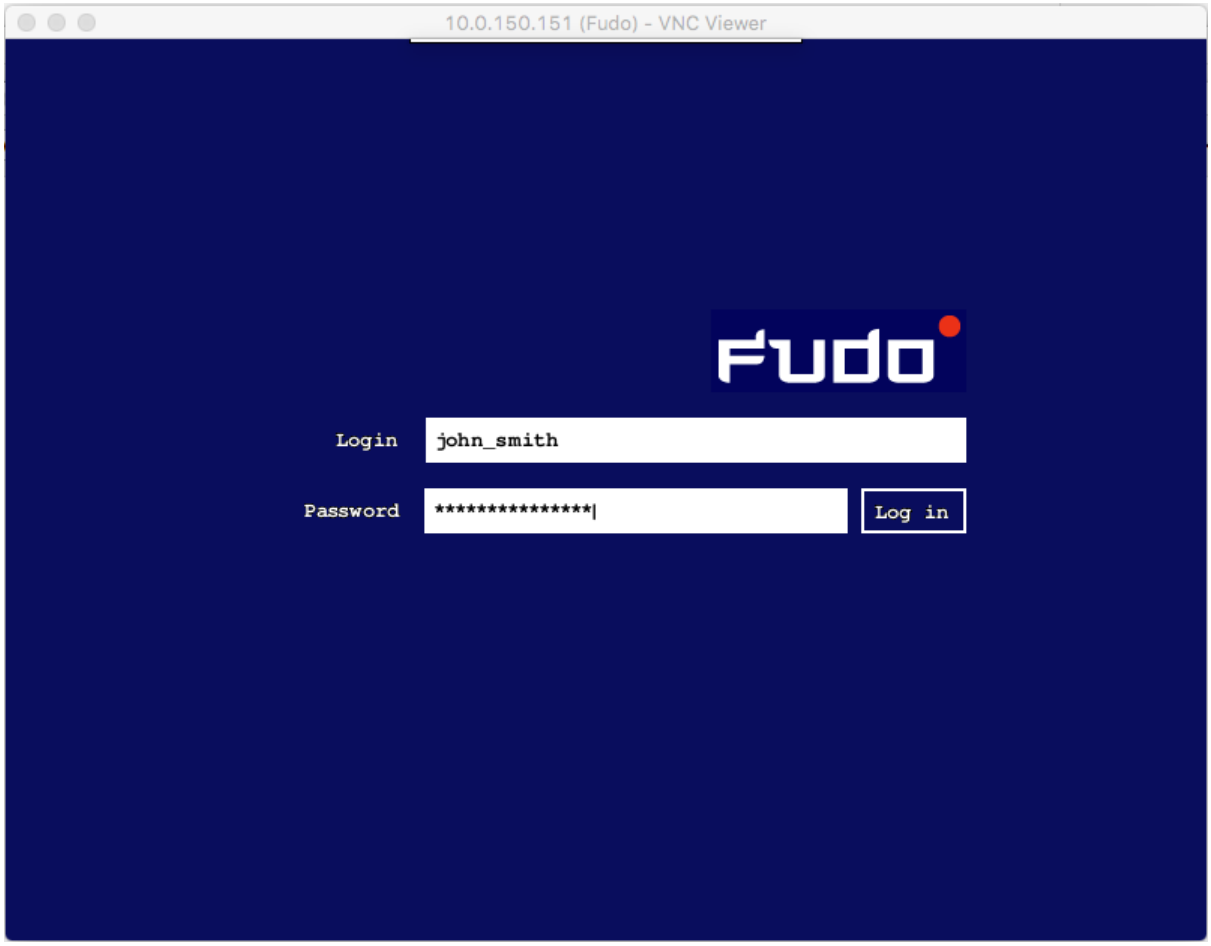
4. Click *Save*.

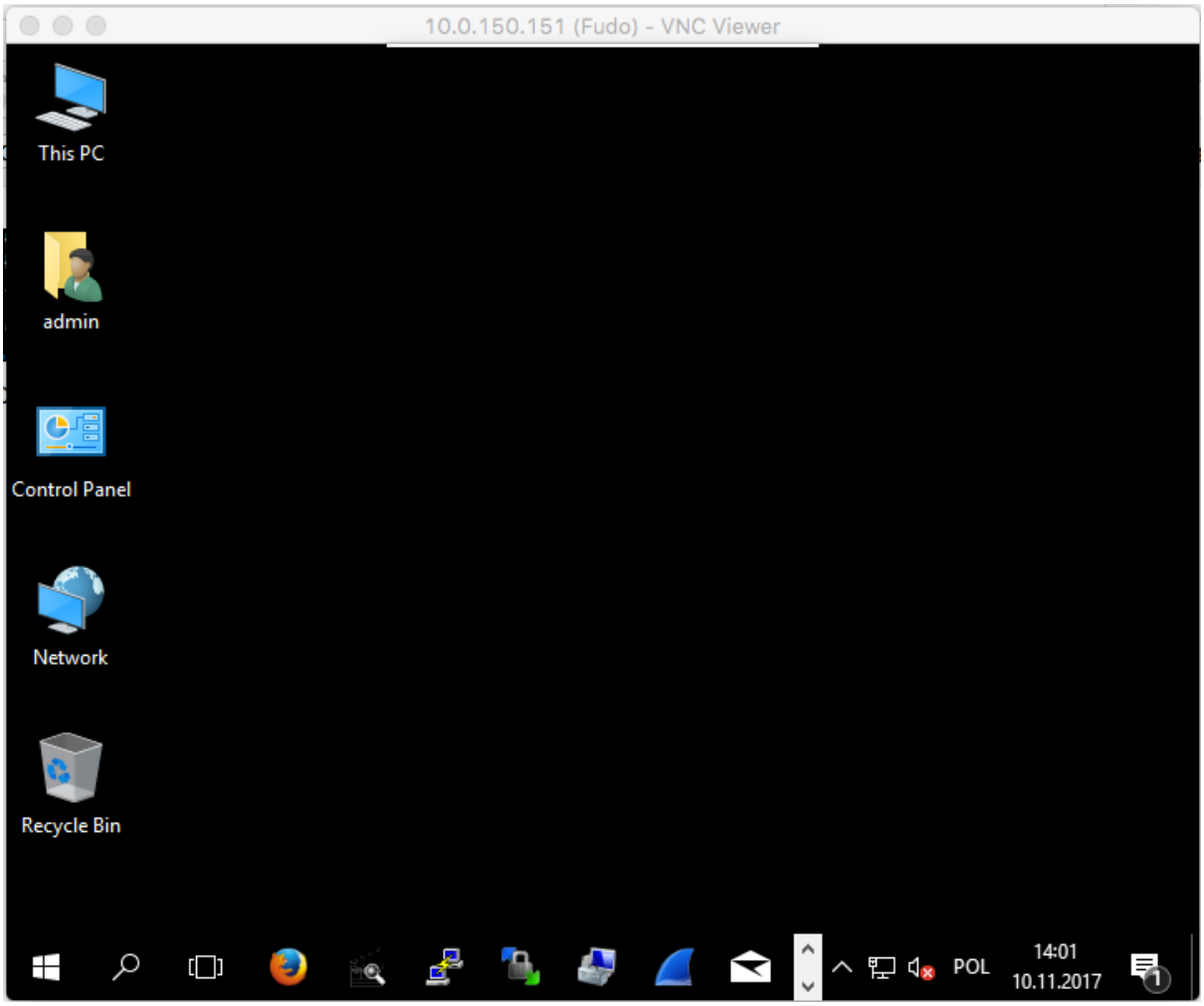
### 4.11.3 Establishing connection

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



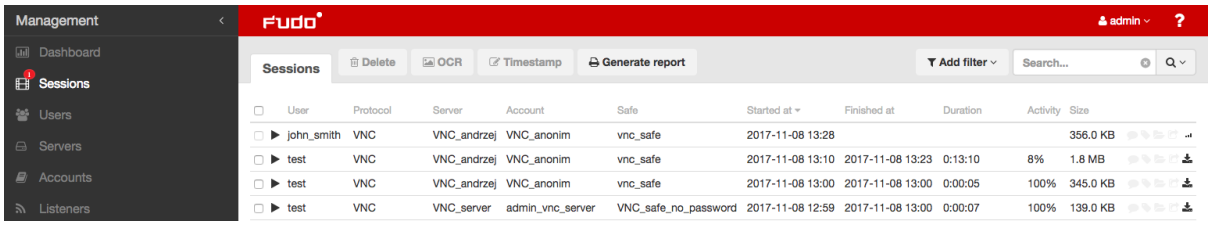

2. Enter username and password and press the enter key.


10.0.150.151 (Fudo) - VNC Viewer
Login
john_smith
Password
Log in




### 4.11.4 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 Wheel Fudo PAM administration panel.
3. Select *Management* > *Sessions*.
4. Find *John Smith's* session and click the playback icon.



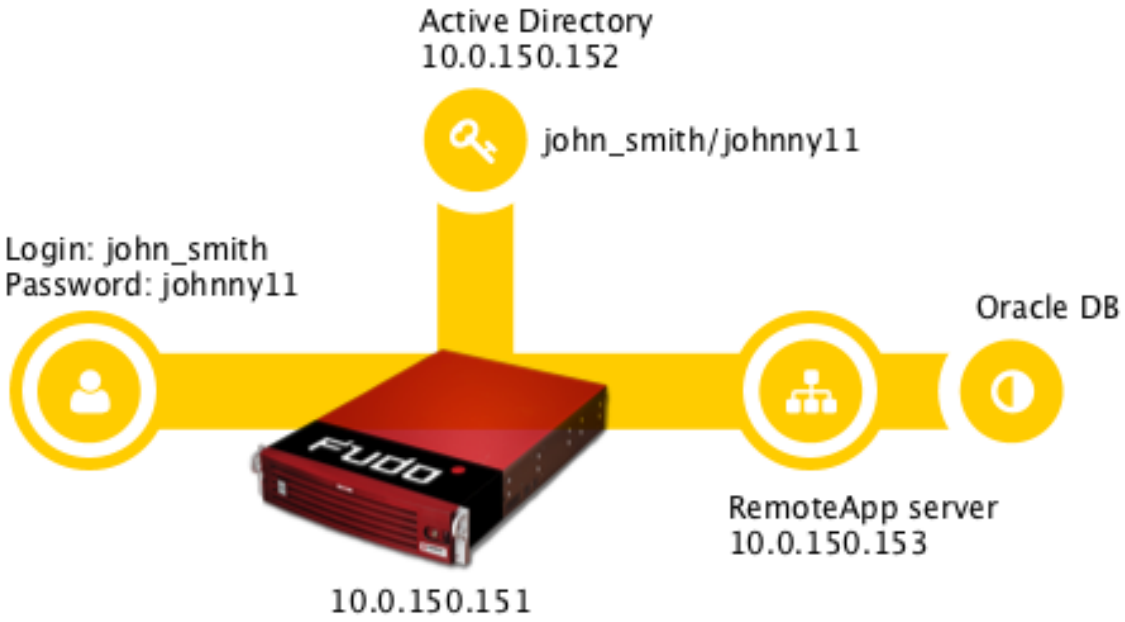

**Related topics:**

- *VNC Viewer*
- *Requirements*
- *Data model*
- *Quick start - RDP connection configuration*

- *Quick start - HTTP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - Telnet connection configuration*

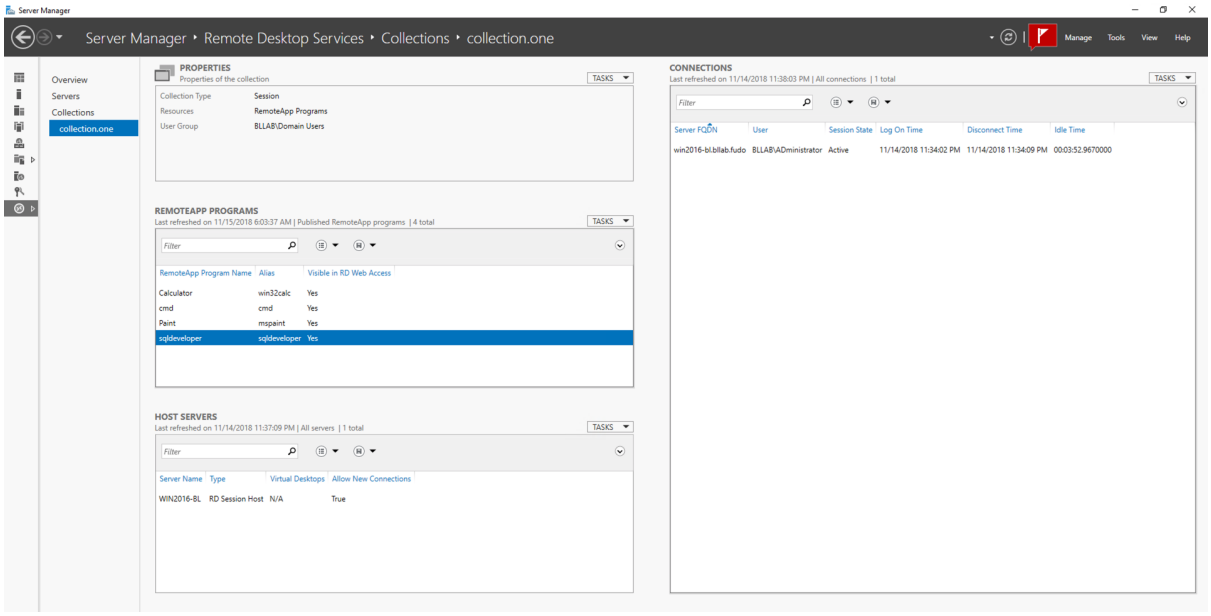
## 4.12 Oracle over RemoteApp

This chapter contains an example configuration, to monitor Oracle database connections over RempteApp. In this scenario, the user connects the the RemoteApp server over *RDP*. Login credentials are checked in the Active Directory and forwarded to the target server. Connection is established in the *proxy* mode.



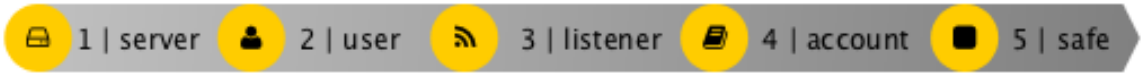

### 4.12.1 Prerequisites

- RDS environment deployed and configured on Windows Server 2016/2012/2012 R2,
- SQL Developer application added to a RDS collection,




- Active Directory service for user authentication,
- Users in Active Directory must be allowed to log in to the RDS server.

### 4.12.2 Configuration




#### Adding a server

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

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

| Parameter | Value |
|---|---|
| *General* | |
| Name | `RemoteApp server` |
| Blocked | |
| Protocol | `RDP` |
| Security | `Enhanced RDP Security (TLS) + NLA` |
| Description | |

| *Permissions* | |
|---|---|
| Granted users | |

| *Destination host* | |
|---|---|
| Address | `10.0.150.153` |
| Port | `3389` |
| Bind address | `Any` |

4. Download or enter target server's public key.
5. Click *Save*.

### 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* | |
| Login | `john_smith` |
| Blocked | |
| Account validity | `Indefinite` |
| Role | `user` |
| Preferred language | `English` |
| Safes | default settings |
| Full name | `John Smith` |
| Email | `john@smith.com` |
| Organization | |
| Phone | |
| AD Domain | |
| LDAP Base | |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Authentication* | |
| Authentication failures | |
| Enforce static password complexity | |
| Type | `External authentication` |
| External authentication source | `Active directory 10.0.150.152:389` |

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 | `RemoteApp-listener` |
| Blocked | |
| Protocol | `RDP` |
| Security | `Enhanced RDP Security (TLS) + NLA` |
| Announcement | |

| *Permissions* | |
|---|---|
| Granted users | |

| *Connection* | |
|---|---|
| Mode | `proxy` |
| Local address | `10.0.150.151` |
| Port | `10025` |
| External address | |

4. Generate or upload proxy server's 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 | `RemoteApp-account` |
| Blocked | |
| Type | `forward` |
| Session recording | `all` |
| OCR sessions | |
| OCR Language | `English` |
| Delete session data after | `61` days |
| | |
| *Permissions* | |
| Granted users | |
| | |
| *Server* | |
| Server | `RemoteApp_server` |
| | |
| *Credentials* | |
| Replace secret with | |
| 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 | `RemoteApp-safe` |
| Blocked | ✗ |
| Notifications | ✗ |
| Login reason | ✗ |
| Require approval | ✗ |
| Policies | ✗ |
| Users | `john_smith` |
| | |
| *Protocol functionality* | |
| RDP | ✓ |
| SSH | ✗ |
| VNC | ✗ |
| | |
| *Accounts* | |
| `RemoteApp-account` | `RemoteApp-listener` |

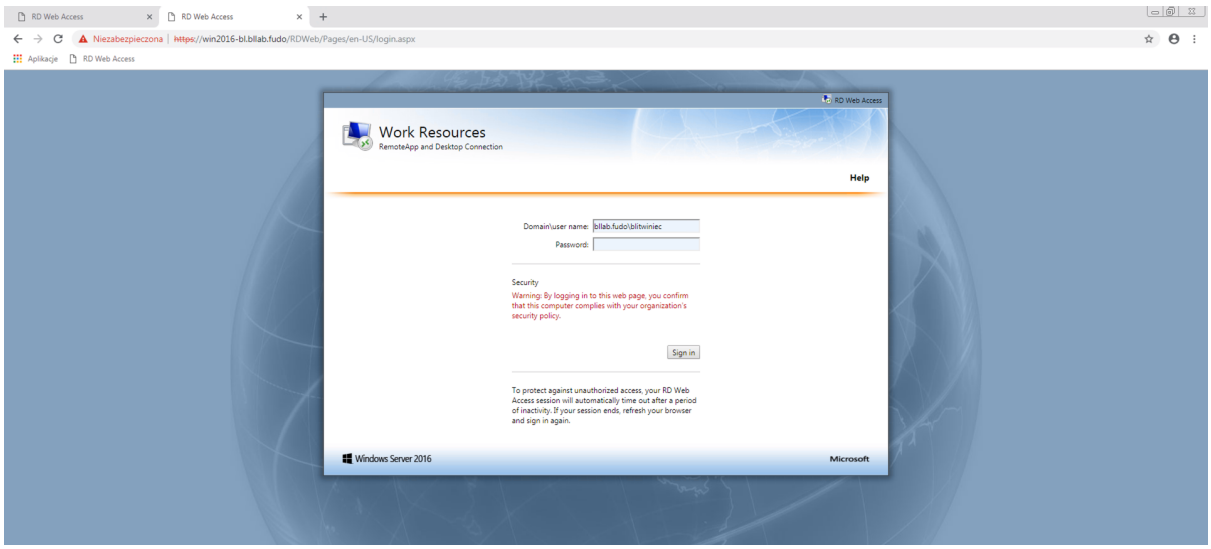
4. Click *Save*.

### 4.12.3 Changing registry entries on the RDS domain controller

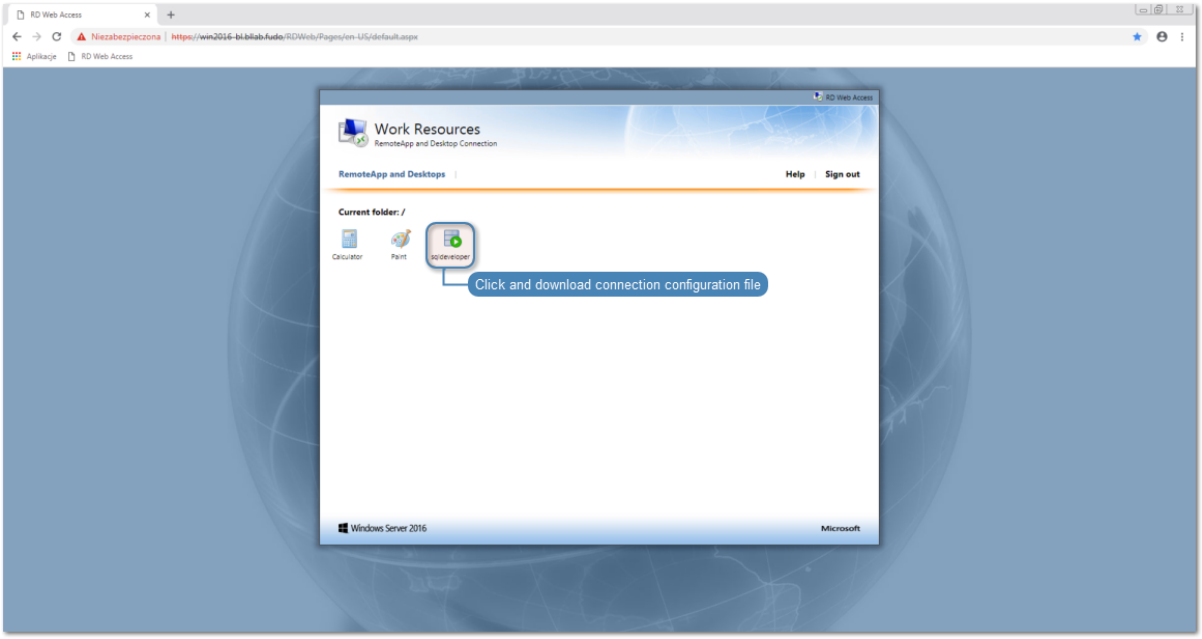
1. Log in, with administrator privileges, onto the server running the RDS service.
2. Start the system registry editor.
3. Browse registry to find the key *HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows NTCurrentVersionTerminalServerCentralPublishedResourcesPublishedFarmscollectiononeApplicationssqldeveloper*
4. In the *RDPFileContent* parameter, find the *full address:s:* and change its value to the IP address and port number of the previously configured listener, i.e. `full address:s:192.168.3.100:10025`

### 4.12.4 Establishing connection

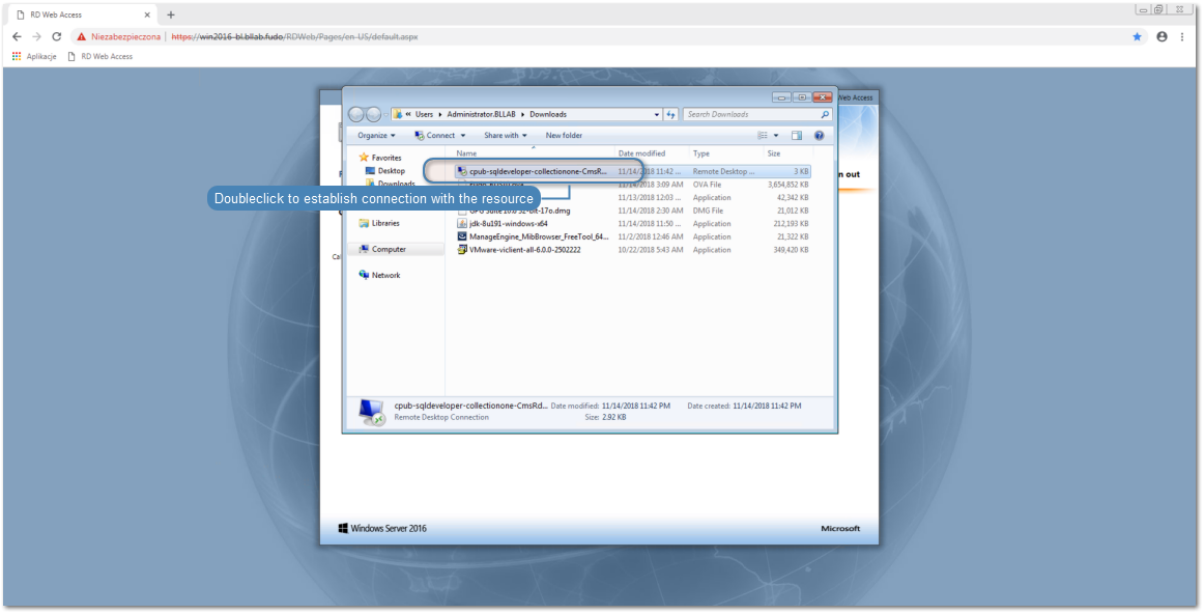
1. Launch the web browser on a client system, navigate to the RDS domain controller application portal and log in.



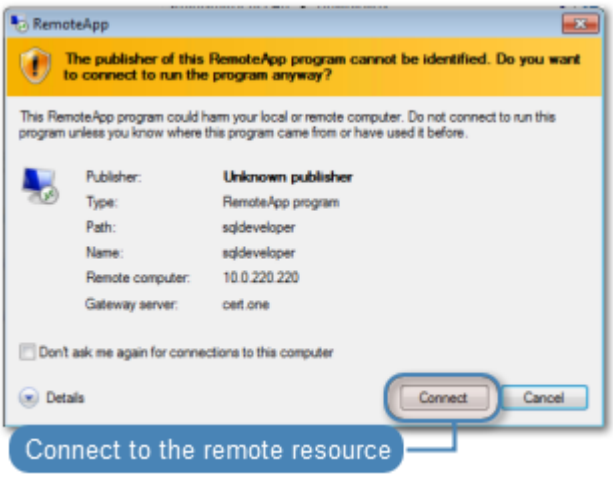

2. Click the *SQL Developer* icon, to download the RemoteApp configuration file.



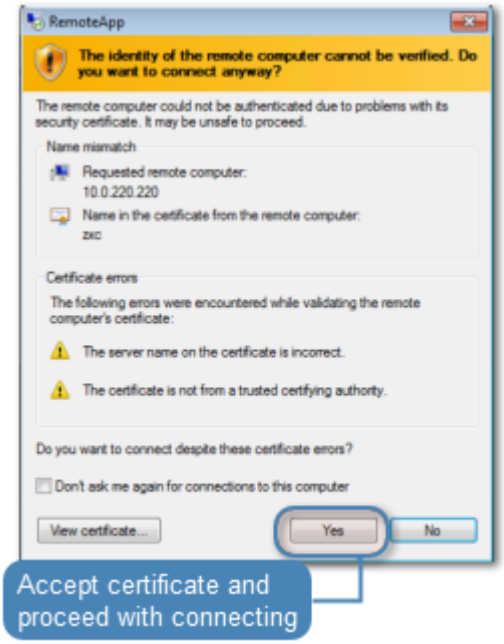

3. Double-click the configuration file.

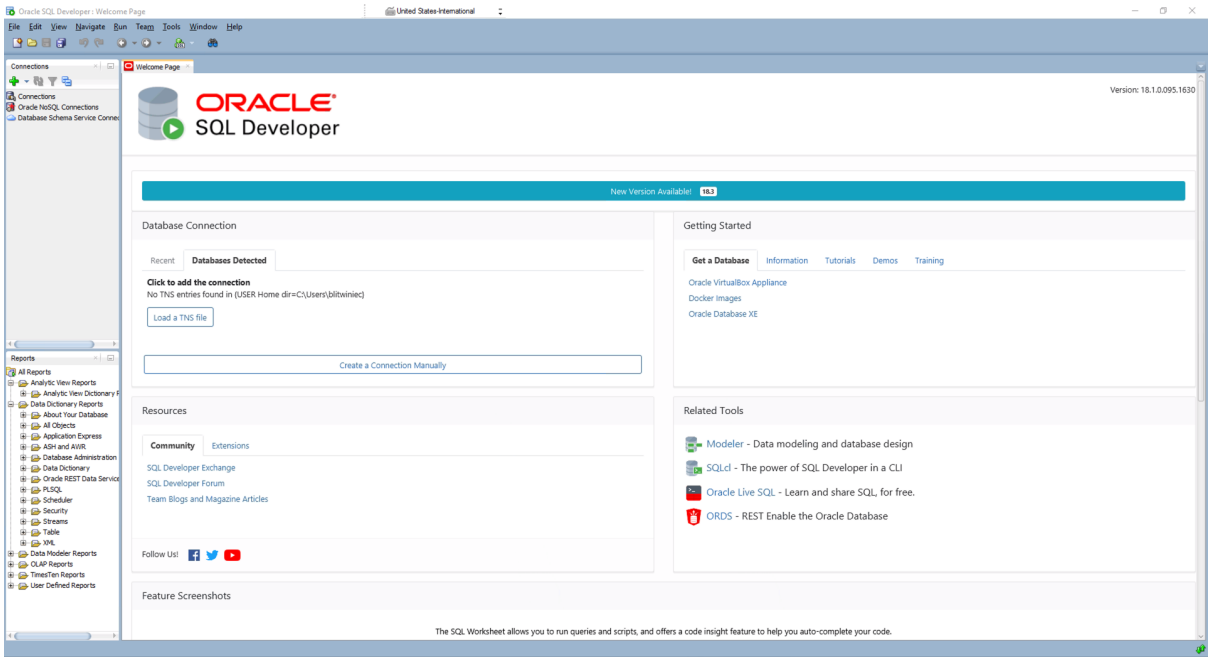



4. Click Connect, to establish connection.



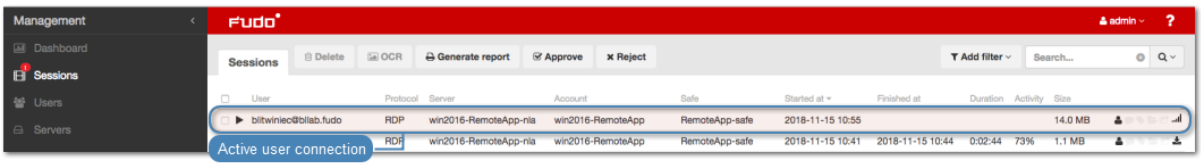

5. Provide login credentials.
6. Accept the certificate and proceed with establishing the connection.

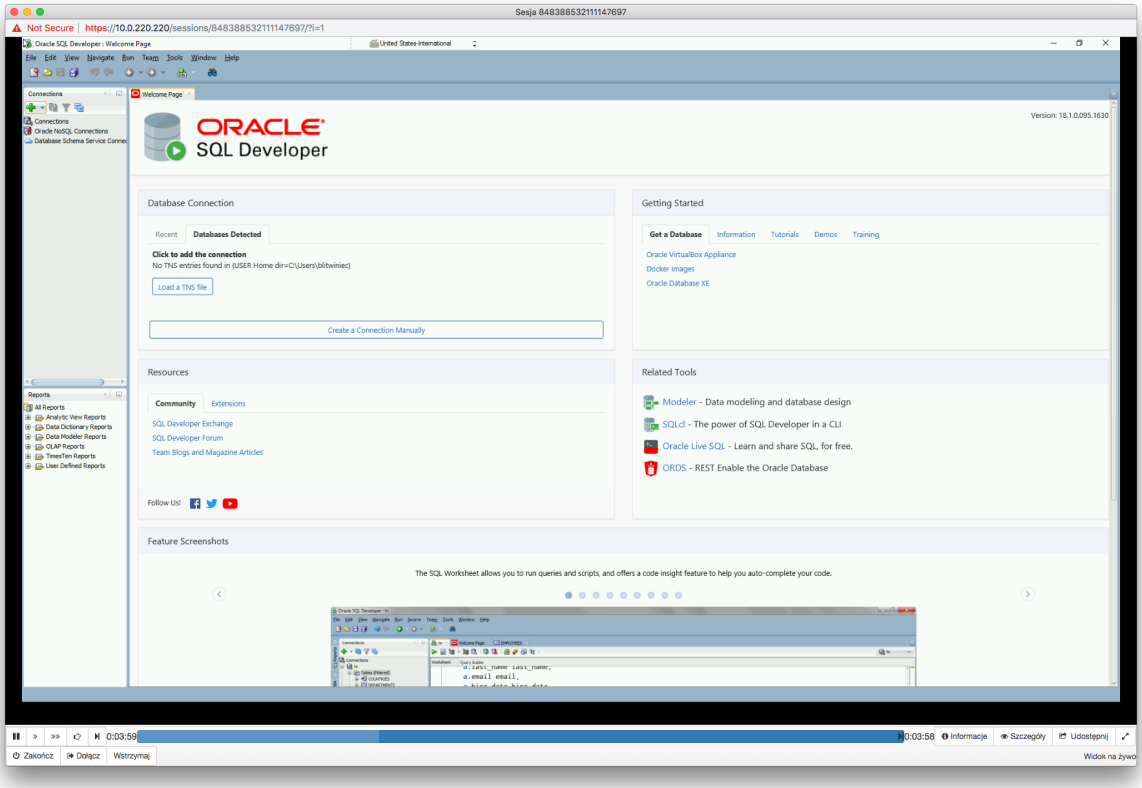



### 4.12.5 Viewing user session

1. Open a web browser and navigate to Fudo's administration panel.
2. Enter login credentials.
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*

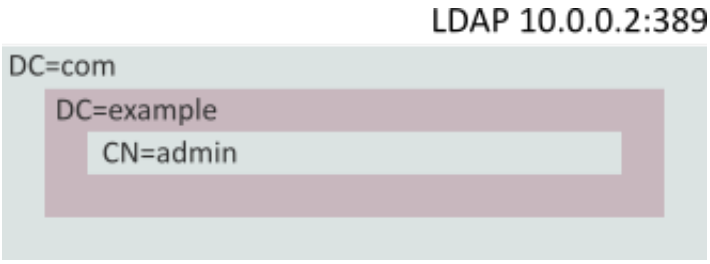
## 4.13 User authentication against external LDAP server

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

### 4.13.1 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`.

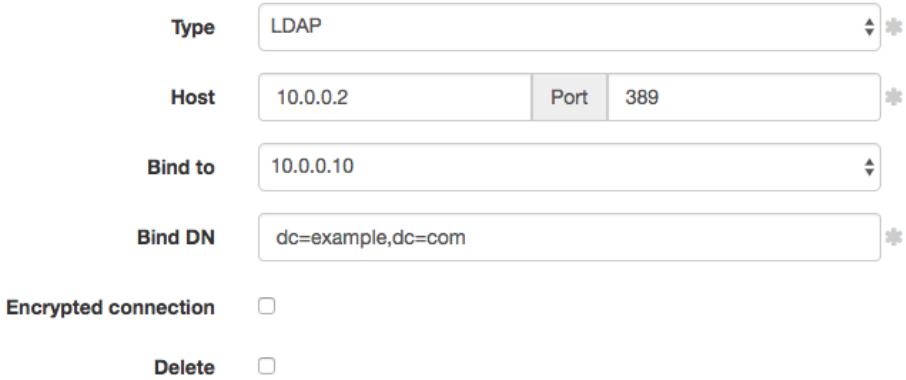



### 4.13.2 Configuration

#### 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`<br><br>**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. In the *LDAP base* field specify the location of *admin* object in the directory structure `cn=admin,dc=example,dc=com`.

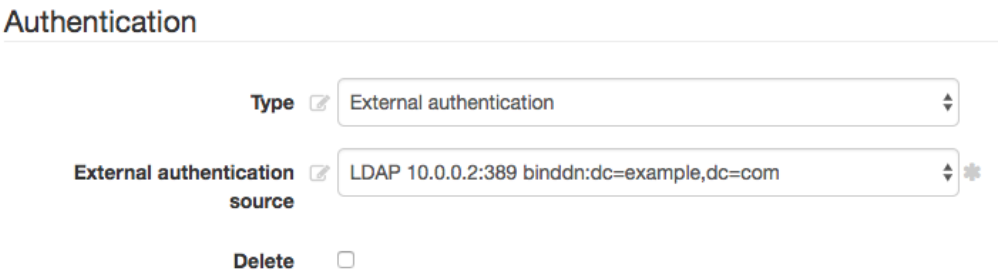
---

**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. Click *+ Add authentication method*.
5. Provide essential configuration parameters:

| Parameter | Value |
|---|---|
| Type | `External authentication` |
| External authentication source | `LDAP 10.0.0.2:389 bind dn:dc=example,dc=com` |
| Delete | |




6. Click *Save*.

**Related topics:**

- *External authentication*
- *Creating a user*
- *Quick start - SSH connections monitoring*

ROZDZIAŁ 5

# 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.

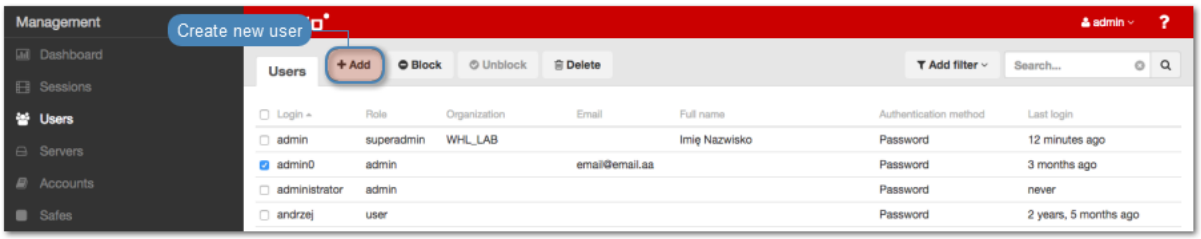
**Note:** Fudo PAM allows importing users definitions from directory services such as Active Directory or LDAP. For more information on users synchronization service, refer to the *Users synchronization* topic.

## 5.1 Creating a user

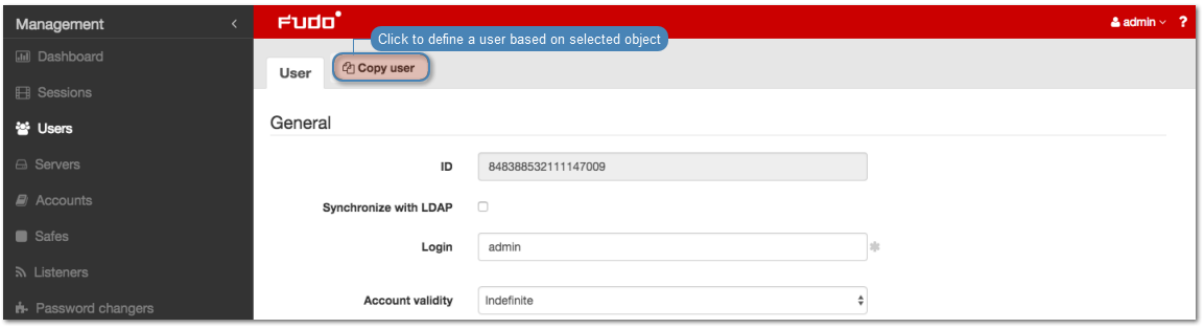
**Warning:** Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances must not be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

**Warning:** Creating a User object for MySQL connections, please note that the MySQL server `caching_sha2_password` plugin isn't supported by Fudo PAM. Supportable MySQL plugins by Fudo PAM 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.

1. Select *Management* > *Users*.
2. Click + *Add*.




**Note:** Fudo PAM enables creating users based on the existing definitions. Click desired user to access its configuration parameters and click *Copy user* to create a new object based on the selected definition.




3. Enter user login.

**Note:**

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

4. Enter Fudo domain.

**Note:**

- With the Fudo domain specified, the user will have to include it when logging into the administration panel or when establishing monitored connections.
- *Default domain* allows for a discretion - user can either include the domain or leave it out.

5. Select the *Blocked* option to prevent user from accessing servers and resources monitored by Fudo PAM.
6. Define account's validity period.
7. Select user's role, which will determine the access rights.

**Note:** Access rights restrictions also apply to API interface access.

| Role | Access rights |
|---|---|
| user | • Connecting to servers through assigned safes.<br>• Loggin to the User Portal (requires adding the user to the `portal` safe)<br>• Fetching servers' passwords (requires additional access right). |
| service | Accessing SNMP information. |
| operator | • Logging in to the administration panel.<br>• Browsing objects: servers, users, safes, accounts, to which the user has been assigned sufficient access permisions.<br>• Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions.<br>• Generating reports on demand and subscribing to periodic reports.<br>• Activating/deactivating email notifications.<br>• Viewing live and archived sessions involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions.<br>• Converting sessions and downloading converted content involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions. |
| admin | • Logging in to the administration panel.<br>• Managing objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions.<br>• Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions.<br>• Generating reports on demand and subscribing to periodic reports.<br>• Activating/deactivating email notifications.<br>• Viewing live and archived sessions involving objects (user, safe, account, server), to which the user has been assigned management privileges.<br>• Converting sessions and downloading converted content involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions.<br>• Managing policies. |
| superadmin | • Full access rights to objects management.<br>• Full access rights to system configuration options. |

8. Select user's preferred language in Fudo PAM administration panel.
9. Grant access to safes.

**Note:**

- Drag and drop safe objects to change the order in which safes are processed upon establishing connection.
- SSH_safe implies that the Reveal password option is disabled.
- RDP_safe implies, that the Reveal password option is enabled.
- Click safe to define *time access policy*.

10. Enter user's full name.
11. Enter user's email address.
12. Enter user's organizational unit.
13. Enter user's phone number.
14. Provide user's *Active Directory* domain.

**Note:** 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 PAM will report authentication problem as it cannot determine which user is trying to connect.

15. Enter *LDAP* service *BaseDN* parameter.

**Note:**

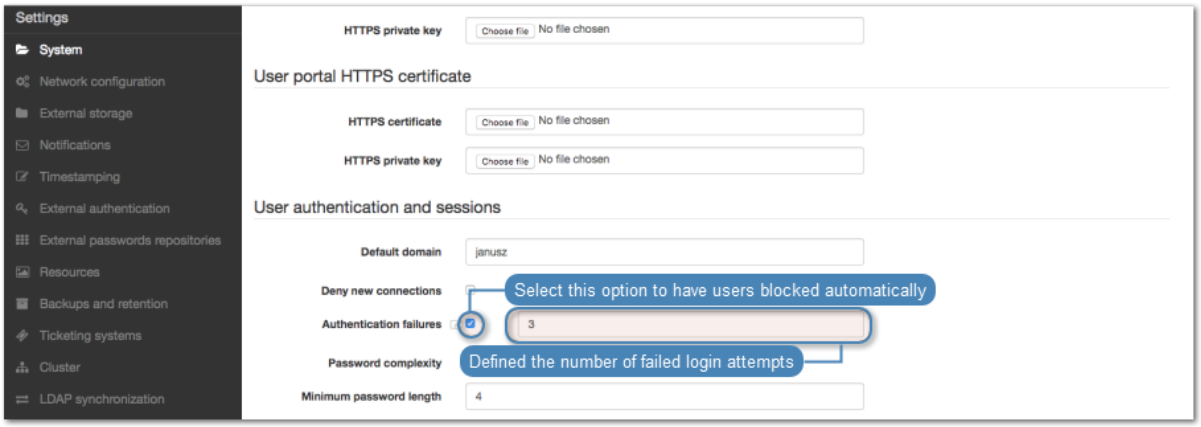
- LDAP base is necessary for authenticating the user using the Active Directory service.
- E.g. for `example.com` domain, the LDAP base parameter value should be `dc=example, dc=com`.

16. In the *Permissions* section, select users allowed to manage this user object and in case of operators/administrators, assign management privileges to selected data model objects.

**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.

17. 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* > *System* in the *User authentication and sessions* section.




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

**Note:** Password complexity is defined in *Settings* > *System* in the *Users authentication and sessions* section.

19. Select authentication type.

*External authentication*

- Select `External authentication` from the *Type* drop-down list.
- Select external authentication source from the *External authentication source* drop-down list.

**Note:** Refer to *External authentication* topic for more information on external authentication sources.

*Password*

- Select `Password` from the *Type* drop-down list.
- Type password in the *Password* field.
- Repeat password in the *Repeat 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 portal*.

*SSH key*

- Select `SSH key` from the *Type* drop-down list.
- Click the upload icon and browse the file system to find the public SSH key used for verifying user's identity.

*One-time password*

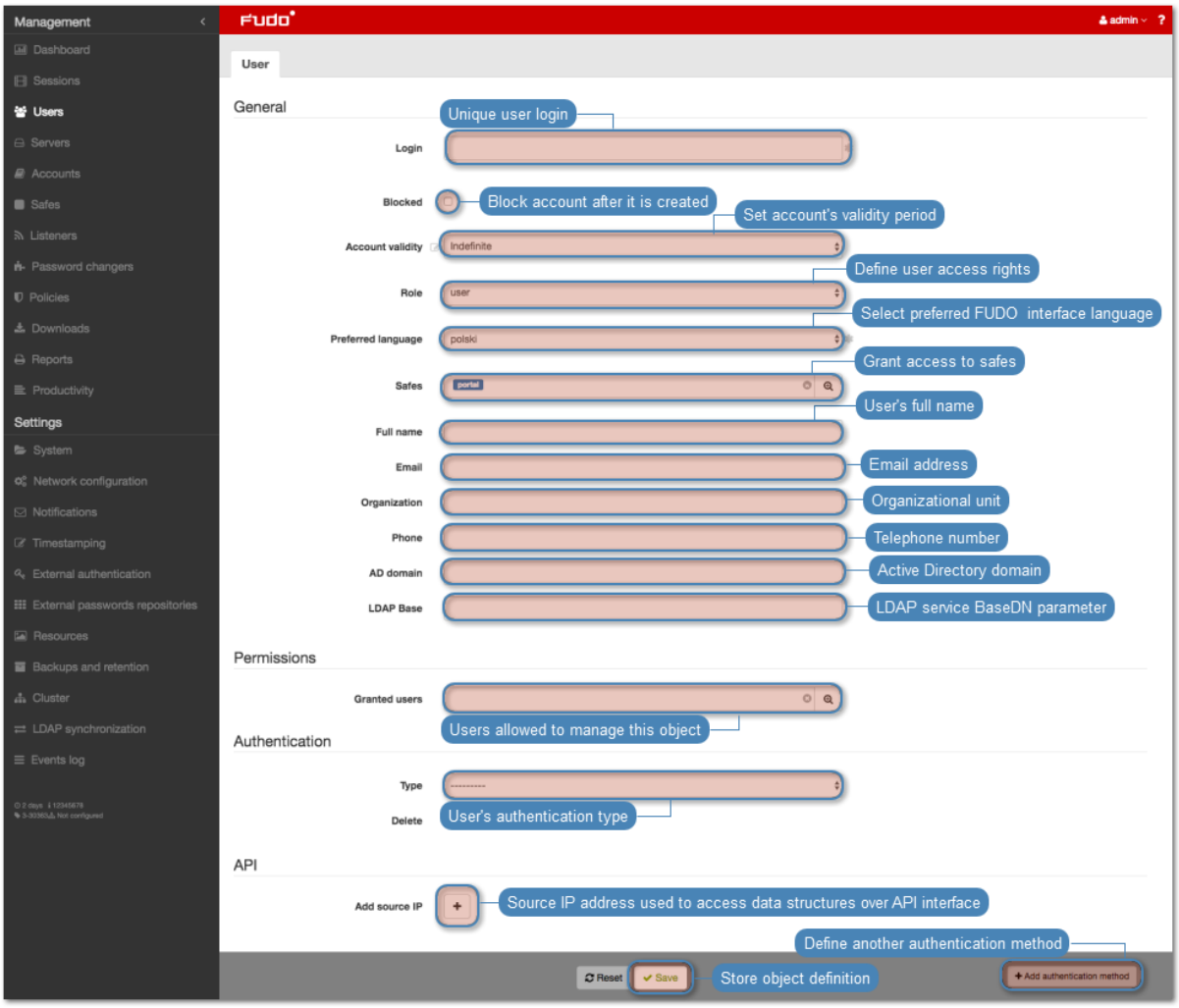
**Warning:** One-time passwords are used for implementing *AAPM* use case scenarios.

- Select `One-time password` from the *Type* drop-down list.

20. Click *+ Add authentication method* to define more authentication methods.

**Note:** When processing user authentication requests, Fudo PAM verifies login credentials against defined authentication methods in order in which those methods have been defined.

21. In the *API section*, click [+] and define IP address used by an external system to communicate with Fudo over API.
22. Click *Save*.



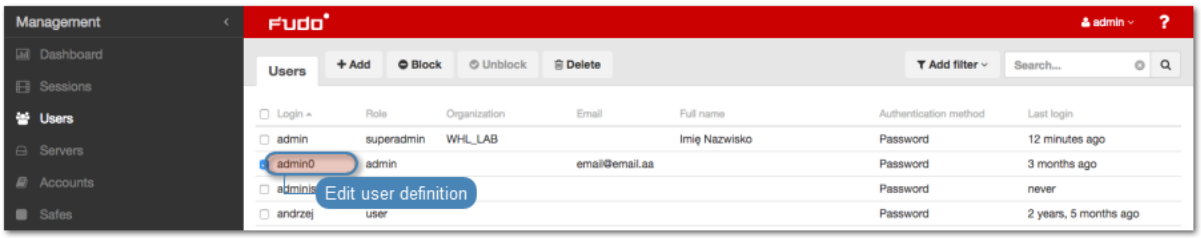

**Related topics:**

- *Authentication failures counter*
- *Users synchronization*
- *Data model*

- *Default domain*
- *System initiation*
- *Servers*
- *Accounts*
- *Approving pending connections*
- *Declining pending connections*

## 5.2 Editing a user

1. Select *Management* > *Users*.
2. Find and click desired user to access its configuration parameters.

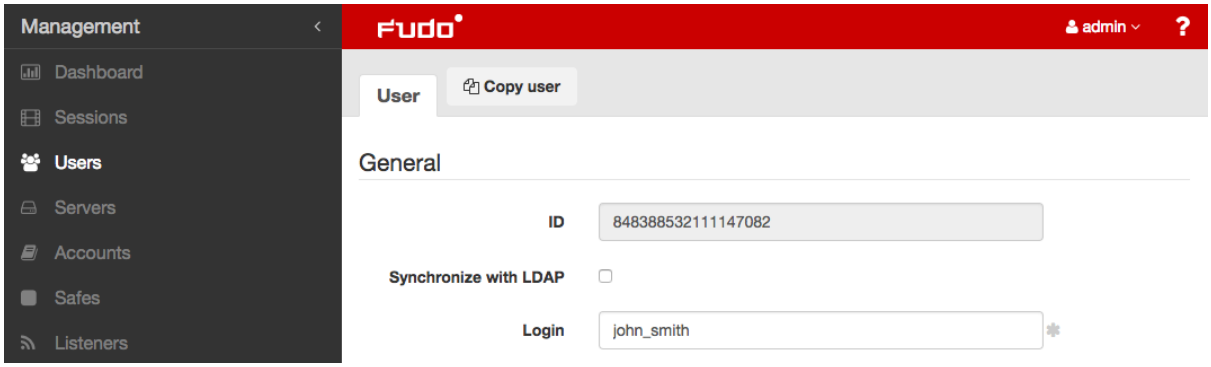



**Note:** Define filters to limit the number of objects displayed on the list.

3. Modify configuration values as needed.

**Note:**

- ID is a read-only, unique object identifier and it is assigned by Wheel Fudo PAM when object is created.




- Unsaved changes are marked with an icon.

4. Click *Save*.

**Related topics:**

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

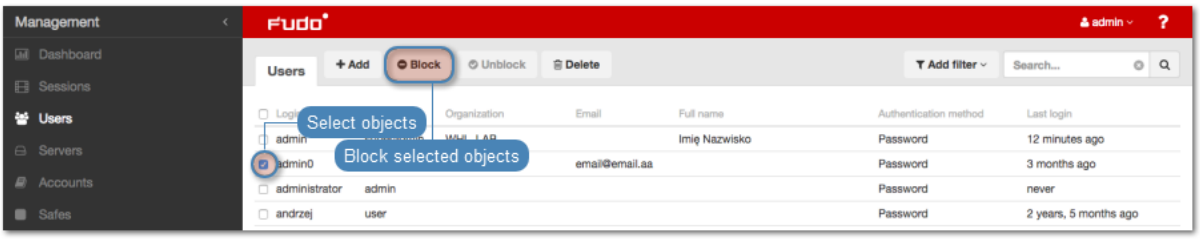
## 5.3 Blocking a user

**Warning:** Blocking a user will terminate its current connections.

1. Select *Management* > *Users*.
2. Find and select desired objects.

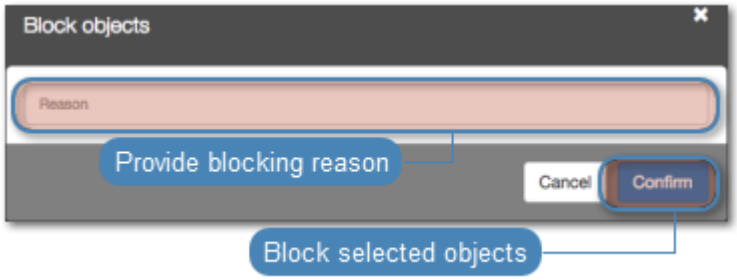
**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Block*.



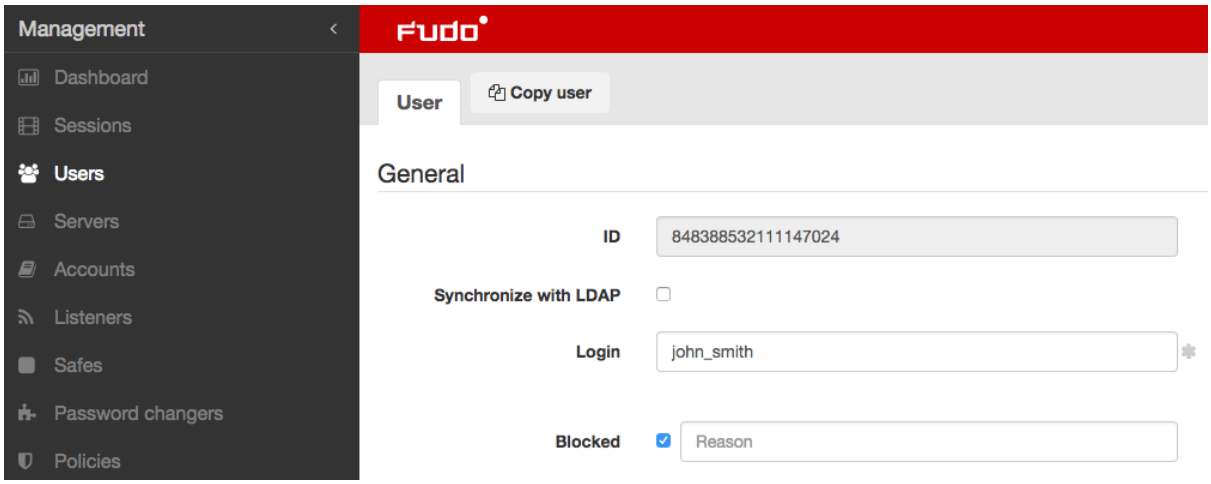

4. Optionally, provide blocking reason and click *Confirm*.

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




**Note:** Users can also be blocked by accessing the user object configuration form.

- Select the *Blocked* option.
- Provide an optional blocking reason.




- Click *Save*.

**Related topics:**

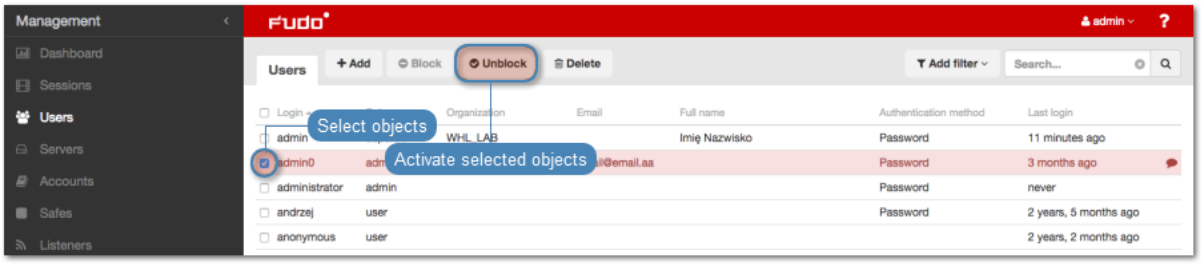
- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*
- *Accounts*

## 5.4 Unblocking a user

1. Select *Management* > *Users*.
2. Find and select desired objects.

**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Unblock*.




4. Click *Confirm* to unblock selected objects.

**Related topics:**

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

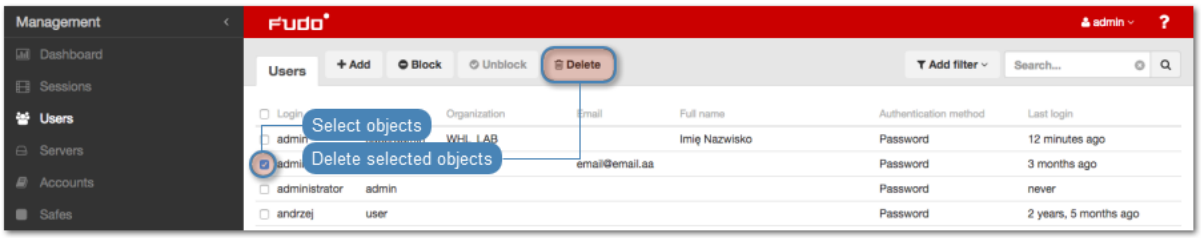
## 5.5 Deleting a user

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

1. Select *Management* > *Users*.
2. Find and select desired object.

**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Delete*.




4. Confirm deleting selected objects.

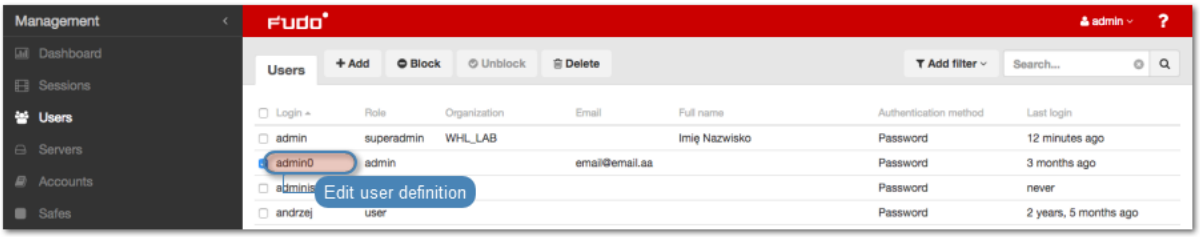
**Related topics:**

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

## 5.6 Time access policy

Wheel Fudo PAM can regulate access to safes based on time. To define time based safe access, proceed as follows.

1. Select *Management* > *Users*.
2. Find and click desired user to access its configuration parameters.




**Note:** Define filters to limit the number of objects displayed on the list.

3. Click desired safe object.

4. Select the *Blocked* option to disable access through given safe.

5. Provide *Valid from* and *Valid to* dates to define time interval when user is allowed to access servers through given safe.
6. Select the *Enable time policy* option.
7. Select the *Reveal password* option to allow user to see the passwords to accounts that are grouped in selected safe.

---

**Note:** Passwords can be viewed in *User Portal*.

---

8. Click the weekly calendar to define time interval.

9. Click *OK*.
10. Click *Save*.

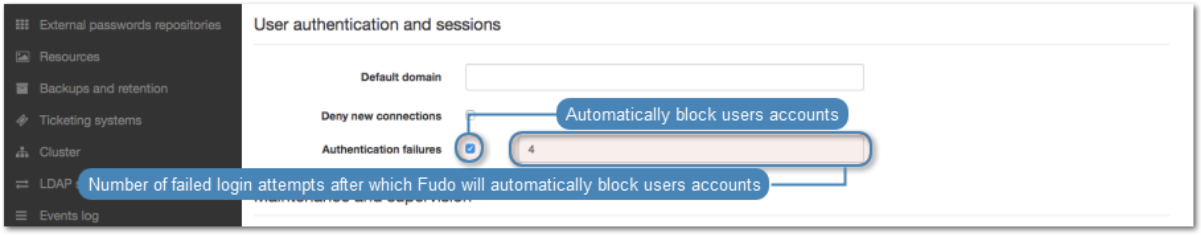
**Related topics:**

- *Creating a user*
- *ServiceNow - granting access*
- *Servers*
- *Accounts*

## 5.7 Authentication failures counter

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

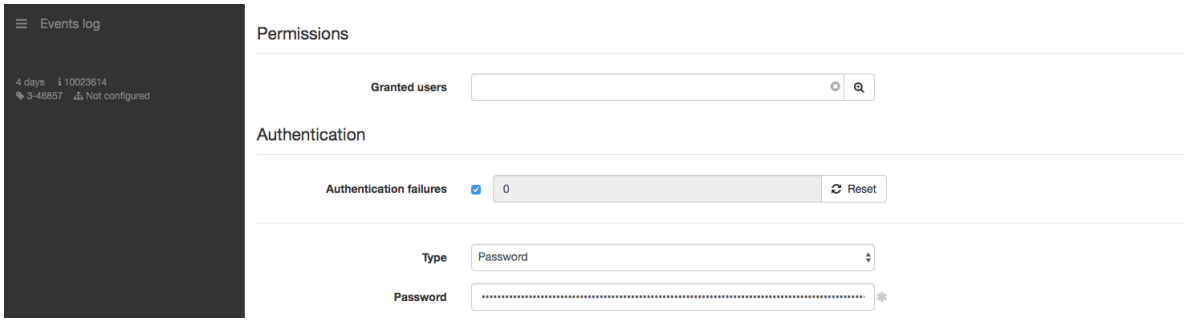
1. Select *Settings* > *System*.
2. In the *Authentication and sessions* section, select *Authentication failures* option.
3. Enter the number of failed login attempts after which the user account will be blocked.




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*

## 5.8 Roles

| Role | Access rights |
|---|---|
| user | • Connecting to servers through assigned safes.<br>• Loggin to the User Portal (requires adding the user to the `portal` safe)<br>• Fetching servers' passwords (requires additional access right). |
| service | Accessing SNMP information. |
| operator | • Logging in to the administration panel.<br>• Browsing objects: servers, users, safes, accounts, to which the user has been assigned sufficient access permisions.<br>• Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions.<br>• Generating reports on demand and subscribing to periodic reports.<br>• Activating/deactivating email notifications.<br>• Viewing live and archived sessions involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions.<br>• Converting sessions and downloading converted content involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions. |
| admin | • Logging in to the administration panel.<br>• Managing objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions.<br>• Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions.<br>• Generating reports on demand and subscribing to periodic reports.<br>• Activating/deactivating email notifications.<br>• Viewing live and archived sessions involving objects (user, safe, account, server), to which the user has been assigned management privileges.<br>• Converting sessions and downloading converted content involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions.<br>• Managing policies. |
| superadmin | • Full access rights to objects management.<br>• Full access rights to system configuration options. |

**Related topics:**

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

## 5.9 Users synchronization

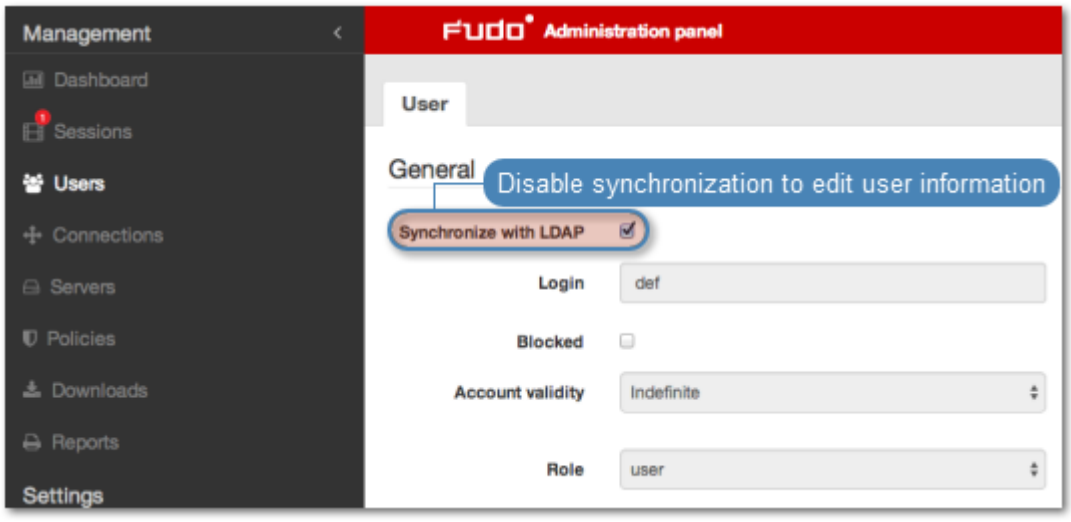
User is one of the fundamental *data model* entity. Only defined users are allowed to connect to monitored servers. Wheel Fudo PAM features automatic users synchronization service which enables importing users information from *Active Directory* servers or other servers compatible with the *LDAP* protocol.

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 Wheel Fudo PAM. The full synchronization process is triggered automatically once a day at 00:00, or can be triggered manually.

---

**Note:**

- Wheel Fudo PAM supports nested LDAP groups.
- Users imported from the catalog service cannot be edited. To edit a user definition imported from an LDAP or an AD server, disable the `Synchronize with LDAP` option for the given user.




---

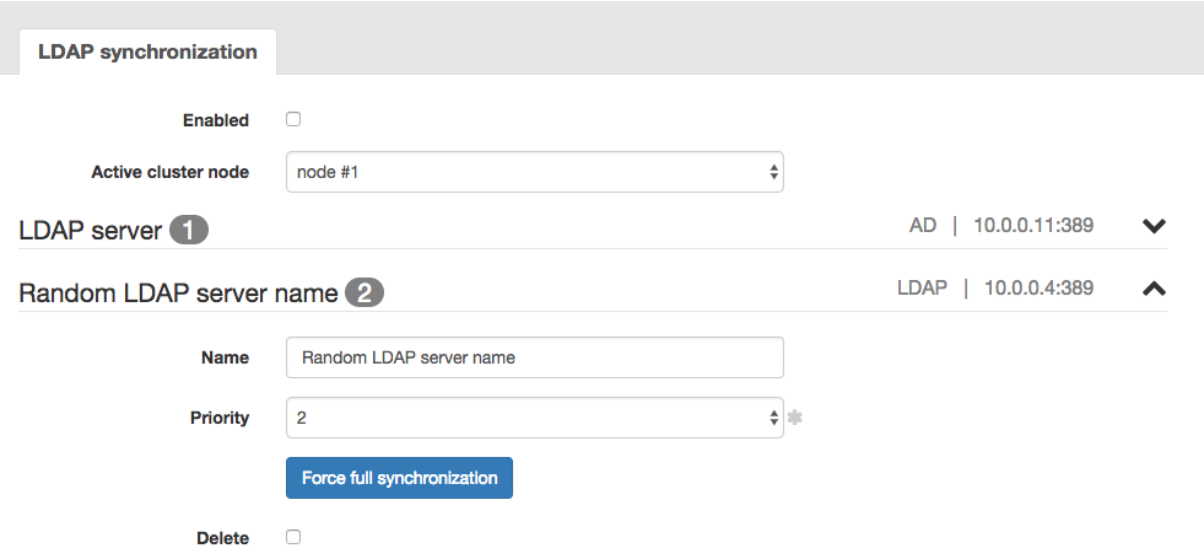
### Configuring users synchronization service

To enable users synchronization feature, proceed as follows.

1. Select *Settings* > *LDAP synchronization*.
2. Select *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 LDAP domain*.
5. Provide domain's name.
6. Define priority, determining the order in which domains are queried.

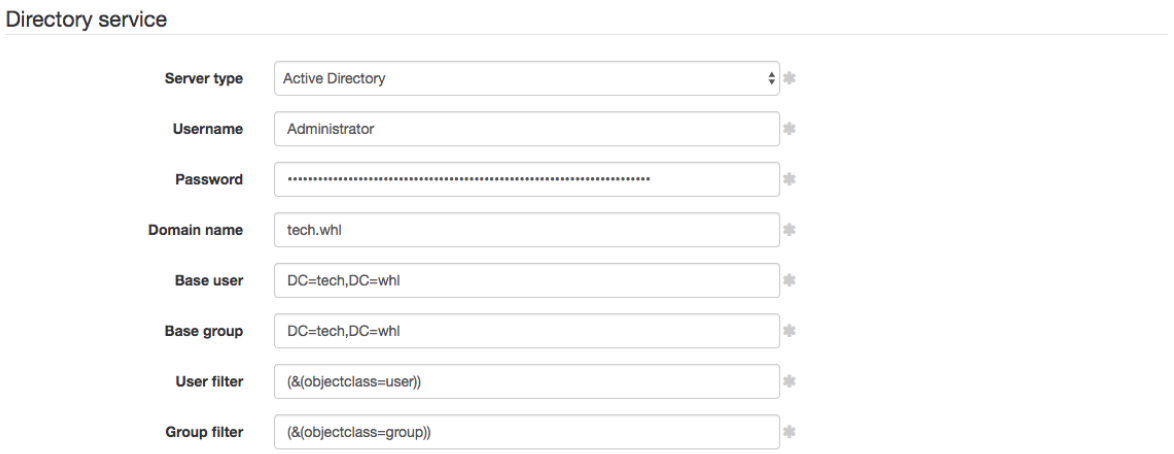
**Note:** Lower number translates to higher priority.




7. In the *Directory service* section, select data source type from the *Server type* drop-down list.
8. Provide the user authentication information 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:** DN parameter should not contain any white space characters.

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.




14. Click + in the *LDAP controllers* section 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.

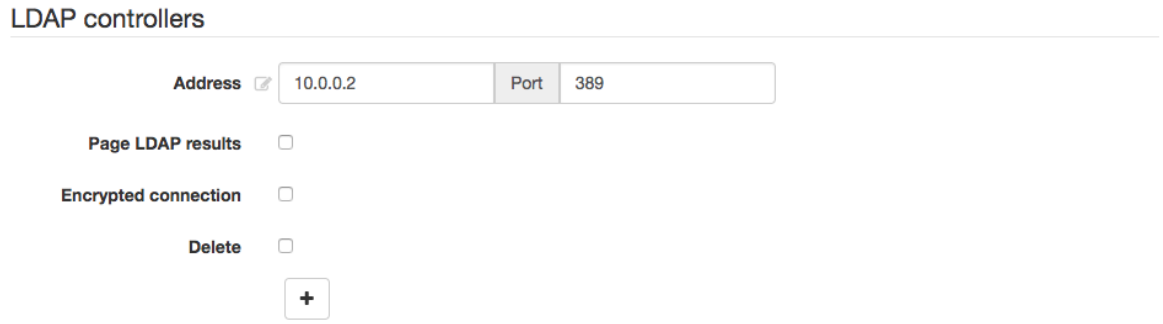
---

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

---

**Note:** Click + to add more directory servers.

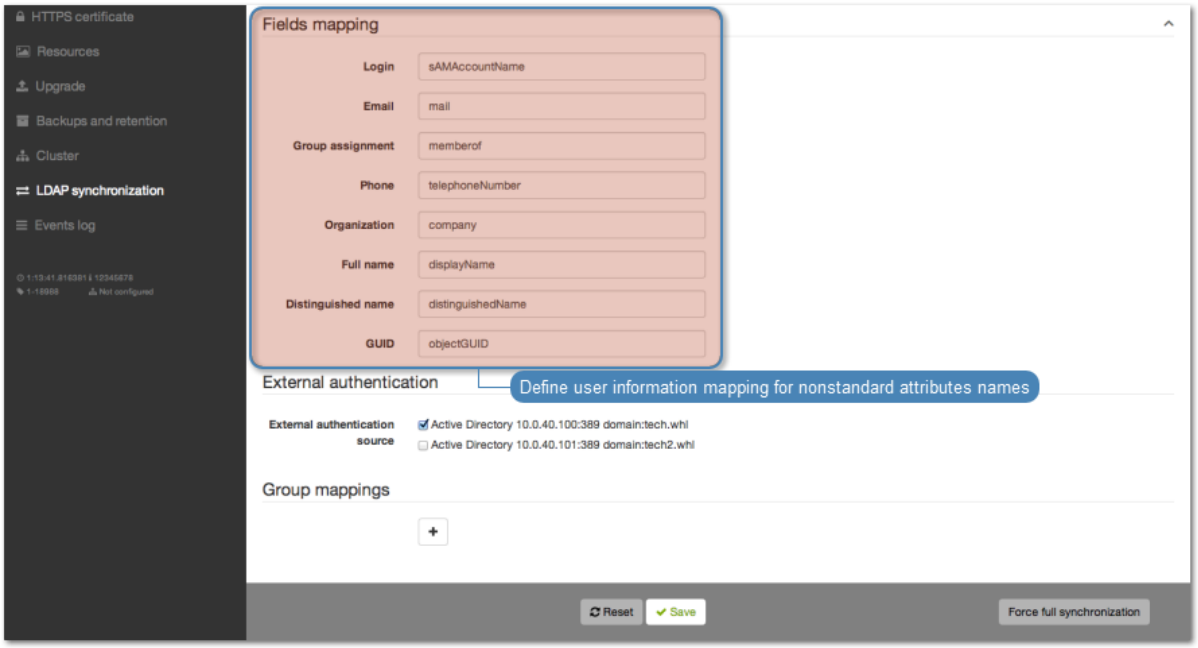
---



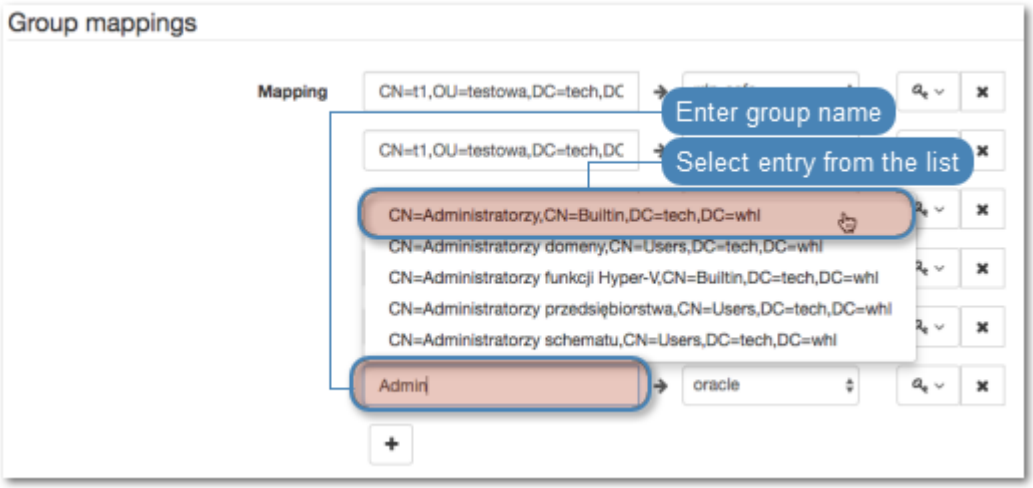

18. Define user information mapping.

---

**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. Click + in the *Groups mapping* section to define user groups to safes assignment.
20. Type in user group and select desired entry.

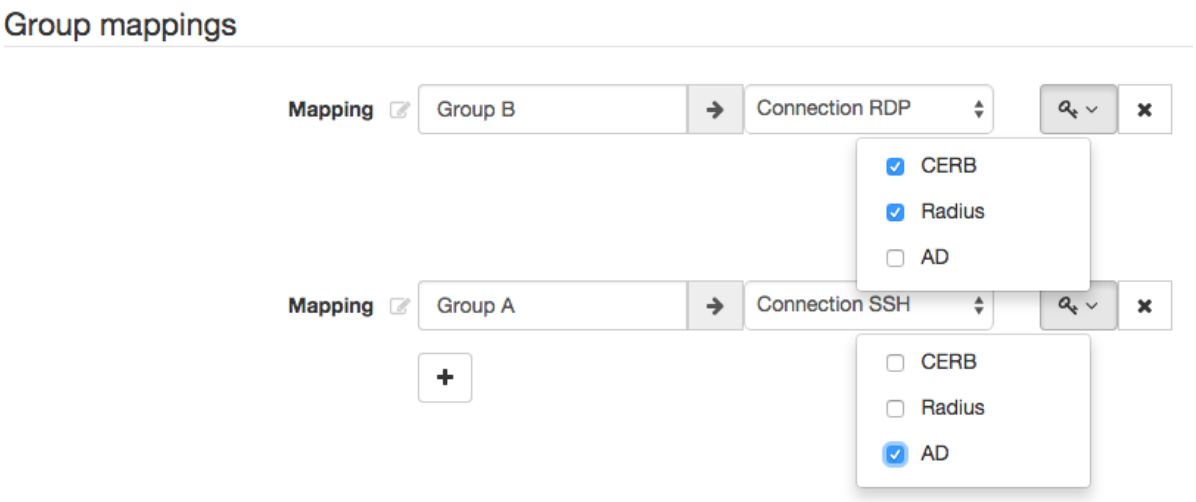



21. Assign safes to user groups.
22. Assign external authentication sources to user groups.

**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, Wheel Fudo PAM 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, Wheel Fudo PAM will send requests to external authentication sources in the following order:

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

---

23. Click *Save*.

---

**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.

---

**Related topics:**

- *User authentication against external LDAP server*
- *Users management*
- *Servers management*
- *Accounts*

## 5.10 Adding a mobile device

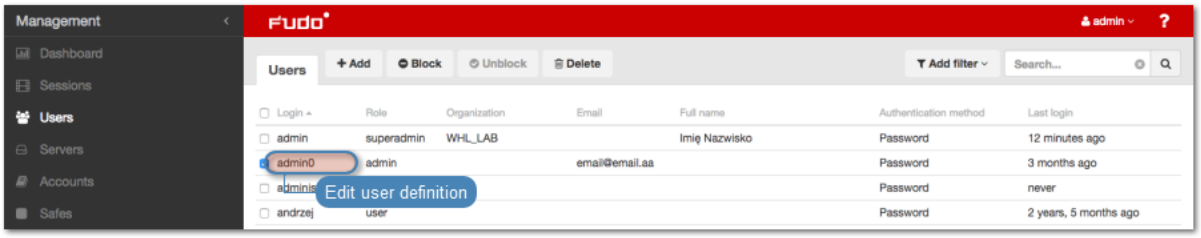
A mobile device enables accepting/rejecting access to servers, accessing which require administrator's approval.

---

**Note:** Before adding a mobile device a proxy service must be configured. For more information on setting up proxy for 4-Eyes authentication, refer to *Proxy servers configuration* topic.

---

1. Login to Wheel Fudo PAM administration panel using login credentials of the user that you want to add a mobile device to.
2. Select *Management* > *Users*.
3. Browse the list and click the user object definition.

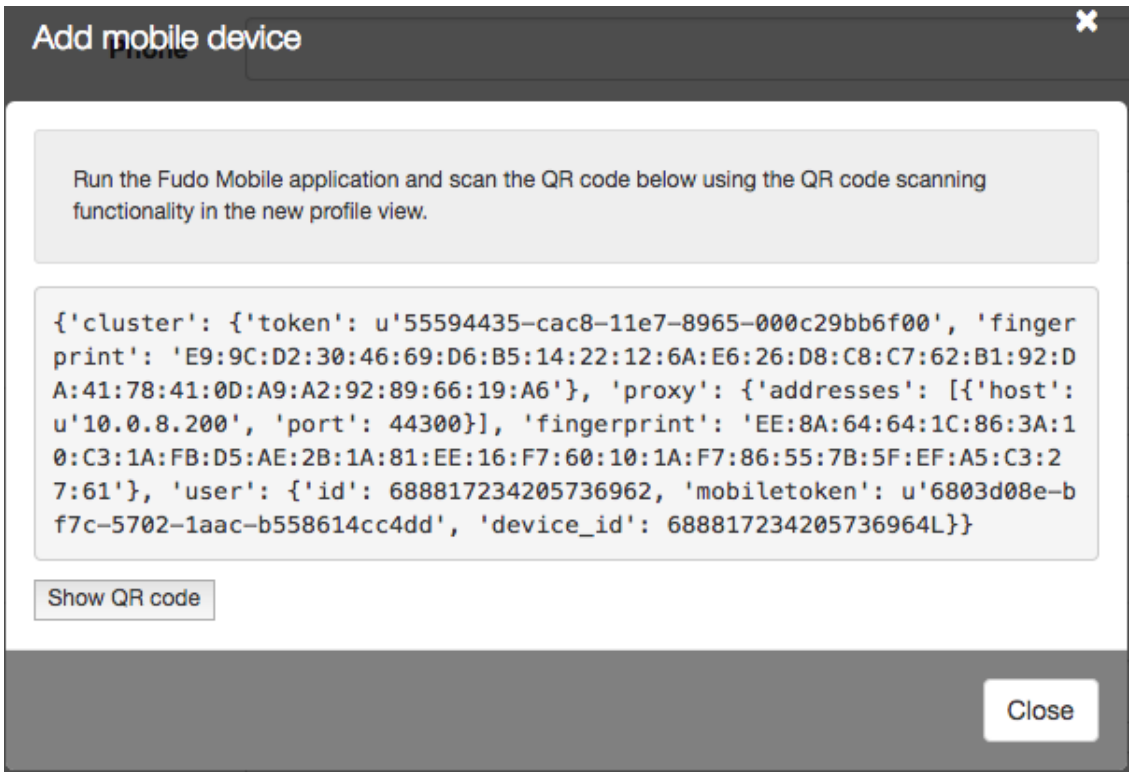



**Note:** Define filters to limit the number of objects displayed on the list.

4. In the *Fudo Mobile* section, click *Add device*.

5. Launch *Fudo Mobile* application.
6. Select + in the top right corner to create new profile.
7. Select *Scan* option and scan the QR code.

**Note:** Alternatively, click *Show JSON data*, select *Paste* and paste profile data.



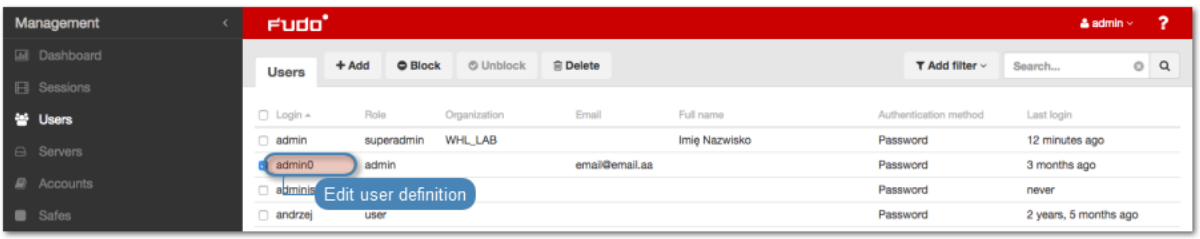

8. Define profile name and select *Save*.
9. Click *OK* to hide the QR code modal window.
10. Click *Save* to store changes in user account.

**Related topics:**

- *User authentication methods and modes*
- *Proxy servers configuration*
- *Removing paired mobile device*

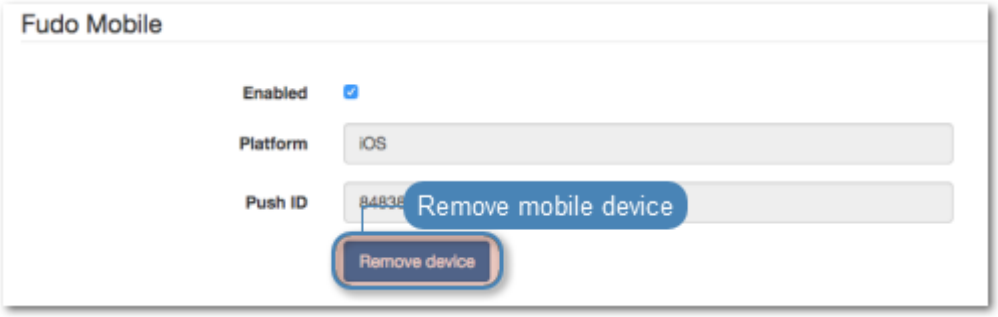
## 5.11 Removing paired mobile device

1. Select *Management* > *Users*.
2. Find and click desired user to access its configuration parameters.




**Note:** Define filters to limit the number of objects displayed on the list.

3. In the *Fudo Mobile* section, click *Remove device*.




4. Click *Confirm* to proceed with device removal.
5. Click *Save*.

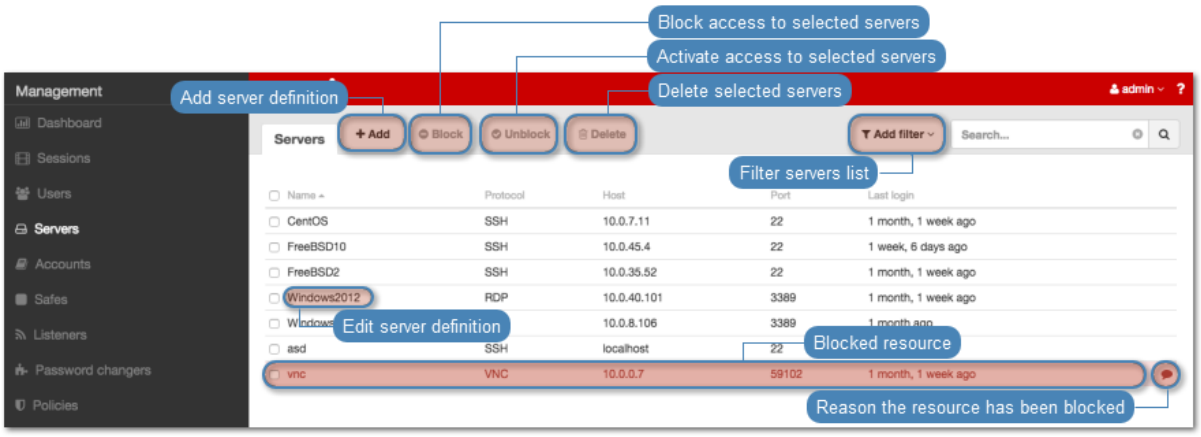
**Related topics:**

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

ROZDZIAŁ 6

# Servers

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

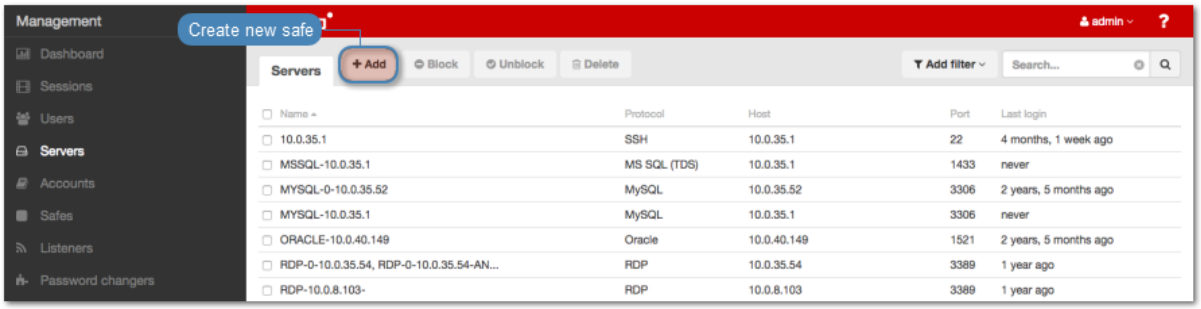



## 6.1 Creating a server

### 6.1.1 Static server

#### 6.1.1.1 Creating a Citrix server

1. Select *Management* > *Servers*.
2. Click + *Add*.




3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `Citrix StoreFront (HTTP)` from the *Protocol* drop-down list.
6. 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.
7. Enter optional description, which will help identifying this server object.
8. In the *Permissions* section, add users allowed to manage this object.
9. In the *Destination host* section, enter server's IP address and port number.
10. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

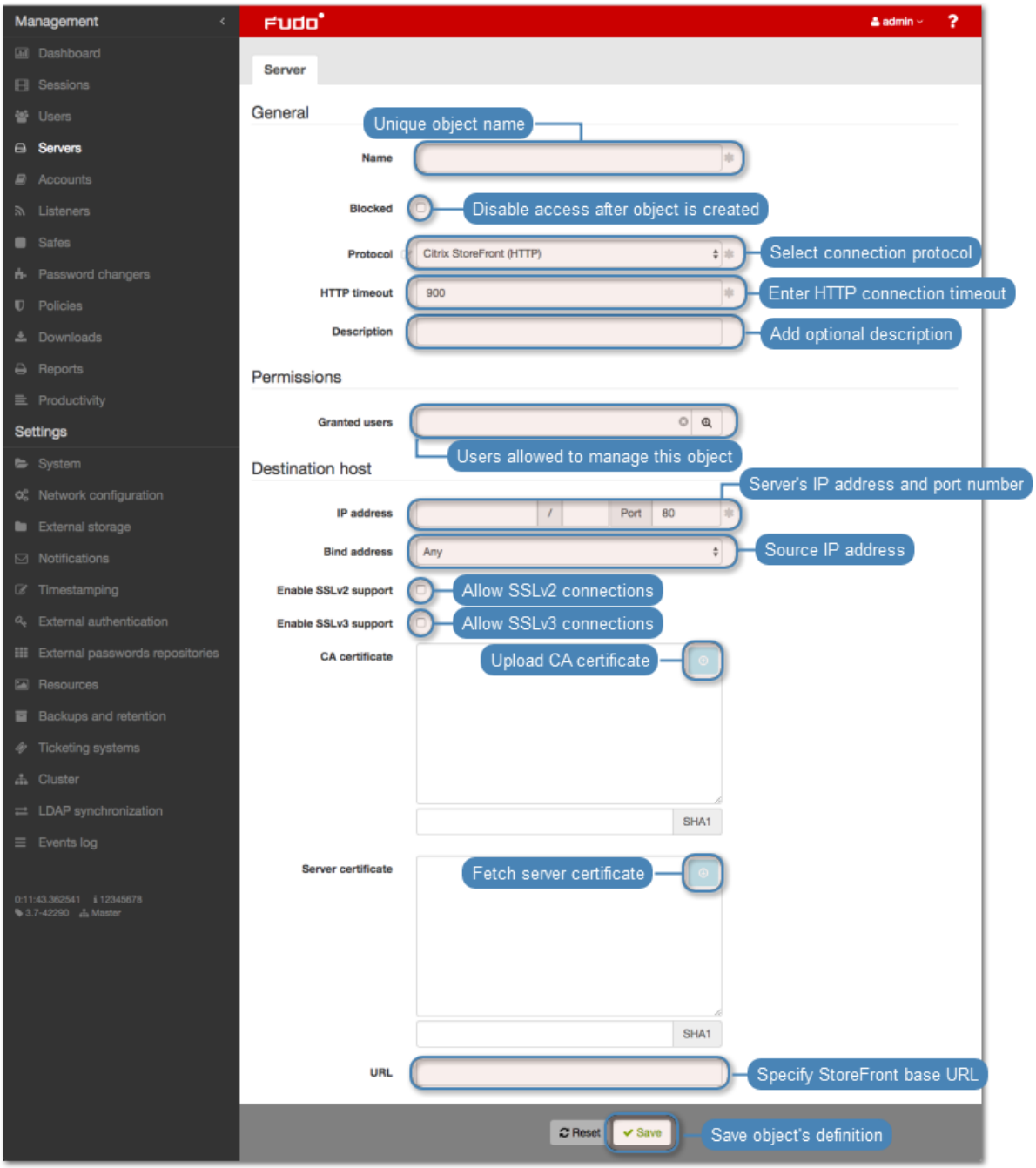
---

**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.

---

11. In the URL field, enter Citrix StoreFront base URL.
12. Select *Enable SSLv2 support* to allow SSL v2 encrypted connections.
13. Select *Enable SSLv3 support* to allow SSL v3 encrypted connections.
14. Click to upload CA certificate.
15. Click to download server key.
16. Click *Save*.




**Related topics:**

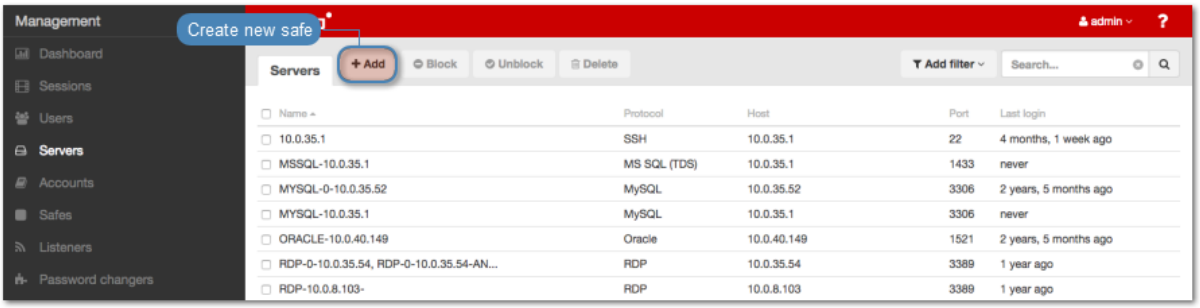
- *Data model*
- *Creating a Citrix listener*
- *ICA via Citrix StoreFront*
- *Citrix StoreFront (HTTP)*
- *ICA*
- *ICA configuration file*

### 6.1.1.2 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.

1. Select *Management* > *Servers*.
2. Click *+ Add*.



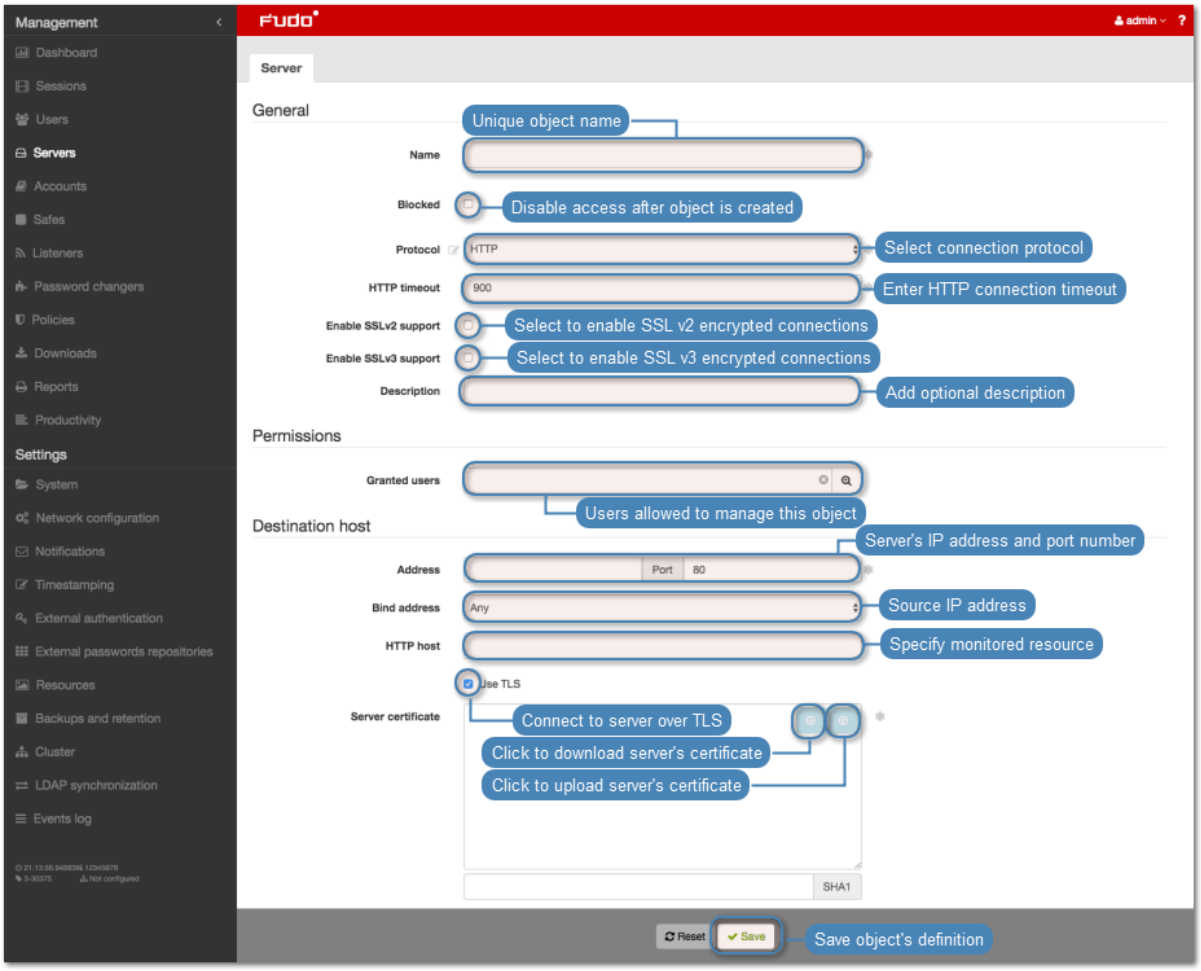

3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `HTTP` from the *Protocol* drop-down list.
6. Enter value of the *HTTP timeout* parameter, determining the time period of inactivity (expressed in seconds), after which the user will have to authenticate again.
7. Enter optional description, which will help identifying this server object.
8. In the *Permissions* section, add users allowed to manage this object.
9. In the *Destination host* section, enter server's IP address and port number.
10. From the *Bind address* drop-down list, select Wheel Fudo PAM 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.

11. Specify the monitored resource in the *HTTP host* field.
12. Select the *Use TLS* options to connect to monitored server over TLS.
13. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
14. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
15. Click to upload CA certificate.

16. Click to download server key.
17. Click *Save*.

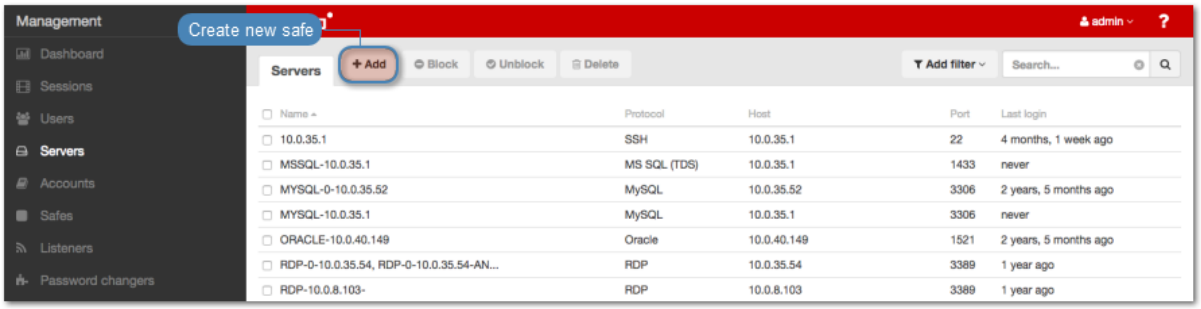



**Related topics:**

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

### 6.1.1.3 Creating an ICA server

1. Select *Management* > *Servers*.
2. Click *+ Add*.




3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `ICA` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

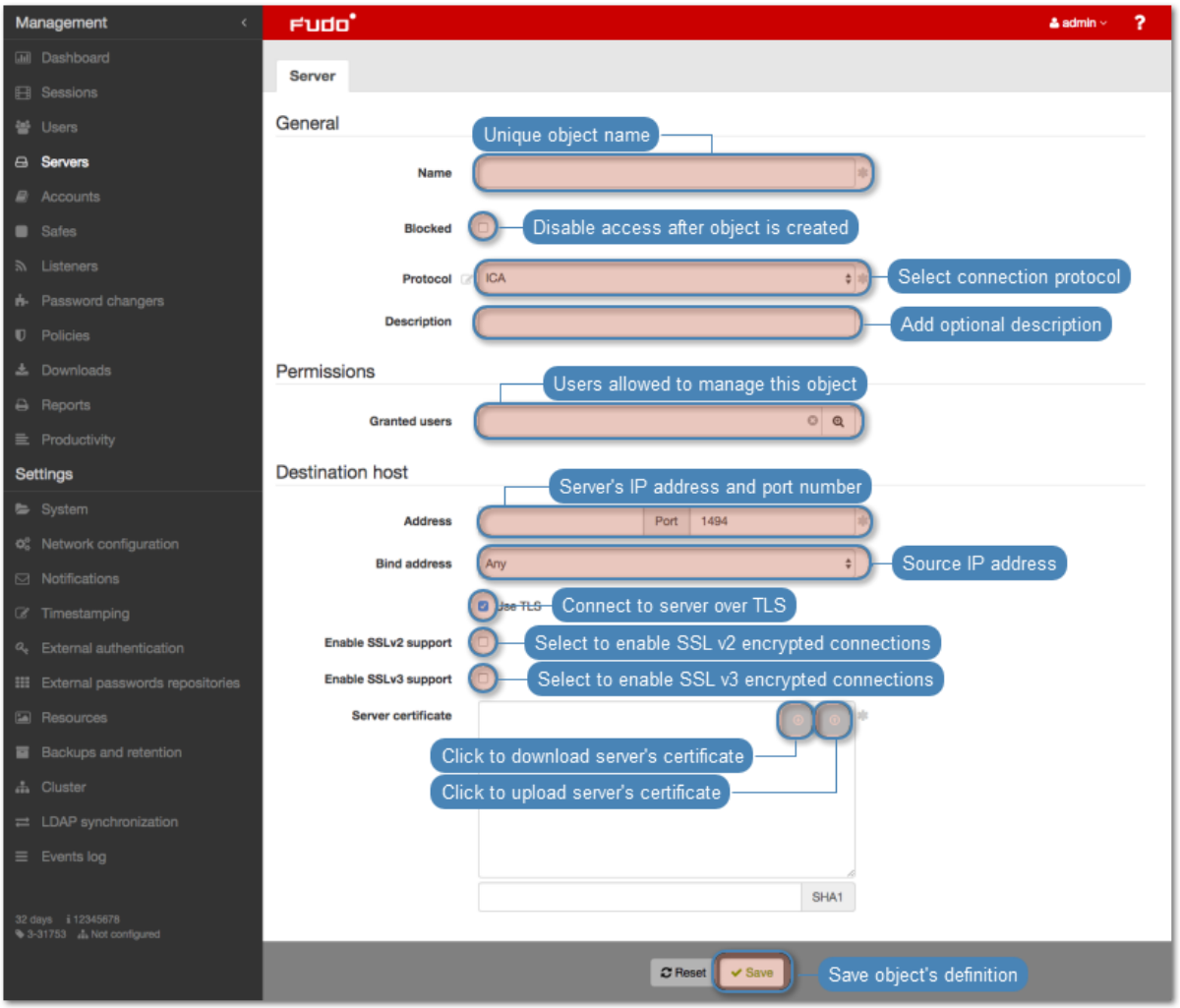
---

**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. Select the *Use TLS* options to connect to monitored server over TLS.
11. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
12. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
13. Click to upload CA certificate.
14. Click to download server key.
15. Click *Save*.




**Related topics:**

- *Data model*
- *ICA*
- *Creating an ICA listener*
- *ICA configuration file*
- *ICA*

### 6.1.1.4 Creating a Modbus server

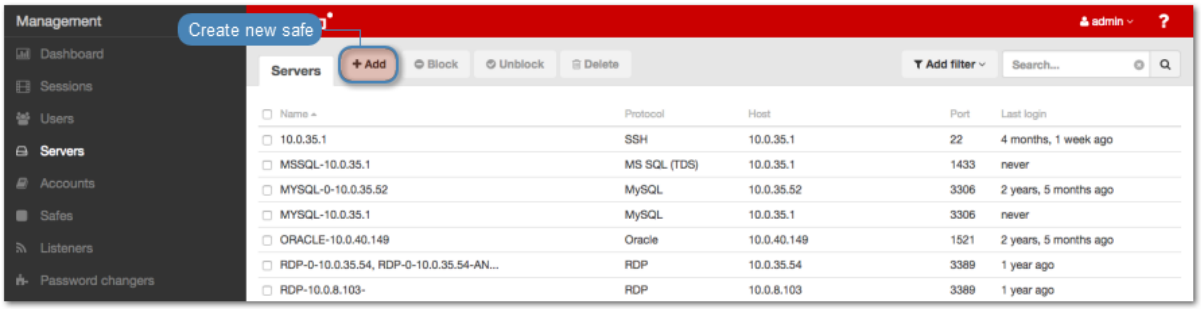
---

**Note:**

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

---

1. Select *Management* > *Servers*.
2. Click *+ Add*.




3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `Modbus` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

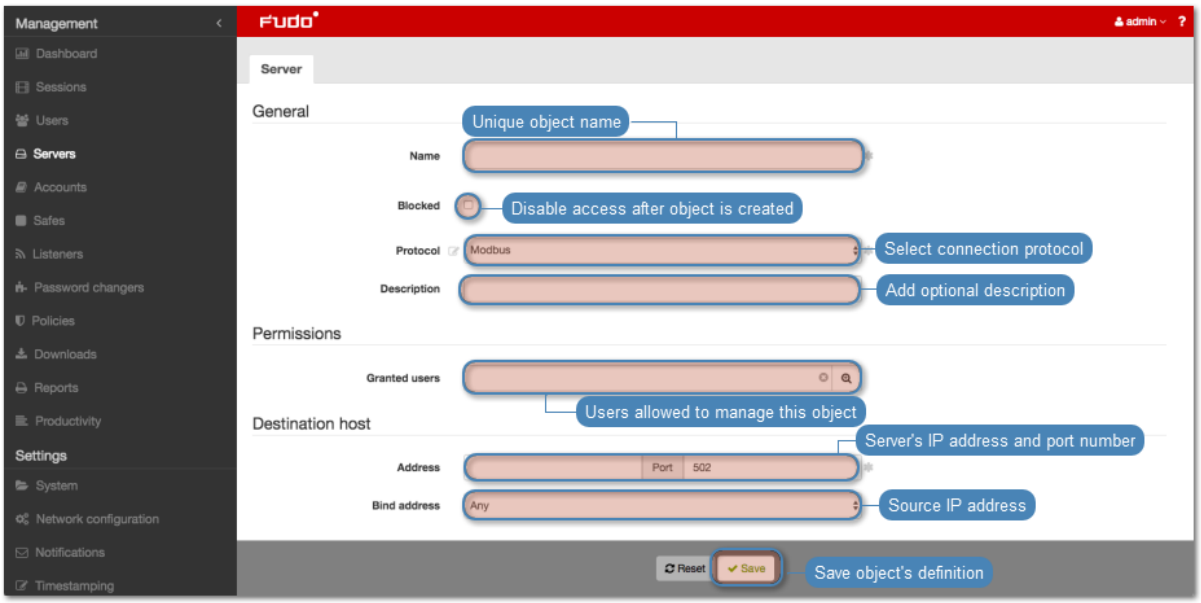
---

**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. Click *Save*.




**Related topics:**

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

#### 6.1.1.5 Creating a MS SQL server

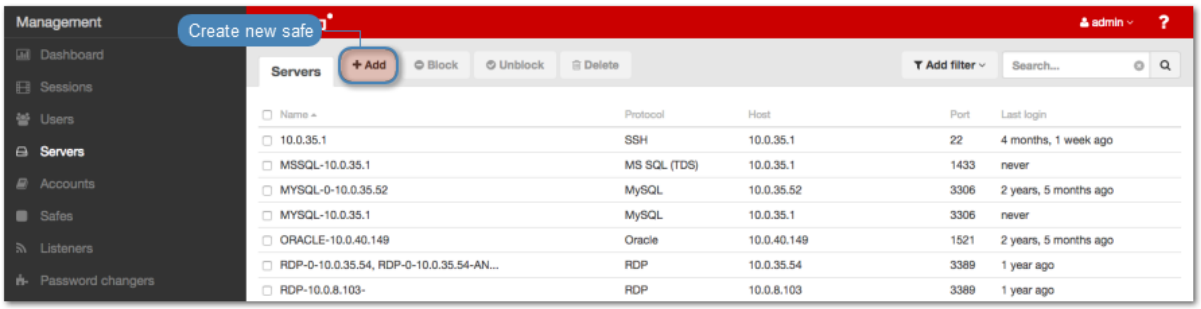
---

**Note:**

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

---

1. Select *Management* > *Servers*.
2. Click *+ Add*.



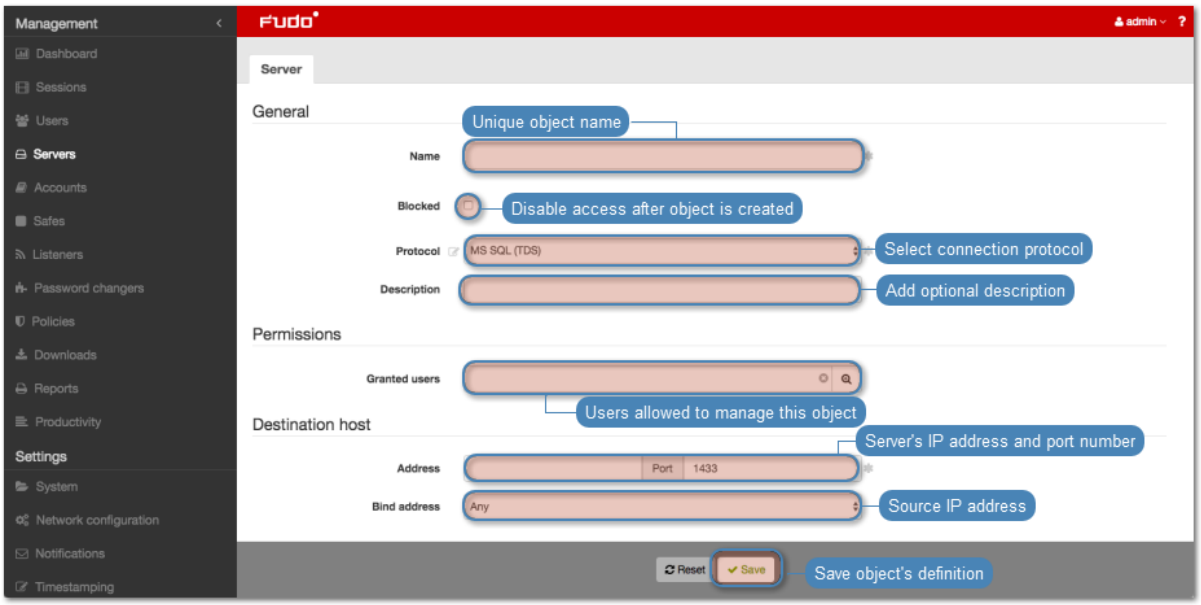

3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `MS SQL (TDS)` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM 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. Click *Save*.




**Related topics:**

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

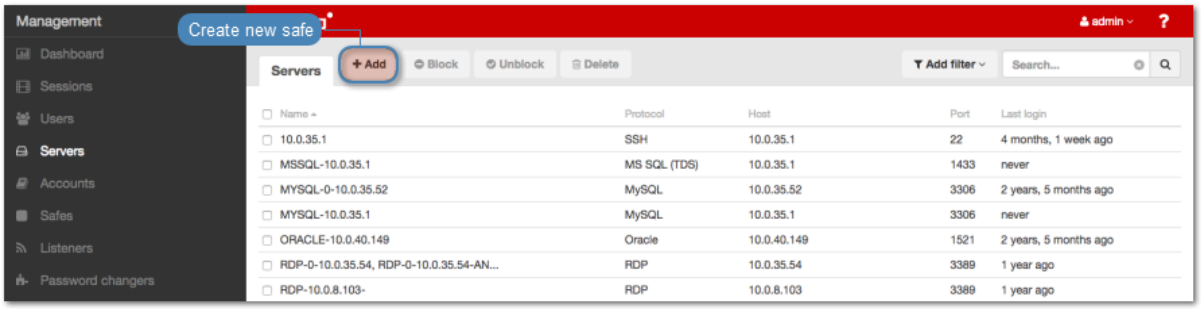
#### 6.1.1.6 Creating a MySQL server

**Warning:** Please note that the MySQL server `caching_sha2_password` plugin isn't supported by Fudo PAM. Supportable MySQL plugins by Fudo PAM 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. Select *Management* > *Servers*.
2. Click *+ Add*.




3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `MySQL` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

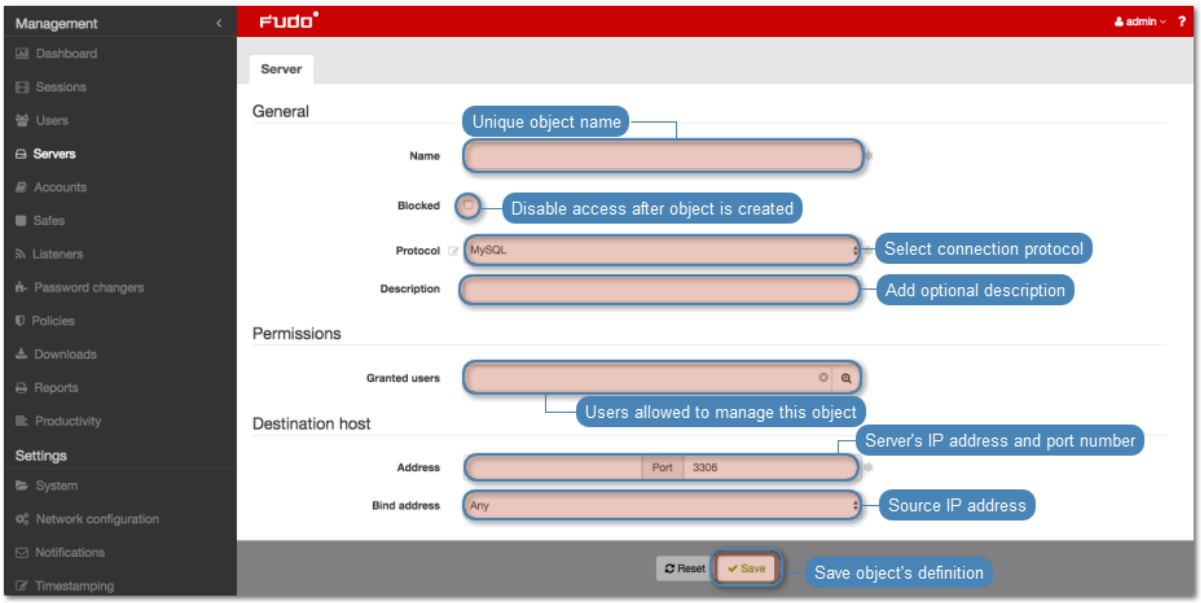
---

**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. Click *Save*.




**Related topics:**

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

#### 6.1.1.7 Creating an Oracle server

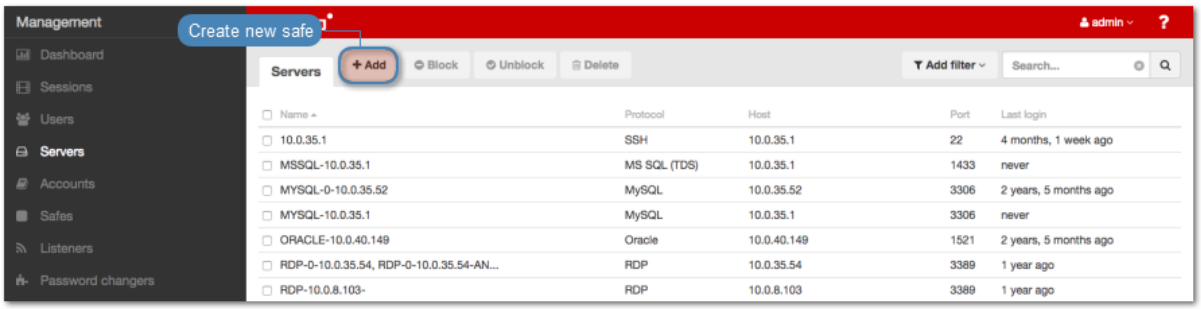
---

**Note:**

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

---

1. Select *Management* > *Servers*.
2. Click *+ Add*.



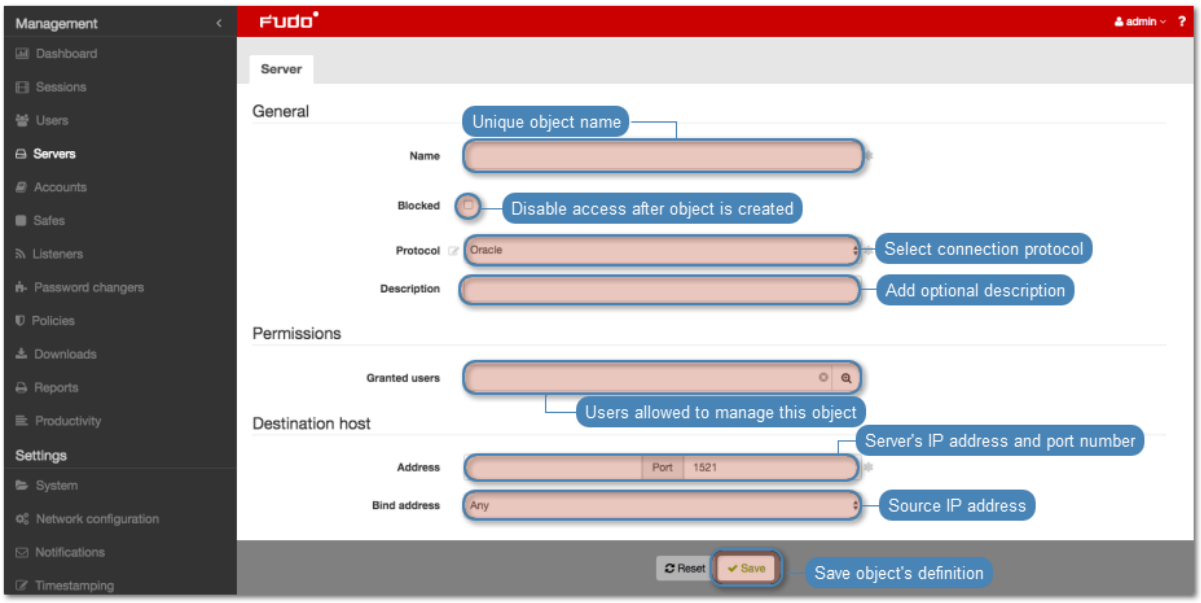

3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `Oracle` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM 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. Click *Save*.




**Related topics:**

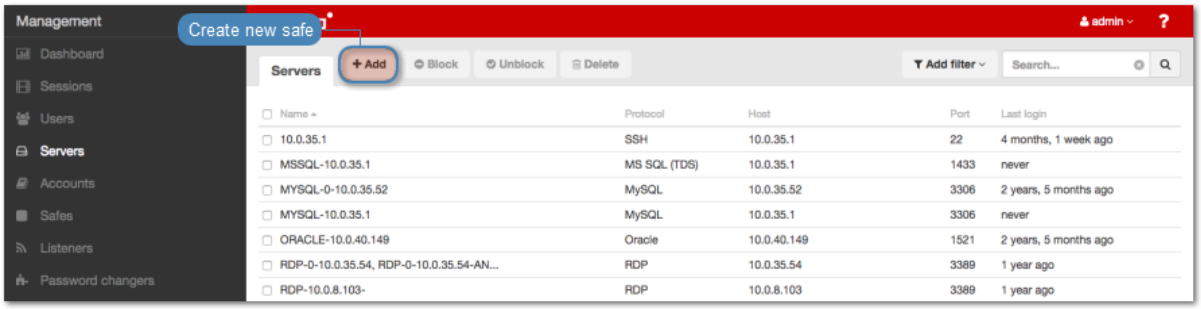
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

#### 6.1.1.8 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.

1. Select *Management* > *Servers*.
2. Click + *Add*.




3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `RDP` from the *Protocol* drop-down list.
6. From the `Security` drop-down list, select RDP connection security mode.
7. Enter optional description, which will help identifying this server object.
8. In the *Permissions* section, add users allowed to manage this object.
9. In the *Destination host* section, enter server's IP address and RDP service port number.
10. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

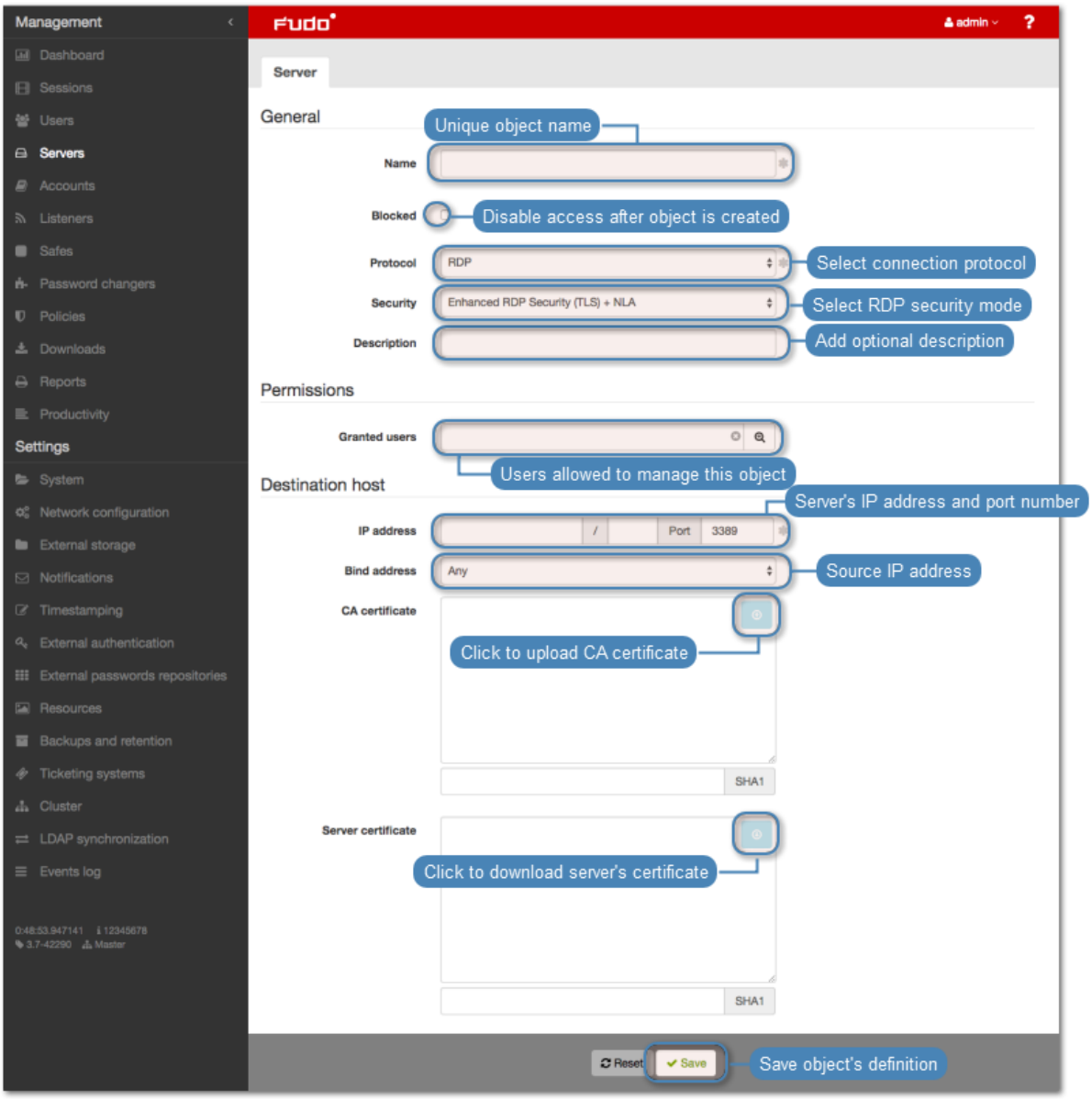
---

**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. Click to upload CA certificate.
11. Click to download server key.
12. Click *Save*.




**Related topics:**

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

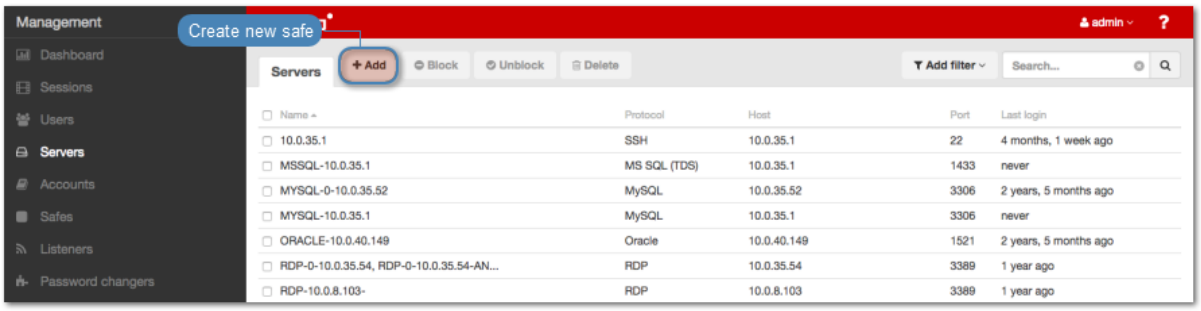
#### 6.1.1.9 Creating an SSH server

**Note:**

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

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

1. Select *Management* > *Servers*.
2. Click + *Add*.

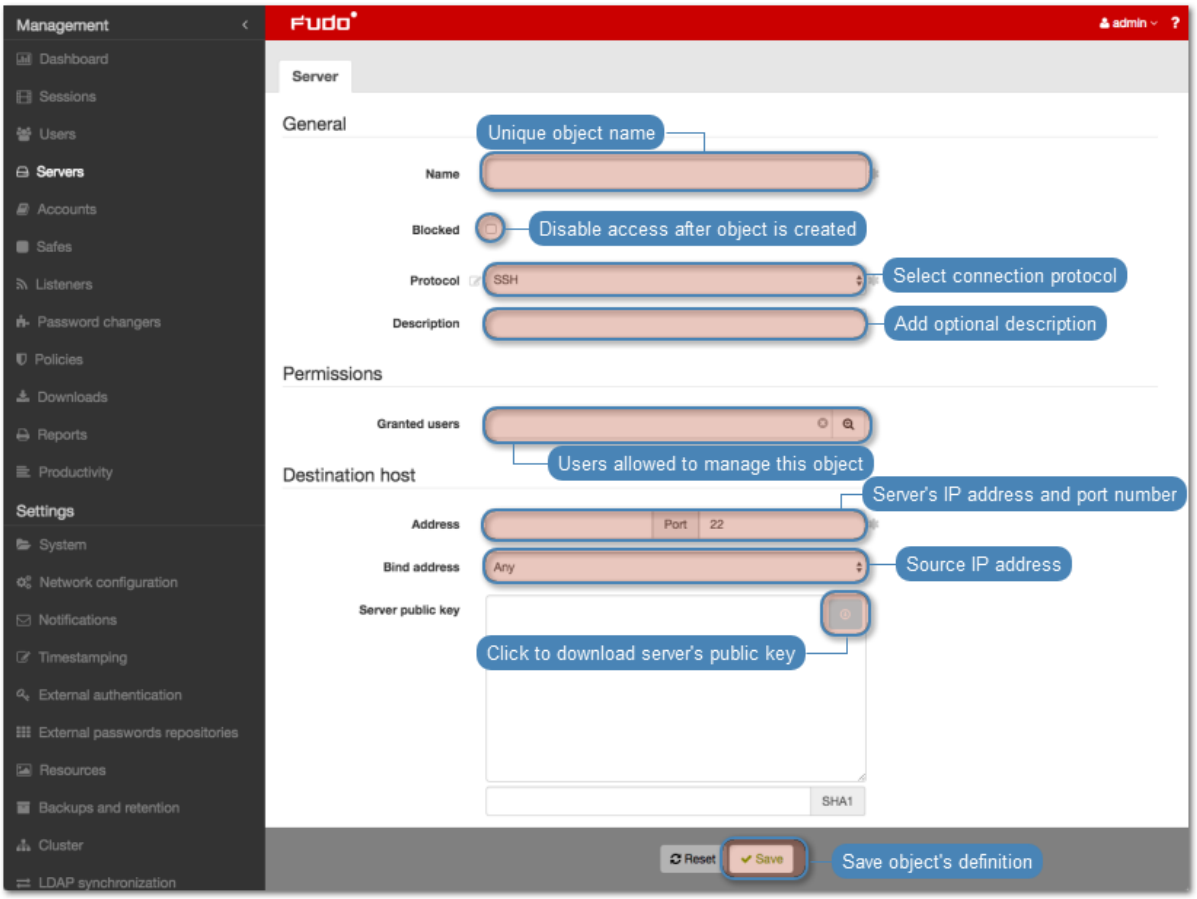



3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `SSH` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and SSH service port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM 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. Click the fetch key icon to download server's public key.
11. Click *Save*.




**Related topics:**

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

#### 6.1.1.10 Creating a Telnet server

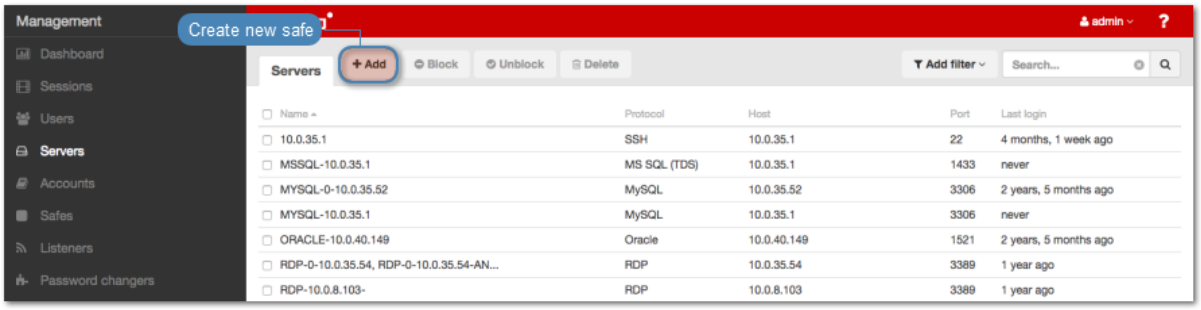
---

**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 Wheel Fudo PAM and then to connect to the target host.

---

1. Select *Management* > *Servers*.
2. Click *+ Add*.




3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `Telnet` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

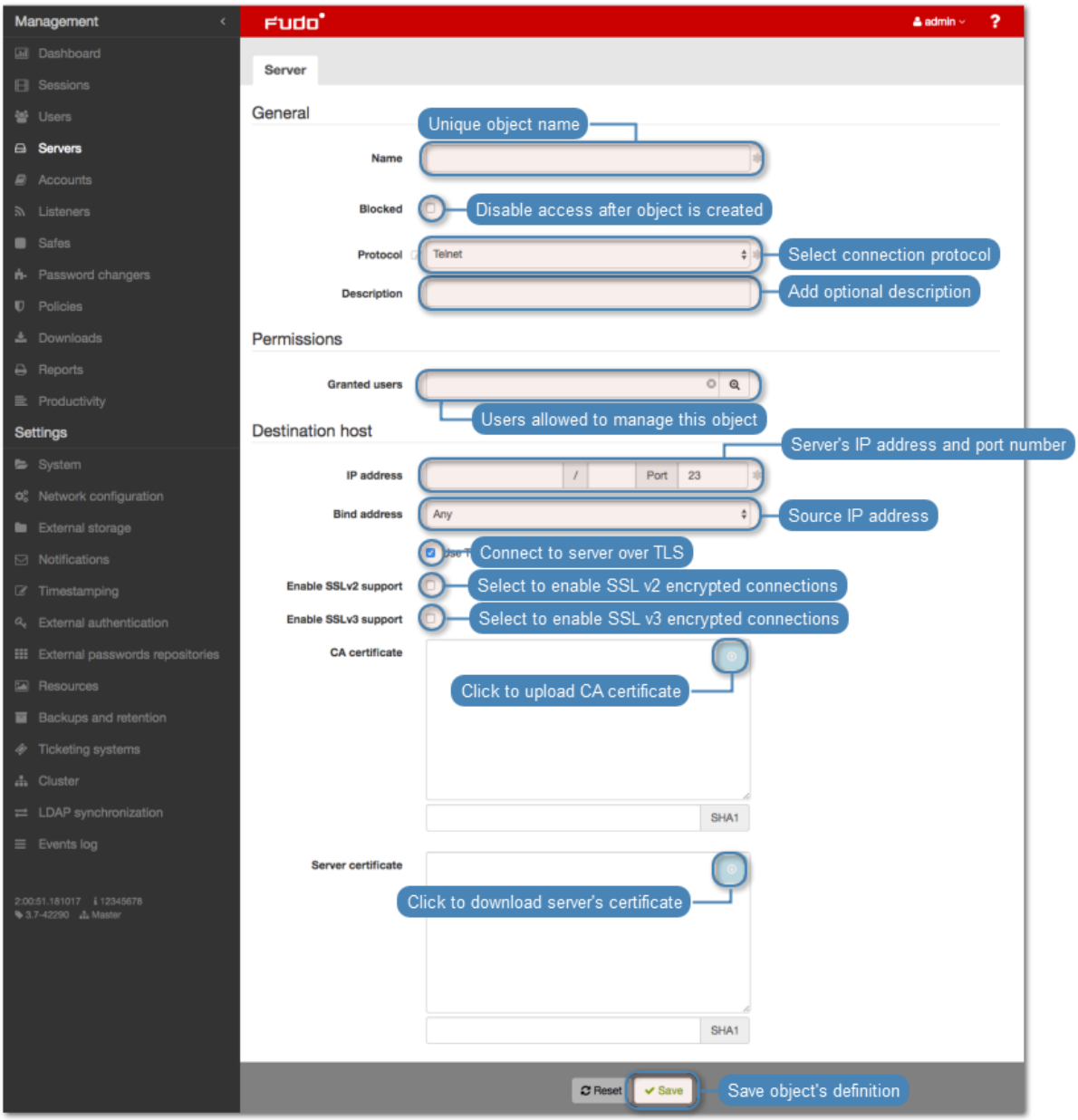
---

**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. Select the *Use TLS* options to connect to monitored server over TLS.
11. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
12. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
13. Click to upload CA certificate.
14. Click to download server key.
15. Click *Save*.




**Related topics:**

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

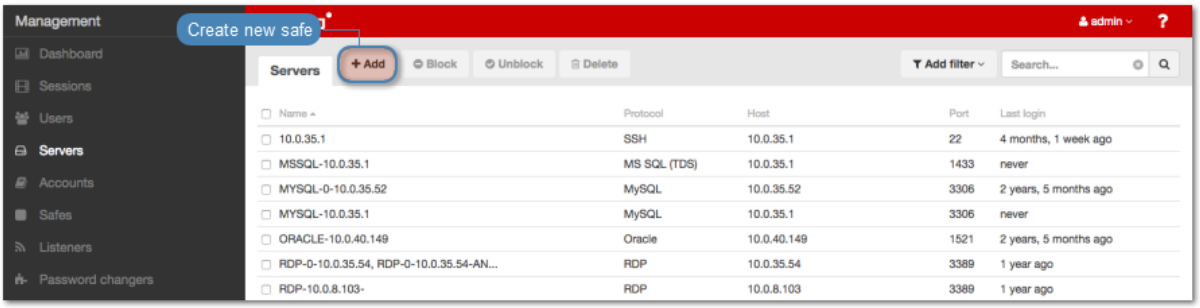
#### 6.1.1.11 Creating a Telnet 3270 server

**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 Wheel Fudo PAM and then to connect to the target host.

---

1. Select *Management* > *Servers*.
2. Click + *Add*.




3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `Telnet 3270` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

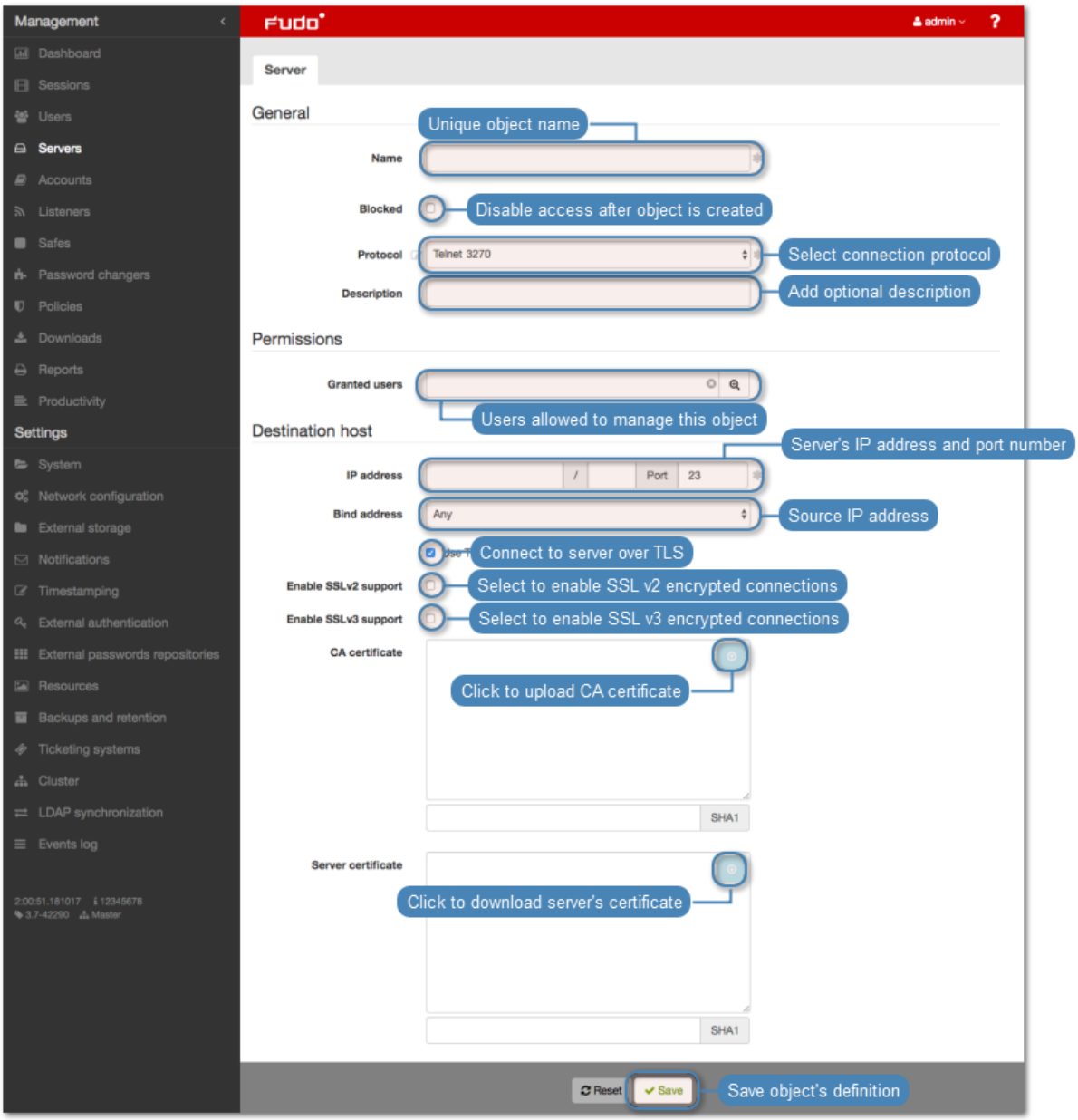
---

**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. Select the *Use TLS* options to connect to monitored server over TLS.
11. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
12. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
13. Click to upload CA certificate.
14. Click to download server key.
15. Click *Save*.




**Related topics:**

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

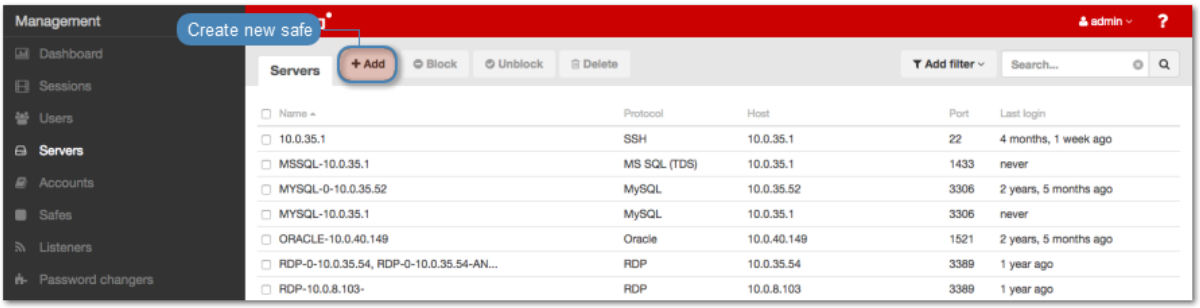
#### 6.1.1.12 Creating a Telnet 5250 server

**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 Wheel Fudo PAM and then to connect to the target host.

---

1. Select *Management* > *Servers*.
2. Click + *Add*.




3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `Telnet 5250` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

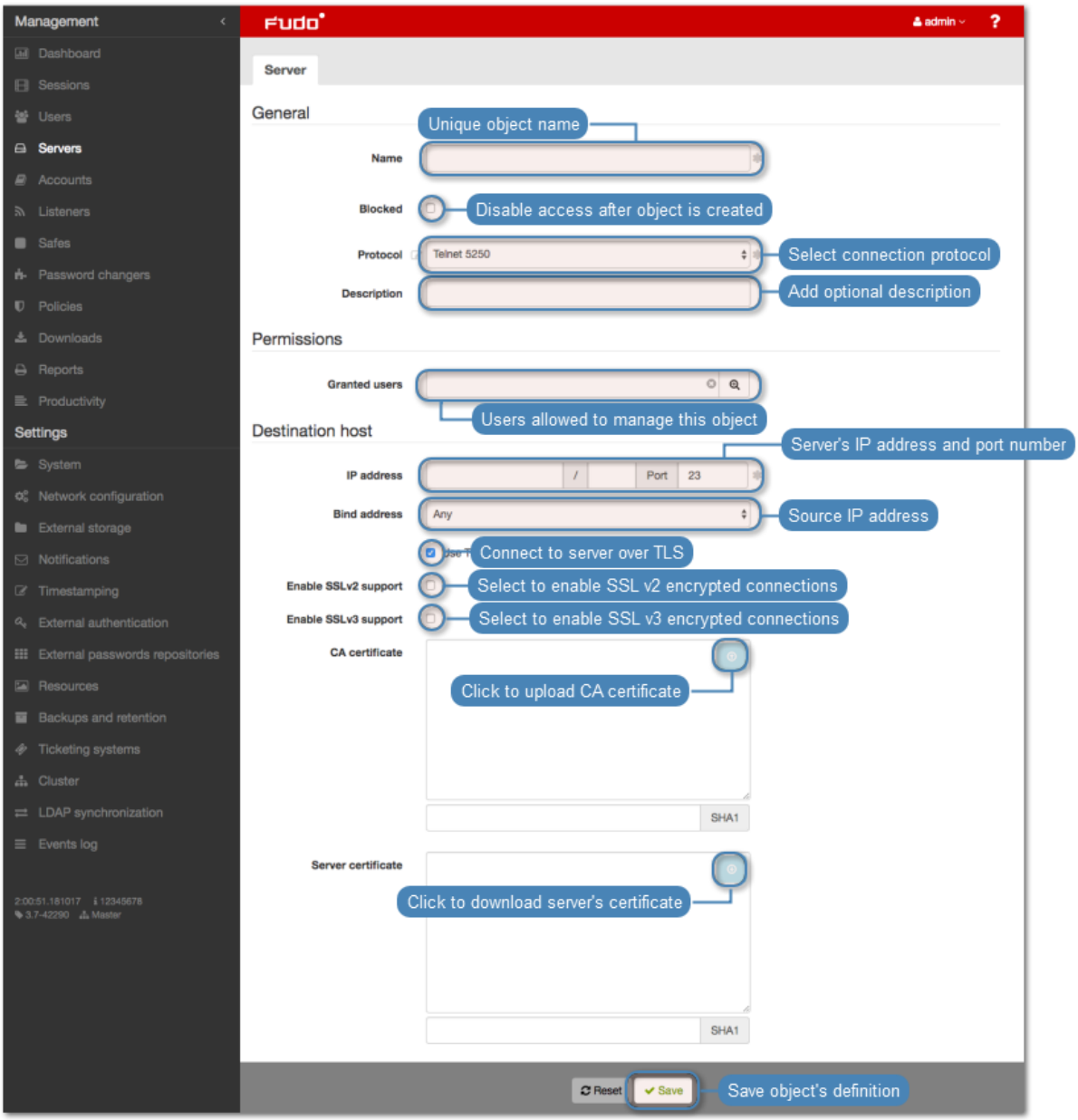
---

**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. Select the *Use TLS* options to connect to monitored server over TLS.
11. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
12. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
13. Click to upload CA certificate.
14. Click to download server key.
15. Click *Save*.




**Related topics:**

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

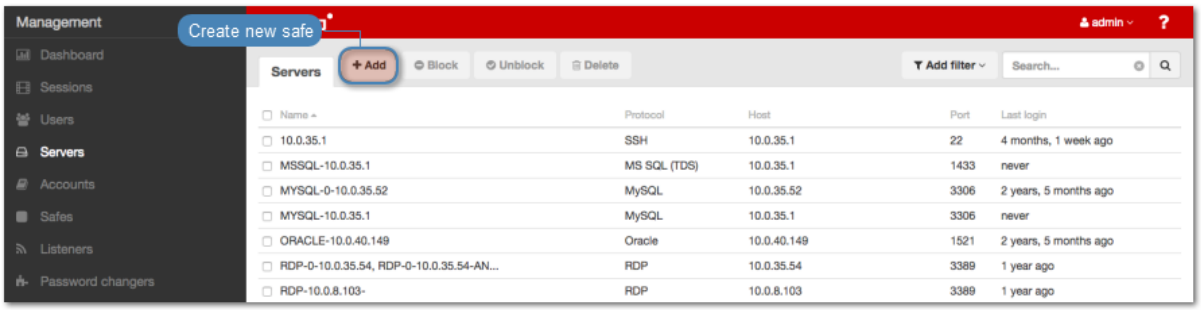
#### 6.1.1.13 Creating a VNC server

---

**Note:**

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

1. Select *Management* > *Servers*.
2. Click *+ Add*.

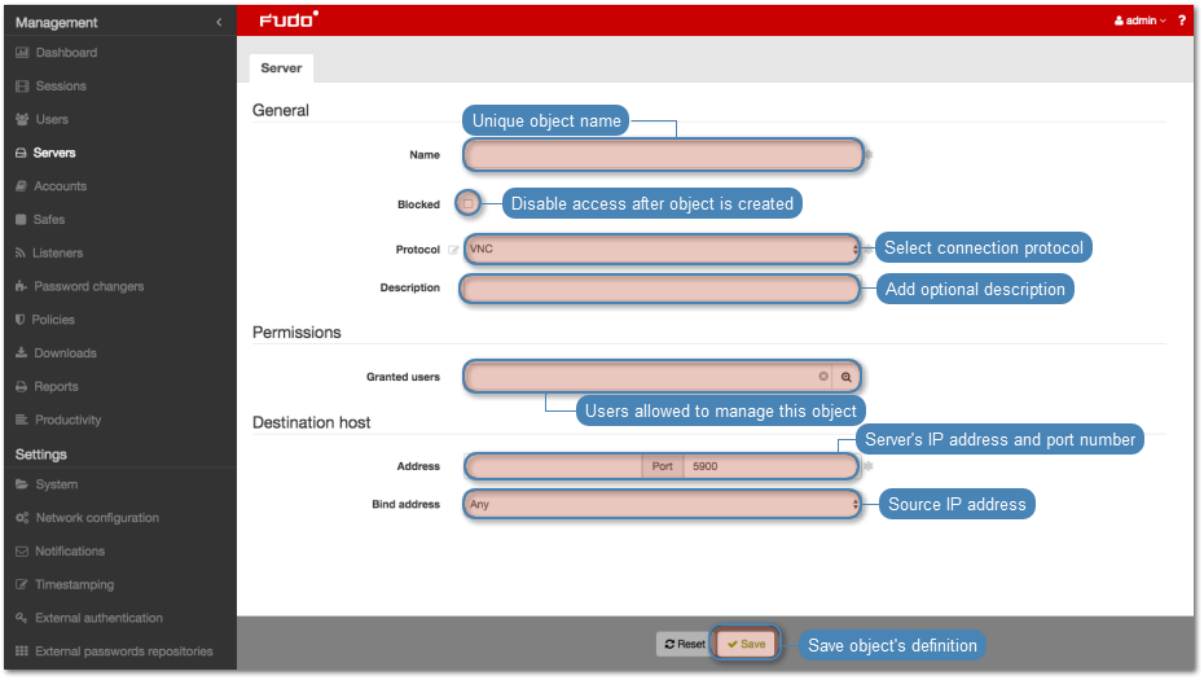



3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `VNC` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM 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. Click *Save*.

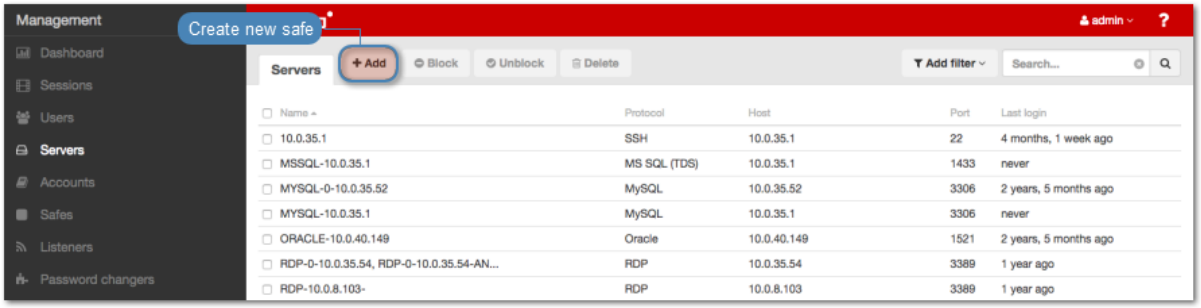



**Related topics:**

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

### 6.1.1.14 Creating a TCP server

1. Select *Management* > *Servers*.
2. Click *+ Add*.




3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `TCP` from the *Protocol* drop-down list.
6. Enter optional description, which will help identifying this server object.

7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Destination host* section, enter server's IP address and port number.
9. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

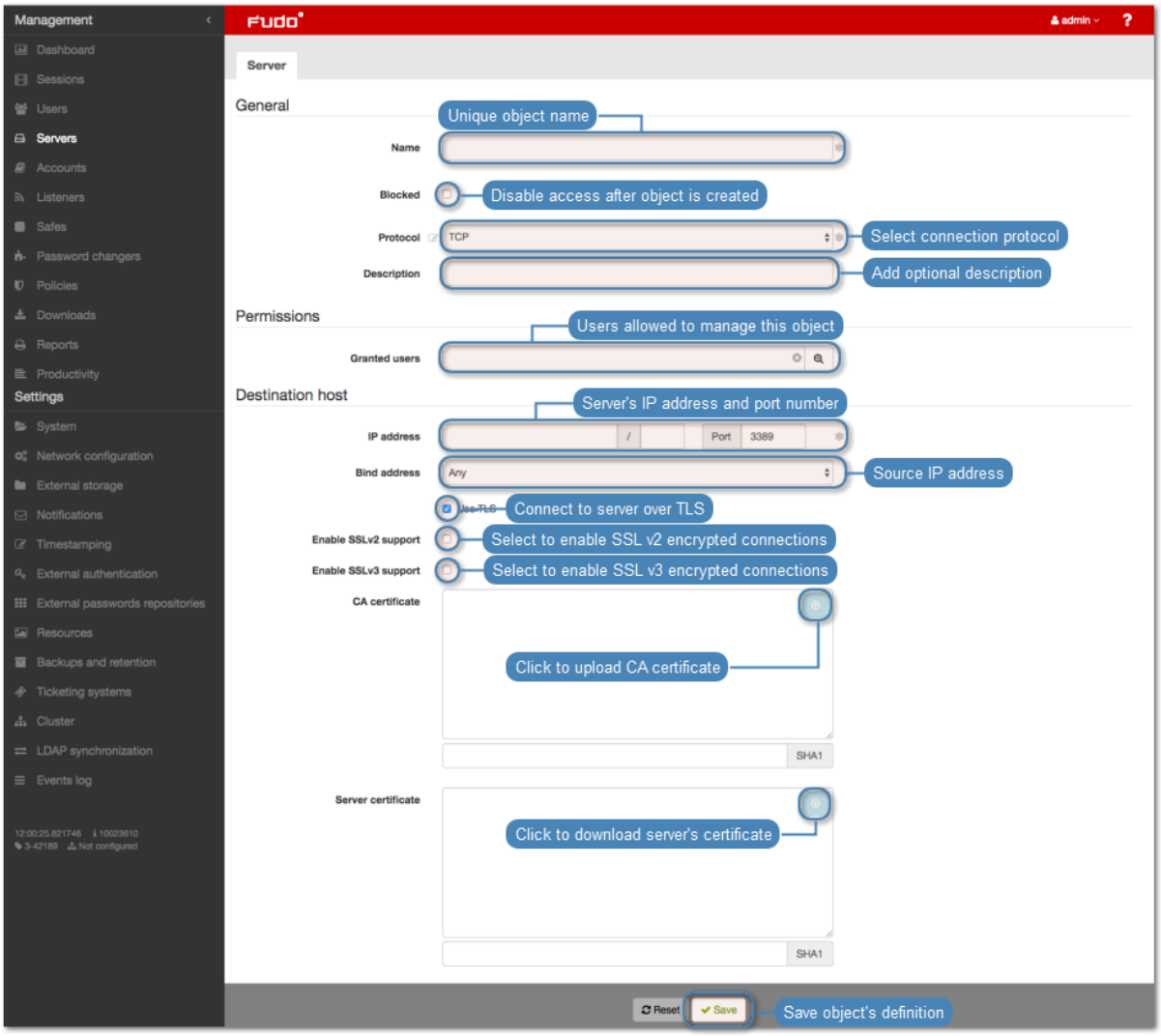
---

**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. Select the *Use TLS* options to connect to monitored server over TLS.
11. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
12. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
13. Click the to upload CA certificate.
14. Click the fetch server's certificate.
15. Click *Save*.




**Related topics:**

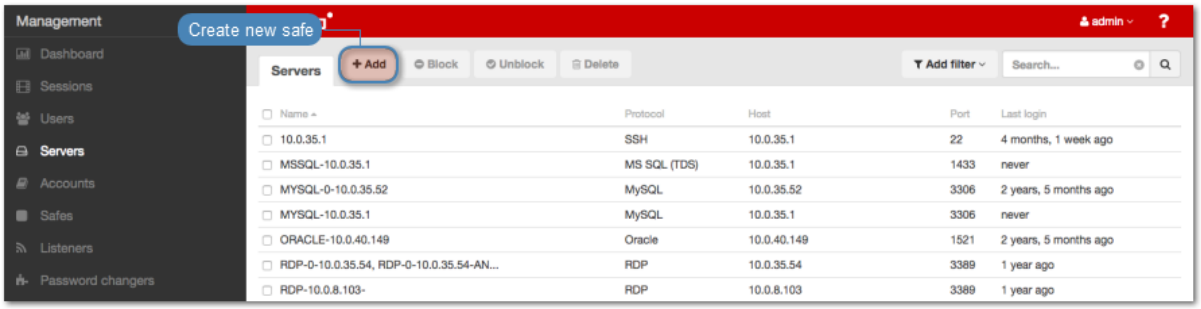
- *TCP*
- *Data model*
- *Creating a TCP listener*

### 6.1.2 Dynamic server

Wheel Fudo PAM enables defining a group of automatically managed servers deployed within a specified network. When a user is trying to establish a connection with a specific resource that is within the defined network, Wheel Fudo PAM verifies whether he has sufficient privileges and automatically adds host within the existing dynamic servers object, downloads its certificate and establishes a monitored connection.

#### 6.1.2.1 Creating a dynamic servers group

1. Select *Management* > *Servers*.
2. Click *+ Add*.




3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select desired protocol and define corresponding configuration parameters.
6. In the *Destination host* section, enter server's IP address, subnet mask in CIDR format and port number.
7. From the *Bind address* drop-down list, select Wheel Fudo PAM 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. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

---

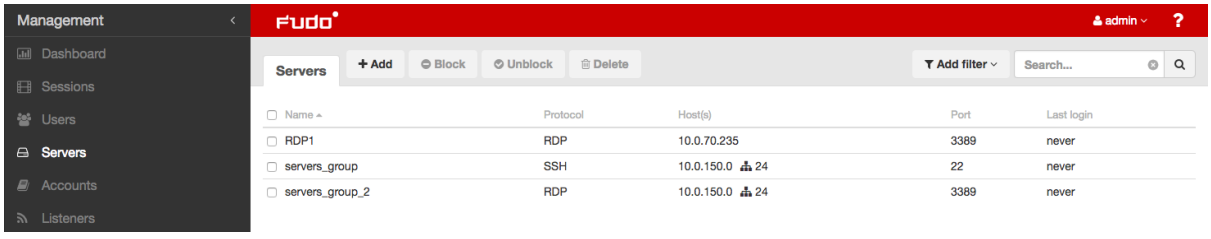
8. Click the icon to upload the CA certificate used for generating certificates for dynamically added servers.
9. Fill in the rest of the parameters and click *Save*.

### 6.1.2.2 Adding a single host to a servers group

1. Select *Management* > *Servers*.
2. Find and click desired servers group object.

---

**Note:** Server group objects are marked with the icon.




---

3. Click *+ Add host*.
4. Provide server's IP address.
5. Click the icon to download server's certificate.

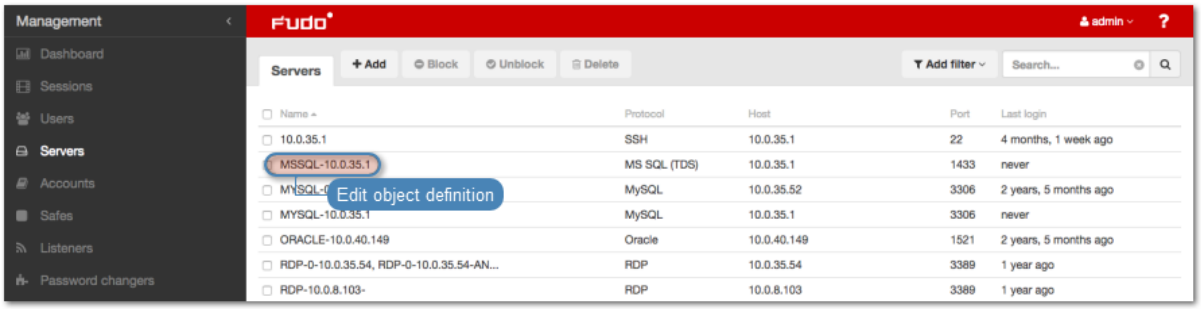
6. Click *Save*.

**Related topics:**

- *Data model*
- *Static server*

## 6.2 Editing a server

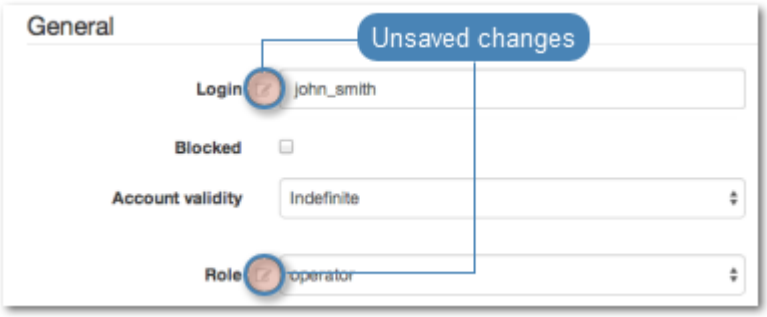
1. Select *Management* > *Servers*.
2. Find and click desired object to open its configuration page.




**Note:** Define filters to limit the number of objects displayed on the list.

3. Modify configuration parameters as needed.

**Note:** Unsaved changes are marked with the icon.




4. Click *Save*.

**Related topics:**

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

- *Accounts*

## 6.3 Blocking a server

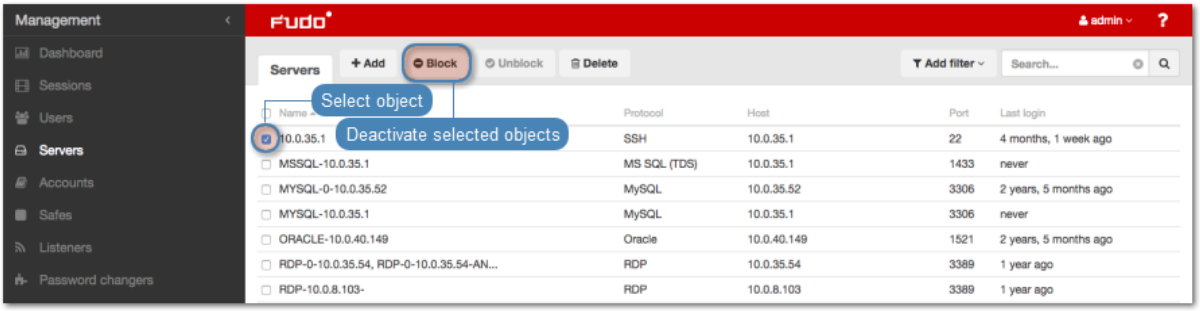
Wheel Fudo PAM allows blocking access to given server for all users.

**Warning:** Blocking a server will terminate current connections with the given server.

1. Select *Management* > *Servers*.
2. Find and select desired objects.

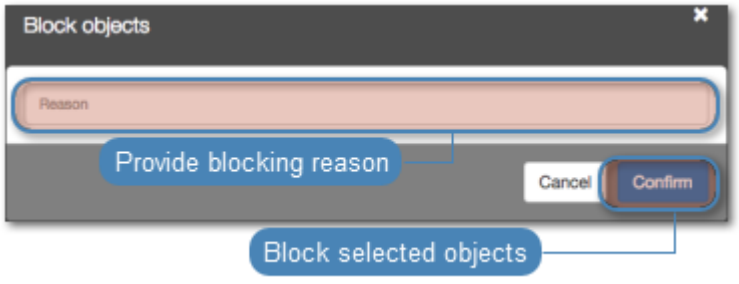
**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Block*.




4. Optionally, provide blocking reason and click *Confirm*.

**Note:** To view the blocking reason, place the cursor over the icon on the servers list.




**Related topics:**

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

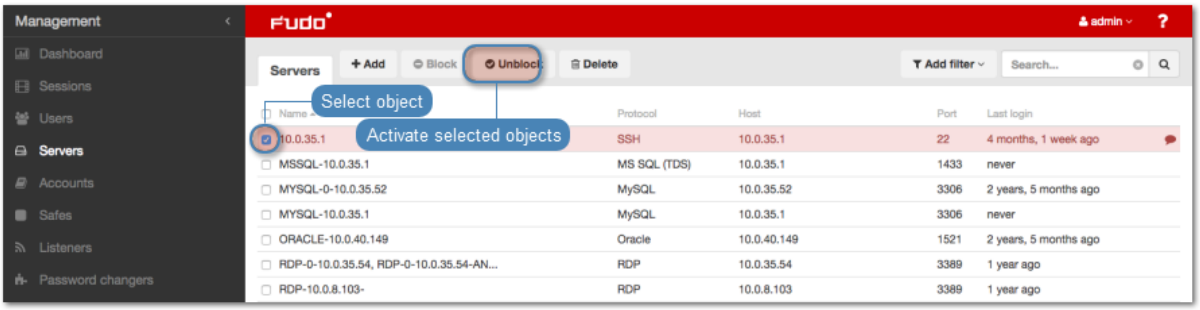
## 6.4 Unblocking a server

**Warning:** Blocking a server will terminate current connections with the given server.

1. Select *Management* > *Servers*.
2. Find and select desired objects.

**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Unblock*.




4. Click *Confirm* to unblock selected objects.

**Related topics:**

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

## 6.5 Deleting a server

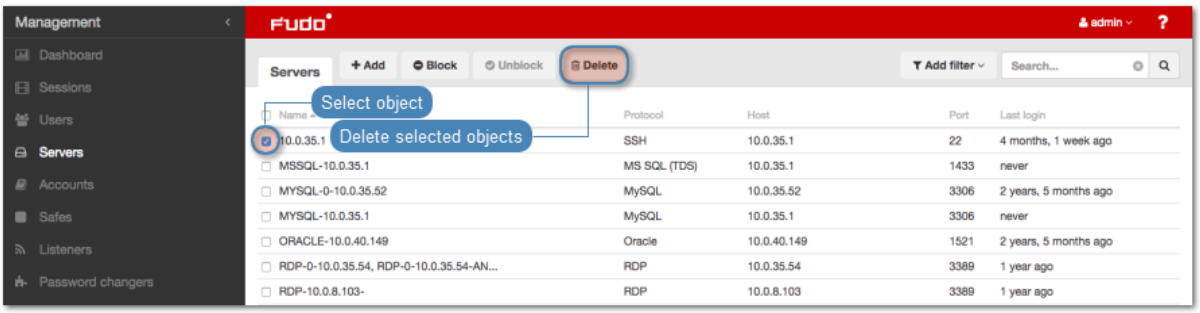
**Warning:** Deleting a server definition will terminate current connections with the given server.

### 6.5.1 Deleting a static server definition

1. Select *Management* > *Servers*.
2. Find and select desired objects.

**Note:** Define filters to limit the number of objects displayed on the list.

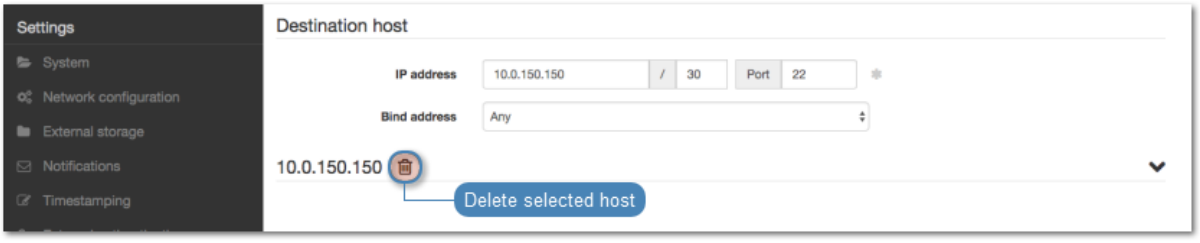
3. Click *Delete*.




4. Confirm deletion of selected objects.

### 6.5.2 Deleting a dynamically added host

1. Select *Management* > *Servers*.
2. Find and click desired dynamic servers object.
3. In the *Destination host* section, find desired host and click the icon.



4. Click *Save*.

**Related topics:**

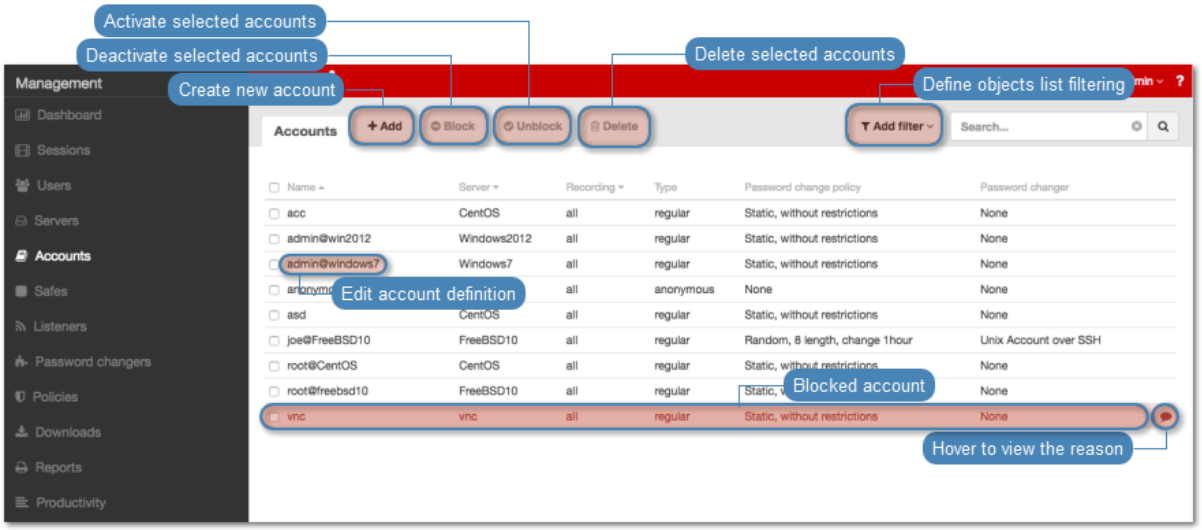
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

ROZDZIAŁ 7

# 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 Wheel Fudo PAM and then to connect to the target host.

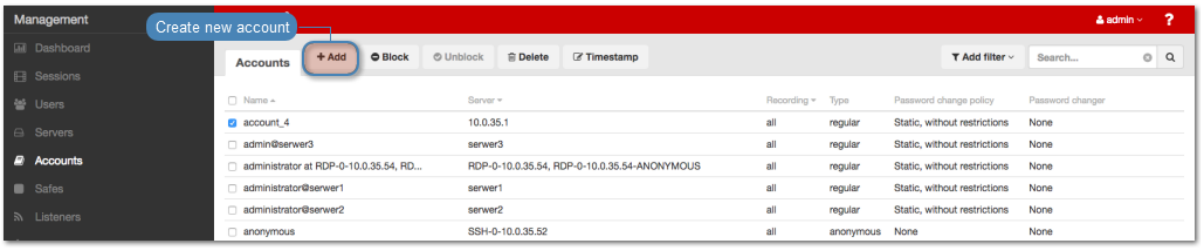


## 7.1 Creating an account

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

### 7.1.1 Creating an *anonymous* account

1. Select *Management* > *Accounts*.
2. Click *+ Add*.



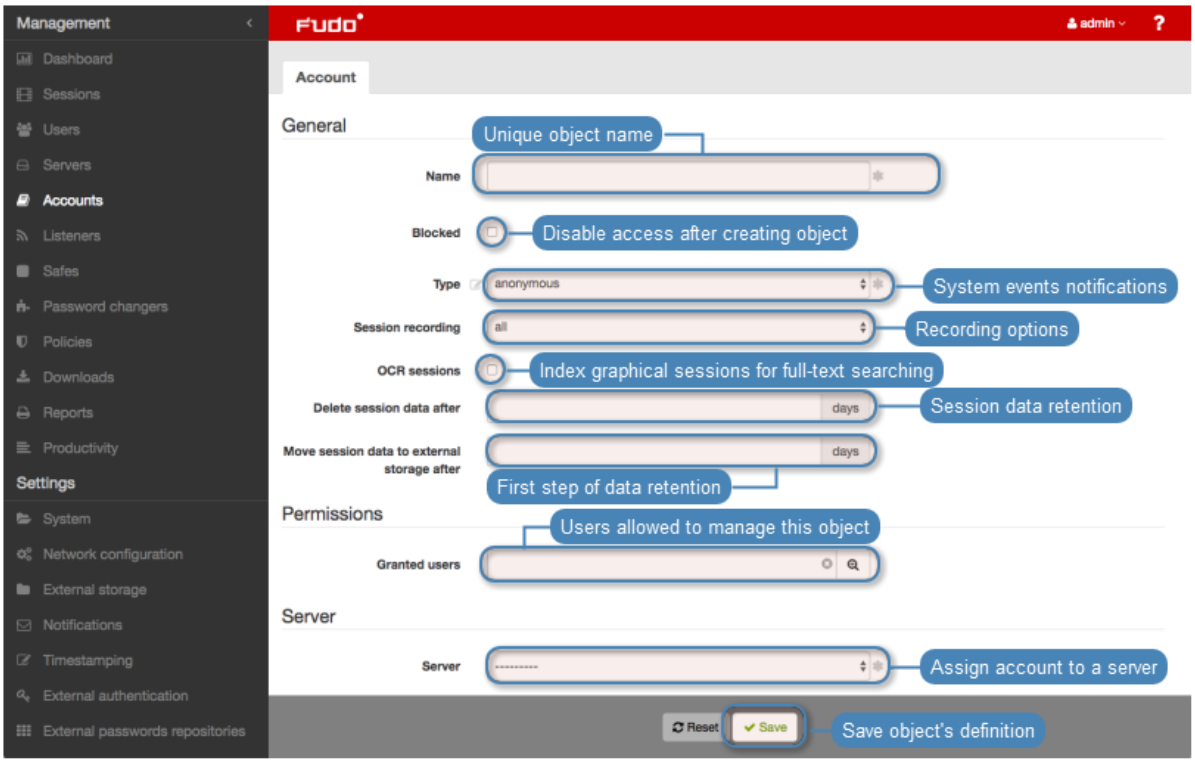

3. Define object's name.
4. Select *Blocked* option to disable account after it's created.
5. Select `anonymous` from the *Type* drop-down list.
6. Select desired session recording option.
    - `all` - Fudo PAM saves session metadata (basic session information), records raw network traffic (RAW file) 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 PAM 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).
    - `none` - Fudo PAM saves only session metadata (basic session information).
7. Select the *OCR sessions* option to fully index RDP and VNC sessions contents.

**Note:** Indexing sessions enables full-text content searching.

**Warning:** *OCR* is a CPU intensive process and may have negative impact on system's performance.

8. Select language used for processing recorded sessions.

9. In the *Move session data to external storage after*, define the number of days after which the session data will moved to external storage device.
10. In the *Delete session data after* field, define the number of days after which the session data will be deleted.
11. In the *Permissions* section, add users allowed to manage this object.
12. In the *Server* section, assign account to a specific server by selecting it from the *Server* drop-down list.
13. Click *Save*.

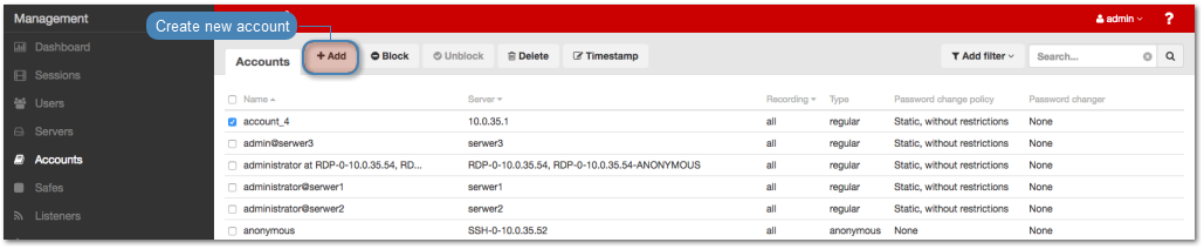



**Related topics:**

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

### 7.1.2 Creating a *forward* account

1. Select *Management* > *Accounts*.
2. Click *+ Add*.




3. Define object's name.
4. Select *Blocked* option to disable account after it's created.
5. Select `forward` from the *Type* drop-down list.
6. Select desired session recording option.
    - `all` - Fudo PAM 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 PAM 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).
    - `none` - Fudo PAM saves only session metadata (basic session information).
7. Select the *OCR sessions* option to fully index RDP and VNC sessions contents.

**Note:** Indexing sessions enables full-text content searching.

**Warning:** *OCR* is a CPU intensive process and may have negative impact on system's performance.

8. Select language used for processing recorded sessions.
9. In the *Move session data to external storage after*, define the number of days after which the session data will moved to external storage device.
10. In the *Delete session data after* field, define the number of days after which the session data will be deleted.
11. In the *Permissions* section, add users allowed to manage this object.
12. In the *Server* section, assign the account to a server by selecting it from the *Server* drop-down list.
13. From the *Replace secret with* drop down list in the *Credentials*, select desired option.

`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.

`key`

- Click the icon and select the key type.
- Click the and browse the file system to find the key definition file.
- Click the i icon and select the key type.
- Click the i icon and browse the file system to find the key definition file.

`password`

- Provide account password.
- Repeat account password.

**Note:** *Two-fold authentication*

With two-fold authentication enabled, user is being prompted twice for login credentials. Once for authenticating against Wheel Fudo PAM and once again for accessing target system.

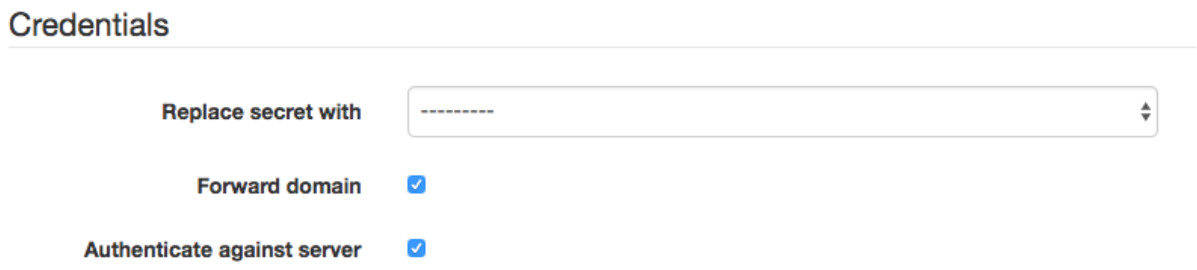
To enable two-fold authentication, select `password` from the *Replace secret with* drop-down list and leave the password and login fields empty.

`password from external repository`

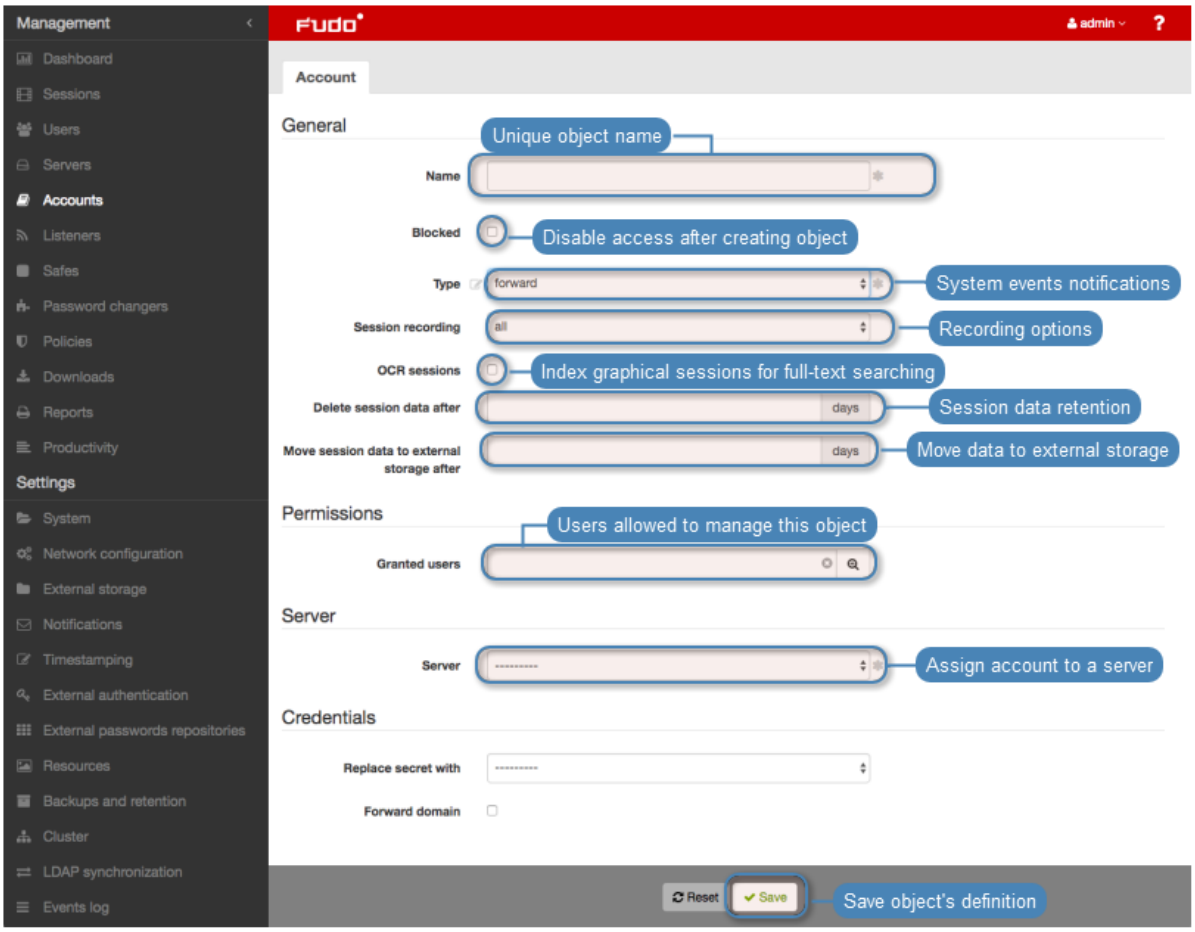
- Select external repository.

**Note:** *Authentication by the server*

With the *Authentication against server* option enabled, Wheel Fudo PAM 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).




14. Select *Forward domain* option to have the domain name included in the string identifying the user.
15. Click *Save*.

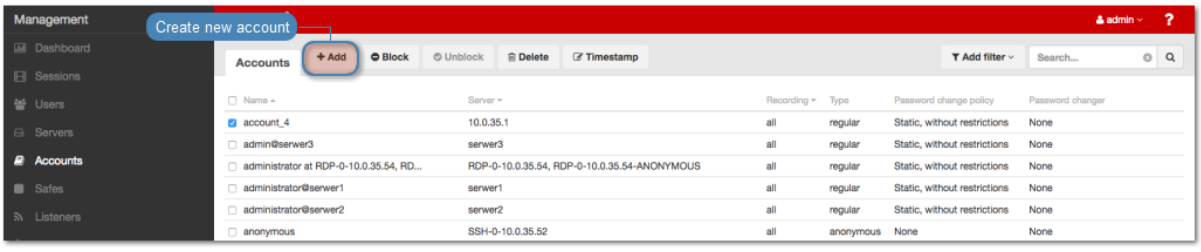



**Related topics:**

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

### 7.1.3 Creating a *regular* account

1. Select *Management* > *Accounts*.
2. Click *+ Add*.




3. Define object's name.
4. Select *Blocked* option to disable account after it's created.

5. Select `regular` from the *Type* drop-down list.
6. Select desired session recording option.
    - `all` - Fudo PAM 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 PAM 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).
    - `none` - Fudo PAM saves only session metadata (basic session information).
7. Select the *OCR sessions* option to fully index RDP and VNC sessions contents.

**Note:** Indexing sessions enables full-text content searching.

**Warning:** *OCR* is a CPU intensive process and may have negative impact on system's performance.

8. Select language used for processing recorded sessions.
9. In the *Move session data to external storage after*, define the number of days after which the session data will moved to external storage device.
10. In the *Delete session data after* field, define the number of days after which the session data will be deleted.
11. In the *Permissions* section, add users allowed to manage this object.
12. In the *Server* section, assign account to a specific server by selecting it from the *Server* drop-down list.
13. In the *Credentials* section, enter privileged account domain.
14. Type in login to the privileged account.
15. From the *Replace secret with* drop down list, select desired option.

    `sercret from a different account`

    - From the *Account* drop-down list, select account object, whose credentials will be used to authenticate user when establishing connection with monitored server.

    `key`

    - Click the icon and select the key type.
    - Click the icon and browse the file system to find the file with a non-passphrase protected private key.

    `password`

- Provide account password.
- Repeat account password.

---

**Note:** *Two-fold authentication*

With two-fold authentication enabled, user is being prompted twice for login credentials. Once for authenticating against Wheel Fudo PAM 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.

---

`password from external repository`

- Select external repository.

16. Select the defined password changing policy from the *Password change policy* drop-down list.
17. In the *Password changer* section, from the *Password changer* drop-down list select password changer specific for given account.

    **Unix Account over SSH**

    - Enter privileged user name.
    - Enter privileged user password.

    **Windows Account over WMI**

    - Enter privileged user name.
    - Enter privileged user password.

    **MySQL User Account on Unix Server over SSH**

    - Provide SSH user name.
    - Provide SSH account password.
    - Enter SSH server address.
    - Provide SSH service port.
    - Enter privileged user name.
    - Enter privileged user password.

    **Cisco Account over Telnet**

    - Provide privileged mode password.
    - Enter privileged user name.
    - Enter privileged user password.

    **Cisco Enable Password over Telnet**

    - Provide privileged mode password.
    - Enter privileged user name.
    - Enter privileged user password.

**Cisco Account over SSH**

- Provide privileged mode password.
- Enter privileged user name.
- Enter privileged user password.

**Cisco Enable Password over SSH**

- Provide privileged mode password.
- Enter privileged user name.
- Enter privileged user password.

**LDAP**

- Enter privileged user name.
- Enter privileged user password.
- Provide LDAP base.
- Upload LDAP CA certificate.

**WinRM**

- Select target host language.
- Enter privileged user name.
- Enter privileged user password.

---

**Note:**

- Select *Use an existing account* option and select existing account from the drop-down list to use it for authentication purposes.
- Privileged user account is used for changing the password when system detects that password has been changed in an unauthorized way.

---

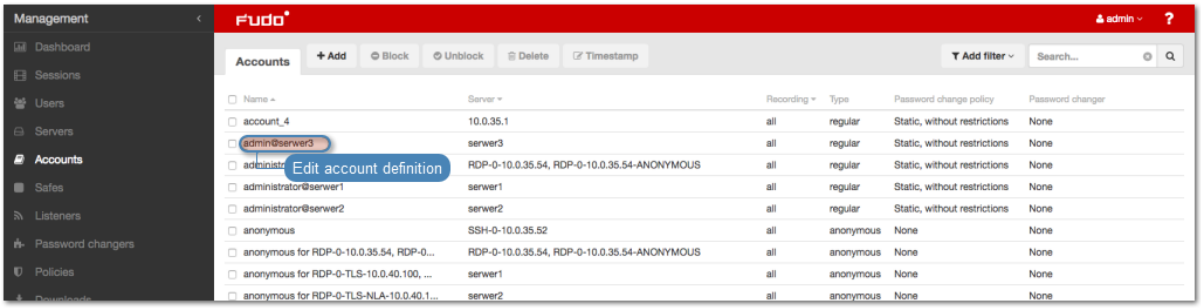
18. Click *Save*.

**Related topics:**

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

## 7.2 Editing an account

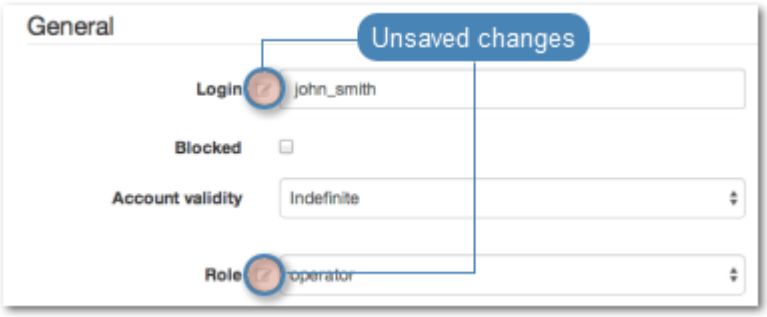
1. Select *Management* > *Accounts*.
2. Find and click desired object to open its configuration page.




**Note:** Define filters to limit the number of objects displayed on the list.

3. Modify configuration parameters as needed.

**Note:** Unsaved changes are marked with the icon.




4. Click *Save*.

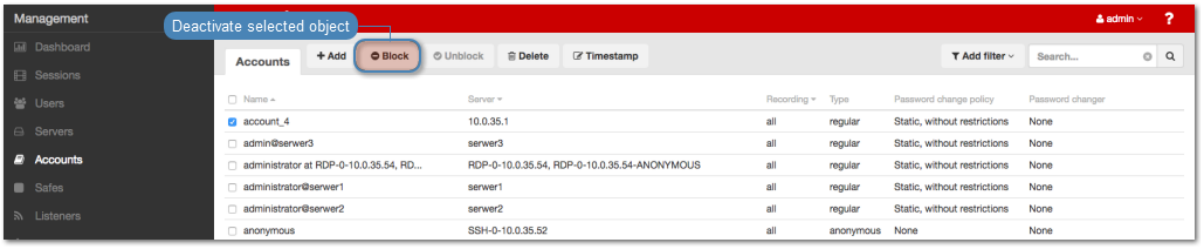
**Related topics:**

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

## 7.3 Blocking an account

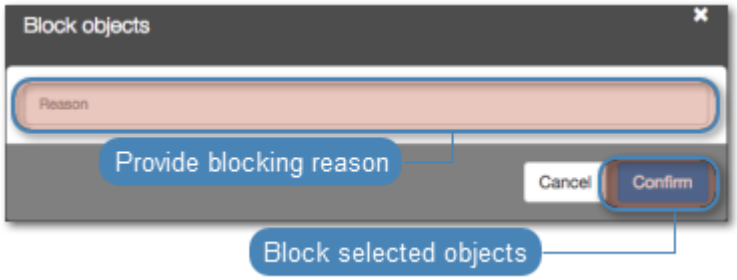
**Warning:** Blocking an accout definition will terminate all current connections to servers which use selected account for accessing those servers.

1. Select *Management* > *Accounts*.
2. Find and select desired objects.
3. Click *Block*.




4. Optionally, provide blocking reason and click *Confirm*.

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

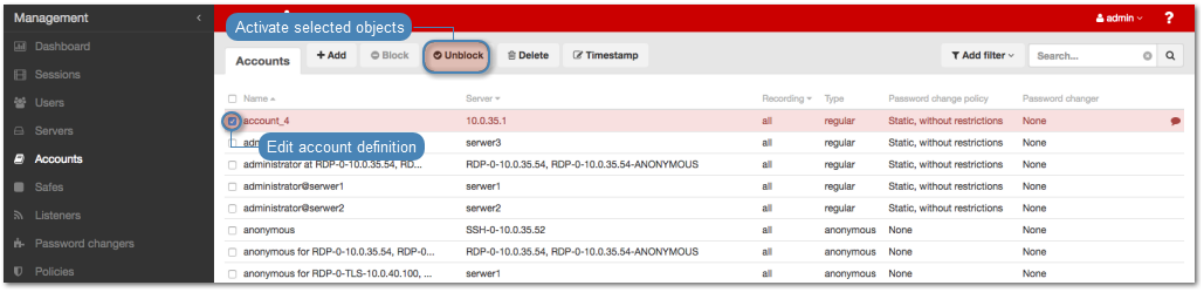



**Related topics:**

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

## 7.4 Unblocking an account

1. Select *Management* > *Accounts*.
2. Find and select desired objects.
3. Click *Unblock*.




4. Confirm unblocking selected objects.

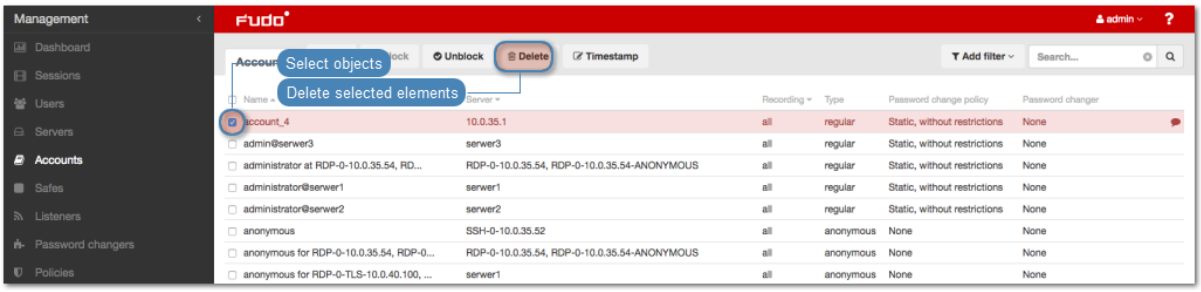
**Related topics:**

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

## 7.5 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. Find and select desired objects.
3. Click *Delete*.




4. Confirm deletion of selected objects.

**Related topics:**

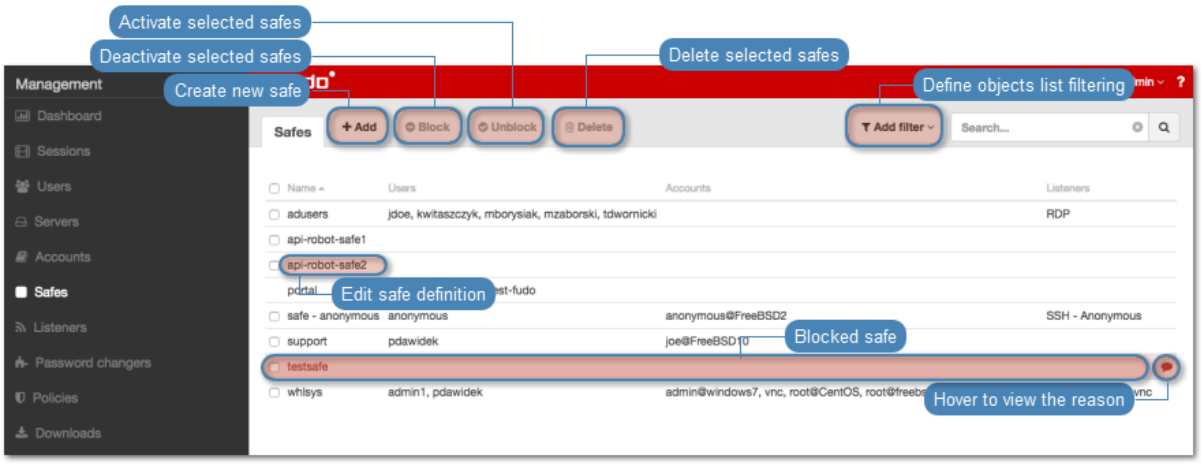
- *Creating an account*

- *Editing an account*
- *Blocking an account*
- *Unblocking an account*

ROZDZIAŁ 8

# Safes

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



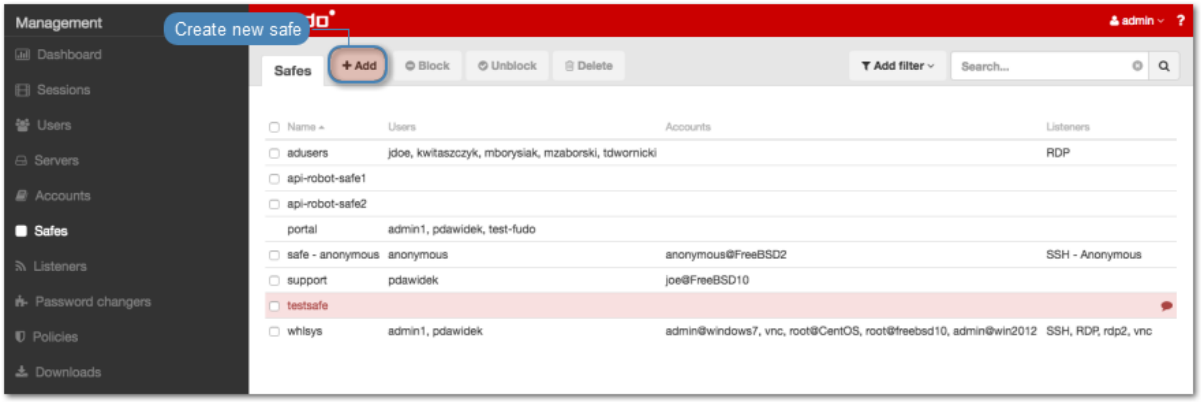

**Note:**

- The `system` safe can only contain `system` account.
- The `portal` safe can only contain the `portal` account.
- `Operator`, `admin` and `superadmin` users always have access to the `system` safe.
- `User` type users cannot have access to the `system` safe.
- Anonymous user must have access to safes containing anonymous accounts.

## 8.1 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. Select *Management* > *Safes*.
2. Click + *Add*.




3. Enter object's name.
4. Select *Blocked* option to disable access to object after it's created.
5. Select *Login reason* option, to display prompt upon logging in, asking user to enter login reason.
6. Select *Require approval* option to have the administrator approve each connection to servers accessed through configured safe.
7. Select *Notifications* option and choose notifications sent out to Wheel Fudo PAM administrator.

---

**Note:**

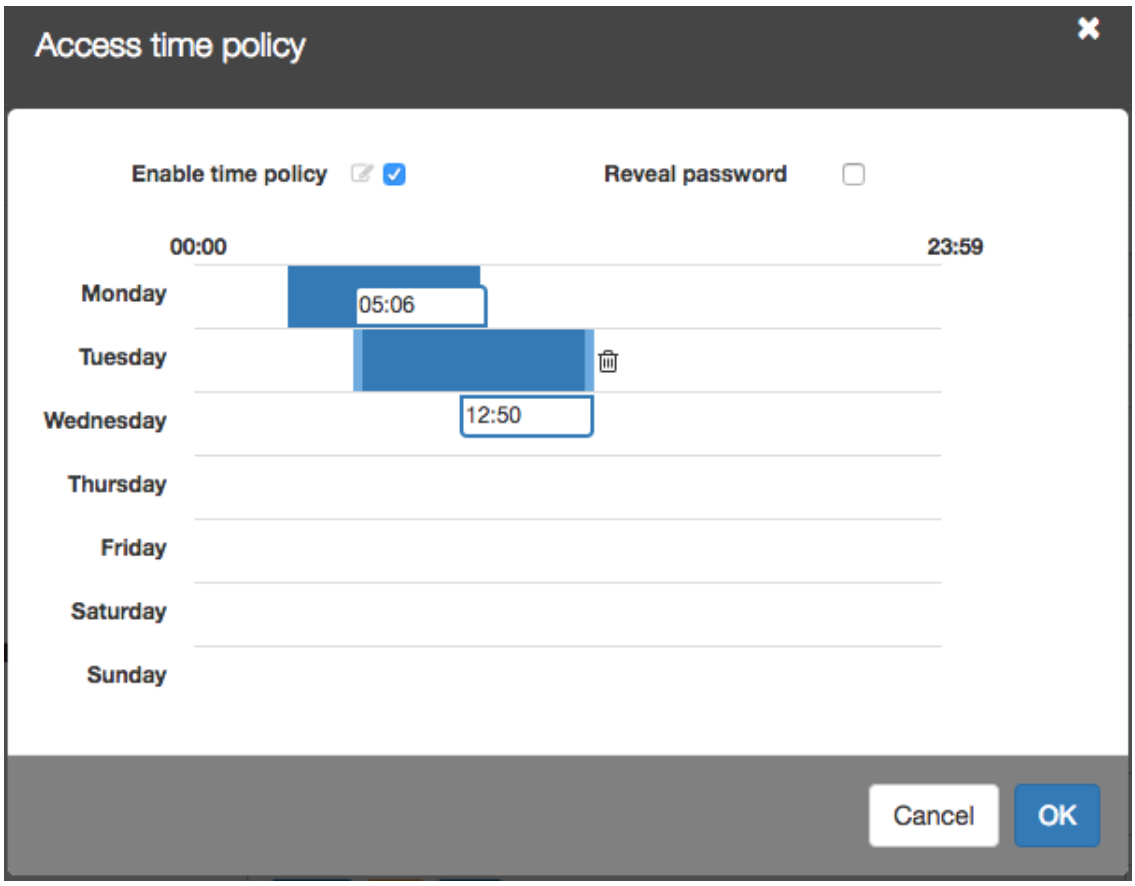
- Notifications settings are applied only to the currently logged in user.
- *Session start (push)* notification requires an external proxy service. For more information on proxy server configuration refer to *Proxy servers configuration* topic.

---

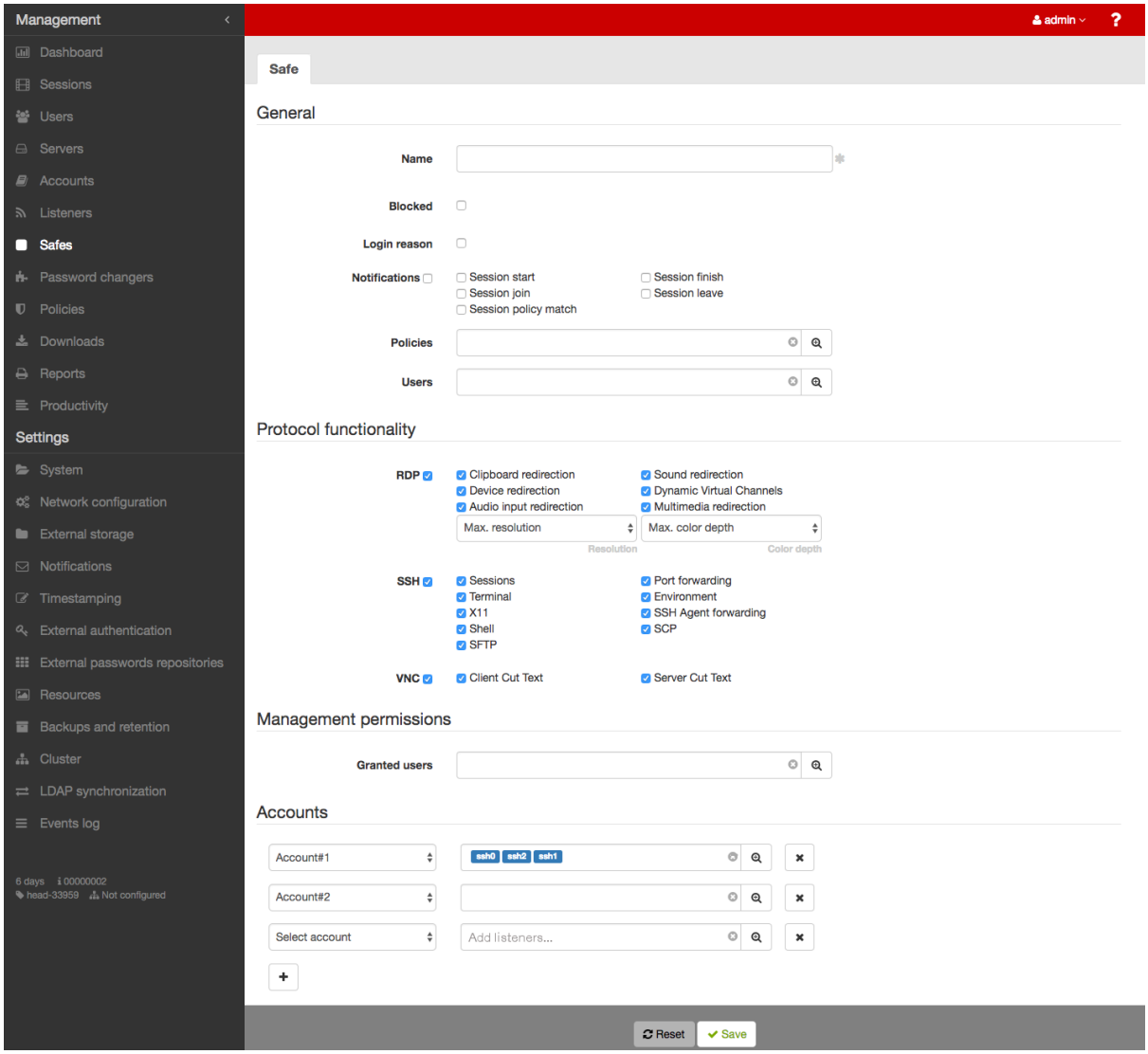
8. Assign *security policies* in the *Policies* field.
9. Add users allowed to connect to servers using accounts assigned to this safe.

---

**Note:** Click a specific user element to define time policy and allow him to see passwords in the User Portal.




10. In the *Protocol functionality* section, select allowed protocols' features.
11. In the *Permissions* section, add users (administrators, operators) allowed to manage this object.
12. In the *Accounts* section, click the + icon.
13. Select privileged account from the drop-down list and assign listeners allowed to initiate connections to hosts using selected account.
14. Click *Save*.

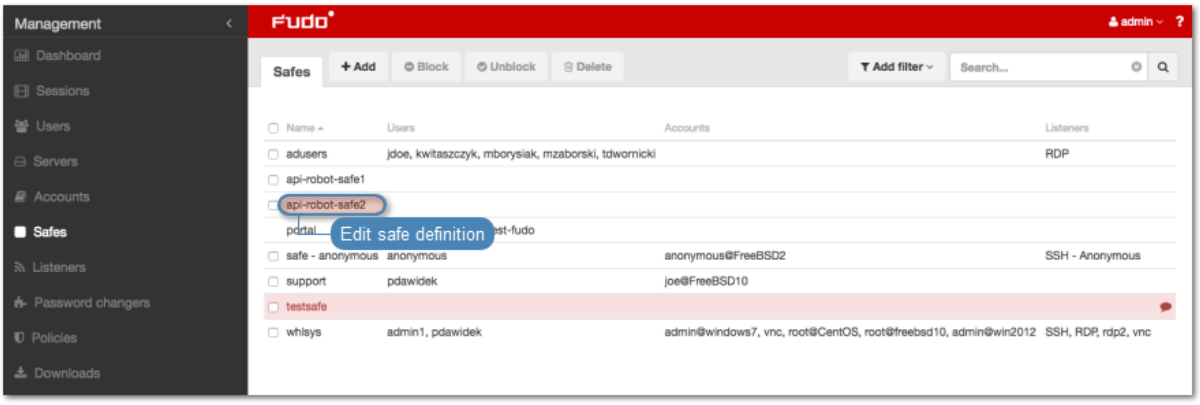



**Related topics:**

- *Data model*
- *Editing a safe*
- *Blocking a safe*
- *Deleting a safe*

## 8.2 Editing a safe

1. Select *Management* > *Safes*.
2. Find and click desired object to open its configuration page.




**Note:** Define filters to limit the number of objects displayed on the list.

3. Modify configuration parameters as needed.

**Note:** Unsaved changes are marked with the icon.

4. Click *Save*.

**Related topics:**

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

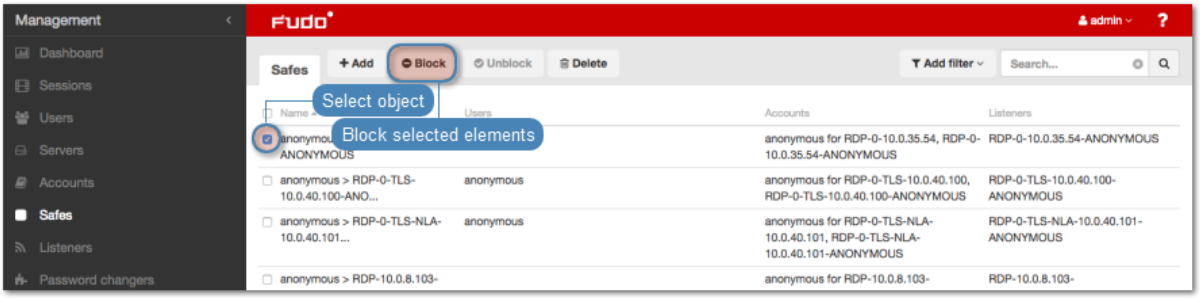
## 8.3 Blocking a safe

**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. Find and select desired objects.

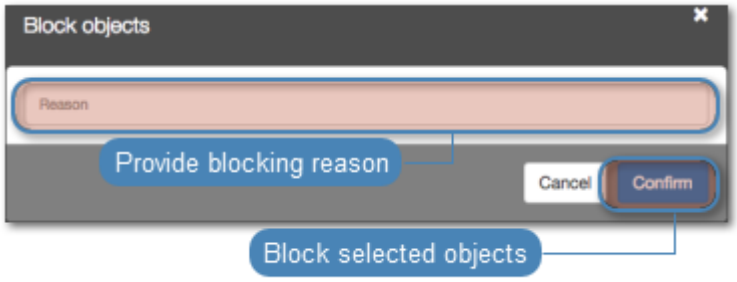
**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Block*.




4. Optionally, provide blocking reason and click *Confirm*.

**Note:** To view the blocking reason, place the cursor over the icon on the safes list.




**Related topics:**

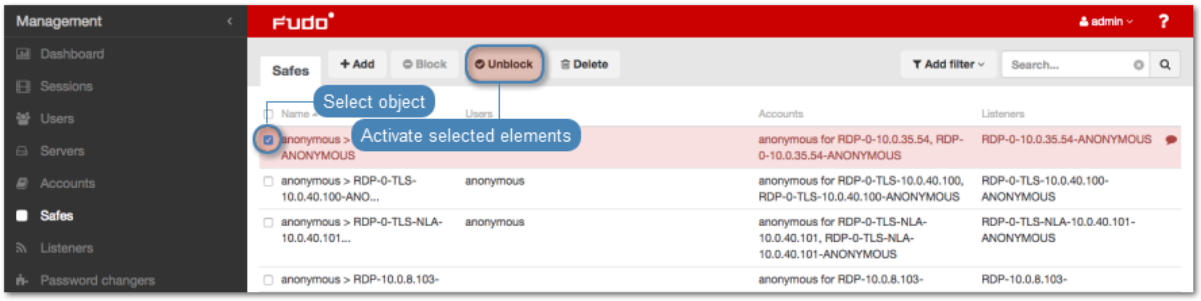
- *Unblocking a safe*
- *Data model*
- *Creating a safe*
- *Blocking a safe*

## 8.4 Unblocking a safe

1. Select *Management* > *Safes*.
2. Find and select desired objects.

**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Unblock*.




4. Click *Confirm* to unblock selected objects.

**Related topics:**

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

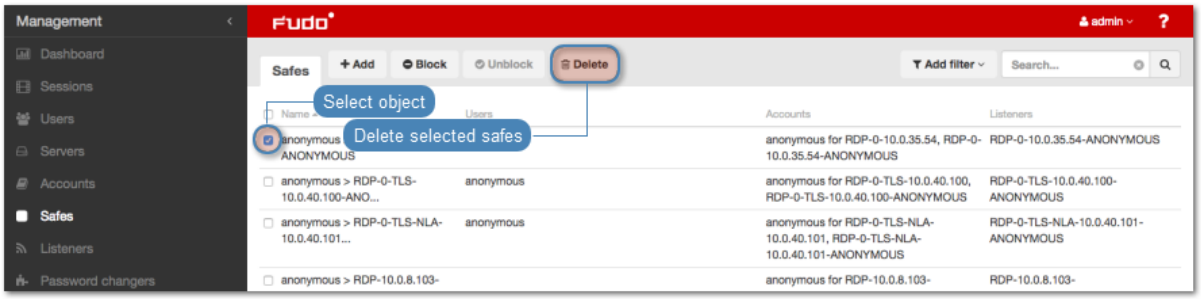
## 8.5 Deleting a safe

**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. Find and select desired objects.

**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Delete*.




4. Confirm deletion of selected objects.

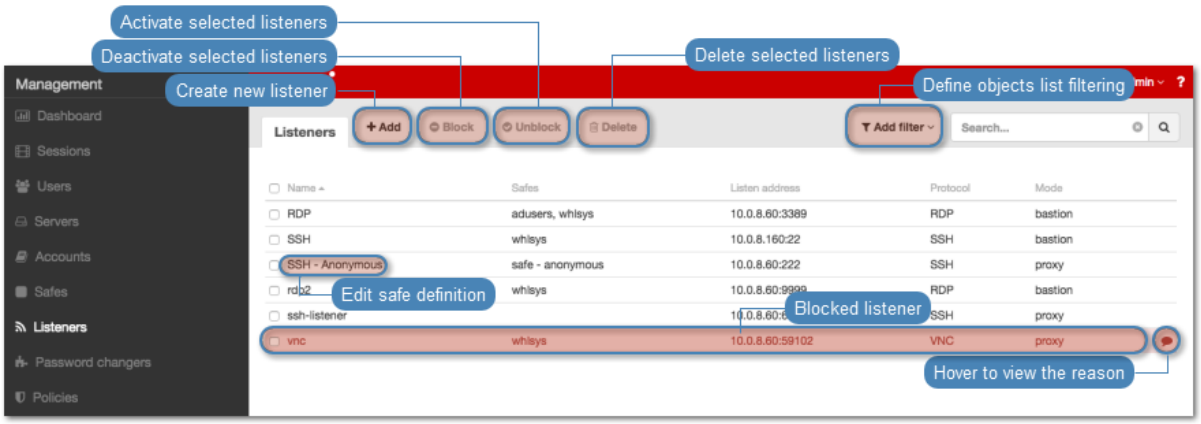
**Related topics:**

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

ROZDZIAŁ 9

# Listeners

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




**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*.

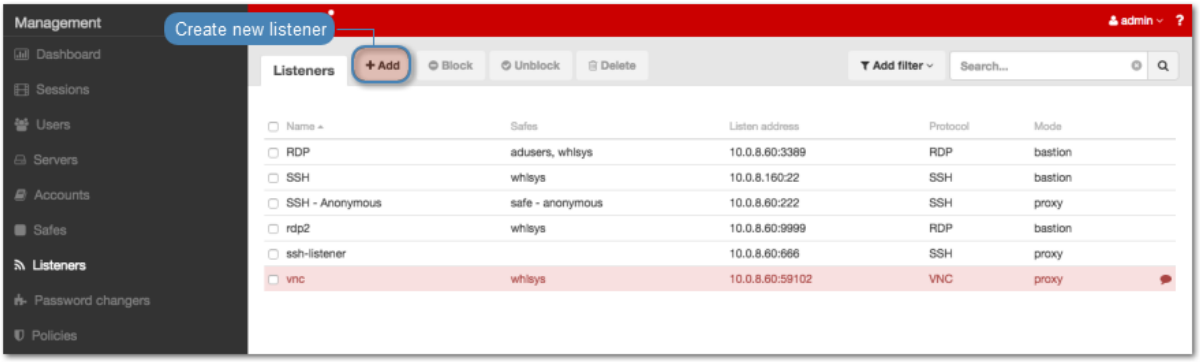
## 9.1 Creating a listener

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

**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.

### 9.1.1 Creating a Citrix listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.




3. Select `Citrix StoreFront (HTTP)` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**gateway**

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

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.

- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

---

**transparent**

---

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

---

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

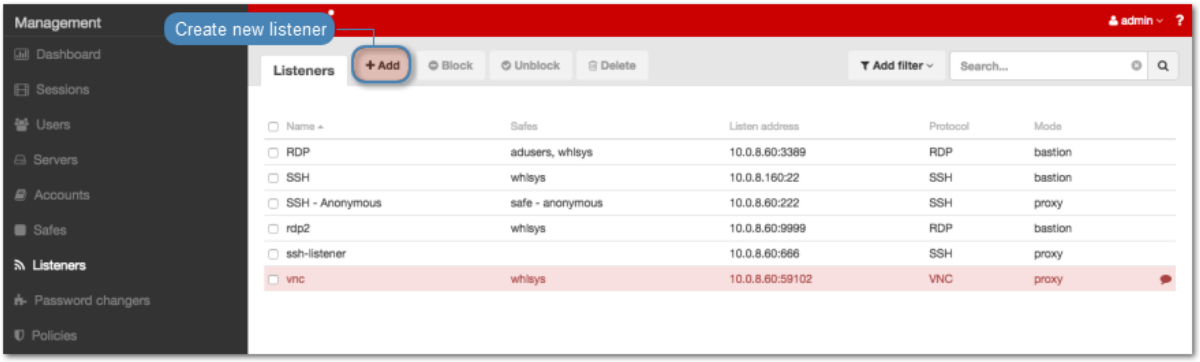
6. Select *Use TLS* option to enable encryption.
7. Select the *Enable SSLv2 support* option to support SSL v2 encrypted connections.
8. Select the *Enable SSLv3 support* option to support SSL v3 encrypted connections.
9. In the *TLS certificate* field, click to generate TLS certificate, or click to 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`.
10. Click *Save*.

**Related topics:**

- *Data model*
- *ICA via Citrix StoreFront*
- *Creating a Citrix server*

### 9.1.2 Creating a HTTP listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.




3. Select `HTTP` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

**transparent**

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

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

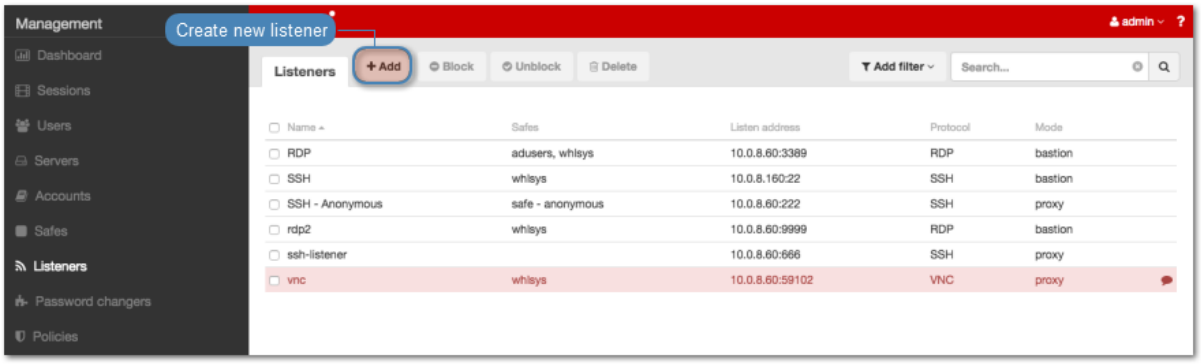
6. Select the *Use TLS* option to enable encryption.
7. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
8. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
9. In the *TLS certificate* field, click to generate TLS certificate, or click to upload server 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`.
10. Click *Save*.

**Related topics:**

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

### 9.1.3 Creating an ICA listener

1. Select *Management* > *Listeners*.
2. Click + *Add*.




3. Select `ICA` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**bastion**

---

**Note:** User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.

---

- Select `bastion` from the *Mode* drop-down list.
- Select the the IP address from the *Local address* drop-down list and enter port number.

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).

- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

---

**transparent**

---

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

---

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

7. Select *Use TLS* option to enable encryption.
8. Select the *Enable SSLv2 support* option to support SSL v2 encrypted connections.
9. Select the *Enable SSLv3 support* option to support SSL v3 encrypted connections.
10. In the *TLS certificate* field, click to generate TLS certificate, or click 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`.

---

**Note:** In case of TLS encrypted connections, Fudo returns an *.ica configuration file* to the Citrix client, which has the *FQDN* server address (*Address*) set to the common name defined in the TLS certificate.

---

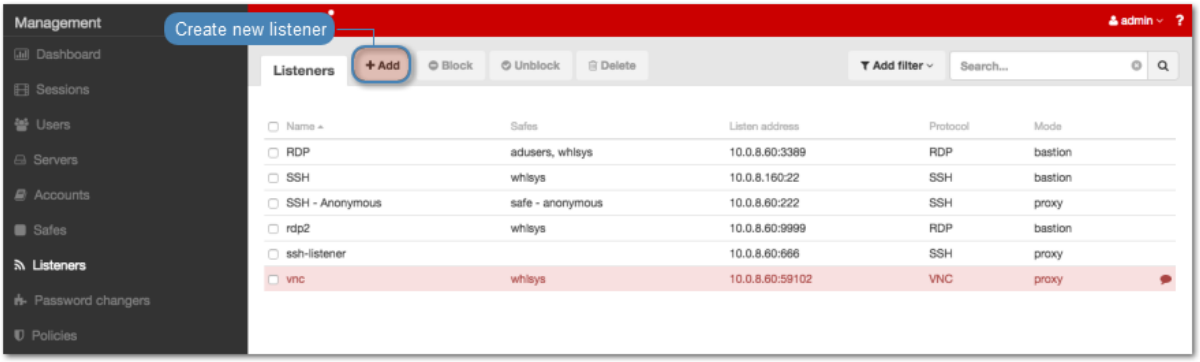
11. Click *Save*.

**Related topics:**

- *ICA*
- *ICA configuration file*
- *Data model*
- *ICA via Citrix StoreFront*
- *ICA*
- *Creating an ICA server*

### 9.1.4 Creating a Modbus listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.




3. Select `Modbus` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

**transparent**

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

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

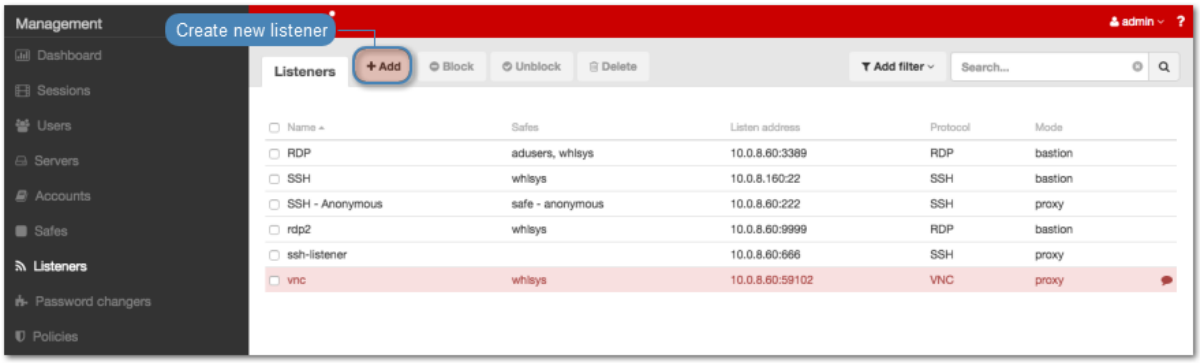
6. Click *Save*.

**Related topics:**

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

### 9.1.5 Creating a MySQL listener

1. Select *Management* > *Listeners*.
2. Click + *Add*.




3. Select `MySQL` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

---

**transparent**

---

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

---

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

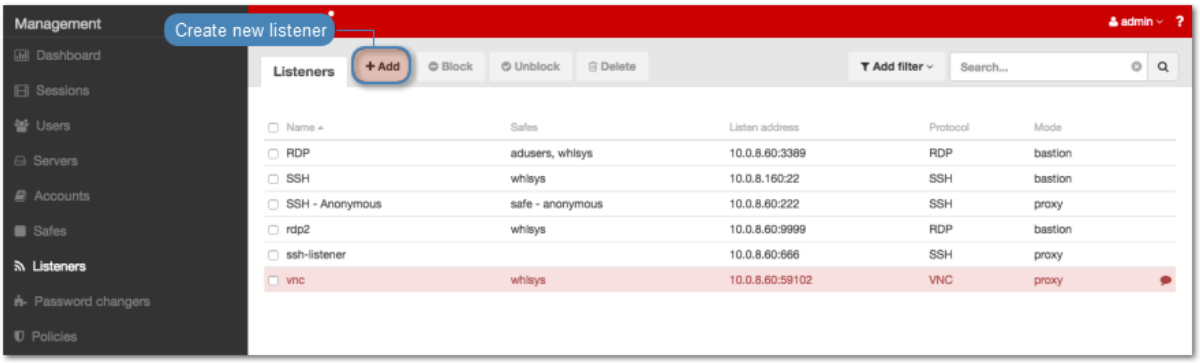
6. Click *Save*.

**Related topics:**

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

### 9.1.6 Creating an Oracle listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.




3. Select `MySQL` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.

- 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*).
- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

---

**transparent**

---

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

---

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

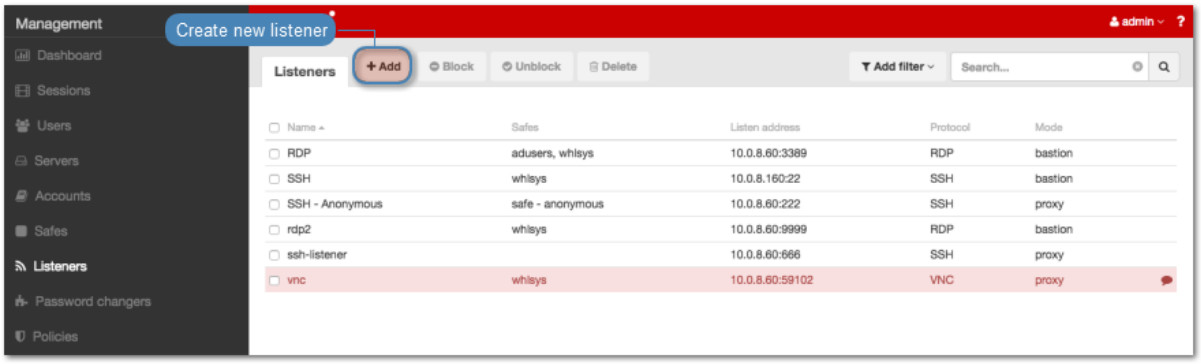
6. Click *Save*.

**Related topics:**

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

### 9.1.7 Creating an RDP listener

1. Select *Management* > *Listeners*.
2. Click + *Add*.




3. Select `RDP` from the *Protocol* drop-down list.
4. From the `Security` drop-down list, select RDP connection security mode.
5. In the *Announcement* field, type in the announcement that will be presented to the user on the login screen.
6. In the *Permissions* section, add users allowed to manage this object.
7. In the *Connection* section, select desired connection mode.

**bastion**

---

**Note:** User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.

---

- Select `bastion` from the *Mode* drop-down list.
- Select the the IP address from the *Local address* drop-down list and enter port number.

---

**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 *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.

---

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

**transparent**

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

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

8. In the *TLS certificate* field, click to generate TLS certificate, or click 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`.
9. Click *Save*.

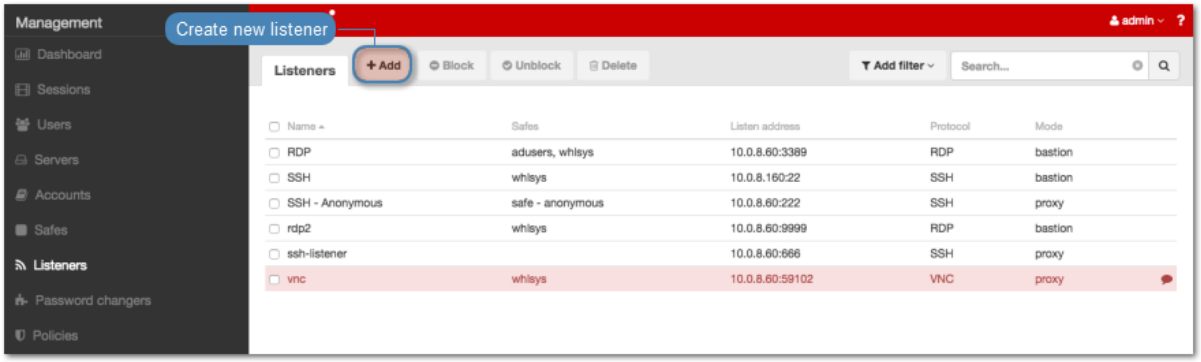
**Related topics:**

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

- *Unblocking a listener*

### 9.1.8 Creating an SSH listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.




3. Select `SSH` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**bastion**

---

**Note:** User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.

---

- Select `bastion` from the *Mode* drop-down list.
- 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*).
- 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.

---

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.

- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

---

**transparent**

---

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

---

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

6. In the *Fudo public key* field, click to upload (optionally provide encryption passphrase) or to generate TLS certificate.
7. Click *Save*.

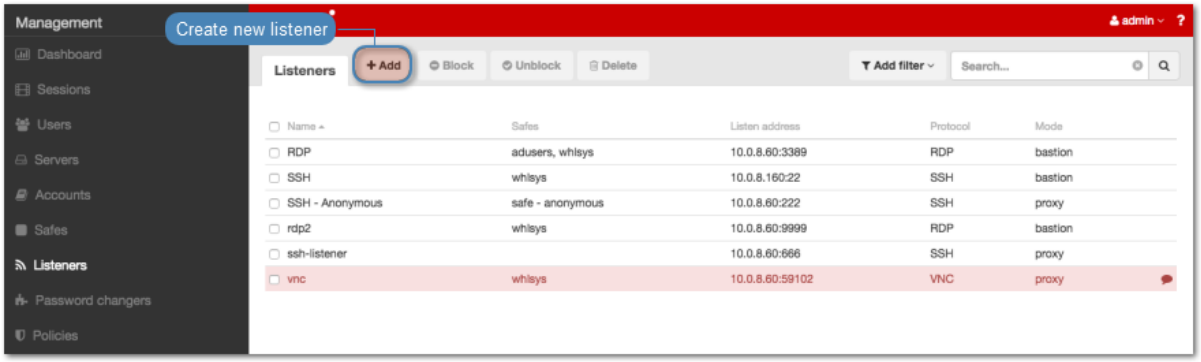
**Related topics:**

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

- *Blocking a listener*
- *Unblocking a listener*

### 9.1.9 Creating a MS SQL listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.




3. Select `MS SQL (TDS)` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

---

**transparent**

---

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

---

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

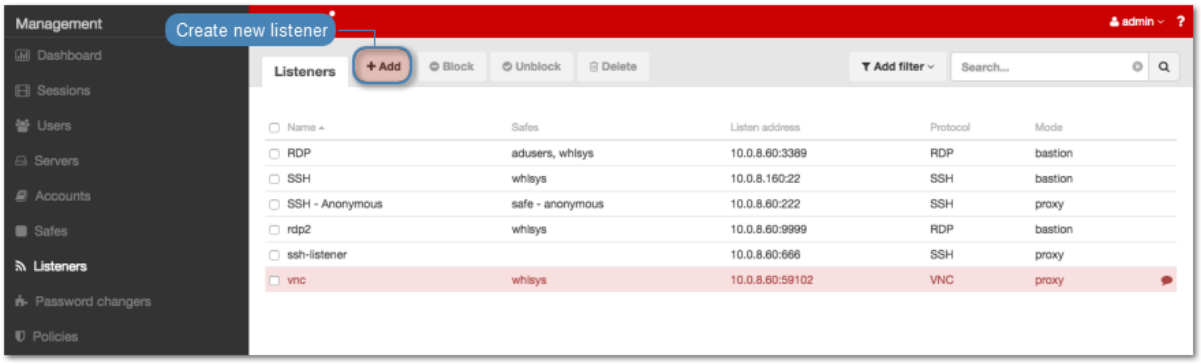
6. Click *Save*.

**Related topics:**

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

### 9.1.10 Creating a Telnet listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.




3. Select `Telnet` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

**transparent**

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

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

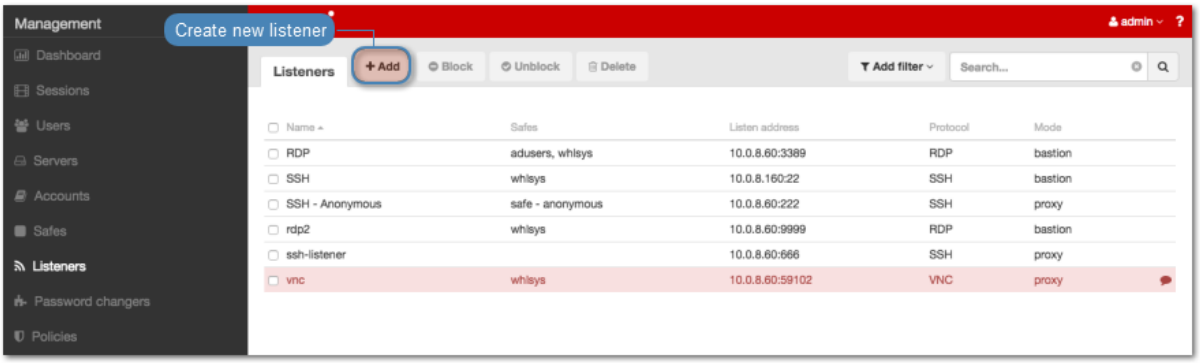
6. Select the *Use TLS* option to enable encryption.
7. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
8. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
9. In the *TLS certificate* field, click to generate TLS certificate, or click to upload server 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`.
10. Click *Save*.

**Related topics:**

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

### 9.1.11 Creating a Telnet 3270 listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.



3. Select `Telnet 3270` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

---

**transparent**

---

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

---

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

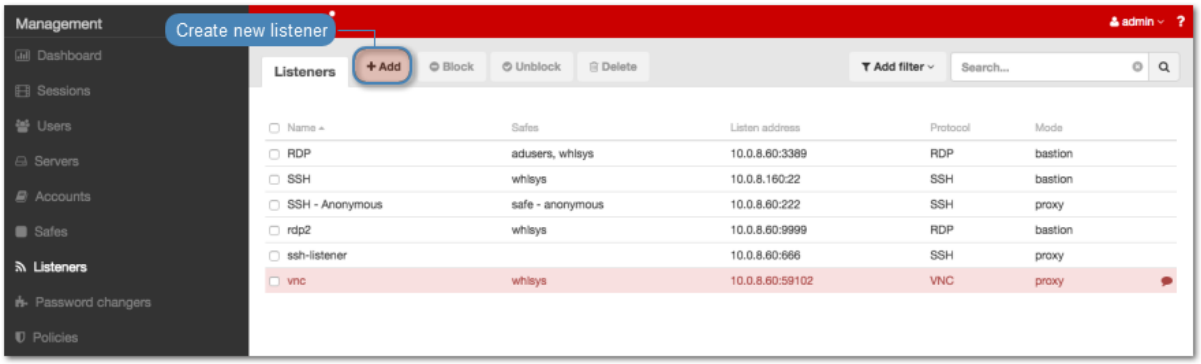
6. Select the *Use TLS* option to enable encryption.
7. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
8. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
9. In the *TLS certificate* field, click to generate TLS certificate, or click to upload server 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`.
10. Click *Save*.

**Related topics:**

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

### 9.1.12 Creating a Telnet 5250 listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.




3. Select `Telnet 5250` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

---

**transparent**

---

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

---

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

6. Select the *Use TLS* option to enable encryption.
7. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
8. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
9. In the *TLS certificate* field, click to generate TLS certificate, or click 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`.

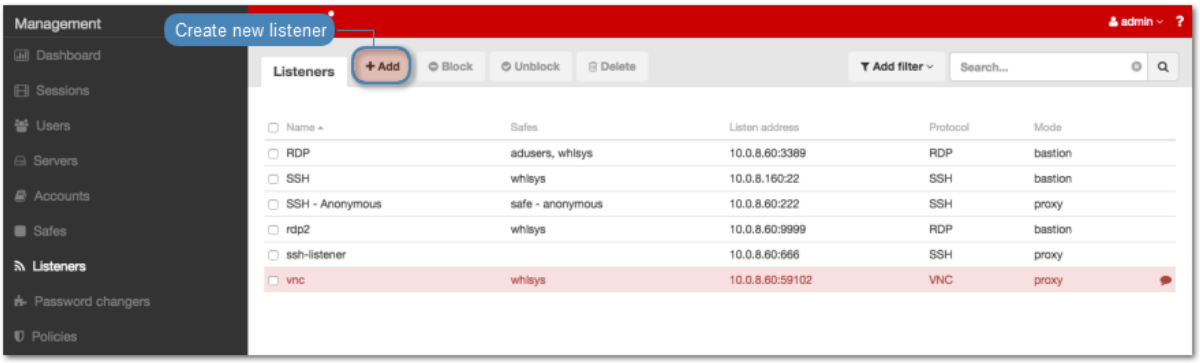
10. Click *Save*.

**Related topics:**

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

### 9.1.13 Creating a VNC listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.




3. Select `VNC` from the *Protocol* drop-down list.
4. In the *Announcement* field, type in the announcement that will be presented to the user on the login screen.
5. In the *Permissions* section, add users allowed to manage this object.
6. In the *Connection* section, select desired connection mode.

**bastion**

---

**Note:** User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.

---

- Select `bastion` from the *Mode* drop-down list.
- 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*).

- 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.

---

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.
- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

---

**transparent**

---

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

---

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

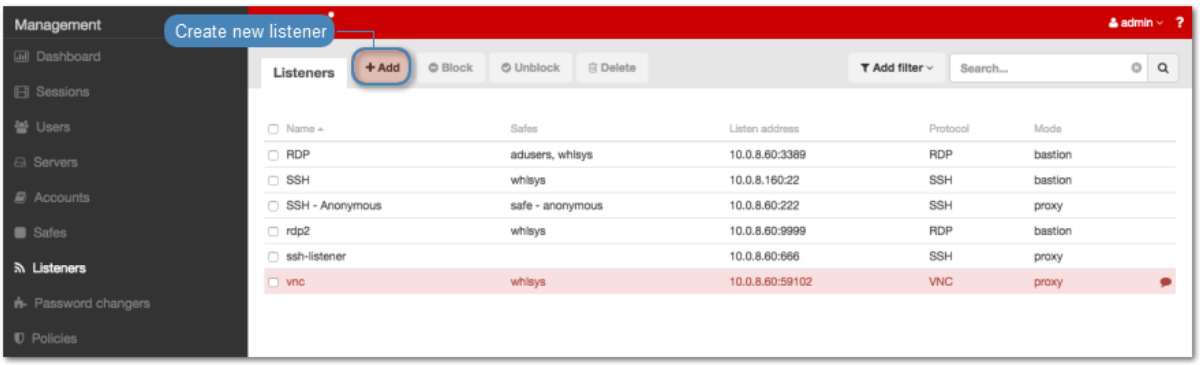
7. Click *Save*.

**Related topics:**

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

### 9.1.14 Creating a TCP listener

1. Select *Management* > *Listeners*.
2. Click *+ Add*.




3. Select `TCP` from the *Protocol* drop-down list.
4. In the *Permissions* section, add users allowed to manage this object.
5. In the *Connection* section, select desired connection mode.

**gateway**

---

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

---

- Select `gateway` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

**proxy**

---

**Note:**

- User connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host.

- Proxy mode is not supported by *dynamically added hosts*.

---

- Select `proxy` from the *Mode* drop-down list.
- 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*).
- 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.

---

- In the *External address* field, 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 external address is listed in *user portal* and it enables establishing connections from external networks.

---

**transparent**

---

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

---

- Select `transparent` from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.

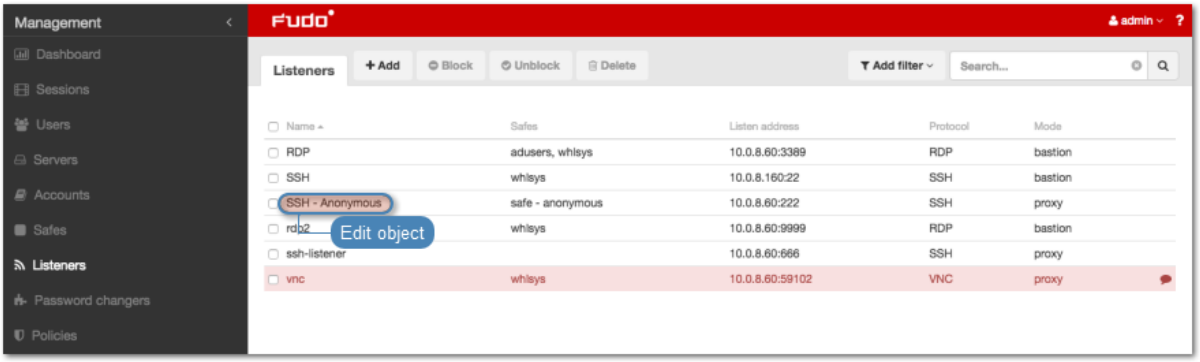
7. Select *Use TLS* option to enable encryption.
8. Select the *Enable SSLv2 support* option to support SSL v2 encrypted connections.
9. Select the *Enable SSLv3 support* option to support SSL v3 encrypted connections.
10. In the *TLS certificate* field, click to generate TLS certificate, or click to 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`.
11. Click *Save*.

**Related topics:**

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

## 9.2 Editing a listener

1. Select *Management* > *Listeners*.
2. Find and click desired listener to access its configuration parameters.




**Note:** Define filters to limit the number of objects displayed on the list.

3. Modify configuration values as needed.

**Note:** Unsaved changes are marked with an icon.

4. Click *Save*.

**Related topics:**

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

## 9.3 Blocking a listener

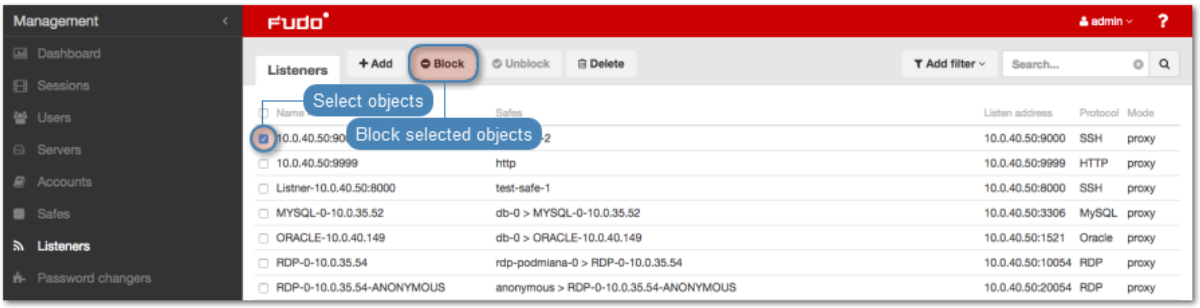
**Warning:** Blocking a listener will terminate current connections with server which uses it.

1. Select *Management* > *Listeners*.

2. Find and select desired listener.

**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Block* to disable access to hosts over selected listeners.




4. Optionally, provide descriptive reason for blocking given resource and click *Confirm*.

**Related topics:**

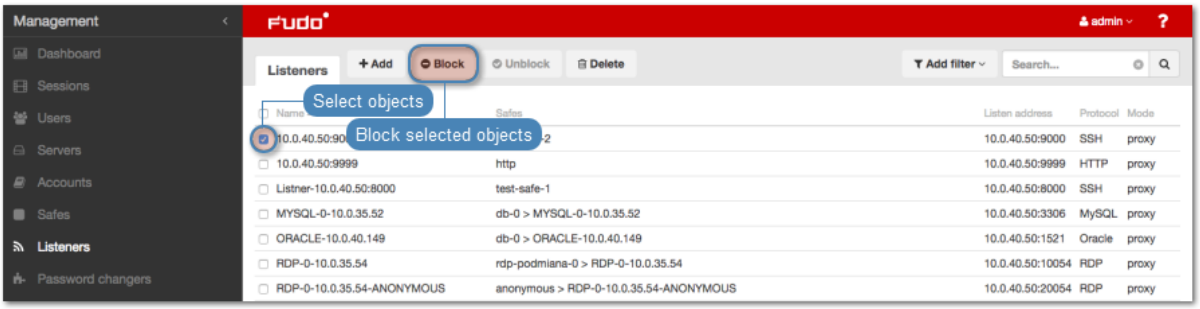
- *Data model*
- *System initiation*
- *Servers*

## 9.4 Unblocking a listener

1. Select *Management* > *Listeners*.
2. Find and select desired listener.

**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Unblock* to enable access to hosts over selected listeners.




4. Click *Confirm* to unblock selected objects.

**Related topics:**

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

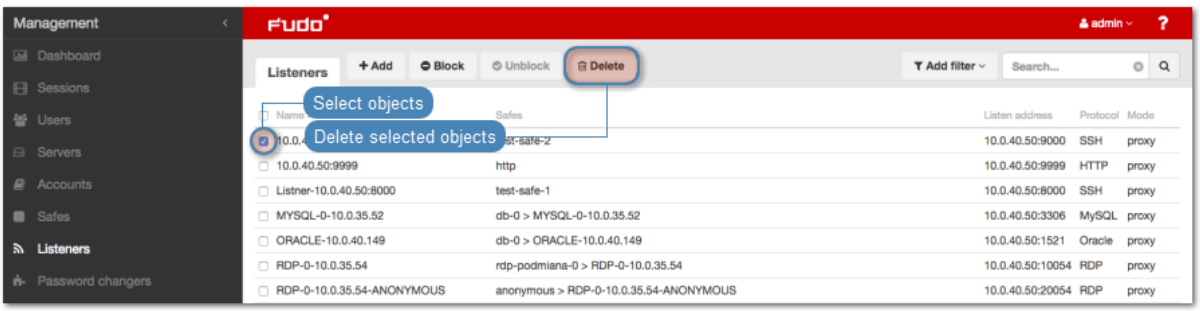
## 9.5 Deleting a listener

**Warning:** Deleting a listener will terminate current connections with server which uses it.

1. Select *Management* > *Listeners*.
2. Find and select desired listener.

**Note:** Define filters to limit the number of objects displayed on the list.

3. Click *Delete*.




4. Confirm deleting selected objects.

**Related topics:**

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

ROZDZIAŁ 10

# Password changers

Wheel Fudo PAM uses proprietary *password changers* to manage credentials to privileged accounts defined on monitored servers. Password changer feature supports the following password management scenarios:

- Unix over SSH
- MySQL over SSH
- Cisco over SSH and Telnet
- Cisco Enable Password over SSH and Telnet
- MS Windows over WMI

## 10.1 Password changer policy

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

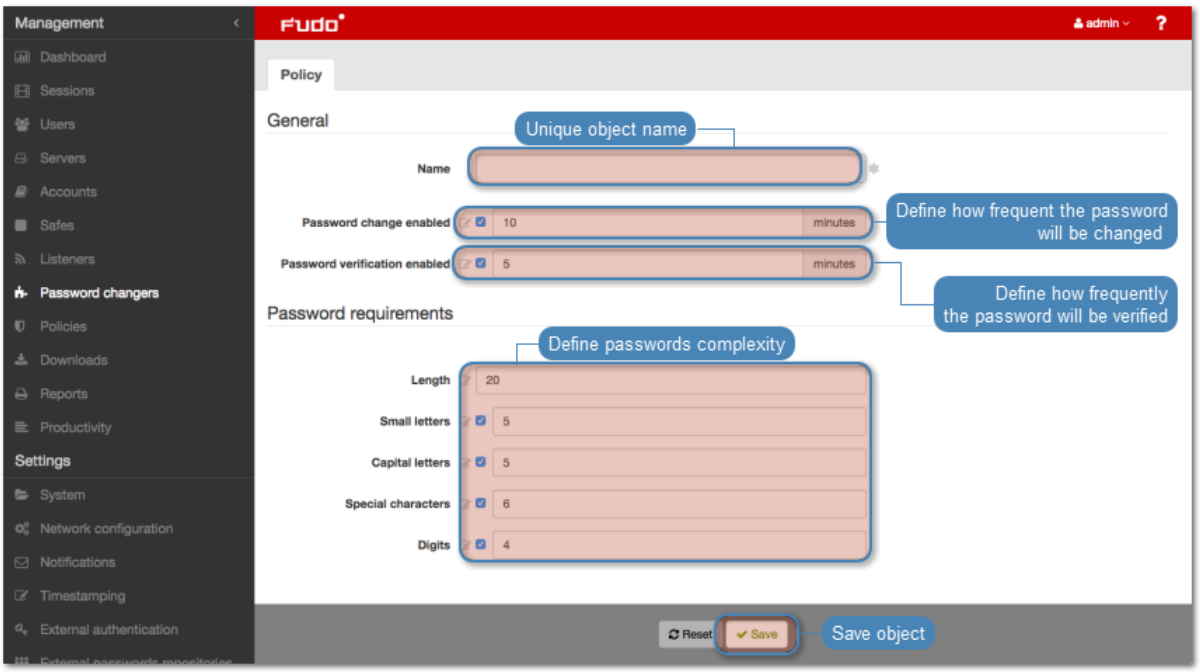
### 10.1.1 Defining a password changer policy

1. Select *Management* > *Password changers*.
2. Click *+ Add*.
3. Enter object name.
4. Select the *Password change enabled* option and specify the time interval between each password change.
5. Select the *Password verification enabled* option and specify the time interval between each password verification.
6. 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*.




### 10.1.2 Editing a password changer policy

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

**Note:** Unsaved changes are marked with an icon.

4. Click *Save*.

### 10.1.3 Deleting a password changer policy

1. Select *Management* > *Password changers*.
2. Find and select desired objects.
3. Click *Delete*.
4. Confirm deletion of selected objects.

**Related topics:**

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

## 10.2 Custom password changers

Custom password changers enable defining a set of commands executed on a remote host in order to change the password.

### 10.2.1 Defining a custom password changer

1. Select *Management* > *Password changers*.
2. Select *Custom changers* tab.
3. Click *+ Add*.
4. Define the password changer's name.
5. Click *+* to add a command.
6. Enter command.

**Note:** Commands allow usage of variables listed in the *List of available variables* section. Variables encapsulated in %% charachters will be replaced in all commands (e.g. `%%host%%`).

- *host* - IP address or hostname of the target system (using hostname requires configuring *DNS server*)
- *port* - port number
- *login* - user login
- *secret* - current user password
- *new_secret* - new password

7. Provide optional comments.
8. Repeat steps 5 through 7 to add additional commands.

**Note:** Drag and drop each command to change the execution order.

9. Repeat steps 5 through 8 and define a password verification commands in the *Password verification commands list* section.
10. Click *Save*.
11. *Define password change policy* and *assign the password changer to account*.

**Note: Example**

In this password changer example, the password is changed is triggered with the `passwd` command, followed by the current password string `secret` and the new secret repeated twice `new_secret`. The last command creates a file, which is later used to verify that the password has been changed successfully.

*Password change*

1. passwd
2. %%secret%%
3. %%new_secret%%
4. %%new_secret%%
5. touch /tmp/%%login%%.passwd-changed

*Password verification*

1. stat /tmp/%%login%%.passwd-changed | | exit 1
2. touch /tmp/%%login%%.passwd-verified

### 10.2.2 Editing a custom password changer

1. Select *Management* > *Password changers*.
2. Select *Custom changers* tab.
3. Click the name of desired password changer.
4. Edit selected commands.

5. Click *X* to remove selected command.
6. Click *Save*.

### 10.2.3 Deleting a custom password changer

1. Select *Management* > *Password changers*.
2. Select *Custom changers* tab.
3. Select desired elements and click *Delete*.
4. Confirm deleting selected objects.

**Related topics:**

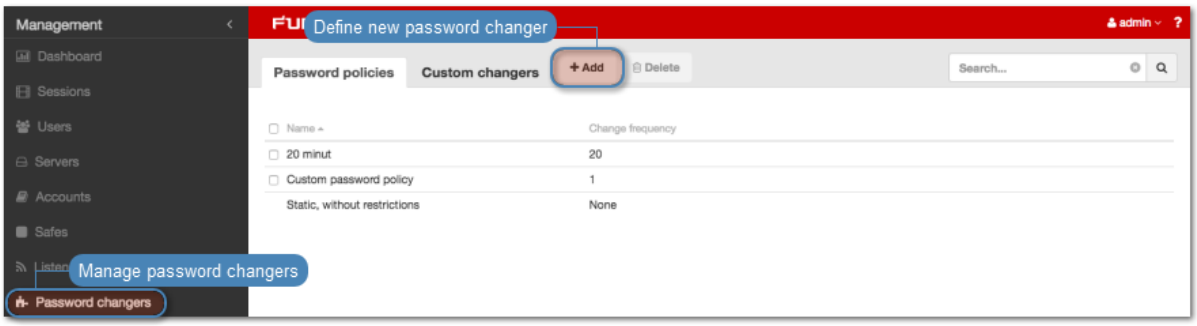
- *Data model*
- *Accounts*
- *Password changer policy*
- *Setting up password changing on a Unix system*

## 10.3 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. Click *+ Add* to create a new password changing policy.




3. Provide password change policy name.

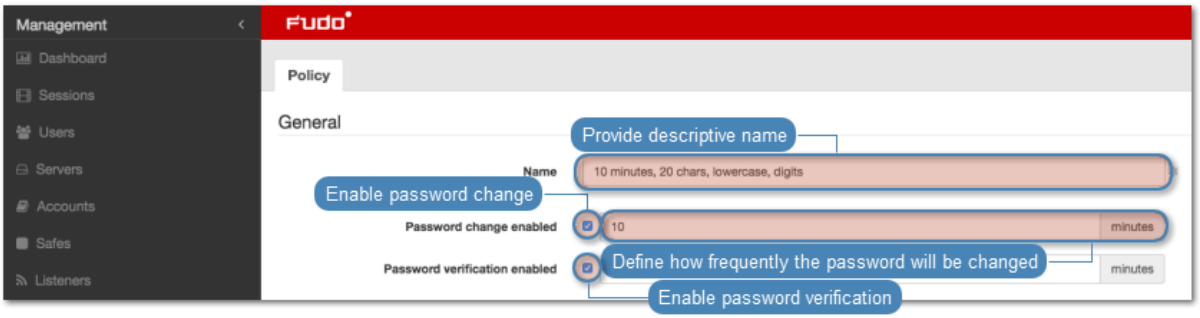
---

**Note:** Provide a descriptive name so that anyone administrating Wheel Fudo PAM can tell what the policy does at a glance. E.g. `10 minutes, 20 characters, special characters, uppercase`.

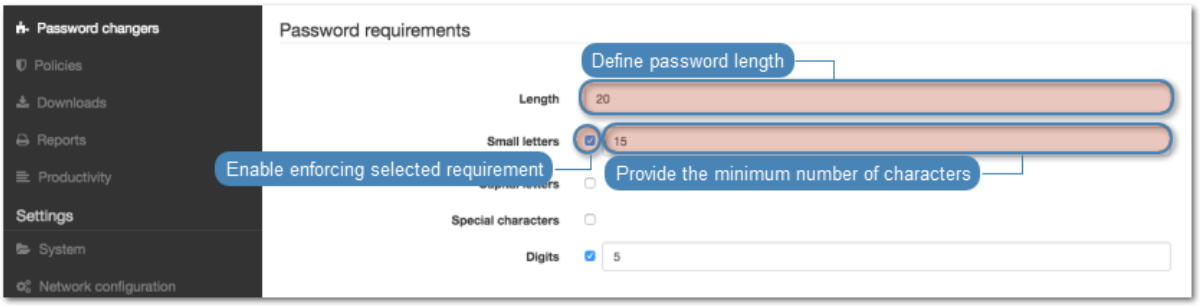
---

4. Select the *Password change enabled* option and define how frequently the password will be changed.

5. Select the *Password verification enabled* option and define how frequently the Secret Manager should verify whether the password has not been changed in any outher way but the Secret Manager itself.



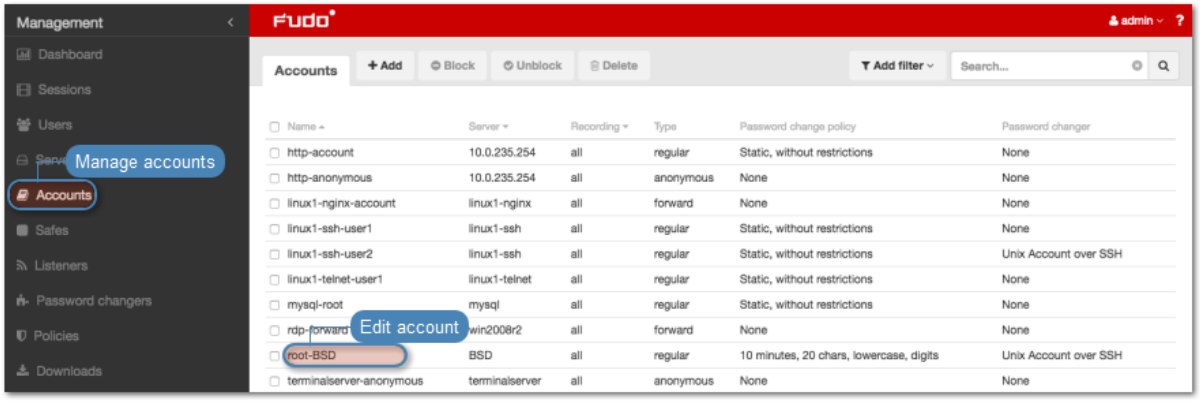

6. Provide the number of characters comprising the password.
7. Select desired password complexity options and provide the minimal number of characters for each.



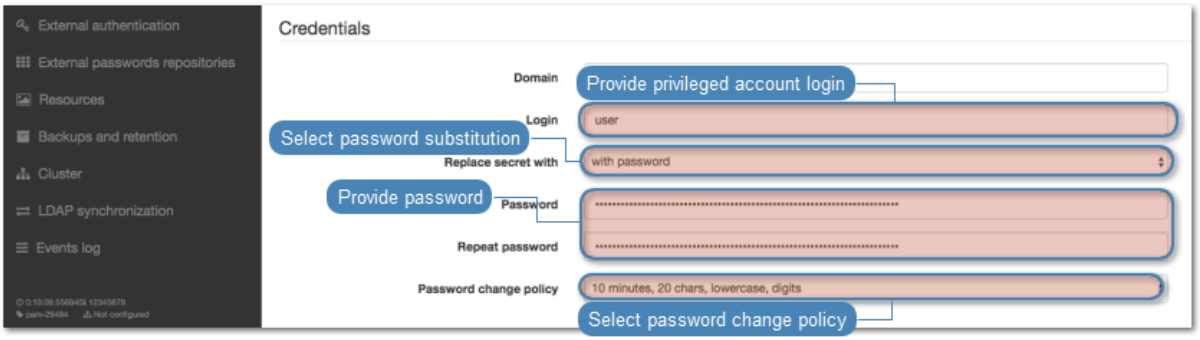

8. Click *Save* to store password changer policy.

**Assigning password changer to the privileged account**

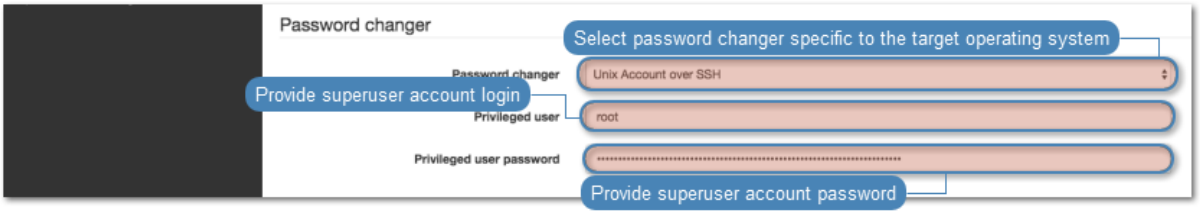
1. Select *Management* > *Accounts*.
2. Find and click desired account object.




3. Provide the privileged account login in the *Credentials* section.
4. Select `with password` from the *Replace secret* drop-down list.
5. Provide privileged account password.
6. Select your policy from the *Password change policy* drop-down list.




7. In the *Password changer* section, select the `Unix Account over SSH` from the *Password changer* drop-down list.
8. Provide superuser login credentials.




**Note:** Superuser account enables resetting the password in case the *Secret manager* detects that it has been changed by someone else.

9. Click *Save*.

**Related topics:**

- *Requirements*
- *Data model*

## 10.4 Setting up password changing on Michrosoft Windows system

This topic contains an example of setting up password changing to Microsoft Windows account over WMI.

**Note: Windows WMI password changer**

Using Windows WMI password changers requires granting sufficient permissions to regular users.

- Run the `winrm quickconfig` command to detect any potential issues, turn on the *LocalAccountTokenFilterPolicy* option and unblock ports on internal firewall.
- In case the *winrm* is unavailable, execute the following command `cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f`

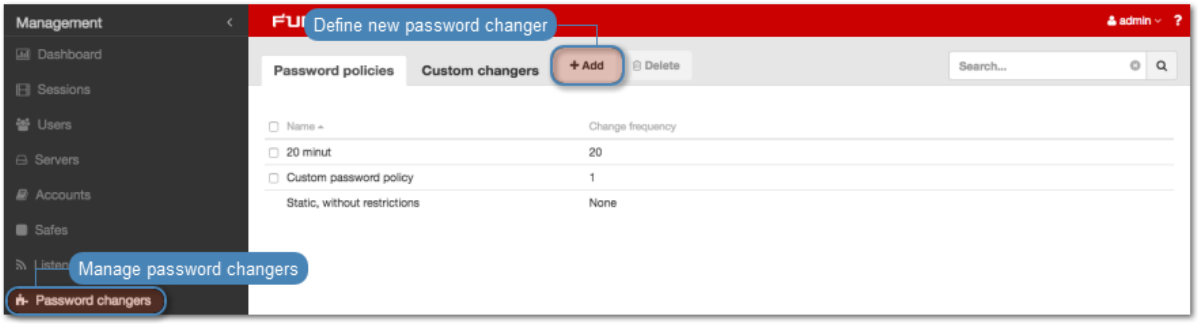
  Additionally, unblock WMI and DCOM ports and change the network interface type to *Office network*.

If neither of the above has brought expected results, the administrator must explicitely asign users and groups priviledges to WMI or DCOM using *wmimgmt.msc* and *dcomcnfg*:

- http://www-01.ibm.com/support/docview.wss?uid=swg21681046
- https://technet.microsoft.com/en-us/library/cc771551(v=ws.11).aspx

### Adding a password change policy

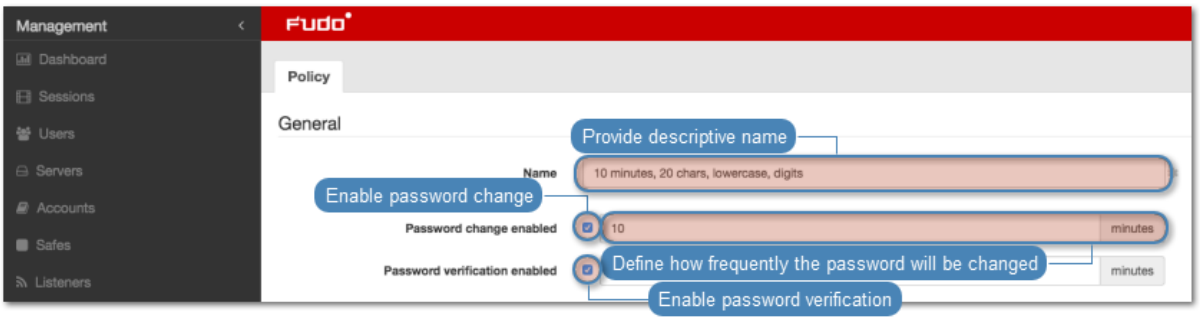
1. Select *Management* > *Password changers*.
2. Click *+ Add* to create a new password changing policy.



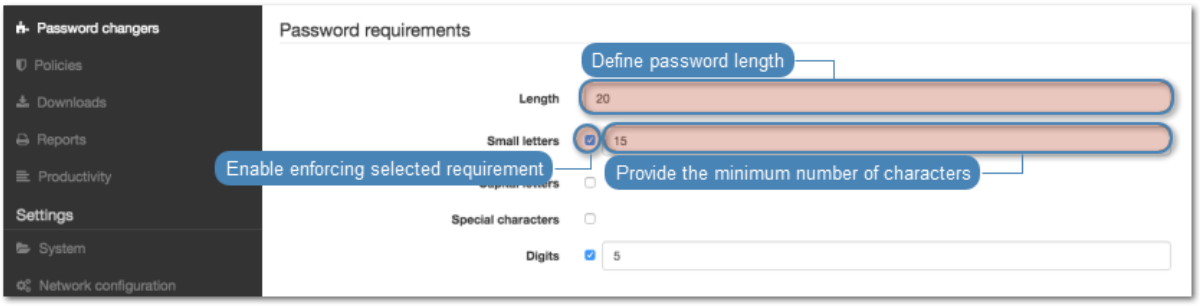

3. Provide password change policy name.

**Note:** Provide a descriptive name so that anyone administrating Wheel Fudo PAM can tell what the policy does at a glance. E.g. `10 minutes, 20 characters, special characters, uppercase`.

4. Select the *Password change enabled* option and define how frequently the password will be changed.
5. Select the *Password verification enabled* option and define how frequently the Secret Manager should verify whether the password has not been changed in any outher way but the Secret Manager itself.



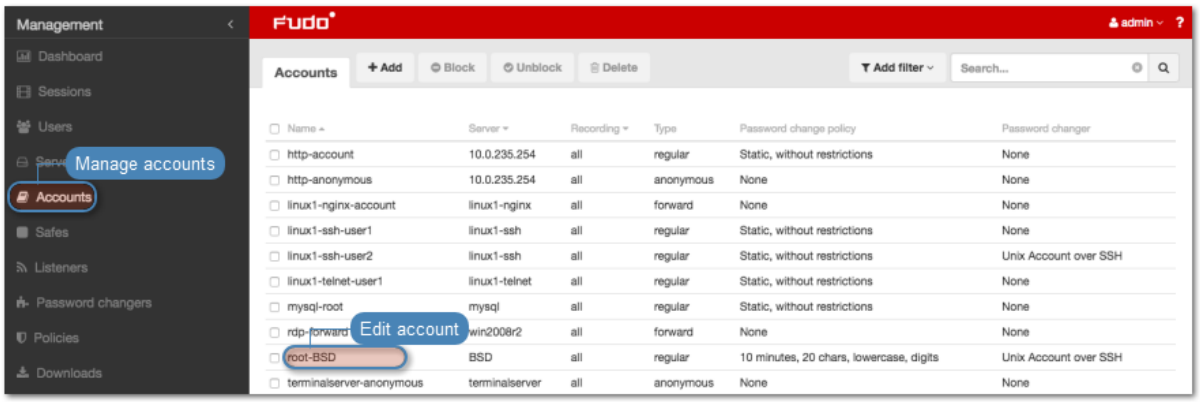

6. Provide the number of characters comprising the password.
7. Select desired password complexity options and provide the minimal number of characters for each.



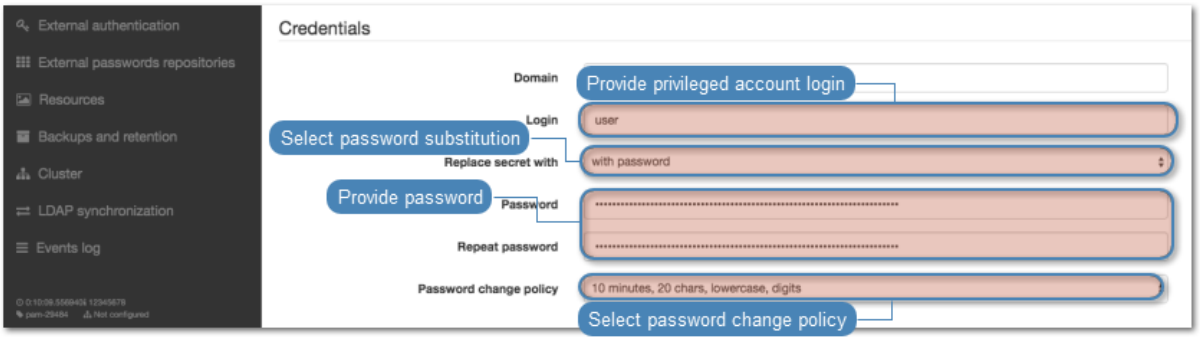

8. Click *Save* to store password changer policy.

**Assigning password changer to the privileged account**

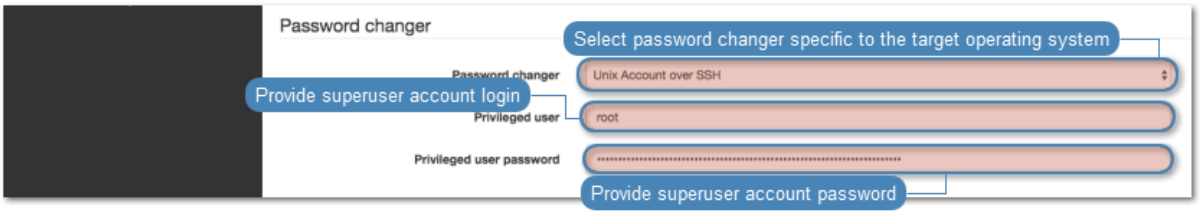
1. Select *Management* > *Accounts*.
2. Find and click desired account object.




3. Provide the privileged account login in the *Credentials* section.
4. Select `with password` from the *Replace secret* drop-down list.
5. Provide privileged account password.
6. Select your policy from the *Password change policy* drop-down list.




7. In the *Password changer* section, select the `Unix Account over SSH` from the *Password changer* drop-down list.
8. Provide superuser login credentials.




**Note:** Superuser account enables resetting the password in case the *Secret manager* detects that it has been changed by someone else.

9. Click *Save*.

**Related topics:**

- *Requirements*
- *Data model*

ROZDZIAŁ 11

# Policies

Policies are patterns definitions facilitating proactive session monitoring. In case a defined pattern is detected, Wheel Fudo PAM can automatically pause or terminate given connection, block the user and send notification to Wheel Fudo PAM administrator.

**Defining patterns**

**Note:** Wheel Fudo PAM supports POSIX extended regular expression.

1. Select *Management* > *Policies*.
2. Select *Regular expressions* tab.
3. Click + *Add regular expression*.

4. Enter pattern name.
5. Define the pattern itself.

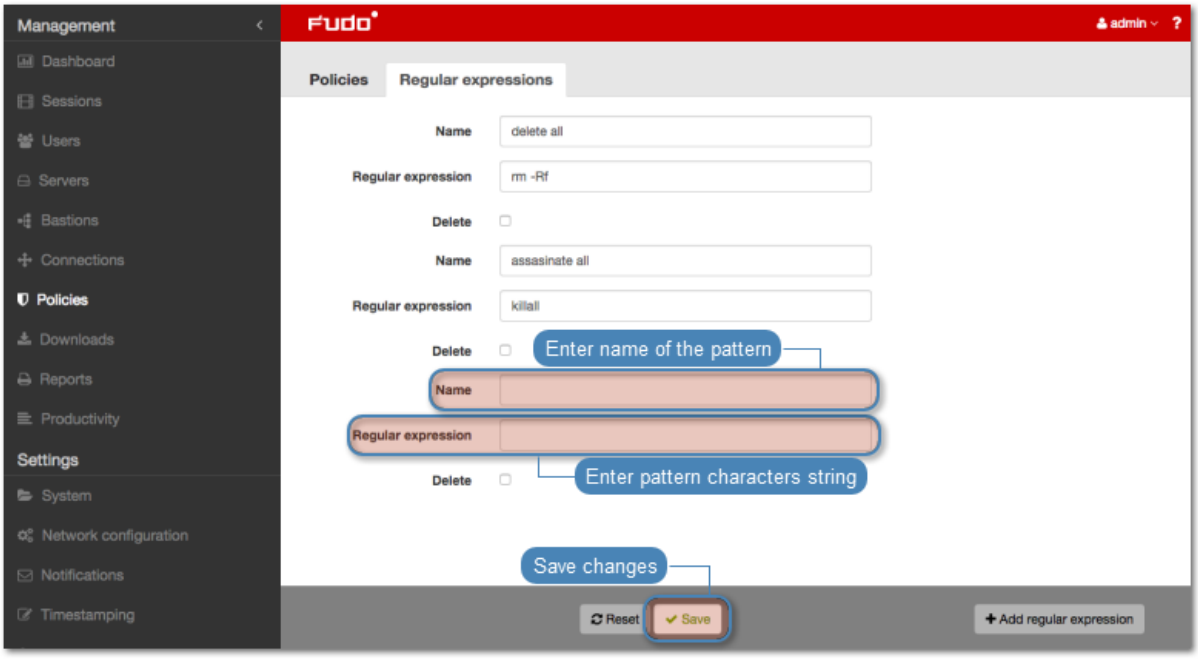
---

**Note:**

- Patterns can be defined as regular expressions.
- Wheel Fudo PAM 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*.




---

**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])
```

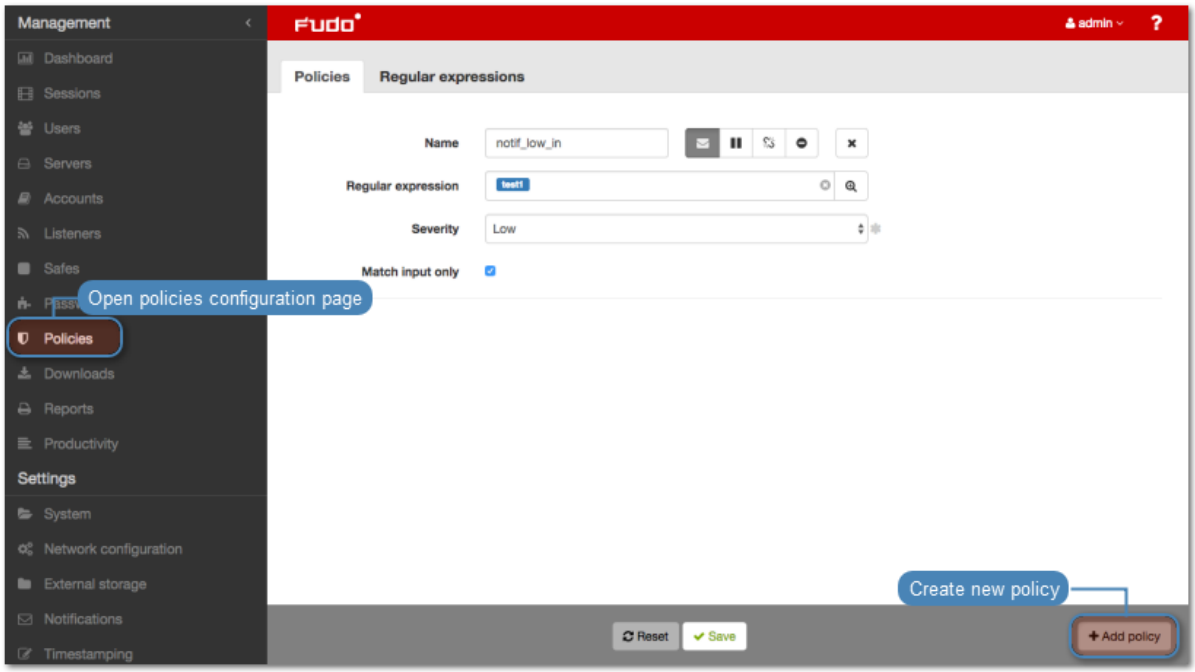
*Command* `rm file`

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

---

### Defining policies

1. Select *Management* > *Policies*.
2. Click *Add policy*.




3. Enter policy name.
4. Select actions.

| | |
|---|---|
| | Send email notification to system administrator. |
| | Pause connection. |
| | Terminate connection. |
| | Block user. |

**Note:**

- Sending email notifications requires configuring and enabling *notification service* as well as *Session policy match* notification enabled in *safe configuration*.
- Note that blocking the user automatically terminates the connection.

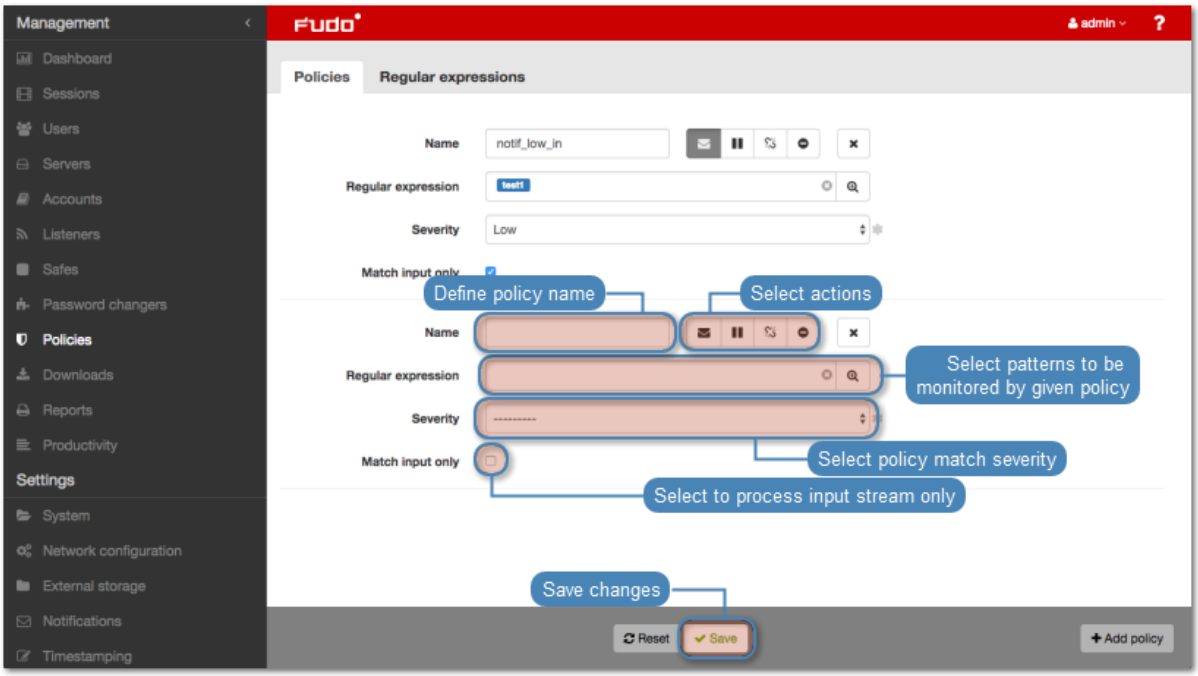
5. Select monitored patterns.
6. Select policy severity.

**Note:** Severity parameter value is included in the email notification message.

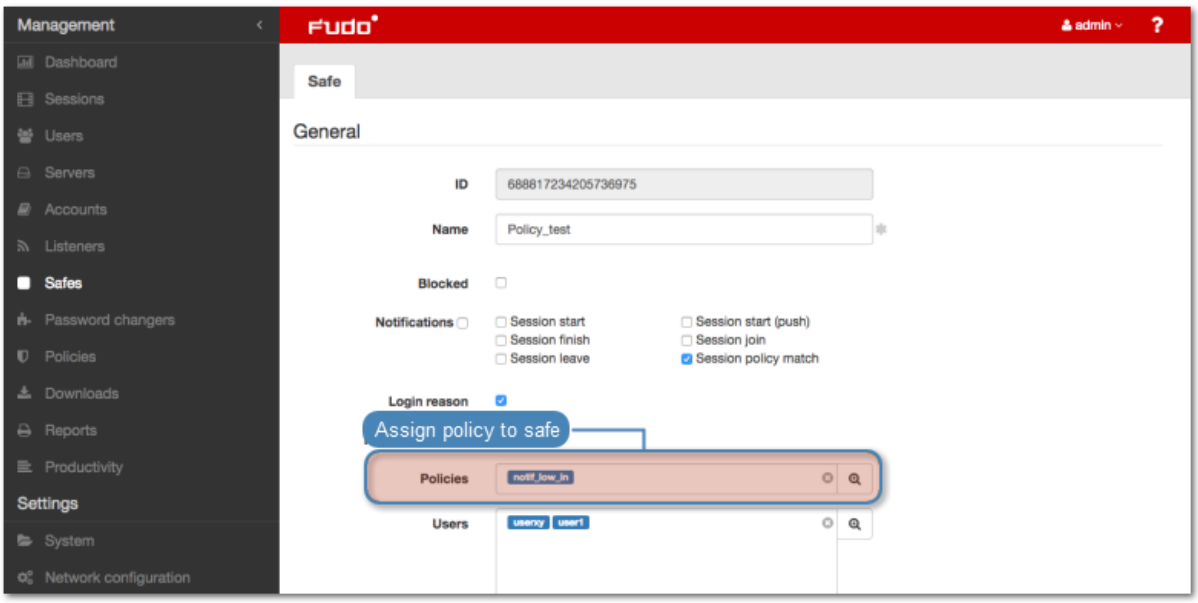
7. Select the *Match input only* option to process input stream only.

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

8. Click *Save*.




**Note:** After defining a policy, you can assign it to a *safe* that is used to establish connections to servers.




### Deleting patterns

1. Select *Management* > *Policies*.
2. Select the *Regular expressions* tab.
3. Find desired pattern definition and select the *Delete* option.
4. Click *Save*.

### Deleting policies

To delete policy definition, proceed as follows.

1. Select *Management* > *Policies*.
2. Find desired policy definition and select corresponding *Delete* option.
3. Click *Save*.

### Related topics:

- *Safes*
- *Terminating connection*
- *Notifications*

- *Security*

ROZDZIAŁ 12

# Sessions

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

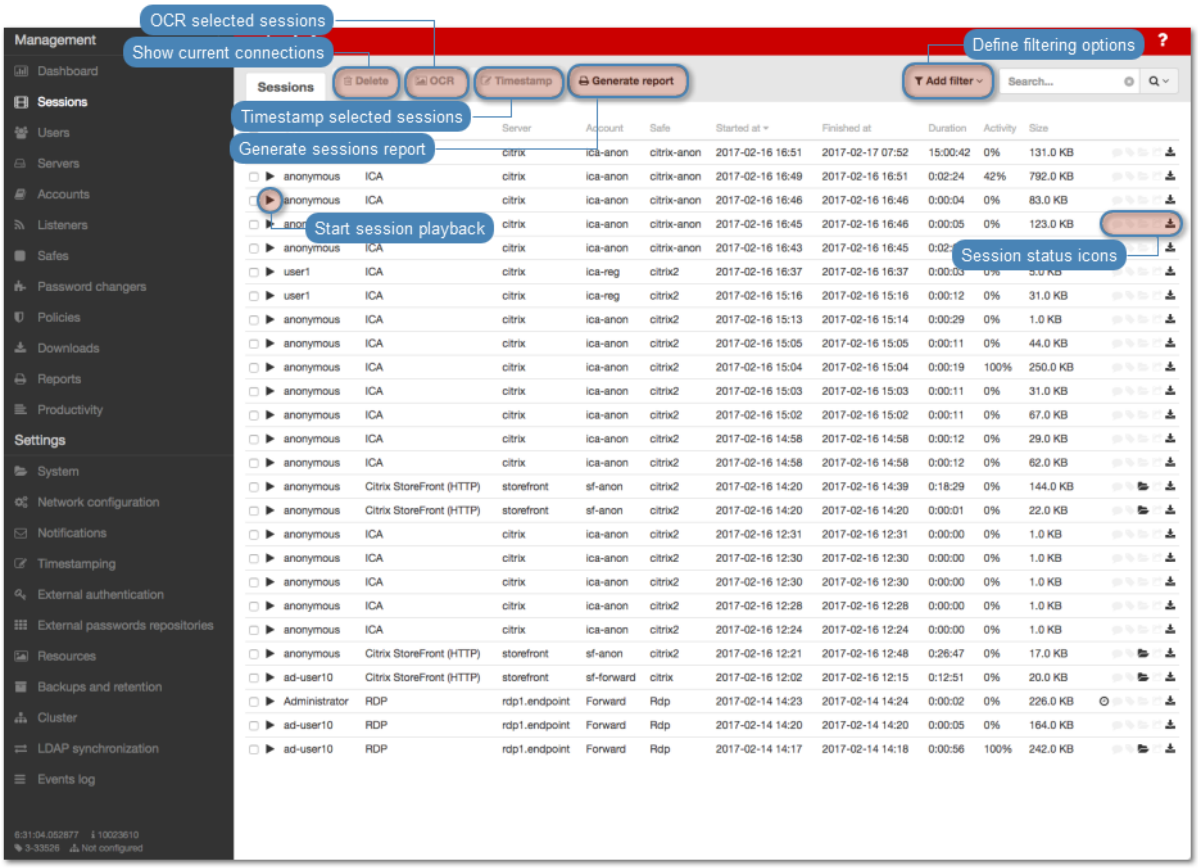
Sessions management page allows filtering stored user sessions, accessing current users connections and downloading stored sessions. It also provides status information on each session and enables access to session sharing options.

**Note:** Cotents of the session list depend on the logged in user's access rights. Being able to access a given session requires having management priviliges 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. |
| ↗ | Access session sharing management options. |
| ⬇ | Download session material i 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 whom approved pending session. |
| ✔ | Approve pending connection. |
| ✖ | Decline pending connection. |
| ? | Pending connection awaiting authorization. |
| ✚ | Element aggregating connections established within the same session. |

To open sessions management page, select *Management* > *Sessions*.

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

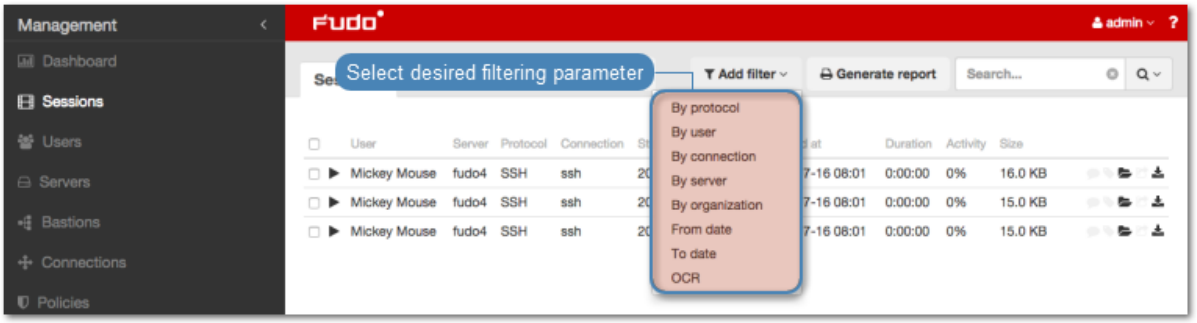



## 12.1 Filtering sessions

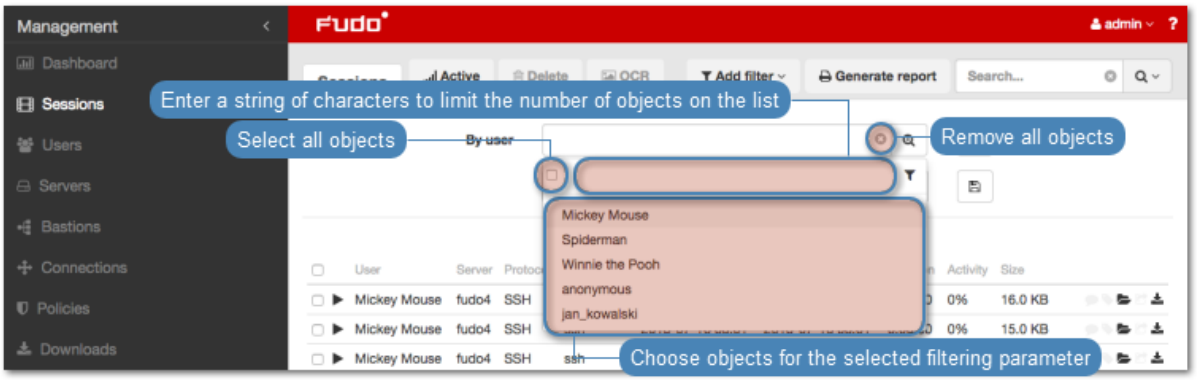
Sessions filtering allows to find desired sessions easily by limiting the number of displayed sessions on the sessions management page.

### 12.1.1 Defining filters

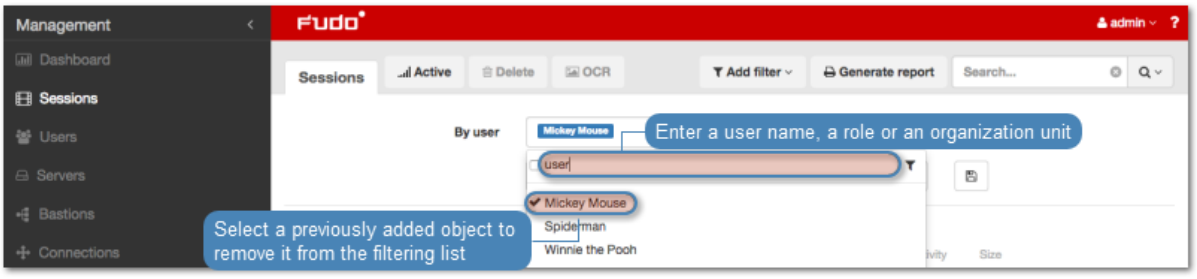
1. Click *Add Filters* and select desired data type from the drop-down list.




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

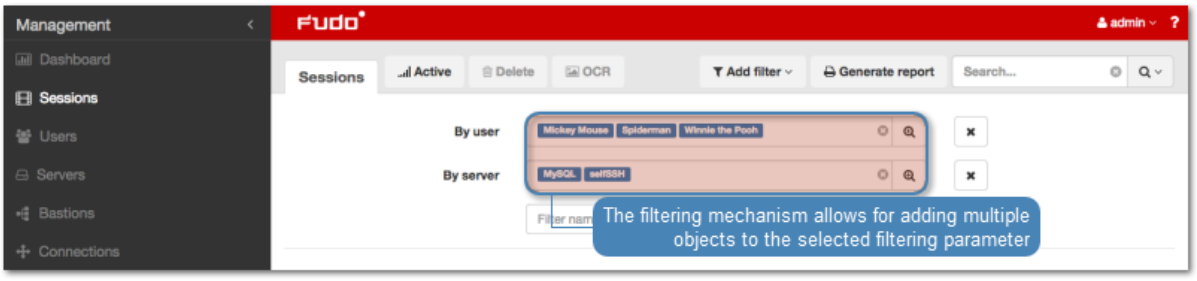



**Note:** Enter a string of characters to limit the number of the elements on the list. In case of users, the elements on the list can be limited to those who have a given user role assigned or belong to the given organization unit.




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

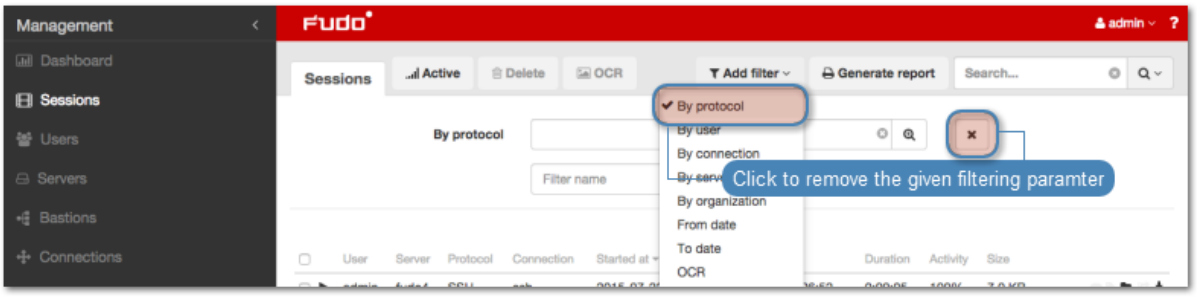
Protocol, user, connection, server and organization parameters allow for selecting multiple objects of the given type.




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

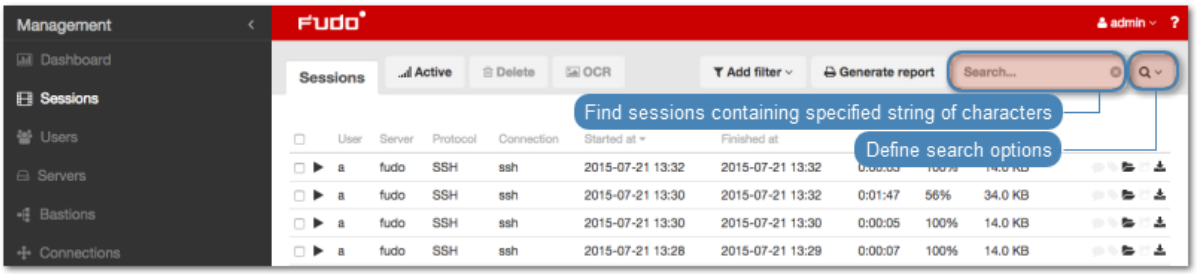
**Note:** Only sessions which match all defined filtering parameters will be displayed.

4. Click *Add Filter* and select previously added filtering parameter to disable given filter.



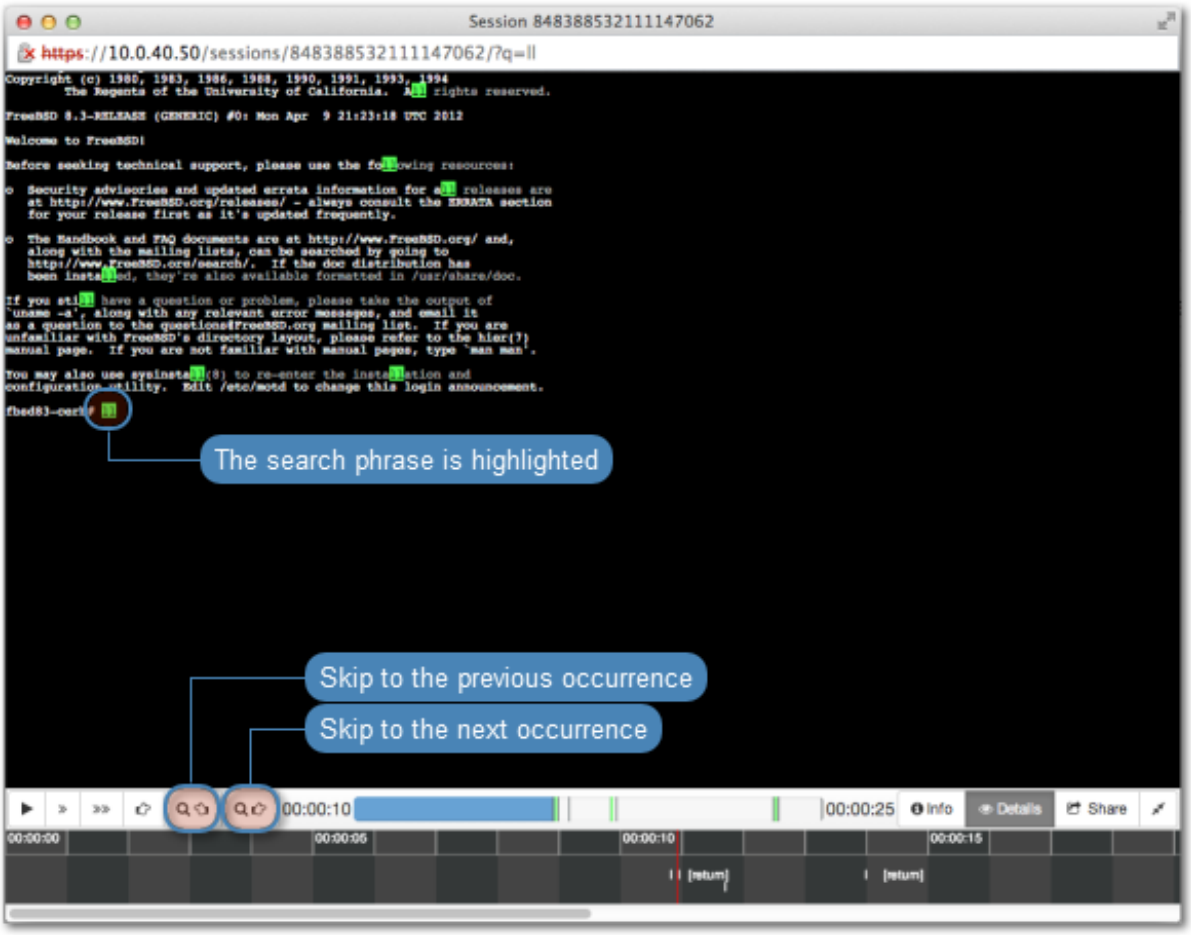

### 12.1.2 Full text search

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




**Note:** 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.

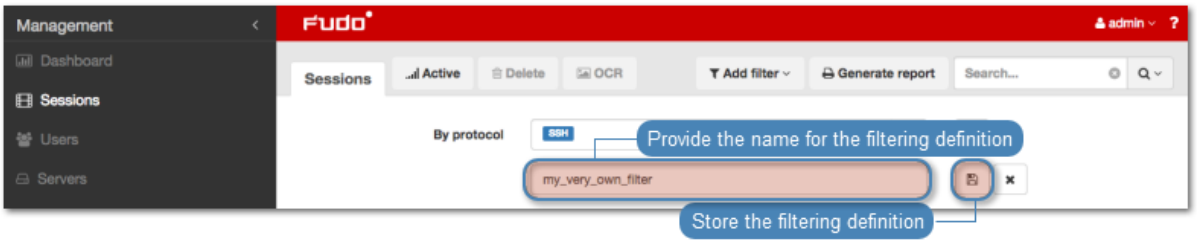



### 12.1.3 Managing user defined filter definitions

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

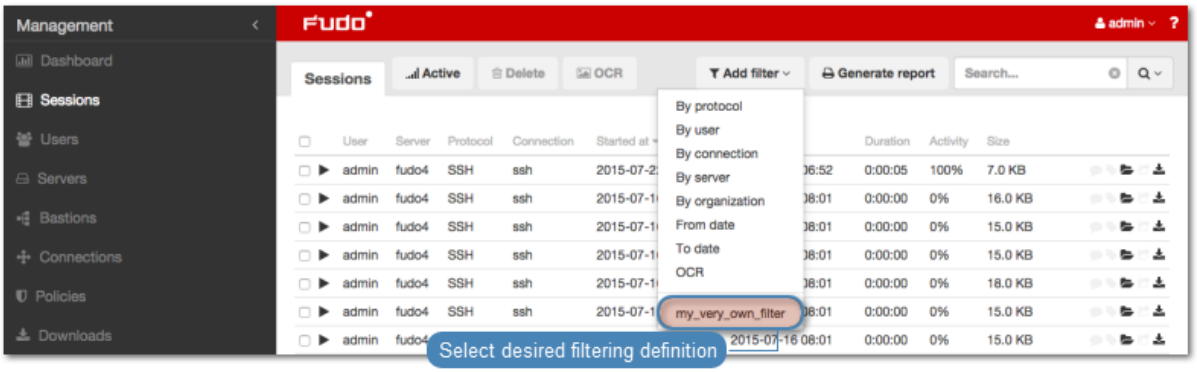
**Storing a user defined filter definition**

1. Define filtering options as described in the *Filtering sessions* section.
2. Provide the name for the filter definition.
3. Click the save icon to store the filter definition.




**Editing a user defined filter definition**

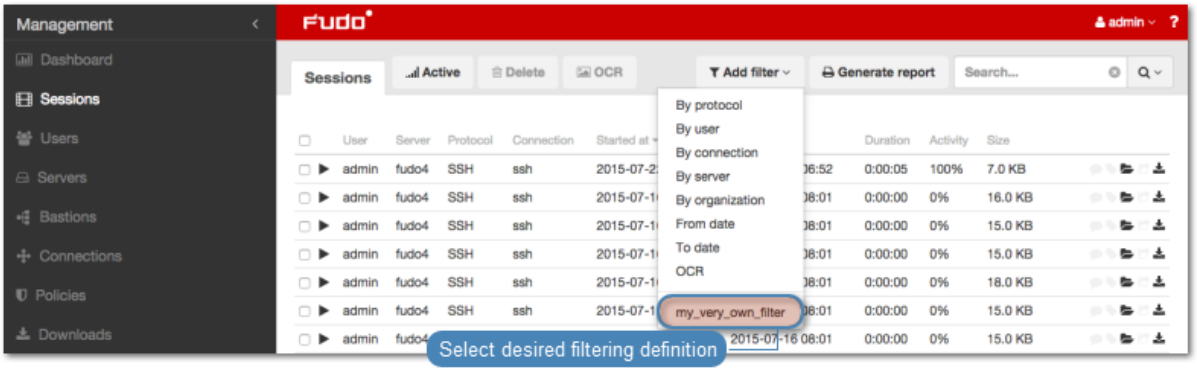
1. Click *Add filter* and select the desired filter definition.



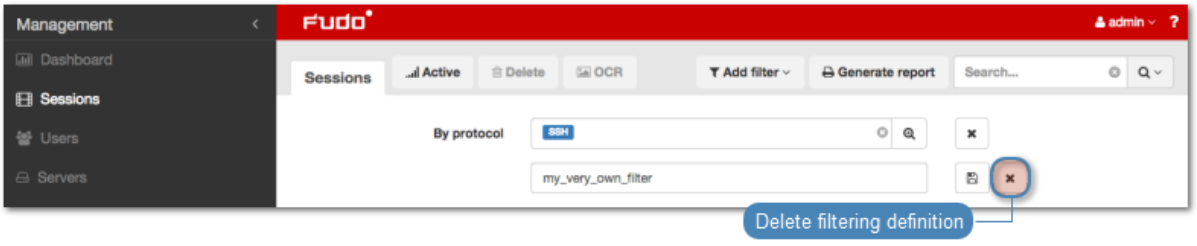

2. Change the filtering parameters as desired.
3. Click the save icon to store changes in the filter definition.

**Deleting a user defined filter definition**

1. Click *Add filter* and select the desired filter definition.




2. Click the delete icon to remove the filtering definition.




3. Confirm deleting the selected filtering definition.

**Related topics:**

- *System overview*
- *Reports*

## 12.2 Viewing sessions

Wheel Fudo PAM allows viewing recorded sessions as well as current user connections.

To view a session, proceed as follows.

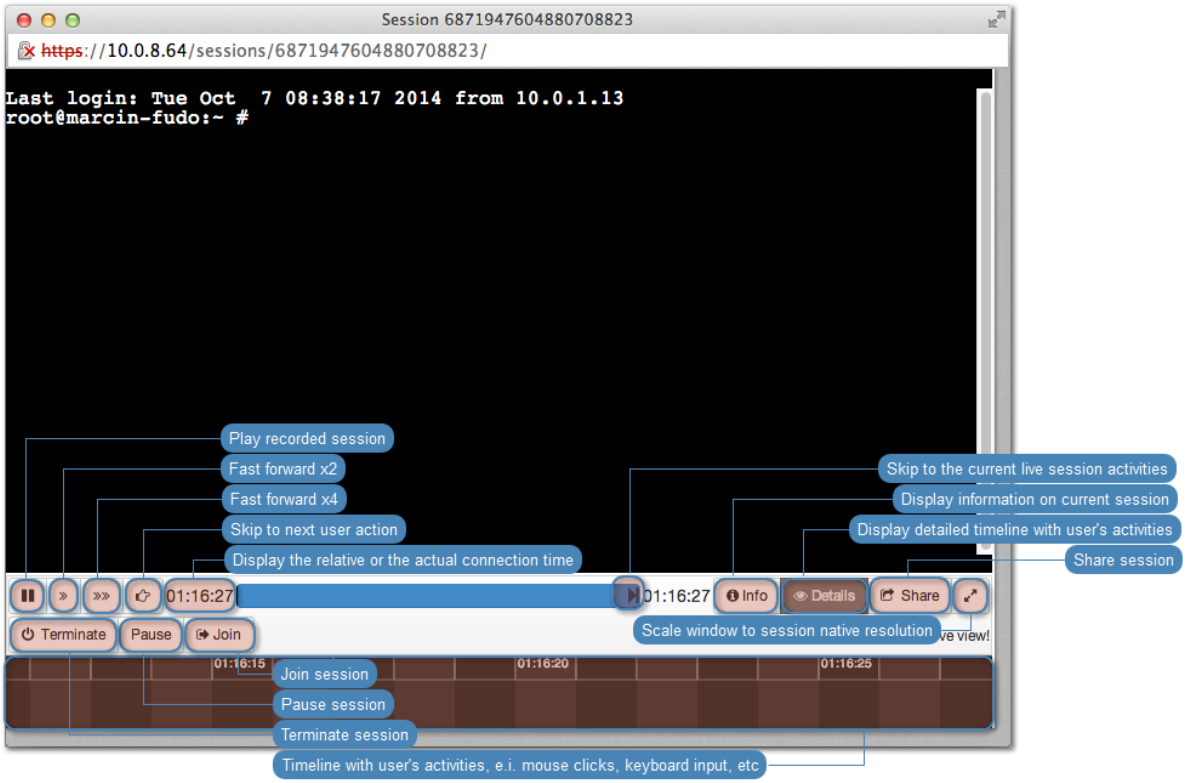
1. Select *Management* > *Sessions*.
2. Find desired session and click the play icon next to it.

**Session player options**

---

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

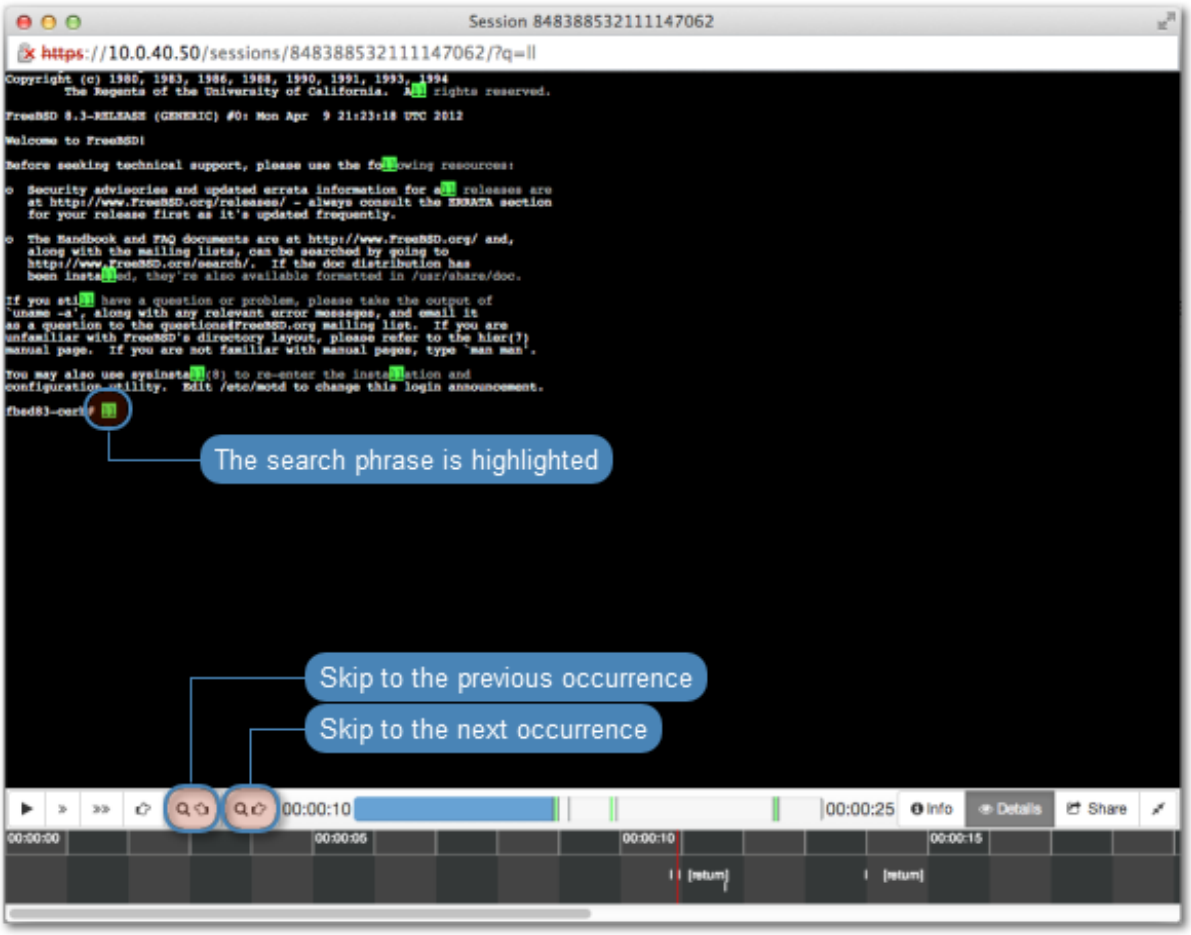
---



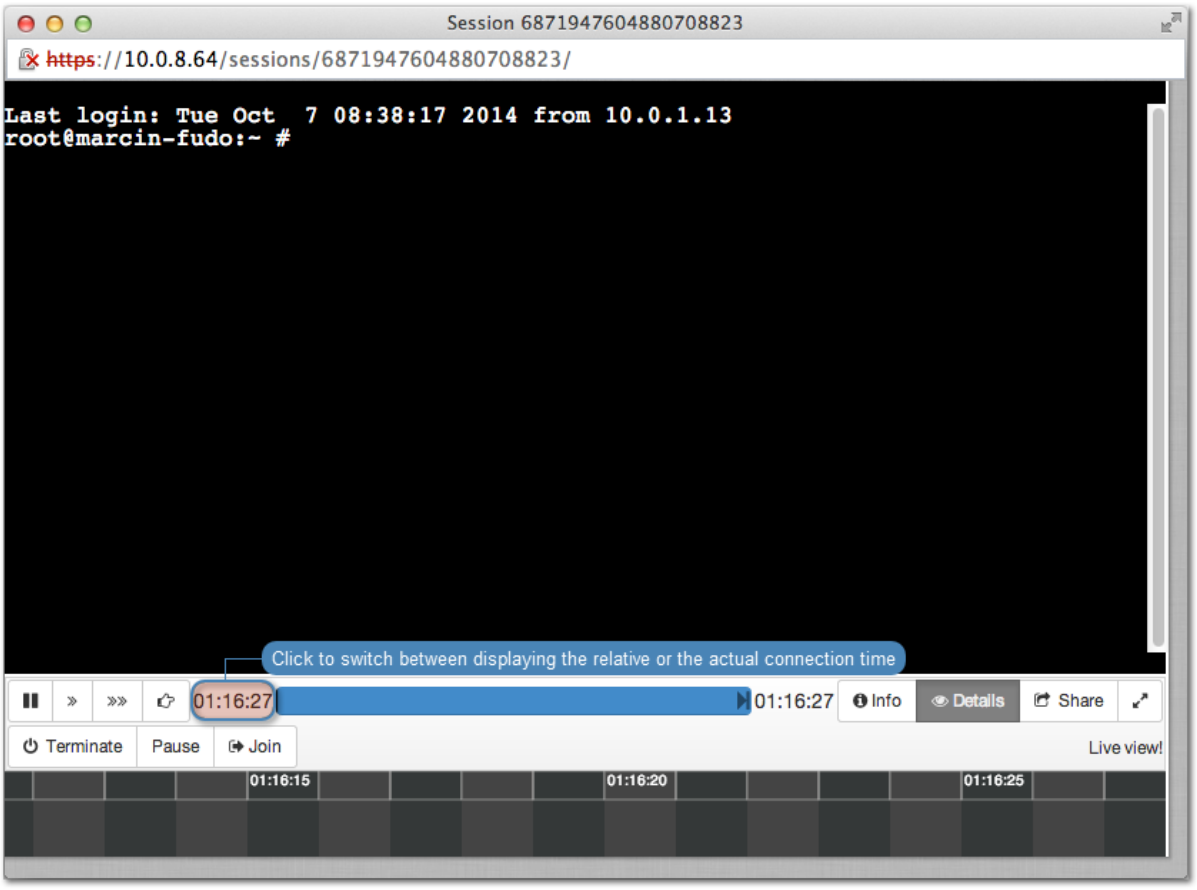

---

**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.




**Related topics:**

- *Sensitive features*

## 12.3 Viewing live sessions

Wheel Fudo PAM enables viewing current connection sessions, allowing to supervise user's activities.

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 play icon to start playback.

**Related topics:**

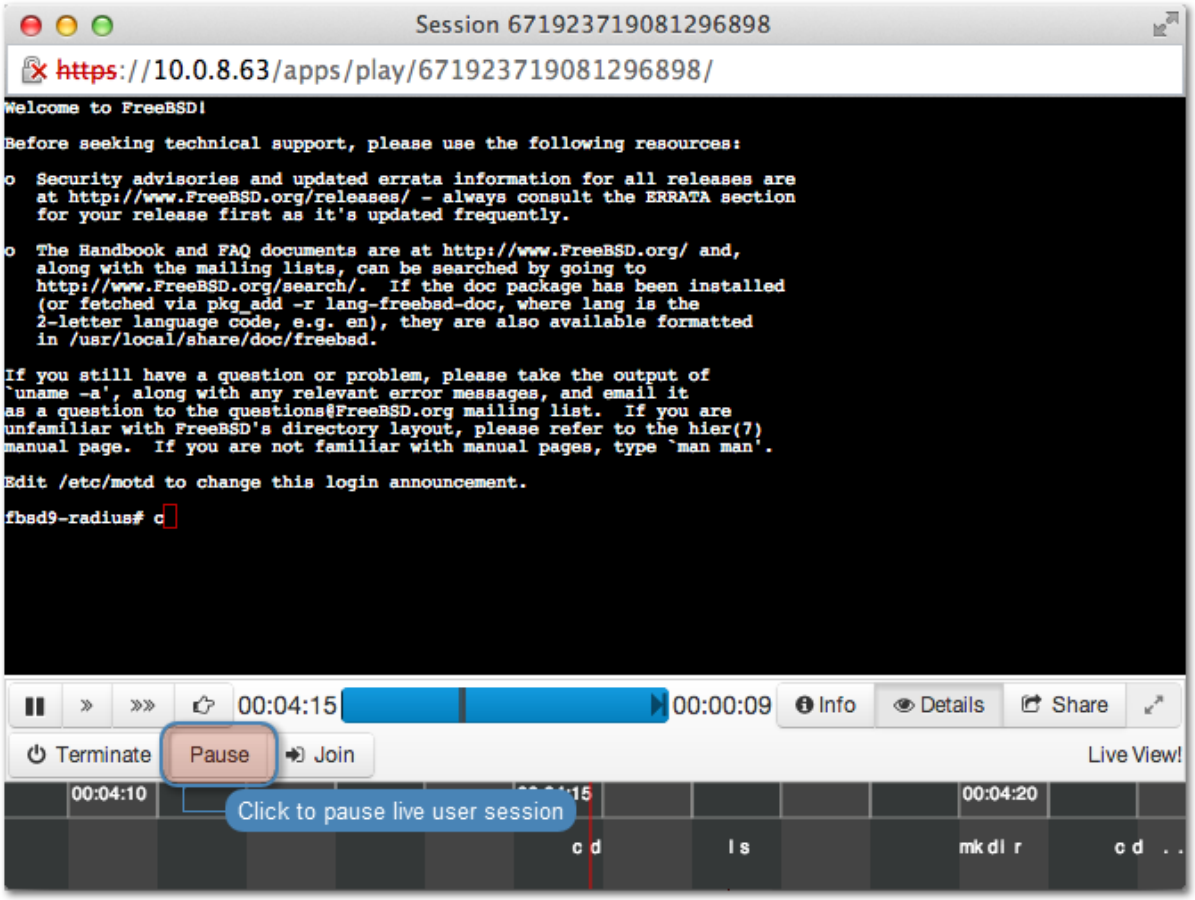
- *Viewing sessions*
- *Terminating connection*

## 12.4 Pausing connection

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

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

1. Select *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*

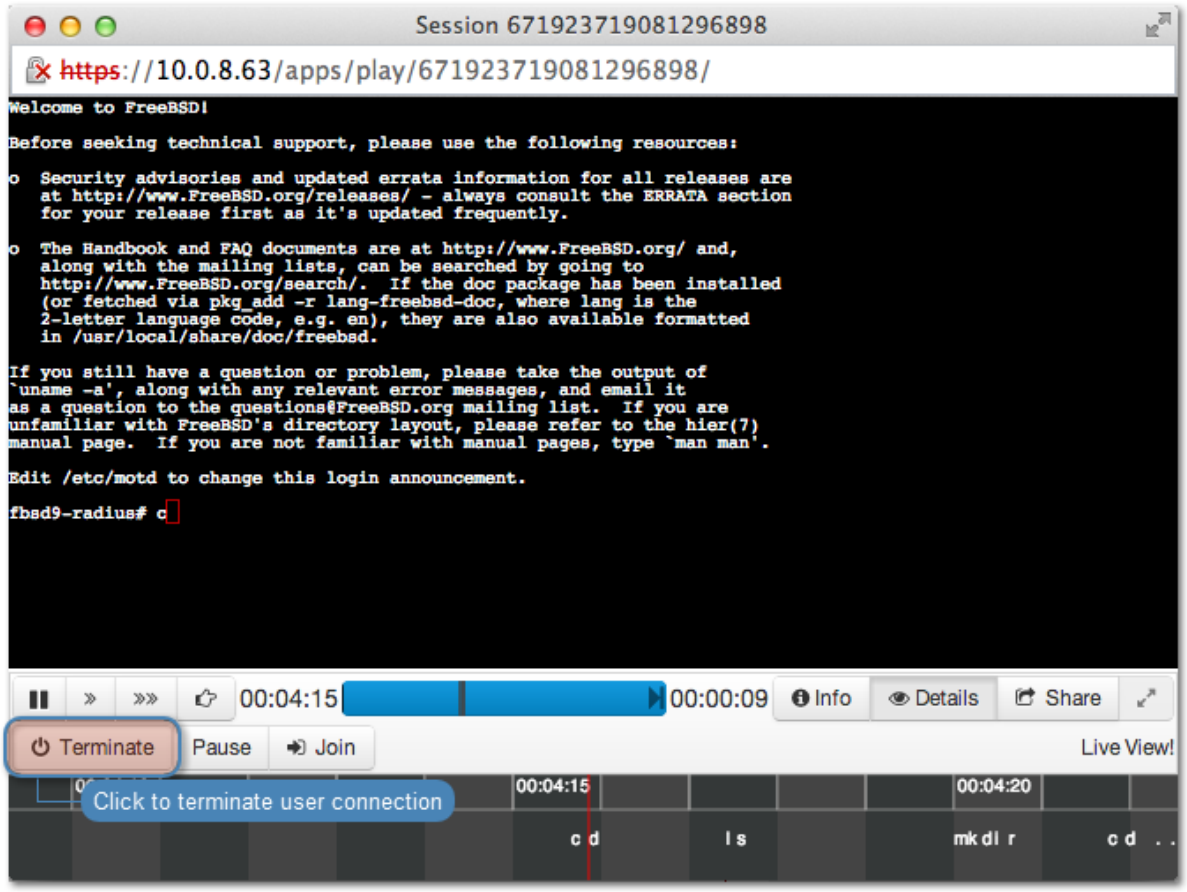
## 12.5 Terminating connection

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

**Note:** Wheel Fudo PAM 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*

## 12.6 Joining live session

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

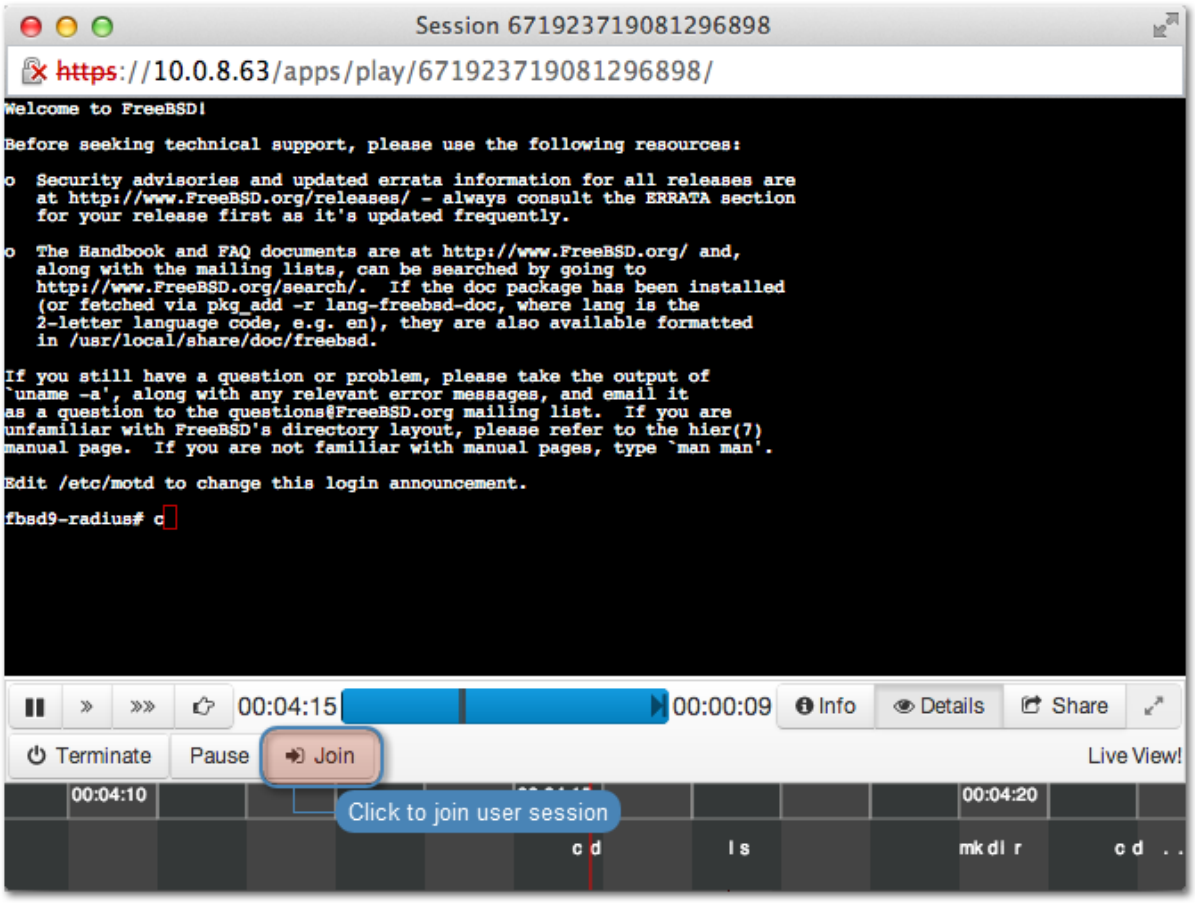
---

**Note:** Session joining feature is supported in SSH, RDP, VNC and Telnet (excluding 5250 and 3270) connections.

---

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*

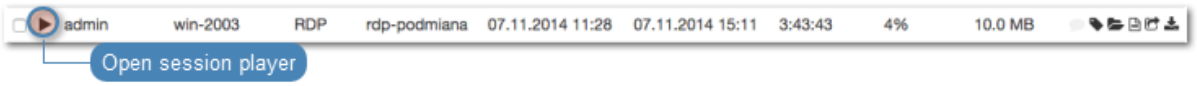
## 12.7 Sharing sessions

Wheel Fudo PAM enables sharing given session with another user.

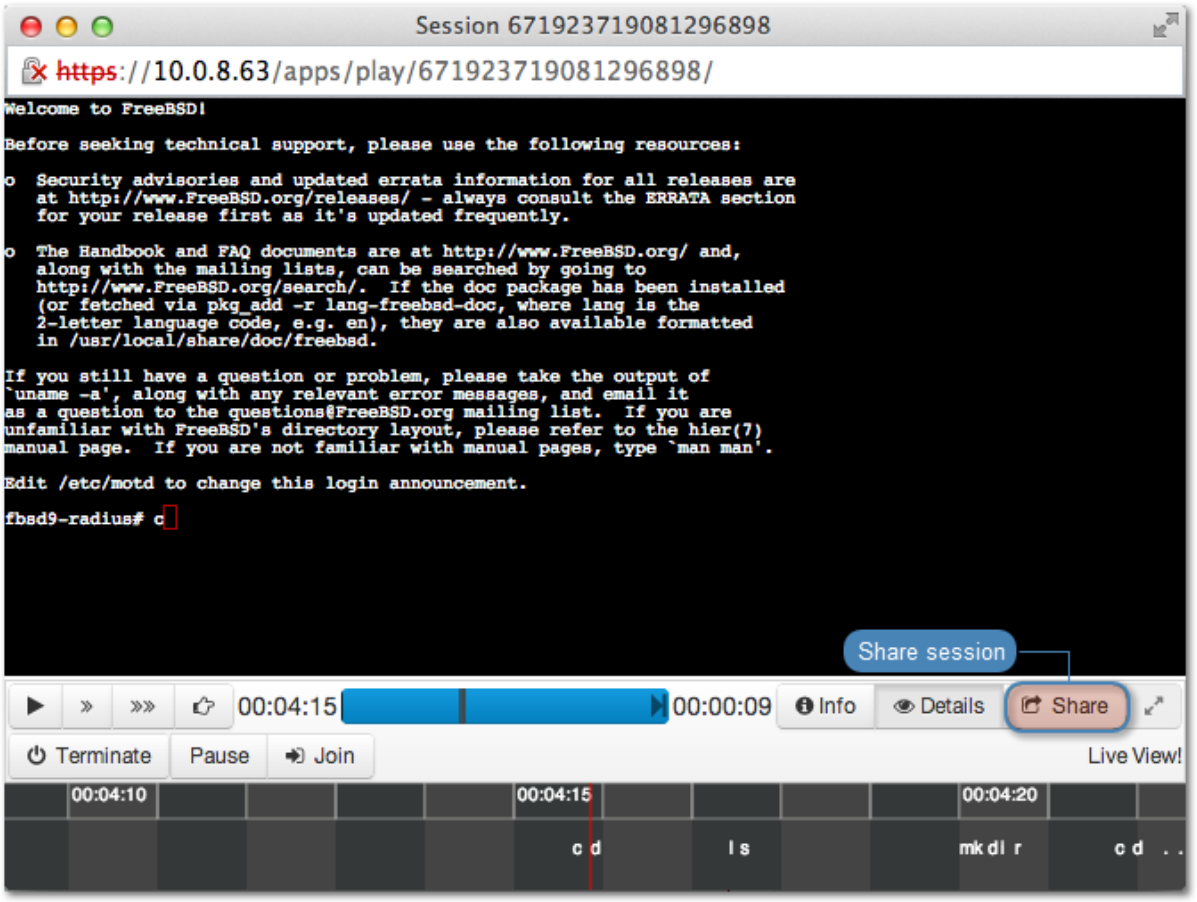
**Sharing a session**

To share a session, proceed as follows.

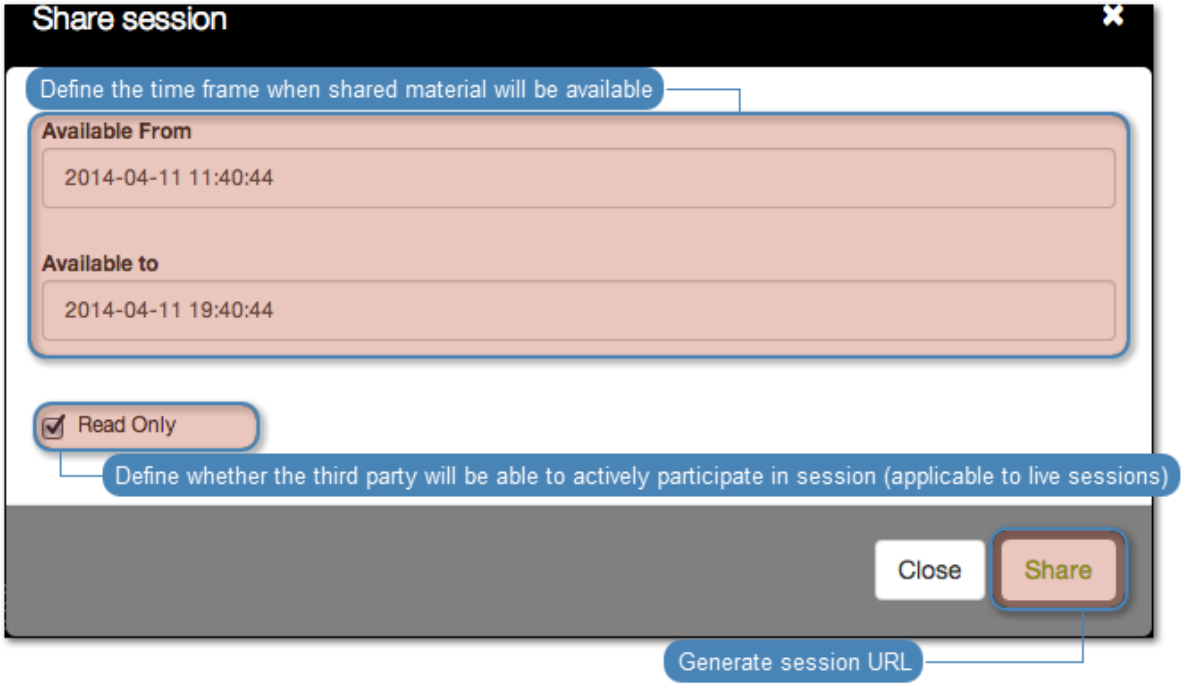
1. Select *Management* > *Sessions*.
2. Find desired session and and click the play icon to start playback.




3. Click *Share*.




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

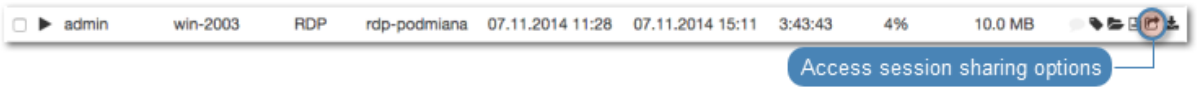



5. Copy the system generated URL and click *Close*.

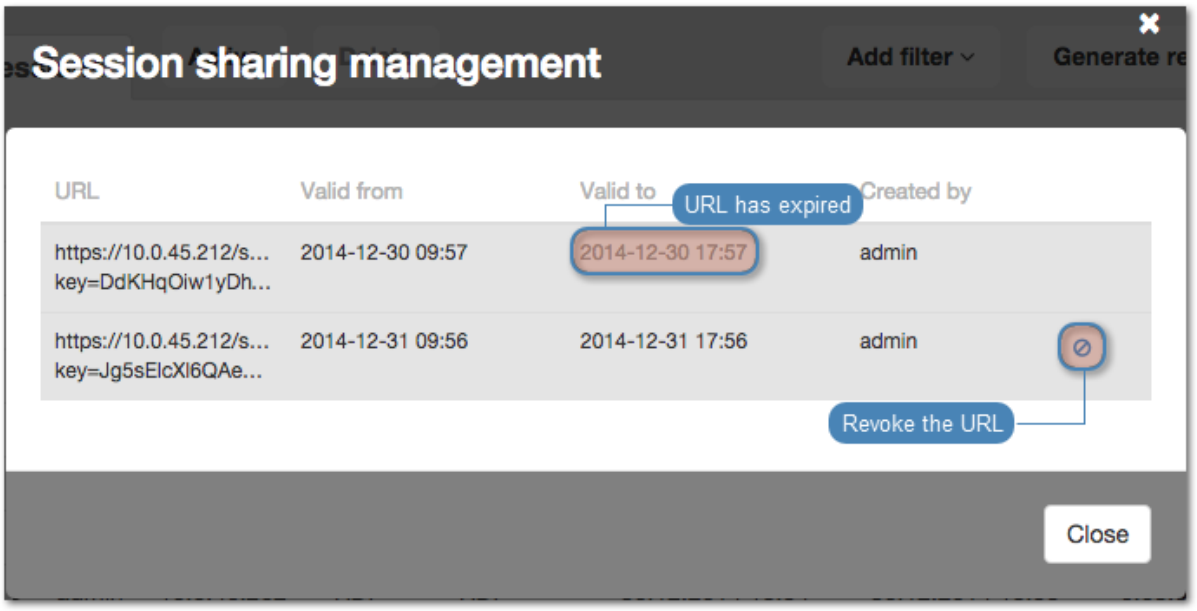
### Revoking session URL

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*

## 12.8 Commenting sessions

Wheel Fudo PAM enables adding comments and tags to recorded sessions.

**Adding a comment**

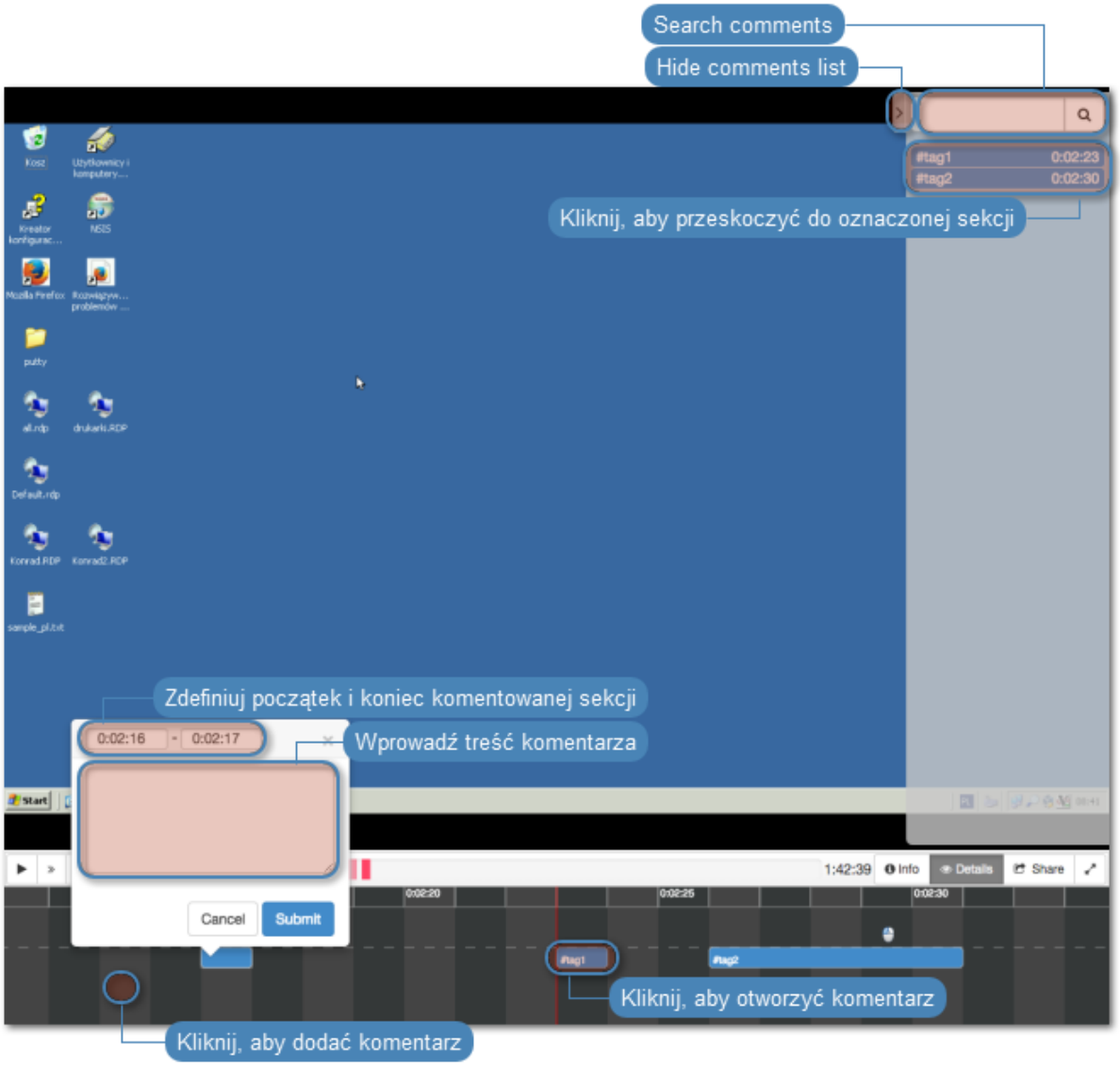
1. Select *Management* > *Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Details*.
4. Click the lower part of the timeline to add a comment.
5. Define time interval which applies to this comment.

---

**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*

## 12.9 Exporting sessions

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

To export a session, proceed as follows.

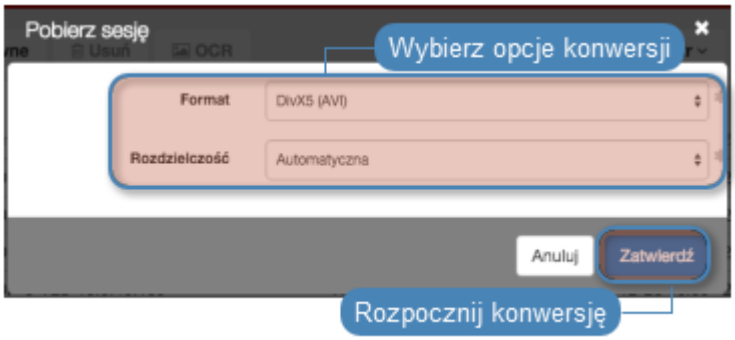
1. Select *Management* > *Sessions*.
2. Find desired session and click the session export icon.

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.

---

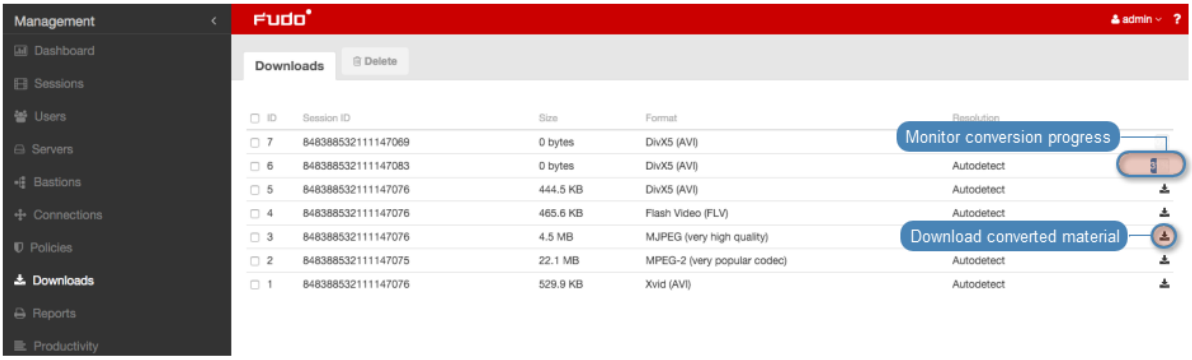
5. Click *Confirm* to start conversion and open the downloads page.

---

**Note:** The *Downloads* page enables monitoring conversion progress.

---

6. Find desired session and click the *Download* icon to download converted session material.




**Related topics:**

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

- *Joining sessions*

## 12.10 Deleting sessions

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:** Wheel Fudo PAM 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*
- *Replaying sessions*
- *Exporting sessions*

## 12.11 OCR processing sessions

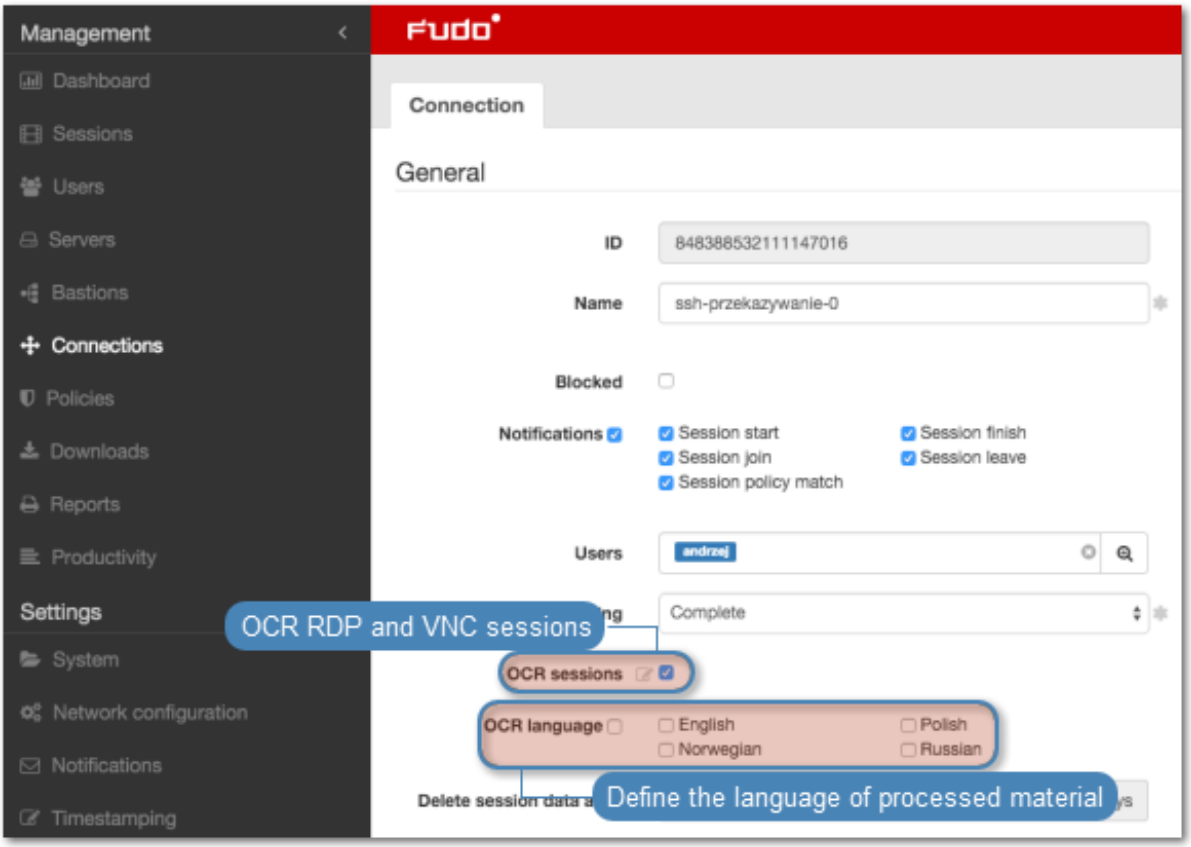
Recorded RDP and VNC sessions can be processed and indexed for full-text search purposes.

**Warning:** OCR processing is CPU intensive and may have negative impact on system's performance.

### Automated sessions processing

To have RDP and VNC sessions automatically processed, proceed as follows.

1. Select *Management* > *Connections*.
2. Find and click desired connection.
3. Select *OCR sessions* option.
4. Select the language of processed material.

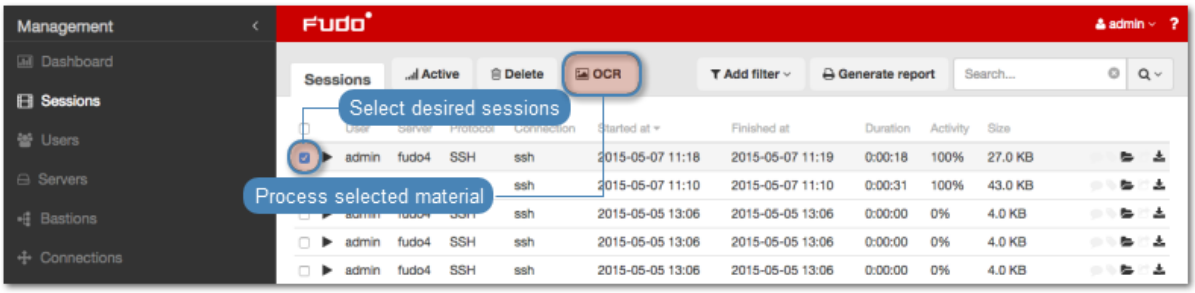



4. Click *Save*.

### Processing selected sessions

To process selected sessions, proceed as follows.

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




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

3. Confirm processing selected sessions.

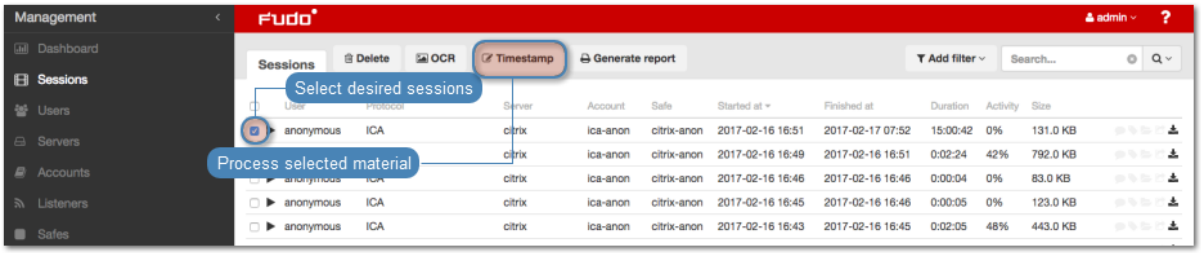
**Related topics:**

- *Filtering sessions*
- *Accounts*

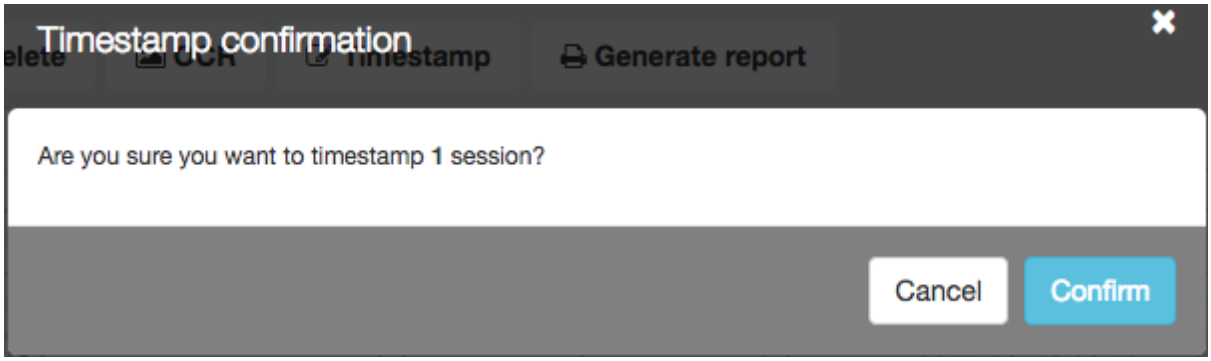
## 12.12 Timestamping selected sessions

To timestamp selected sessions, proceed as follows.

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




3. Click *Confirm*.




**Note:** Click the ⏲ to view the timestamp data.

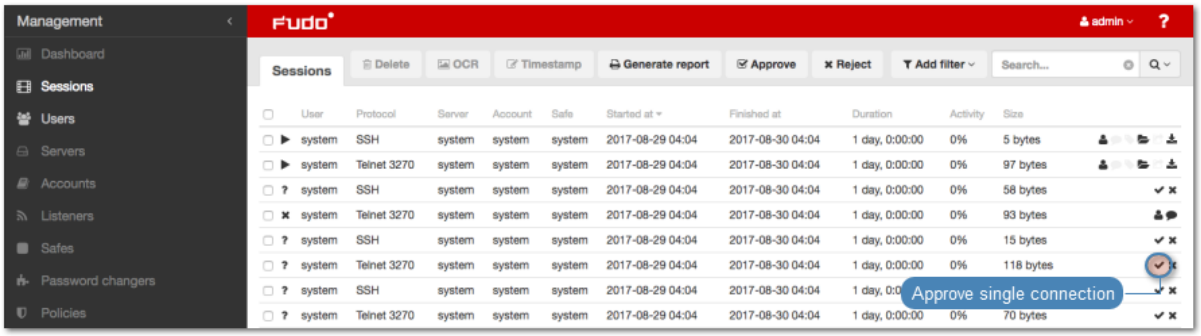
**Related topics:**

- *Filtering sessions*
- *Accounts*

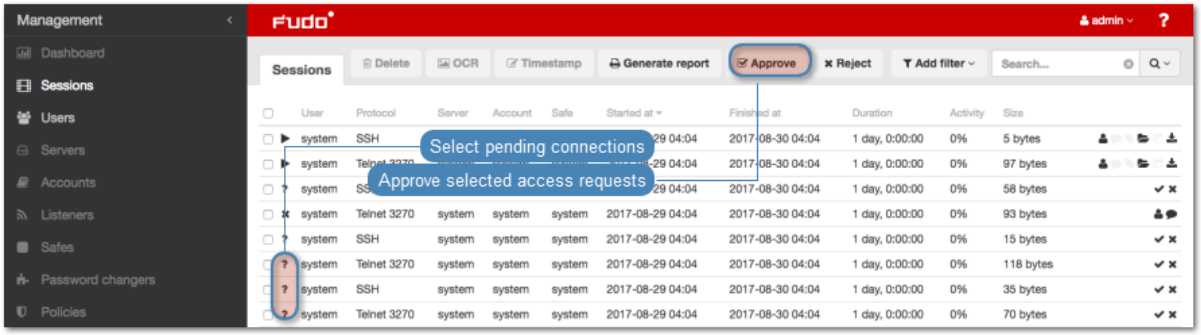
## 12.13 Approving pending connections

### 12.13.1 Fudo management interface

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




or select desired pending sessions and click *Approve*.




### 12.13.2 Fudo Mobile

1. Start and login to the *Fudo mobile* application.
2. Select profile that you want to list connections from.
3. Select pending connection and tap *Approve* or swipe it right and tap .

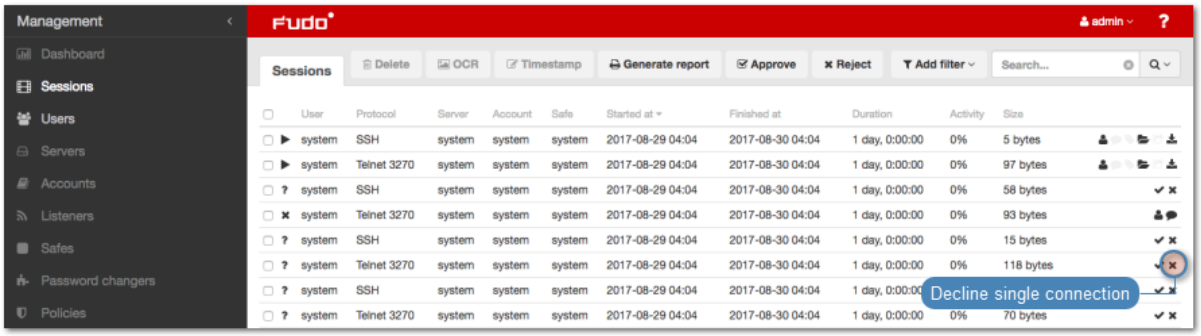
**Related topics:**

- *User authentication methods and modes*
- *Declining pending connections*
- *Sessions*

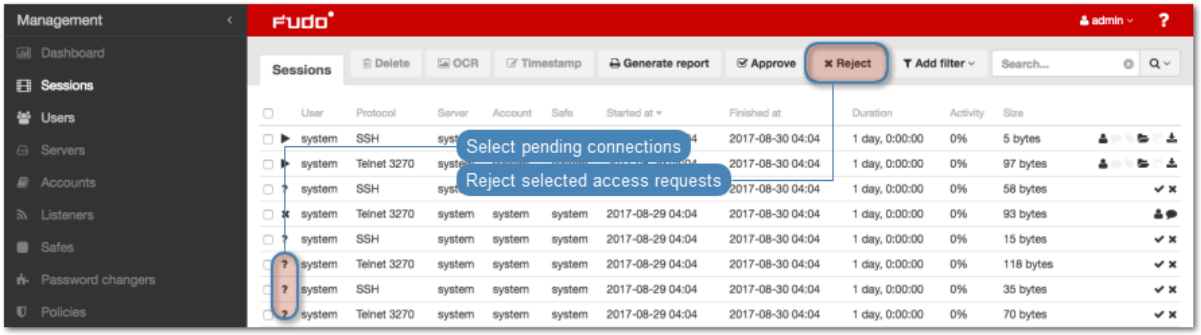
## 12.14 Declining pending connections

### 12.14.1 Fudo administration interface

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




or select pending sessions and click *Reject*.



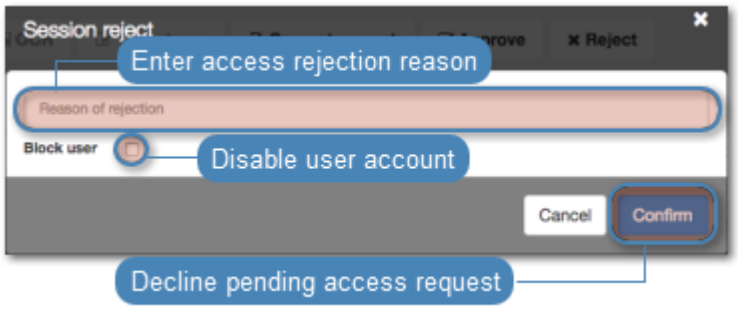

3. Optionally, enter the reason for rejecting given access request.

**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*.




### 12.14.2 Fudo Mobile

1. Start and login to the *Fudo mobile* application.
2. Select profile that you want to list connections from.
3. Select pending connection and tap *Deny* or swipe it left and tap ✖.

4. Enter reason why you decline given connection.
5. Optionally, select the option to disable user account.
6. Tap *Decline* to confirm access disapproval.

**Related topics:**

- *User authentication methods and modes*
- *Approving pending connections*
- *Terminating connection*
- *Blocking a user*
- *Sessions*

ROZDZIAŁ 13

# Reports

Reporting service generates detailed statistics of users access sessions.

Full reports are generated periodically (daily, weekly, monthly, quarterly) by the system and can be accessed by users with the `superadmin` role assigned. Reports generated periodically upon users with `admin` or `operator` requests, will include only information regarding sessions objects which they have access permission assigned to.

In addition to the system default settings, cyclic reports can be also generated based on the user defined *filtering definition*.

Report can also be generated on demand and include data related to specified user sessions.

**Subscribing to a periodic report**

To enable automatic periodic report generation for the logged in user, proceed as follows.

---

**Note:** Periodic reports, generated upon specific user's request, include only sessions, to which given user has sufficient access rights.

---

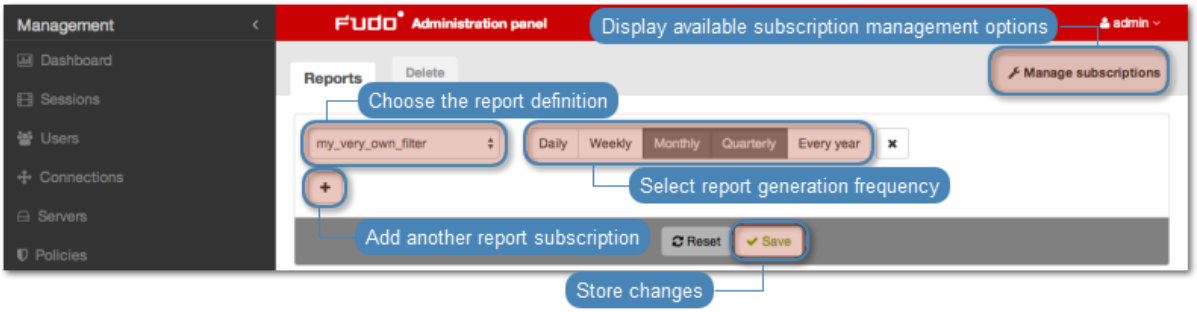
1. Select *Management* > *Reports*.
2. Click *Manage subscriptions*.
3. Select the report definition from the drop-down list.

---

**Note:** The list contains system default options and user defined *filtering definitions*.

---

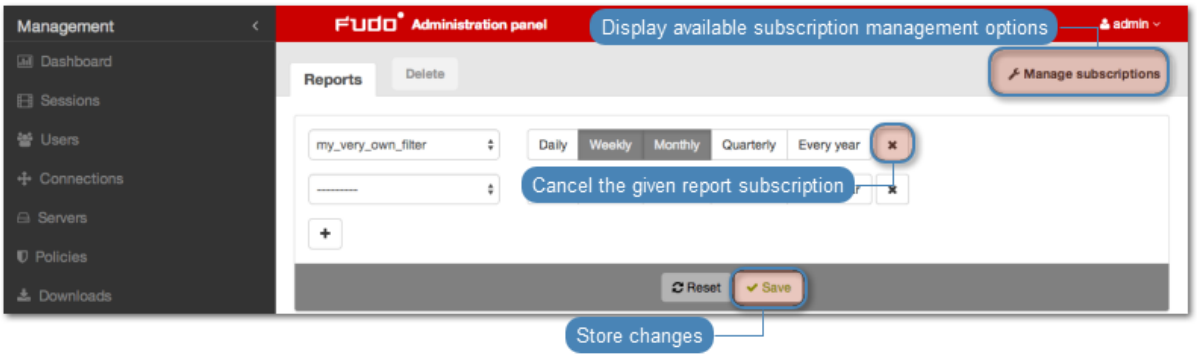
4. Choose how often the given report should be generated.
5. Click *Save*.




### Cancelling a periodic report subscription

To cancel a subscription to a cyclic report, proceed as follows.

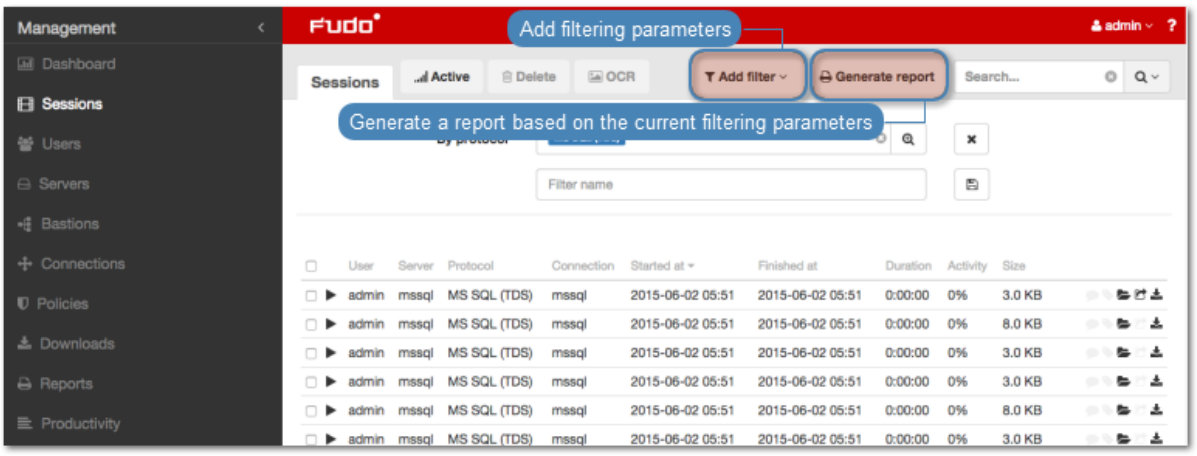
1. Select *Management* > *Reports*.
2. Click *Manage subscriptions*.
3. Click the report definition removal icon.
4. Click *Save*.



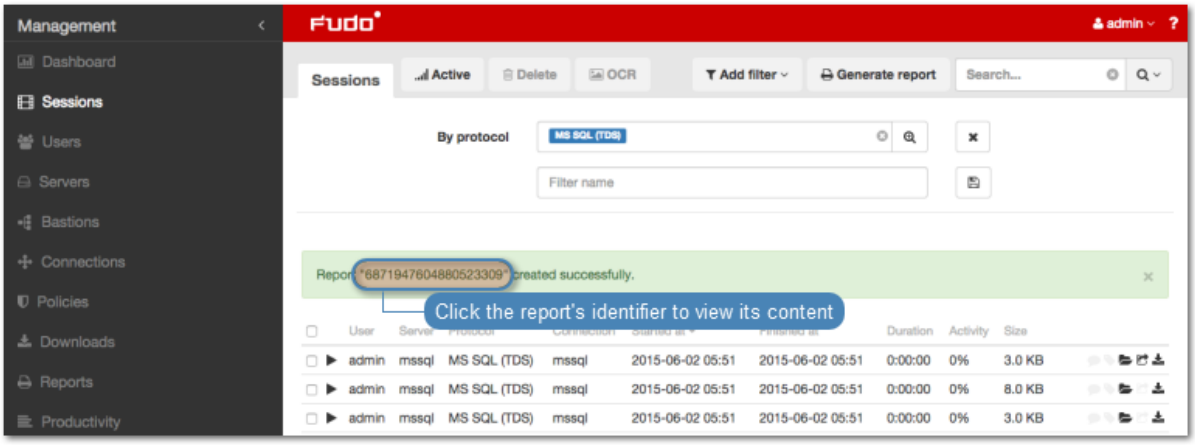

### Generating reports on demand

A report can be prepared for a specified subset of user sessions, determined by filtering options.

1. Select *Management* > *Sessions*.
2. Click *Add filters* and define filtering parameters (for more information on sessions filtering, refer to the *Sessions: Sessions filtering* topic).
3. Click *Generate report*, to have the report generated based on the current filtering criteria.



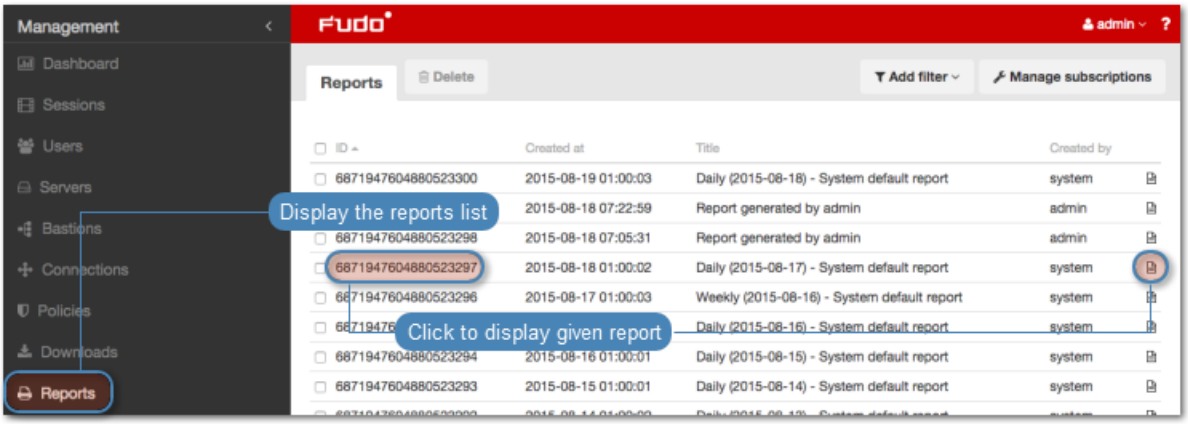
4. Note your report's identifier or click it to display the report.



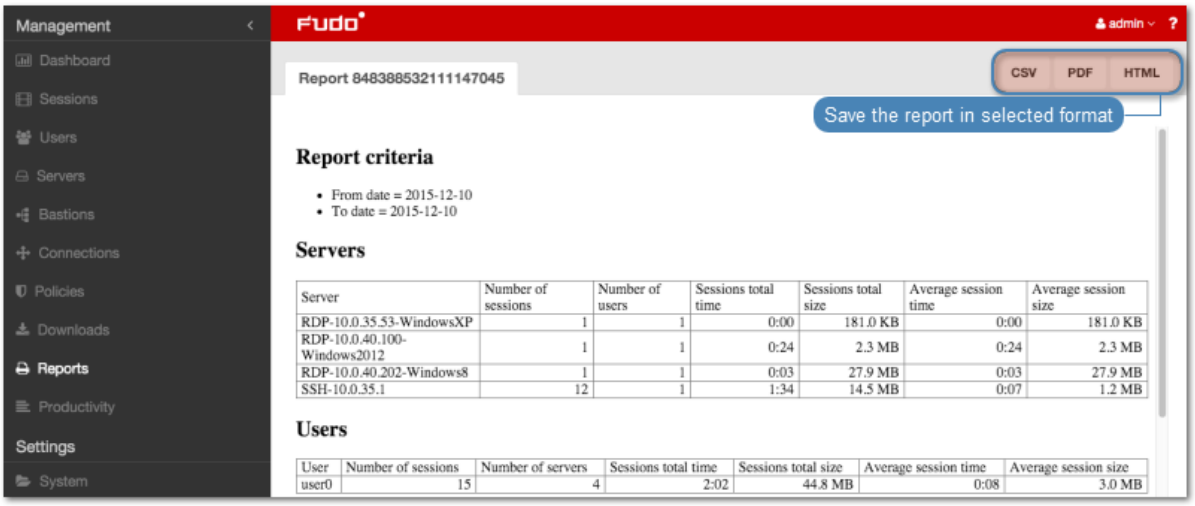

5. Select *Management* > *Reports*.
6. Find desired report and click the view icon.
7. Click the corresponding button to save the report in selected format.

### Opening and downloading reports

1. Select *Management* > *Reports*.
2. Find desired report and click the view icon.




3. Click the corresponding button to save the report in selected format.




### Deleting reports

1. Select *Management* > *Reports*.
2. Find, select desired reports and click *Delete*.
3. Confirm deleting selected reports.

### Related topics:

- *Notifications*
- *Filtering sessions*

ROZDZIAŁ 14

# Efficiency analyzer

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

## 14.1 Overview

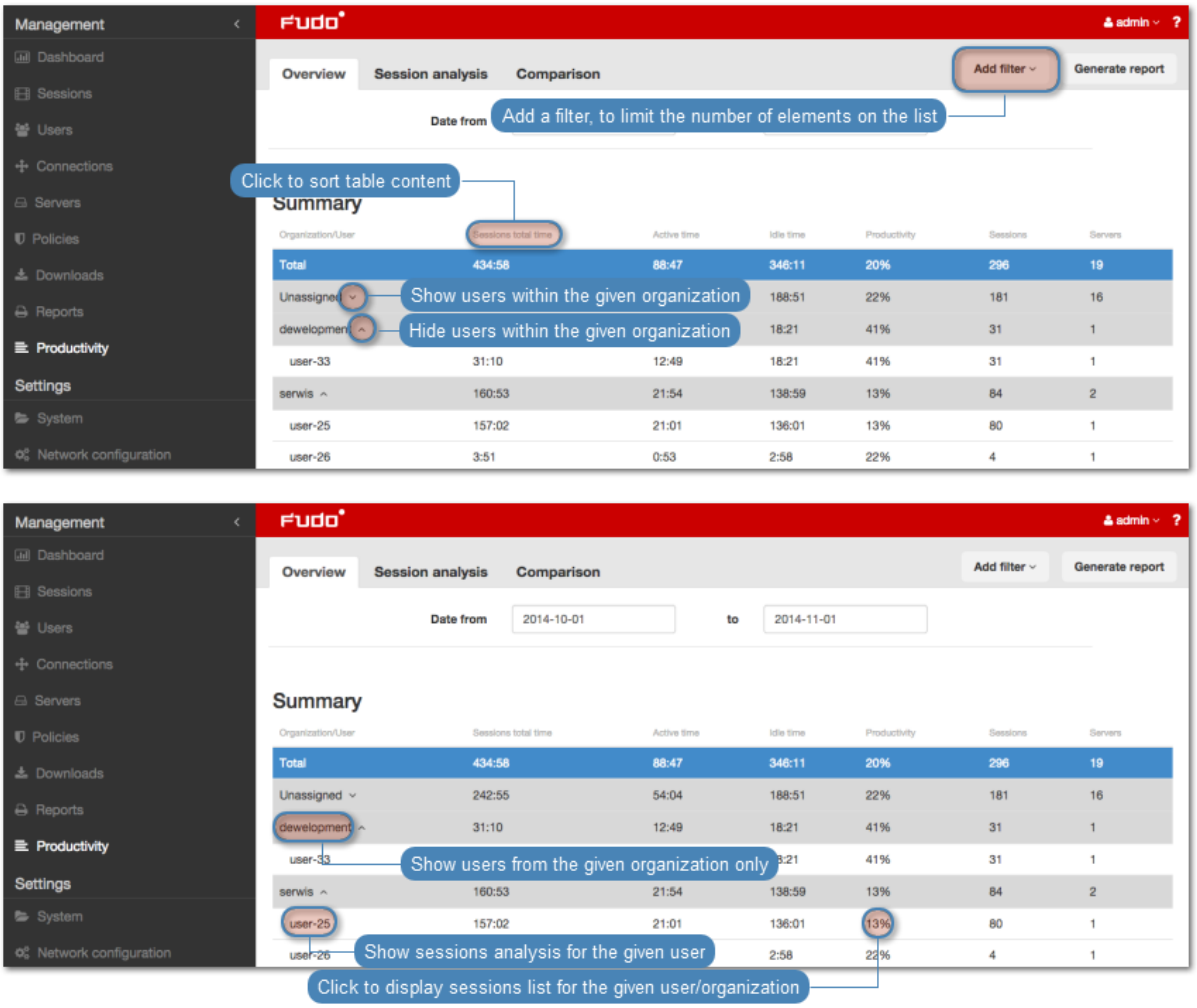
Overview displays data on users' activity in selected time interval.

**Note:** Activity rating is based on the user's interaction with the monitored system. Wheel Fudo PAM 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*

## 14.2 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.

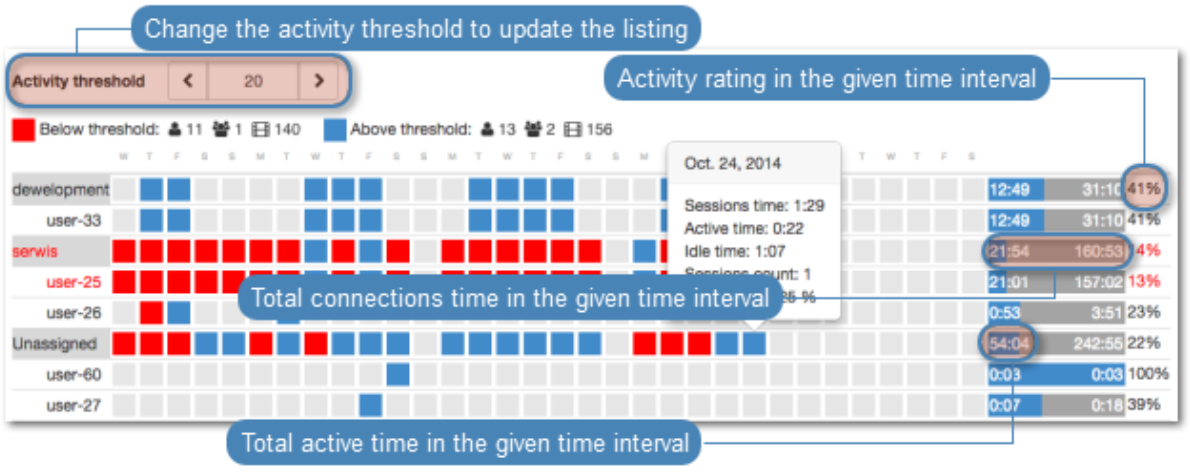
### Users activity rating

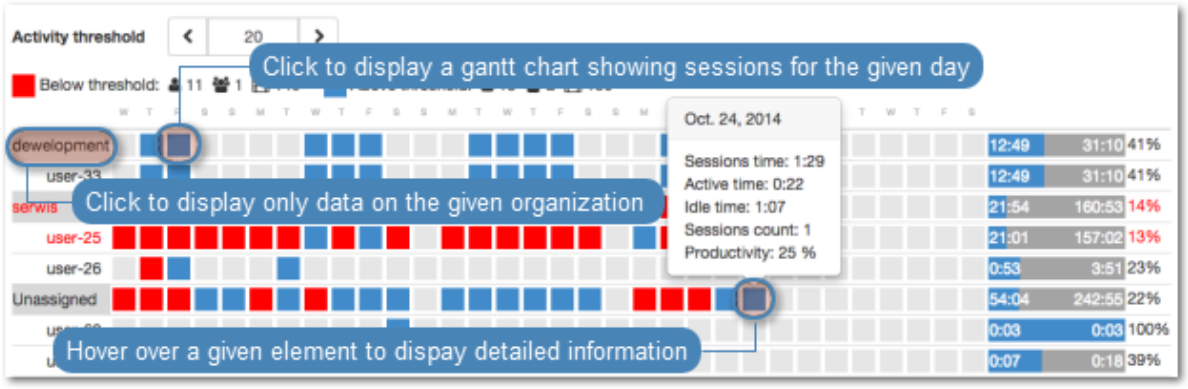
Users activity rating allows identifying sessions which do not exceed the required user activity level. Further material analysis helps determining the reason for low activity in the given session and draw relevant conclusions.

---

**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*

## 14.3 Activity comparison

Efficiency analyzer 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.
4. Select the time interval.
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*

ROZDZIAŁ 15

# Administration

This section covers Wheel Fudo PAM administration topics.

## 15.1 System

### 15.1.1 Date and time

System events registered by Wheel Fudo PAM (sessions, system log events, etc.) are timestamped. Wheel Fudo PAM can obtain the time information either from an NTP server or the system clock.

**Warning:**

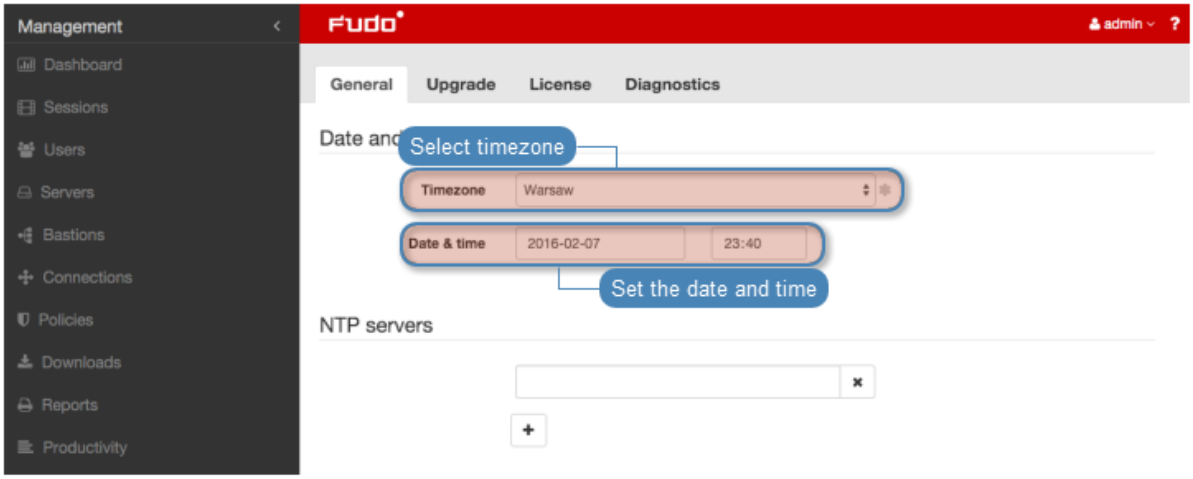
- It is strongly advised for the date and time settings to be obtained from a reliable NTP server. Changing date and time settings manually may result in system malfunction.
- Date and time synchronization with NTP server is required in *cluster configurations*.

**Changing date and time settings**

**Note:** Manual time setting is disabled if there are NTP servers configured.

To change the Wheel Fudo PAM's system clock settings, proceed as follows.

1. Select *Settings* > *System*.
2. Change date and time parameters in the *Date and time* section.




3. Click *Save*.

### Time servers configuration

---

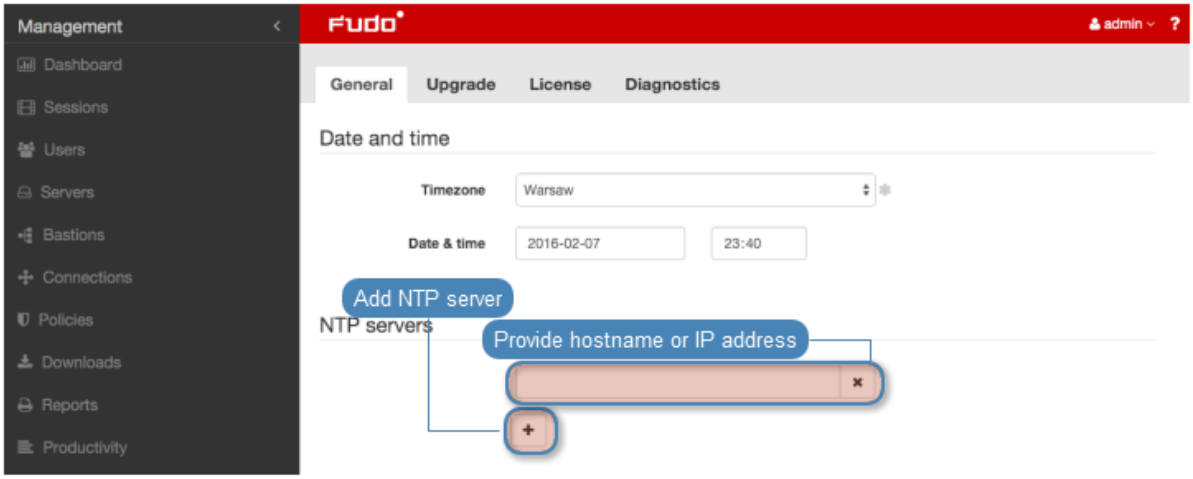
**Note:** NTP servers ensure that the system time on all IT infrastructure devices is synchronized. Using NTP servers guarantees that the timestamp of the recorded session matches the time settings on the monitored server.

---

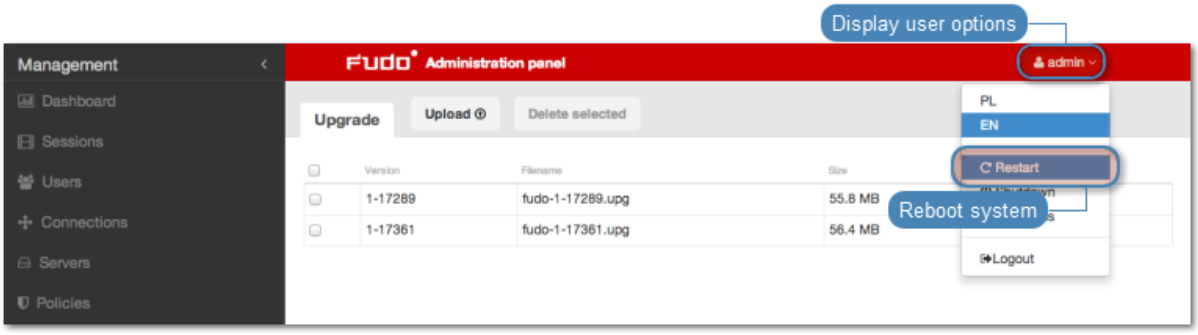
### Adding an NTP server definition

To add an NTP server definition, proceed as follows.

1. Select *Settings* > *System*.
2. Click + in the *NTP servers* section to add an NTP server.
3. Enter NTP server IP address or host name.




4. Click *Save*.
5. Select *Restart* from user menu to reboot Wheel Fudo PAM and apply new time settings.

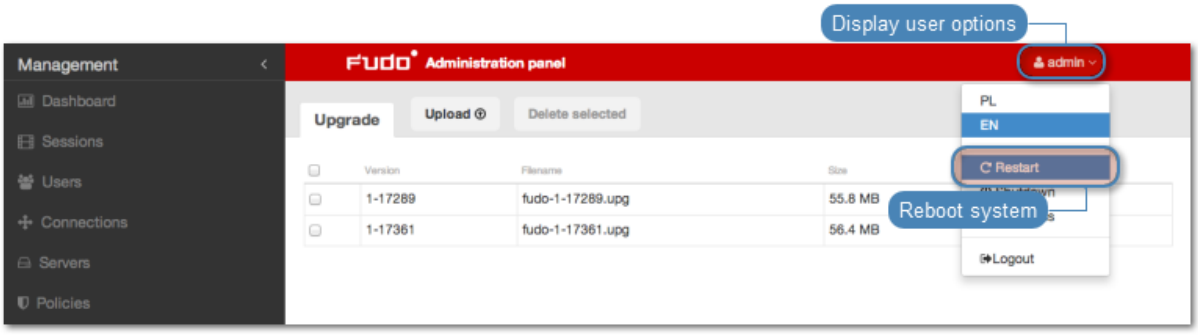



### Editing an NTP server definition

To edit an NTP server definition, proceed as follows.

1. Select *Settings* > *System*.
2. Find and change desired NTP server configuration parameters in the *NTP servers* section.

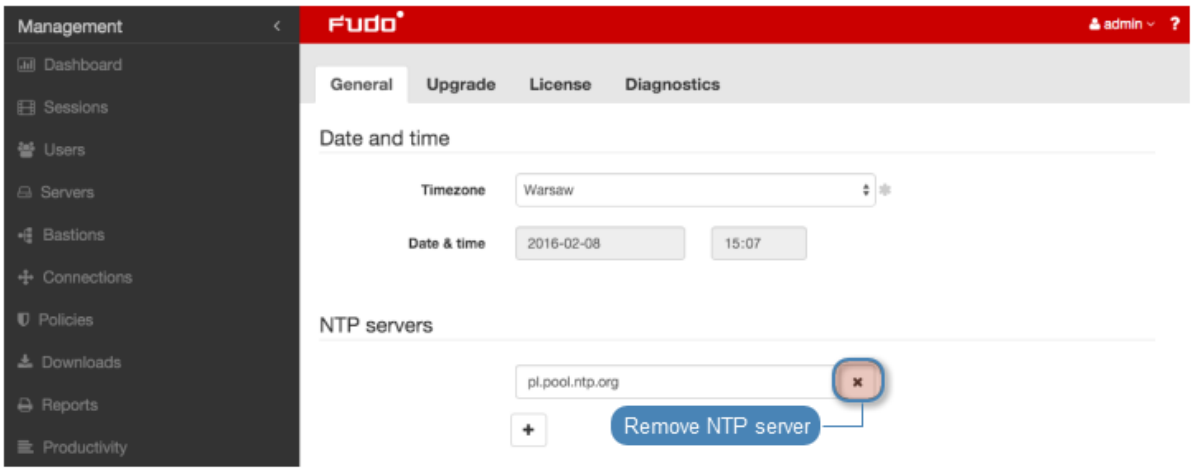
3. Click *Save*.
4. Select *Restart* from user menu to reboot Wheel Fudo PAM and apply new time settings.




### Deleting an NTP server definition

To remove and NTP server definition, proceed as follows.

1. Select *Settings* > *System*.
2. Find desired NTP server definition in the *NTP servers* section and click the *X* icon.




3. Click *Save*.

**Related topics:**

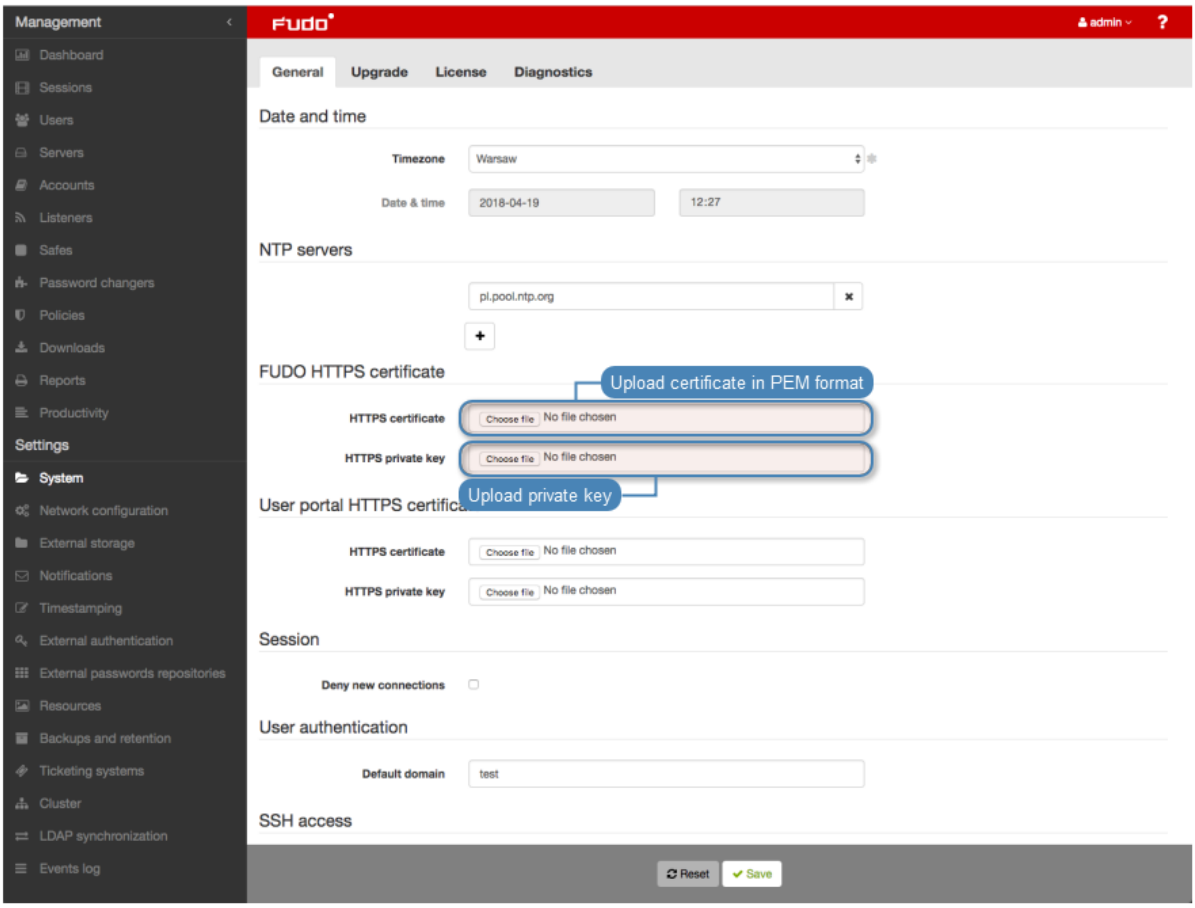
- *Timestamping*

### 15.1.2 SSL certificates

SSL certificate allows prevent phishing attacks.

**Configuring SSL certificate for Fudo administration panel**

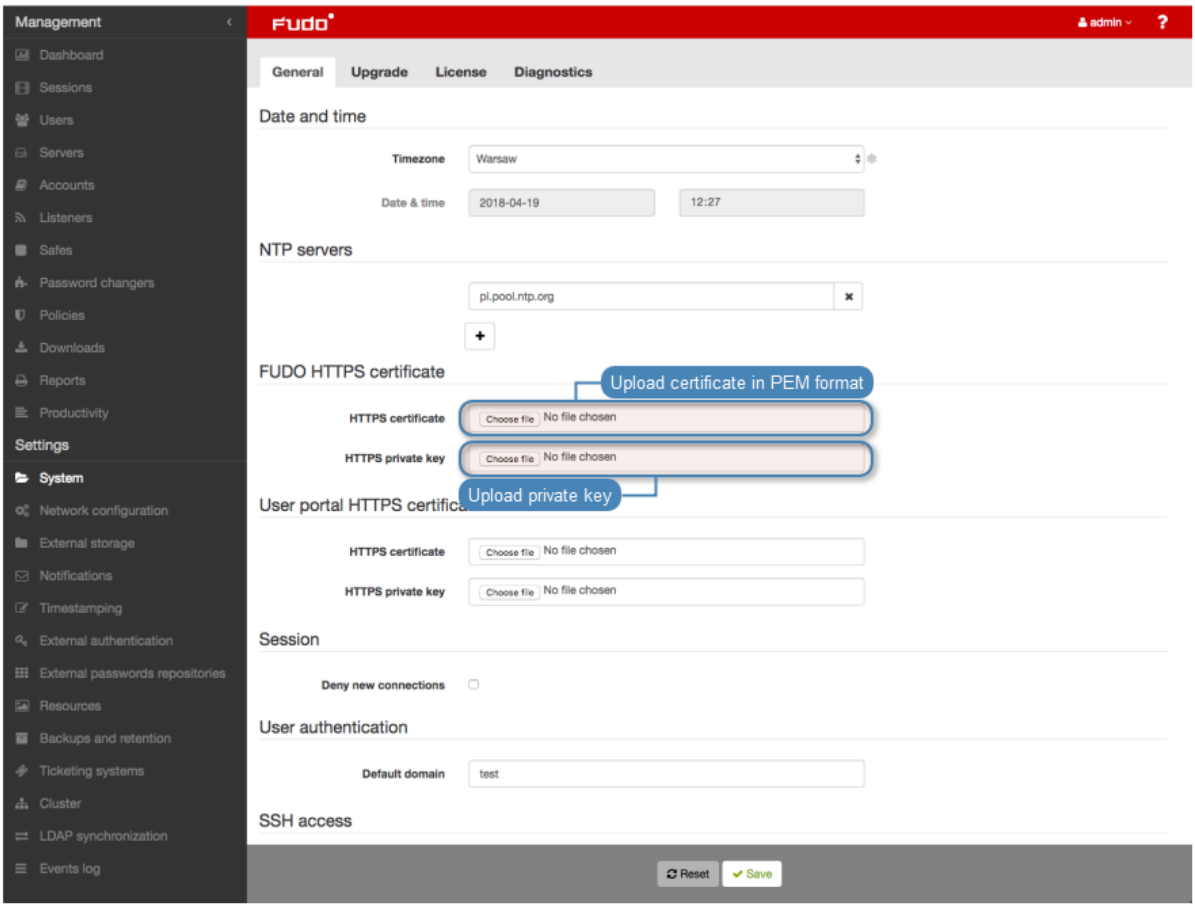
1. Select *Settings* > *System*.
2. In the *Fudo HTTPS certificate* section, click the *Browse* button next to the *HTTPS Certificate* field and point to the location of the SSL certificate file in PEM format.
3. Click the *Browse* button next to the *HTTPS Private Key* field and point to the location of the SSL key definition.




4. Click *Save*.

### Configuring user portal SSL certificate

1. Select *Settings* > *System*.
2. In the *Fudo HTTPS certificate* section, click the *Browse* button next to the *HTTPS Certificate* field in the *HTTPS certificate* section and point to the location of the SSL certificate file in PEM format.
3. Click the *Browse* button next to the *HTTPS Private Key* field and point to the location of the SSL key definition.




4. Click *Save*.

**Related topics:**

- *Security measures*
- *Servers*

### 15.1.3 Deny new connections

Enabling this option results in a denial of all new connections requests.

**Blocking new connections**

1. Select *Settings* > *System*.
2. Select *Deny new connections* option in the *Session* section.
3. Click *Save* button.

**Related topics:**

- *Network interfaces configuration*

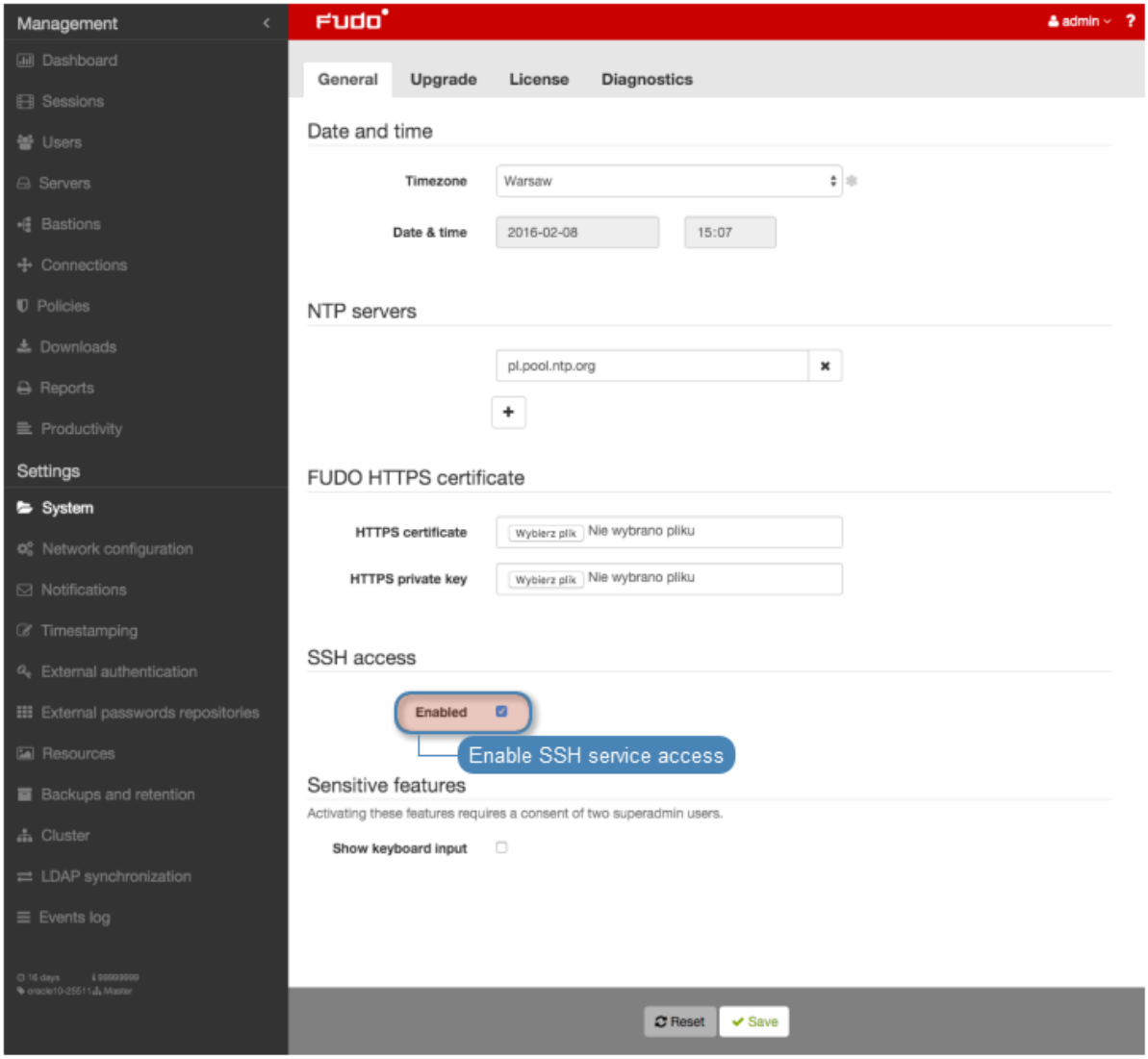
### 15.1.4 SSH access

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

### Enabling SSH access

To enable SSH access, proceed as follows.

1. Select *Settings* > *System*.
2. Select *Enabled* option in the *SSH access* section.




3. Click *Save* button.

**Related topics:**

- *Network interfaces configuration*

## 15.1.5 Reset account

Reset account enables resetting Wheel Fudo PAM to factory settings.

### Enabling reset account

To enable reset account, proceed as follows.

1. Select *Settings* > *System*.

2. Select *Enabled* option in the *Reset account* section.
3. Click *Save* button.

**Related topics:**

- *Network interfaces configuration*

### 15.1.6 Sensitive features

Sensitive features is a set of options enabling which requires a consent from two `superadmin` users.

**Enabling displaying keyboard input**

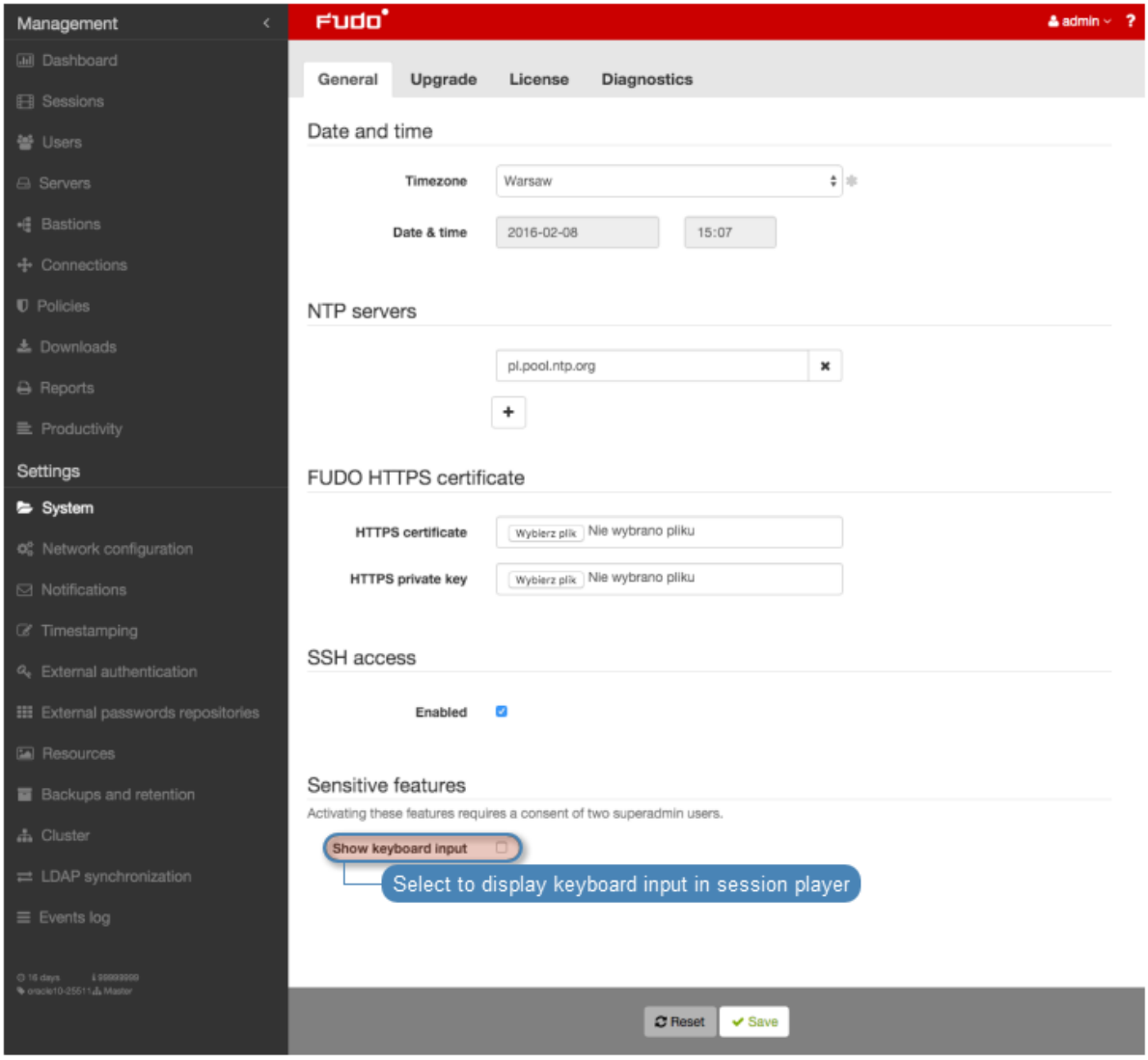
---

**Note:** Keystrokes are not displayed in the session player by default. Enabling keystrokes display requires a consent from two `superadmin` users.

---

To enable keyboard input display, proceed as follows.

1. Select *Settings* > *System*.
2. Select *Show user input* in the *Sensitive features* section to initiate the feature.
3. Click *Save*.




4. Notify another system administrator that the keyboard input showing feature has been initiated and requires a confirmation.

**Related topics:**

- *Viewing sessions*

### 15.1.7 System update

---

**Note:**

- In addition to the current system version, Fudo PAM stores the previous revision, allowing for restoring the system to its previous state.
- The system update process does not influence the system configuration or the session data stored on Fudo PAM.
- The storage usage may temporarily increase during system update.

---

#### 15.1.7.1 Updating system

The upgrade mechanism consists of two phases: *Prepare* phase and actual *Execute* phase.

*Prepare* phase is responsible for migrating data in monthly batches to the new database in the background during normal operational use of Fudo PAM.

It is advised to allow the mechanism to copy as much data as possible during this phase as the final upgrade will have to copy the remaining data, hence data copied in the prepare phase reduces overall time required to perform the final offline upgrade.

The upgrade mechanism makes resumable snapshots of migration progress. At each step of the migration, a snapshot is made and in case of failure, the mechanism is able to restart the process from the last valid state both with the same package and potentially with a new package released at a later time. This step is important especially for large installations where the *Prepare* phase can take significant time.

---

**Note:** Session retention is unavailable during the *Prepare* phase as it could attempt to remove data that has been already copied to the new database.

---

---

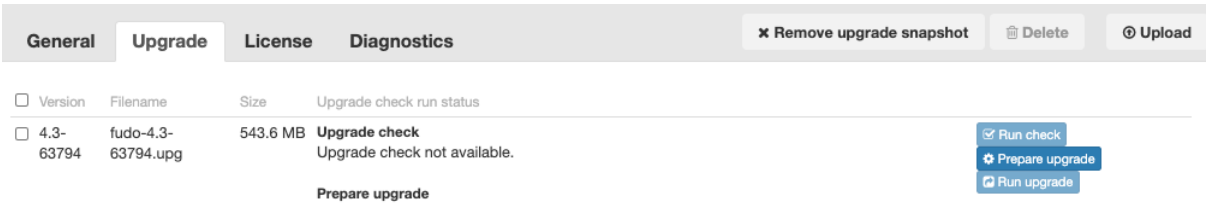
**Note:** *Run check* button is disabled as it has no use due to big database version changes.

---

**Warning:**

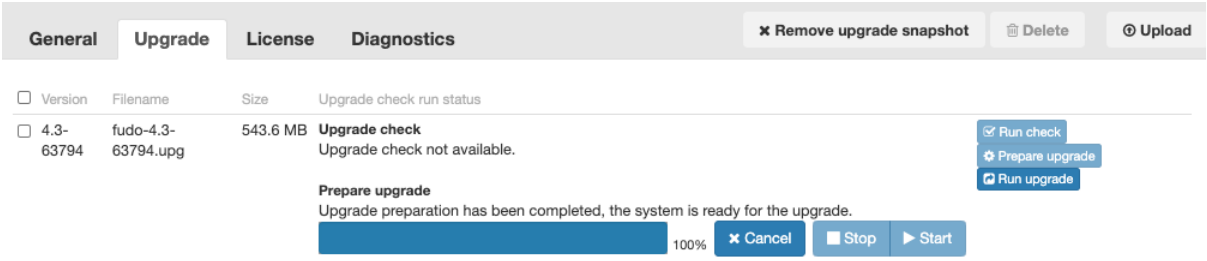
- The storage required for performing the upgrade is estimated before the process is executed. Fudo mechanism reports how much additional space is required if the currently available storage is too small to safely perform the upgrade.
- If the storage usage on the system being updated exceeds 85%, contact Fudo Security 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 *Sessions* section of the system settings menu to *limit the number* of active connections before performing system upgrade.

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. Click *Prepare upgrade*.



**Note:** Running *Prepare upgrade* can be put on hold by clicking the *Stop* button. When the current batch of data is copied (1 month) the *Prepare* phase will stop instead of starting to copy the next batch. Clicking the *Start* button resumes the process. Prepare phase can be canceled completely by clicking *Cancel*, which however does not remove resumable snapshots. If this is required, please contact Fudo Security support.

6. Once *Upgrade Preparation* phase is completed, you can click *Run upgrade*.




**Warning:**

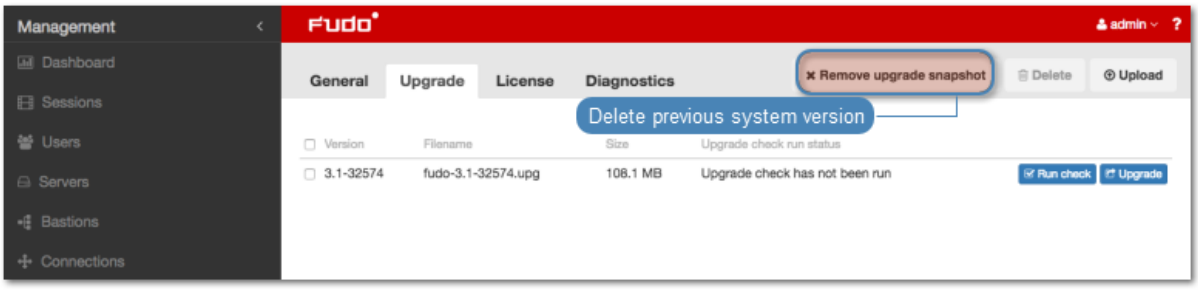
- After running system update, Fudo PAM will restart automatically.
- Rebooting a physical appliance requires the encryption key. Connect the USB flash drive containing the encryption key to the USB port before proceeding.
- In case of virtual machine instances, system will prompt for passphrase upon boot up after running upgrade scripts. Entering incorrect passphrase will restart the machine in previous revision.
- If an executed upgrade fails, the upgrade package will remain in the *Upgrade* tab so you don't need to re-upload the package again.

#### 15.1.7.2 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 *Remove upgrade snapshot*.




4. Confirm deleting previous system version.

**Related topics:**

- *System version restore*
- *Restarting system*

### 15.1.8 License

#### Uploading new license

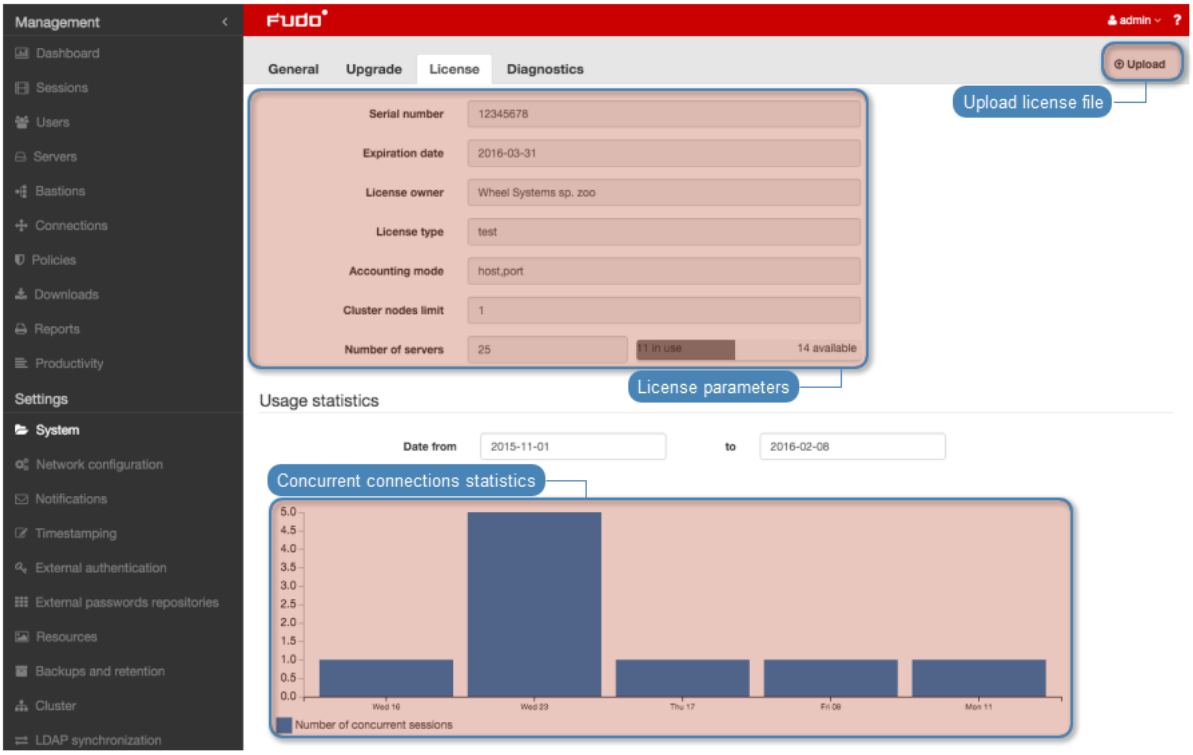
To upload a new license file, proceed as follows.

---

**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:**

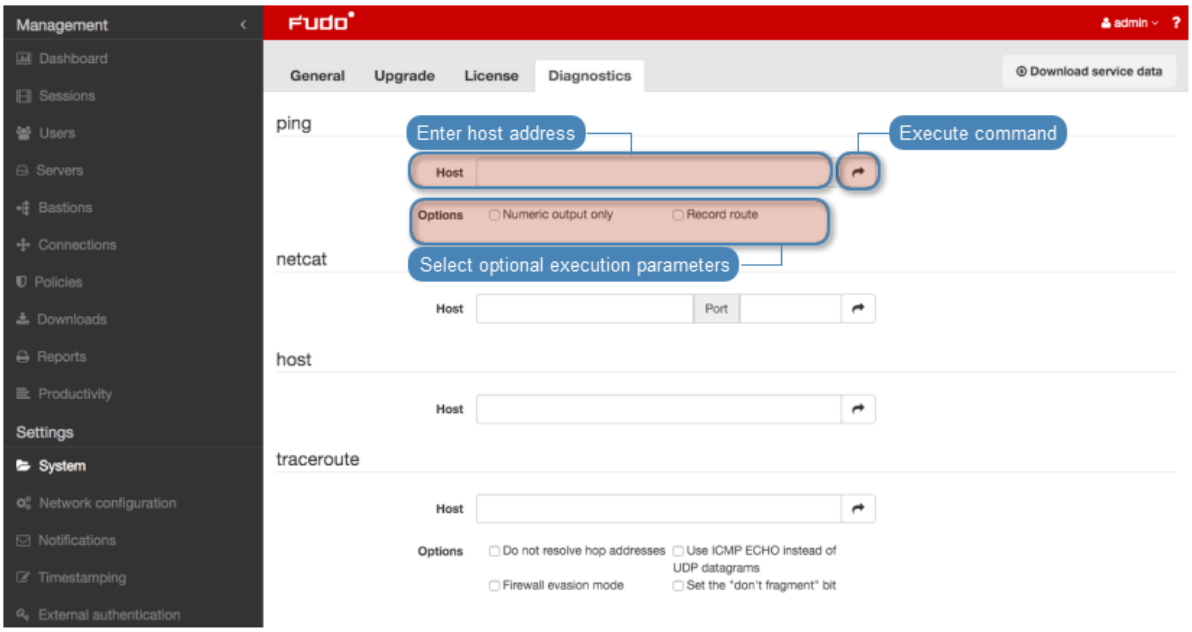
- *System*

### 15.1.9 Diagnostics

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

To run a diagnostic utility, proceed as follows.

1. Select *Settings* > *System*.
2. Select the Diagnostics tab.
3. Find desired utility, provide necessary parameters and execute the command.



| Command/parameter | Description |
|---|---|
| Ping | Ping sends a sequence of 10 ICMP packets to selected host. |
| Numeric output only | Does not resolve host's IP address to its mnemonic name. |
| Record route | Enables tracking packets' route. |
| | |
| netcat | `etcat` allows establishing connection with remote host on specified port number. |
| | |
| host | `host` is used to determine if the DNS server correctly resolves mnemonic hostnames. |
| | |
| traceroute | `traceroute` allows for determining packets' route between Wheel Fudo PAM and the specified host. |
| 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*

### 15.1.10 Default domain

---

**Note:**

- In case user does not have a domain defined, login string is supplemented with the default domain value.
- 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, Wheel Fudo PAM will report authentication problem as it cannot determine which user is trying to connect.

---

**Defining default domain**

1. Select *Settings* > *System*.
2. In the *User authentication* section, provide the default domain.
3. Click *Save*.

**Related topics:**

- *Creating a user*
- *Users synchronization*

### 15.1.11 Password complexity

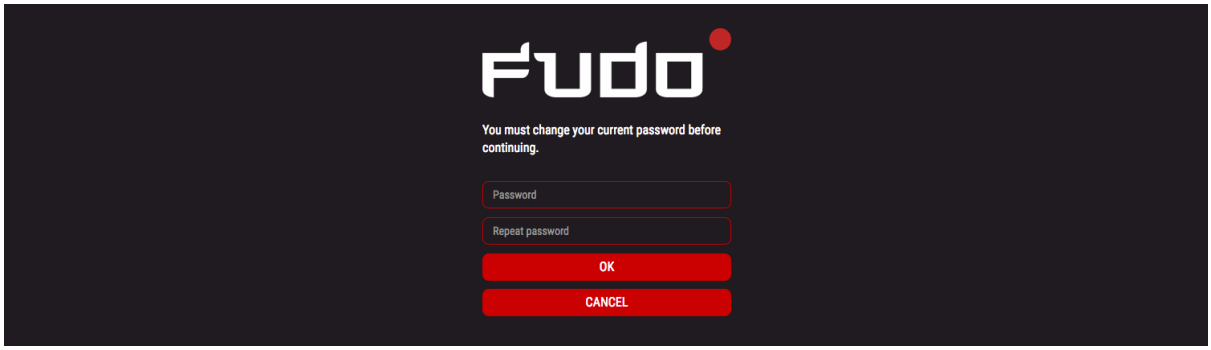
Fudo PAM enables defining static passwords complexity enabling you to enforce passwords that meet your internal regulations.

**Defining password complexity**

1. Select *Settings* > *System*.
2. In the *User authentication and sessions* section, select *Password complexity* to enforce defined rules.

---

**Note:** 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 *User Portal*.

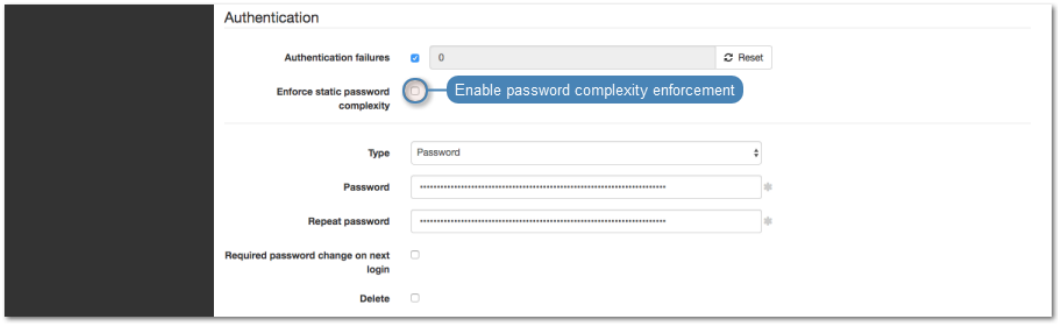



---

3. Define the minimum number of characters.
4. Select *Small letters* and provide the minimal number of small letters in the password.
5. Select *Capital letters* and provide the minimal number of capital letters in the password.
6. Select *Special characters* and provide the minimal number of special characters in the password.
7. Select *Digits* and provide the minimal number of digits in the password.
8. Select the *Different password than current* option to enforce a password different from the current one.
9. Click *Save*.

---

**Note:** To enable static password complexity for a particular user, select the *Enforce static password complexity* option in the *Authentication* section on the user form.



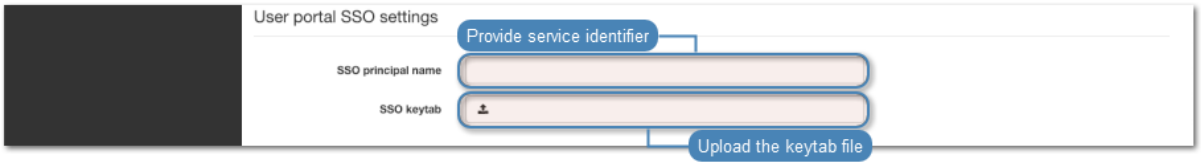
**Related topics:**

- *Creating a user*
- *Users synchronization*

### 15.1.12 Single Sign On in User Portal

Single Sign On automatically authenticates the user when logging into the User Portal.

1. Select *Settings* > *System*.
2. In the *User portal SSO settings* section, provide service identifier that will match the user account with the service instance.
3. Upload the keytab file containing user's ID and encryption keys for encrypting and decrypting Kerberos tickets.



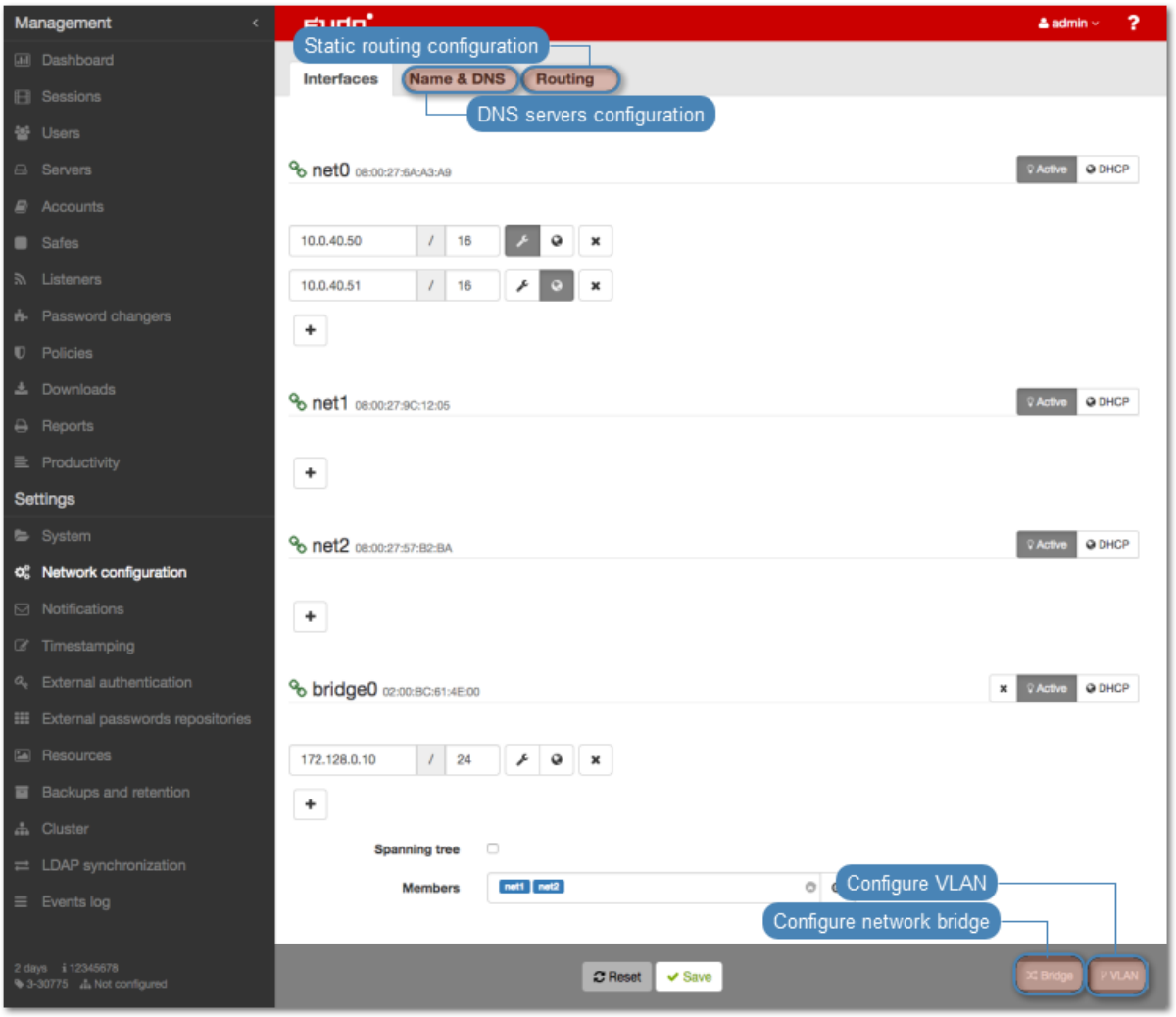

4. Click *Save*.

**Related topics:**

- *Creating a user*
- *Users synchronization*

## 15.2 Network settings

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




### 15.2.1 Network interfaces configuration

#### 15.2.1.1 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 the assigned IP addresses is empty and the is no option to define an IP address, check if given interface is a member of a bridge.

---

To define an IP of a physical network interface, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Click + and provide IP address and subnet mask in CIDR format.

---

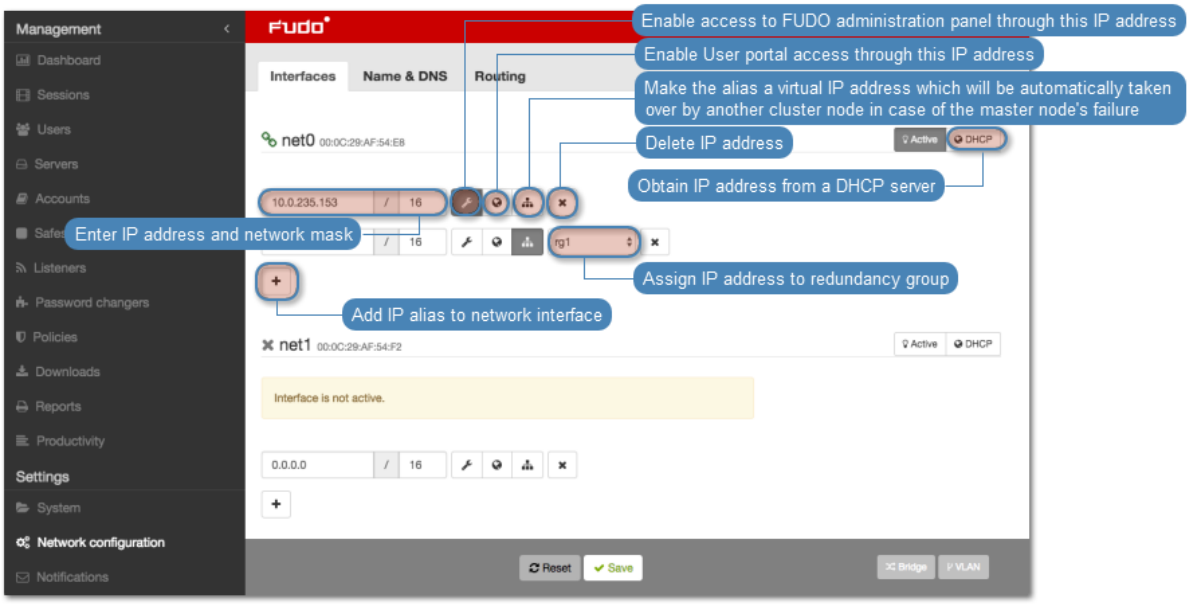
**Note:** + will be inactive if the *DHCP* option is enabled on the given interface.

---

3. Choose additional options for the IP address being defined.

| | |
|---|---|
| | Enable access to administration panel on given IP address. Note that the management IP address is also used for replicating data between cluster nodes. |
| | Make the alias a virtual IP address which will be take over by another cluster node in case of the master node's failure.<br>**Note:** Cluster IP address must be added manually on every cluster node, with the option enabled. |
| | Enable access to *User portal* on given IP address. |

4. Click *Save*.




**Note:** Current state of each network 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.

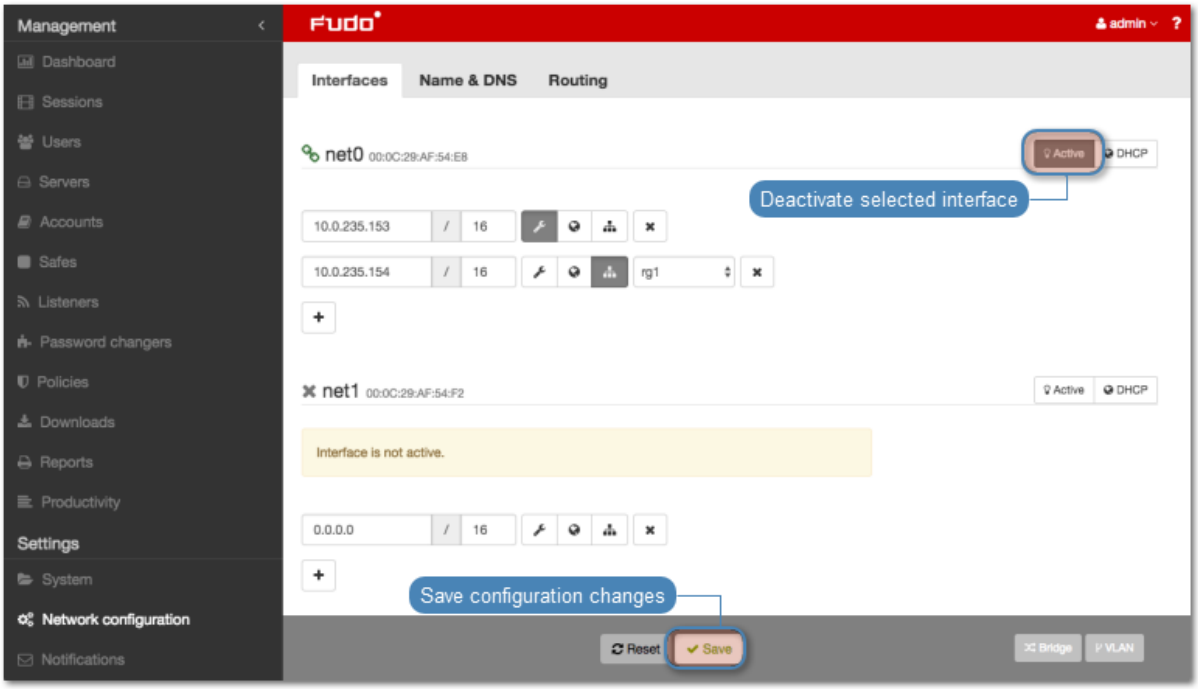
To delete an IP address assigned to a given network interface, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Select desired IP address assigned to given network interface and click *x*.
3. Click *Save*.

*Disabling network interface*

To disable a network interface, proceed as follows.

1. Select *Settings* > *Network configuration*
2. Click the *Active* icon next to given interface to deactivate it.

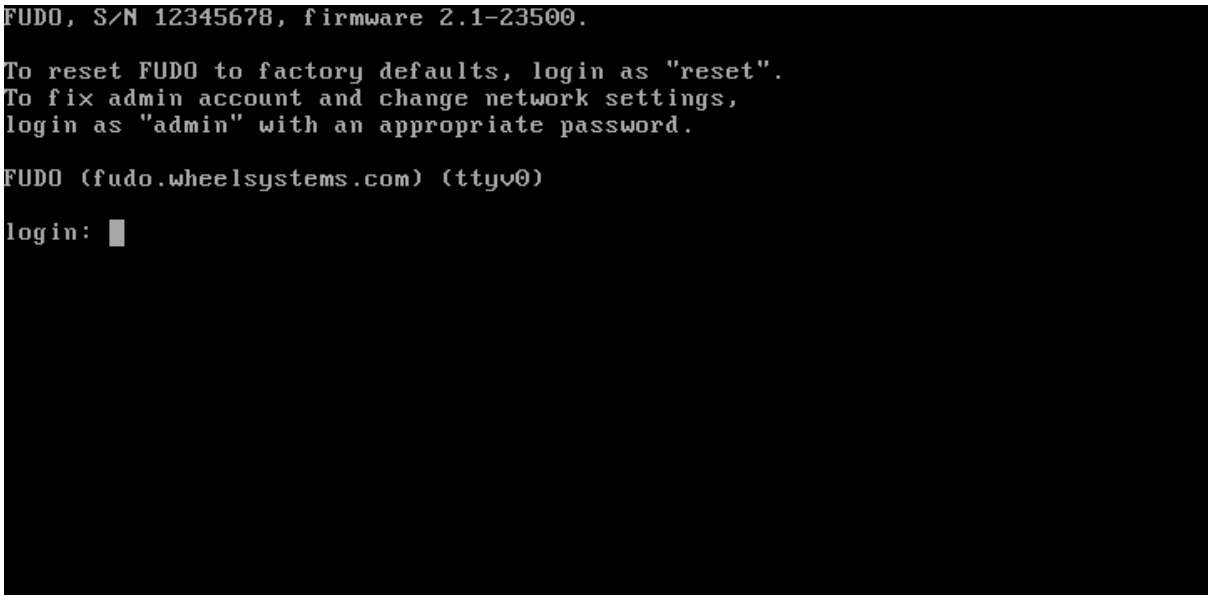


3. Click *Save*.

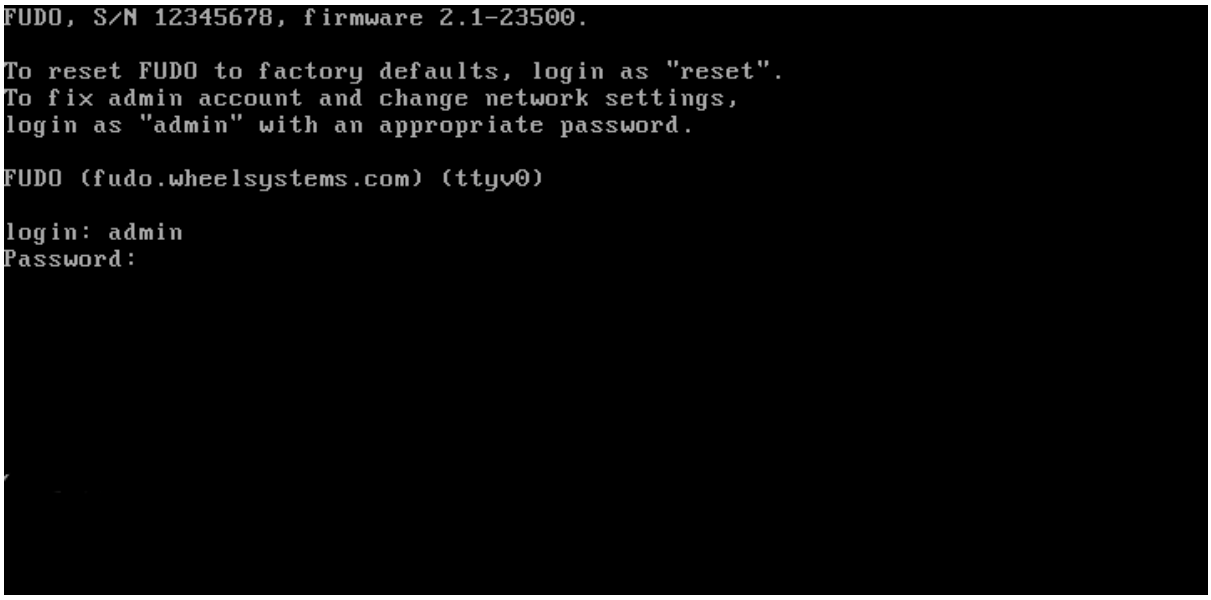
#### 15.2.1.2 Defining IP address using system console

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*.




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




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

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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

Choose an option (0):
```

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

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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

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

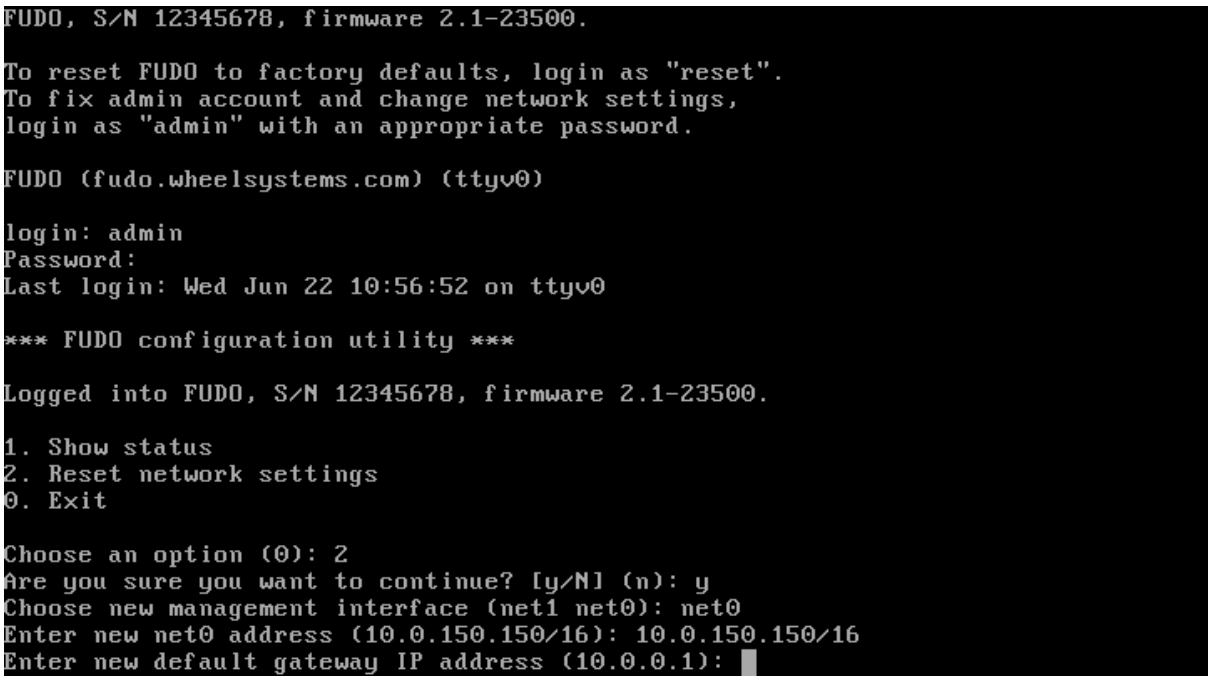
6. Enter the name of the new management interface (Wheel Fudo PAM web interface is accessible through the management interface).

```
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*.




#### 15.2.1.3 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 *Bridge*.
3. Assign network interfaces or VLANs to the bridge.

---

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

---

4. Enter IP address and network subnet in CIDR notation.
5. Select *Spanning tree* option to enable bridge loops prevention.
6. Select the *Management* option if the administration interface should be available under assigned IP addresses and click *Active*.
7. Click *Save*.

#### 15.2.1.4 Setting up virtual networks (VLANs)

VLAN networks allow separating broadcast domains.

To configure a VLAN on , proceed as follows.

1. Select *Settings* > *Network configuration*
2. Click *VLAN*.
3. Select the physical interface and define VLAN ID.
4. Add IP addresses to given VLAN.

---

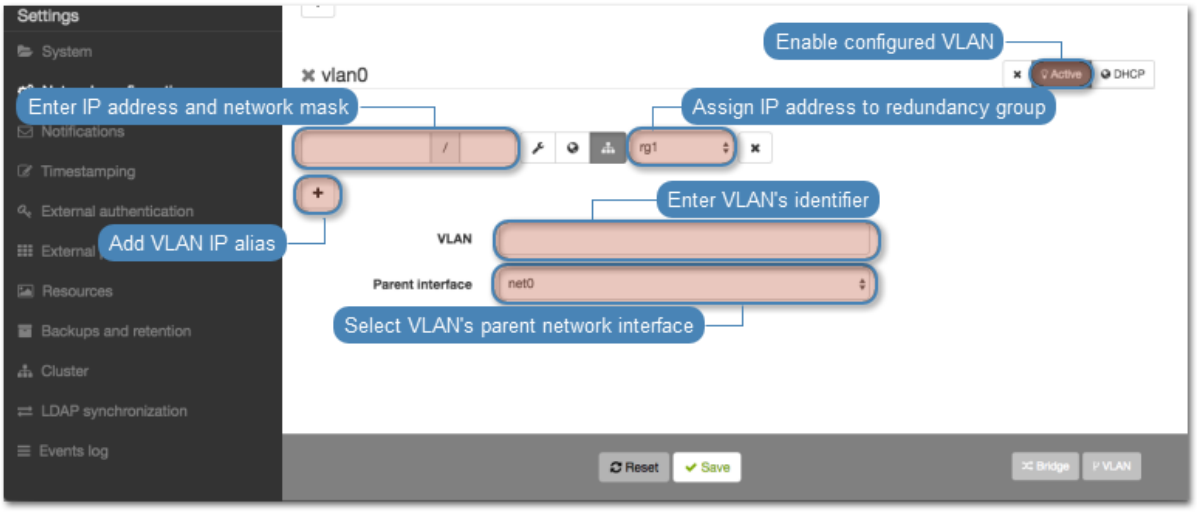
**Note:** Select *DHCP* option, to obtain IP address from a DHCP server.

---

**Note:** The IP addresses are aliases to the physical interface and are used in *servers configuration* as proxy server address.

---

5. Click *Active* to activate defined VLAN.
6. Click *Save*.

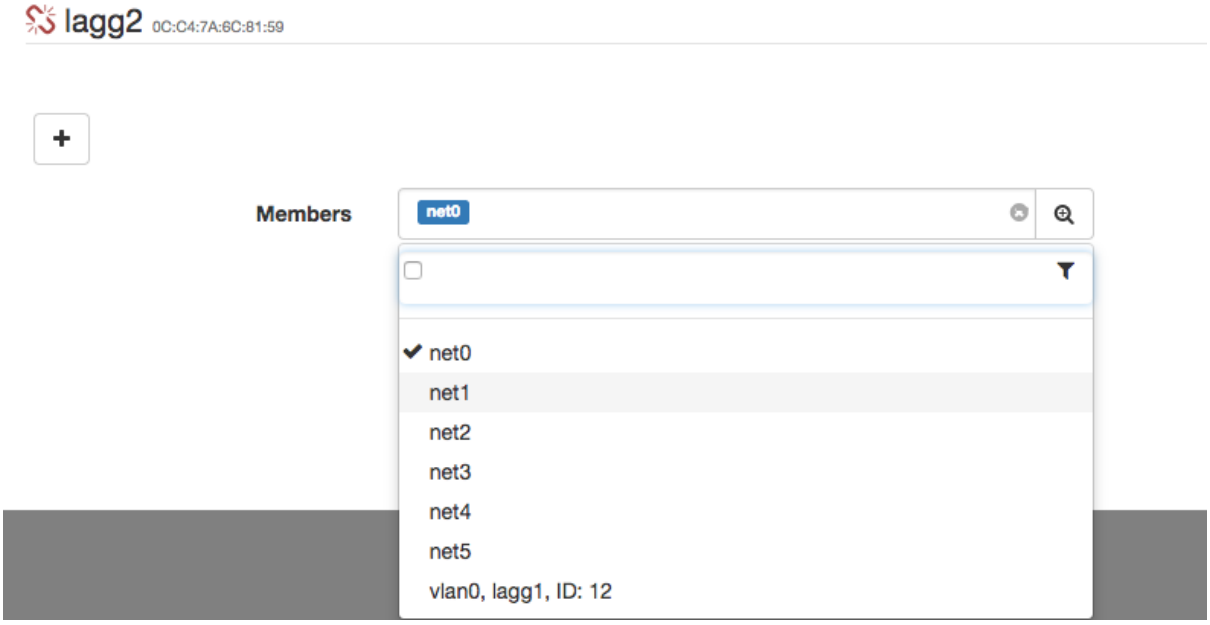



### 15.2.1.5 Setting up LACP link aggregation

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 *Link aggregation*.
3. Assign network interfaces.




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

4. Enter IP address and network subnet in CIDR notation.

5. Choose additional options for the IP address being defined.

| | |
|---|---|
| | Enable access to administration panel on given IP address. Note that the management IP address is also used for replicating data between cluster nodes. |
| | Make the alias a virtual IP address which will be take over by another cluster node in case of the master node's failure. |
| | Enable access to *User portal* on given IP address. |

6. Click *Save*.

**Related topics:**

- *Servers management*
- *Accounts*

### 15.2.2 Labeled IP addresses

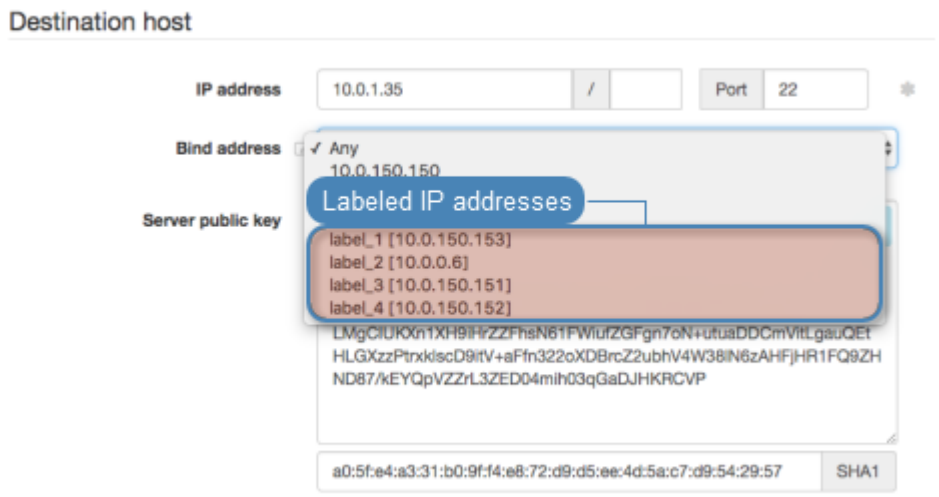
IP address labels are global configuration parameters. They are replicated throughout cluster's nodes, but their assignment is strictly local, applicable to each node separately. Labels enable ensuring constant access to LDAP authentication services in case of a node failure and allow for implementing load balancing scenarios.

**Defining a labeled IP address**

1. Select *Settings* > *Network configuration*.
2. Select the *IP labels* tab.
3. Click .
4. Provide IP address and enter label name.

**Note:** Label name can comprise small letters, digits, _ and - characters.

5. Click *Save*.
6. Use labeled IP address in listener, server or external authentication source configuration.




**Related topics:**

- *Network interfaces configuration*
- *External authentication*
- *Servers*
- *Listeners*

### 15.2.3 Bypasses configuration

Bypasses enable to physically re-route network packages in case of a system failure.

---

**Note:** Bypasses configuration is not available if Wheel Fudo PAM is running in virtualized environment.

---

1. Select *Settings* > *Network configuration*.
2. Select *Bypasses* tab.
3. Select bypass mode.
   - Bypass mode permanently enabled - this option enforces bypass mode on the network interface card. This mode may be used for maintenance purposes or when troubleshooting network issues.
   - Bypass mode enabled only in case of system failure - network packets are re-routed only in case of a system failure or in case the Wheel Fudo PAM is powered off.
   - Bypass mode disabled - in case of system failure, the network packets will not be routed to the next network appliance.
4. Click *Save*.

**Related topics:**

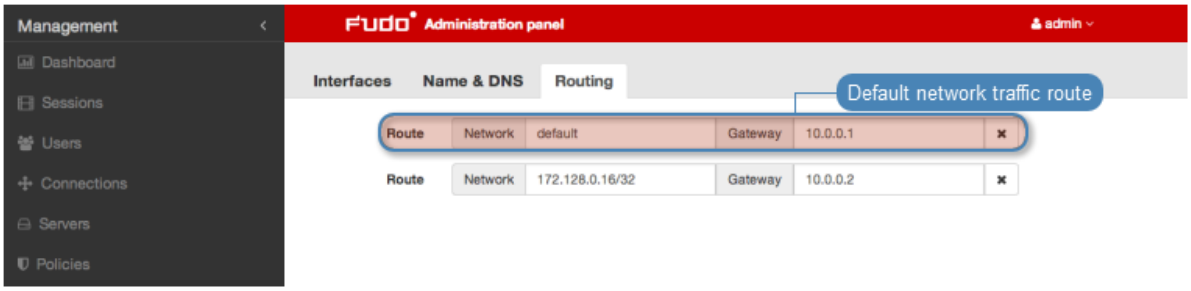
- *Network interfaces configuration*

### 15.2.4 Routing configuration

In default configuration, Wheel Fudo PAM 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.

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

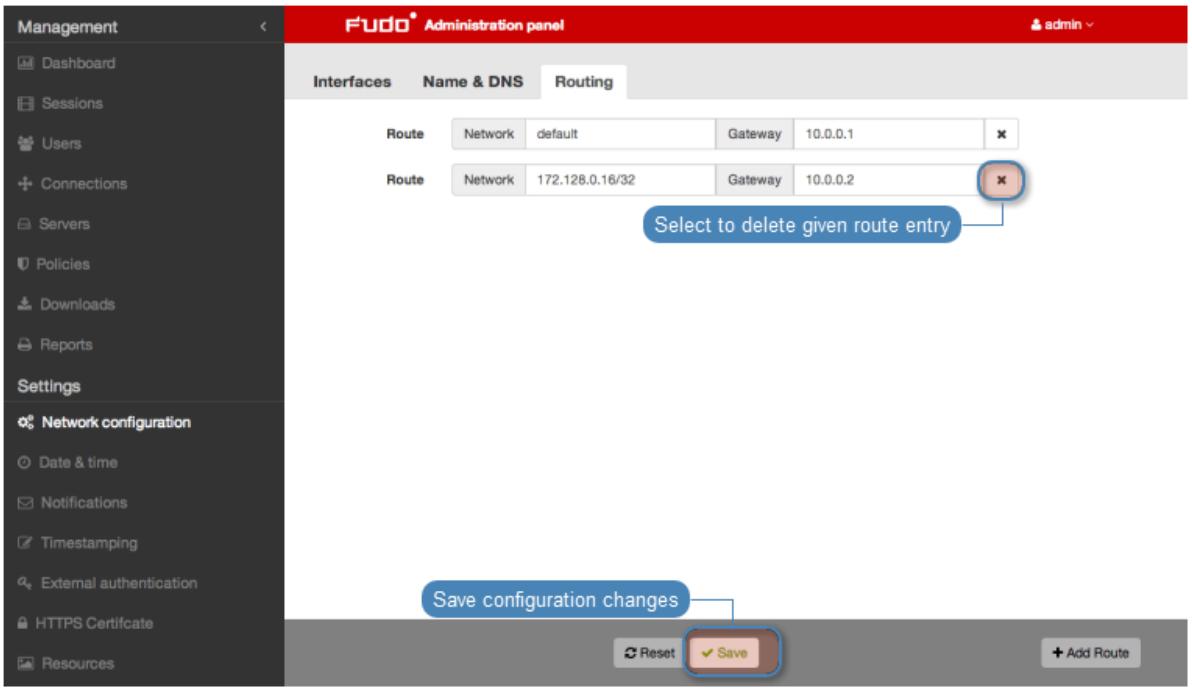
To edit a route, proceed as follows.

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. Find desired route entry and click the delete icon.
4. Click *Save*.

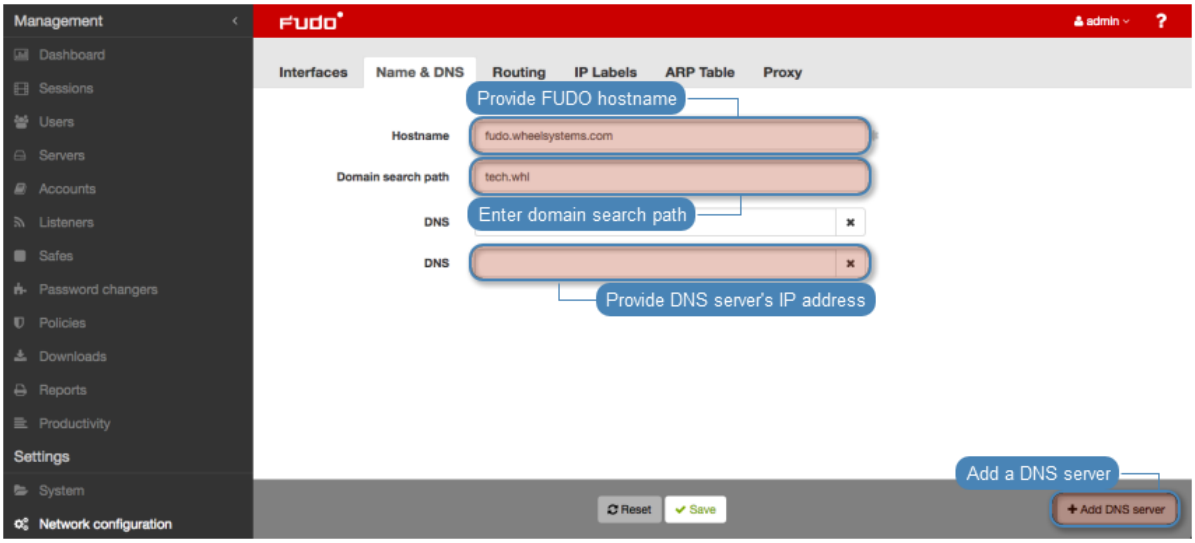



**Related topics:**

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

### 15.2.5 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 new* 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 and double-click desired field.
4. Change parameter value as needed.
5. 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. Find and select given DNS server definition.
4. Click *Delete*.

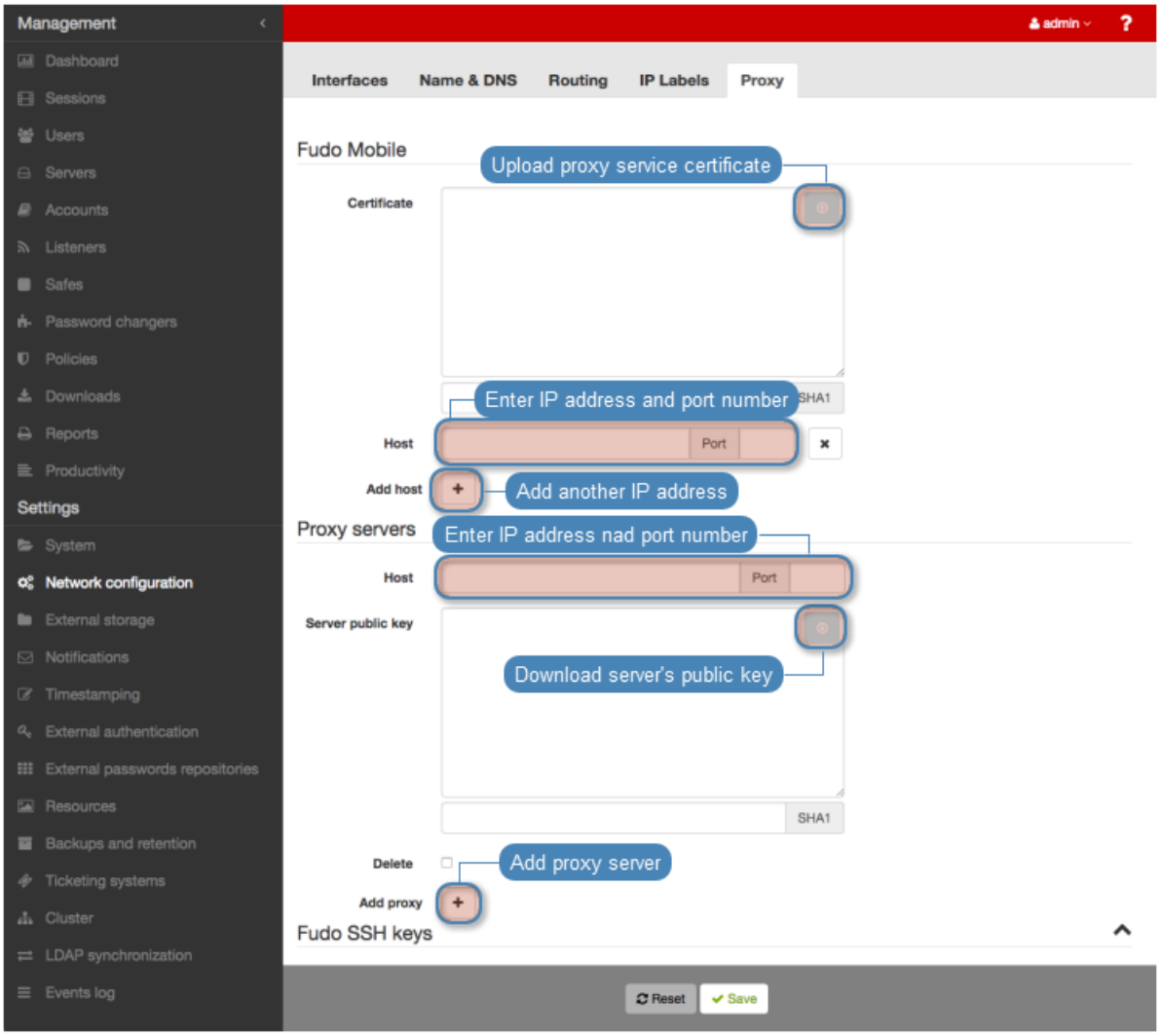
5. Click *Save* .

**Related topics:**

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

### 15.2.6 Proxy servers configuration

**Note:** Proxy server is required for facilitating communication between *Fudo Mobile* application and Wheel Fudo PAM system.




#### Adding a proxy server definition

To add a proxy server definition, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Switch to the *Proxy* tab.

3. In the *Fudo Mobile* section, click to upload certificate for communication between Fudo Mobile application and Fudo's API.
4. Provide IP address or hostname and port number for Fudo Mobile application access.

---

**Note:** Click to define additional hosts.

---

5. Provide IP address or hostname and port number of proxy host for communication over SSH.
6. Click to download server's public key.

---

**Note:** Click to define additional proxy hosts.

---

7. Click *Save*.

---

**Note:** SSH keys displayed in the *Fudo SSH keys* section, are used to configure an external proxy service on a dedicated host. For more information refer to *4-Eyes authentication proxy service* topic.

---

#### Editing a proxy server definition

To edit a proxy server definition, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Switch to the *Proxy* tab.
3. Find desired proxy server and change its parameters as needed.
4. Click *Save*.

#### Deleting a Fudo Mobile communication IP address

To delete an IP address used for communication with *Fudo Mobile* application, proceed as follows.

---

**Note:** Deleting an IP address may result in communication problems between *Fudo Mobile* application instances and Wheel Fudo PAM.

---

1. Select *Settings* > *Network configuration*.
2. Switch to the *Proxy* tab.
3. In the *Fudo Mobile* section find desired IP address and click .
4. Click *Save*.

#### Deleting a proxy server definition

To delete a proxy server definition, proceed as follows.

**Note:** Deleting a proxy server definition may cause issues with delivering push notifications to *Fudo Mobile* application.

1. Select *Settings* > *Network configuration*.
2. Switch to the *Proxy* tab.
3. In the *Proxy servers* section, find desired proxy server definition and select *Delete*.
4. Click *Save*.

**Related topics:**

- *Adding a mobile device*
- *Network interfaces configuration*
- *Time servers configuration*
- *Approving pending connections*
- *Declining pending connections*

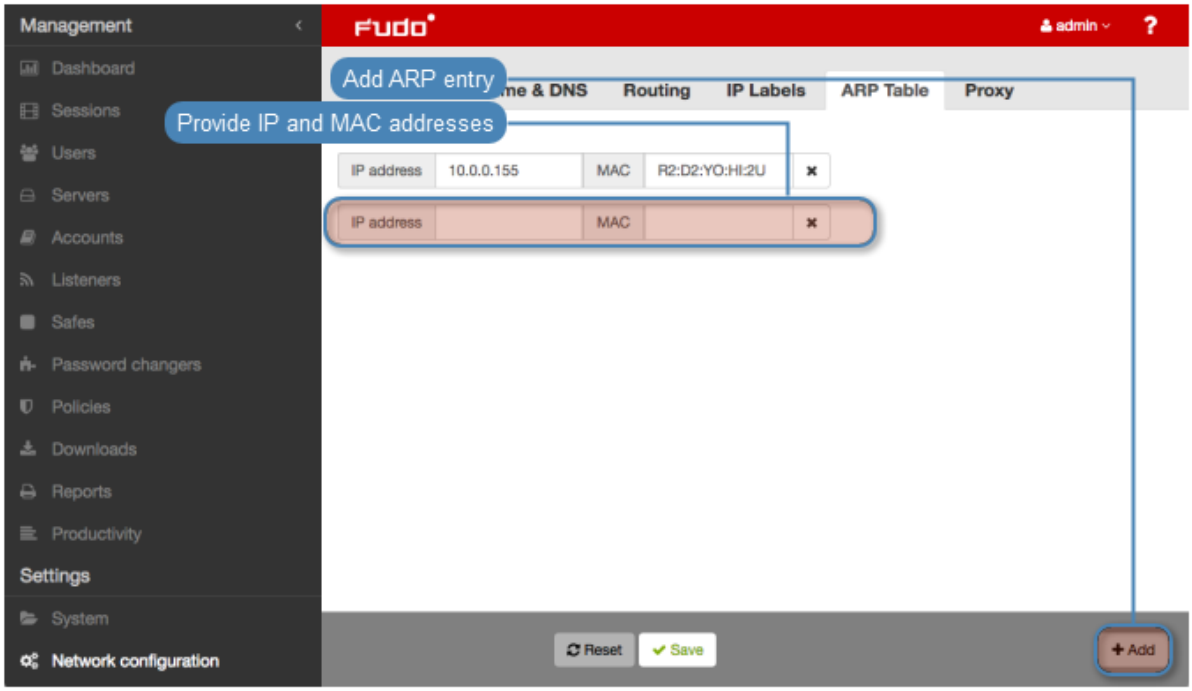
### 15.2.7 ARP table configuration

**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* 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

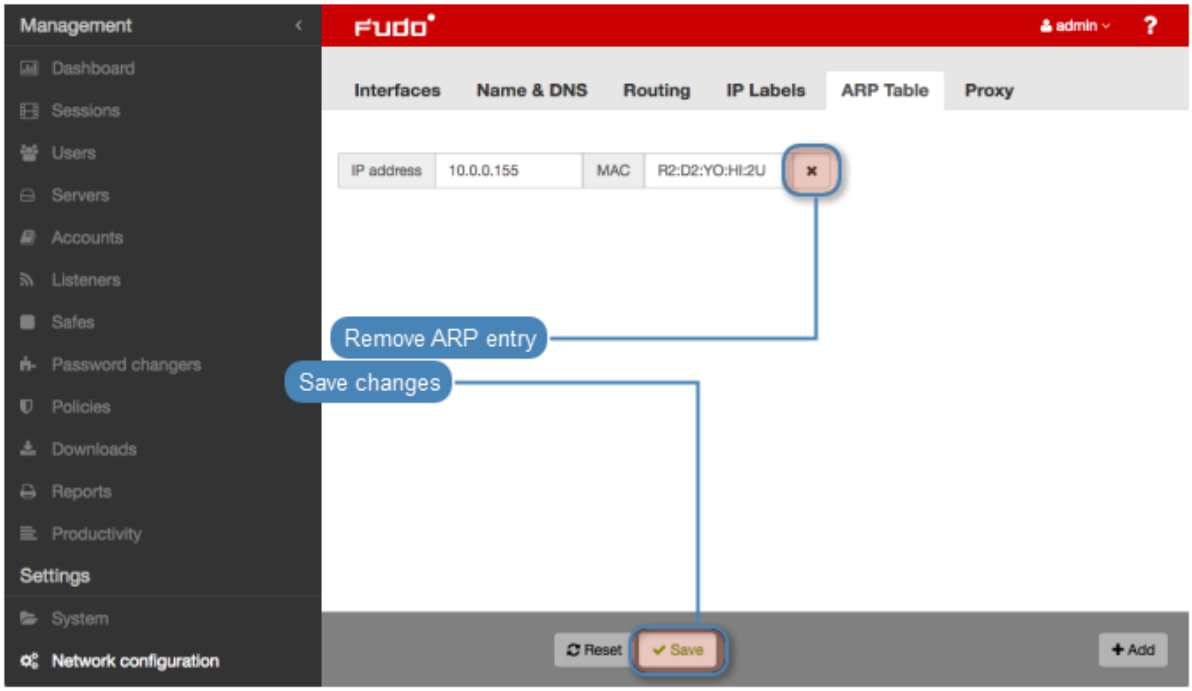
---

**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. Find desired ARP entry and click the ✖ icon.
4. Click *Save* .




**Related topics:**

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

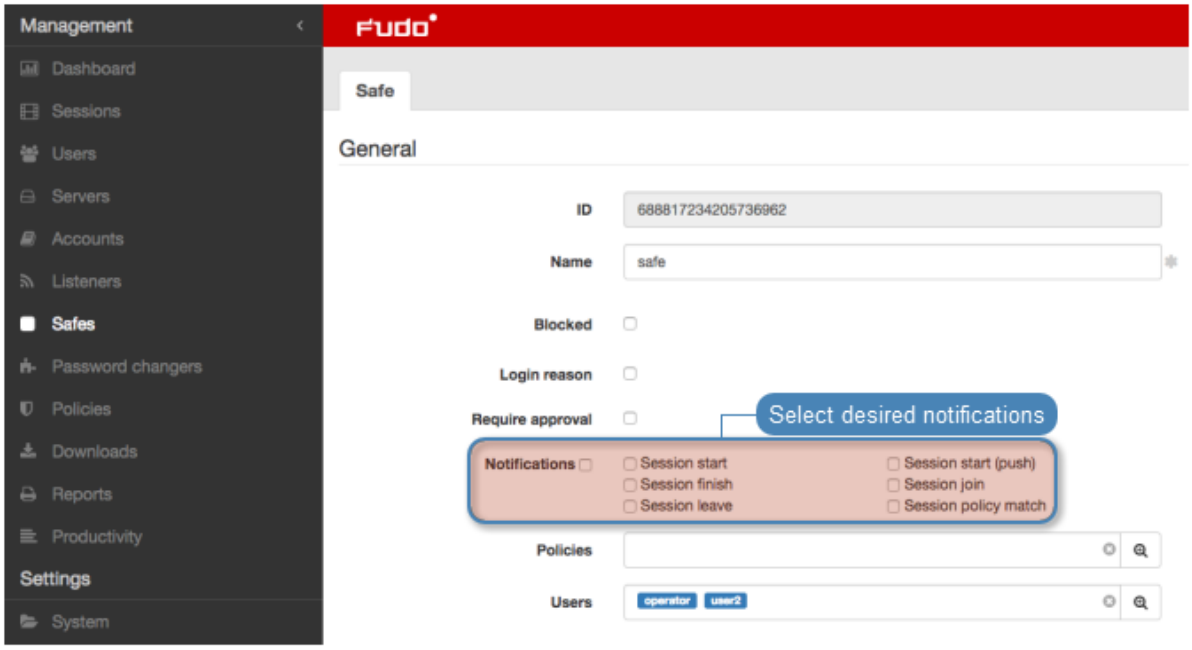
## 15.3 Notifications

Wheel Fudo PAM can send email notifications concerning defined connections (session start, session end, session inject start, session inject end). Notification service is configured when creating new or editing existing connection.

---

**Note:**

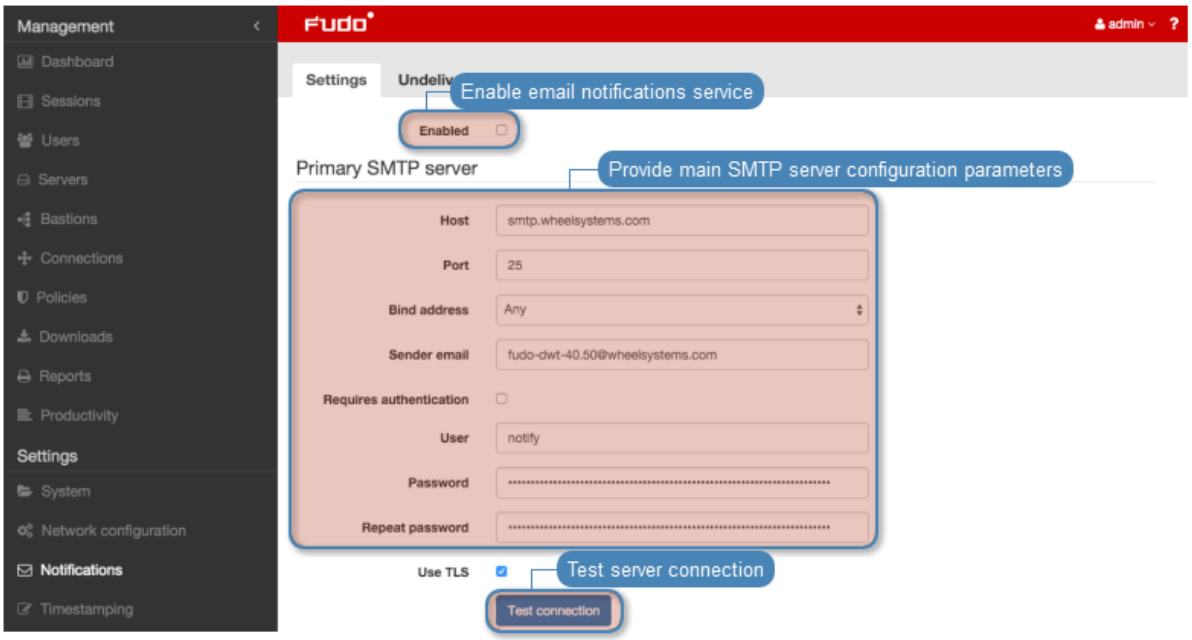
- Notifications can be received by users with *operator*, *admin* or *superadmin* roles.
- To receive notifications, login to Wheel Fudo PAM administration panel and select desired notifications in safe's configuration.




Email notifications service requires configuring SMTP server.

To configure SMTP server, proceed as follows.

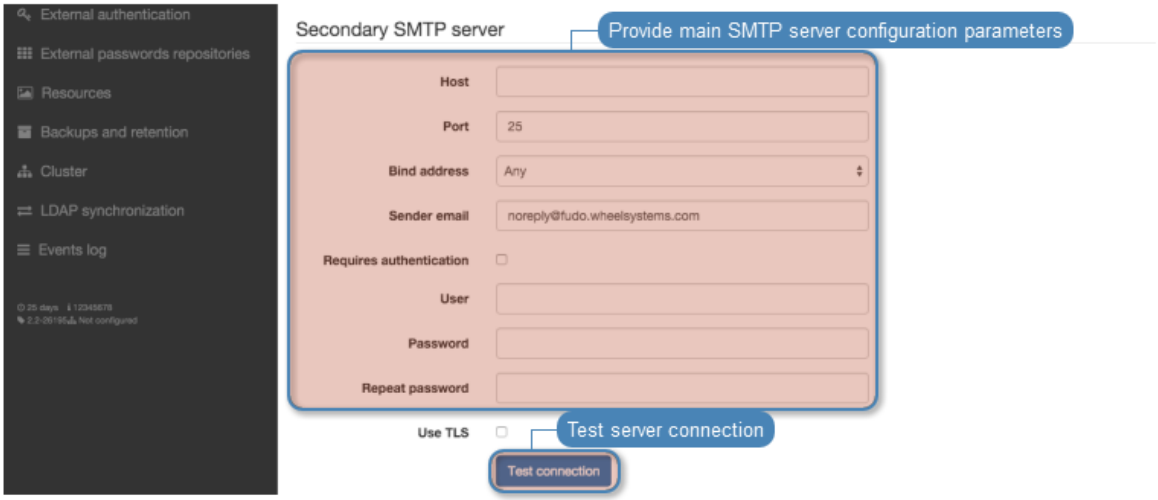
1. Select *Settings* > *Notifications*.
2. Select *Enabled* option.
3. Enter configuration parameters for the primary SMTP server.



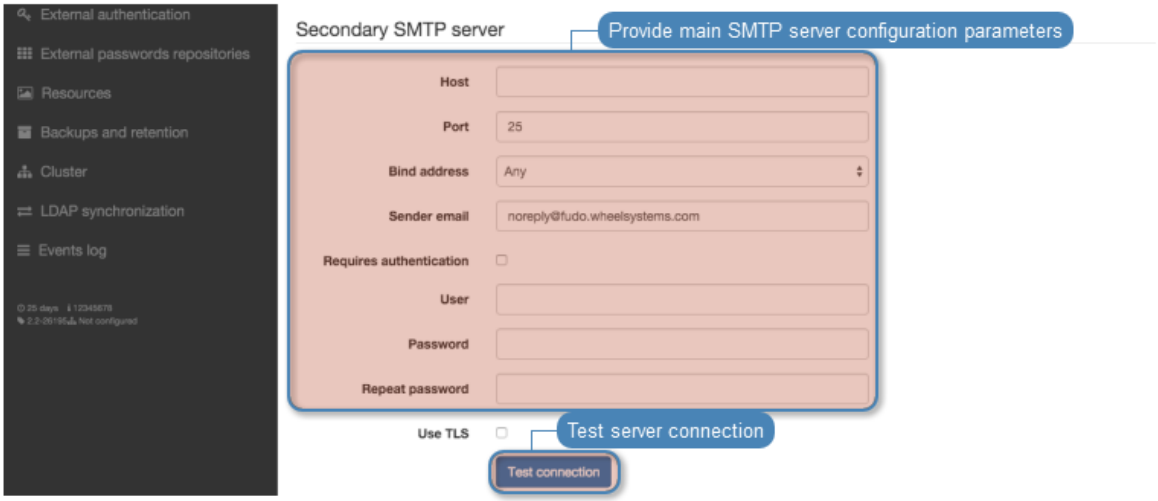
| Parameter | Description |
|---|---|
| Address | SMTP server IP address. |
| Port | SMTP service port number. |
| Sender email | Email address from which the emails will be sent. |
| Requires authentication | Select if the SMTP server requires authentication. |
| User | User name for authentication on SMTP server. |
| Password | User password for authentication on SMTP server. |
| Use secure connection (*TLS*) | Select if the mail server uses TLS protocol. |

**Note:** Click *Test connection* to make sure server parameters are correct.

4. Optionally, enter configuration parameters for the secondary SMTP server.




5. Enter server certificate in PEM format.



6. Click *Save*.

**Related Topics:**

- *Accounts*

## 15.4 Trusted time-stamping

A trusted timestamp makes recorded session a more convincing evidence in court.

---

**Note:** Trusted time-stamping feature requires signing a contract with an institution providing time-stamping services.

---

**Enabling and configuring trusted time-stamping**

---

**Note:** Wheel Fudo PAM will also timestamp sessions recorded before the feature was enabled.

---

1. Select *Settings* > *Trusted Timestamping*.
2. Select *Enabled* option.
3. Select from the *Provider* drop-down list the institution providing trusted time-stamping services.
4. Provide the certificate and the private key of the time-stamping service.

---

**Note:** You should receive these information from your time-stamping service provider.

---

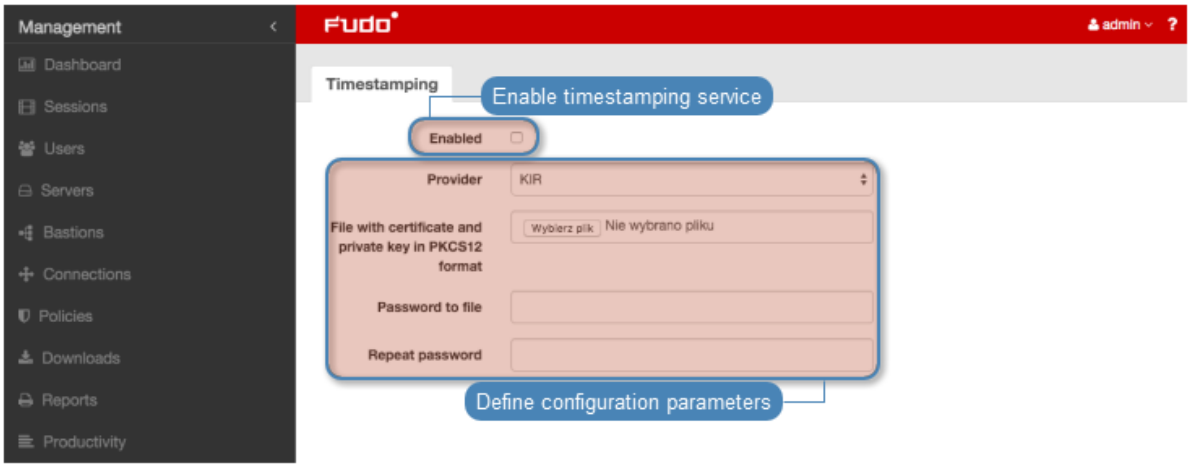
5. Click *Save*.

---

**Note:** Trusted time-stamping requires that Wheel Fudo PAM can reach the following resources:

- `193.178.164.5` (in case of time-stamping service being supplied by the *PWPW*)
- `http://www.ts.kir.com.pl/HttpTspServer` (in case of time-stamping service being supplied by the *KIR*)

---




**Related topics:**

- *Security measures*

## 15.5 External authentication

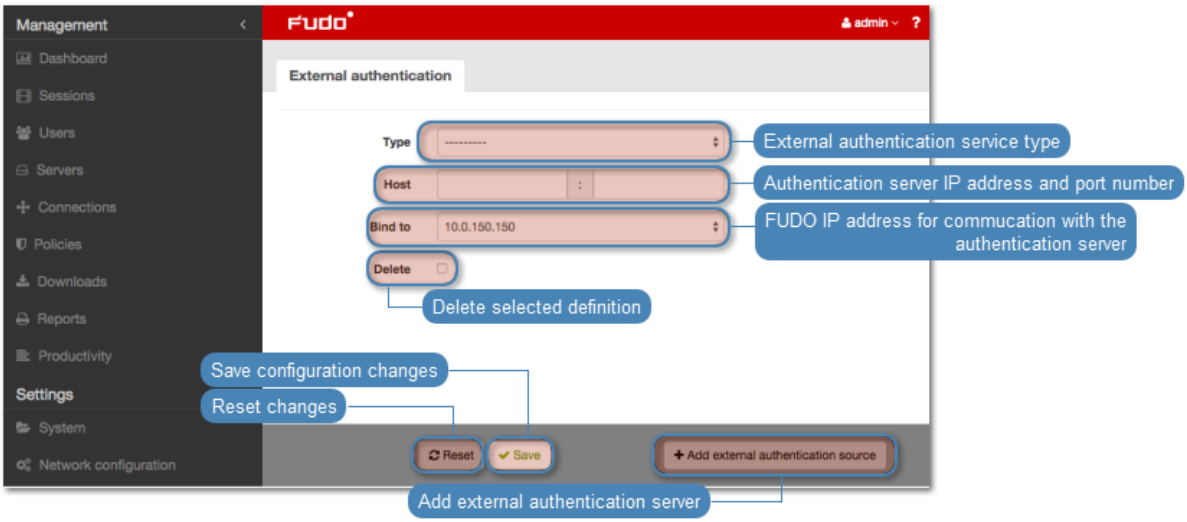
Some of the authentication methods, require defining connections to external authentication servers. These are:

- *CERB*,
- *RADIUS*,
- *LDAP*,
- *Active Directory*.

### Authentication servers configuration page

Authentication servers configuration page enables adding new and editing existing authentication servers.

To open the authentication servers configuration page, select *Settings* > *External authentication*.




### Adding a new external authentication server

To add an external authentication server, proceed as follows.

1. Select *Settings* > *External authentication*.
2. Click *+ Add external authentication source*.
3. Select authentication service type.
4. Provide configuration parameters depending on selected authentication system type.

| Parameter | Description |
|---|---|
| **CERB** | |
| Host | Server's IP address. |
| Port | Port used to establish connections with given server. |
| Bind address | IP address used for sending requests to given host. |
| Secret | Secret used to establish server connection. |
| Service | CERB service used for authenticating Wheel Fudo PAM users. |
| **RADIUS** | |
| Host | Server's IP address. |
| Port | Port used to establish connections with given server. |
| Bind address | IP address used for sending requests to given host. |
| Secret | Secret used to establish server connection. |
| NAS ID | RADIUS server NAS-Identifier parameter. |
| **LDAP** | |
| Host | Server's IP address. |
| Port | Port used to establish connections with given server. |
| Bind address | IP address used for sending requests to given host. |
| User DN template | Template containing a path which will be used to create queries to LDAP server. |
| **Active Directory** | |
| Host | Server's IP address. |
| Port | Port used to establish connections with given server. |
| Bind address | IP address used for sending requests to given host. |
| Domain | Domain which will be used for authenticating users in Active Directory. |

**Note:** 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.

5. Click *Save*.

**Editing authentication server definition**

To edit an authorization server definition, proceed as follows.

1. Select *Settings* > *External authentication*.
2. Find the server definition and change its configuration as desired.
3. Click *Save*.

**Deleting authentication server definition**

To delete authentication server definition, proceed as follows.

1. Select *Settings* > *External authentication*.
2. Find desired server definition and select the *Delete* option.
3. Click *Save*.

**Related topics:**

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

## 15.6 External passwords repositories

Wheel Fudo PAM supports external passwords repositories for managing passwords to monitored servers.

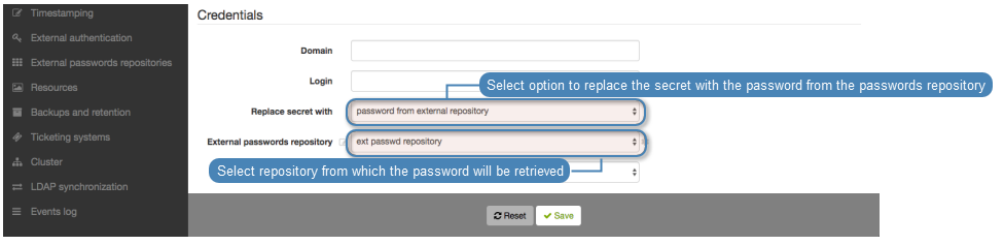
### 15.6.1 CyberArk Enterprise Password Vault

**Adding a new passwords repository**

1. Select *Settings* > *External passwords repositories*.
2. Click *+ Add server*.
3. Select `CyberArk Enterprise Password Vault` from the *Type* drop-down list.
4. Enter object's name.
5. Provide the URL to the passwords server's API.
6. Provide application identification.
7. Define the account format string.
8. Click *Save*.
9. Define server's object name and *ERPM namespace* in the *External password repository* sections.
    - Select *Management* > *Servers*.
    - Browse object and click an server to access the settings form.
    - In the *External password repository* section, provide the *Server object name* and *ERPM namespace*.

    - Click *Save*
10. 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, select *password from external repository* from the *Replace secret with* drop-down list.
- From the *External passwords repository* select one of the previously defined password repository.




- Click *Save*.

**Editing a passwords repository**

To edit a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find the repository definition and change its configuration as desired.
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 and select the *Delete* option.
3. Click *Save*.

**Related topics:**

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

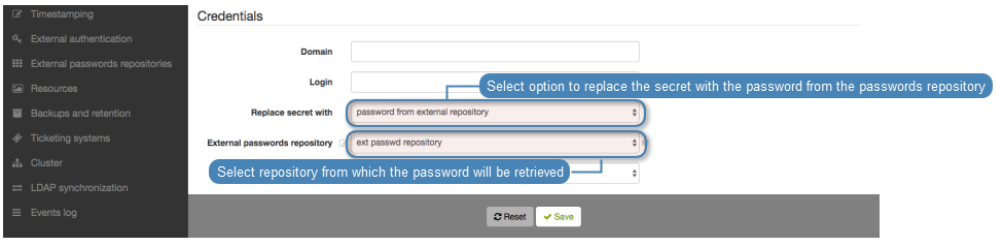
### 15.6.2 Hitachi ID Privileged Access Manager

**Adding a new passwords repository**

1. Select *Settings* > *External passwords repositories*.
2. Click *+ Add server*.
3. Select `Hitachi ID Privileged Access Manager` from the *Type* drop-down list.
4. Enter object's name.
5. Provide the URL to the paswords server's API.
6. Enter user login allowed to access passwords directory.

7. Provide user password in the *Password* and *Repeat password* fields.
8. Click *Save*.
9. Define server's object name and *ERPM namespace* in the *External password repository* sections.
    - Select *Management* > *Servers*.
    - Browse object and click an server to access the settings form.
    - In the *External password repository* section, provide the *Server object name* and *ERPM namespace*.

    - Click *Save*
10. 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, select *password from external repository* from the *Replace secret with* drop-down list.
    - From the *External passwords repository* select one of the previously defined password repository.




    - Click *Save*.

**Editing a passwords repository**

To edit a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find the repository definition and change its configuration as desired.
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 and select the *Delete* option.
3. Click *Save*.

**Related topics:**

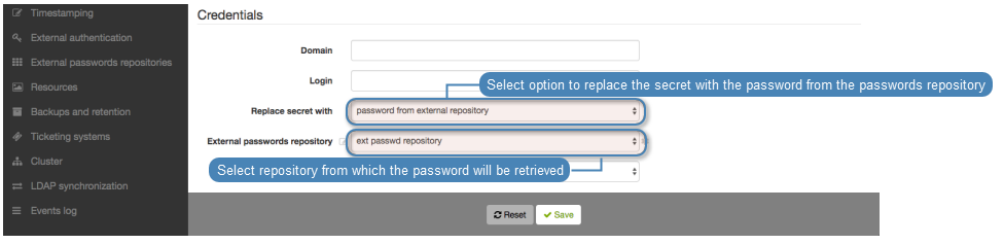
- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

### 15.6.3 Lieberman Enterprise Random Password Manager

**Adding a new passwords repository**

1. Select *Settings* > *External passwords repositories*.
2. Click *+ Add server*.
3. Select `Lieberman Enterprise Random Password Manager` from the *Type* drop-down list.
4. Enter object's name.
5. Provide the URL to the paswords server's API.
6. Define authention module assigned to the user who is allowed to access passwords repository.
7. Enter user login allowed to access passwords repository.
8. Provide user password in the *Password* and *Repeat password* fields.
8. Click *Save*.
9. Define server's object name and *ERPM namespace* in the *External password repository* sections.
    - Select *Management* > *Servers*.
    - Browse object and click an server to access the settings form.
    - In the *External password repository* section, provide the *Server object name* and *ERPM namespace*.

    - Click *Save*
10. 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, select *password from external repository* from the *Replace secret with* drop-down list.
    - From the *External passwords repository* select one of the previously defined password repository.




- Click *Save*.

**Editing a passwords repository**

To edit a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find the repository definition and change its configuration as desired.
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 and select the *Delete* option.
3. Click *Save*.

**Related topics:**

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

### 15.6.4 Thycotic Secret Server

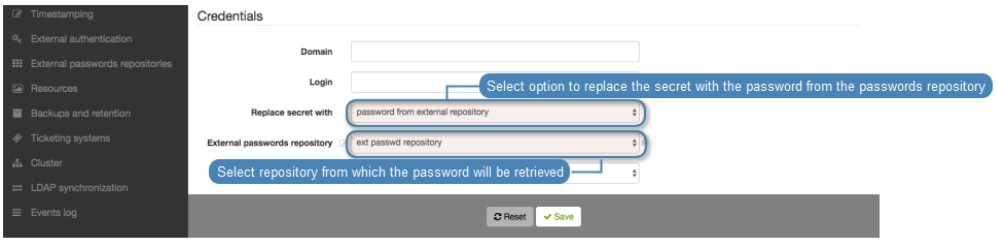
**Adding a new passwords repository**

1. Select *Settings* > *External passwords repositories*.
2. Click *+ Add server*.
3. Select `Thycotic Secret Server` from the *Type* drop-down list.
4. Enter object's name.
5. Provide the URL to the paswords server's API.
6. Enter user login allowed to access passwords repository.
7. Provide user password in the *Password* and *Repeat password* fields.
8. Define secret string format used for identifying objects on Thycotic Secret Server.
8. Click *Save*.
9. Define server's object name and *ERPM namespace* in the *External password repository* sections.
    - Select *Management* > *Servers*.

- Browse object and click an server to access the settings form.
- In the *External password repository* section, provide the *Server object name* and *ERPM namespace*.

- Click *Save*

10. 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, select *password from external repository* from the *Replace secret with* drop-down list.
    - From the *External passwords repository* select one of the previously defined password repository.




- Click *Save*.

**Editing a passwords repository**

To edit a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find the repository definition and change its configuration as desired.
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 and select the *Delete* option.
3. Click *Save*.

**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*

## 15.7 Resources

### 15.7.1 RDP/VNC login screen configuration

Wheel Fudo PAM enables customizing RDP and VNC login screen.

**Changing logo**

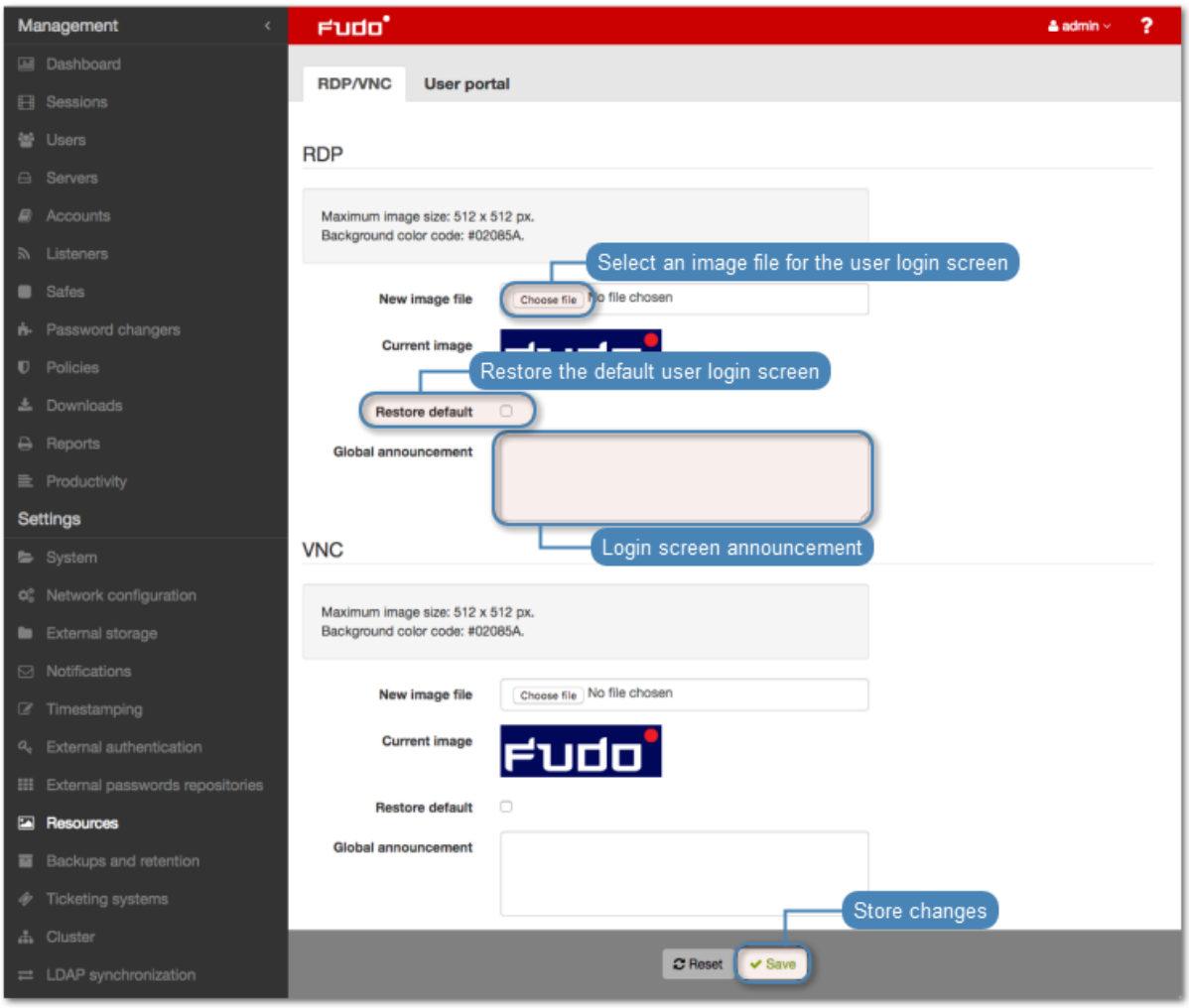
1. Select *Settings* > *Resources*.
2. Select the *RDP/VNC* tab.
3. In the *RDP* or *VNC* section, click *Choose File* button and select desired image.

---

**Note:** Maximum image size is 512 x 512 px.

---

4. Click *Save*.




### Restoring default logo

1. Select *Settings* > *Resources*.
2. Select *RDP/VNC* tab.
3. In the *RDP* or *VNC* section, select *Restore default* option.
4. Click *Save*.

### Defining global announcement

Global announcement is displayed on RDP and VNC login screen.

---

**Note:** Apart from global announcement, WHEEL Wheel Fudo PAM PAM also enables configuring local server message in server configuration form.

---

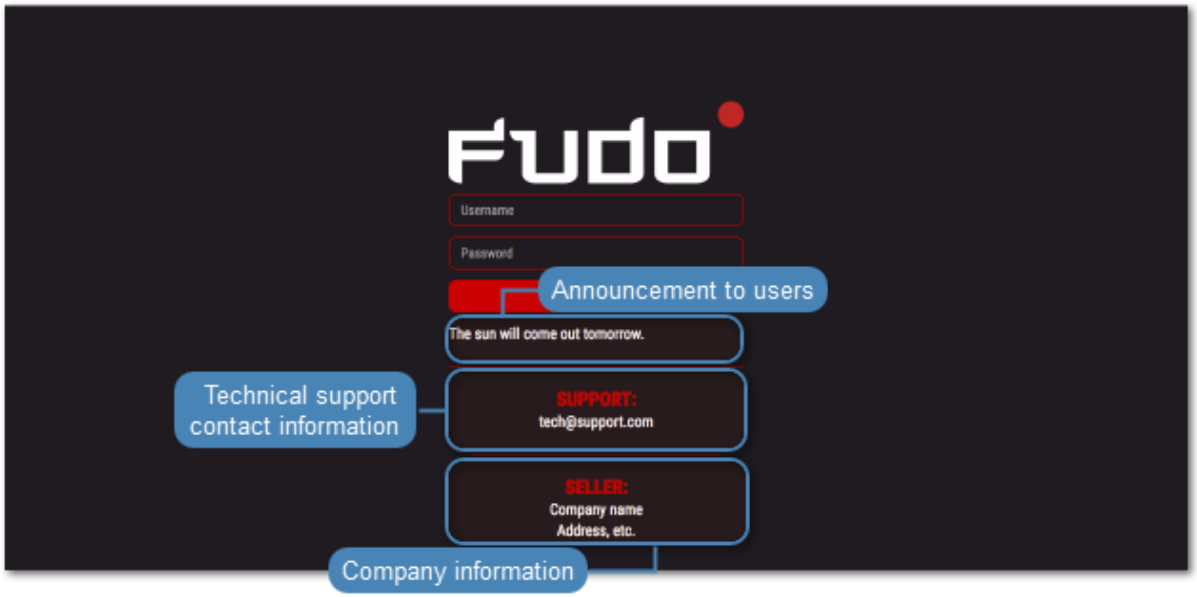
1. Select *Settings* > *Resources*.
2. Select *RDP/VNC* tab.
3. In the *RDP* or *VNC* section, enter desired message in the *Global announcement* field.
4. Click *Save*.

### Related topics:

- *Quickstart - RDP*

### 15.7.2 *User portal* login screen configuration

Wheel Fudo PAM enables customizing information displayed on the *User portal* login screen.




1. Select *Settings* > *Resources*.
2. Select the *User portal* tab.
3. Provide company information.

**Note:** Company information can be five lines, up to 70 characters.

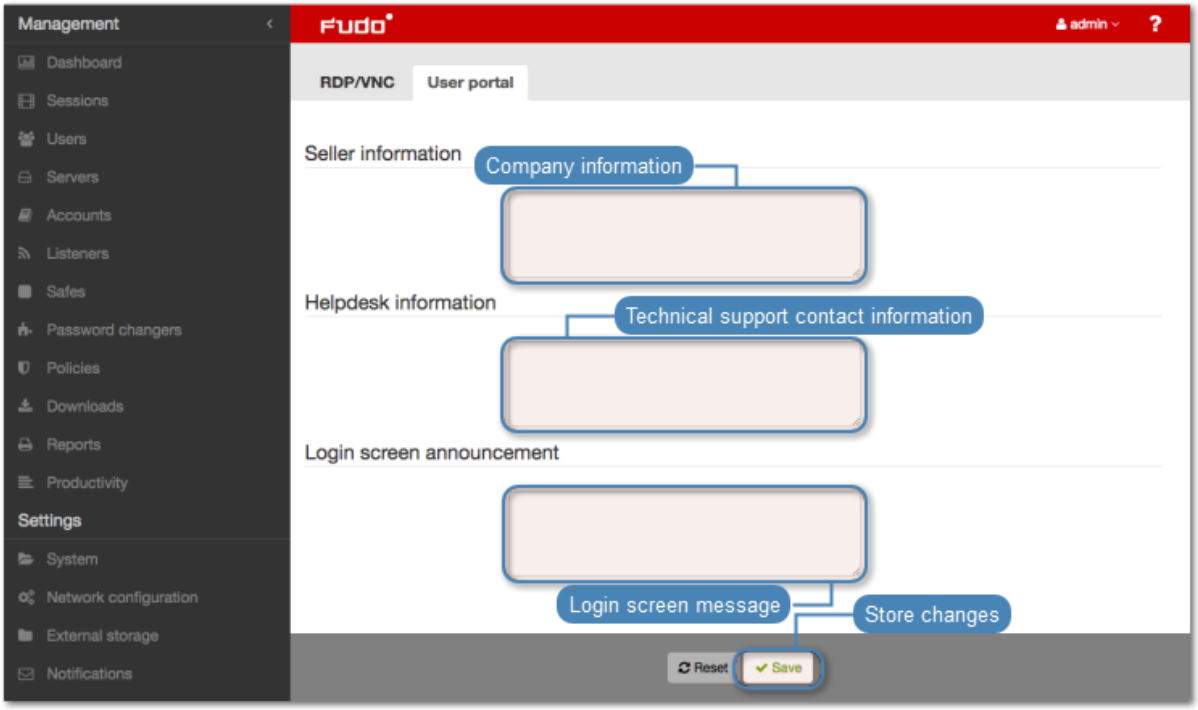
4. Enter help desk contact information.

**Note:** Helpdesk contact information can be five lines, up to 70 characters.

5. Provide the login screen announcement.

**Note:** Login screen announcement can be four lines, up to 120 characters.

5. Click *Save*.




**Related topics:**

- *User portal*

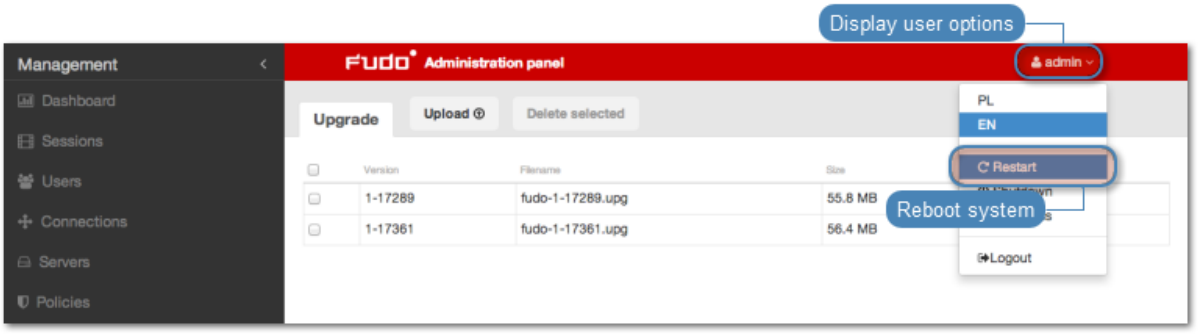
## 15.8 System version restore

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.

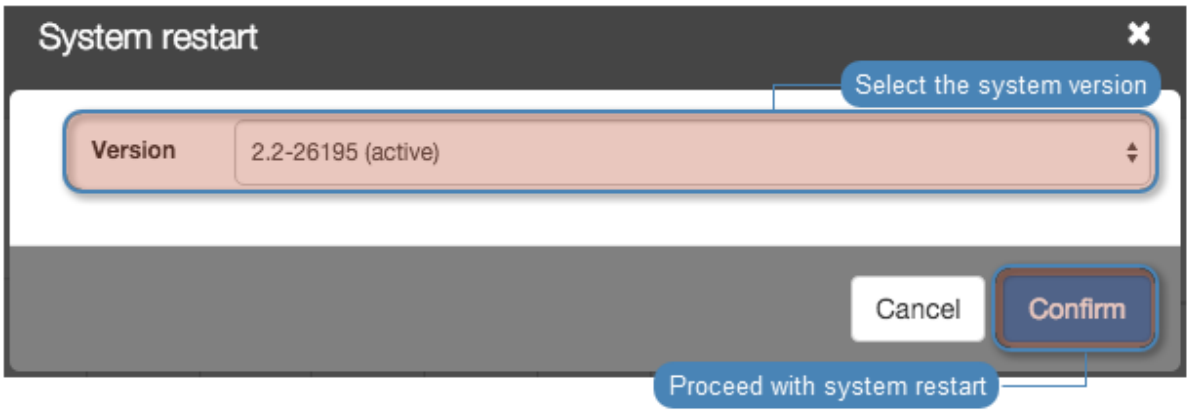
To restore the system to the previous revision, proceed as follows.

1. Connect one of the USB flash drives containing the encryption key.
2. Select *Restart* 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.




4. Click *Confirm* to proceed with restarting the system to the selected revision.

**Warning:** Restrating the system will terminate all current users' connections.

**Related topics:**

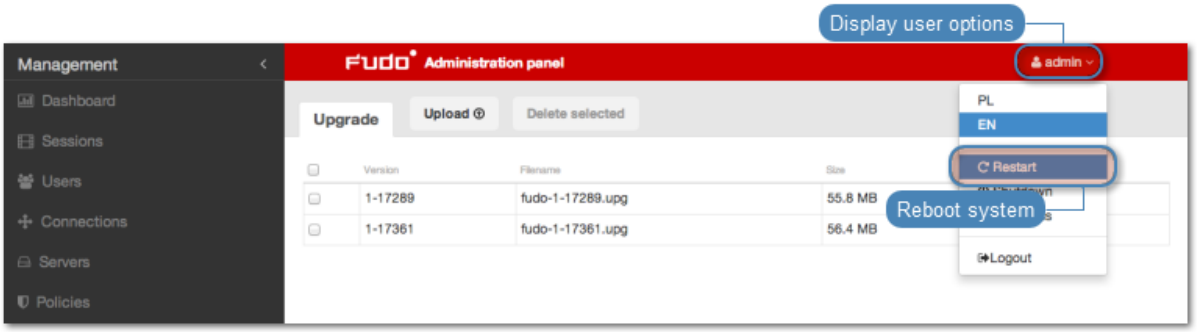
- *System initiation*
- *System update*

## 15.9 System restart

**Note:**

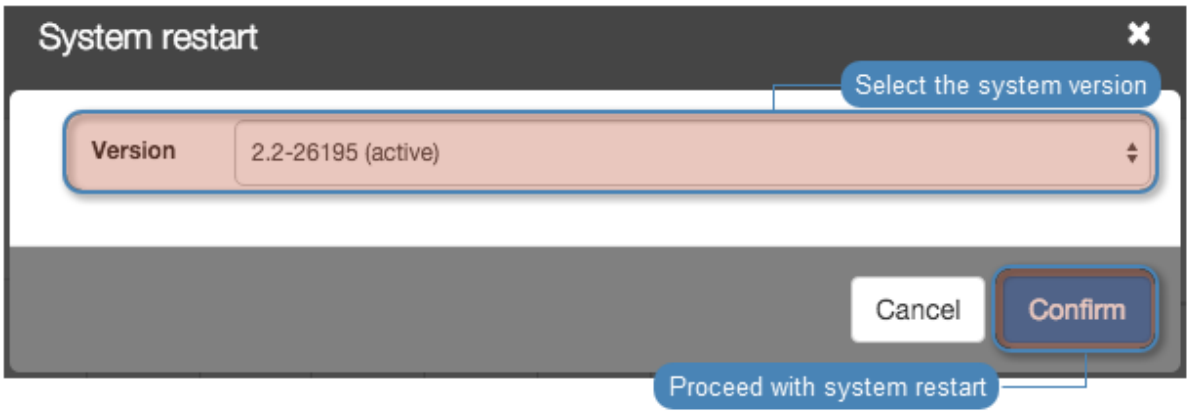
- System restart requires USB flash drive with the encryption key connected to the device.
- Restrating the system will terminate all current users' connections.
- Use the *Deny new connections* option in the *Sessions* section in the system settings menu.

1. Connect one of the USB flash drives containing the encryption key.
2. Select *Restart* 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.




4. Click *Confirm* to proceed with restarting the system to the selected revision.

**Related topics:**

- *System initiation*
- *System version restore*

## 15.10 SNMP

Wheel Fudo PAM's status can be monitored over SNMPv3 protocol.

### 15.10.1 Configuring SNMP

1. Select *Settings* > *System*.
2. Select *Enabled* option in the *SNMPv3* section.
3. From the *IP address* drop-down list select IP address, which will be used for SNMP communication.
4. Click *Save*.
5. Select *Management* > *Users*.
6. Click *+ Add*.
7. Select `service` from the *Role* drop-down list and fill in the rest of the *General* section parameters.
8. Select `password` from the *Authentication* drop-down list and enter the password string.

**Note:**

- SNMP user password must be at least eight characters long.
- SNMP service authenticates the service account using the first defined password.

9. Select *Enabled* option in the *SNMP* section.
10. Select authentication methods from the *Authentication method* drop-down list.
11. Select the SNMP encryption algorithm from the *Encryption* drop-down list.
12. Clikc *Save*.

### 15.10.2 SNMP MIBs

Wheel Fudo PAM supports following MIBs:

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790) - partly supported
- UCD-SNMP-MIB

### 15.10.3 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<br>**Note:** This feature is not supported on all Wheel Fudo PAM units. Contact Wheel Systems 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 |

### 15.10.4 Wheel Fudo PAM 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

Provided MIB file specification can be uploaded to the SNMP manager to enable Wheel Fudo PAM specific SNMP extensions.

```
WHEEL-SYSTEMS-MIB DEFINITIONS ::= BEGIN

--
-- MIB definition for Wheel Systems products
--

IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, Gauge32, Counter32, enterprises
                FROM SNMPv2-SMI;

wheel MODULE-IDENTITY
        LAST-UPDATED "201704240000Z"    -- 24 April 2017
        ORGANIZATION "www.wheelsystems.com"
        CONTACT-INFO
                 "Postal:   Wheel Systems Inc. (USA)
                                    31 N 2nd Street 370,
                                    San Jose, CA 95113
                  Phone:    +1 (415) 800 3230
                  email:    info@wheelsystems.com"
        DESCRIPTION
        "Top-level infrastructure of the Wheel Systems enterprise MIB tree"
        REVISION     "201704240000Z"
        DESCRIPTION
        "Moved common to .1, fudo to .2."
        REVISION     "201703270000Z"
        DESCRIPTION
        "Added objects for checking CPU temperature."
        REVISION     "201703150000Z"
        DESCRIPTION
        "Added objects describing status of power supply units."
        REVISION     "201703060000Z"
        DESCRIPTION
        "New objects to monitor disk status."
        REVISION     "201702140000Z"
        DESCRIPTION
        "First draft"
        ::= { enterprises 24410 }

products  OBJECT IDENTIFIER ::= { wheel 1 }

common OBJECT IDENTIFIER ::= { products 1 } -- Objects common to more than one␣
↪product.
fudo   OBJECT IDENTIFIER ::= { products 2 }

zpool OBJECT IDENTIFIER ::= { common 1 }

syncPercentage OBJECT-TYPE
        SYNTAX     Integer32 (0..100)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Percentage of vdev synchronization."
```

(continues on next page)

(continued from previous page)

```
        ::= { zpool 1 }

syncTimeLeft OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Time left for synchronization or N/A if it cannot be determined."
        ::= { zpool 2 }

vdevTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF VdevEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "The table of vdevs. The vdev is an element in ZFS pool"
        ::= { zpool 3 }

vdevEntry OBJECT-TYPE
        SYNTAX      VdevEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "An entry for one vdev status in ZFS pool."
        INDEX { vdevIndex }
        ::= { vdevTable 1 }

VdevEntry ::= SEQUENCE {
        vdevIndex         Integer32,
        vdevStatus        OCTET STRING
}

vdevIndex OBJECT-TYPE
        SYNTAX     Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A unique value for each vdev in ZFS pool."
        ::= { vdevEntry 1 }

vdevStatus OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Status of the vdev in ZFS pool."
        ::= { vdevEntry 2 }

powerSupply OBJECT IDENTIFIER ::= { common 2 }

powerSupplyTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF PowerSupplyEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "The table of power supply units status, such as which unit is
```

(continues on next page)

(continued from previous page)

```
                operating."
        ::= { powerSupply 1 }

powerSupplyEntry OBJECT-TYPE
        SYNTAX      PowerSupplyEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "An entry in power supply table representing the status of the
                 associated power supply unit."
        INDEX { powerSupplyIndex }
        ::= { powerSupplyTable 1 }

PowerSupplyEntry ::= SEQUENCE {
        powerSupplyIndex   Integer32,
        powerSupplyStatus  INTEGER
}

powerSupplyIndex OBJECT-TYPE
        SYNTAX     Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A unique index for each power supply unit."
        ::= { powerSupplyEntry 1 }

powerSupplyStatus OBJECT-TYPE
        SYNTAX     INTEGER {
                unknown(1),
                present(2),
                absent(3),
                configError(4),
                acLost(5),
                predictiveFailure(6),
                failed(7)
        }
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The status of power supply unit. When everything is working, reported
                 status should be present(1). This information is gathered from IPMI
                 subsystem."
        ::= { powerSupplyEntry 2 }

cpu OBJECT IDENTIFIER ::= { common 3 }

cpuTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF CpuEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "The table of CPUs statuses."
        ::= { cpu 1 }

cpuEntry OBJECT-TYPE
        SYNTAX      CpuEntry
```

(continues on next page)

(continued from previous page)

```
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "An entry in CPU table representing the status of the associated CPU."
        INDEX { cpuIndex }
        ::= { cpuTable 1 }

CpuEntry ::= SEQUENCE {
        cpuIndex       Integer32,
        cpuTemperature Gauge32
}

cpuIndex OBJECT-TYPE
        SYNTAX     Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A unique index for each CPU."
        ::= { cpuEntry 1 }

cpuTemperature OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The temperature of CPU in degree Celsius."
        ::= { cpuEntry 2 }

smart OBJECT IDENTIFIER ::= { common 4 }

smartTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF SmartEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "The table contains devices with enabled SMART and their statuses.␣
↪Note
                that interpretation all elements reported in this table are hard disk
                manufacturer dependent. Values are reported as raw value or as
                (normalized value - threshold). The lower is value of
                (normalized value - threshold) the worst. Keep in mind that every
                manufacturer uses their own algorithms for calculating 'normalized
                value'."
        ::= { smart 1 }

smartEntry OBJECT-TYPE
        SYNTAX      SmartEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "An entry in SMART table representing the status of the associated
                device."
        INDEX { smartIndex }
        ::= { smartTable 1 }

SmartEntry ::= SEQUENCE {
```

(continues on next page)

(continued from previous page)

```
        smartIndex              Integer32,
        smartModelFamily        OCTET STRING,
        smartDeviceModel        OCTET STRING,
        smartSerialNumber       OCTET STRING,
        smartHealth             INTEGER,
        smartTemperature        Gauge32,
        smartReallocatedSectors Gauge32,
        smartPendingSectors     Gauge32,
        smartUncorrectable      Gauge32,
        smartUdmaCrcErrors      Gauge32,
        smartReadErrorRate      Gauge32,
        smartSeekErrorRate      Gauge32
}

smartIndex OBJECT-TYPE
        SYNTAX     Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A unique index for each SMART-enabled device."
        ::= { smartEntry 1 }

smartModelFamily OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Model family of device."
        ::= { smartEntry 2 }

smartDeviceModel OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Device model."
        ::= { smartEntry 3 }

smartSerialNumber OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Serial number of the device."
        ::= { smartEntry 4 }

smartHealth OBJECT-TYPE
        SYNTAX     INTEGER {
                unknown(1),
                ok(2),
                failed(3)
        }
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Health of the device as reported by SMART system."
```

(continues on next page)

(continued from previous page)

```
        ::= { smartEntry 5 }

smartTemperature OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The temperature of disk in degree Celsius."
        ::= { smartEntry 6 }

smartReallocatedSectors OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The number of reallocated sectors: bad sectors found and then␣
↪remapped.
                Reported as raw value of 'Reallocated Sectors Count' SMART attribute."
        ::= { smartEntry 7 }

smartPendingSectors OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The number of sectors waiting to be remapped. Reported as raw value␣
↪of
                'Current Pending Sector Count' SMART attribute."
        ::= { smartEntry 8 }

smartUncorrectable OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The number of uncorrectable errors when accessing sectors. Reported␣
↪as
                raw value of 'Offline Uncorrectable Sector Count' SMART attribute."
        ::= { smartEntry 9 }

smartUdmaCrcErrors OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The number of errors in data transfer determined by the means of␣
↪ICRC.
                Reported as raw value of 'UltraDMA CRC Error Count' SMART attribute."
        ::= { smartEntry 10 }

smartReadErrorRate OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The rate of hardware read errors. Reported as
```

(continues on next page)

(continued from previous page)

```
                (normalized value - threshold) of 'Read Error Rate' SMART attribute."
        ::= { smartEntry 11 }

smartSeekErrorRate OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The rate of seek errors. Reported as (normalized value - threshold)␣
↪of
                'Seek Error Rate'."
        ::= { smartEntry 12 }

sessionTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF SessionEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "The table of active sessions on Fudo."
        ::= { fudo 1 }

sessionEntry OBJECT-TYPE
        SYNTAX      SessionEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "An entry for one session type on Fudo. For example, information about
                active RDP sessions."
        INDEX { sessionIndex }
        ::= { sessionTable 1 }

SessionEntry ::= SEQUENCE {
        sessionIndex         Integer32,
        sessionName          OCTET STRING,
        sessionDescription   OCTET STRING,
        sessionActive        Counter32
}

sessionIndex OBJECT-TYPE
        SYNTAX     Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A unique value for each supported sessions on Fudo."
        ::= { sessionEntry 1 }

sessionName OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A name of session type."
        ::= { sessionEntry 2 }

sessionDescription OBJECT-TYPE
        SYNTAX     OCTET STRING
```

(continues on next page)

(continued from previous page)

```
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A description of session type."
        ::= { sessionEntry 3 }

sessionActive OBJECT-TYPE
        SYNTAX     Counter32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A number of active sessions of this type."
        ::= { sessionEntry 4 }

END
```

**Related topics:**

- *Security measures*
- *Troubleshooting*

## 15.11 Backups and retention

### Data retention

Wheel Fudo PAM implements two stage data retention. First data is moved from the internal storage to the external storage connected over fiber channel interface. After defined time period session data is automatically deleted.

To enable data retention service, proceed as follows.

1. Select *Settings* > *Backups and retention*.
2. Select *Moving session data to external storage enabled* option in the *Data retention* section.
3. Define how long data will be stored locally before it is moved to the external storage.
4. Select *Session data removal enabled* option to have the data automatically removed after specified time period.
5. Define how long data will be stored before being deleted.

**Note:** Global retention parameter values have lower priority than the values set in the *accounts*.

6. Click *Save*.

### System backup

**Warning:** Data backup contains confidential information.

Data stored on Wheel Fudo PAM can be backed up on an external server running `rsync` service. Backup service has to be enabled on Wheel Fudo PAM and requires uploading external server's

public SSH key, to authorize access to Wheel Fudo PAM.

Automated data backup requires configuring `rsync` service on a remote server and granting access rights to data stored on Wheel Fudo PAM by uploading to Wheel Fudo PAM server's public SSH key.

---

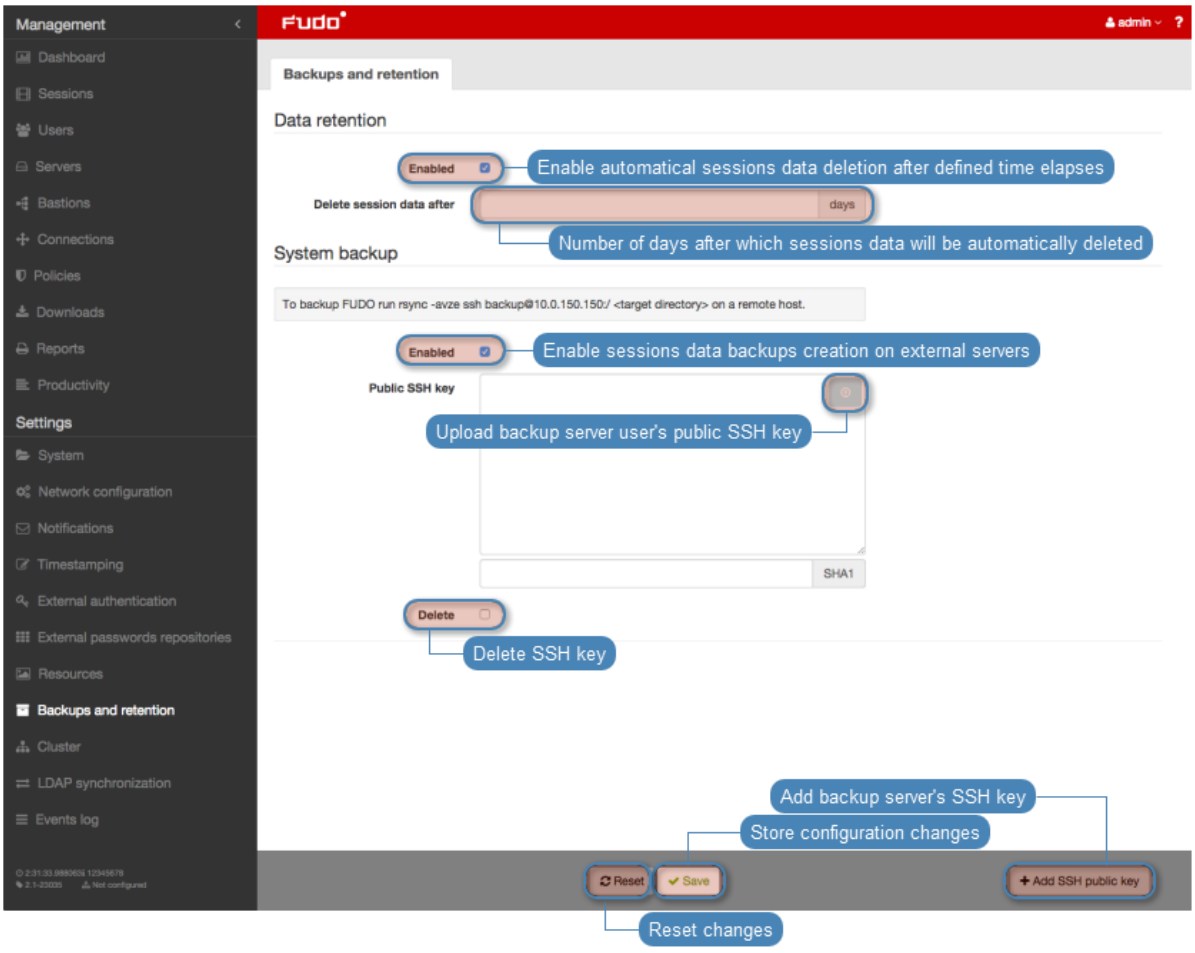
**Note:** Sessions data is stored on a compressed file system with compression ratio of up to 12:1. Data is decompressed upon being copied by `rsync` thus it will occupy more space on the target server than indicated by Wheel Fudo PAM storage usage. Make sure there is enough storage space on the target server to store uncompressed data.

---

To enable automated backups service, proceed as follows.

1. Select *Settings* > *Backups and retention*.
2. Select *Enabled* option in the *System backup* section.
3. Click *Add SSH public key*.
4. Paste or upload the remote server user's public SSH key.
5. Click *Save*.
6. Run `rsync` on the backup server:

```
rsync -avze ssh backup@fudo_ip_address:/  <destination_folder>
```




### Restoring system from backup

System restore service is provided by Wheelsystems technical support department on terms agreed in the SLA.

**Related topics:**

- *Exporting/importing system configuration*
- *Security measures*

## 15.12 External storage

Wheel Fudo PAM enables storing session data on external storage devices connected to Fudo through a fiber channel interface.

---

**Note:** External storage in cluster configuration

- In cluster configuration, each node must have a dedicated *WWN* object.
- Data stored externally is not replicated between cluster nodes.

---

### 15.12.1 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.

---

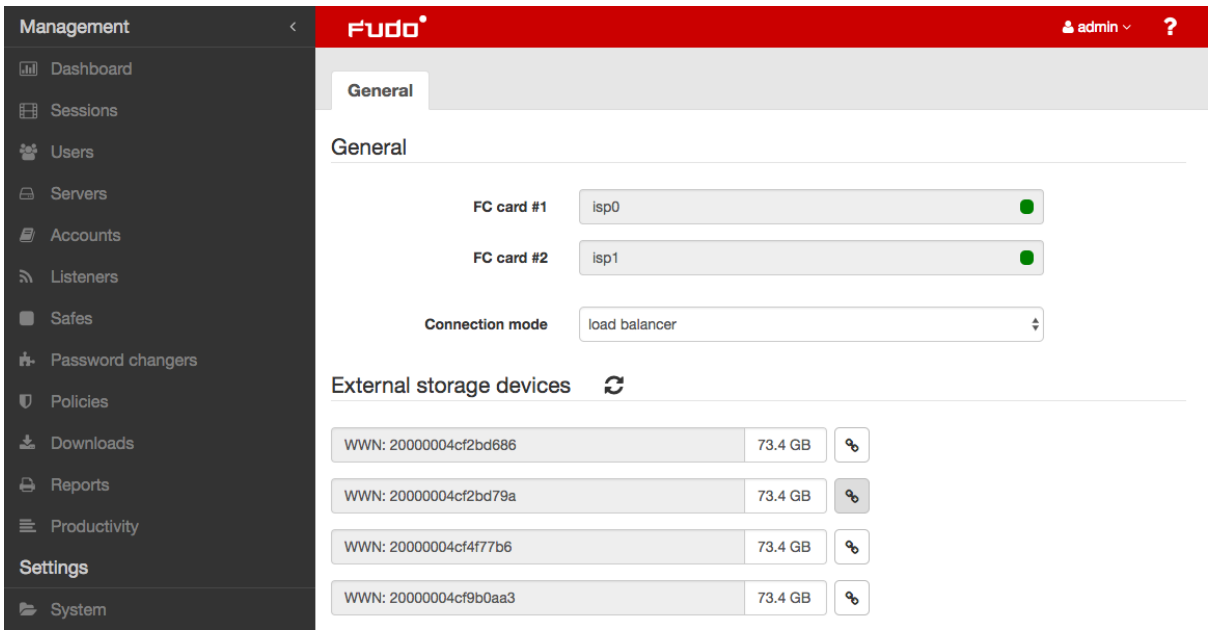
2. Select fiber channel cards operating mode.
   - Failover - data is transmitted using one fiber channel interface. If the card fails, the other one takes over ensuring continuous availability of the external storage device.
   - Load balancing - both fiber channel interfaces are used to transfer data between Wheel Fudo PAM 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*.

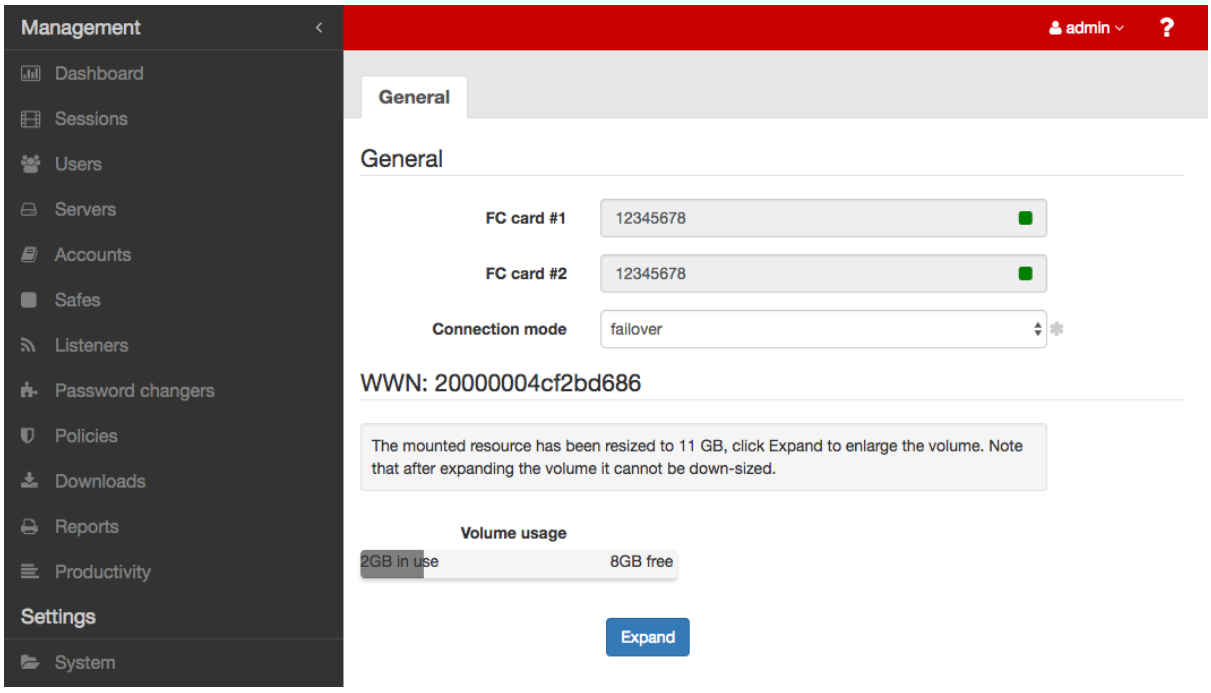



### 15.12.2 Expanding external storage device

After resizing the WWN object, it must be expanded in Wheel Fudo PAM 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:**

- *Backups and retention*

## 15.13 Exporting/importing system configuration

Wheel Fudo PAM enables exporting current system state, defined objects and configuration settings, which later can be used to initiate the system.

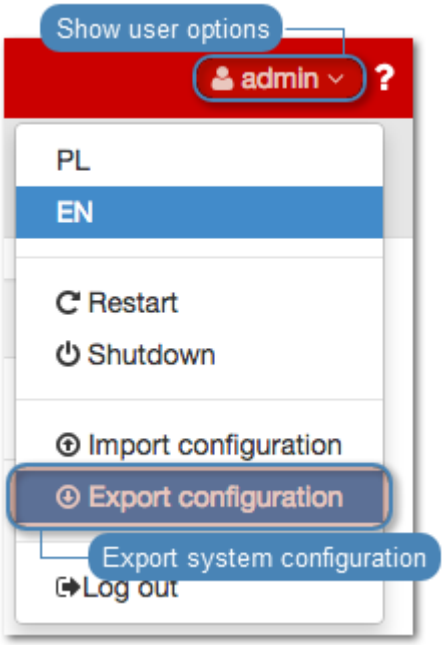
**Warning:** Exported configuration data contains confidential information.

**Note:** Configuration export and import options are available only for the *superadmin* users.

### 15.13.1 Exporting system configuration

To export system configuration, proceed as follows.

1. Select *Export configuration* from the user menu.
2. Save the configuration file.



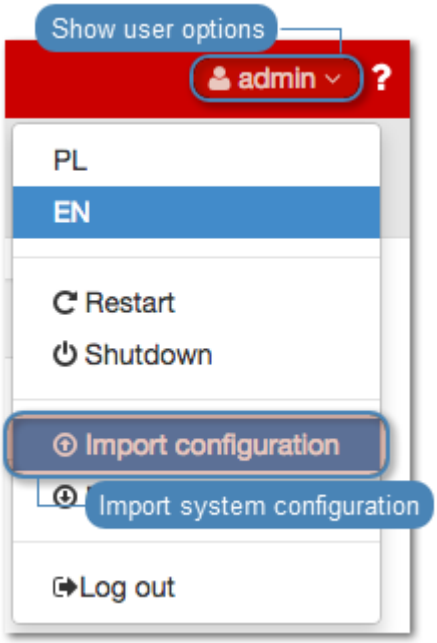
### 15.13.2 Importing system configuration

**Warning:**

- Configuration data importing is not allowed in *cluster configuration*.
- 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. Select *Import configuration* from the user menu.




2. Provide the path to the desired configuration file and click *Confirm*.
3. Click *Confirm* to proceed with initiating the system with the imported data.

**Related topics:**

- *Backups and retention*
- *System initiation*
- *System update*

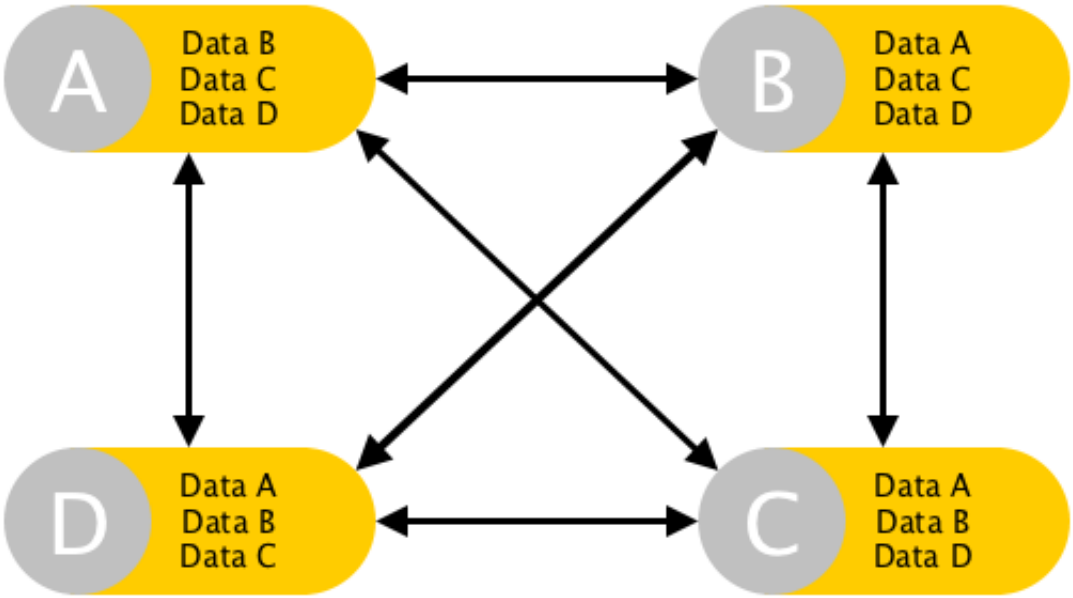
## 15.14 Cluster configuration

Wheel Fudo PAM 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.

All data model objects and sessions data are replicated between cluster nodes. Each node stores a copy of data recorded on other nodes within the cluster instance.

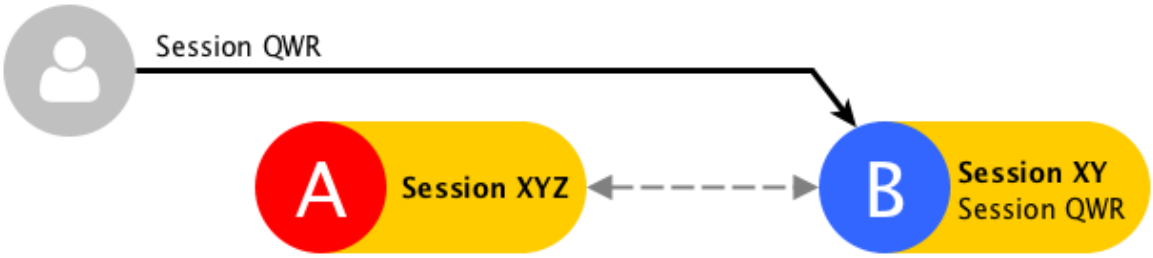



In case of a node failure, user access requests will be picked up by another cluster node, determined by the *redundancy group priority*.

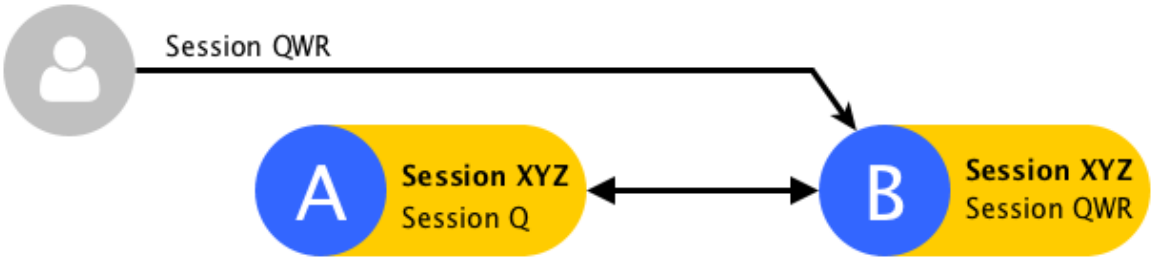
Current session data is replicated to other nodes while the connection is still ongoing.

If the node that fails was recording sessions, those sessions will be terminated...

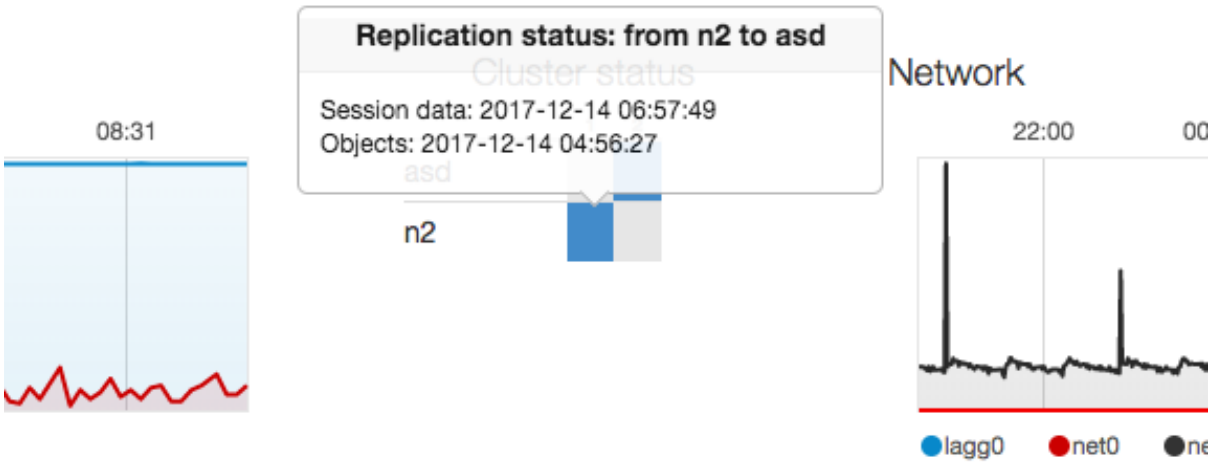
...and users will have to reconnect.



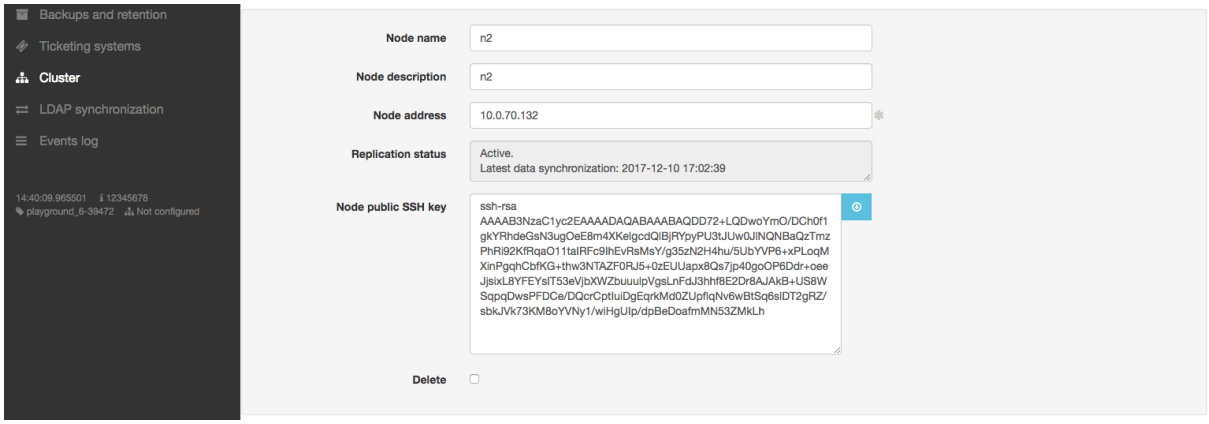

A part of the session data from the node that malfunctioned, which has synchronized, can be accessed on the other nodes, but the session will be fully accessible once the node becomes operational and session data is synchronized between cluster nodes.




Cluster replication status can be reviewed on the dashboard or on the cluster settings view.




- *Session data* - the timestamp of the session data replicated from the given node.
- *Objects* - the timestamp of the replicated data model objects.

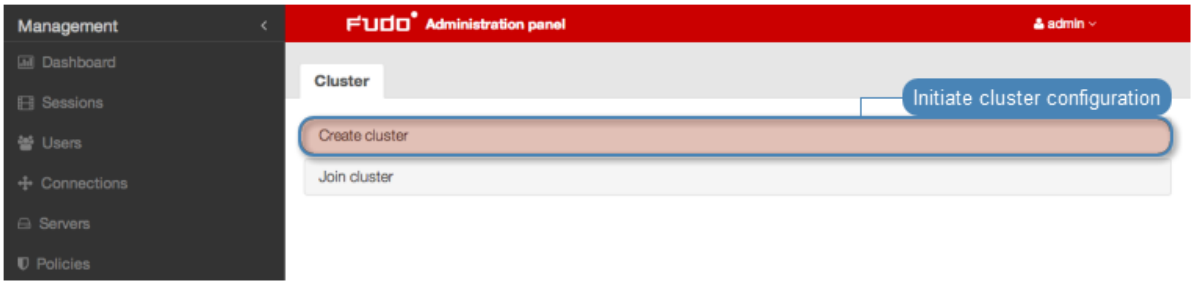



### 15.14.1 Initiating cluster

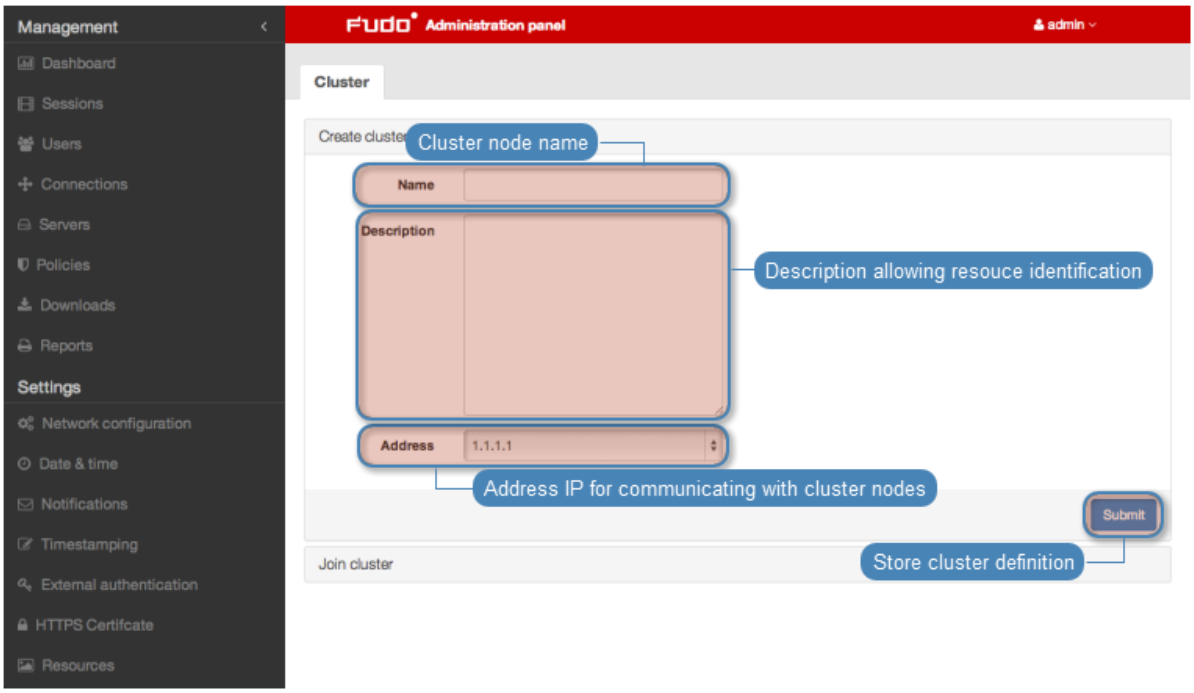
**Warning:** In cluster configuration all cluster nodes must have *NTP server configured*.

To initiate Wheel Fudo PAM 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.




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*
- *Security: Cluster configuration*
- *Redundancy groups*
- *Cluster configuration*

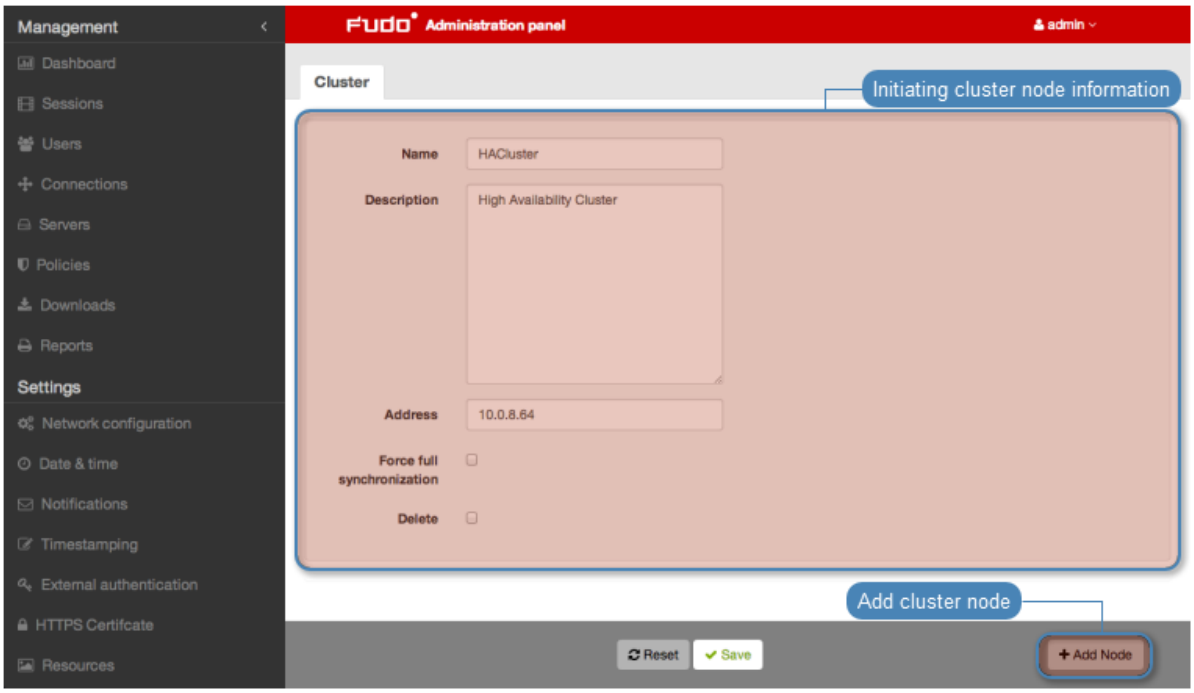
### 15.14.2 Adding cluster nodes

**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.

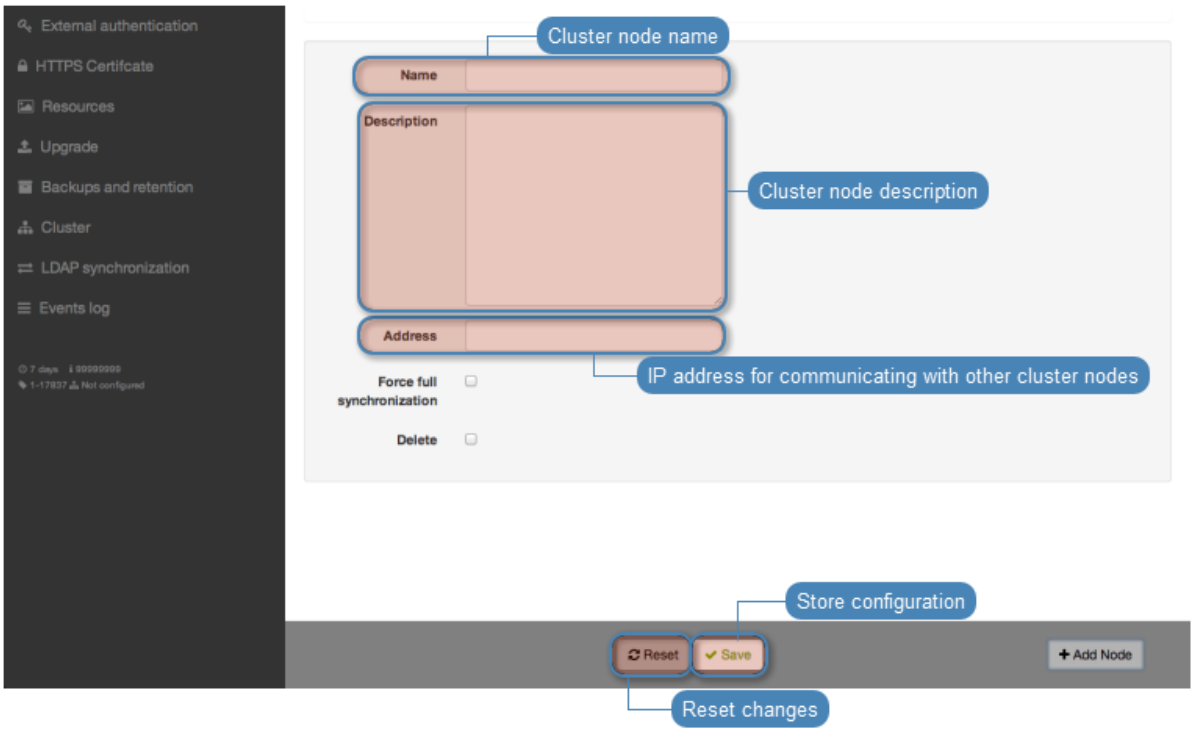
To add a node to Wheel Fudo PAM cluster, proceed as follows.

1. Log in to the Wheel Fudo PAM administration panel where the cluster has been *initiated*.
2. Select *Settings* > *Cluster*.
3. Click *Add node* to display new node configuration parameters.

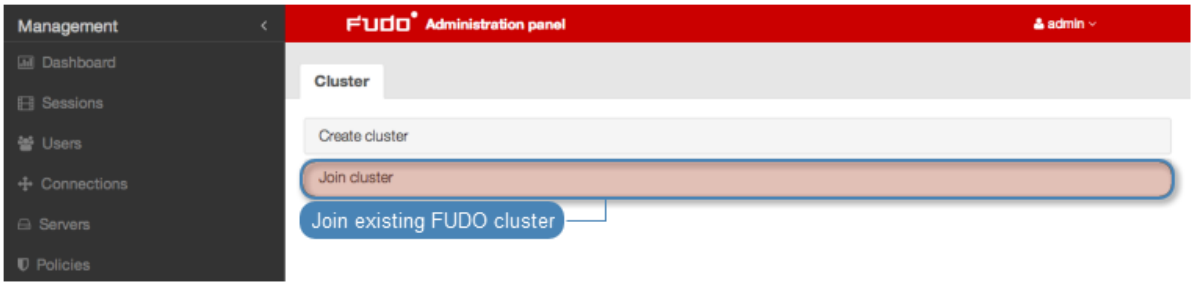



4. Provide node's name and optional description.
5. Provide node's IP address.

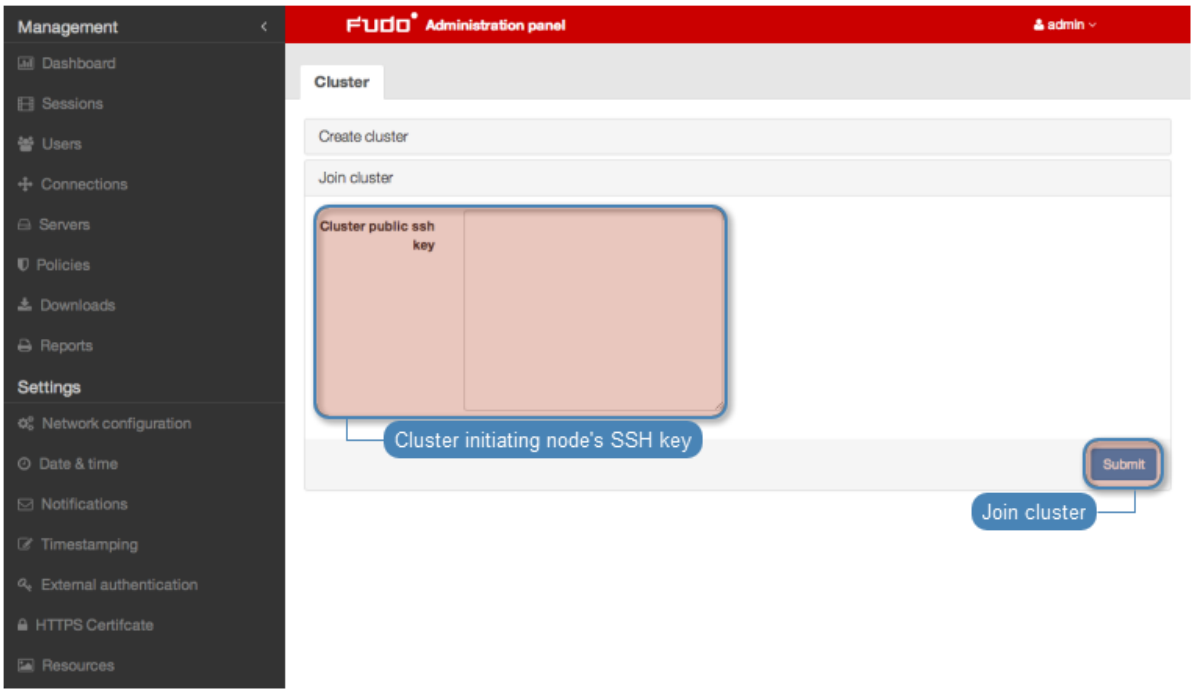
**Note:** Management option has to be enabled on given network interface. Refer to *Network settings: Network interfaces configuration* for details on configuring network interfaces.




6. Click *Submit*, to add node definition.
7. Copy cluster key to clipboard.
8. Log in to administration panel of the joining node.
9. Select *Settings* > *Cluster*.
10. Click *Join cluster*.



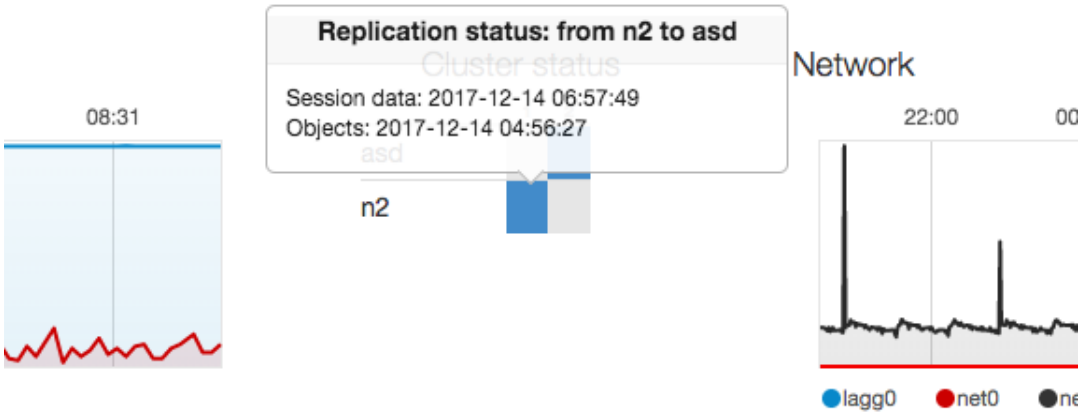

11. Paste cluster public SSH key and click *Submit*.



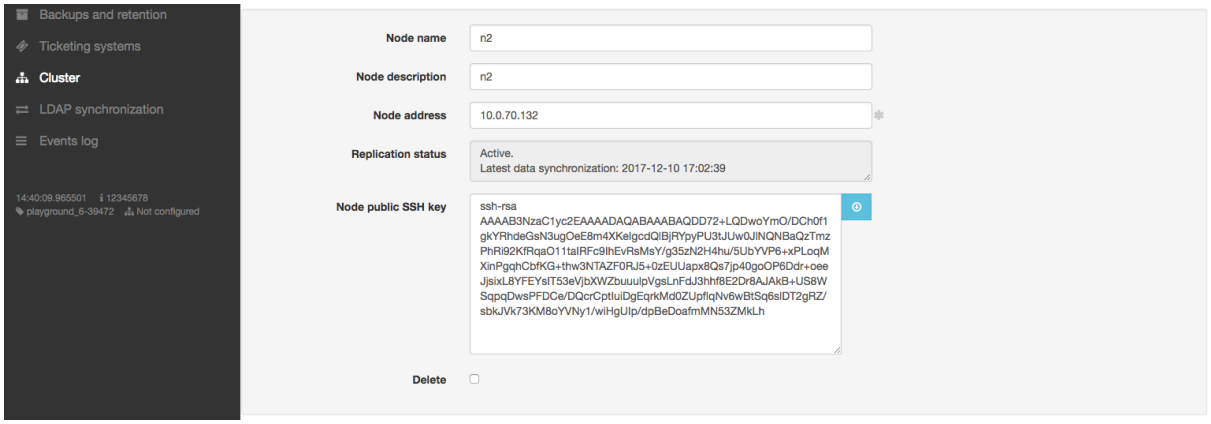

12. Click *I understand the consequences, proceed.*

---

**Note:** Cluster replication status can be reviewed on the dashboard or on the cluster settings view.




- *Session data* - the timestamp of the session data replicated from the given node.
- *Objects* - the timestamp of the replicated data model objects.




**Related topics:**

- *Editing cluster nodes*
- *Deleting cluster nodes*
- *Security: Cluster configuration*

### 15.14.3 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:**

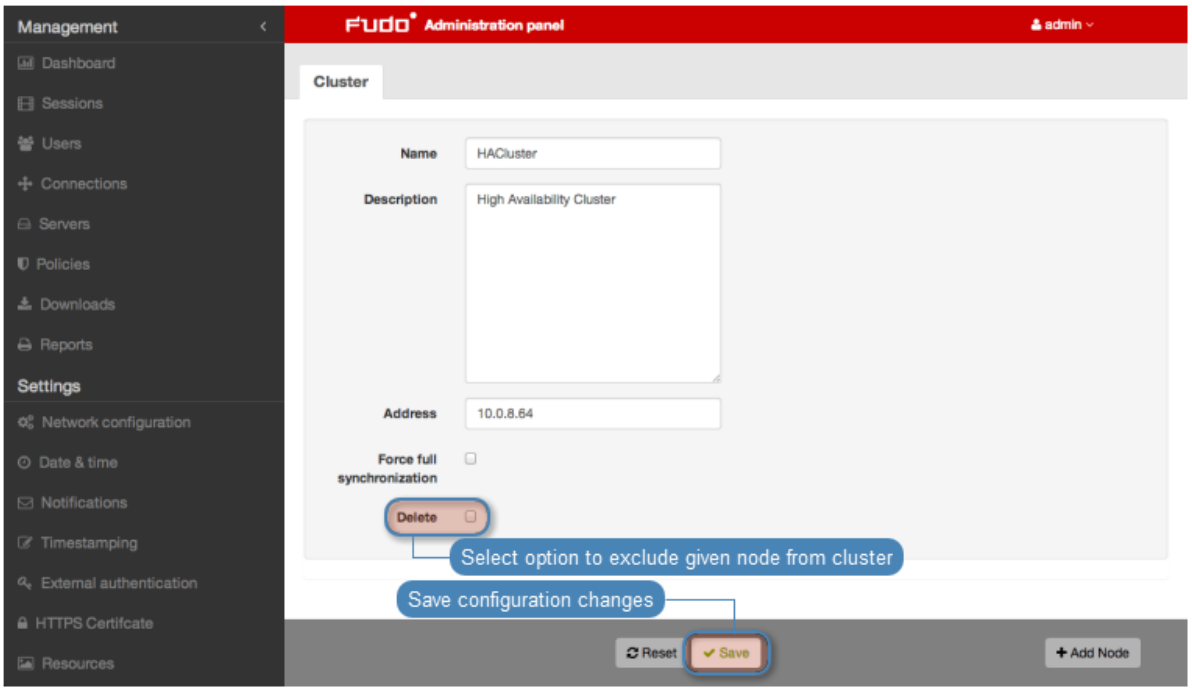
- *Adding cluster nodes*
- *Deleting cluster nodes*
- *Security: Cluster configuration*

### 15.14.4 Deleting cluster nodes

> **Warning:** Removing a node and re-adding it to a cluster may result in data loss.

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*

### 15.14.5 Redundancy groups

Redundancy groups agregate IP addresses assigned to network interfaces enabling implementing static load balancing scenarios while fully preserving high availability features.

---

**Note:** Redundancy groups configuration options are available only after initializing the cluster.

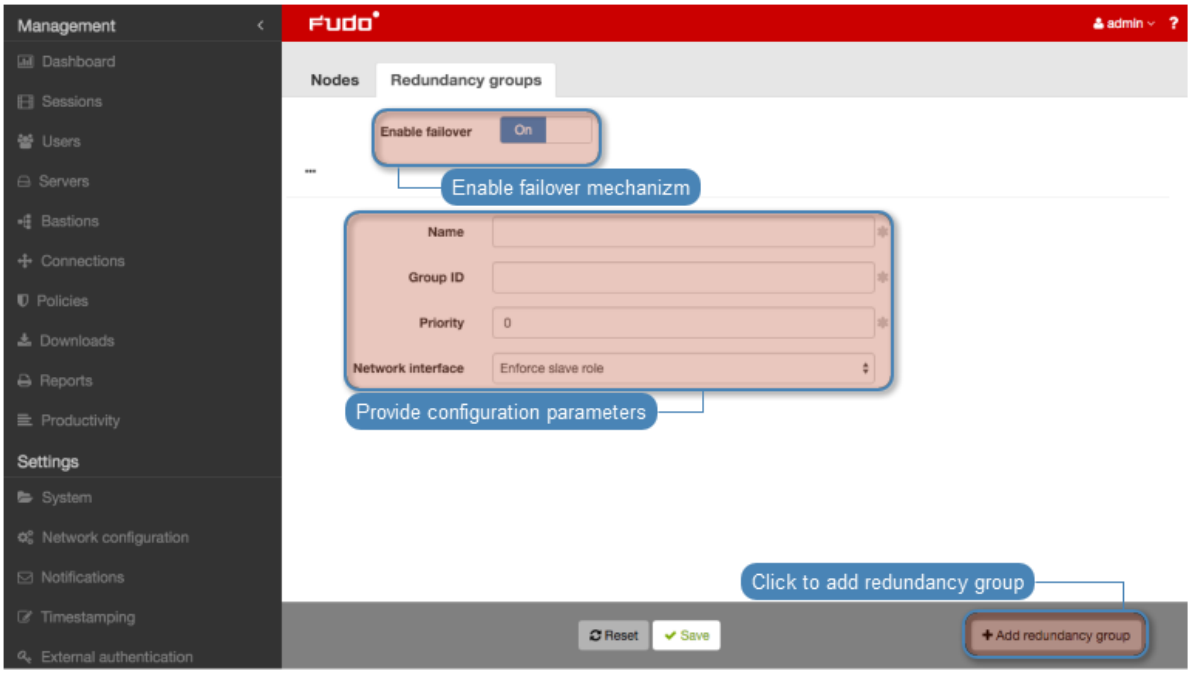
---

#### Adding redundancy groups

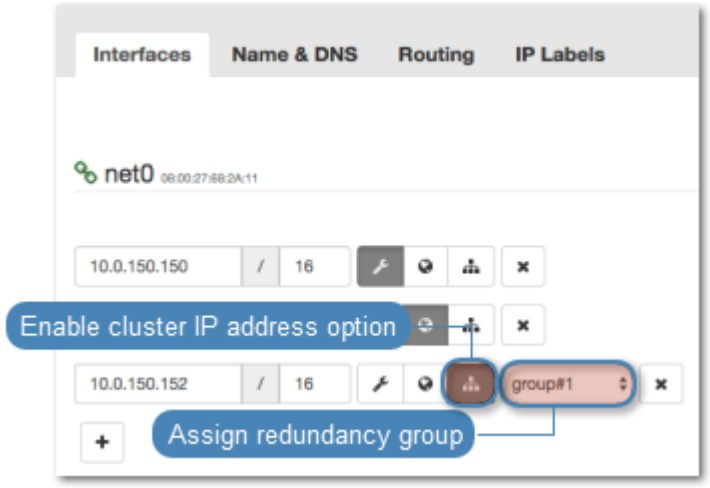
To add a redundancy group, proceed as follows.

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. |
| Interface | Network interface used for communicating with other cluster nodes. |




5. Click *Save*.
6. Select *Settings* > *Network configuration*.
7. Click + to add new IP address.
8. Enter IP address and click the icon to mark the entry as a cluster IP address.
9. Assign previously added redundancy group.
10. Click *Save*.

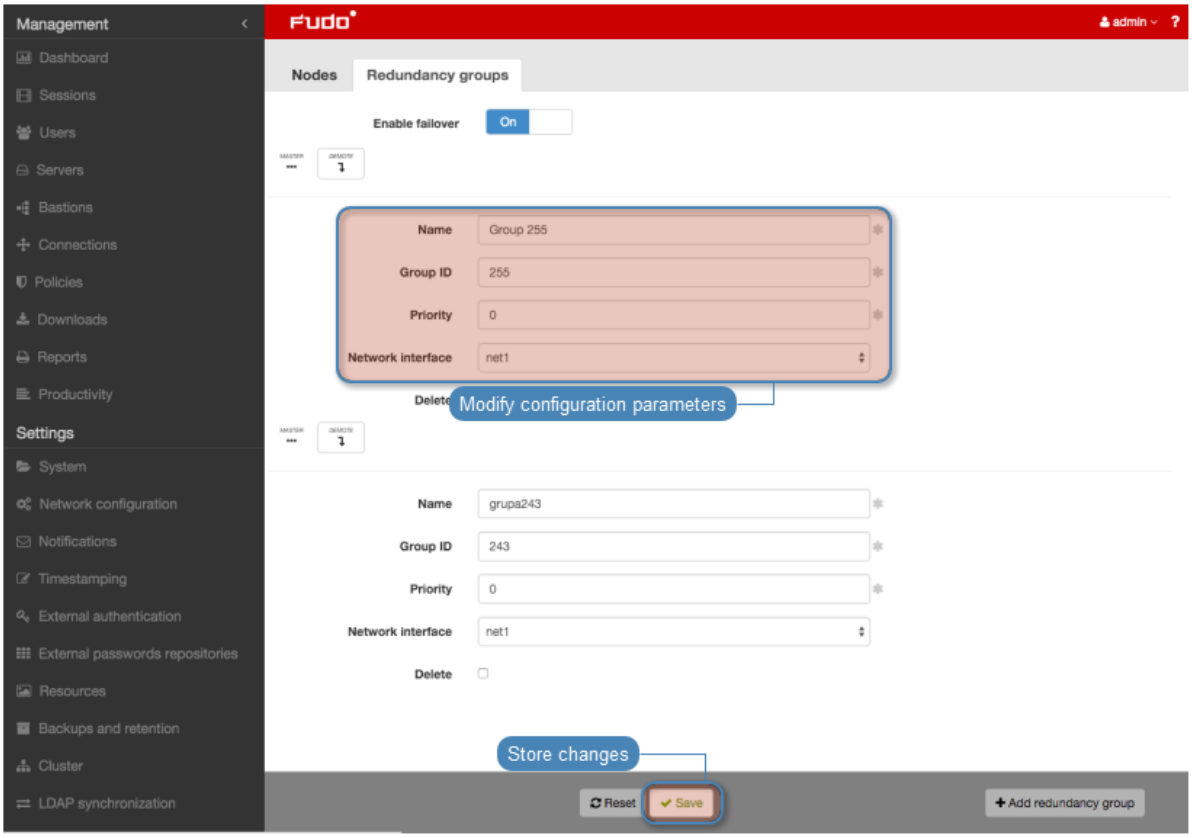



**Note:** Cluster IP address must be defined on every cluster node.

### Editing redundancy groups

To modify a redundancy group, proceed as follows.

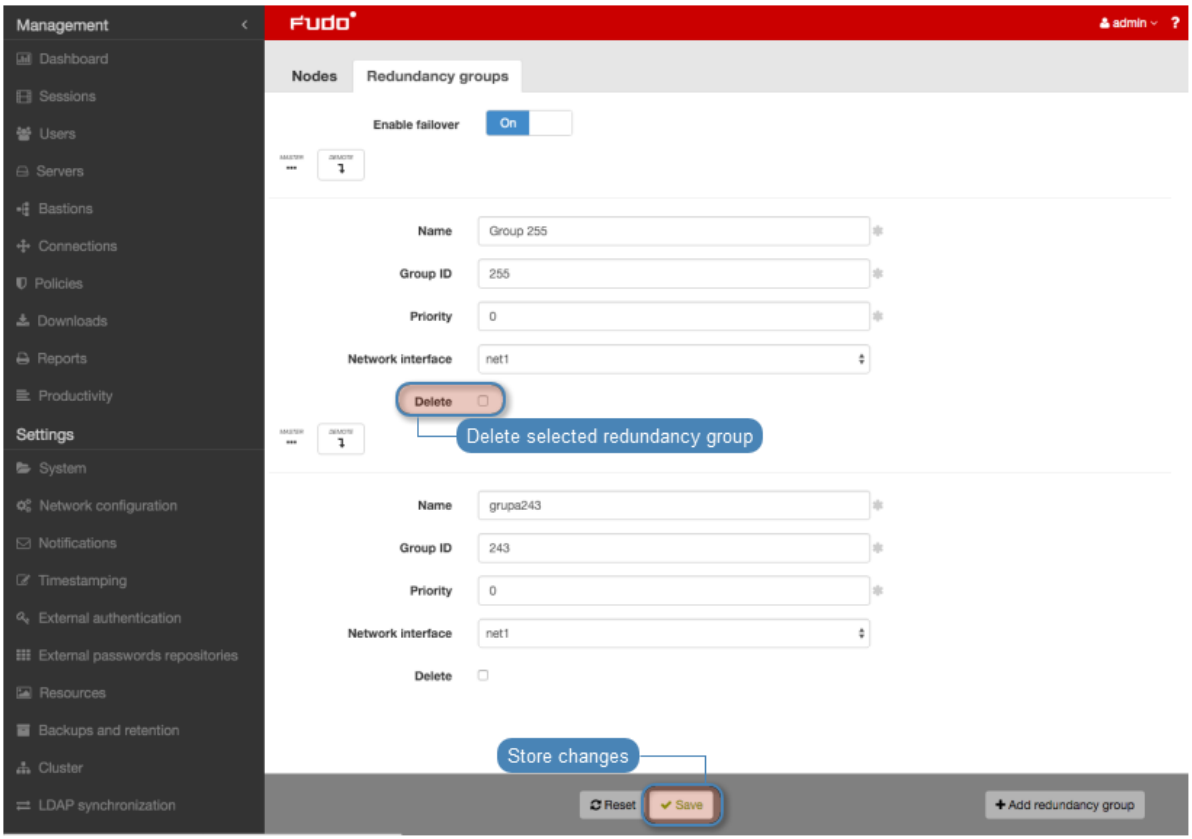
1. Select *Settings* > *Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Find and edit desired redundancy group definition.
4. Click *Save*.



### 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

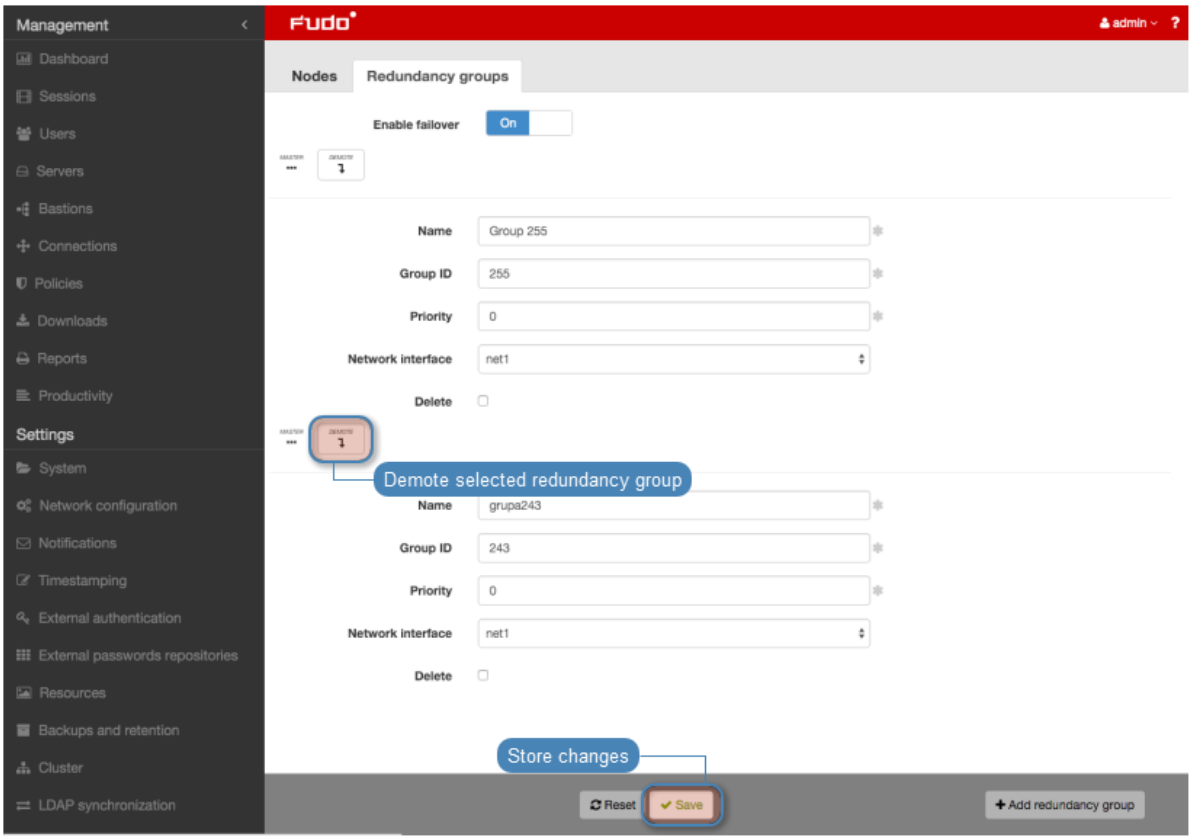
---

**Note:** Demoting redundancy group transfers the master role for given group to another cluster node. The master role is assumed by on 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.

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*.

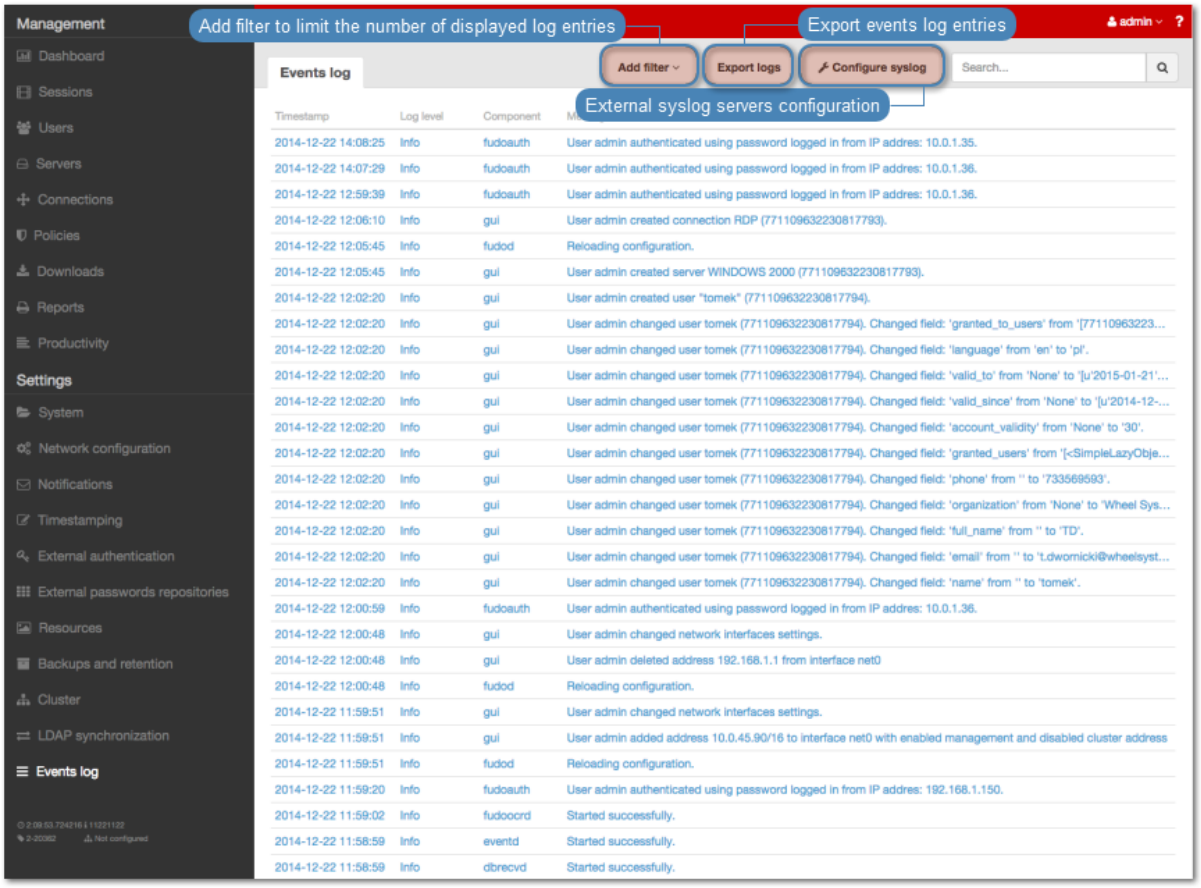
**Related topics:**

- *Security: Cluster configuration*
- *Initiating cluster*
- *Cluster configuration*

## 15.15 Events log

System log is an internal registry of users activities which influence system state (login information, administrative actions, etc.).

To display system log contents, select Settings > System log.




### 15.15.1 External syslog servers

---

**Note:**

- Wheel Fudo PAM communicates with the syslog server over UDP protocol.
- Messages to the syslog server are send through an interface with the option enabled, with an IP address that the target host's network is reachable from or using the default gateway.

---

#### 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. Click *+*.
5. Provide server's IP address and port number.
6. Click *Save*.

---

**Note:**

- Log entries sent to syslog servers are formatted as follows:

```
[<log_level>] (<component_name>) (object_name: object_id) <message>
```

Example:

```
[INFO] (fudordp) (fudo_server: 848388532111147015) (fudo_session:
848388532111147219) (fudo_user: 848388532111147012) (fudo_connection:
848388532111147014) User user0 authenticated using password logged in from IP
addres: 10.0.40.101.
```

- 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*.

### 15.15.2 Exporting events log

To export events log entries, proceed as follows.

1. Select *Settings* > *Events log*.
2. Click *Export logs* and select where to save exported log entries.

**Related topics:**

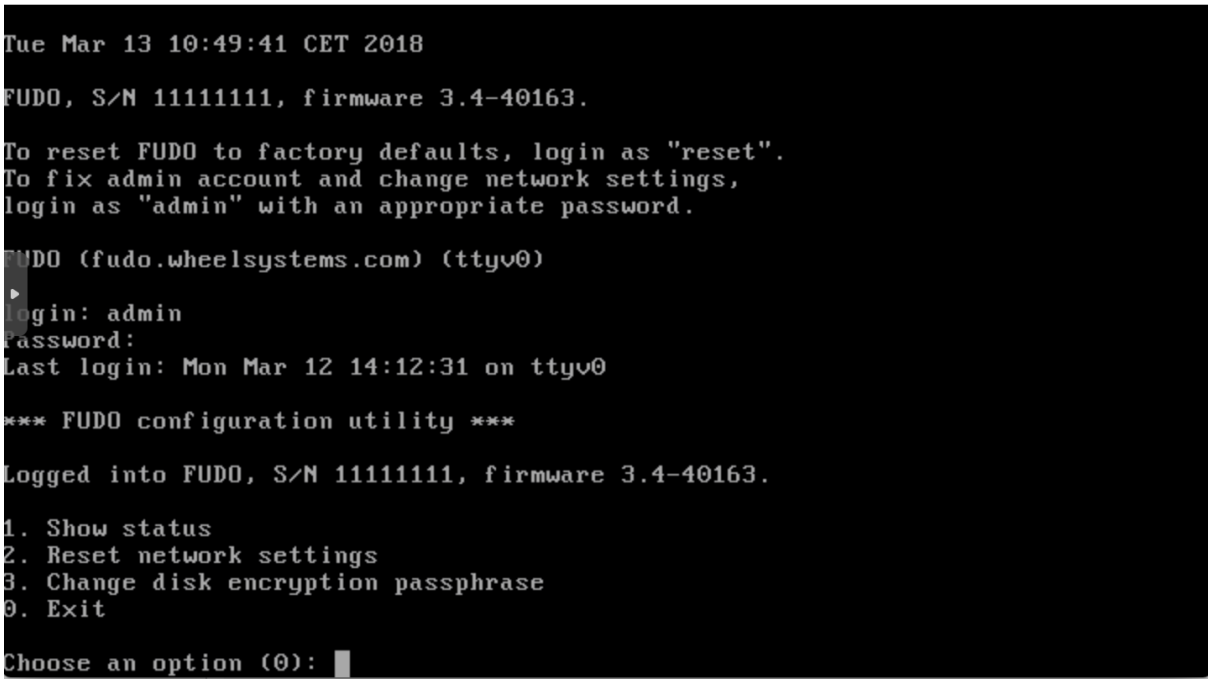
- *Log messages*
- *Security*

- *Managing servers*

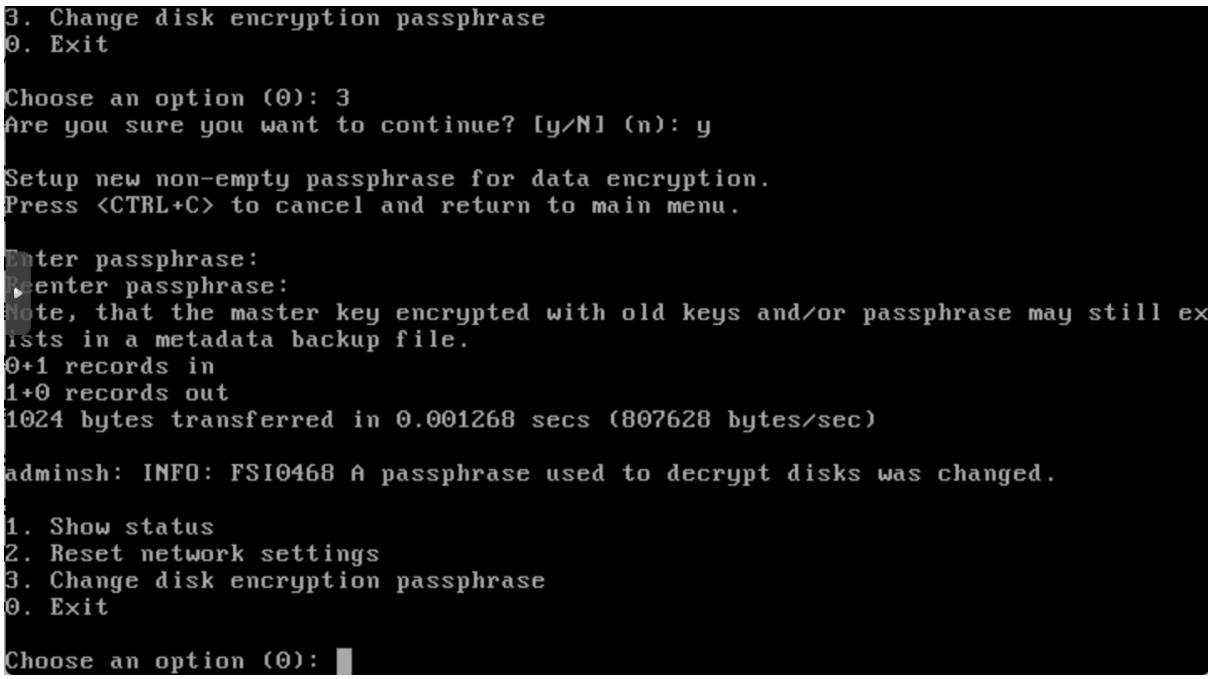
## 15.16 Changing encryption passphrase

In case of Wheel Fudo PAM 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*
- *Backups and retention*

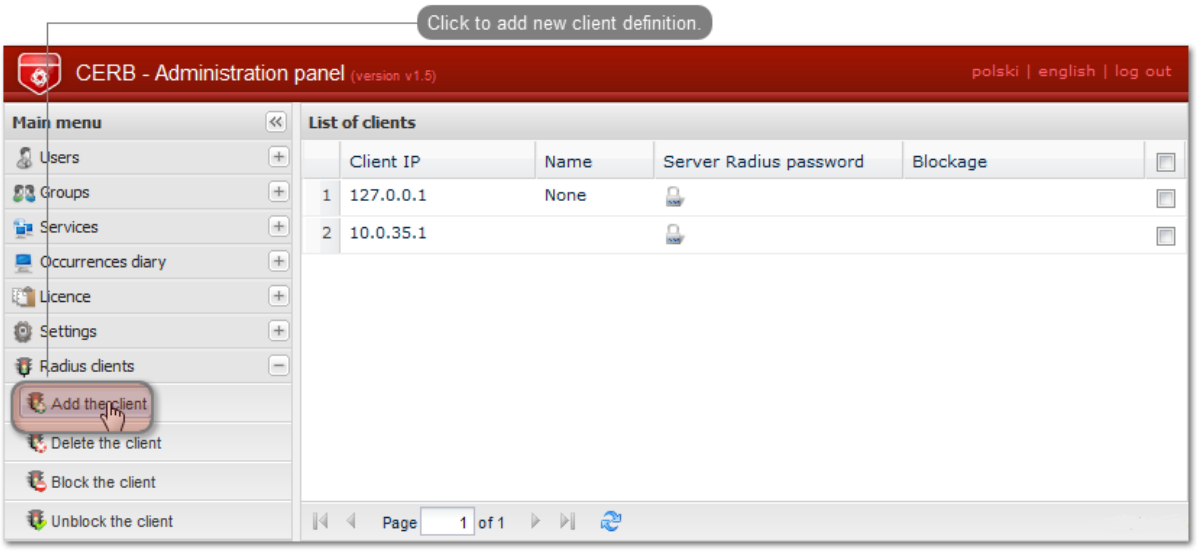
## 15.17 Integration with CERB server

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 Wheel Fudo PAM to verify users credentials using CERB server.

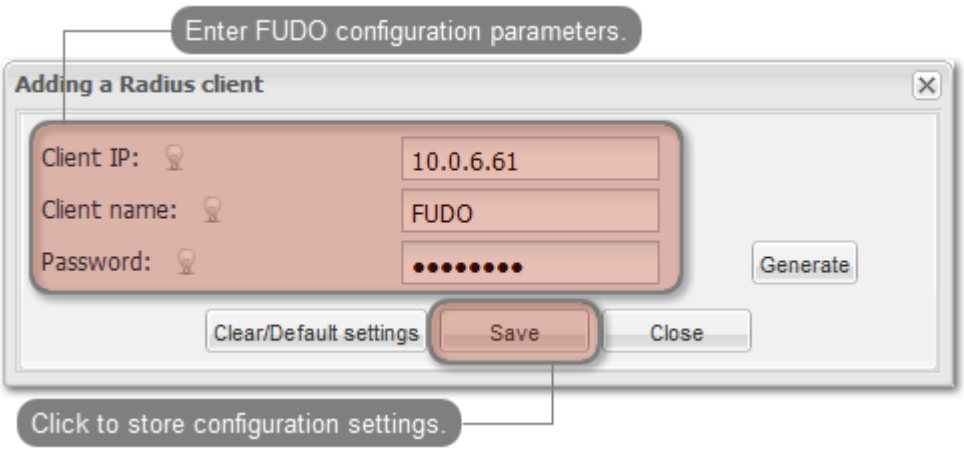
**CERB server configuration**

1. Adding RADIUS client.

- Select *RADIUS clients* > *Add client* to add Wheel Fudo PAM as a RADIUS client.



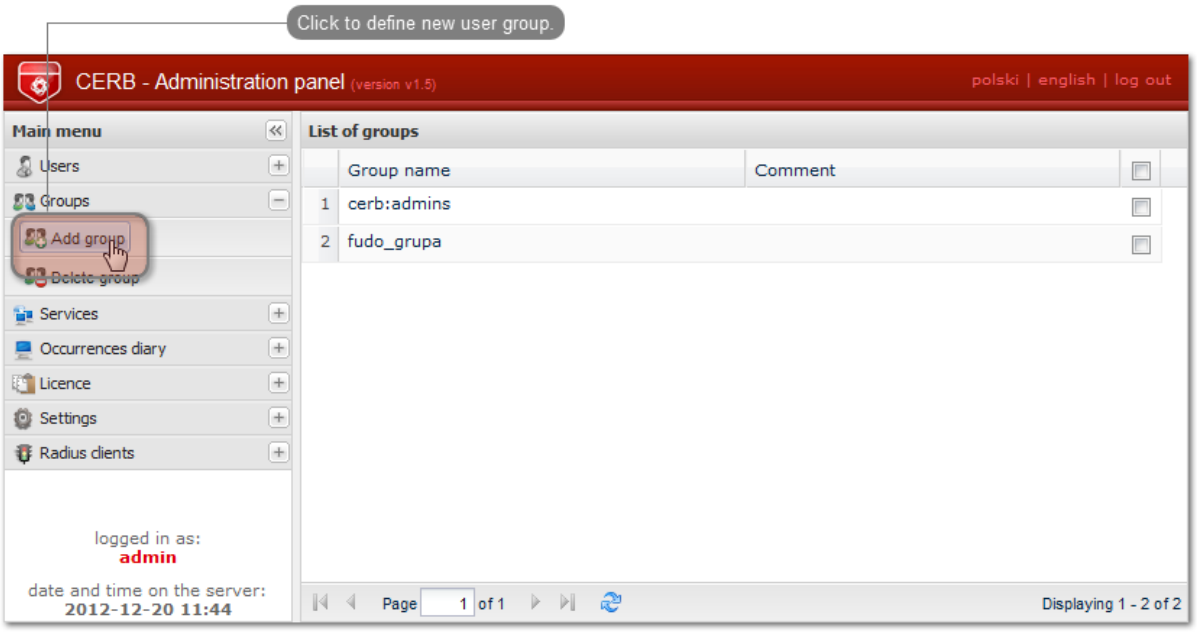

- Provide Wheel Fudo PAM IP address, client's name and password and click *Save*.



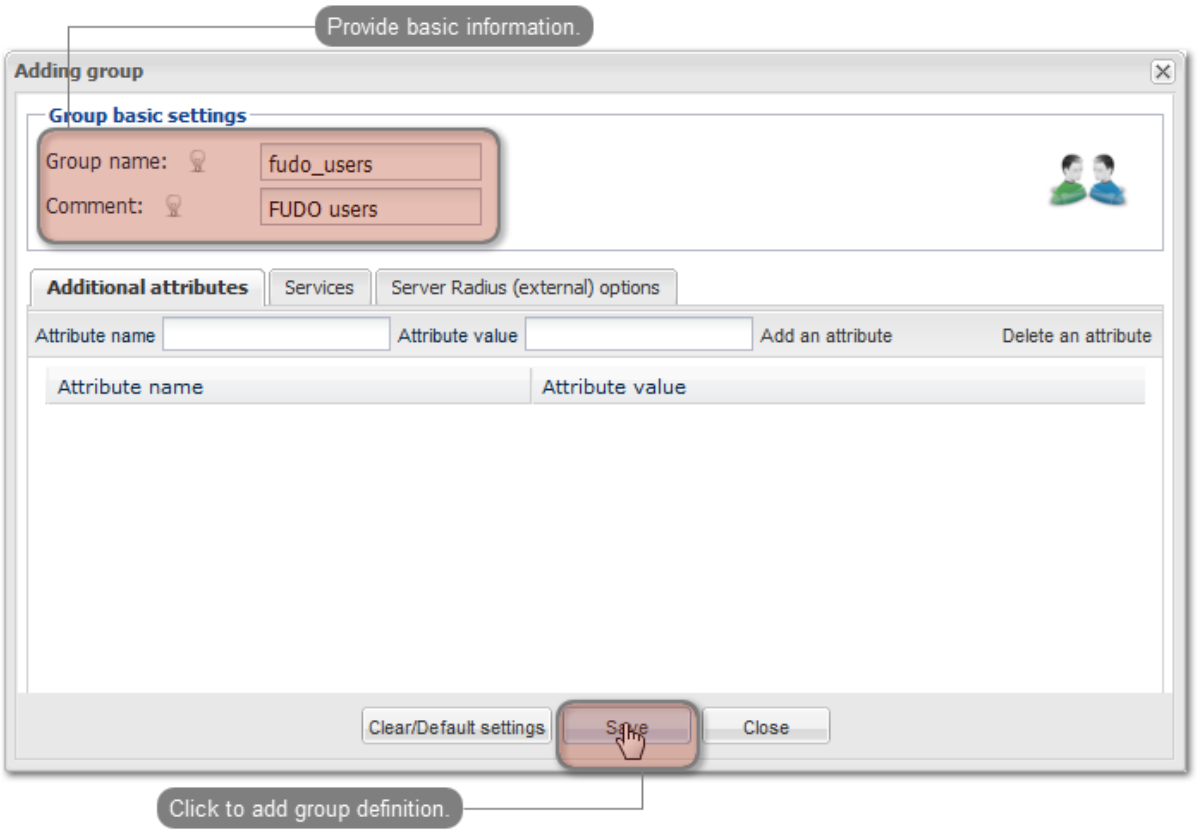

**Note:** Password will be required to define external authorization server in Wheel Fudo PAM administration panel.

2. Adding user group.

- Select *Groups* > *Add group* to define Wheel Fudo PAM users who will be authorized by the CERB server.

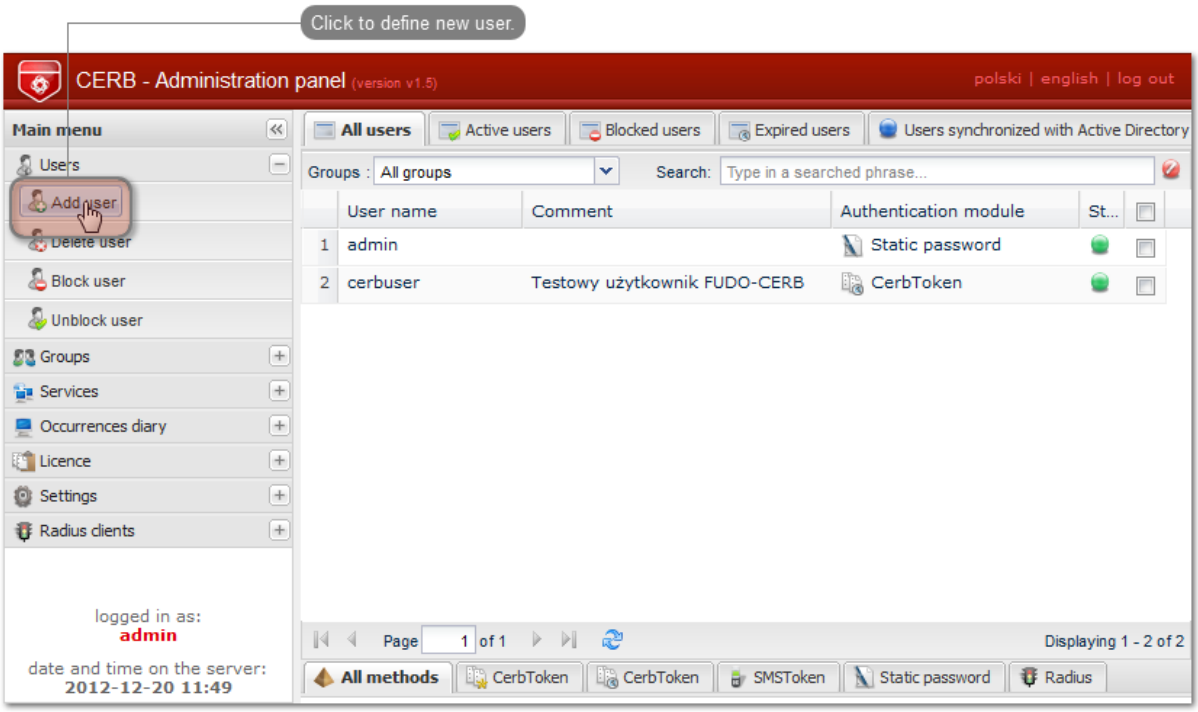



- Enter group's name (`fudo_users`) and click *Save*.

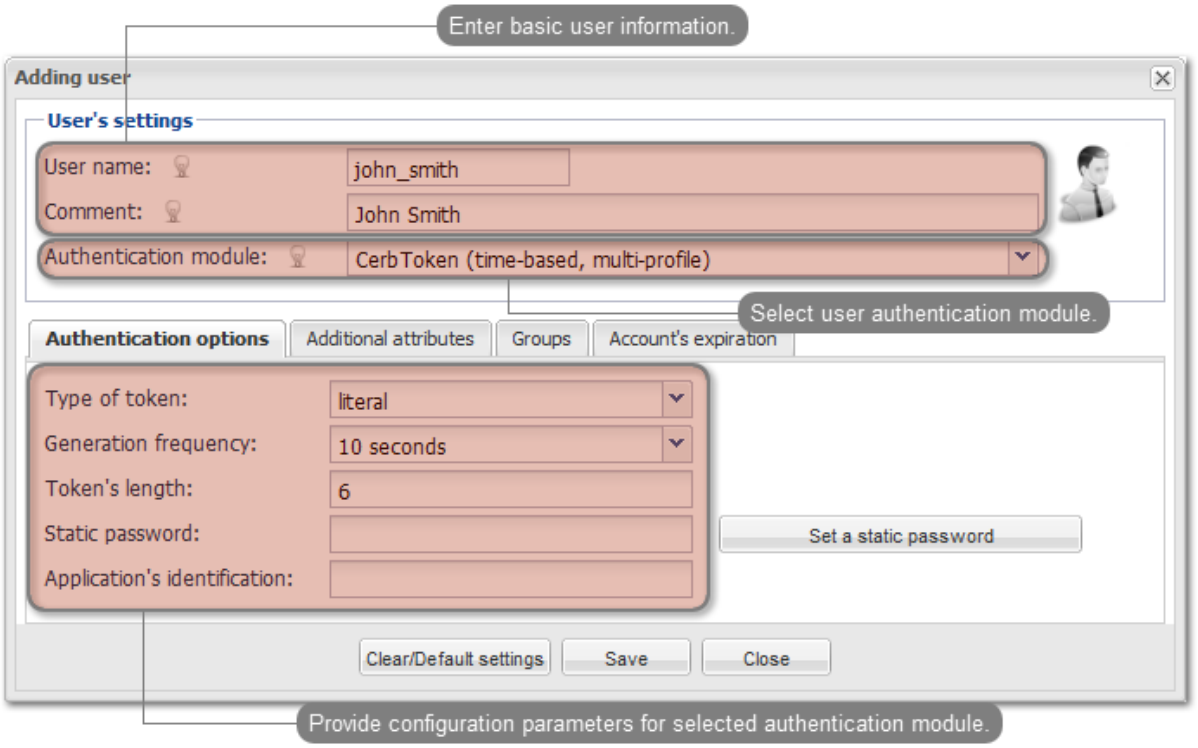



3. Adding user.

- Select *Users* > *Add user* to open new user definition window.

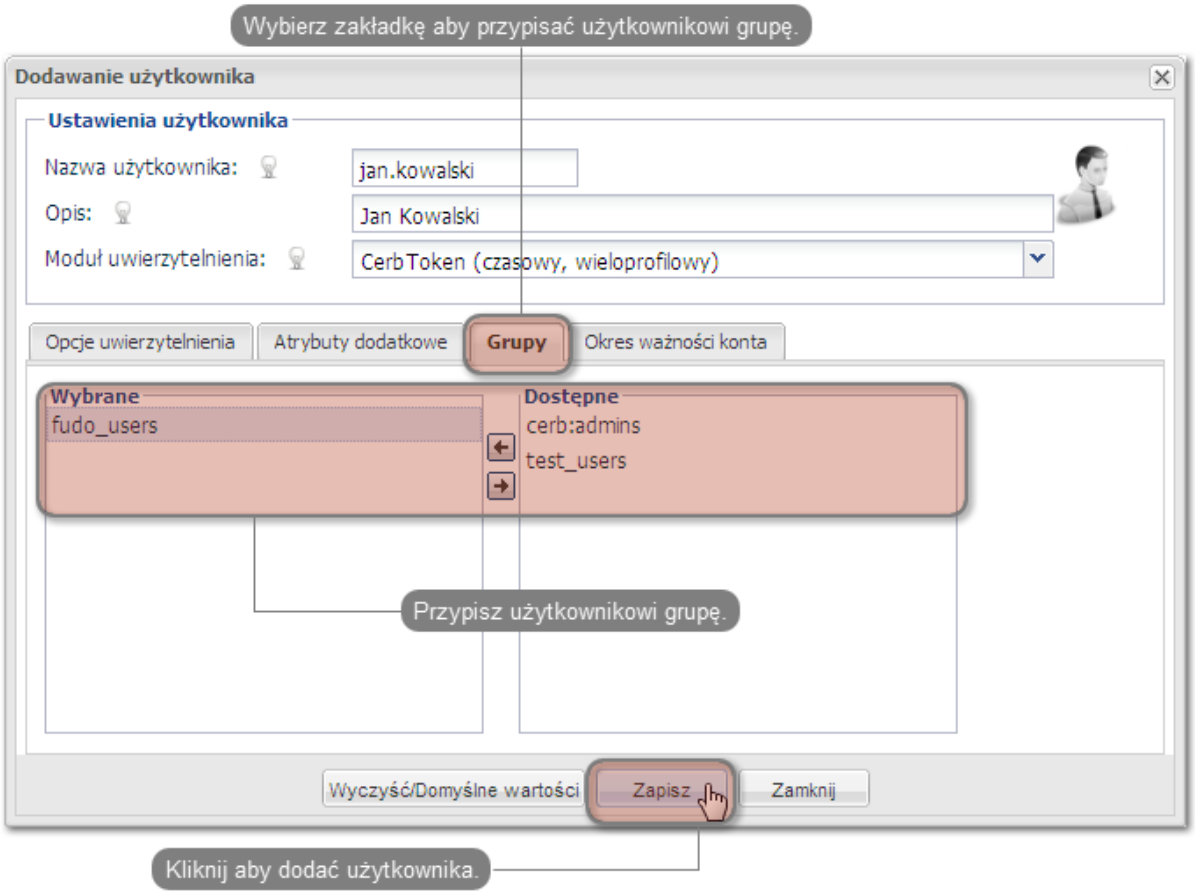



- Provide user name, description and select desired authorization module (refer to CERB server documentation form more information on authorization modules).



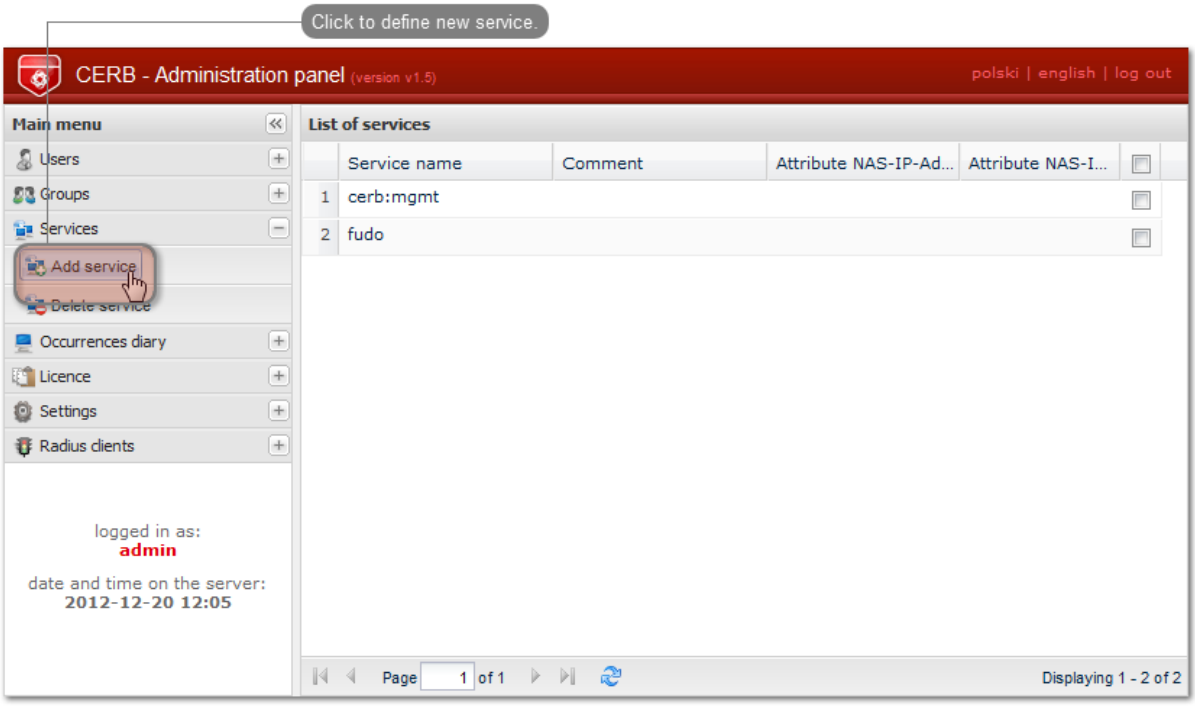

**Note:** Username is used to authenticate users on Wheel Fudo PAM.

- Assign user to previously created `fudo_users` group and click *Save*.



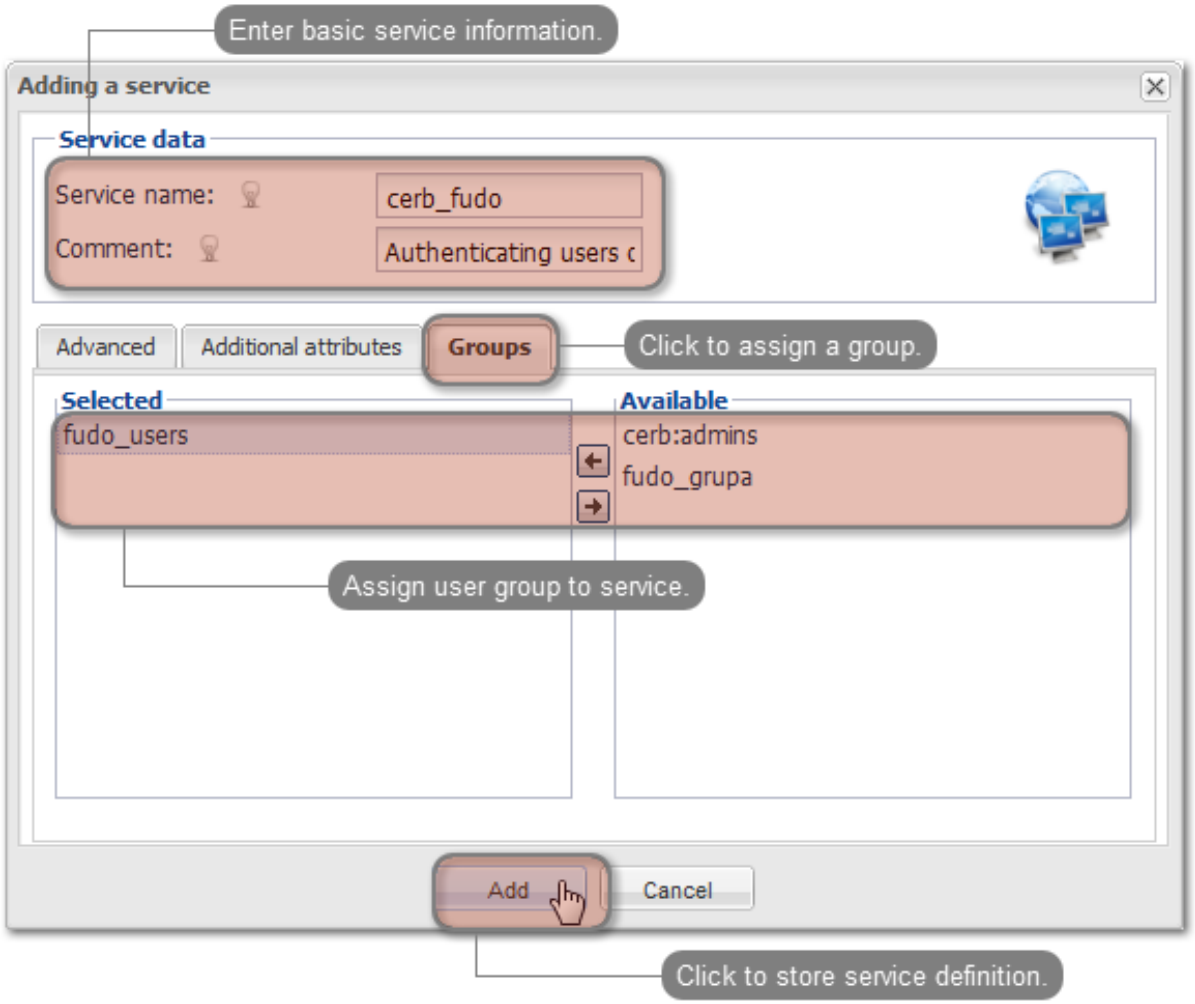

4. Configuring service.

- Select *Services* > *Add service* to open new service definition window.




- Provide name identifying authorization service (`cerb_fudo`) and service description.

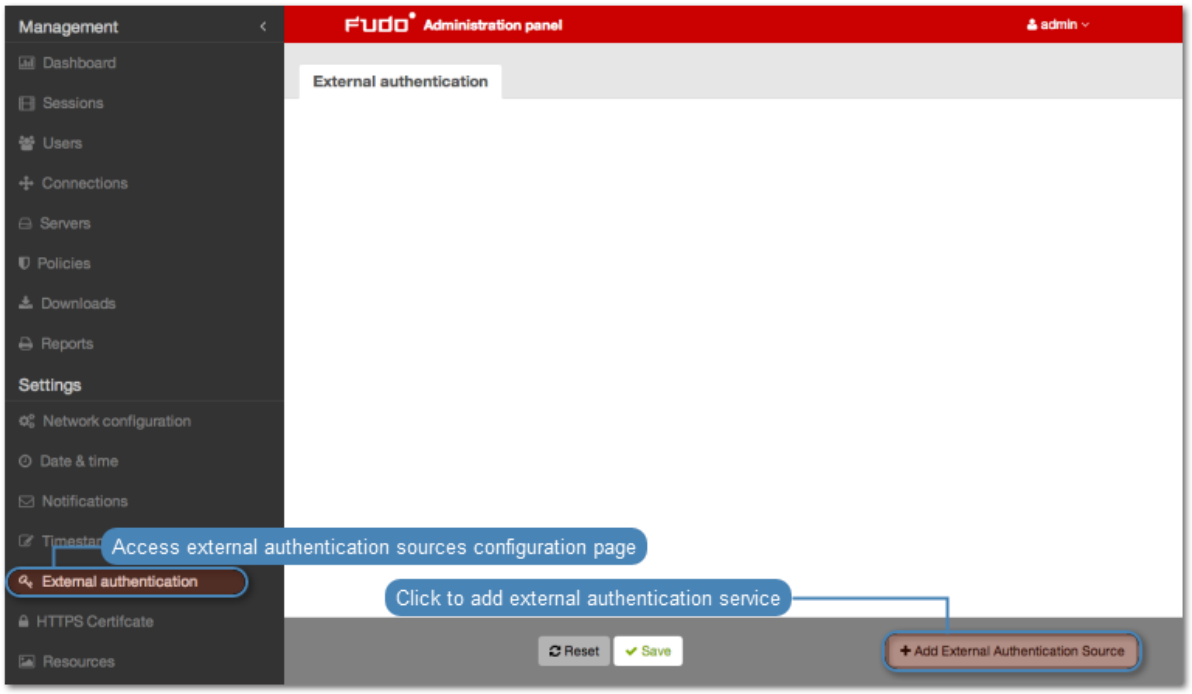
- Add `fudo_users` group to service and click *Add*.




### Wheel Fudo PAM server configuration

1. Adding CERB external authorization server.

- Select *Settings* > *External authentication*.
- Click *Add external authentication source* to add CERB server definition.

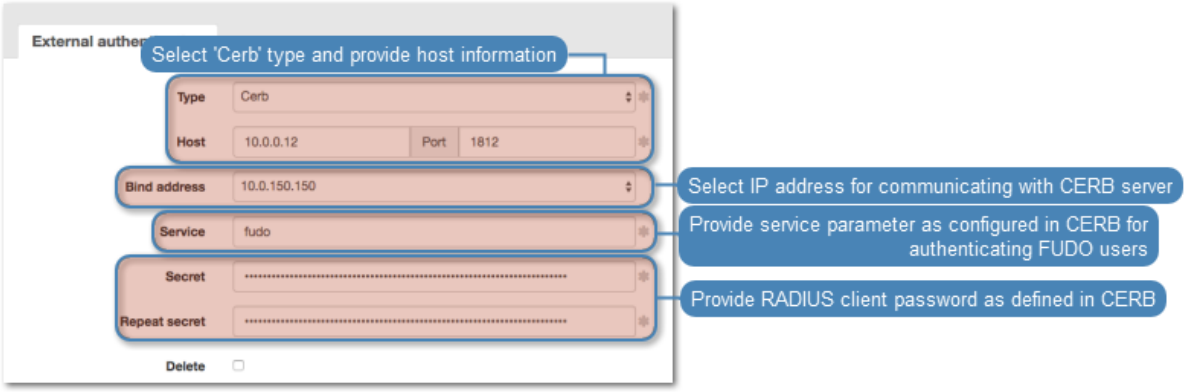



- Provide CERB server IP address, *secret* and service name identifying authorization service.

---

**Note:** Secret must match the RADIUS client password on CERB server. Service name must match the service name on CERB

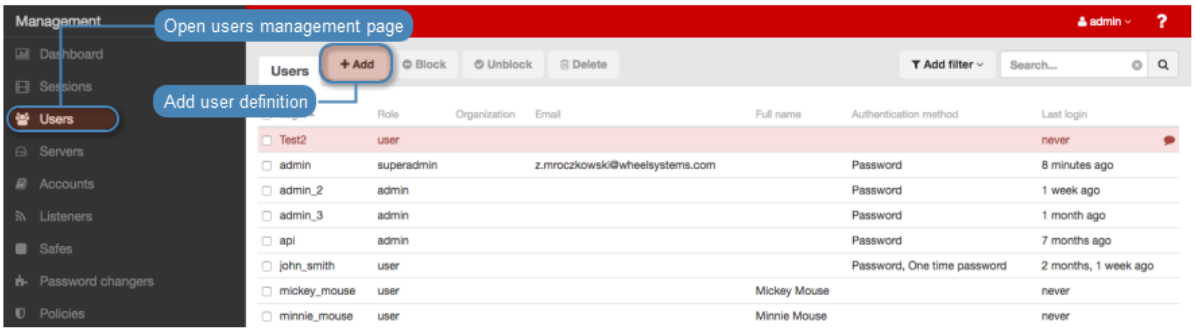
---




- Click *Save*.

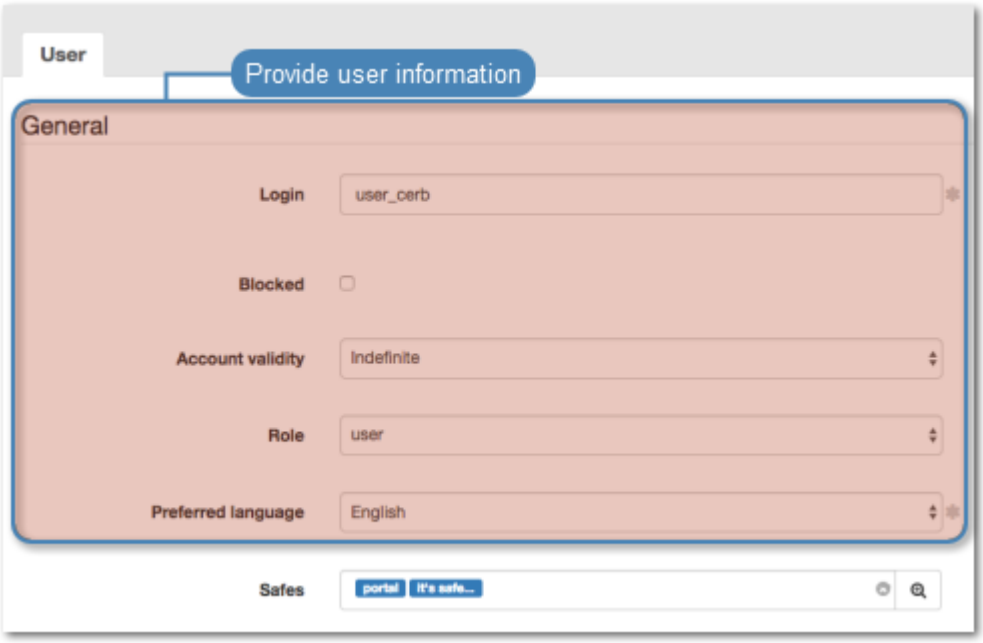
2. Adding user.

- Select *Management* > *Users*.
- Click *Add*.

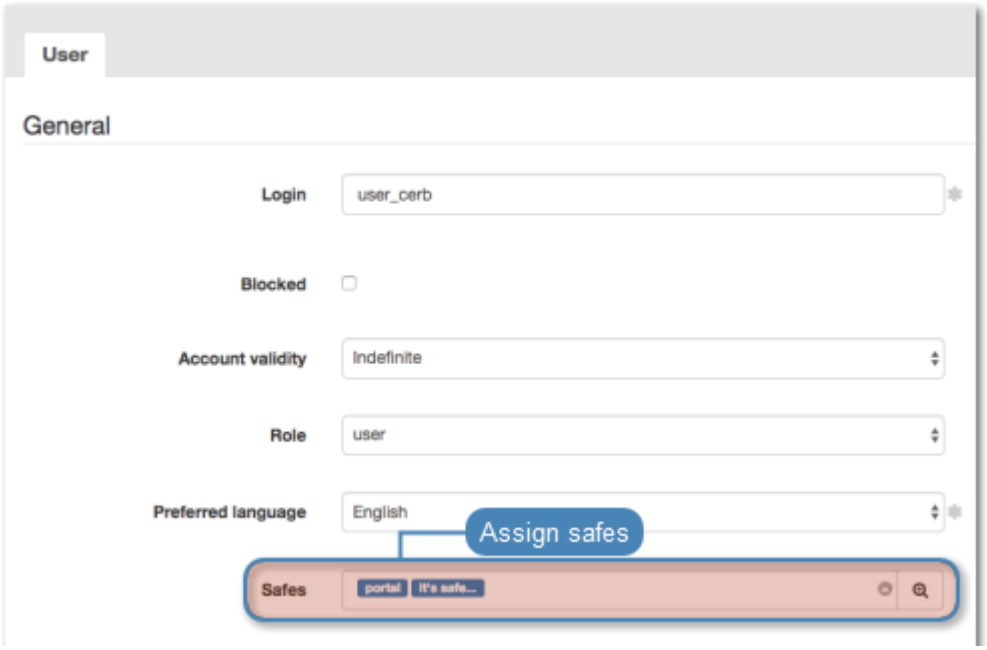



- Provide basic user information.

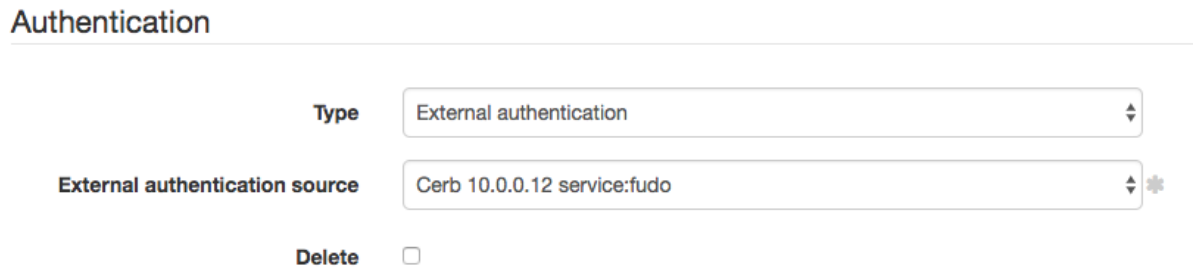
**Note:** Username must match the user name defined on CERB server.




- 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*
- *External authentication*
- *User authentication methods and modes*

## 15.18 System maintenance

The following section contains descriptions of maintenance procedures.

### 15.18.1 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**

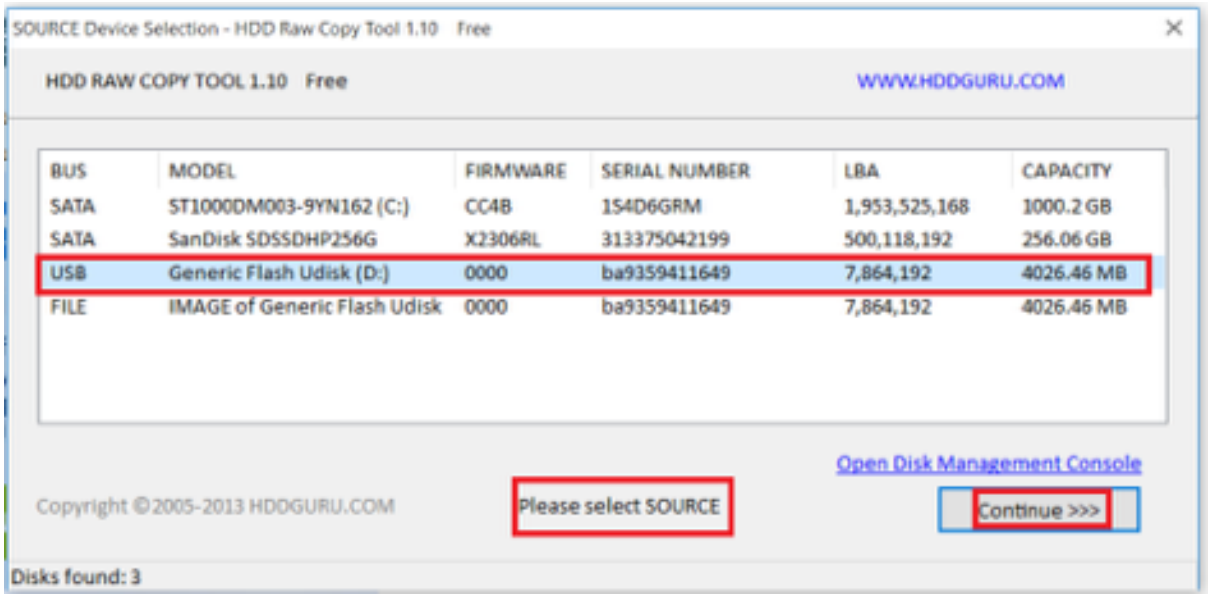
**Warning:** After connecting the flash drive to your computer, do not initiate or format it. Ignore the system message about it not being able to read data and proceed with the backup procedure.

1. Download and install *HDD Raw Copy Tool*.

   `http://hddguru.com/software/HDD-Raw-Copy-Tool/` (portable version is also available)

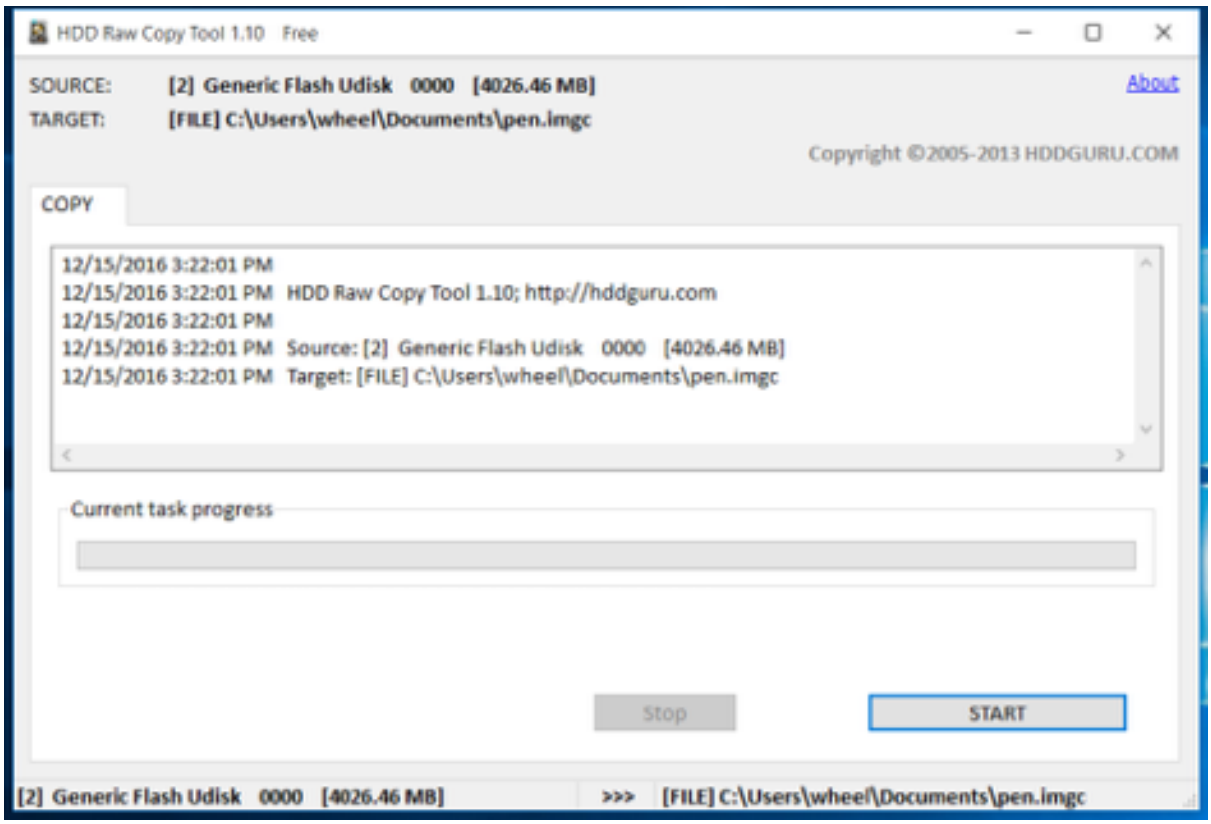
2. Start the program.

3. On the source drive selection window, choose the USB drive with the encription key and click *Continue*.



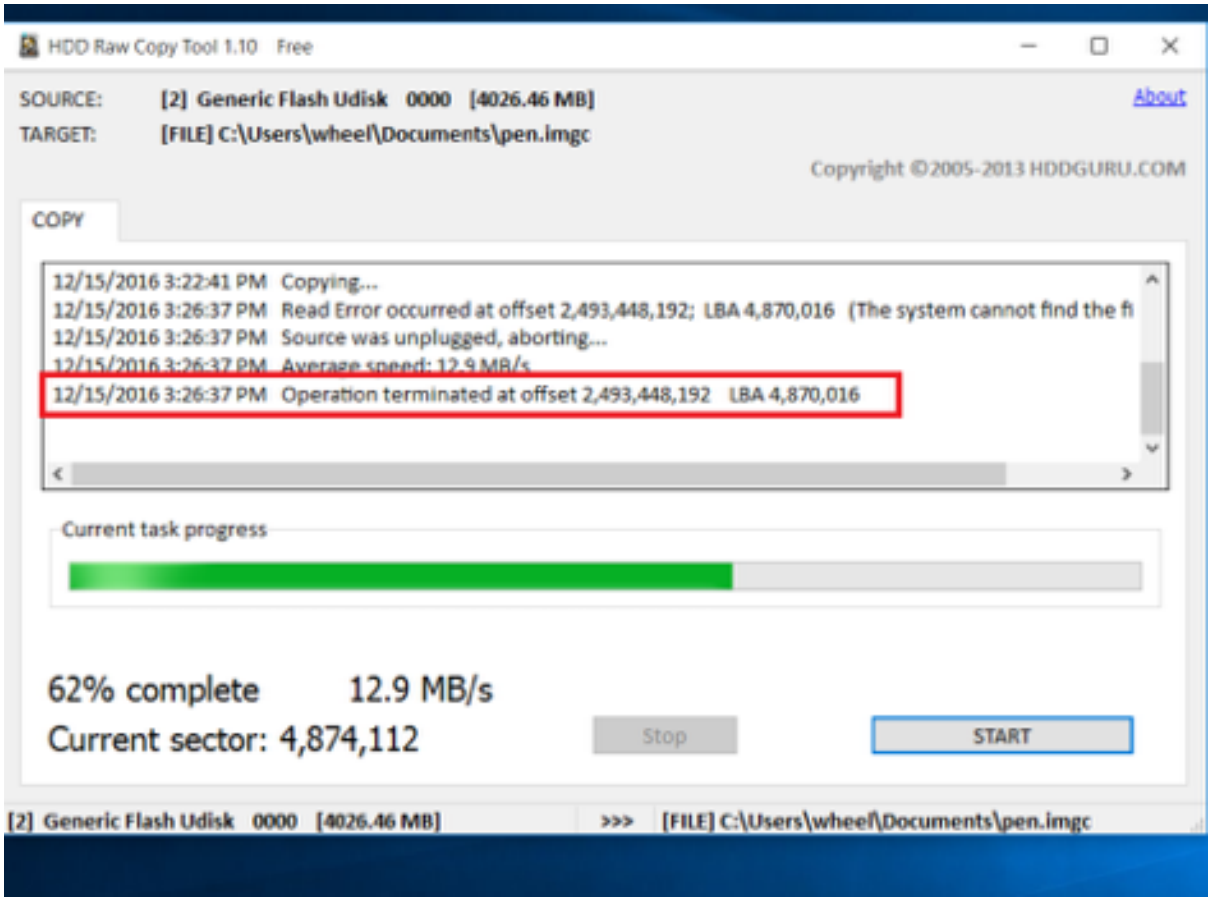

4. Click *FILE* twice, select the target image file and click *Continue*.

5. Click *START* to proceed with copying data.

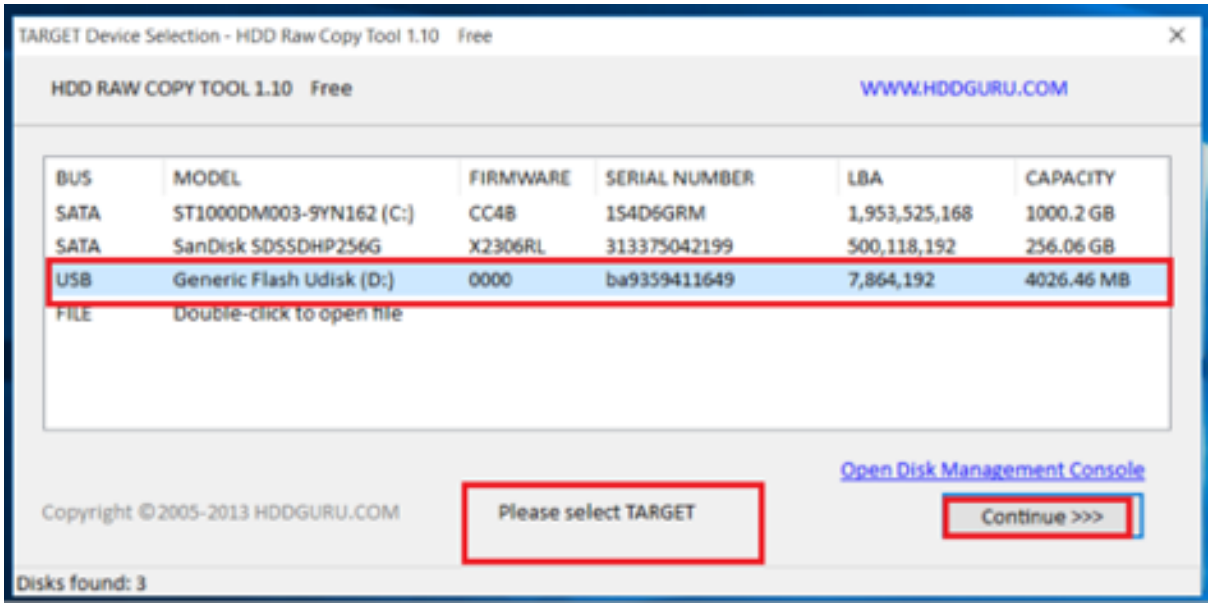



6. Once the following message occurs

   `Operation terminated at offset...` close the application and disconnect the USB drive.



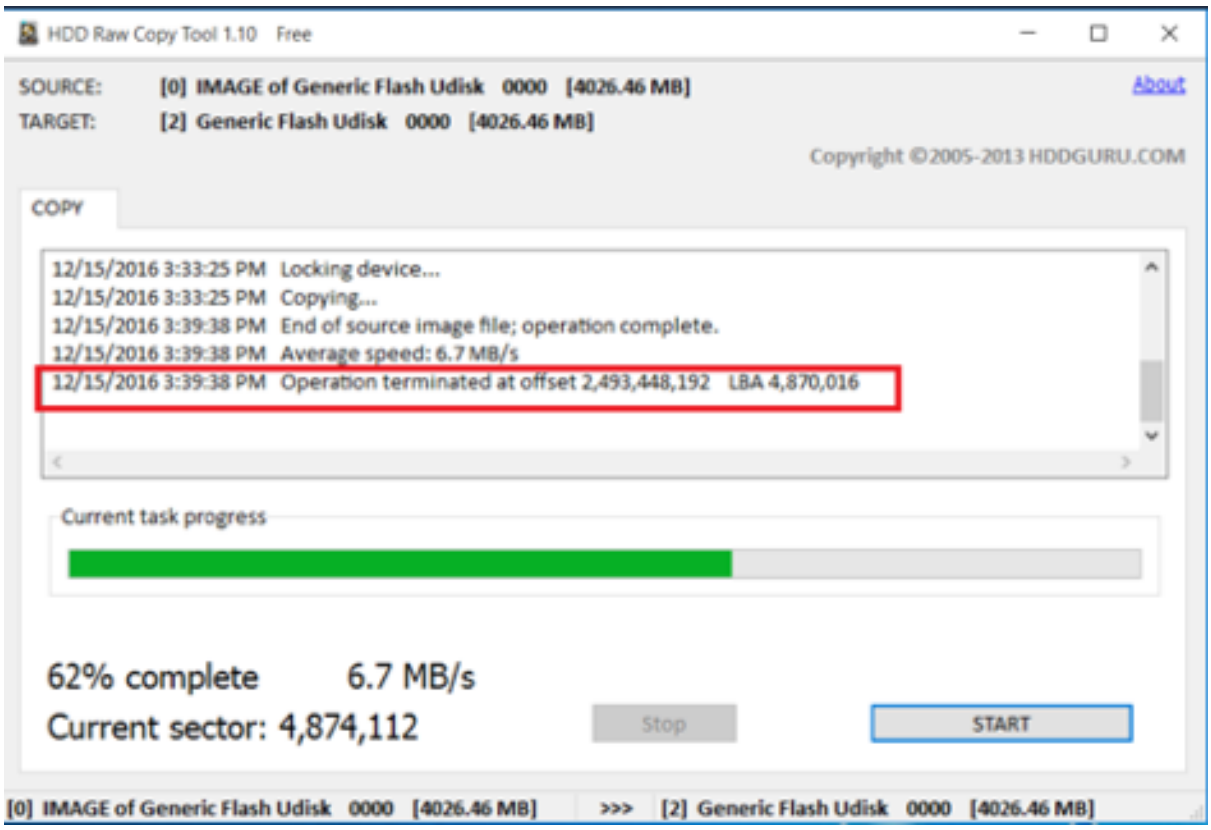

7. Connect another USB drive and start *HDD Raw Copy Tool*.
8. On the source drive selection screen select *FILE* and browse the file system to find the encryption keys image file.
9. Select the newly connected USB flash drive as a target device and click *Continue*.




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*

### 15.18.2 Monitoring system condition

Monitoring system condition allows preventing system failures and overloads, ensuring Wheel Fudo PAM Wheel Fudo PAM remains operational.

**Monitoring active sessions**

1. Login to Wheel Fudo PAM administration panel.
2. Select *Management* > *Dashboard*.
3. Check the number of currently running user sessions.

---

**Note:** Wheel Fudo PAM supports up to 300 RDP connections.

---

**Monitoring network bandwidth**

1. Login to Wheel Fudo PAM administration panel.
2. Select *Management* > *Dashboard*.
3. Check current network transfer rate.

---

**Note:** Wheel Fudo PAM features 1Gbps network interface cards. In case the current network bandwidth usage exceeds 500Mbps, users may notice a decrease in system communication performance.

---

**Related topics:**

- *System log*
- *Frequently asked questions*

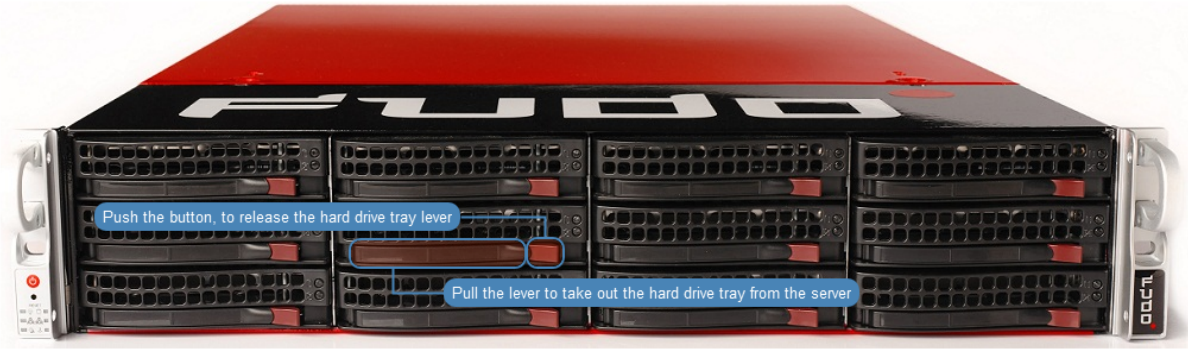
### 15.18.3 Hard drive replacement

In default configuration, Wheel Fudo PAM'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:** Wheel Fudo PAM 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.

---

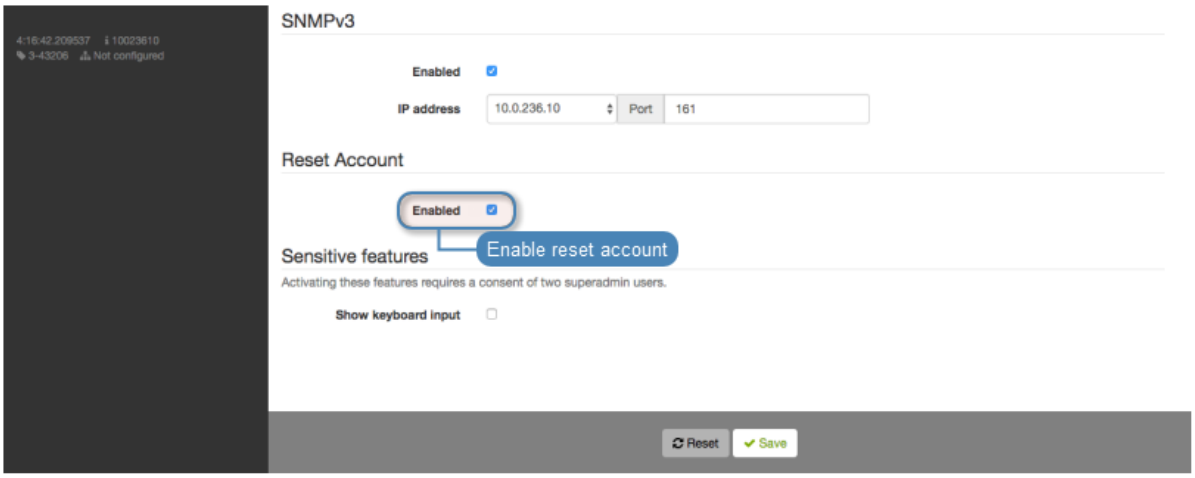
**Related topics:**

- *Hardware overview*
- *Frequently asked questions*

### 15.18.4 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.

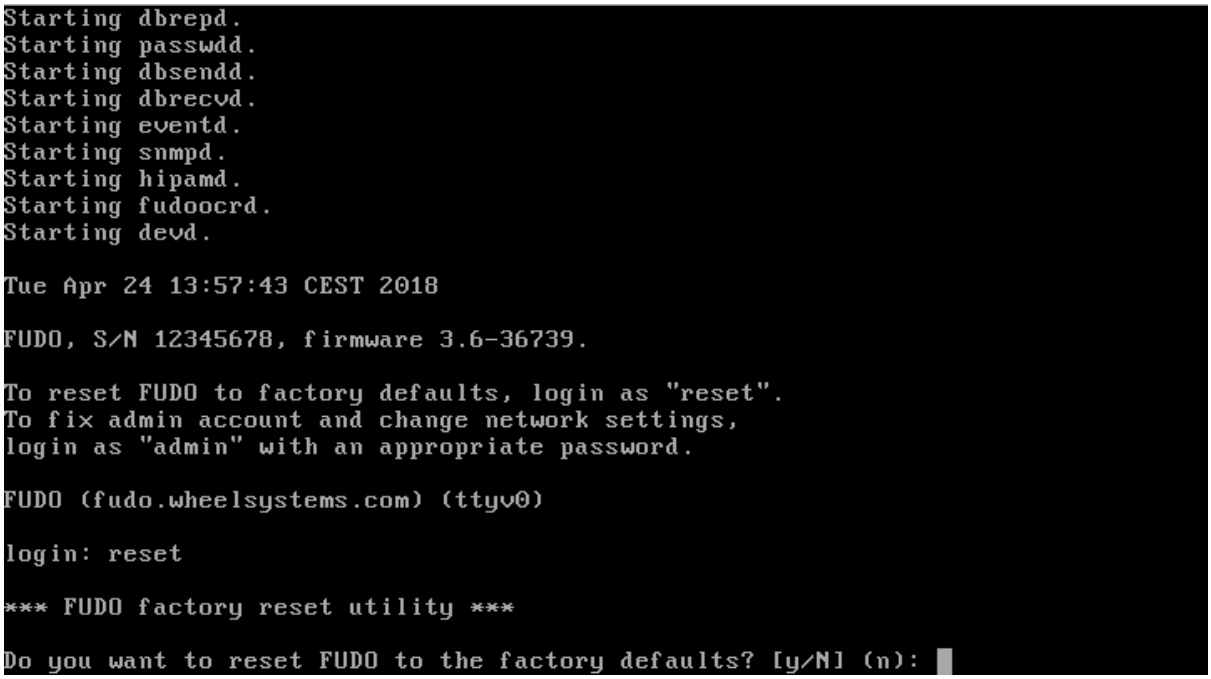
1. Log in to Fudo administration panel.
2. Select *Settings* > *System*.
3. Select *Enabled* in the *Reset account* section.



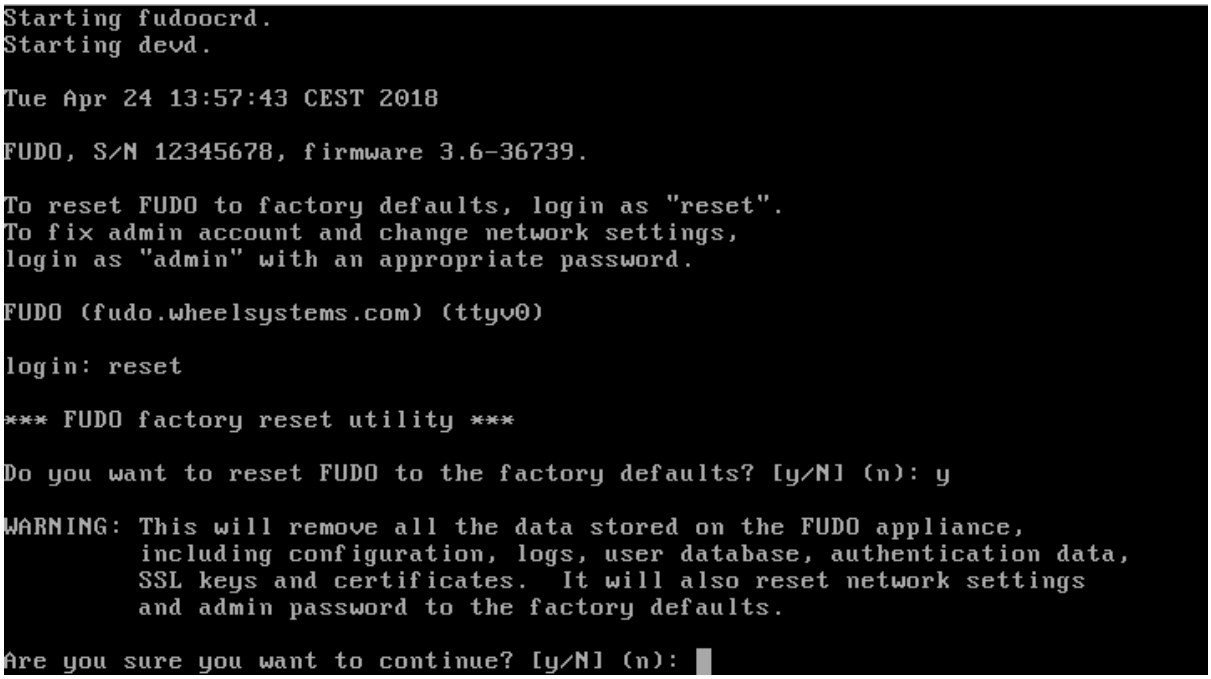

4. On terminal login screen, enter `reset` as login.

```
Starting fcgiportal.
Starting nginx.
Starting nginxportal.
Starting cron.
Starting dbrepd.
Starting passwdd.
Starting dbsendd.
Starting dbrecvd.
Starting eventd.
Starting snmpd.
Starting hipamd.
Starting fudoocrd.
Starting devd.

Tue Apr 24 13:57:43 CEST 2018

FUDO, S/N 12345678, firmware 3.6-36739.

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: reset
```

5. Enter `y` and press `Enter` to confirm.




6. Enter `y` and confirm by pressing `Enter`.




**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*

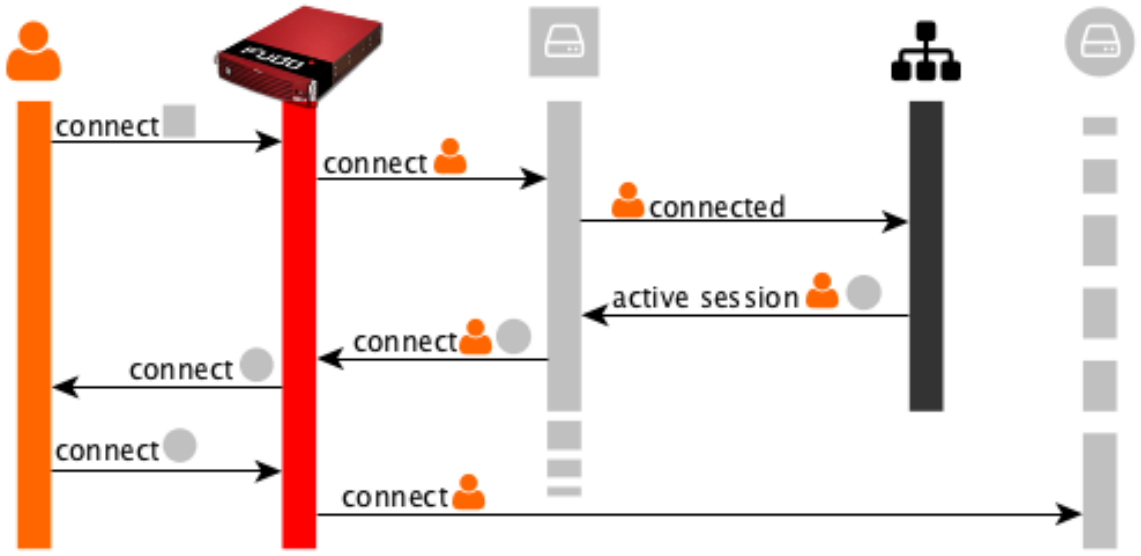
ROZDZIAŁ 16

Reference information

## 16.1 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.



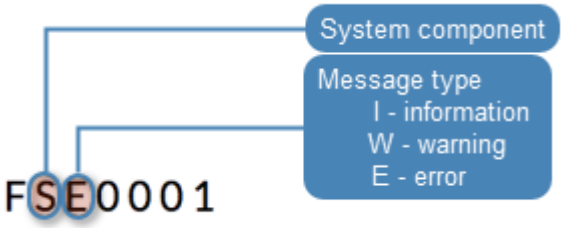

**Note:** To successfuly redirect a connection, the server identified by the broker must be defined on Wheel Fudo PAM, it must listen on default RDP port (3389) and user must be allowed to connect to given server.

**Related topics:**

- *Data model*
- *RDP*
- *Servers*
- *Accounts*

## 16.2 Log messages

**Note:** Message code contains information on the type of the log message and the component that logged the information.




| Message code | Message and description |
|---|---|
| FSE0001 | Internal system error. |
| FSE0002 | Fudo certificate error. |
| FSE0003 | Unable to change configuration settings. |
| FSE0004 | Configuration import error. |
| FSE0005 | Unable to initialize ${disk}. |
| FSE0006 | Invalid license. |
| FSE0007 | Unable to find license file. |
| FSE0008 | Unable to attach hard drive ${disk}. |
| FSE0009 | Upgrade failed. |
| FSE0010 | License expired. |
| FSW0011 | Retention module was unable to delete session ${sessid} from database. |
| FSW0012 | Retention module error, session ${sessid} skipped. |
| FSI0013 | Session ${sessid} removed according to retention policy. |
| FSW0014 | Retention module was unable to remove session ${sessid}. |
| FSI0015 | Redundancy group ${name} switched to master role. |
| FSW0016 | Unable to send email, SMTP server not configured. |
| FSI0017 | Redundancy group ${name} switched to slave role. |
| FSI0018 | Hard drive ${disk} initialization started. |
| FSI0019 | Hard drive ${disk} initialization completed. Data synchronization may take a moment. |
| FSE0020 | System backup error. |
| FSI0021 | Hard drive ${disk} attached. |
| FSI0022 | Unsupported hard drive hot-swap. |
| FSI0023 | Manual encryption does not support hard drive hot-swap. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FSE0024 | Hard drive belongs to another Fudo (${diskserial}) ${disk}. |
| FSI0025 | Cluster node ${name} (${address}) host key set to ${hostkey}. |
| FSE0026 | Cluster communication error. |
| FSI0027 | Cluster node ${name} initialized. |
| FSE0028 | Unable to join node to cluster. |
| FSI0029 | Resumed data synchronization. |
| FSI0030 | Node ${node} initially synchronized. |
| FSE0031 | Timestamping service communication error. |
| FSE0032 | Unable to timestamp session. |
| FSE0033 | Unknown timestamping service provider. |
| FSI0034 | Session ${SESSION} was timestamped. |
| FSI0035 | Email ${mailname} sent to ${admin_email}. |
| FSW0036 | Unable to send email ${mailname} to ${admin_email} through ${account} server. |
| FSW0037 | Output from SMTP client: ${out}. |
| FSI0038 | Saved email ${mailname} sent to ${admin_email}. |
| FSI0039 | System image version ${FULLNEW} uploaded successfully. |
| FSE0040 | Communication error with cluster node %s (%s): Fudo version mismatch (local: %s, remote: %s). |
| FSI0041 | Initial connection from master cluster node. |
| FSI0042 | Cluster node %s (%s) connected from address %s. |
| FSI0043 | Connection from another cluster node. |
| FSI0044 | Connected to cluster node %s (%s) on address %s. |
| FSI0045 | Initial database replication to cluster node %s (%s) completed. |
| FSE0046 | There is no filter called %s. |
| FSW0047 | Error sending notification. |
| FSE0048 | Error authenticating user over RADIUS. |
| FUI0049 | User %s authenticated using password logged in from IP address: %s. |
| FUI0050 | User %s authenticated using password. |
| FUI0051 | User %s authenticated through %s (Host: %s, Port: %d, %s: %s) logged in from IP address: %s. |
| FUI0052 | User %s authenticated through %s (Host: %s, Port: %d, %s: %s). |
| FUI0053 | User %s authenticated through LDAP (Host: %s, Port: %d) logged in from IP address: %s. |
| FUI0054 | User %s authenticated through LDAP (Host: %s, Port: %d). |
| FUI0055 | User %s (domain %s) authenticated through Active Directory (Host: %s, Port: %d) logged in from IP address: %s. |
| FUI0056 | User %s (domain %s) authenticated through Active Directory (Host: %s, Port: %d). |
| FUE0057 | Authentication method 'password', required by MySQL, requested by the user %s, logging in from IP address %s, was not found. |
| FUE0058 | Authentication method 'password', required by MySQL, requested by the user %s, was not found. |
| FUW0059 | User %s, logging in from IP address %s, has more than one 'password' method, using the first password. |
| FUW0060 | User %s has more than one 'password' method, using the first password. |
| FSE0061 | Incorrect password repository configuration: login is empty. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FSE0062 | Incorrect password repository configuration: password is empty. |
| FSE0063 | Incorrect server configuration: ERPM namespace is empty. |
| FSE0064 | Incorrect server configuration: ERPM name is empty. |
| FSE0065 | License configuration error. |
| FSE0066 | Unable to block user %jd. |
| FSE0067 | Error connecting to Lieberman ERPM server %s: incorrect URL in configuration. |
| FSE0068 | Error connecting to Lieberman ERPM server %s: incorrect protocol specified. |
| FSE0069 | Error fetching password from Lieberman ERPM server %s: unable to get sessid for user %s. |
| FSE0070 | Error fetching password from Lieberman ERPM server %s: unable to get password for user %s for the %s/%s server. |
| FSI0070 | Established proxy connection from %s to %s (%s:%u). |
| FSI0071 | Established gateway connection from %s to %s (%s:%u). |
| FSI0072 | Established transparent connection from %s to %s (%s:%u). |
| FSI0073 | Bastion connection from %s to %s (%s:%u). |
| FSW0074 | Connection terminated because license has expired or was not set. |
| FSW0075 | Connection terminated because number of nodes in cluster exceeded license limit. |
| FSE0076 | Unable to establish connection, could not find specified transparent server (tcp://%s:%u). |
| FSE0077 | LDAP authentication error. |
| FSE0078 | LDAP authentication error: unable to connect from %s to %s. |
| FUE0079 | Authentication timeout after %ju key attempt%s and %ju password attempt%s. |
| FUE0080 | Authentication timeout after %lu key attempt%s. |
| FUE0081 | Authentication timeout after %lu password attempt%s. |
| FSE0082 | Unable to establish connection to server %s (%s). |
| FSE0083 | Unable to establish connection from %s to server %s (%s). |
| FSI0084 | Terminating session: %s. |
| FSI0085 | Session finished. |
| FUI0086 | User %s blocked due to connection policy violation. |
| FUW0087 | Session has been terminated due to user %s account expiration. |
| FUW0088 | Session has been terminated due to exceeding the time window defined in the connection %s time policy. |
| FUE0089 | Authentication timeout. |
| FSE0090 | Unable to connect to the passwords repository server %s. |
| FSE0091 | Unable to add server %s. |
| FSE0092 | Passwords repository server %s communication error. |
| FSE0093 | Error connecting to Thycotic server %s: incorrect URL in configuration. |
| FSE0094 | Error connecting to Thycotic server %s: incorrect protocol specified. |
| FSE0095 | Error fetching password from Thycotic server %s: unable to get sessid for user %s. |
| FSE0096 | Error fetching password from Thycotic server %s. |
| FSE0097 | Error fetching password from Thycotic server %s: unable to get secretid for server %s. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FSE0098 | Error fetching password from Thycotic server %s: unable to get password for user %s for the %s server. |
| FUE0099 | Connection terminated. |
| FUI0100 | HTTP connection beetwen client and server initiated. |
| FUE0101 | Unable to find matching HTTP connection. |
| FUI0102 | Session terminated by system administrator. |
| FUE0103 | HTTP connection error. |
| FUI0104 | %s connection terminated. |
| FUI0105 | HTTP session inactive, terminating. |
| FUE0106 | Authentication failed: %s. |
| FUW0107 | Invalid inactivity timeout, falling back to %d seconds. |
| FUE0108 | MySQL connection error. |
| FUI0109 | MySQL connection terminated. |
| FUE0110 | Oracle connection error. |
| FUI0111 | Oracle connection terminated. |
| FUE0112 | RDP connection error. |
| FUE0113 | TLS Security configured, but missing TLS private key. |
| FUE0114 | TLS Security configured, but missing TLS certificate. |
| FUE0115 | Standard RDP Security configured, but missing private key. |
| FUE0116 | TLS certificate verification failed. |
| FUE0117 | RSA key verification failed. |
| FUI0118 | Successfully authenticated against the server. |
| FUI0119 | Successfully authenticated against the server as user %s using %s. |
| FUI0120 | Successfully authenticated against the server as user %s within domain %s using %s. |
| FUI0121 | An anonymous user successfully authenticated against the server. |
| FUI0122 | An anonymous user successfully authenticated against the server as user %s. |
| FUI0123 | An anonymous user successfully authenticated against the server as user %s within domain %s. |
| FUE0124 | SSH connection error. |
| FUE0125 | User %s failed to authenticate after %d attempts, disconnecting. |
| FUI0126 | Successfully authenticated against the server as user %s using password. |
| FUE0127 | Invalid authentication method: expected passwordor sshkey, got %s. |
| FUI0128 | User %s authenticated using SSH key. |
| FUE0129 | Failed to authenticate against the server as user %s using %s. |
| FUE0130 | Failed to authenticate against the server as user %s using %s (received %s). |
| FUW0131 | Functionality %s is not allowed. |
| FUE0132 | Client requested incorrect terminal dimensions (%dx%d). |
| FUE0133 | MSSQL connection error. |
| FUE0134 | TN3270 connection error. |
| FUE0135 | Unknown TN3270 command: %02x. |
| FUW0136 | Functionality %s not allowed. |
| FUE0136 | Telnet connection error. |
| FSE0137 | Unable to read private key. |
| FSE0138 | Server's certificate does not match configured certificate. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FUE0139 | VNC connection error. |
| FUE0140 | Client version: %s is higher than the client integrated in Fudo: %s. |
| FUE0141 | VNC connection error. Client answered with unsupported security type: %hhu. |
| FUE0142 | VNC connection error. Server version: %s is lower than client version: %s. |
| FUI0143 | VNC connection closed: %s. |
| FUE0144 | User %s failed to authorize logging in from IP address: %s. |
| FUE0145 | User %s failed to authorize. |
| FUE0146 | User %s failed to authenticate logging in from IP address: %s. |
| FUE0147 | User %s failed to authenticate. |
| FSE0148 | Listening on %s:%u failed while adding bastion %s. |
| FAI0149 | User %s deleted previous system version. |
| FAI0150 | User %s changed backup and retention settings. |
| FAI0151 | User %s %s bastion %s. |
| FAI0152 | User %s deleted bastion %s. |
| FSE0153 | Session indexing failure. |
| FSE0154 | Session conversion failure for session %s. |
| FSI0155 | Starting encoding session video %s. |
| FSI0156 | Completed session video %s encoding. |
| FAI0157 | User %s %s failover configuration. |
| FAI0158 | User %s added node %s. |
| FAI0159 | User %s changed %s in node %s. |
| FAI0160 | User %s deleted node %s. |
| FAI0161 | User %s disconnected node from the cluster. |
| FAI0162 | Cluster has no active nodes. Cluster will be disabled. |
| FAI0163 | User %s created new cluster. |
| FAI0164 | User %s attached current node to cluster. |
| FAE0165 | Error authenticating user %s. |
| FAI0166 | User %s restored original logo for protocol %s. |
| FAI0167 | User %s changed logo for protocol %s. |
| FAI0168 | User %s confirmed sensitive feature %s. |
| FAI0169 | User %s removed confirmation for sensitive feature %s. |
| FAI0170 | User %s changed following notifications settings: %s. |
| FAI0171 | User %s enabled email notifications. |
| FAI0172 | User %s disabled email notifications. |
| FAI0173 | User %(username)s is upgrading Fudo. |
| FAI0174 | User %(username)s upgraded Fudo. |
| FAI0175 | User %(username)s uploaded new upgrade image (version: %(version)s, size: %(size)d). |
| FAI0176 | User %(username)s deleted upgrade files. |
| FAI0177 | User %s uploaded license file. |
| FAW0178 | User %(username)s triggered system restart. |
| FAW0179 | User %(username)s triggered system shutdown. |
| FAW0180 | User %s %s remote SSH access. |
| FAW0181 | User %(username)s changed timestamping settings. |
| FAW0182 | User %(username)s uploaded new PKCS12 file. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FAW0183 | User %(username)s changed timestamping provider to %(provider)s. |
| FAW0184 | User %(username)s %(action)s timestamping. |
| FAI0185 | User %s imported system configuration. |
| FAI0186 | User %s exported system configuration. |
| FAI0187 | User %s added NTP server %s. |
| FAI0188 | User %s removed NTP server %s. |
| FAE0189 | Error saving NTP servers: "%s". |
| FAI0190 | User %(username)s changed date & time from %(old_date)s to %(new_date)s. |
| FAI0191 | User %s changed timezone to %s. |
| FAI0192 | User %s changed Fudo HTTPS private key and certificate. |
| FAI0193 | User %s %s SSH access. |
| FAI0194 | User %s requested service data. |
| FAI0195 | User %s added %s to %s for %s %s. |
| FAI0196 | User %s removed %s from %s for %s %s. |
| FAI0197 | User %s changed %s from %s to %s for %s %s. |
| FAI0198 | User %(username)s added IP address %(new_inet)s/%(new_netmask)s to interface %(interface)s with %(new_management)s management and %(new_cluster)s cluster address. |
| FAI0199 | User %(username)s changed subnet mask from %(old_netmask)s to %(new_netmask)s on %(new_inet)s/%(new_netmask)s address on interface %(interface)s. |
| FAI0200 | User %(username)s %(new_cluster)s cluster address on %(new_inet)s/%(new_netmask)s address on interface %(interface)s. |
| FAI0201 | User %(username)s %(new_management)s management on %(new_inet)s/%(new_netmask)s address on interface %(interface)s. |
| FAI0202 | User %(username)s deleted IP address %(old_ip)s from interface %(interface)s. |
| FAI0203 | User %(username)s %(action)s interface %(interface)s. |
| FAI0204 | User %(username)s added member %(member)s to bridge %(interface)s. |
| FAI0205 | User %(username)s removed member %(member)s from bridge %(interface)s. |
| FAI0206 | User %(username)s enabled spanning tree propagation on bridge %(interface)s. |
| FAI0207 | User %(username)s disabled spanning tree propagation on bridge %(interface)s. |
| FAI0208 | User %(username)s changed VLAN %(interface)s parent interface from %(old_parent_interface)s to %(new_parent_interface)s. |
| FAI0209 | User %(username)s changed VLAN %(interface)s ID from %(old_vlan)s to %(new_vlan)s. |
| FAI0210 | User %s deleted interface %s. |
| FAI0211 | User %s changed LDAP synchronization settings. |
| FAW0213 | LDAP error during fetching groups: %s. |
| FAI0214 | User %s enforced full LDAP synchronization. |
| FAI0215 | User %s disabled events logging on syslog servers. |
| FAI0216 | User %s removed syslog server: %s:%s. |
| FAI0217 | User %s added syslog server: %s:%s. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FAI0218 | User %s removed syslog server %s. |
| FAI0219 | User %s changed remote log dispatch settings. |
| FAI0220 | User %s changed network interfaces settings. |
| FAI0221 | User %s changed hostname from %s to %s. |
| FAI0222 | User %s added DNS server IP address %s. |
| FAI0223 | User %s removed DNS server IP address %s. |
| FAI0224 | User %s added new route for network %s with gateway %s. |
| FAI0225 | User %s changed gateway for network %s from %s to %s. |
| FAI0226 | User %s deleted network %s with gateway %s. |
| FAI0227 | User %s (%s) terminated session. |
| FAI0228 | Anonymous user from IP address %s with access rights granted by user %s joined session. |
| FAI0229 | User %s from IP address %s joined session. |
| FAI0230 | User %s (%s) suspended session. |
| FAI0231 | User %s (%s) resumed session. |
| FAE0232 | MySQL session playback error. |
| FAI0233 | Anonymous user from IP address %s accessed session %s shared by %s with key %s. |
| FAI0234 | User %s from IP address %s accessed session %s. |
| FAI0235 | User %s %s comment %d for session. |
| FAI0236 | User %s generated key %s with %s access. |
| FAI0237 | User %s is viewing user input for session. |
| FAI0238 | User %s blocked server %s. |
| FAI0239 | User %s unblocked server %s. |
| FAI0240 | User %s blocked connection %s. |
| FAI0241 | User %s unblocked connection %s. |
| FAI0242 | User %s addedd new time policy to connection %s for %s from %s to %s. |
| FAI0243 | User %s changed connection %s %s time policy %s from %s to %s. |
| FAI0244 | User %s deleted time policy for %s %s - %s from connection %s. |
| FAI0247 | User %s deleted server %s. |
| FAI0248 | User %s %s server %s. |
| FAI0251 | User %s deleted connection %s. |
| FAI0252 | User %s %s connection %s. |
| FAI0253 | User %s deleted session. |
| FAI0254 | User %s requested OCR processing for session. |
| FAW0255 | User %s tried to disable a non-exisitent sharing key for session. |
| FAI0256 | User %s disabled anonymous access key %s for session. |
| FAI0259 | User %s deleted download %s. |
| FAI0260 | User %s downloaded file %s for session %s. |
| FAI0261 | Anonymous user from IP address %s terminated session shared by %s with key %s. |
| FAI0262 | User %s terminated session. |
| FAI0263 | User %s blocked user %s. |
| FAI0264 | User %s modified policies settings. |
| FAI0265 | User %s modified regular expressions settings. |
| FSW0266 | Failed to send email. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FSE0267 | Error generating report %d: %s. |
| FAI0268 | User %s deleted report "%s". |
| FAW0269 | User %s cannot delete report "%s". |
| FAI0270 | Report {} created by user {}. |
| FAW0271 | User %(username)s is blocked. |
| FAW0272 | User %(username)s is not allowed to log in. |
| FAW0273 | User %(username)s logging from IP %(ip)s not found. |
| FAI0276 | User %s unblocked user %s. |
| FAI0277 | User %s deleted user %s. |
| FAI0278 | User %s added user %s to connection %s. |
| FAI0279 | User %s changed user %s. |
| FAI0281 | User %s logged out from Fudo administration panel. |
| FAI0282 | User %s successfully changed his password. |
| FSE0283 | Unable to process pattern: %s |
| FSW0284 | Pattern %s matched on %s with priority %s in session. |
| FSE0285 | Unable to read certificate. |
| FSE0286 | No peer certificate received. |
| FSW0287 | No server key configured, skipping verification. |
| FSI0288 | Server key verification failed. |
| FUI0289 | MSSQL connection terminated. |
| FSI0290 | User %s (%d) was removed. Reason: user wasn't in any of synchronized groups. |
| FSI0291 | System backup initiated, fingerprint: ${fingerprint}. |
| FSI0292 | System backup initiated. |
| FSI0293 | System backup completed, fingerprint: ${fingerprint}. |
| FSI0294 | System backup completed. |
| FAI0295 | User %s blocked bastion %s. |
| FAI0296 | User %s unblocked bastion %s. |
| FAI0297 | User %s created bastion %s. |
| FAI0298 | User %s changed bastion %s. |
| FAI0299 | User %s created server %s. |
| FAI0300 | User %s changed server %s. |
| FAI0301 | User %s changed connection %s. |
| FAI0302 | User %s created connection %s. |
| FAI0303 | User %s created user %s with role %s. |
| FAI0304 | User %s modified %s for %s %s. |
| FUE0305 | Client connection closed: encryption is not available. |
| FUE0306 | Client connection closed. |
| FSE0307 | Error fetching password from HiPAM server %s: unable to get sessid for user %s. |
| FSE0308 | HiPAM server internal error. |
| FSE0309 | Error fetching password from HiPAM server %s: unable to get sessdat for user %s. |
| FSE0310 | Incorrect server configuration: HiPAM name is empty. |
| FSE0311 | Unable to fetch password from HiPAM. |
| FSE0312 | Error connecting to HiPAM server %s: incorrect URL in configuration. |
| FSE0313 | Error connecting to HiPAM server %s: incorrect protocol specified. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FUE0314 | Invalid pixel format. |
| FSE0330 | Bad login field configured on LDAP server %s. Error while processing user %s. |
| FSE0331 | Error while processing userAccountControl value of user %s. |
| FSI0332 | User %s will be blocked. |
| FSI0333 | User %s will be unblocked. |
| FSW0334 | User %s has incorrect principal name. |
| FSI0335 | User %s synchronized from LDAP server %s. |
| FSI0336 | Remove pair connection %s user %s. |
| FSI0337 | Add conection %s to user %s. |
| FSW0338 | User %s paired with connection %s, server conflict. |
| FSI0339 | User %s (%s) was removed. Reason: user was not in any of synchronized groups. |
| FSI0340 | Full synchronization from LDAP server %s started. |
| FSI0341 | User %s connections cleared. |
| FSI0342 | User %s will be resynchronized from server %s. |
| FSI0343 | Resynchronized user %s will be removed. |
| FSW0344 | Connection to LDAP server error: %s. |
| FSI0345 | Successfully fetched password from %s. |
| FUE0346 | Client sent a packet bigger than %d bytes. |
| FSE0348 | Unable to get configuration settings. |
| FAI0349 | Anonymous user from IP address %s with access rights granted by user %s left session. |
| FAI0350 | User %s from IP address %s left session. |
| FUE0351 | Client sent unsupported NTLM v1 response. |
| FSE0352 | Bastion requires login and server delimited with one of '%s' (%s). |
| FAI0353 | User %(username)s is deleting upgrade snapshost. |
| FAI0354 | User %(username)s deleted upgrade snapshot. |
| FSE0355 | Inconsistent data, starting recovery replication to cluster node %s (%s). |
| FUW0356 | Unsupported X11 extension: %s. |
| FUW0357 | Server uses higher resolution than the current limit: %dx%d. |
| FUW0358 | Server uses higher color depth than the current limit: %d bpp. |
| FUE0359 | Server rejected X11 connection: %.*s. |
| FUE0360 | Server requires unsupported X11 authentication: %.*s. |
| FSW0361 | Fudo started. |
| FSE0362 | Unable to propagate ARP. |
| FUE0363 | User %s has no access to host %s:%u. |
| FUI0364 | RDP server sent a redirection packet. |
| FUE0365 | RDP server %s:%u has to listen on the default RDP port in order to redirect sessions. |
| FSE0366 | Error connecting to CyberArk server %s: incorrect URL in configuration. |
| FSE0367 | Error connecting to CyberArk server %s: incorrect protocol specified. |
| FSE0368 | Error fetching password from CyberArk server %s. |
| FSE0369 | Error fetching password from CyberArk server %s: unable to get password for user %s for server %s. |
| FUI0370 | User %s authenticated using OTP logged in from IP address: %s. |
| FUI0371 | User %s authenticated using OTP. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FSE0372 | Unable to invalidate OTP password %jd. |
| FUW0373 | Session has been terminated due to exceeding the time window defined in a time policy for the user %s and the safe %s. |
| FSI0374 | Established %s connection from %s to %s:%u. |
| FSE0375 | Unable to add listener %s. |
| FSE0376 | Unable to add listener %s because %s is listening on same IP address and port. |
| FSE0377 | Bastion requires login and server to be delimited with one of the '%s' characters (listener: %s, login: %s). |
| FSE0378 | Unable to establish connection: server not found, user not found or user has no access to the server (listener: %s, login: %s). |
| FSE0379 | Unable to establish connection: transparent server (tcp://%s:%u) not found or cannot be reached through listener (listener: %s, login: %s). |
| FSE0380 | Unable to authenticate user %s: server is blocked. |
| FSE0381 | Unable to authenticate user %s: account not found. |
| FSE0382 | Unable to authenticate user %s: account is blocked. |
| FSE0383 | Unable to authenticate user %s: user not found. |
| FSE0384 | Unable to authenticate user %s: user is blocked. |
| FSE0385 | Unable to authenticate user %s: safe not found. |
| FSE0386 | Unable to authenticate user %s: safe is blocked. |
| FSI0387 | Password for account %s verified successfully. |
| FSI0389 | Password for account %s changed successfully. |
| FAI0393 | User %s displayed password history for account %s. |
| FAI0394 | User %s displayed password to account %s changed at %s. |
| FAI0395 | User %s displayed current password for account %s. |
| FAI0396 | User %s blocked safe %s. |
| FAI0397 | User %s unblocked safe %s. |
| FAI0398 | User %s deleted safe %s. |
| FAI0399 | User %s changed safe %s. |
| FAI0400 | User %s created safe %s. |
| FAI0401 | User %s blocked account %s. |
| FAI0402 | User %s unblocked account %s. |
| FAI0403 | User %s deleted account %s. |
| FAI0404 | User %s changed account %s. |
| FAI0405 | User %s created account %s. |
| FAI0406 | User %s blocked listener %s. |
| FAI0407 | User %s unblocked listener %s. |
| FAI0408 | User %s deleted listener %s. |
| FAI0409 | User %s changed listener %s. |
| FAI0410 | User %s created listener %s. |
| FAI0411 | User %s blocked password change policy %s. |
| FAI0412 | User %s unblocked password change policy %s. |
| FAI0413 | User %s deleted password change policy %s. |
| FAI0414 | User %s changed password change policy %s. |
| FAI0415 | User %s created password change policy %s. |
| FSI0416 | Connection between safe %s and user %s has been removed. |
| FSI0417 | Connection between safe %s and user %s has been added. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FSI0418 | User %s was removed from safes %s. |
| FSE0420 | Unable to authenticate user %s against server %s. |
| FAI0421 | User %s assigned listener %s to safe %s. |
| FAI0422 | User %s unassigned listener %s from safe %s. |
| FAI0423 | User %s assigned account %s to safe %s. |
| FAI0424 | User %s unassigned account %s from safe %s. |
| FAI0425 | User %s assigned authentication method %s to user %s. |
| FAI0426 | User %s unassigned authentication mathod %s from user %s. |
| FAI0427 | User %s changed authentication mathod %s assigned to user %s. |
| FAI0428 | User %s assigned user %s to safe %s. |
| FAI0429 | User %s unassigned user %s from safe %s. |
| FAI0430 | User %s blocked password changer %s. |
| FAI0431 | User %s unblocked password changer %s. |
| FAI0432 | User %s deleted password changer %s. |
| FAI0433 | User %s changed password changer %s. |
| FAI0434 | User %s created password changer %s. |
| FSW0435 | Password changer timed out for acccount %s. |
| FUI0436 | User %s authenticated using token logged in from IP address: %s. |
| FUI0437 | User %s authenticated using token. |
| FAW0438 | User %s authenticated using new token while the old one still exists. |
| FAW0439 | User %s authenticated using old token. |
| FAI0440 | User %s granted access for account %s to user %s. |
| FAI0441 | User %s revoked access for account %s from user %s. |
| FAI0442 | User %s granted access for listener %s to user %s. |
| FAI0443 | User %s revoked access for listener %s from user %s. |
| FAI0444 | User %s created policy %s. |
| FAI0445 | User %s deleted policy %s. |
| FAI0446 | User %s changed policy %s. |
| FAI0447 | User %s assigned regexp %s to policy %s . |
| FAI0448 | User %s unassigned regexp %s from policy %s. |
| FAI0449 | User %s created regexp %s. |
| FAI0450 | User %s deleted regexp %s. |
| FAI0451 | User %s changed regexp %s. |
| FAI0452 | User %s granted access for safe %s to user %s. |
| FAI0453 | User %s revoked access for safe %s from user %s. |
| FAI0454 | User %s granted access for server %s to user %s. |
| FAI0455 | User %s revoked access for server %s from user %s. |
| FAI0456 | User %s granted access for user %s to user %s. |
| FAI0457 | User %s revoked access for user %s from user %s. |
| FAI0458 | User %s displayed password history for account %s. Reason: %s. |
| FAI0459 | User %s displayed password to account %s changed at %s. Reason: %s. |
| FAI0460 | User %s displayed current password for account %s. Reason: %s |
| FSE0461 | Invalid data from %s LDAP server. |
| FAI0462 | User {} created redundancy group {}. |
| FAI0463 | User {} deleted redundancy group {}. |
| FAE0464 | User %s is not allowed to login from address %s. |
| FUW0465 | Establishing new connections has been disabled. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FSE0466 | Fudo versions do not conform. |
| FUE0467 | Client tried to authenticate using an invalid UTF-8 login. |
| FSI0468 | A passphrase used to decrypt disks was changed. |
| FSE0469 | Unexpected number of bastions (%s). |
| FSE0470 | Unexpected number of servers (%s). |
| FSE0471 | Unexpected number of users (%s). |
| FSE0472 | RDP servers %s must all use TLS (NLA) or Standard RDP Security. |
| FSE0473 | Fudo cannot be upgraded to PAM. |
| FSI0474 | Fudo can be upgraded to PAM. |
| FSE0475 | Connection %s replaces a login and forwards a secret for servers %s which is not allowed. |
| FSE0476 | ZVOL with encryption key does not exist. |
| FSE0477 | Replication of encryption key to cluster node %s (%s) failed. |
| FSE0478 | Unable to join cluster's node ${name}. Fudo versions do not conform (local: ${VERSION}, remote: ${rversion}). |
| FSE0479 | Servers %s must all use the same %s settings. |
| FSE0480 | Servers %s must all use the same protocol. |
| FAI0481 | New OTP for user %s has been generated. |
| FSW0482 | Unable to verify password for account %s. |
| FUI0483 | User %s authenticated using Citrix logon ticket logged in from IP address: %s. |
| FUI0484 | User %s authenticated using Citrix logon ticket. |
| FUE0485 | ICA connection error. |
| FUI0486 | ICA server closed connection. |
| FAI0487 | User %s requested timestamping for session. |
| FAI0488 | User %s requested timestamping for account. |
| FSI0489 | Label %s not defined on this node, skipping listener %s. |
| FAI0490 | User %s created external authentication %s. |
| FAI0491 | User %s changed external authentication %s: %s. |
| FAI0492 | User %s deleted external authentication %s. |
| FSE0493 | Unable to establish connection to server %s (%s): label %s not defined on this node. |
| FSI0494 | Label %s not defined on this node, skipping external authentication %s. |
| FSE0495 | Communication error with cluster node %s (%s): connection failure. |
| FSE0496 | Communication error with cluster node %s (%s): unable to replicate a batch with object %jd to table %s. |
| FSE0497 | Communication error with cluster node %s (%s): unable to replicate a batch with object %jd (name: %s) to table %s. |
| FSE0498 | Communication error with cluster node %s (%s): unable to store object %jd in table %s. |
| FSE0499 | Communication error with cluster node %s (%s): unable to store object %jd (name: %s) in table %s. |
| FSE0500 | Communication error with cluster node %s (%s): unable to connect to %s. |
| FSE0501 | Communication error with cluster node %s (%s): failure during handshake. |
| FSE0502 | Database error. |

Continued on next page

Tablica 1 – continued from previous page

| Message code | Message and description |
|---|---|
| FSE0503 | Communication error with a cluster node: Fudo version mismatch (local: %s, remote: %s). |
| FSE0504 | Communication error with cluster node %s (%s): %s. |
| FSE0505 | Communication error with a cluster node: failure during handshake. |
| FSI0508 | Successfully replicated encryption key to node %s (%s). |
| FSE0509 | Communication error with cluster node %s (%s): unable to replicate session data. |
| FSE0510 | Communication error with cluster node %s (%s): intial replication failed. |
| FSW0511 | There has been an attempt to reset Fudo to factory defaults. Resetting Fudo to factory defaults has been administratively disabled. |
| FAI0512 | User %s enabled reset account. |
| FAI0513 | User %s disabled reset account. |
| FAW0514 | User %s of role %s tried to view %s, but has insufficient privileges for this action. |
| FSE0515 | Unable to upload backup #${currno} at ${datetime}. |
| FSI0516 | Backup #${currno} at ${datetime} successfully uploaded. |
| FSE0517 | Backup configuration error: %s. |
| FSE0518 | Backup internal error. |
| FSI0519 | ${type} backup snapshot ${snapname} successfully taken. |
| FUE0520 | User %s tried to access ICA server %s:%u using Citrix StoreFront which is not permitted. |
| FUE0521 | Citrix StoreFront sent an ICA file without a destination address. |
| FSW0522 | Roolback to ${oldversion} failed. |
| FSW0523 | Upgrade to ${oldversion} failed. |
| FSW0524 | Roolback to ${version} succeeded. |
| FSW0525 | Upgrade to ${version} succeeded. |
| FSE0526 | Error communicating with bypass card. Error setting nextboot mode. |
| FSE0527 | Error communicating with bypass card. Error setting bpe mode. |
| FSE0528 | Error communicating with bypass card. Error switching card mode. |
| FSE0529 | Error communicating with bypass card. |
| FAI0530 | User %s enabled snmp. |
| FAI0531 | User %s disabled snmp. |
| FSW0532 | External storage is unavailable. |
| FSE0533 | Unable to attach external storage. |
| FSI0534 | External storage attached. |
| FSE0535 | External storage is unavailable in this configuration. |
| FSW0536 | External storage detached. |
| FSI0537 | External storage attached successfully. |
| FAI0538 | Set external storage connection mode to %s |
| FAI0539 | Set configured WWN to %s, external storage connection mode to %s |
| FAI0540 | Interface discovery while configuring external storage: %s |
| FSW0540 | Found ${cdisk} paths to fiber channel ${wwn} from ${cscbus} devices. |
| FSW0541 | Retention module was unable to move session ${sessid}. |
| FAI0542 | User %s assigned account %s, listener %s to safe %s. |
| FAI0543 | User %s unassigned account %s, listener %s from safe %s. |
| FSE0544 | Failed to list snapshots. |
| FSW0545 | Unable to change password for account %s. |

Continued on next page

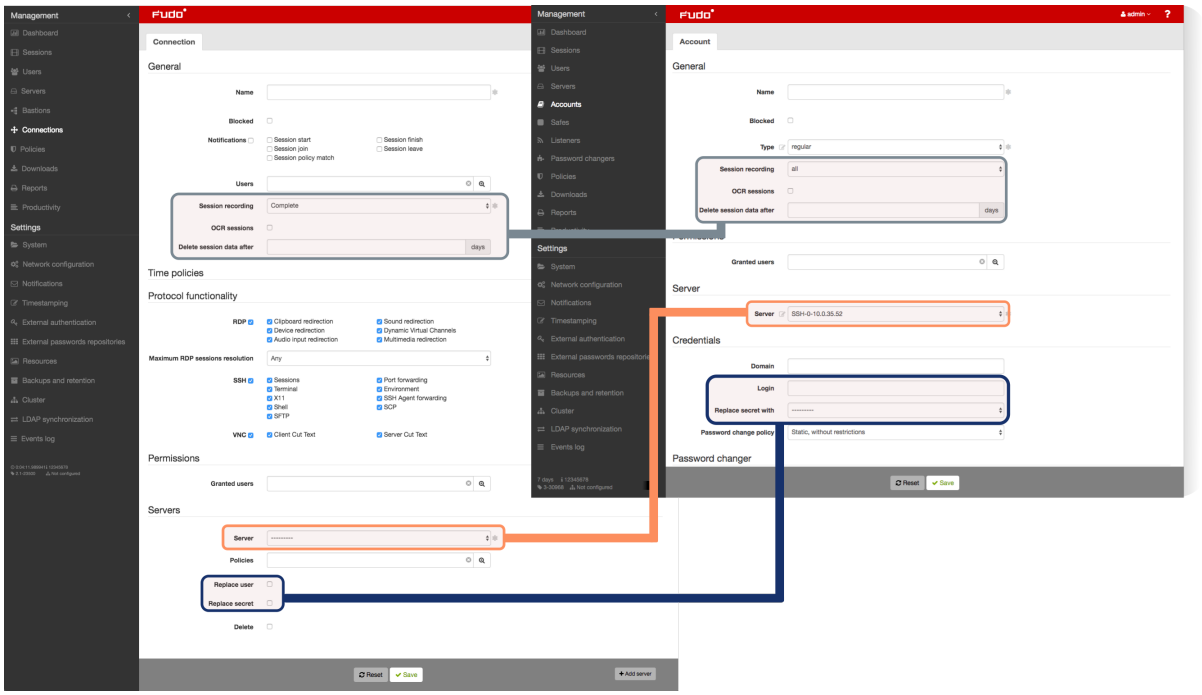
Tablica 1 – continued from previous page

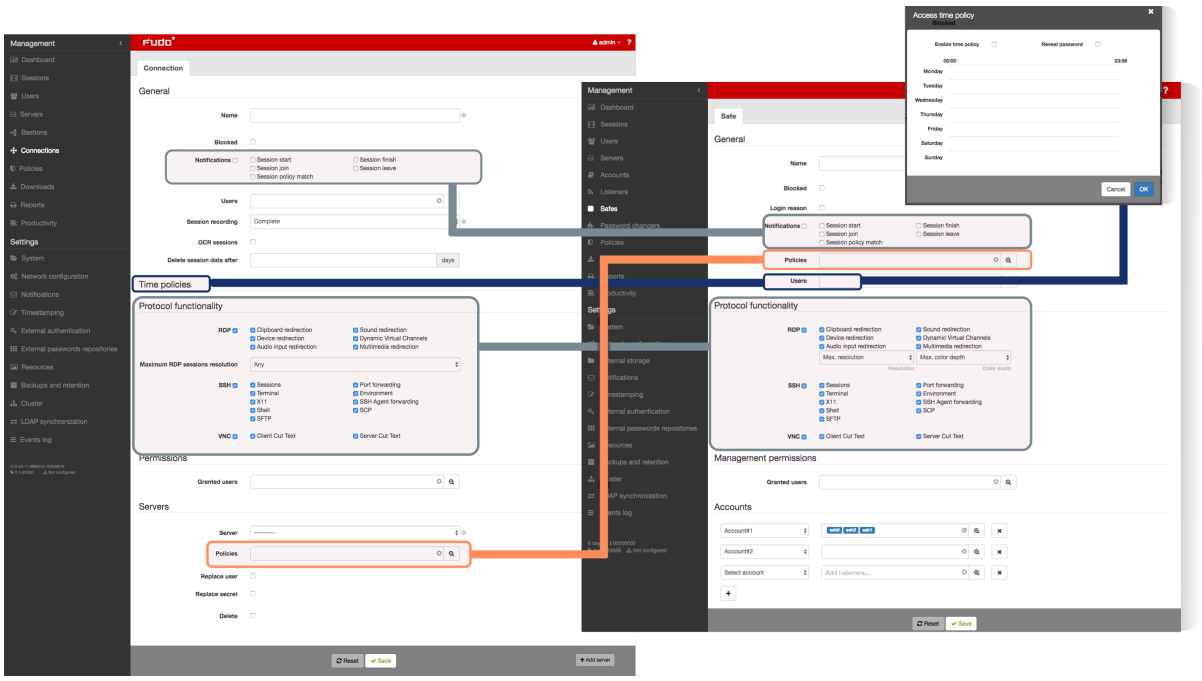
| Message code | Message and description |
|---|---|
| FUI0546 | ICA client closed connection. |
| FAE0547 | User %s could not create a ticket requesting an access to safe %s. |
| FAI0548 | User %s created ticket %s requesting an access to safe %s. |
| FAI0549 | User %s approved ticket %s requesting an access for user %s to safe %s. |
| FAI0550 | User %s rejected ticket %s requesting an access for user %s to safe %s. |
| FAI0551 | User %(username)s added member %(member)s to lagg %(interface)s. |
| FAI0552 | User %(username)s removed member %(member)s from lagg %(interface)s. |
| FSE0553 | Unable to extract public key from CA. |
| FUE0554 | SFTP server uses an unsupported version %u. |
| FAI0555 | User %s added address %s to server %s. |
| FAI0556 | User %s removed address %s from server %s. |
| FAI0557 | User %s changed address %s assigned to server %s. |
| FSI0558 | Starting encoding file for session %s. |
| FSI0559 | Completed encoding file for session %s. |
| FSE0560 | Session has not been approved nor rejected. |
| FSE0561 | Unexpected number of connections (%s). |
| FAI0562 | User %s rejected session %s. Reason: %s. |
| FAI0563 | User %s rejected session %s. |
| FAI0564 | User: {} tried to accept session: {} but it was accepted by: |
| FAI0565 | User: {} rejected session: {} |
| FAI0566 | User: {} tried to reject session: {} but it was accepted by: |
| FAI0567 | User: {} tried to reject session: {} but it was rejected by: |
| FAI0568 | User: {} accepted session: {} |
| FAI0569 | User: {} tried to accept session: {} but it was rejected by: |
| FAI0570 | User %s approved session %s. |
| FSI0571 | Proxy connection closed. |
| FSE0572 | Proxy connection error. |
| FSI0573 | Client sent an invalid token. |
| FSE0574 | Unable to resolve ${ip} domain to address. |
| FSE0575 | Unable to convert raw file to pcap. |
| FAI0576 | User {} changed 4 Eyes proxy API certificate settings. |
| FAI0577 | User {} changed 4 Eyes proxy settings. |
| FSI0578 | User %s (%s) was removed. Reason: user's external server dosen't exists any more. |
| FAI0579 | User {} changed 4 Eyes Fudo Mobile settings. |
| FSE0580 | Cluster %s has an invalid token: %s. |
| FAI0581 | User %s changed domain search path from %s to %s. |
| FSW0582 | Disk $cdev was removed. |

## 16.3 Fudo 2.2 to Fudo 3.0 parameters mapping

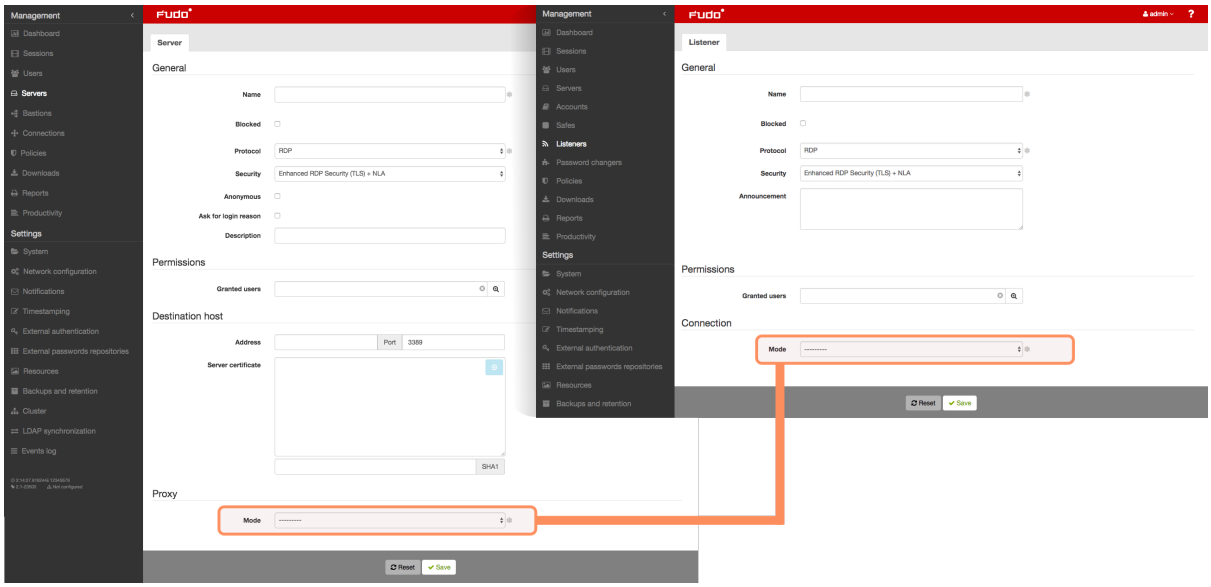
This topic describes how certain parameters from Fudo 2.2 map to Fudo 3.0 data model.

### 16.3.1 Connection



### 16.3.2 Server




## 16.4 Data model migration from Wheel Fudo PAM version 2.2 to 3.0

This topic describes data model migration mechanisms that are applied when performing upgrade from Wheel Fudo PAM version 2.2 to 3.0.

---

**Note:** In case of unsuccessful upgrade to version 3.0 data model issues which caused upgrade procedure to fail can be found in the system evetns log.

---

### 16.4.1 Server

*Servers*, which have the same IP address and port number assigned are replaced with a single object. Name of the resulting object is a concatenation of the servers' names in ascending order, separated by comma.

**Warning:** If there are two servers with the same IP address and port number assigned but with different protocol, description, external password repositorie, RDP security level, HTTP settings, TLS settings, certificates or public keys, upgrade will fail.

### 16.4.2 Safe (previously *connection*)

- Anonymous connection becomes a *safe* object, which can be deleted.
- For each *bastion* object (a group of servers operating in *bastion* mode, assigned to the same *bastion*) and associated connection, there is a *safe* object created using the following naming convention: `<connection name> > <bastion name>`.

- For each server operating in *gateway*, *proxy* or *transparent* mode, migration procedure creates a *safe* object named `<connection name> > <server name`.
- Automatically created *safe* object inherits connection's access rights, granted privileges, protocols settings, notifications settings and LDAP mapping.
- OCR settings, sessions recording and session data retention parameters are moved to corresponding *account* objects.
- Time policies are replicated as user specific regulations applicable to each safe.

**Note:** Click selected safe on user's configuration form to display time access settings.

- After migration, login credentials policies are reflected within the safe.

### 16.4.3 Account (previously *login credentials*)

For each login credentials sections in every connection, migration mechanism creates a separate *account* object.

- If login credentials contain the user login string the resulting account is of the *regular* type and its name is a combination of the login and server's name - `<login> @ <final server name>`.
- If login credentials do not contain the user login string and concern credentials forwarding connection, the resulting account object is of the *forward* type and it is named `forward for <final server name>`.
- If login credentials do not contain the user login and are used for anonymous connections, the resulting account object is of the *anonymous* type and it is named `anonymous for <final server name>`.
- Duplicated loign credentials are replaced by a single *account* object. Object's management rights, OCR settings, sessions recording settings, session data retention settings are inherited from the connection object that the *account* object derives from.

**Warning:** If login credentials contain the login string but do not contain the secret (if the login is substituted but the secret field remains empty) the data migration process will fail.

### 16.4.4 Listener (previously *bastion* or part of a server)

- For each server operating in *proxy*, *transparent* or *gateway* mode, there is a *listener* object created with the same connection mode.
- Newly created object inherits server's access rights, TLS settings and RDP security level parameter.
- Server announcement setting is also passed on to the *listener* object.
- Listener is assigned to all safes that have been created based on connections which were associated with the server that the listener derived from.
- Bastion becomes a listener operating in the *bastion* mode. Access rights and bastion settings are transferred to the listener. The listener is assigned to all safes that have been created based on connections associated with at least one server from the bastion that the listener derived from.

### 16.4.5 Sessions

- Each session has its safe, server and account identifiers updated accordingly. If a session concerned a server, which was not operating in *bastion* mode, it also has the listener identifier set.

## 16.5 ICA configuration file

The `.ica` configuration file defines connection parameters for establishing connections with remote host over the ICA protocol.

### 16.5.1 Non-TLS connections ICA file

```
[ApplicationServers]
<connection name>=

[<connection name>]
ProxyType=SOCKSV5
ProxyHost=<host>:<port>
ProxyUsername=*
ProxyPassword=*
Address=<username>
Username=<username>
ClearPassword=<password>
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

**Note:** `<connection name>` is for information purpose only and can be any string of characters. Provided value is displayed in the title of the ICA client application window.

### 16.5.2 TLS connections ICA file

```
[ApplicationServers]
<connection name>=

[<connection name>]
SSLEnable=On
SSLProxyHost=<FQDN>:<port>
Address=<username>
Username=<username>
ClearPassword=<password>
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

**Note:** `<connection name>` is for information purpose only and can be any string of characters. Provided value is displayed in the title of the ICA client application window.

**Related topics:**

- *ICA*
- *ICA protocol*
- *Data model*

ROZDZIAŁ 17

# AAPM (Application to Application Password Manager)

The AAPM module enables secure passwords exchange between applications.

An essential part of the AAPM module is the `fudopv` script. It is installed on the application server and it communicates with the Wheel Fudo PAM Secret Manager module to retrieve passwords.

The AAPM module supports Microsoft Windows, Linux and BSD family operating systems.

## 17.1 Compiling *fudopv* tool

The result of this procedure is `fudopv` application with Python interpreter included.

**Note:** For information on deploying *fudopv* without compiling sources files, refer to the *Deploying fudopv without compiling source files* topic.

### 17.1.1 Python

**Windows**

Download and install Python version 2.7.9 or newer:

https://www.python.org/downloads/

**Note:** Make sure to select the option to add `python.exe` to the execution path.

**Linux**

Install Python environment according to the guide provided by the manufacturer.

Exemplary configuration for RedHat 6.7 system:

```
./configure \
  --prefix=/opt/python-2.7.14 \
  --with-ensurepip=install \
  --disable-optimizations \
  --enable-shared
```

**Note:**

- `--disable-optimizations` - optimizations may result in build failures,
- `--with-ensurepip=install` - installs tools for managing Python's packages,
- `--enable-shared` - one of the `fudopv's` dependencies requires the Python interpreter `.so` library.

### 17.1.2 Virtual environment

Compiling the package requires the `virtualenv` module.

1. Execute `pip install virtualenv` or `easy_install virtualenv` command.
2. In the `fudopv/` execute the `virtualenv deps` command.

The environment required for building `fudopv` will be created in the `deps/` folder.

**Windows**

Run the `deps\Scripts\Activate` command to activate the environment.

**Linux**

In case of the interpreter build from the source code you can use the included `pip` and `easy_install` tools. You must also set the path to the shared libraries and run the `virtualenv` with the `-p` option:

```
export LD_LIBRARY_PATH=/opt/python-2.7.14/lib
virtualenv -p /opt/python-2.7.14/bin/python deps
LD_LIBRARY_PATH=/opt/python-2.7.14/lib
/opt/python-2.7.14/bin/pip install virtualenv
/opt/python-2.7.14/bin/virtualenv -p /opt/python-2.7.14/bin/python deps
```

To activate the environment, run the `source deps/bin/activate` command.

### 17.1.3 Fetching dependencies

In active virtual environment run the `pip install -r requirements.txt` to install `fudopv` dependencies. Dependencies are installed in the `deps/`

**Note:** If the `ImportError: No module named _markerlib` problem occurs, execute `pip install --upgrade distribute` and install dependencies once again.

**Windows**

Download and install *pywin32*: https://sourceforge.net/projects/pywin32/files/

**Note:** Make sure to select the installer for Python 2.7.

After activating the `virtualenv` environment, execute the following command with the path to the *pywin32*:

```
easy_install path\to\pywin32
```

**Linux**

Linux operating system does not require taking any additional actions.

### 17.1.4 Package creation script

Execute the `python setup.py` command, which will create package in the *fudopv* folder.

**Note:** The *PyInstaller* does not support package creation on a privileged account. If the `ERROR: You are running PyInstaller as user root. This is not supported.` error occurs, you can change the `check_not_running_as_root()` function in the `./deps/lib/python2.7/site-packages/PyInstaller/utils/misc.py` so that it return the result without checking anything.

**Related topics:**

- *Using fudopv*
- *Deploying fudopv without compiling source files*
- *Authentication methods*

## 17.2 Deploying *fudopv* without compiling source files

To use *fudopv* without compiling source files, proceed as follows.

1. Download and install Python environment, version 2.7.9 or newer.

**Note:** It is advised to run *fudopv* in virtual environment.

2. Execute `pip install virtualenv` or `easy_install virtualenv` command to install virtual environment.
3. In the `fudopv/` execute `virtualenv deps` command.
4. Execute `python -m fudopv`, to start *fudopv*.

**Related topics:**

- *Using fudopv*
- *Compiling fudopv tool*

- *API interface*

## 17.3 Using *fudopv*

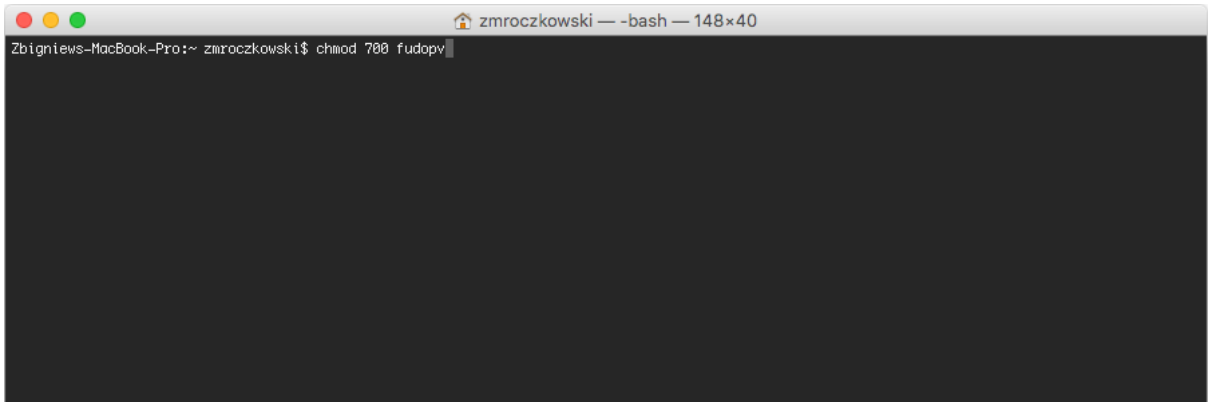
### Execution parameters

```
fudopv [<options>] <command> [<parameters>]
```

| Command/option/parameter | Description |
|---|---|
| *Commands* | |
| `getcert` | Fetch Wheel Fudo PAM SSL certificate. |
| `getpass` <type> <account> | Fetch password to selected account.<br>type:<br>• `direct` - direct, unmonitored connection;<br>• `fudo` - connection monitored by the *PSM* module |

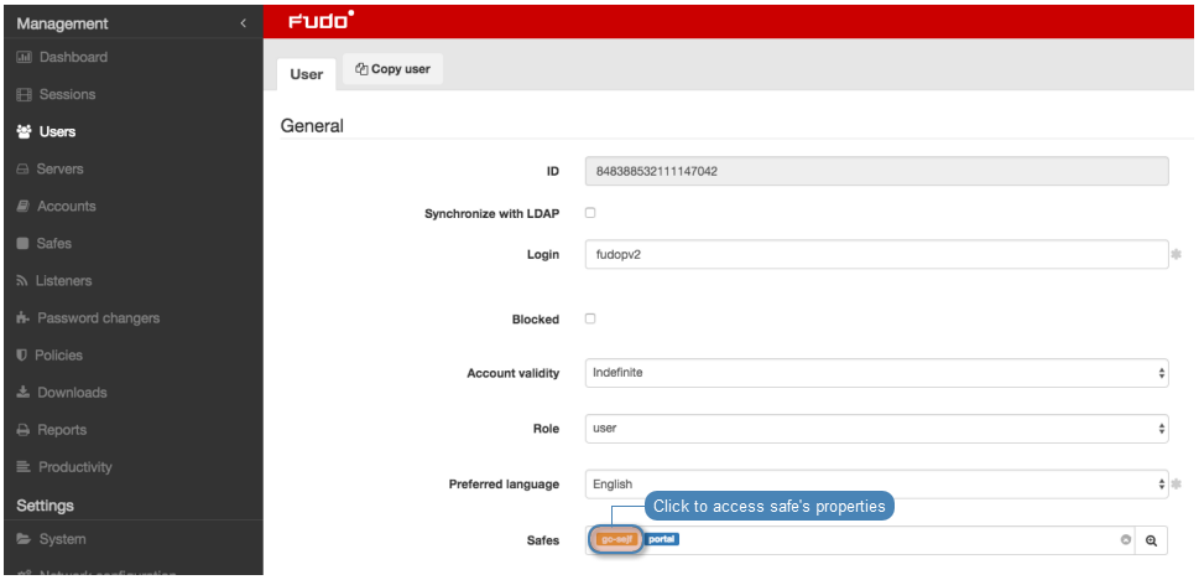
| *Options* | |
|---|---|
| `-c <path>` | Use configuration file from provided path. |
| `--cfg <path>` | |
| `-h, --help` | Show options and parameters list. |

1. Upload `fudopv` script to the server and change its access rights to allow execution.

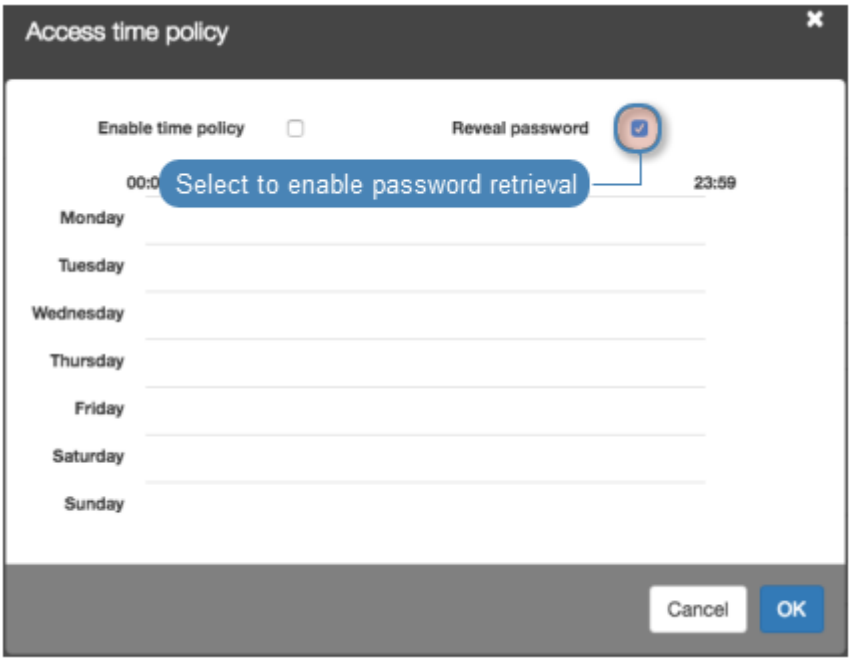



2. Log in to the Wheel Fudo PAM administration panel.
3. Create a user object with `user` role, static or one-time password authentication and server's IP address defined in the *API* section.

- Select *Management* > *Users*.
- Click *+Add*.
- Enter user's name.
- Define account's validity period.
- Select `user` from the *Role* drop-down list.
- Assign safe and click the object to open its properties.

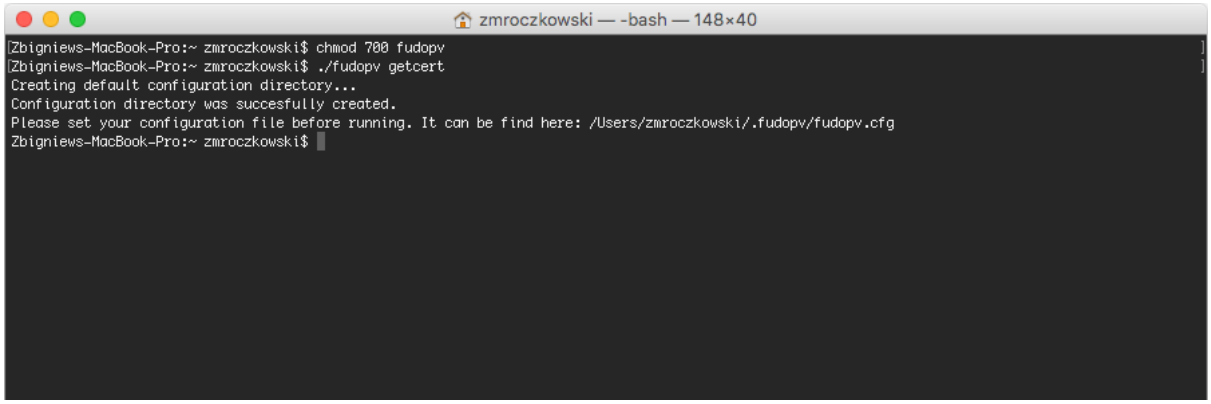



- Select the *Reveal password* option.



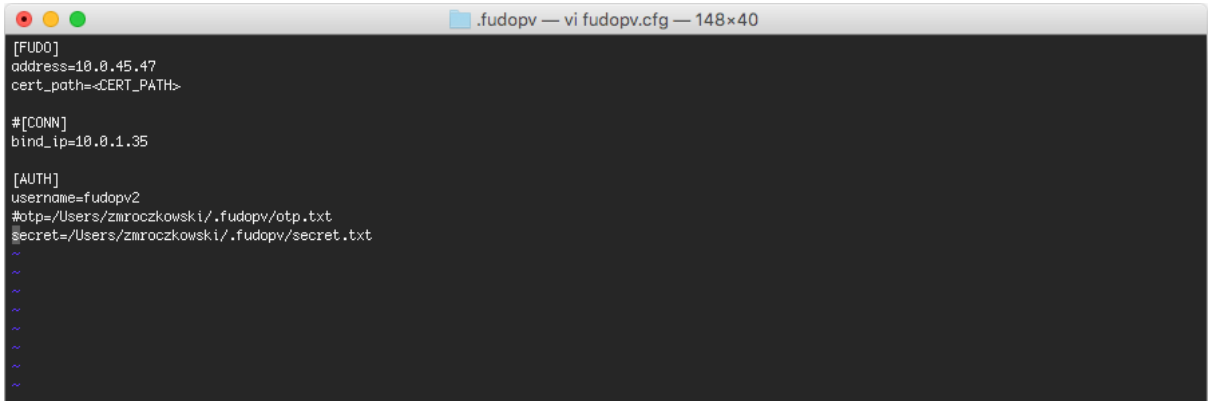

- In the *Authentication* section, select `Password` or `One time password` from the *Type* drop-down list.
- In case of static password authentication, type in the password in *Password* and *Repeat password* fields.
- In the *API* section, click the + icon and enter the IP address of the server, which will be requesting passwords using `fudopv` script.
- Click *Save*.

4. Run `fudopv getcert` command to initiate the configuration.




**Note:** `fudopv` configuration files are stored in the `.fudopv` folder in user's home folder.

5. Open `fudopv.cfg` file in a text editor of your choice.




| Section | Description |
|---|---|
| `[FUDO]` | |
| `address` | Wheel Fudo PAM's IP address. |
| `cert_path` | Path to the Wheel Fudo PAM's SSL certificate files. |

| `[CONN]` | |
|---|---|
| `bind_ip` | IP address of the server, running the `fudopv` script. The IP address must be the same as the IP address defined in the *API* section in user configuration. |

| `[AUTH]` | |
|---|---|
| `username` | User login as defined in step 3. |
| `otp` | Path to the otp.txt file containing the one time password. |
| `secret` | Path to the secret.txt file containing user's static password. |

**Note:**

- In the `[FUDO]` section, in the `address` line, enter the Wheel Fudo PAM IP address.
- Leave the `cert_path` line as is, it will be updated automatically after successfully running the `fudopv getcert` command.
- In the `[CONN]` section, uncomment the `bind_ip` line and provide the IP address of the

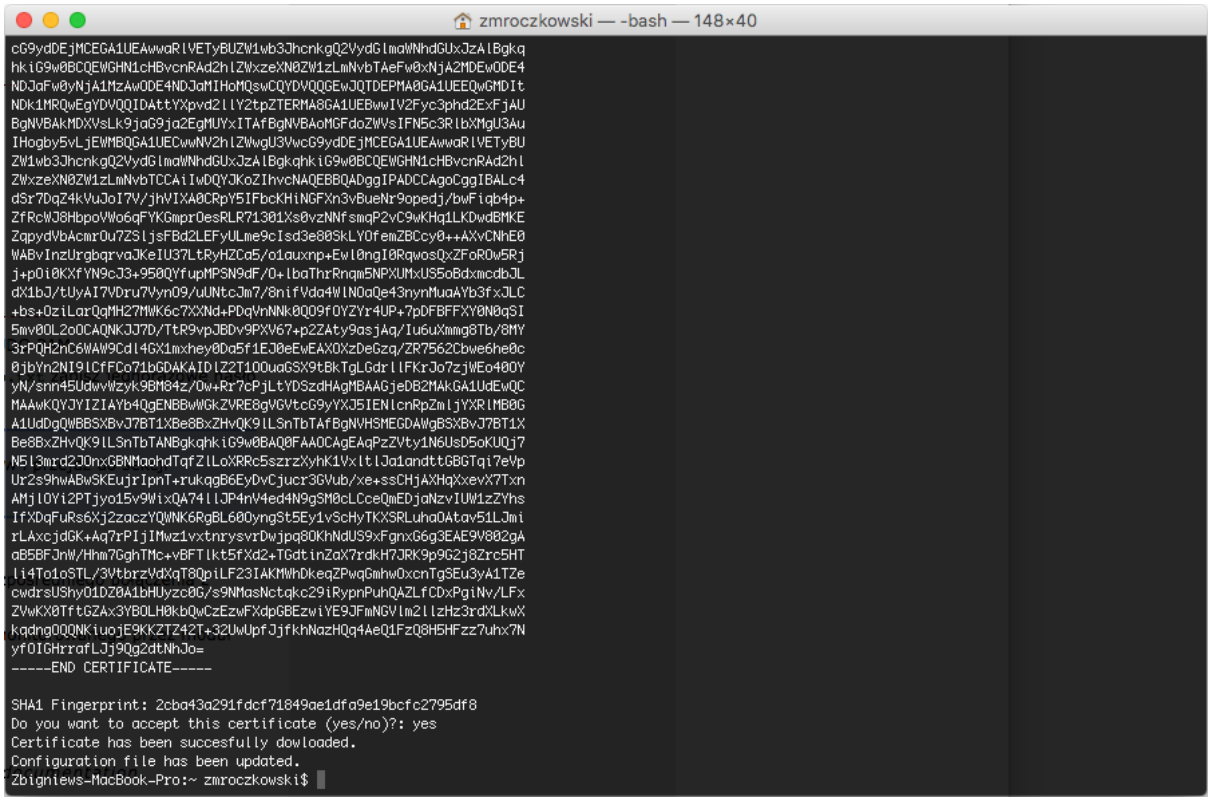
server running the `fudopv` script.

- In the `[AUTH]` section, in the `username` line, provide the login of the user object defined in step 3.
- Depending on the users authentication method, comment the corresponding line defining the authentication secret information.

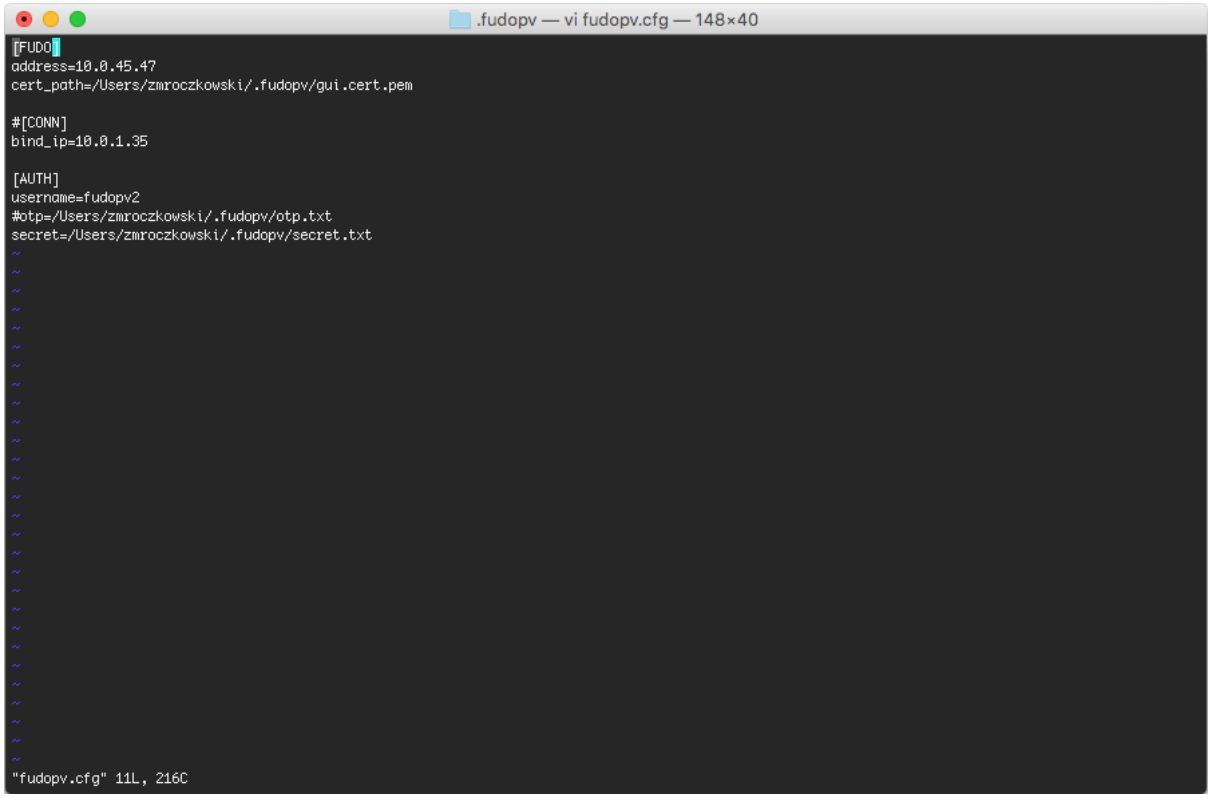
For example:

```
[FUDO]
address=10.0.0.8.61
cert_path=<CERT_PATH>

#[CONN]
bind_ip=10.0.0.8.11

[AUTH]
username=fudopv
#otp=/Users/zmroczkowski/.fudopv/otp.txt
secret=/Users/zmroczkowski/.fudopv/secret.txt
```

6. Run `fudopv getcert` command to fetch Wheel Fudo PAM's SSL certificate.




**Note:** After running the script successfully, the path to the certificate in the configuration file will be automatically updated.



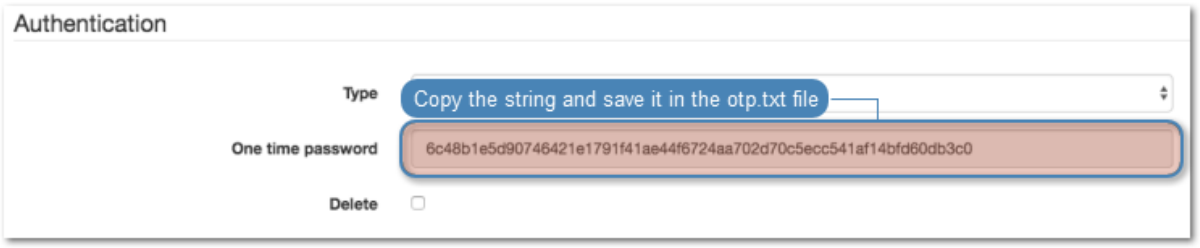

7. Edit the `secret.txt` file and provide user's static password; or edit the `otp.txt` file and store the one time password.

---

**Note:**

- The one time password can be found in user's properties, in the *Authentication* section.

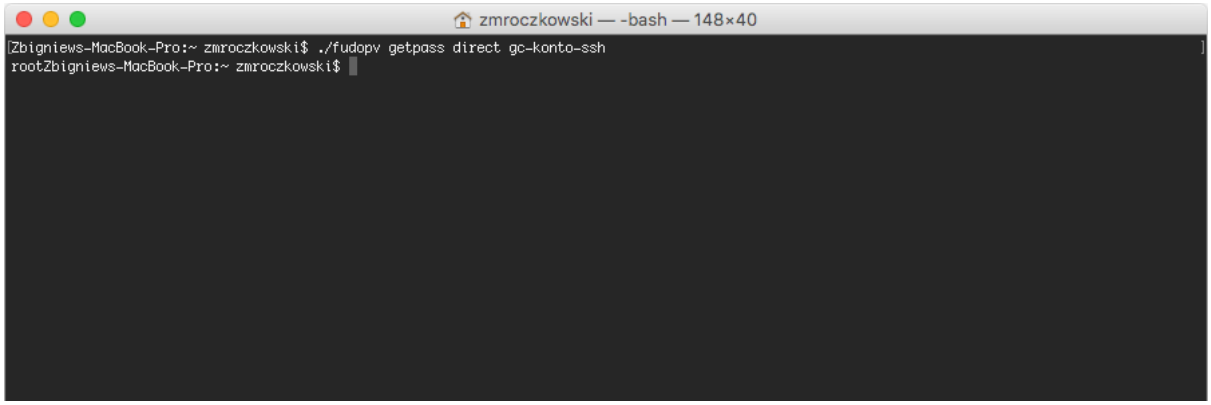
---



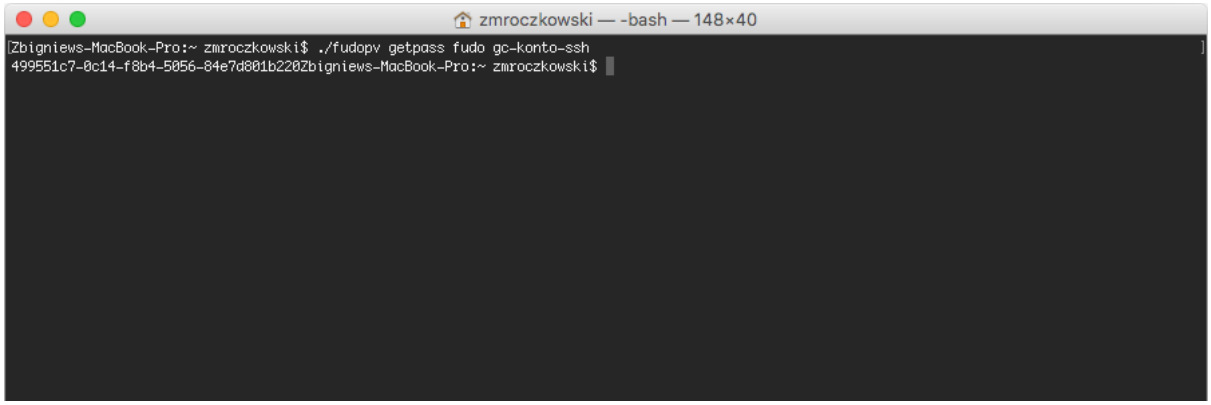

- The `otp.txt` file will be automatically updated each time the `fudopv getpass` command is run.

8. Run command:

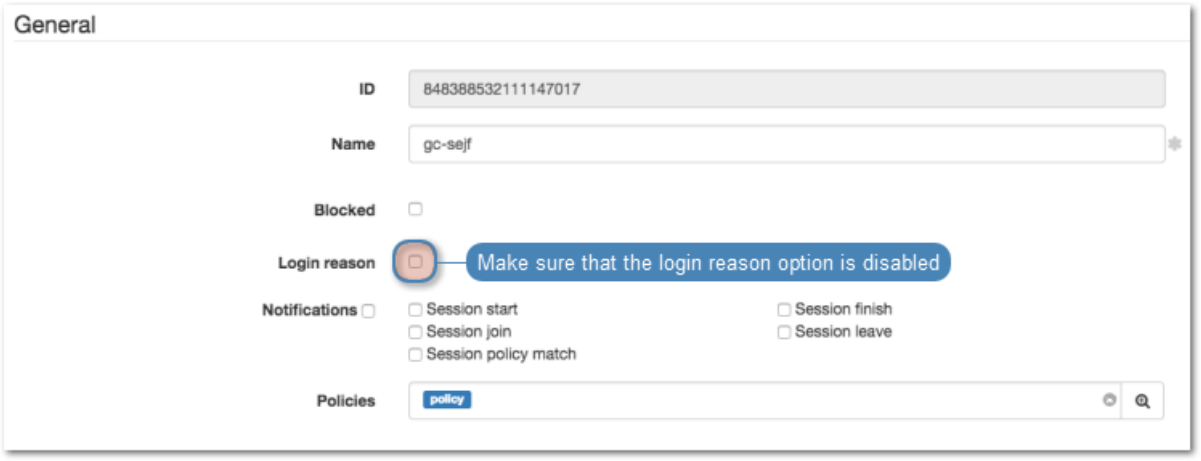
- `fudopv getpass direct <account_name>`, to fetch password to connect directly to the server.




- `fudopv getpass fudo <account_name>`, to fetch password to establish monitored connection with the target host.




**Warning:** Correct operation of the `fudopv` script requires disabling the login reason prompt option in the safe's properties.




**Related topics:**

- *Compiling fudopv tool*
- *Deploying fudopv without compiling source files*
- *Authentication methods*
- *Data model*

- *System overview*
- *Setting up password changing on a Unix system*

## 17.4 API interface

AAPM's API interface is described in detail in the *Wheel Fudo PAM - API documentation* manual.

**Related topics:**

- *Compiling fudopv tool*
- *Using fudopv*
- *Deploying fudopv without compiling source files*
- *Data model*
- *System overview*
- *Setting up password changing on a Unix system*

## 17.5 Authentication methods

Conventions and symbols:

- **url**: `fudo` connection address,
- **->**: `fudopv` request,
- **<-**: response from Wheel Fudo PAM,
- **status**: response status,
- **FUDO**: Fudo IP address,
- **USER**: username,
- **SECRET**: password (static/OTP),
- **SESSIONID**: session token,
- **method**: HTTP protocol method: GET/POST/PUT,
- **{"key": "value"}**: JSON included in the request/response.

### 17.5.1 Static password

Static user password, stored in the `secret.txt` file.

- -> url: https://FUDO/api/portal/login
- -> method: POST
- -> `{"username": "USER", "password": "SECRET"}`
- <- status:

  - 200, OK
    * <- `{"sessionid": "SESSIONID"}`
  - 401, UNAUTHORIZED
  - <- *Not applicable.*

### 17.5.2 Token

One time password stored in the `otp.txt` file.

- -> url: https://FUDO/api/portal/login
- -> method: POST
- -> `{"username": "USER", "otp": "SECRET"}`
- <- status:
  - 200, OK
    * <- `{"otp": NEW_SECRET, "sessionid": "SESSIONID"}`
  - 401, UNAUTHORIZED
  - <- *Not applicable.*

After saving new password in the `otp.txt`, `fudopv` sends a confirmation message.

- -> url: https://FUDO/api/portal/confirm
- -> method: POST
- -> `{"otp": "NEW_SECRET"}`
- <- status: 204, NO CONTENT

**Related topics:**

- *Compiling fudopv tool*
- *Deploying fudopv without compiling source files*
- *Using fudopv*

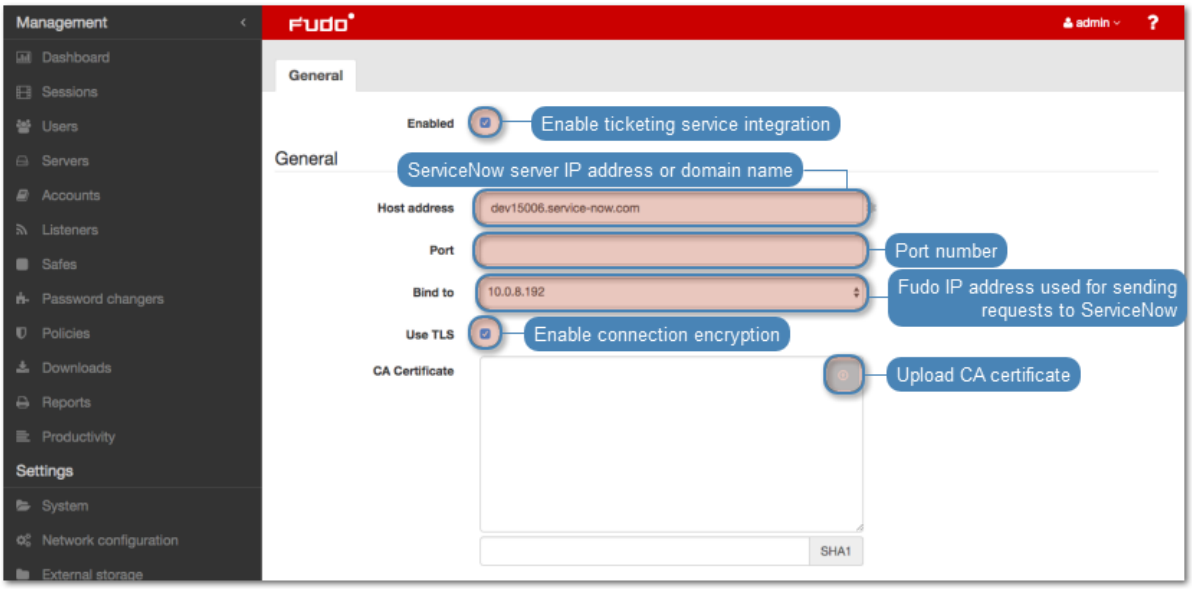
ROZDZIAŁ 18

# Service Now

## 18.1 Configuration

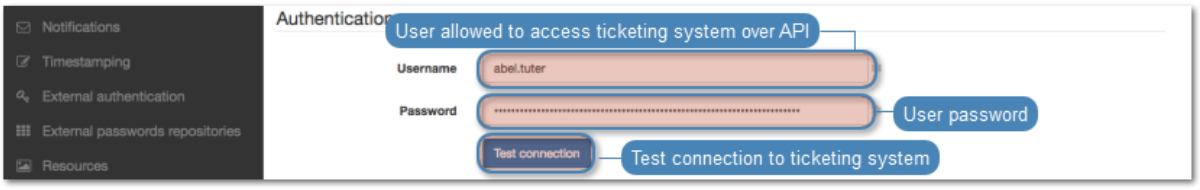
To configure *ServiceNow*, proceed as follows.

1. Select *Settings* > *Ticketing system*.
2. Select *Enable* option to enable ticketing service integration.
3. In the *General* section, provide IP address and port number of *ServiceNow* REST API.
4. Select the *Use TLS* option to enable connection encryption.
5. From the *Bind to* drop-down list, select the IP address used by Wheel Fudo PAM for sending requests to *ServiceNow* API.

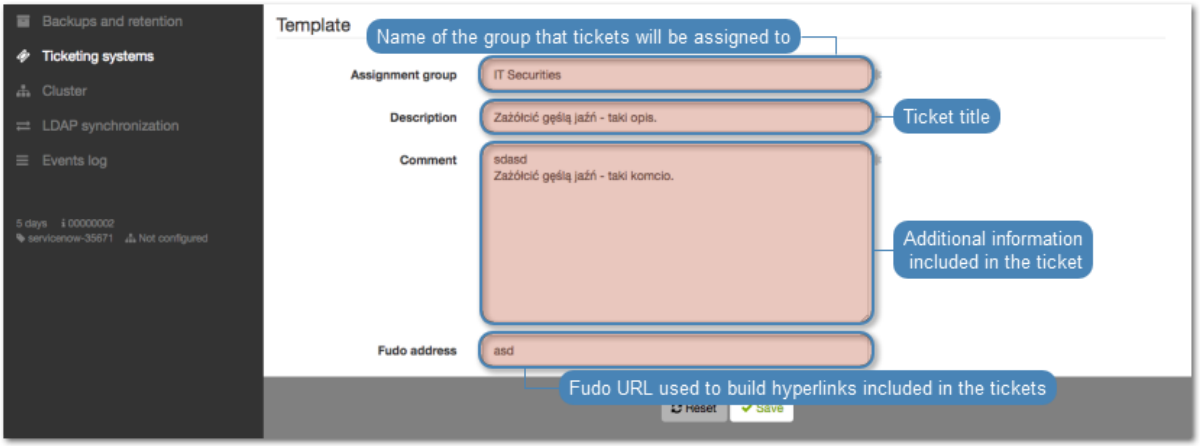



6. In the *Authentication* section, provide user credentials allowed to access *ServiceNow* over defined REST API.

**Note:** Click *Test connection* to verify configuration parameter values. The result of testing will be a ticket in *ServiceNow*, containing the configuration values prefixed with the `test_` string.




7. In the *Template* section, in the *Assignment group*, define the *ServiceNow* users group to which the tickets will be assigned.
8. In the *Description* field, provide the ticket template title.
9. In the *Comment* field, provide additional information to be included in the ticket.
10. Enter Fudo URL that will be used to create quick access hyperlinks included in tickets.




11. Click *Save*.

**Related topics:**

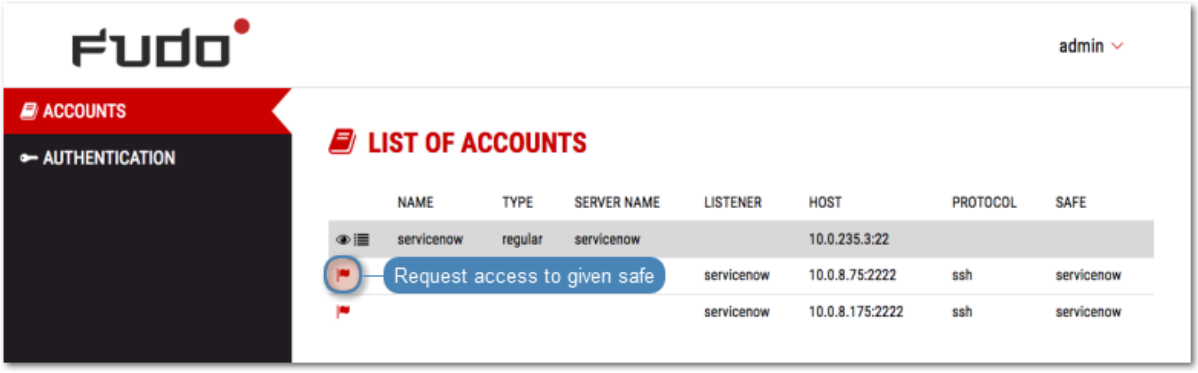
- *Requesting access to safe*
- *Granting access*

## 18.2 Requesting access to safe

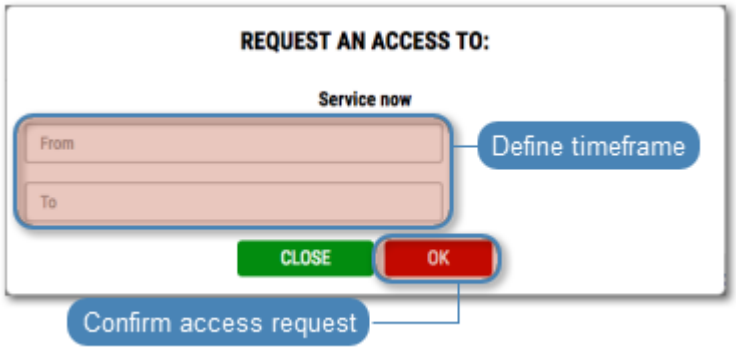
**Note:** Usernames on Wheel Fudo PAM and *ServiceNow* must be the same to ensure correct requests processing.

To request access to safe, proceed as follows.

1. Log in to *User Portal*.
2. Find desired safe and click .




3. Define time period and click *OK*.




**Note:** Click the icon to access time settings.

**Related topics:**

- *Configuration*
- *Granting access*

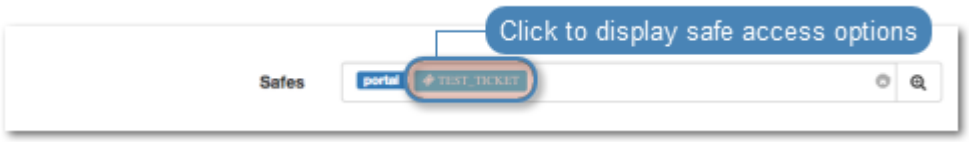
## 18.3 Granting access

To grant access based on a *ServiceNow* ticket, proceed as follows.

1. Select *Management* > *Users*.
2. Find and click user requesting access.

**Note:** Users with pending access requests are marked with icon.

3. In the *Safes* field, find and click the object that the user requests to access.




4. Deselect *Blocked* option and define access time period.
5. Click *Accept*.

**Note:** Safe access management options can be also accessed from within the safe edit form.

**Related topics:**

- *Configuration*

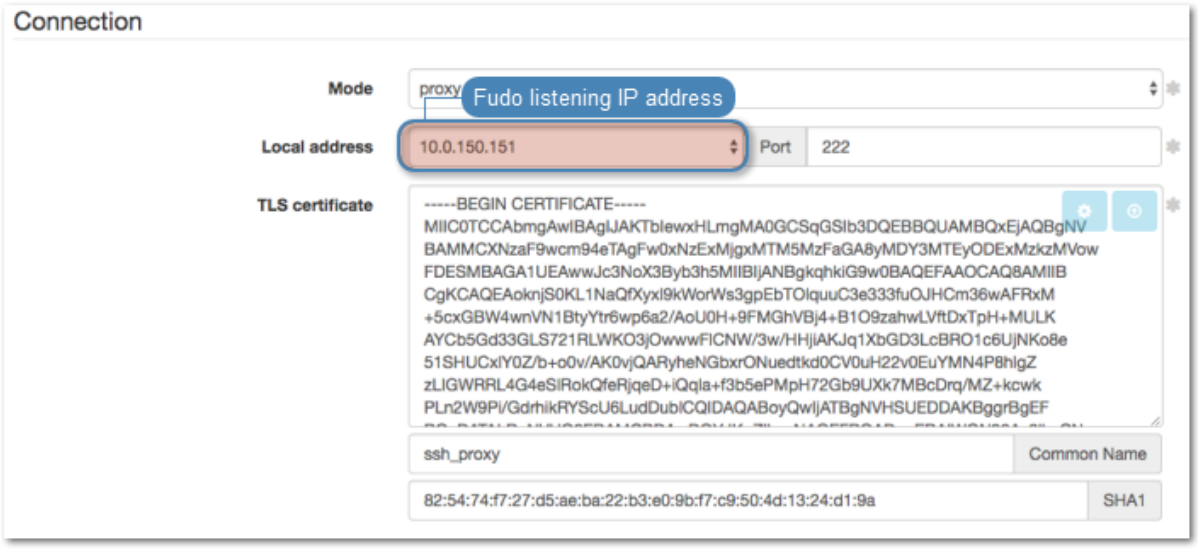
- *Requesting access to safe*

ROZDZIAŁ 19

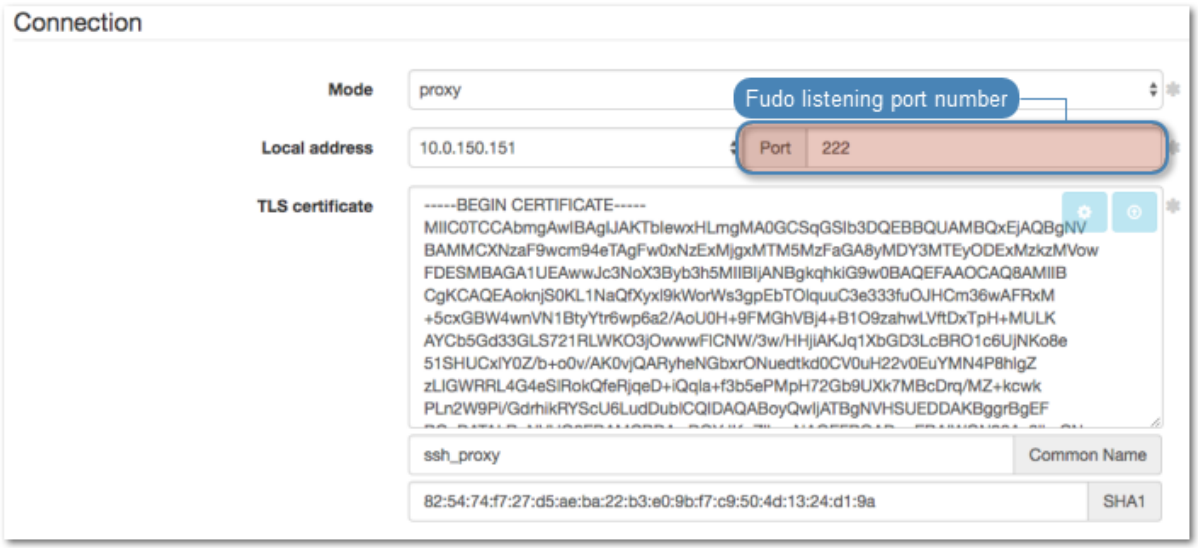
# Client applications

## 19.1 PuTTY

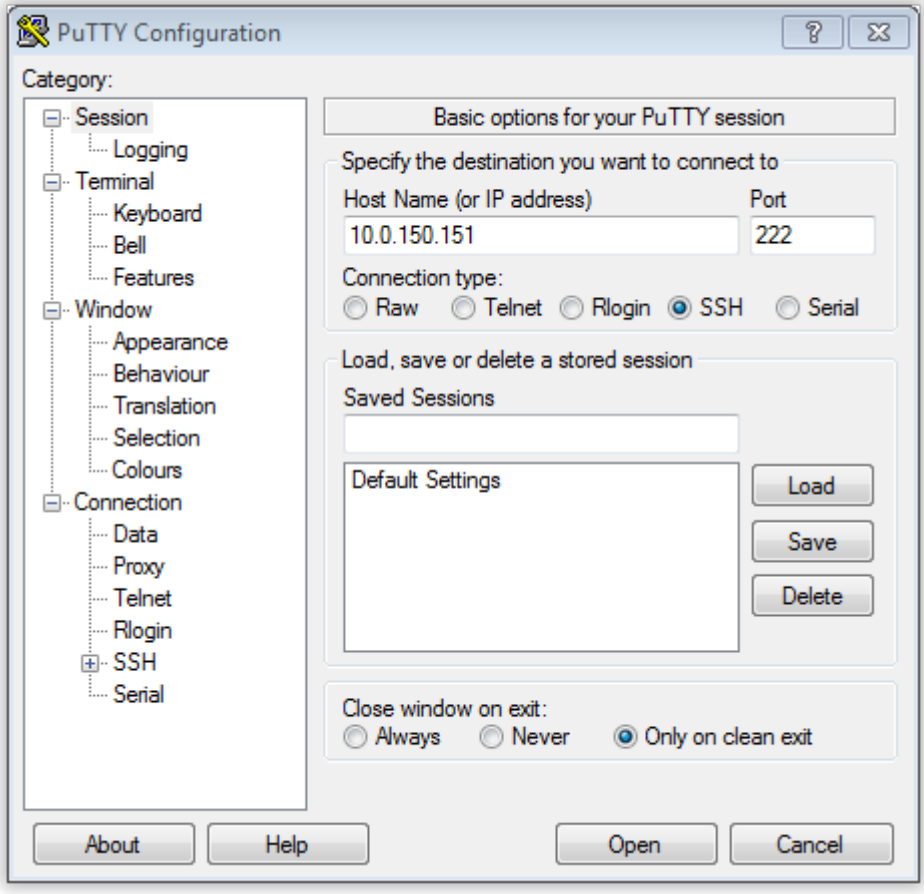
1. Download and launch PuTTY.
2. In the *Host Name (or IP address)* field, enter IP address defined in the listener.




3. In the *Port number* field, enter port number defined in the listener.

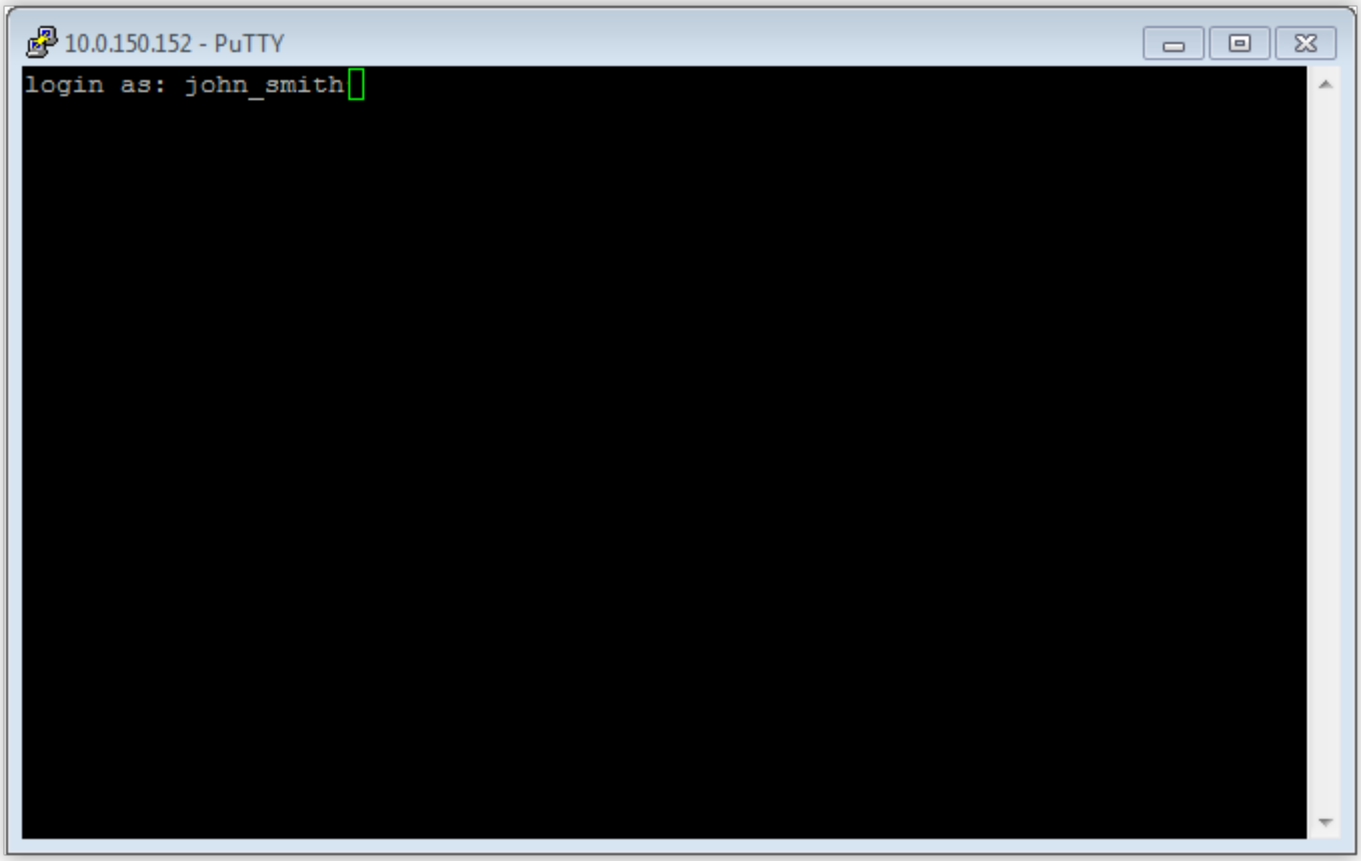



4. Select the `SSH` connection type.




5. Click *Open*.

6. Enter username.



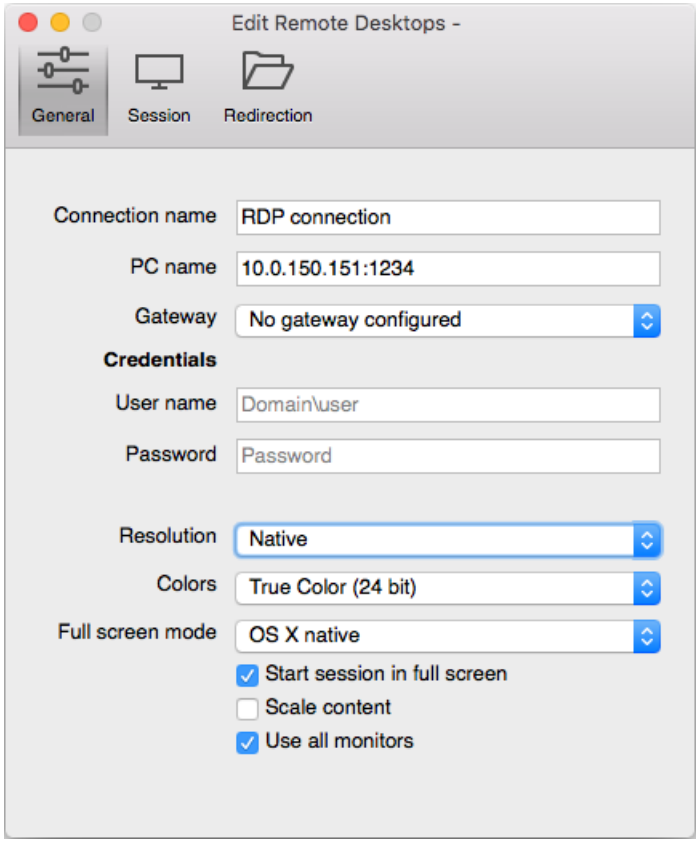

7. Enter password.

**Related topics:**

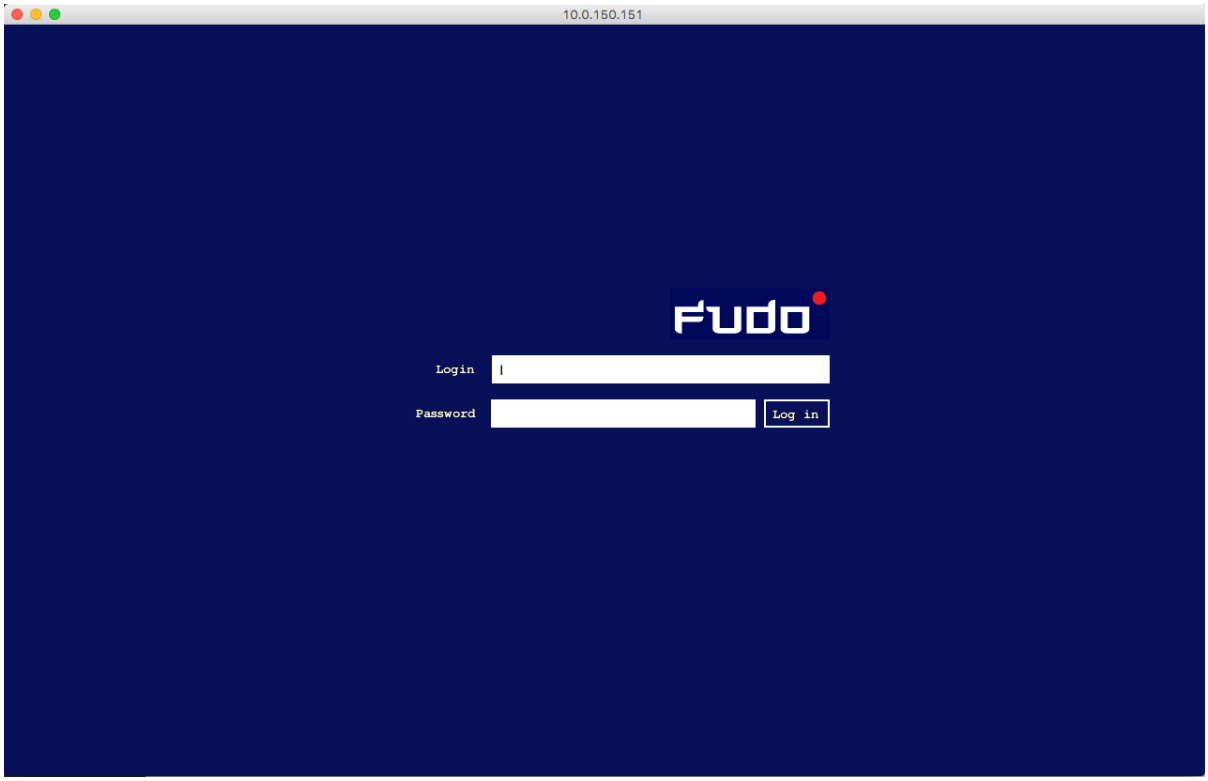
- *SSH*
- *Creating an SSH server*
- *Creating an SSH listener*

## 19.2 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.

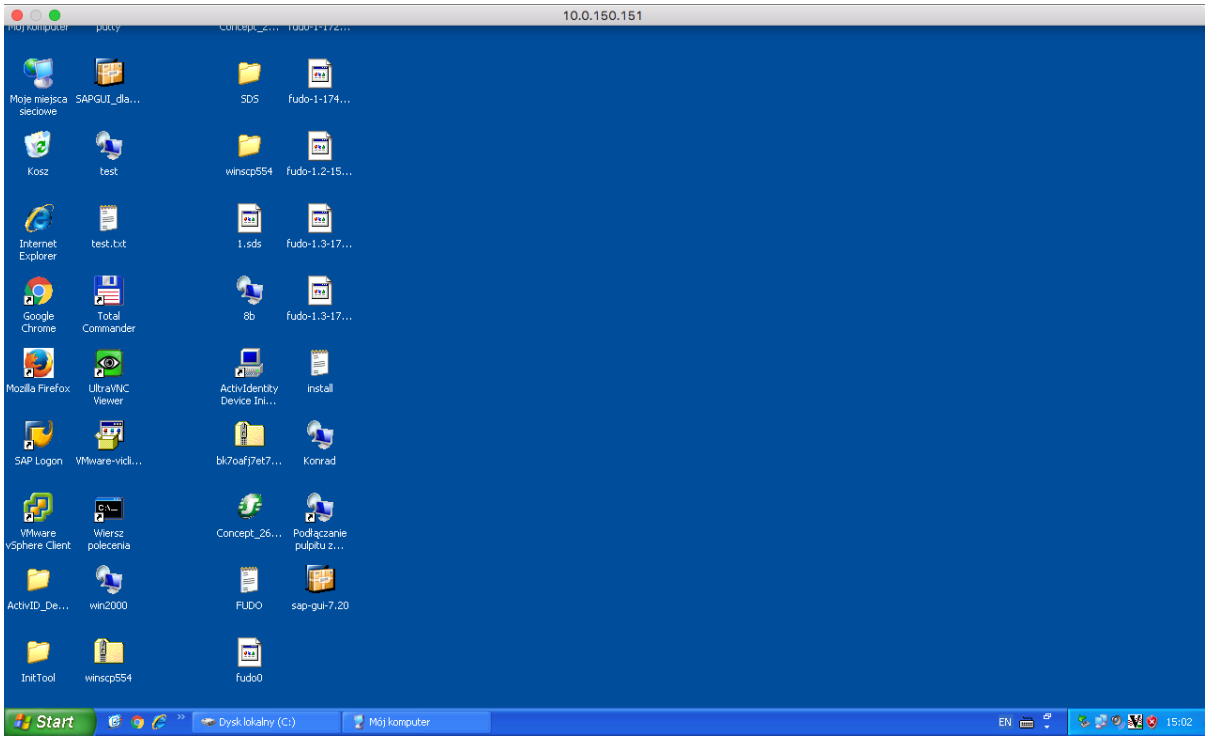



3. Enter user login and password and press the [Enter] keyboard key.




**Note:** Wheel Fudo PAM 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.

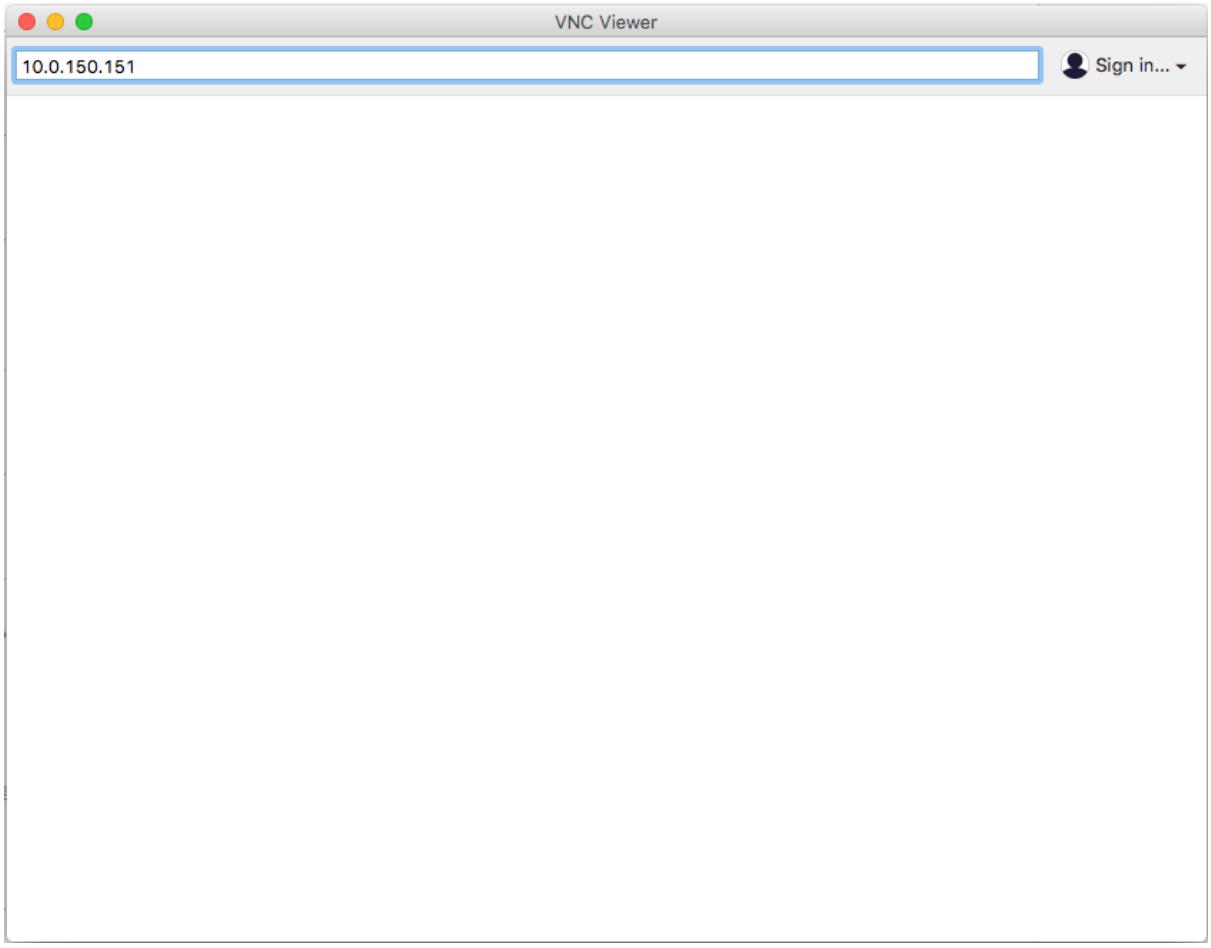



**Related topics:**

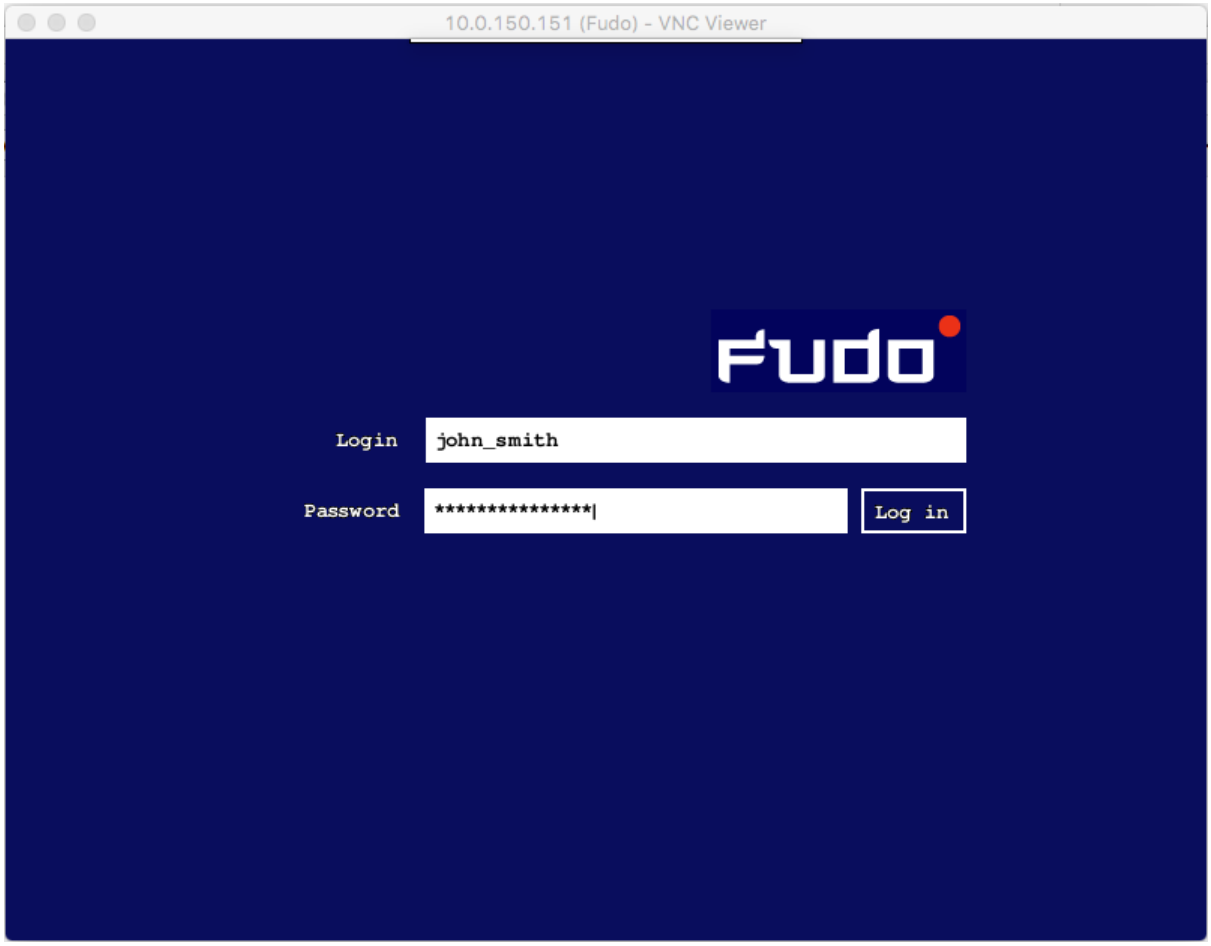
- *RDP*
- *Creating an RDP server*
- *Creating an RDP listener*

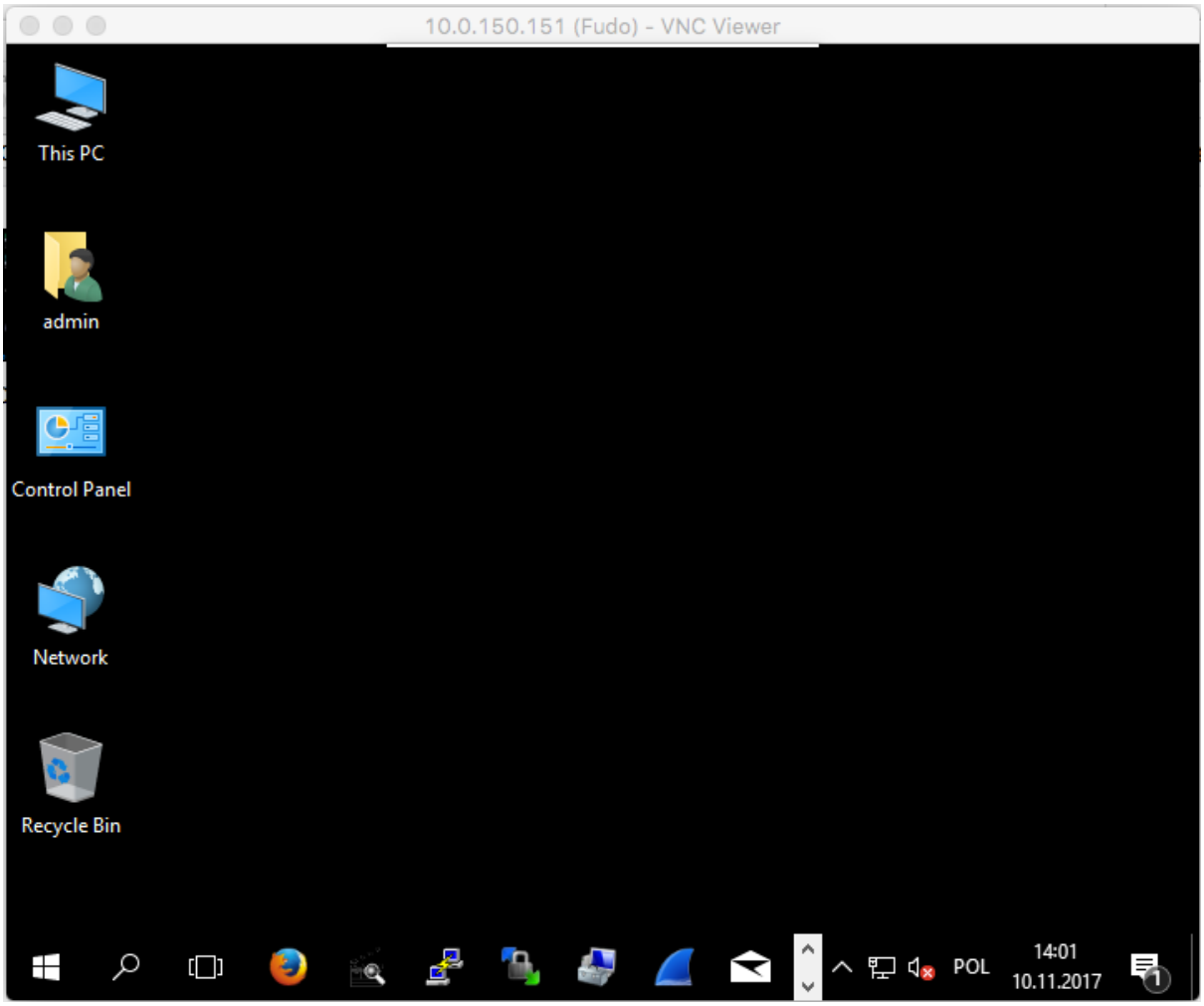
## 19.3 VNC Viewer

1. Launch *VNC Viewer*.
2. Enter IP address in the server address field as defined in the listener object.




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


10.0.150.151 (Fudo) - VNC Viewer
Login
john_smith
Password
Log in

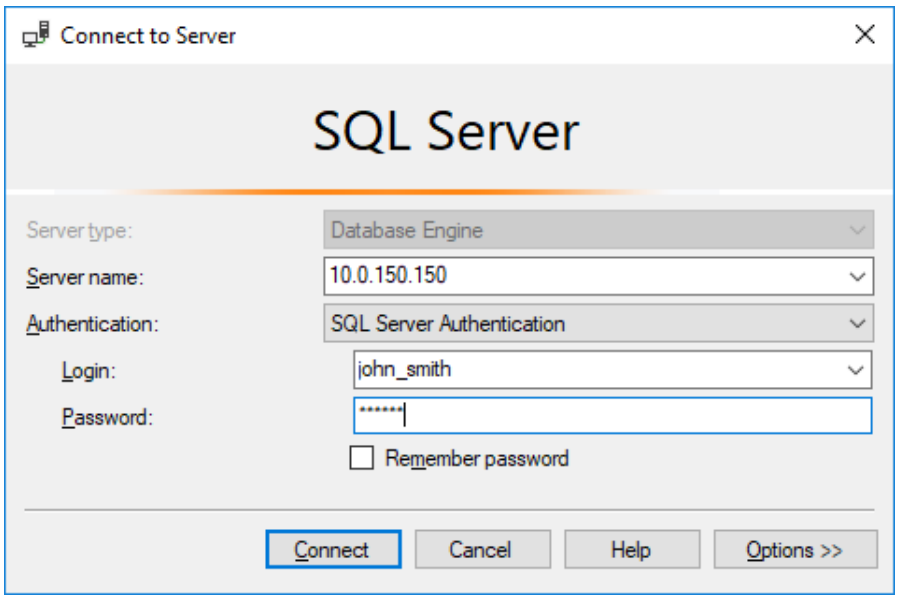


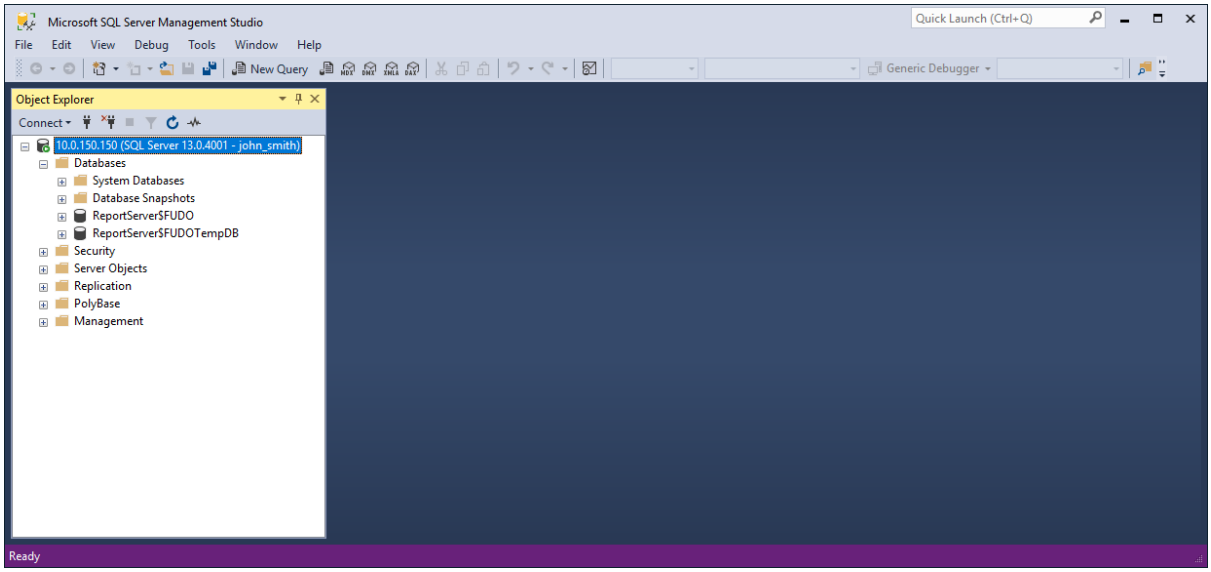

**Related topics:**

- *VNC*
- *Creating a VNC server*
- *Creating a VNC listener*

## 19.4 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*
- *Creating a MS SQL listener*

ROZDZIAŁ 20

# 4-Eyes authentication proxy service

4-Eyes proxy service facilitates communication between Wheel Fudo PAM and Fudo Mobile application enabling system administrators to accept/decline pending access requests.

## 20.1 Installing proxy service

1. Install FreeBSD version 10.
2. Add the following to the `/boot/loader.conf` file:

   ```
   pf_load="YES"
   ```
3. Run command:

   ```
   kldload pf
   ```

**Note:** Alternatively, recompile the operating system with `pf` support.

4. Upload `whlproxy` package and run:

   ```
   pkg add /path/to/whlproxy.txz
   ```

## 20.2 Initializing configuration using `whlproxyinit`

1. Run `whlproxyinit`.
2. Enter hostname.
3. Define network interface for communication with Wheel Fudo PAM.
4. Enter IP address along with the network mask, e.g. `10.0.8.201/16`.
5. Define network interface with access to the internet.

6. Enter IP address used for communication with the internet.
7. Enter port number for communication with Wheel Fudo PAM's API.
8. Enter default routing path.
9. Enter cluster's name.
10. Provide description.
11. Enter node's serial number.
12. Provide node's SSH key.

---

**Note:** Serial numbers and SSH keys can be found in the Fudo administration panel, in the *Settings* > *Network Configuration* view, *Proxy* tab, *Fudo SSH keys* section.

---

13. Enter `Y`, to add another cluster node.
14. Enter `n`, to finish proxy service configuration.

Exemplary configuration process' console output:

```
System configuration.
You can modify configuration files after initialization.

Hostname: whlproxy1
Interface with an access to Fudo: em0
Internal IP address and netmask for em0: 10.0.8.201/16
Interface with an access to the Internet: em0
Public IP address and netmask for em0: 10.0.8.201/16
Public API port for 10.0.8.201: 44300
Default route: 10.0.0.1

TLS certificate for the proxy.

Now you will be asked to provide your Fudo cluster configuration.

Enter cluster details.
Name (only digits and uppercase letters): TEST
Description: Test
Enter nodes' details.
Serial: 12345678
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAA...
Add another node? [Y/n]: n

Your Fudo cluster configuration was successfully created.
In order to manage your clusters in the future run whlproxyctl tool.

Restarting services...

Wheel Systems Proxy is ready to use.
```

## 20.3 Managing clusters using `whlproxyctl`

### 20.3.1 Adding a cluster

To add a cluster, run the following command:

```
whlproxyctl cluster add <cluster_name> <cluster_description>
```

---

**Note:** The name of the cluster must start with `F` character and can contain only uppercase letters or digits, e.g. `FJMSBND007`.

---

Example:

```
whlproxyctl cluster add F007 "Optional description"
```

### 20.3.2 Deleting a cluster

To delete a cluster, run the following command:

```
whlproxyctl cluster del <cluster_name>
```

Example:

```
whlproxyctl cluster del F007
```

### 20.3.3 Displaying cluster's details

To display cluster's details, run the following command:

```
whlproxyctl cluster show <cluster_name>
```

Example:

```
root@whlproxy1:~ # whlproxyctl cluster show F007
Name:           F007
GID:            1009
Description:    Optional description
Token:
Nodes:          F23456789
```

### 20.3.4 Listing clusters

To list clusters, run the following command:

```
whlproxyctl cluster list
```

Example:

```
root@whlproxy1:~ # whlproxyctl cluster list
F007
FKW
FTEST
```

## 20.4 Managing nodes using `whlproxyctl`

### 20.4.1 Adding a node to a cluster

To add a node to a cluster, run the following command:

```
whlproxyctl node add <node_name> <cluster_name> <ssh_key>
```

---

**Note:**

- Node's name must start with `F` followed by the serial number, e.g. `F23456789`.
- Serial numbers and SSH keys can be found in the Fudo administration panel, in the *Settings* > *Network Configuration* view, *Proxy* tab, *Fudo SSH keys* section.

---

Example:

```
whlproxyctl node add F23456789 F007 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAA...
```

### 20.4.2 Deleting a node

To delete a node, run the following command:

```
whlproxyctl node del <node_name>
```

Example:

```
whlproxyctl node del F007
```

### 20.4.3 Displaying node's details

To display detailed information on given node, run the following command:

```
whlproxyctl node show name
```

Example:

```
root@whlproxy1:~ # whlproxyctl node show F12345678
Name:           F12345678
UID:            1007
Cluster:        FTEST
Key:            ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAA...
Rules:
```

### 20.4.4 Listing nodes

To list nodes, run the following command:

```
whlproxyctl node list
```

Example:

```
root@whlproxy1:~ # whlproxyctl node list
F00000005
F12345678
F23456789
```

**Related topics:**

- *Adding a mobile device*
- *Removing paired mobile device*
- *Proxy servers configuration*

ROZDZIAŁ 21

# Troubleshooting

## 21.1 Booting up

| Problem | Symptoms and solution |
|---|---|
| Wheel Fudo PAM 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.<br>• Make sure that encryption key is properly connected.<br>• In case the problem is a result of unsuccessful system update, wait a few minutes. During that time, Wheel Fudo PAM will detect the problem and will restore previous system revision. |

## 21.2 Connecting to servers

| Problem | Symptoms and solution |
|---|---|
| Cannot connect to server | **Symptoms:**<br>• User cannot log in.<br>• Events log entry: *Authentication failed: Invalid username kowalski or password.* |
| | **Solution:**<br>• Verify that user definition exists in Wheel Fudo PAM database.<br>• Make the login credentials are correct.<br>• Make sure that the client software does not have outdated credentials stored.<br>• 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, Wheel Fudo PAM 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:**<br>• Verify that the server in question is properly configured (IP address, port number).<br>• Check if the server is reachable from Wheel Fudo PAM:<br>1. Log in to Wheel Fudo PAM administration panel.<br>2. Select *Settings* > *System*, *Diagnostics* tab.<br>3. Enter server address in the *Ping* section and execute command and test host's availability.<br>• Check if the server is reachable on given port number:<br>1. Log in to Wheel Fudo PAM administration panel.<br>2. Select *Settings* > *System*, *Diagnostics* tab.<br>3. Enter server address along with the port number in the *Netcat* section and execute command. |

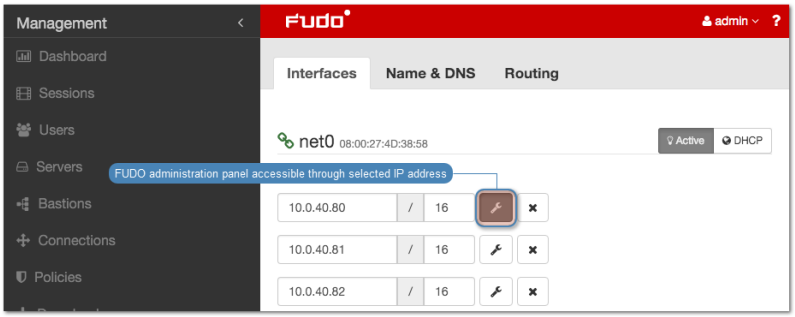
| Problem | Symptoms and solution |
|---|---|
| When logging in not all of the users see the Wheel Fudo PAM logon screen. | **Cause:**<br>• Credentials stored in RDP client result in users being automatically logged in to remote host.<br>• Credentials stored in RDP client, user is successfully authenticated against credentials stored so the Wheel Fudo PAM logon screen is not displayed. Next, Wheel Fudo PAM forwards user credentials to target server but they are no longer valid which results in Windows gina being displayed. |
| | **Symptoms:**<br>• Client software message: *Connection closed by remote host.*<br>• 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:**<br>• RDP client message: *Connection refused.*<br>• SSH client message: *ssh: connect to host 10.0.1.111 port 10011: Connection refused* |
| | **Cause:** server has been blocked. |
| | **Solution:** log in to Wheel Fudo PAM administration panel and unblock the server. |
| | |

| Problem | Symptoms and solution |
|---|---|
| Connection is terminated | **Symptoms:**<br>• User tries to log in to server monitored by Wheel Fudo PAM, after entering username and password session is immediately terminated.<br>• Events log entry: *TLS certificate verification failed.* |
| | **Solution:** |
| | Download new target host certificate in the *Target host* section. |
| | |
| | **Symptoms:**<br>• After entering username and password the connection is terminated.<br>• 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:**<br>• Cannot log in to server with error message *User user0 not allowed to connect to server.*<br>• 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:**<br>• After entering username and password, the screen freezes.<br>• Events log entry *Terminating session: User user0 (id=848388532111147010) is blocked.* |
| | **Cause:** user is blocked. |
| | **Solution:** log in to Wheel Fudo PAM 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 Wheel Fudo PAM and second time against the target host. |
| | |
| Cannot connect to server over RDP protocol | **Symptoms:**<br>• User connecting over RDP is disconnected a moment after establishing connection.<br>• 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:**<br>• 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 Wheel Fudo PAM or the user does not have sufficient access rights to connect to given server. |
| | **Solution:**<br>• Make sure that the server object exists.<br>• Add user to proper *safe* object. |

| Problem | Symptoms and solution |
|---|---|
| Cannot connect to Telnet5250 server using PC5250 klient revision 20091005 S/20111019 S | **Symptoms:** cannot establish connection to target host. |
| | **Cause:** in case of aforementioned client applications, Wheel Fudo PAM requires setting up additional objects to enable TCP traffic on ports number 449, 8470 and 8476. |
| | **Soluiton:**<br>• Add Telnet TN5250 server with default port number.<br>• Add three server objects with `TCP` protocol and following port numbers 449, 8470 and 8476.<br>• Add `TN5250` listener, in `Proxy` mode with default port number.<br>• Add three `TCP` listener objects, in `Proxy` mode, with port numbers 449, 8470 and 8476.<br>• Add `regular` account, define authentication parameters and assign it to the main TN5250 server definition.<br>• Add three `anonymous` accounts and assign each to one of supporting servers.<br>• Add safe and assign account with corresponding listeners. |

## 21.3 Logging to administration panel

| Problem | Symptoms and solution |
|---|---|
| Cannot log in to administration panel | • Make sure that Wheel Fudo PAM IP address is correct.<br>• Set Wheel Fudo PAM IP address from the console as described in the *Wheel Fudo PAM System documentation* in the *Network interfaces configuration* topic.<br>• Make sure that the IP address in question has the management access option enabled.<br>  |

## 21.4 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. |

## 21.5 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.<br>**Solution:** Contact technical support department. |

## 21.6 Trusted timestamping

| Problem | Symptoms and solution |
|---|---|
| Session are not timestamped | **Symptoms:**<br>• System log entry: *Timestamping service communication error.* |
| | **Reason:** Time-stamping host is not reachable by Fudo. |
| | **Solution:** Make sure that firewall settings allow traffic to the time-stamping service server.<br>• PWPW time-stamping service IP address: `193.178.164.5`<br>• KIR time-stamping service IP address: `http://www.ts.kir.com.pl/HttpTspServer` |
| | **Symptoms:**<br>• System log entry: *Unable to timestamp session.*<br>• No session timestamp icon on sessions list. |
| | **Reason:** Time-stamping service misconfiguration. |
| | **Solution:** Make sure that time-stamping service has been *configured properly*. |

## 21.7 Support mode

Support mode is enabled via terminal and it allows for remote accessing Fudo in case it does not boot up properly.

**Enabling support mode**

1. During the boot up, enter `1` and press the *Enter* key to confirm.

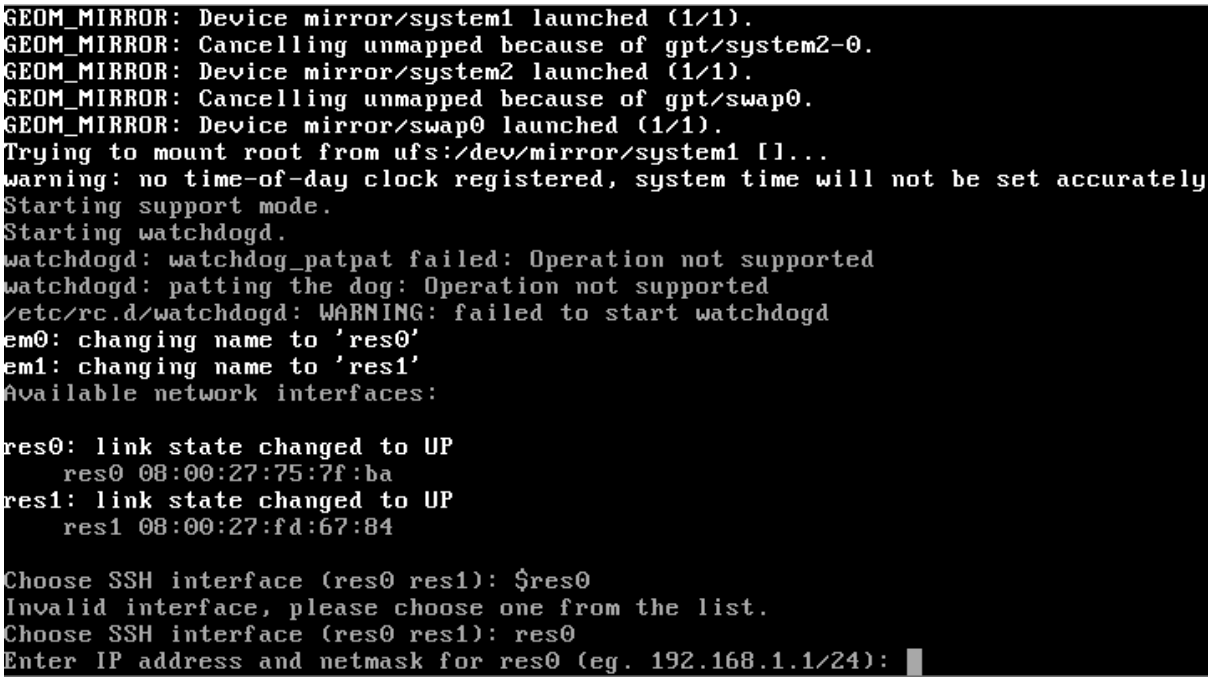
2. Select network interface.

**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): $
```

3. 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.




4. Enter the gateway's 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
```

- Use a combination of `[Ctrl]` + `C` keys to reset the network interface 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*

ROZDZIAŁ 22

# Frequently asked questions

*1. How many user sessions can be stored on Wheel Fudo PAM at once?*

*2. How Wheel Fudo PAM 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 Wheel Fudo PAM?*

*5. How to determine unauthorized access attempts to supervised servers?*

*6. Is it possible to hide the Wheel Fudo PAM 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 Wheel Fudo PAM?*

*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?*

**1. How many user sessions can be stored on Wheel Fudo PAM at once?**

Wheel Fudo PAM F1000 series is delivered with 24 TB of RAW hard drive space (18.2 TB usable) while the F3000 series appliances come with 96 TB of RAW storage space (71.8 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.
- Wheel Fudo PAM 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 Wheel Fudo PAM supports sessions archiving?**

All sessions are stored on Wheel Fudo PAM internal storage space. In addition to that, Wheel Fudo PAM 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 Wheel Fudo PAM?**

In case of the SSH protocol, Wheel Fudo PAM 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 Wheel Fudo PAM 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 Wheel Fudo PAM login screen when connecting over the RDP protocol?**

Hiding the Wheel Fudo PAM 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 Wheel Fudo PAM?**

Deleting a user object from an AD or an LDAP server requires performing the full synchronization to reflect those changes on Wheel Fudo PAM. 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 keystorkes 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.

ROZDZIAŁ 23

# Glossary

**ARP** Address Resolution Protocol - protocol used for mapping Internet layer addresses (IP addresses) to the physical - link layer addresses (MAC addresses).

**DNS** Domain Name Server - name server service which maps IP addresses to hosts names which are easier to remember.

**SSH** Secure Shell - networking protocol for secure communication with remote systems.

**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.

**Fingerprint** Characters string being a result of a hash function on input data, allowing to determine if the input data has been altered.

**RDP** Remote Desktop Protocol - remote access protocol to computer systems running Microsoft operating system.

**VNC** Remote access protocol to graphical user interfaces.

**RADIUS** Remote Authentication Dial In User Service - networking protocol used to control access to different services within IT infrastructure.

**Static password** Basic user authorization method which uses login and password combination to determine users's identity.

**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.

**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.

**LDAP** Lightweight Directory Access Protocol - distributed catalog services management and access protocol in IP networks.

**Active Directory** Users authorization and authentication in Windows domain.

**AD** Active Directory - users authorization and authentication in Windows domain.

**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).

**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.

**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.

**AAPM** AAPM (Application to Application Password Manager) module enables secure password exchange between applications.

**Efficiency Analyzer** Efficiency Analyzer module delivers statistical information on users' activity.

**PSM (Privileged Session Management)** PSM module is used for recording remote access sessions.

**server**

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

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

**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.

**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.

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

**hot-swap** Hot-swap mechanism enables replacing hardware components without the necessity to turn the system off.

**time policy** Time policy mechanism enables defining time periods during which users are allowed to connect to monitored hosts.

**password changer** Tool which enables facilitating automated password changing on a server.

**policy** Mechanism which enables defining patterns which in case of being detected will trigger defined actions.

**shared session** User session which was joined by another user.

**fudopv** AAPM module script, installed on the server, which enables secure password exchange between applications.

**SSH access** Service access to Fudo PAM over SSH protocol.

**VLAN** Virtual networks mechanism, enabling separation of broadcast domains.

**DHCP** Mechanism for dynamic IP addressing management i LAN networks.

**timestamp** Session data hash value, which enables verifying that the data has not been modified.

**external authentication server** Server storing user data used for verification of user login credentials when connecting to Fudo PAM or the monitored server.

**passwords repository** Passwords repository manages password to privileged accounts on monitored hosts.

**data retention** Data retention mechanism automatically deletes session data after define time period transpires.

**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.

**RDP connections broker** Remote sessions management mechanism for server farms.

**PSM** PSM (Privileged Session Monitoring) module enables monitoring and recording remote access sessions.

**WWN** World Wide Name - unique object identifier in external storage solutions.

**OCR** Optical Character Recognition - image processing for identifying and indexing text.

# Index


## A

AAPM, **458**
account, **458**
Active Directory, **457**
AD, **457**
administration
    configuration export/import, 357
anonymous safe, **458**
API
    users, 138
ARP, **457**

## C

CERB, **457**
CIDR, **458**
Citrix
    servers, 159
Citrix StoreFront
    protocol, 7
    protocols, 7
configuration
    Network configuration, 309, 318, 319
    notifications, 327
    users synchronization, 151
connection mode
    bastion, 17
    gateway, 16
    proxy, 17
    transparent, 16
creating
    servers, 159

## D

data retention, **459**
deleting
    servers, 190
deployment scenario
    bridge, 15
    forced routing, 15
DHCP, **459**
DNS, **457**
dynamic
    servers, 185

## E

editing
    servers, 187
Efficiency Analyzer, **458**
external authentication server, **459**

## F

Fingerprint, **457**
fudopv, **458**

## H

heartbeat, **458**
hot-swap, **458**
HTTP
    protocol, 7
    protocols, 7
    servers, 161

## I

ICA
    protocol, 7
    protocols, 7
    servers, 163

## L

LDAP, **457**
listener, **458**

## M

Modbus
    protocol, 8
    protocols, 8
    servers, 165
MS SQL

servers, 167
MS SQL (*TDS*)
protocol, 8
protocols, 8
MySQL
protocol, 9
protocols, 9
servers, 168

## N

Network configuration
IP labels, 318
network bypass configuration, 319
network interface configuration, 309
network configuration
routing, 319

## O

OCR, **459**
Oracle
protocol, 9
protocols, 9
servers, 170

## P

password changer, **458**
passwords repository, **459**
policy, **458**
protocol
Citrix StoreFront, 7
HTTP, 7
ICA, 7
Modbus, 8
MS SQL (*TDS*), 8
MySQL, 9
Oracle, 9
RDP, 10
SSH, 11
TCP, 13
Telnet, 12
Telnet 3270, 11
Telnet 5250, 12
VNC, 12
X11, 13
protocols
Citrix StoreFront, 7
HTTP, 7
ICA, 7
Modbus, 8
MS SQL (*TDS*), 8
MySQL, 9
Oracle, 9
RDP, 10
SSH, 11
TCP, 13
Telnet, 12
Telnet 3270, 11
Telnet 5250, 12
VNC, 12
X11, 13
PSM, **459**
PSM (*Privileged Session Management*), **458**
Public key, **457**

## R

RADIUS, **457**
RDP, **457**
RDP
protocol, 10
protocols, 10
servers, 171
RDP connections broker, **459**
RDP connections broker, 393
redundancy group, **459**

## S

safe, **458**
server, **458**
servers, **458**
servers
Citrix, 159
creating, 159
deleting, 190
dynamic, 185
editing, 187
HTTP, 161
ICA, 163
Modbus, 165
MS SQL, 167
MySQL, 168
Oracle, 170
RDP, 171
ssh, 173
TCP, 183
Telnet, 175
Telnet 3270, 177
Telnet 5250, 179
VNC, 181
sessions
commenting, 275
filtering, 262
play and preview, 266
shared session, **458**
SSH, **457**

SSH
    protocol, 11
    protocols, 11
ssh
    servers, 173
SSH access, 458
Static password, 457
Syslog, 457

## T

TCP
    protocol, 13
    protocols, 13
    servers, 183
Telnet
    protocol, 12
    protocols, 12
    servers, 175
Telnet 3270
    protocol, 11
    protocols, 11
    servers, 177
Telnet 5250
    protocol, 12
    protocols, 12
    servers, 179
time policy, 458
timestamp, 459

## U

user, 458
users
    access rights, 138
    API, 138
    roles, 138
users synchronization, 151
    configuration, 151

## V

VLAN, 458
VNC, 457
VNC
    protocol, 12
    protocols, 12
    servers, 181

## W

WWN, 459

## X

X11
    protocol, 13
    protocols, 13