



Wheel Fudo PAM 3.5 - System
Documentation

Release is not supported

Wheel Systems

September 09, 2021

1	General information	1
1.1	About documentation	1
2	System overview	3
2.1	PSM	3
2.1.1	Citrix StoreFront (HTTP)	3
2.1.2	HTTP	4
2.1.3	ICA	4
2.1.4	Modbus	4
2.1.5	MS SQL (TDS)	5
2.1.6	MySQL	5
2.1.7	Oracle	5
2.1.8	RDP	6
2.1.9	SSH	6
2.1.10	Telnet 3270	7
2.1.11	Telnet 5250	7
2.1.12	Telnet	7
2.1.13	VNC	8
2.1.14	X11	8
2.2	AAPM (Application to Application Password Manager)	9
2.3	Secret manager	9
2.4	Efficiency Analyzer	9
2.5	User portal	10
2.6	Data model	10
2.7	Deployment scenarios	12
2.8	Connection modes	13
2.9	User authentication methods and modes	15
2.10	Security measures	17
2.10.1	Data encryption	17
2.10.2	Backups	18
2.10.3	Permissions	18
2.10.4	Sandboxing	18
2.10.5	Reliability	18
2.10.6	Cluster configuration	18
3	System deployment	21

3.1	Requirements	21
3.2	Hardware overview	21
3.3	System initiation	22
4	Quick start	29
4.1	SSH	29
4.2	RDP	35
4.3	Telnet	43
4.4	Telnet 5250	49
4.5	MySQL	57
4.6	HTTP	64
4.7	Citrix	70
4.7.1	ICA	71
4.7.1.1	Prerequisites	71
4.7.1.2	Configuration	71
4.7.1.3	Creating .ica file with connection parameters	76
4.7.1.4	Connecting to remote resource	77
4.7.1.5	Viewing user session	77
4.7.2	ICA via Citrix StoreFront	77
4.7.2.1	Prerequisites	78
4.7.2.2	Configuration	78
4.7.2.3	Connecting to remote resource	85
4.7.2.4	Viewing user session	86
5	Users	89
5.1	Creating a user	90
5.2	Editing a user	94
5.3	Blocking a user	96
5.4	Unblcoking a user	97
5.5	Deleting a user	98
5.6	Roles	99
5.7	Users synchronization	100
6	Servers	105
6.1	Creating a server	105
6.1.1	Static server	106
6.1.1.1	Creating a Citrix server	106
6.1.1.2	Creating an HTTP server	107
6.1.1.3	Creating an ICA server	109
6.1.1.4	Creating a Modbus server	112
6.1.1.5	Creating a MS SQL server	113
6.1.1.6	Creating a MySQL server	115
6.1.1.7	Creating an Oracle server	117
6.1.1.8	Creating an RDP server	119
6.1.1.9	Creating an SSH server	121
6.1.1.10	Creating a Telnet server	123
6.1.1.11	Creating a Telnet 3270 server	125
6.1.1.12	Telnet 5250 server	127
6.1.1.13	Creating a VNC server	129
6.1.2	Dynamic server	130
6.1.2.1	Creating a dynamic servers group	130
6.1.2.2	Adding a single host to a servers group	131

6.2	Editing a server	132
6.3	Blocking a server	133
6.4	Unblocking a server	134
6.5	Deleting a server	135
6.5.1	Deleting a static server definition	135
6.5.2	Deleting a dynamically added host	135
7	Accounts	137
7.1	Creating an account	138
7.1.1	Creating an <i>anonymous</i> account	138
7.1.2	Creating a <i>forward</i> account	139
7.1.3	Creating a <i>regular</i> account	142
7.2	Editing an account	147
7.3	Blocking an account	148
7.4	Unblocking an account	148
7.5	Deleting an account	149
8	Safes	151
8.1	Creating a safe	152
8.2	Editing a safe	155
8.3	Blocking a safe	156
8.4	Unblocking a safe	156
8.5	Deleting a safe	157
9	Listeners	159
9.1	Creating a listener	160
9.1.1	Creating a Citrix listener	160
9.1.2	Creating a HTTP listener	161
9.1.3	Creating an ICA listener	163
9.1.4	Creating a Modbus listener	164
9.1.5	Creating a MySQL listener	166
9.1.6	Creating an Oracle listener	167
9.1.7	Creating an RDP listener	168
9.1.8	Creating an SSH listener	170
9.1.9	Creating a MS SQL listener	172
9.1.10	Creating a Telnet listener	173
9.1.11	Creating a Telnet 3270 listener	174
9.1.12	Creating a VNC listener	176
9.2	Editing a listener	177
9.3	Blocking a listener	178
9.4	Unblocking a listener	179
9.5	Deleting a listener	180
10	Password changers	183
10.1	Password changer policy	183
10.1.1	Defining a password changer policy	183
10.1.2	Editing a password changer policy	184
10.1.3	Deleting a password changer policy	185
10.2	Custom password changers	185
10.2.1	Defining a custom password changer	185
10.2.2	Editing a custom password changer	187
10.2.3	Deleting a custom password changer	187

10.3	Setting up password changing on a Unix system	187
11	Policies	191
12	Sessions	197
12.1	Filtering sessions	198
12.1.1	Defining filters	198
12.1.2	Full text search	200
12.1.3	Managing user defined filter definitions	201
12.2	Viewing sessions	202
12.3	Viewing live sessions	205
12.4	Pausing connection	205
12.5	Terminating connection	206
12.6	Joining live session	208
12.7	Sharing sessions	208
12.8	Commenting sessions	211
12.9	Exporting sessions	213
12.10	Deleting sessions	215
12.11	OCR processing sessions	215
12.12	Timestamping selected sessions	217
13	Reports	219
14	Efficiency analyzer	223
14.1	Overview	223
14.2	Sessions analysis	224
14.3	Activity comparison	226
15	Administration	227
15.1	System	227
15.1.1	Date and time	227
15.1.2	SSL certificate	229
15.1.3	Deny new connections	230
15.1.4	SSH access	231
15.1.5	Reset account	232
15.1.6	Sensitive features	233
15.1.7	System update	234
15.1.7.1	Updating system	235
15.1.7.2	Running update check	235
15.1.7.3	Deleting upgrade snapshot	236
15.1.8	License	237
15.1.9	Diagnostics	237
15.2	Network settings	238
15.2.1	Network interfaces configuration	239
15.2.1.1	Managing physical interfaces	239
15.2.1.2	Defining IP address using system console	242
15.2.1.3	Setting up a network bridge	246
15.2.1.4	Setting up virtual networks (VLANs)	246
15.2.1.5	Setting up LACP link aggregation	247
15.2.2	Labeled IP addresses	248
15.2.3	Bypasses configuration	249
15.2.4	Routing configuration	250

15.2.5	DNS servers configuration	251
15.3	Notifications	253
15.4	Trusted timestamping	255
15.5	External authentication	256
15.6	External passwords repositories	258
15.6.1	CyberArk Enterprise Password Vault	258
15.6.2	Hitachi ID Privileged Access Manager	259
15.6.3	Lieberman Enterprise Random Password Manager	259
15.6.4	Thycotic Secret Server	260
15.7	Resources	261
15.8	System version restore	263
15.9	System restart	264
15.10	SNMP	265
15.10.1	Configuring SNMP	265
15.10.2	SNMP MIBs	265
15.10.3	Wheel Fudo PAM specific SNMP extensions	266
15.11	Backups and retention	268
15.12	External storage	269
15.12.1	Configuring external storage	270
15.12.2	Expanding external storage device	271
15.13	Exporting/importing system configuration	271
15.13.1	Exporting system configuration	272
15.13.2	Importing system configuration	272
15.14	Cluster configuration	273
15.14.1	Initiating cluster	273
15.14.2	Adding cluster nodes	275
15.14.3	Editing cluster nodes	277
15.14.4	Deleting cluster nodes	277
15.14.5	Forcing full data synchronization	278
15.14.6	Redundancy groups	279
15.15	Events log	284
15.16	Integration with CERB server	285
15.17	System maintenance	295
15.17.1	Backing up encryption keys	295
15.17.2	Monitoring system condition	299
15.17.3	Hard drive replacement	300
16	Reference information	303
16.1	RDP connections broker	303
16.2	Error codes	304
16.3	Fudo 2.2 to Fudo 3.0 parameters mapping	307
16.3.1	Connection	308
16.3.2	Server	309
16.4	Data model migration from Wheel Fudo PAM version 2.2 to 3.0	310
16.4.1	Server	310
16.4.2	Safe (previously <i>connection</i>)	310
16.4.3	Account (previously <i>login credentials</i>)	311
16.4.4	Listener (previously <i>bastion</i> or part of a server)	311
16.4.5	Sessions	312
16.5	Supported protocols	312
16.5.1	Citrix StoreFront (HTTP)	312

16.5.2	HTTP	312
16.5.3	ICA	313
16.5.4	Modbus	313
16.5.5	MS SQL (TDS)	313
16.5.6	MySQL	313
16.5.7	Oracle	314
16.5.8	RDP	314
16.5.9	SSH	315
16.5.10	Telnet	315
16.5.11	Telnet 3270	315
16.5.12	Telnet 5250	316
16.5.13	VNC	316
16.5.14	X11	316
16.6	ICA configuration file	316
16.6.1	Plik ICA do połączeń bez TLS	317
16.6.2	Plik ICA do połączeń bez TLS	317
17	AAPM (Application to Application Password Manager)	319
17.1	Overview	319
17.2	<i>fudopv</i>	319
17.3	API interface	327
18	Service Now	329
18.1	Configuration	329
18.2	Requesting access to safe	330
18.3	Granting access	332
19	Troubleshooting	335
19.1	Booting up	335
19.2	Connecting to servers	336
19.3	Logging to administration panel	340
19.4	Session playback	340
19.5	Cluster configuration	341
20	Frequently asked questions	343
21	Glossary	347
	Index	351

1.1 About documentation

Documentation Structure

1. *General information*

This chapter covers system overview, data model and user authorization methods.

2. *Configuration*

This chapter covers detailed configuration procedures.

3. *Sessions*

This chapter contains information on stored access sessions.

4. *Productivity analysis*

This chapter describes the productivity analysis module.

5. *Administration*

This chapter contains administration procedures.

6. *Reference information*

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

7. *Troubleshooting*

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

8. *Frequently asked questions*

This chapter contains frequently requested information about Wheel Fudo PAM.

9. *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 related with described topic, e.g. suggestion concerning given procedure step; additional conditions which have to be met.

<p>Warning: Warning. Essential information concerning system's operation. Not adhering to this information may have irreversible consequences.</p>

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.

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.

Supported protocols and systems

2.1.1 Citrix StoreFront (HTTP)

Supported connection modes:

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

Notes:

- 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.

2.1.2 HTTP

Supported connection modes:

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

Notes:

- 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.

2.1.3 ICA

Supported connection modes:

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

Supported client applications:

- Citrix Receiver.

2.1.4 Modbus

Supported connection modes:

- *Gateway*,
- *Proxy*,

- *Transparent.*

Notes:

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

2.1.5 MS SQL (TDS)

Supported connection modes:

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

Supported client applications:

- SQL Server Management Studio,
- sqsh.

2.1.6 MySQL

Supported connection modes:

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

Supported client applications:

- Official MySQL client,
- PyMySQL libraries for Python.

Notes:

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

2.1.7 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:

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

2.1.8 RDP

Supported connection modes:

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

Supported client applications:

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

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.
- RemoteApp support is in development.

2.1.9 SSH

Supported connection modes:

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

Supported features:

- Connections multiplexing,
- SCP,
- Ports redirection.

Notes:

- SFTP sessions playback is not supported,

- SSH keys forwarding is not supported.

2.1.10 Telnet 3270

Supported connection modes:

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

Notes:

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

Supported client applications:

- IBM Personal Communications,
- c3270.

2.1.11 Telnet 5250

Supported connection modes:

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

Notes:

- User must authenticate twice - first against Fudo and then against the target host.
- It is not possible to join a Telnet 5250 session.

Supported client applications:

- IBM Personal Communications,
- tn5250.

2.1.12 Telnet

Supported connection modes:

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

Notes:

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

2.1.13 VNC

Supported connection modes:

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

Supported client applications:

- TightVNC,
- RealVNC.

2.1.14 X11

X11 protocol is supported within the SSH protocol.

Supported servers:

- Xorg,
- Xming,
- XQuartz.

The PSM module supports following system configurations:

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

Related topics:

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

2.2 AAPM (Application to Application Password Manager)

AAPM module enables secure passwords exchange between applications.

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

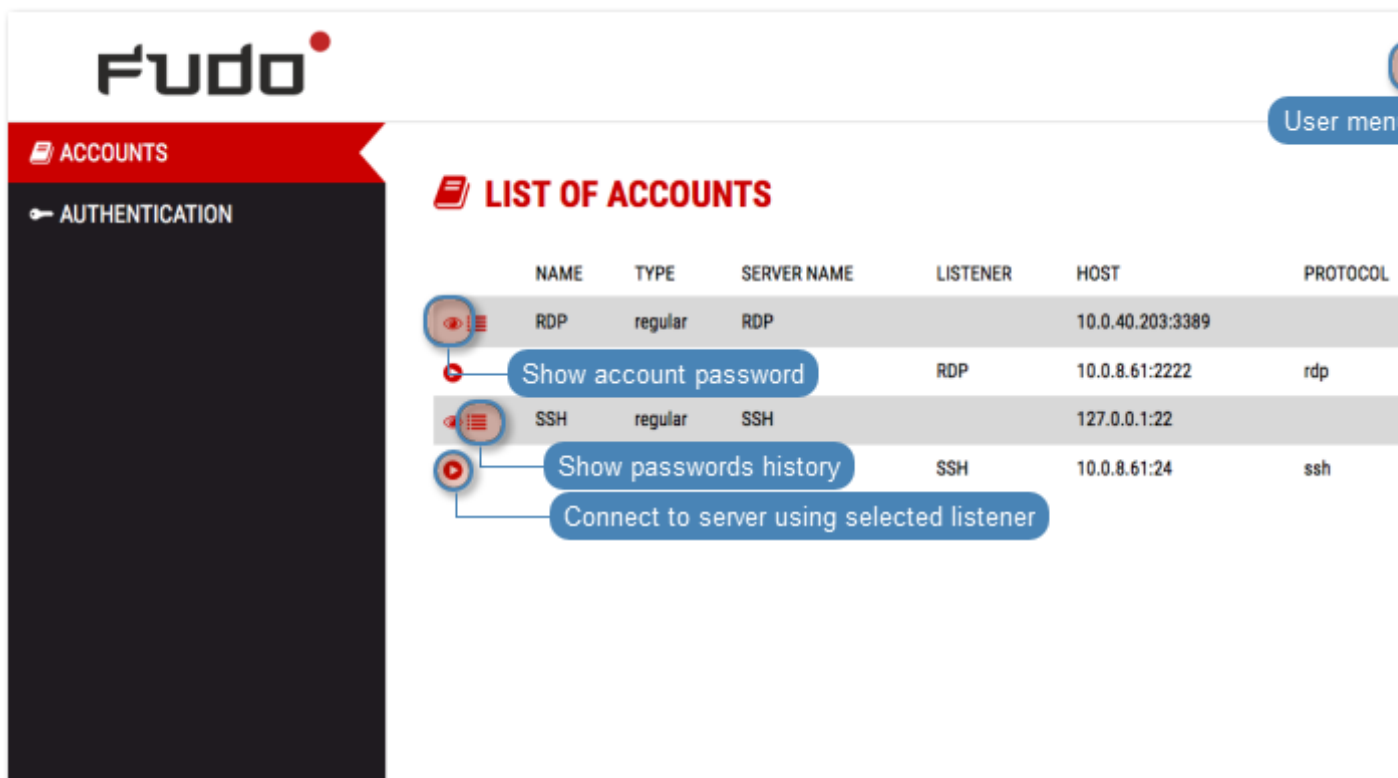
Efficiency Analyzer module tracks users' actions and provides precise information on their activity and idle times.

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 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, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

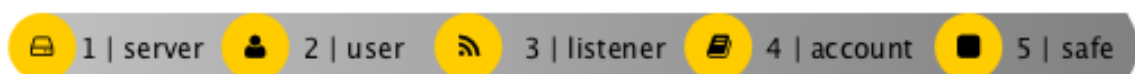
Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

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.

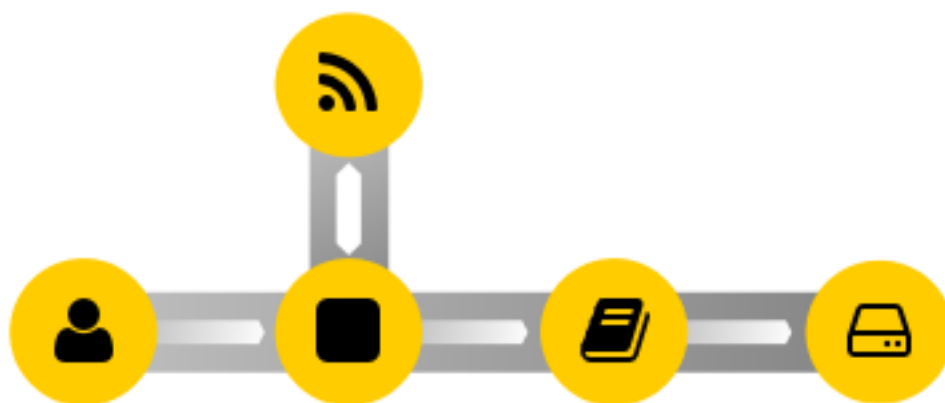
Listener determines server connection mode (proxy, gateway, transparent, bastion) as well as its specifics.

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



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:

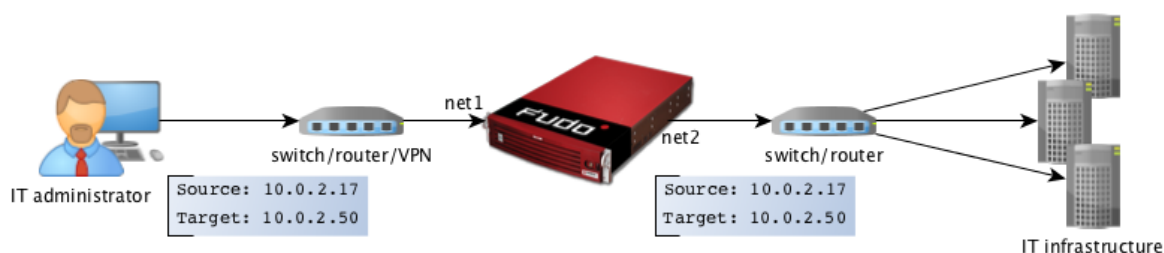
- [System overview](#)
- [User authorization methods and modes](#)
- [Quick start](#)

2.7 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.



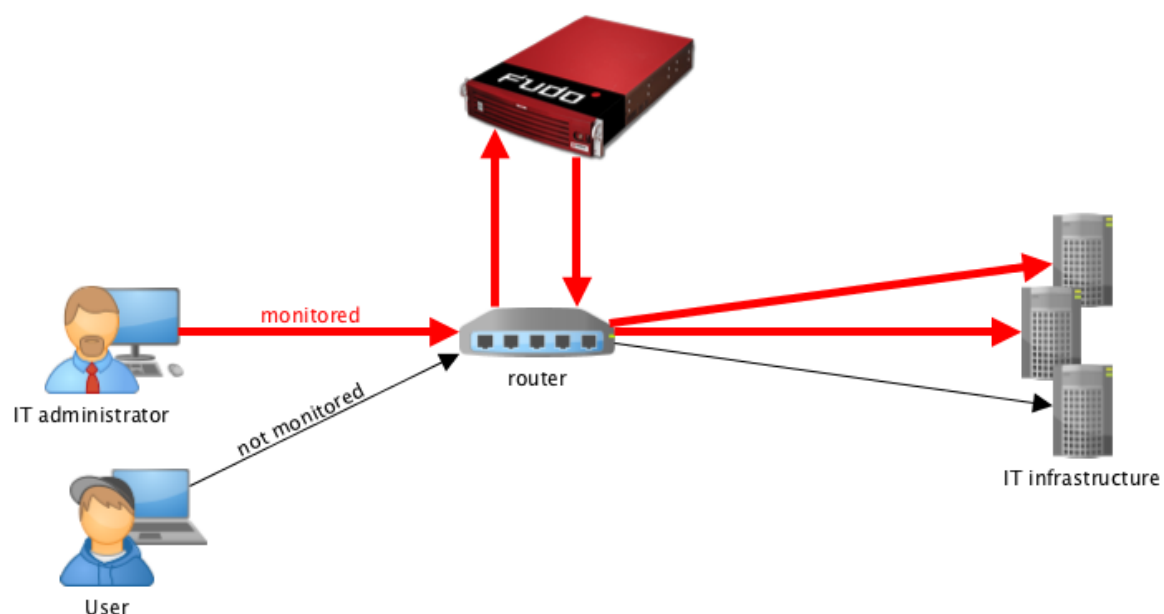
Mediating packages transfer, Wheel Fudo PAM preserves source IP address when forwarding requests to destination servers.

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.

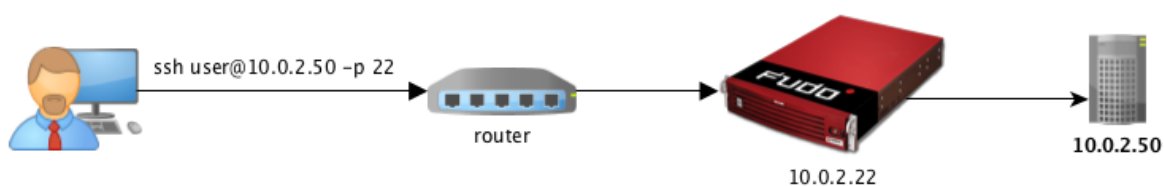
Related topics:

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

2.8 Connection modes

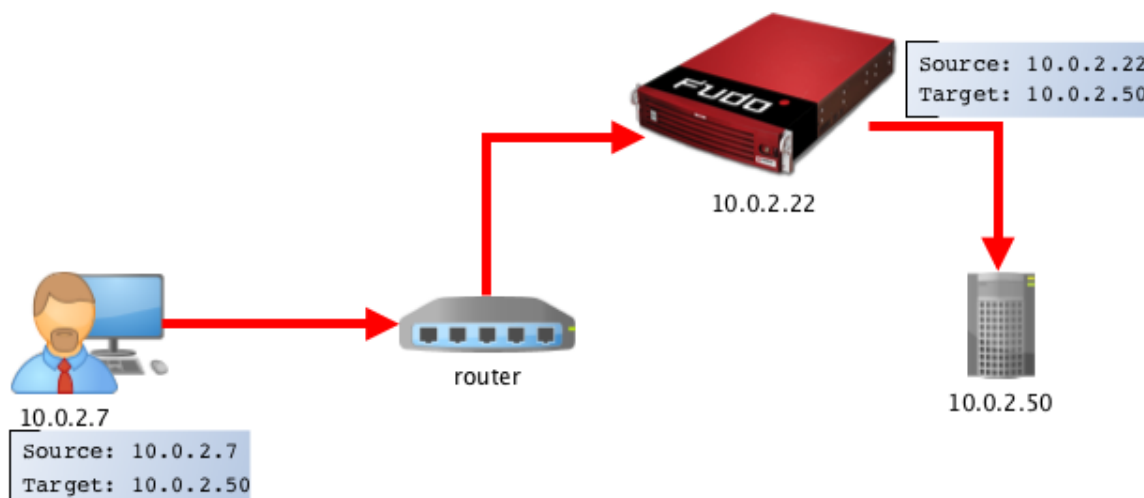
Transparent

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



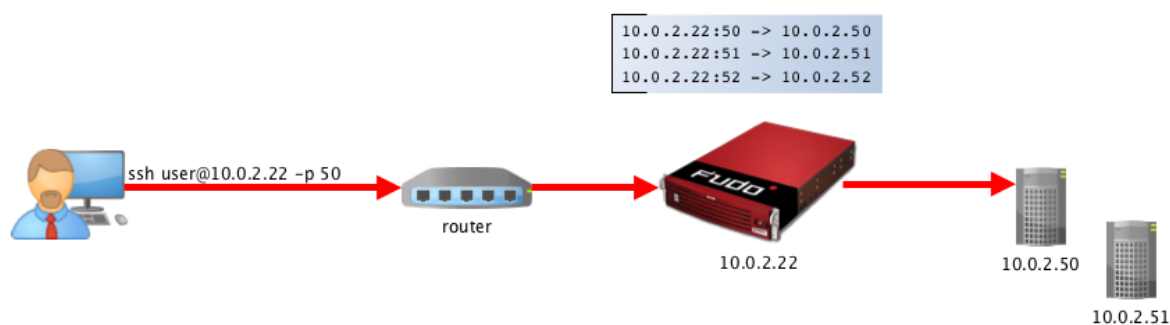
Gateway

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

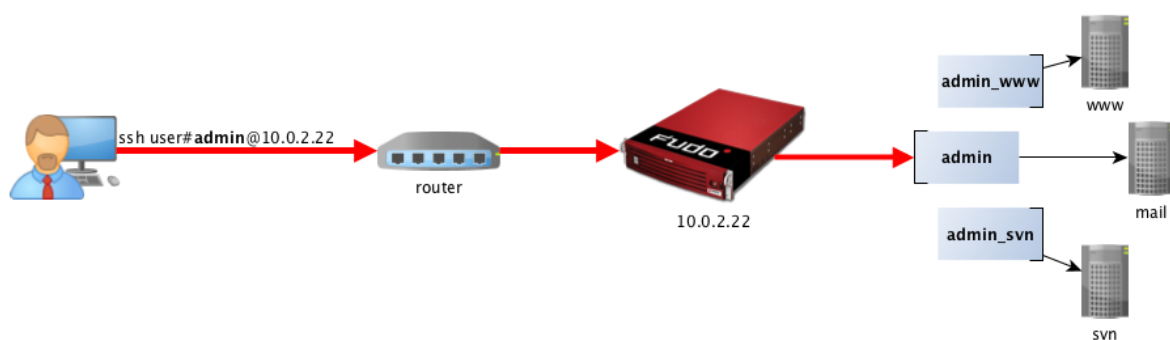
In proxy mode, administrator connects to destination server using combination of Wheel Fudo PAM IP address and unique port number assigned to given server. Uniqueness of this combination enables establishing connection with a particular resource.



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 is specified within the string identifying the user, e.g. `ssh john_smith#admin@10.0.0.8`. 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 or Telnet 3270 protocols.
 - In case the specified account is not found, Wheel Fudo PAM will try to match the name with a server object.
-

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*

2.9 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.

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.

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.

Authentication with login substitution

In this authentication mode, Fudo substitutes login with a value defined in connection and forwards the password provided by user.



Related topics:

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

2.10 Security measures

2.10.1 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.

2.10.2 Backups

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

2.10.3 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.

2.10.4 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.

2.10.5 Reliability

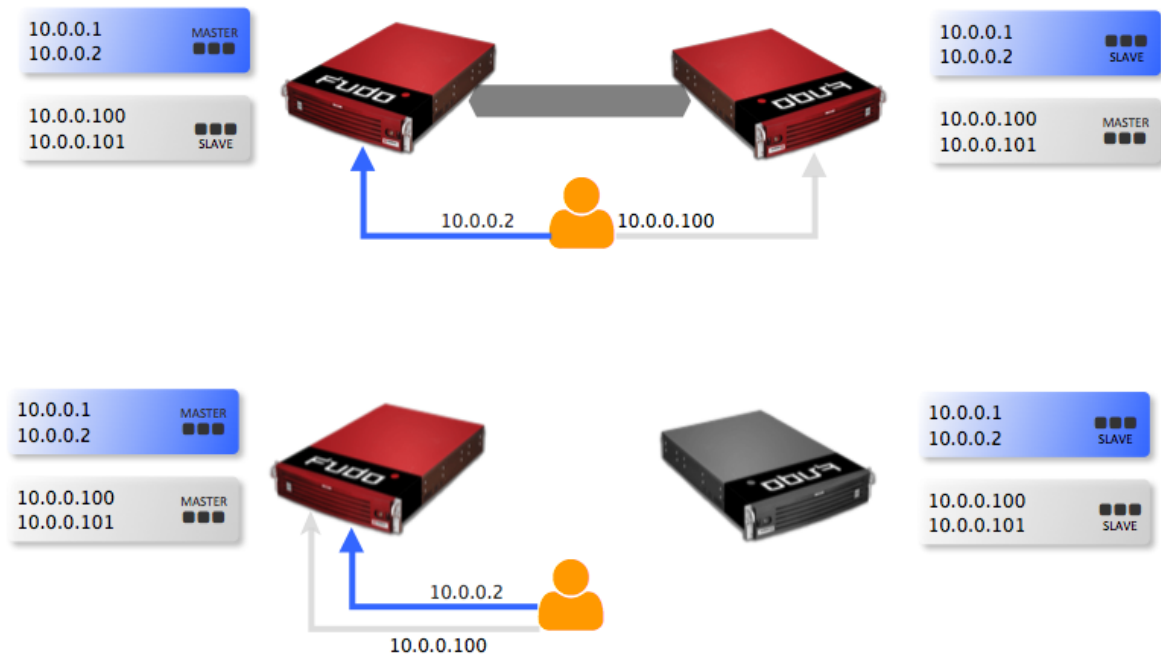
System hardware configuration is optimized to deliver high performance and high availability.

2.10.6 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.

<p>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.</p>

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*

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 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

Wheel Fudo PAM is delivered in a 2U 19" rack server case.

Front panel view



Hard drive bays

Front panel covers hard drives in hot swap enclosures allowing for removing them without having to shutdown the system.



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 connecting 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*.

```
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: █
```

3. Enter administrator account password 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:
```

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*.

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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0

*** FUDO configuration utility ***

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

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

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

Related topics:

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

4.1 SSH

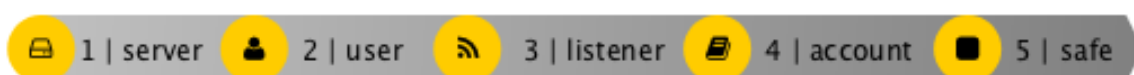
This chapter contains an example of a basic Wheel Fudo PAM configuration, to monitor SSH access to a remote server. In this scenario, the user connects to the remote server over the *SSH* protocol and logs in to the Wheel Fudo PAM using an individual login and password combination (`john_smith/john`).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



Prerequisites

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

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
<i>General</i>	
Name	ssh_server
Blocked	
Protocol	SSH
Description	
<i>Permissions</i>	
Granted users	
<i>Destination host</i>	
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, 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
<i>General</i>	
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	
<i>Permissions</i>	
Granted users	
<i>Authentication</i>	
Type	Password
Password	john
Repeat password	john

4. Click *Save*.

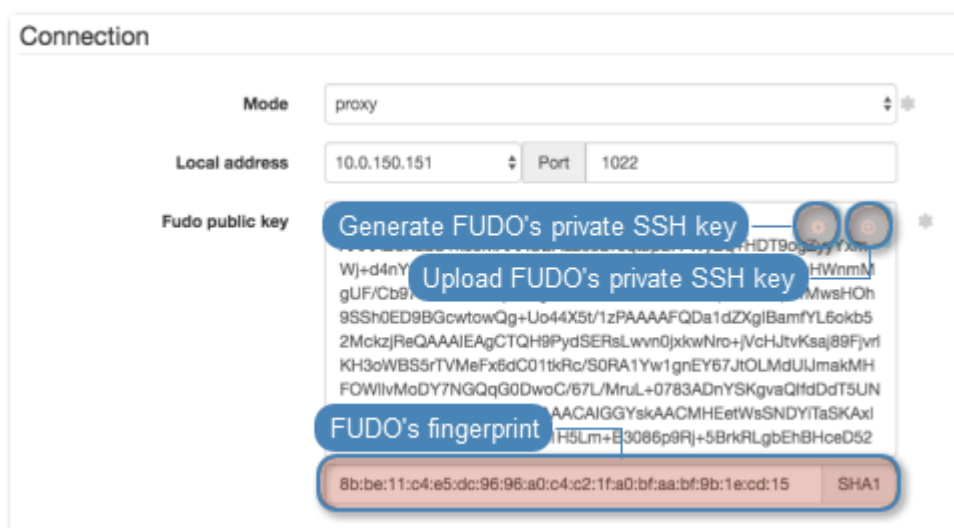
Adding a listener

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
<i>General</i>	
Name	ssh_listener
Blocked	
Protocol	SSH
<i>Permissions</i>	
Granted users	
<i>Connection</i>	
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
<i>General</i>	
Name	admin_ssh_server
Account type	regular
Session recording	complete
OCR sessions	
Delete session data after	61 days
<i>Permissions</i>	
Granted users	
<i>Server</i>	
Server	ssh_server
<i>Credentials</i>	
Domain	
login	root
Replace secret with	with password
Password	password
Repeat password	password
Password change policy	Static, without restrictions
Replace secret	
<i>Password changer</i>	
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:

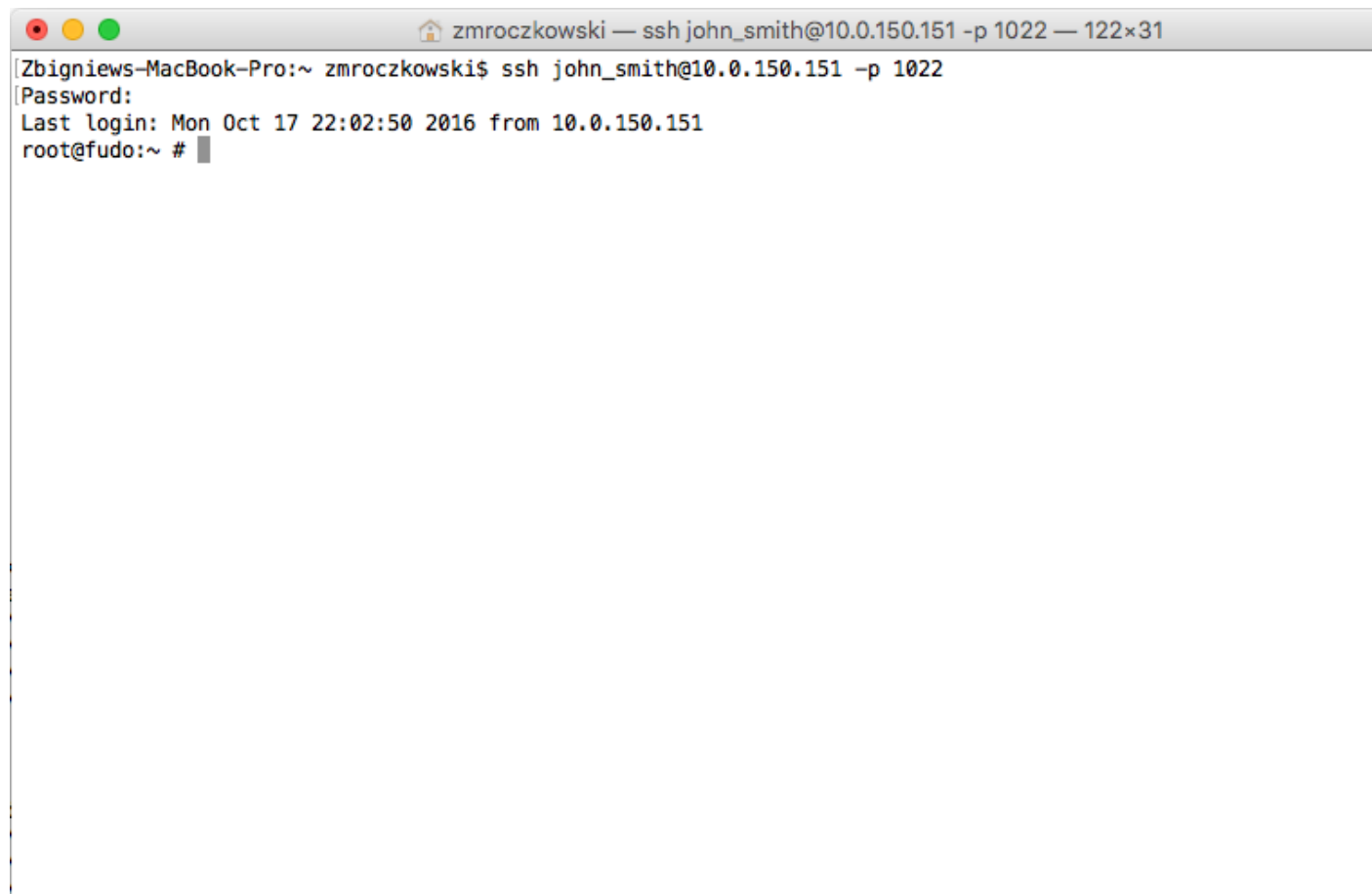
Parameter	Value
<i>General</i>	
Name	ssh_safe
Notifications	
Ask for login reason	
Policies	
Users	john_smith
<i>Protocol functionality</i>	
RDP	
SSH	
VNC	
<i>Accounts</i>	
admin_ssh_server	ssh_listener

4. Click *Save*.

Establishing connection

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

Example:



```

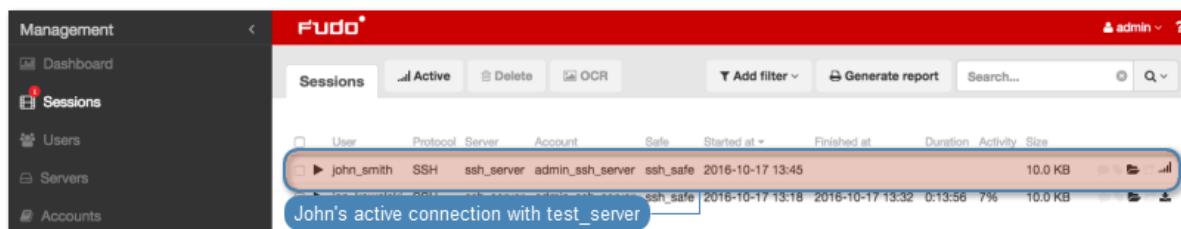
zmroczkowski — ssh john_smith@10.0.150.151 -p 1022 — 122x31
Zbigniews-MacBook-Pro:~ zmroczkowski$ ssh john_smith@10.0.150.151 -p 1022
[Password:
Last login: Mon Oct 17 22:02:50 2016 from 10.0.150.151
root@fudo:~ #
    
```

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.

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. Click *Active*.
5. Find *John Smith's* session and click the playback icon.



Related topics:

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

4.2 RDP

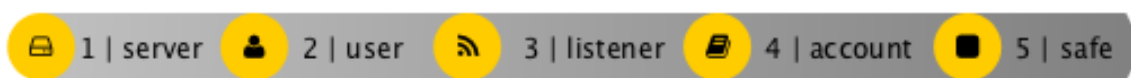
This chapter contains an example of a basic Wheel Fudo PAM configuration, to monitor RDP access to a remote server. In this scenario, the user connects to the remote server over the *RDP* protocol and logs in to the Wheel Fudo PAM using an individual login and password combination (*john_smith/john*).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



Prerequisites

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

Configuration



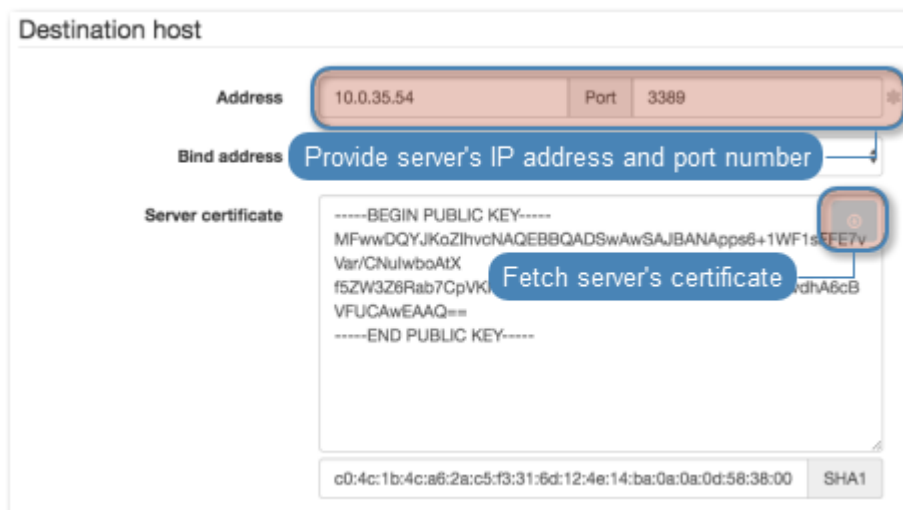
Adding a server

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	
<i>Permissions</i>	
Granted users	
<i>Destination host</i>	
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, 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
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	
<i>Permissions</i>	
Granted users	
<i>Authentication</i>	
Type	Password
Password	john
Repeat password	john

4. Click *Save*.

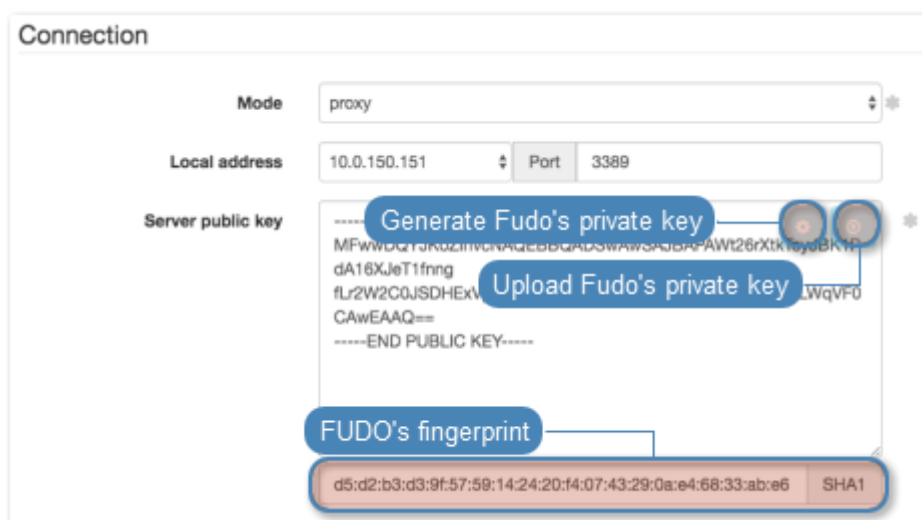
Adding a listener

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
<i>General</i>	
Name	rdp_listener
Blocked	
Protocol	RDP
Security	Standard RDP Security
Announcement	
<i>Permissions</i>	
Granted users	
<i>Connection</i>	
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
<i>General</i>	
Name	admin_rdp_server
Blocked	
Type	regular
Session recording	all
OCR sessions	
OCR Language	English
Delete session data after	61 days
<i>Permissions</i>	
Granted users	
<i>Server</i>	
Server	rdp_server
<i>Credentials</i>	
Domain	
Login	administrator
Replace secret with	with password
Password	password
Repeat password	password
Password change policy	Static, without restrictions
<i>Password changer</i>	
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*.

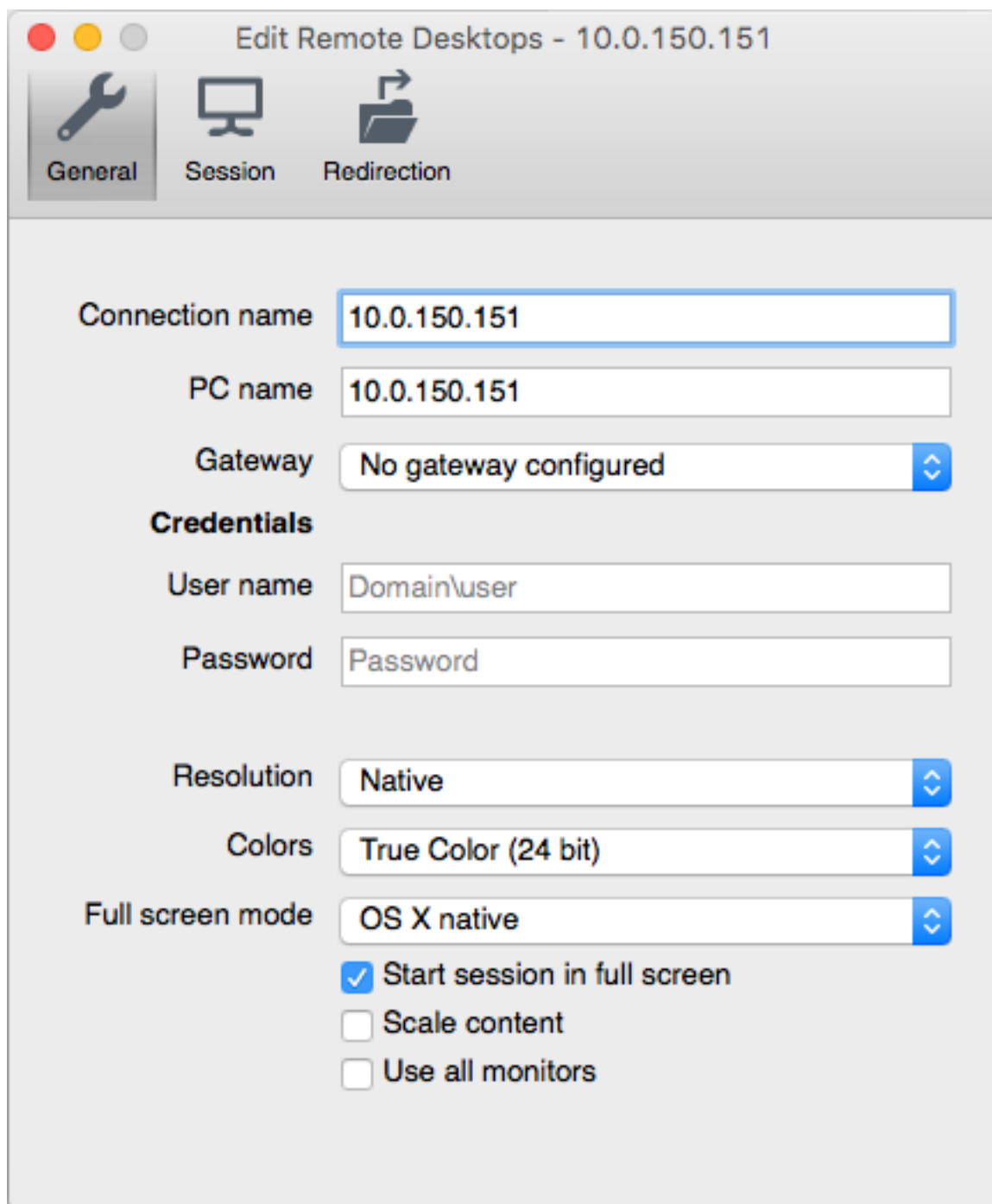
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
<i>General</i>	
Name	rdp_safe
Blocked	
Login reason	
Notifications	
Policies	
Users	john_smith
<i>Protocol functionality</i>	
RDP	
SSH	
VNC	
<i>Accounts</i>	
admin_rdp_server	rdp_listener

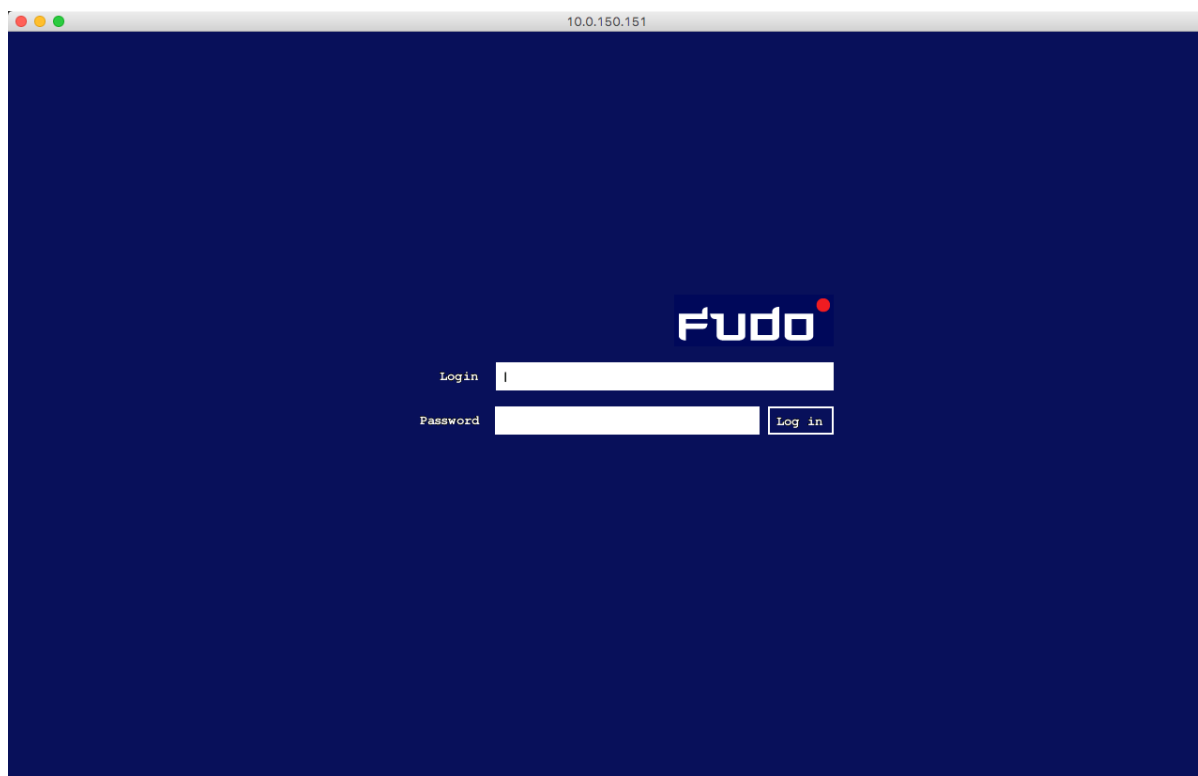
4. Click *Save*.

Establishing an RDP connection with a remote host

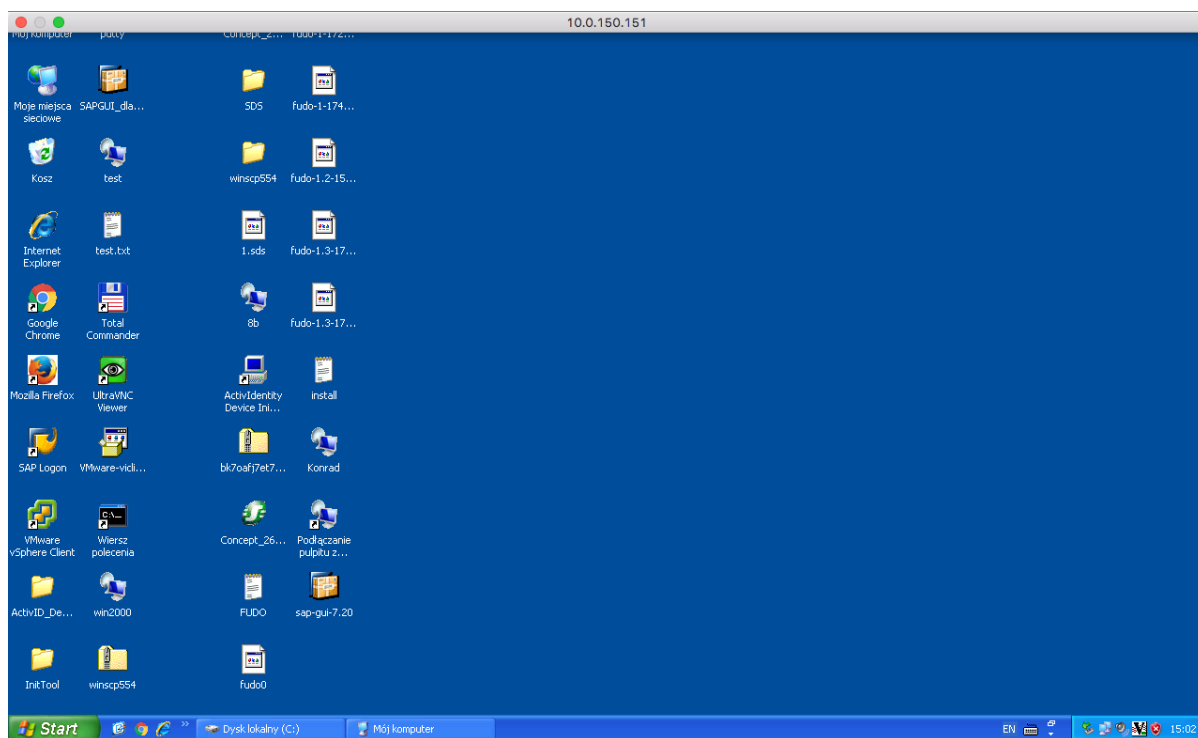
1. Launch RDP client of your choice.
2. Enter destination host IP address and RDP service port number.



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.



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. Click *Active*.
5. Find *John Smith's* session and click the playback icon.



Related topics:

- [Requirements](#)
- [Data model](#)
- [Configuration](#)
- [Quick start - RDP connection configuration](#)
- [Quick start - HTTP connection configuration](#)
- [Quick start - MySQL connection configuration](#)
- [Quick start - Telnet connection configuration](#)

4.3 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.

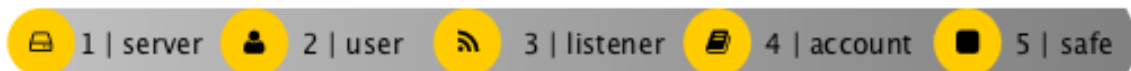
Note: Telnet connections do not support login credentials forwarding and login credentials substitution. When connecting to target host over telnet protocol, users are asked to provide their login credentials twice. First time to authenticate against Wheel Fudo PAM and then again, to connect to the target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



Prerequisites

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

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
<i>General</i>	
Name	telnet_server
Blocked	X
Protocol	Telnet
Enable SSLv2 support	X
Enable SSLv3 support	X
Description	X
<i>Permissions</i>	
Granted users	X
<i>Destination host</i>	
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, 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
Login	john_smith
Blocked	
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	
Phone	
AD Domain	
LDAP Base	
<i>Permissions</i>	
Granted users	
<i>Connections</i>	
Connections	
<i>Authentication</i>	
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
<i>General</i>	
Name	telnet_listener
Blocked	
Protocol	Telnet
Enable SSLv2 support	
Enable SSLv3 support	
<i>Permissions</i>	
Granted users	
<i>Connection</i>	
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
<i>General</i>	
Name	admin_telnet_server
Blocked	
Type	forward
Session recording	all
OCR sessions	
Delete session data after	61 days
<i>Permissions</i>	
Granted users	
<i>Server</i>	
Server	telnet_server
<i>Credentials</i>	
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
<i>General</i>	
Name	telnet_safe
Blocked	X
Login reason	X
Notifications	X
Policies	X
Users	john_smith
<i>Protocol functionality</i>	
RDP	X
SSH	X
VNC	X
<i>Permissions</i>	
Granted users	X
<i>Accounts</i>	
admin_telnet_server	telnet_listener

4. Click *Save*.

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:
```

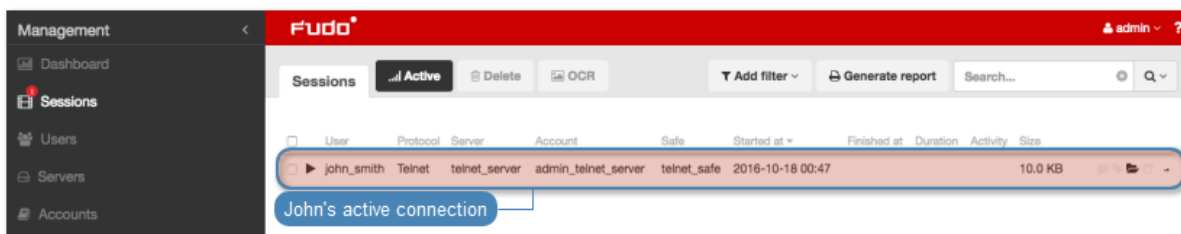
4. Provide user authentication information defined on the target host:

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

Note: Telnet connections do not support user credentials substitution.

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. Click *Active*.
5. 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](#)
- [Configuration](#)
- [Resources](#)

4.4 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.

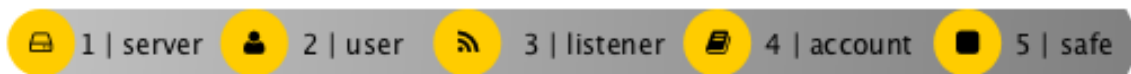
Note: Telnet connections do not support login credentials forwarding and login credentials substitution. When connecting to target host over telnet protocol, users are asked to provide their login credentials twice. First time to authenticate against Wheel Fudo PAM and then again, to connect to the target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



Prerequisites

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

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
<i>General</i>	
Name	telnet_server
Blocked	
Protocol	Telnet 5250
Enable SSLv2 support	
Enable SSLv3 support	
Description	
<i>Permissions</i>	
Granted users	
<i>Destination host</i>	
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, 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
Login	john_smith
Blocked	
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	
Phone	
AD Domain	
LDAP Base	
<i>Permissions</i>	
Granted users	
<i>Connections</i>	
Connections	
<i>Authentication</i>	
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
<i>General</i>	
Name	telnet_listener
Blocked	
Protocol	Telnet
Enable SSLv2 support	
Enable SSLv3 support	
<i>Permissions</i>	
Granted users	
<i>Connection</i>	
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
<i>General</i>	
Name	admin_telnet_server
Blocked	
Type	forward
Session recording	all
OCR sessions	
Delete session data after	61 days
<i>Permissions</i>	
Granted users	
<i>Server</i>	
Server	telnet_server
<i>Credentials</i>	
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
<i>General</i>	
Name	telnet_safe
Blocked	X
Login reason	X
Notifications	X
Policies	X
Users	john_smith
<i>Protocol functionality</i>	
RDP	X
SSH	X
VNC	X
<i>Permissions</i>	
Granted users	X
<i>Accounts</i>	
admin_telnet_server	telnet_listener

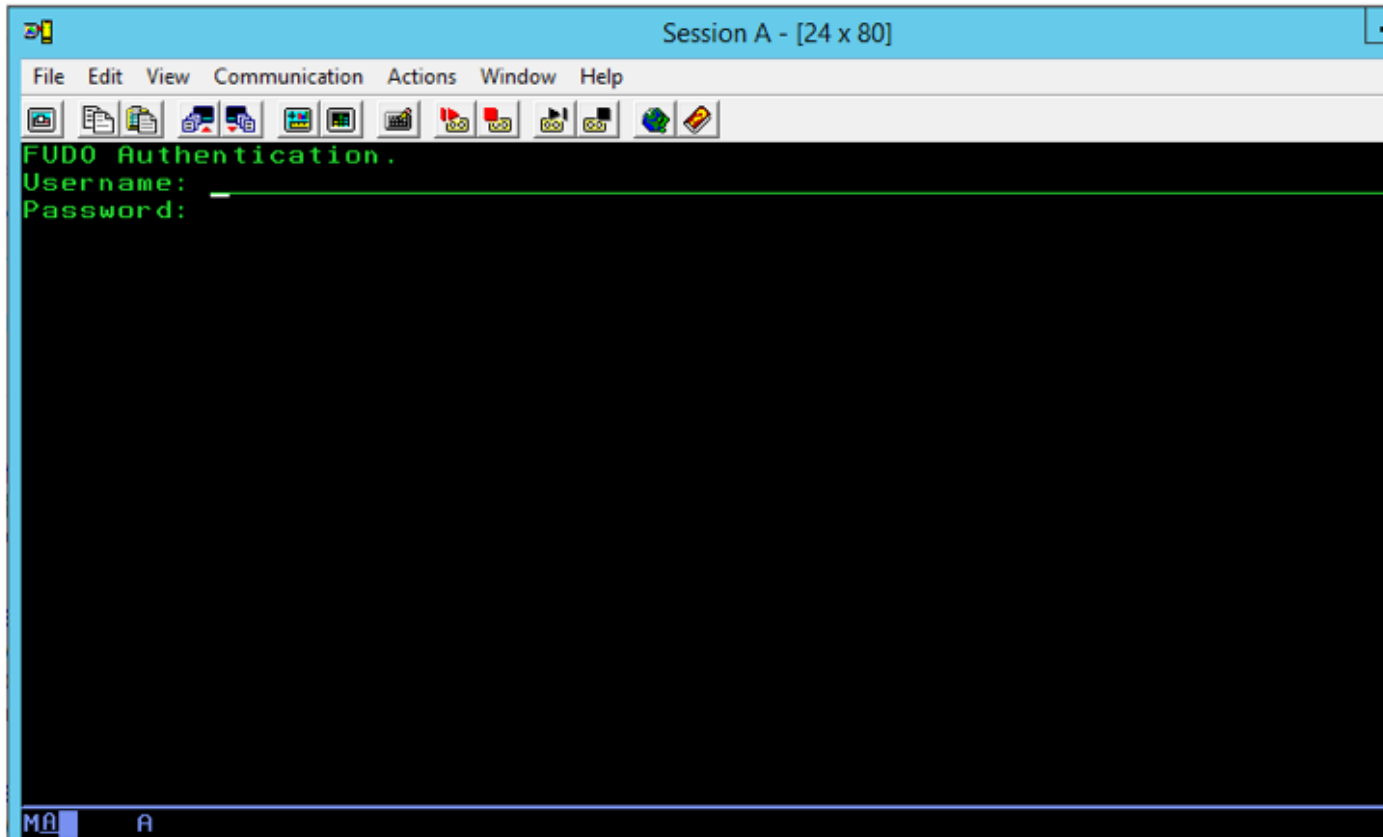
4. Click *Save*.

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 '^['.
```

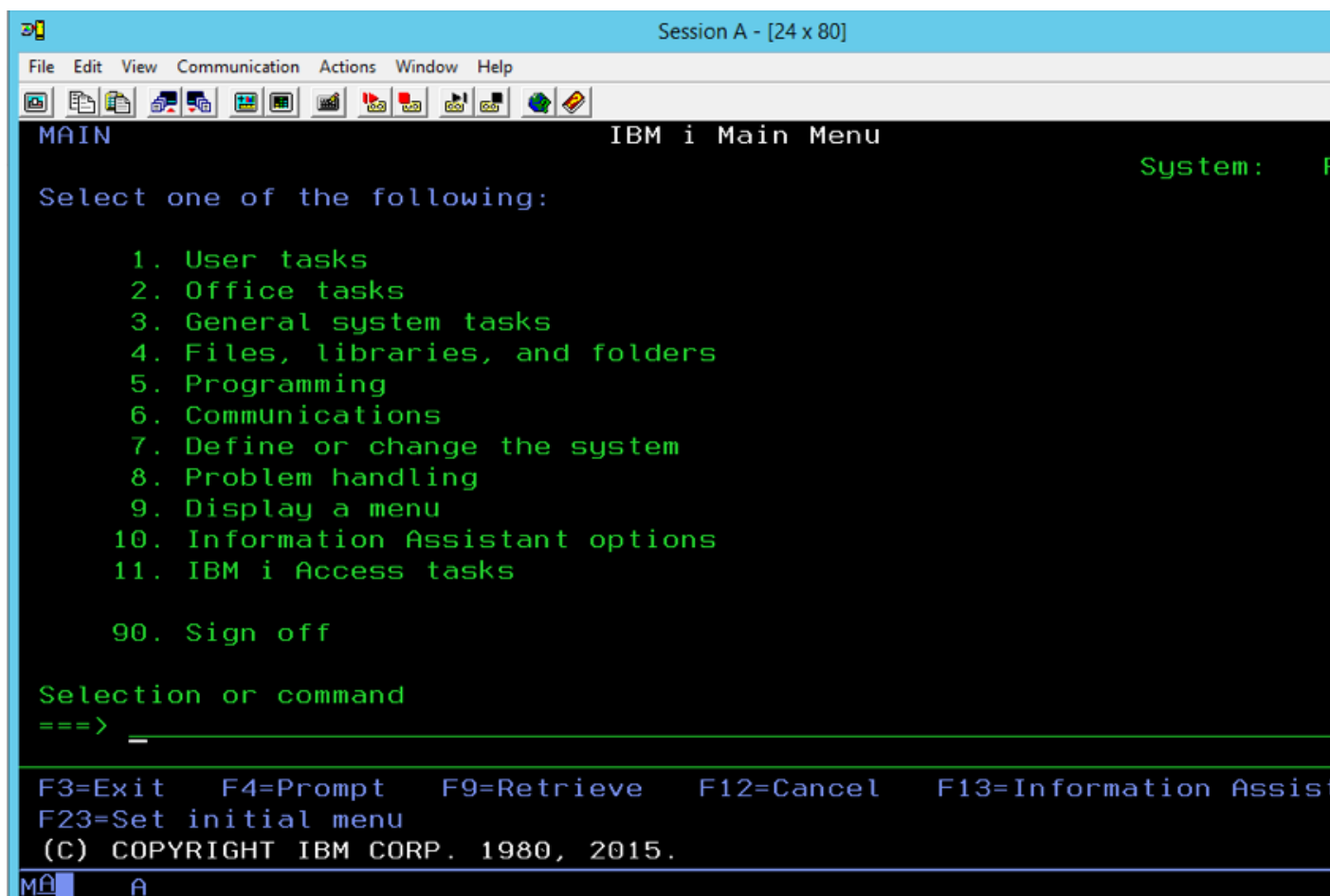
3. Provide user authentication information defined on Wheel Fudo PAM:



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

```
FreeBSD/amd64 (fbsd83-cerb.wh1) (pts/0)
login:
password:
```

Note: Telnet connections do not support user credentials substitution.



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. Click *Active*.
5. Find *John Smith's* session and click the playback icon.


```
MAIN                                IBM i Main Menu                                System:  PUB400
Select one of the following:
    1. User tasks
    2. Office tasks
    3. General system tasks
    4. Files, libraries, and folders
    5. Programming
    6. Communications
    7. Define or change the system
    8. Problem handling
    9. Display a menu
   10. Information Assistant options
   11. IBM i Access tasks
    90. Sign off

Selection or command
====>
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2015.
```



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](#)
- [Configuration](#)
- [Resources](#)

4.5 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).



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.

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
<i>General</i>	
Name	mysql_server
Blocked	
Protocol	MySQL
Description	
<i>Permissions</i>	
Granted users	
<i>Destination host</i>	
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, 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
Login	john_smith
Blocked	
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	
Phone	
AD Domain	
LDAP Base	
<i>Permissions</i>	
Granted users	
<i>Connections</i>	
Connections	
<i>Authentication</i>	
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
<i>General</i>	
Name	mysql_listener
Blocked	
Protocol	Mysql
<i>Permissions</i>	
Granted users	
<i>Connection</i>	
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
<i>General</i>	
Name	admin_mysql_server
Blocked	
Type	regular
Session recording	all
OCR sessions	
Delete session data after	61 days
<i>Permissions</i>	
Granted users	
<i>Server</i>	
Server	mysql_server
<i>Credentials</i>	
Domain	
Login	root
Replace secret with	with password
Password	password
Repeat password	password
Password change policy	Static, without restrictions
<i>Password changer</i>	
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
<i>General</i>	
Name	mysql_safe
Blocked	X
Login reason	X
Notifications	X
Policies	X
Users	john_smith
<i>Protocol functionality</i>	
RDP	X
SSH	X
VNC	X
<i>Accounts</i>	
admin_mysql_server	mysql_listener

4. Click *Save*.

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.

```

zmroczkowski — mysql -h 10.0.150.151 -u john_smith -p — 122x31
Last login: Tue Oct 18 13:53:49 on ttys001
Zbigniew-MacBook-Pro:~ zmroczkowski$ mysql -h 10.0.150.151 -u john_smith -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2544
Server version: 5.7.16 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

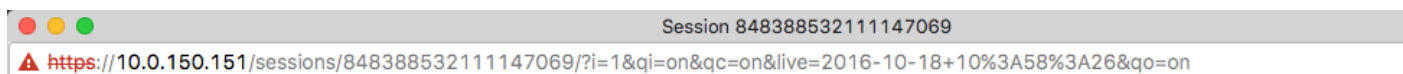
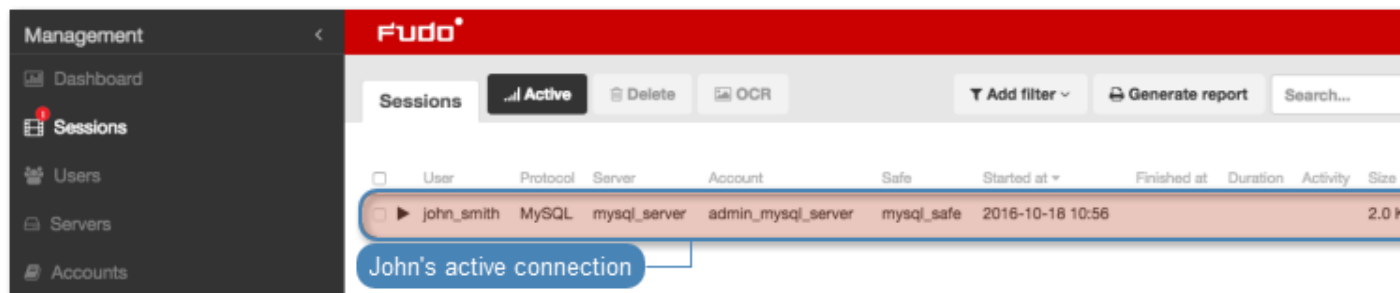
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
    
```

4. Continue browsing the database contents using SQL queries.

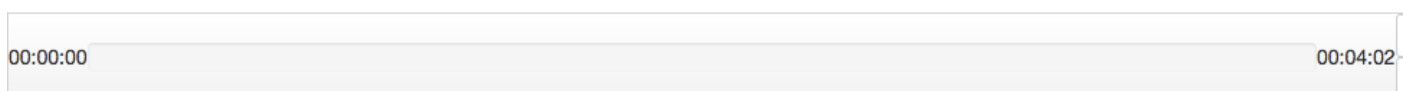
Viewing user session

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. Click *Active*.
5. Find *John Smith's* session and click the playback icon.



Session: 848388532111147069, user: john_smith, server: mysql_server

INIT	2016-10-
<p>Protocol version: 10 Server version: 5.7.16 Connection ID: 2545 Authentication plugin name: mysql_native_password Capabilities: CLIENT_IGNORE_SPACE, CLIENT_RESERVED, CLIENT_PLUGIN_AUTH, CLIENT_INTERACTIVE, CLIENT_SECURE_CONNECTION, CLIENT_MULTI_RESULTS, CLIENT_CONNECT_ATTRS, CLIENT_NO_SCHEMA, CLIENT_TRANSACTIONS, CLIENT_IGNORE_SIGPIPE, CLIENT_LONG, CLIENT_CONNECT_WITH_DB, CLIENT_FOUND_ROWS, CLIENT_PLUGIN_AUTH_LENENC_CLIENT_DATA, CLIENT_LOCAL_FILES, CLIENT_COMPRES, CLIENT_MULTI_STATEMENTS, CLIENT_LONG_PASSWORD, CLIENT_ODBC, CLIENT_PS_MULTI_RESULTS, CLIENT_PROTOCOL_41</p>	
OK	2016-10-
<p>Affected rows: 0 Last inserted_id rows: 0 Status: 2 Warnings: 0 Info:</p>	
COM_QUERY	2016-10-
<p>Query:</p> <pre>select @@version_comment limit 1</pre>	



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*
- Configuration

4.6 HTTP

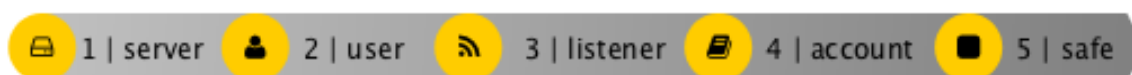
This chapter contains an example of a basic Wheel Fudo PAM configuration, to monitor HTTP access to a remote server. In this scenario, the user browses resources of the monitored server using a web browser. The user is authenticated by Wheel Fudo PAM against the local user database. The connection will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



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.







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
<i>General</i>	
Name	http_server
Blocked	
Protocol	HTTP
HTTP timeout	900
Enable SSLv2 support	
Enable SSLv3 support	
Description	
<i>Permissions</i>	
Granted users	
<i>Destination host</i>	
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, 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
Login	john_smith
Blocked	
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	
Phone	
AD Domain	
LDAP Base	
<i>Permissions</i>	
Granted users	
<i>Connections</i>	
Connections	
<i>Authentication</i>	
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
<i>General</i>	
Name	http_listener
Blocked	
Protocol	HTTP
Enable SSLv2 support	
Enable SSLv3 support	
<i>Permissions</i>	
Granted users	
<i>Connection</i>	
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
<i>General</i>	
Name	admin_http_server
Blocked	
Type	forward
Session recording	all
OCR sessions	
Delete session data after	61 days
<i>Permissions</i>	
Granted users	
<i>Server</i>	
Server	http_server
<i>Credentials</i>	
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.

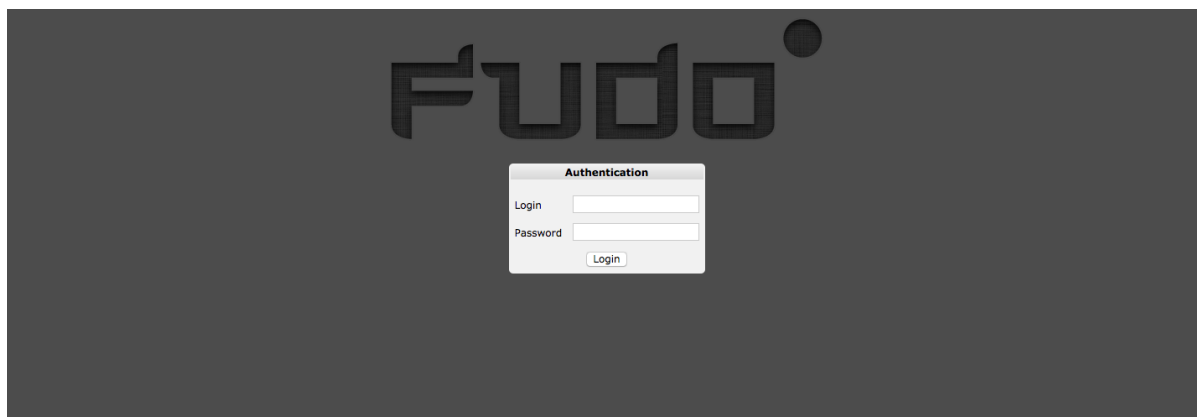
1. Select *Management > Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
<i>General</i>	
Name	http_safe
Blocked	X
Login reason	X
Notifications	X
Policies	X
Users	john_smith
<i>Protocol functionality</i>	
RDP	X
SSH	X
VNC	X
<i>Accounts</i>	
admin_http_server	http_listener

4. Click *Save*.

Connecting to remote resource

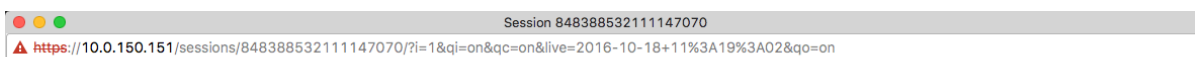
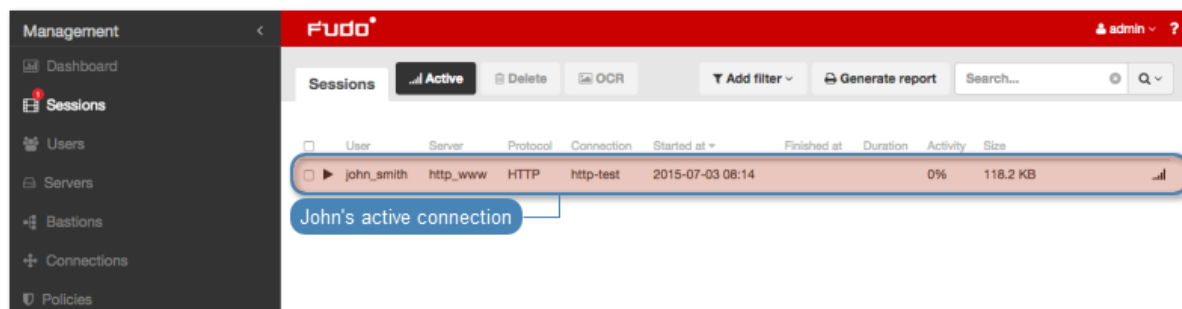
1. Launch a web browser.
2. Go to the 10.0.150.151:8080 web address.
3. Enter user login and password and press the [Enter] key or click the *Login* button.



4. Continue browsing the website.

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. Click *Active*.
5. Find *John Smith's* session and click the playback icon.



Session: 84838853211147070, User: john_smith ⏻ Terminate

Path	Method	Content-Type	Size	Start Time	End Time	URL
/webman/resources/images/icon_dsm_48.png? v=4398	GET	image/png	1.6 KB	2016-10-18 11:18:54.158837		http://10.0.150.151:8080/
/webman/resources/images/icon_dsm_64.png? v=4398	GET	image/png	1.7 KB	2016-10-18 11:18:54.204921		http://10.0.150.151:8080/
/webman/resources/images/icon_dsm_96.png? v=4398	GET	image/png	2.1 KB	2016-10-18 11:18:54.240588		http://10.0.150.151:8080/
/scripts/ext-3/ux/images/default/1x/Components/checkbox v=0846062016020243	GET	image/png	2.1 KB	2016-10-18 11:18:55.159765		http://10.0.150.151:8080/scripts/ext-3/ux/ux-all.css?v=1470092212
/webman/resources/images/default/1x/login/ch v=5934	GET	image/png	1.9 KB	2016-10-18 11:18:55.174328		http://10.0.150.151:8080/webman/resources/css/desktop.css?v=1471385610
/webman/resources/images/default/1x/login/sp sd716acf281.png	GET	image/png	1.8 KB	2016-10-18 11:18:55.472084		http://10.0.150.151:8080/webman/resources/css/desktop.css?v=1471385610
/webman/3rdparty/VideoStation/font/Roboto-Bold.ttf	GET	application/octet-stream	132.6 KB	2016-10-18 11:18:55.481876		http://10.0.150.151:8080/webman/3rdparty/VideoStation/style.css?v=1468242934
/webman/3rdparty/VideoStation/font/Roboto-Regular.ttf	GET	application/octet-stream	141.9 KB	2016-10-18 11:18:55.491117		http://10.0.150.151:8080/webman/3rdparty/VideoStation/style.css?v=1468242934
/webman/resources/images/default/1x/login/lo v=08560520161740167	GET	image/png	4.4 KB	2016-10-18 11:18:55.540508		http://10.0.150.151:8080/webman/resources/css/desktop.css?v=1471385610
/webman/resources/images/default/1x/login/lo v=08560520161740167	GET	image/png	2.0 KB	2016-10-18 11:18:55.557389		http://10.0.150.151:8080/webman/resources/css/desktop.css?v=1471385610
/webman/resources/images/default/1x/login/lo v=08560520161740167	GET	image/png	1.4 KB	2016-10-18 11:18:55.677498		http://10.0.150.151:8080/webman/resources/css/desktop.css?v=1471385610
/webman/resources/images/default/1x/login/lo v=08560520161740167	GET	image/png	1.3 KB	2016-10-18 11:18:55.691060		http://10.0.150.151:8080/webman/resources/css/desktop.css?v=1471385610
/webman/resources/images/default/1x/default_ v=1476386269	GET	image/jpeg	295.5 KB	2016-10-18 11:18:55.870018		http://10.0.150.151:8080/

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](#)
- [Configuration](#)

4.7 Citrix

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

4.7.1 ICA

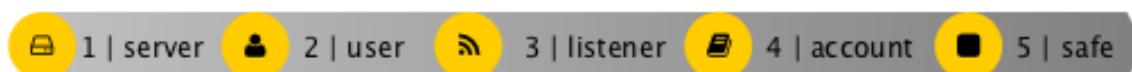
This chapter contains an example of a basic Wheel Fudo PAM configuration, to monitor direct ICA protocol connections.



4.7.1.1 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.





4.7.1.2 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
<i>General</i>	
Name	ica_server
Blocked	
Protocol	ICA
Description	
<i>Permissions</i>	
Granted users	
<i>Destination host</i>	
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
<i>General</i>	
Name	ica_listener
Blocked	
Protocol	ICA
<i>Permissions</i>	
Granted users	
<i>Connection</i>	
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
<i>General</i>	
Name	admin_ica_server
Blocked	
Type	regular
Session recording	all
OCR sessions	
Delete session data after	61 days
<i>Permissions</i>	
Granted users	
<i>Server</i>	
Server	ica_server
<i>Credentials</i>	
Domain	
Login	citrixuser
Replace secret with	password
Password	password
Repeat password	password
Password change policy	Static, without restrictions
<i>Password changer</i>	
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, 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
Login	john_smith
Blocked	
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	
Phone	
AD Domain	
LDAP Base	
<i>Permissions</i>	
Granted users	
<i>Connections</i>	
Connections	
<i>Authentication</i>	
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
<i>General</i>	
Name	ica_safe
Blocked	X
Login reason	X
Notifications	X
Policies	X
Users	john_smith
<i>Protocol functionality</i>	
RDP	X
SSH	X
VNC	X
<i>Accounts</i>	
admin_ica_server	ica_listener

4. Click *Save*.

4.7.1.3 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
EncryptionLevelSession=Basic
Compress=Off
```

2. Save the file with .ica extension.

4.7.1.4 Connecting to remote resource

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

4.7.1.5 Viewing user session

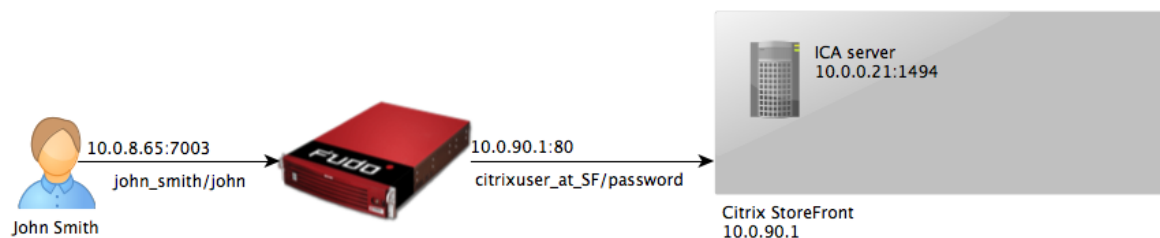
1. Open a web browser and go to the Wheel Fudo PAM administration page.
2. Enter user login and password to log in to Wheel Fudo PAM administration panel.
3. Select *Management > Sessions*.
4. Find *John Smith's* session and click the playback icon.

Related topics:

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

4.7.2 ICA via Citrix StoreFront

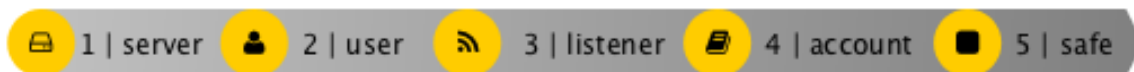
This chapter contains an example of a basic Wheel Fudo PAM configuration, to monitor access to a remote server over ICA protocol with the connection itself being initiated via the Citrix StoreFront.



4.7.2.1 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.

4.7.2.2 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
<i>General</i>	
Name	ica_server
Blocked	
Protocol	ICA
Description	
<i>Permissions</i>	
Granted users	
<i>Destination host</i>	
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
<i>General</i>	
Name	ica_listener
Blocked	
Protocol	ICA
<i>Permissions</i>	
Granted users	
<i>Connection</i>	
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
<i>General</i>	
Name	ICA_forward
Blocked	
Type	forward
Session recording	all
OCR sessions	
Delete session data after	61 days
<i>Permissions</i>	
Granted users	
<i>Server</i>	
Server	ica_server
<i>Credentials</i>	
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
<i>General</i>	
Name	citrix_storefront
Blocked	
Protocol	Citrix StoreFront (HTTP)
HTTP timeout	900
Description	
<i>Permissions</i>	
Granted users	
<i>Destination host</i>	
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
<i>General</i>	
Name	citrix_storefront_listener
Blocked	
Protocol	Citrix StoreFront (HTTP)
<i>Permissions</i>	
Granted users	
<i>Connection</i>	
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
<i>General</i>	
Name	citrixuser_at_SF
Blocked	
Type	regular
Session recording	all
OCR sessions	
Delete session data after	61 days
<i>Permissions</i>	
Granted users	
<i>Server</i>	
Server	citrix_storefront
<i>Credentials</i>	
Domain	tech.whl
Login	citrixuser
Replace secret with	password
Password	password
Repeat password	password
Password change policy	Static, without restrictions
<i>Password changer</i>	
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, 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
Login	john_smith
Blocked	
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	
Phone	
AD Domain	
LDAP Base	
<i>Permissions</i>	
Granted users	
<i>Connections</i>	
Connections	
<i>Authentication</i>	
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.

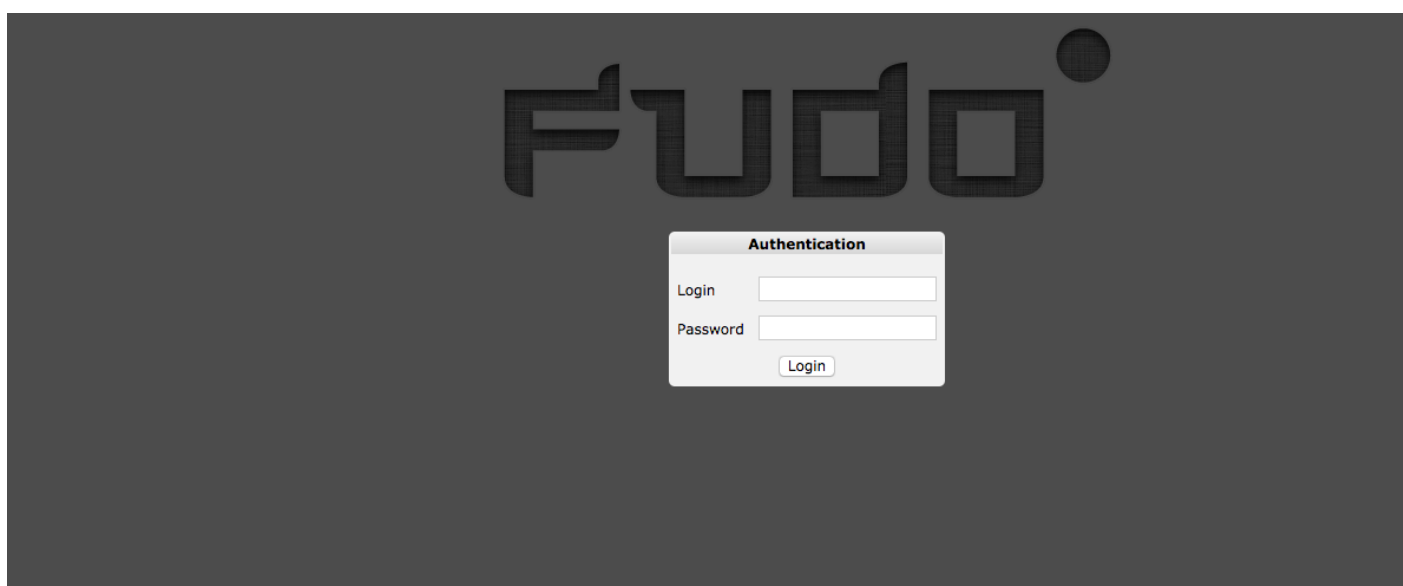
1. Select *Management > Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

Parameter	Value
<i>General</i>	
Name	ica_safe
Blocked	X
Login reason	X
Notifications	X
Policies	X
Users	john_smith
<i>Protocol functionality</i>	
RDP	X
SSH	X
VNC	X
<i>Accounts</i>	
citrixuser_at_SF	citrix_storefront_listener
ICA_forward	ica_listener

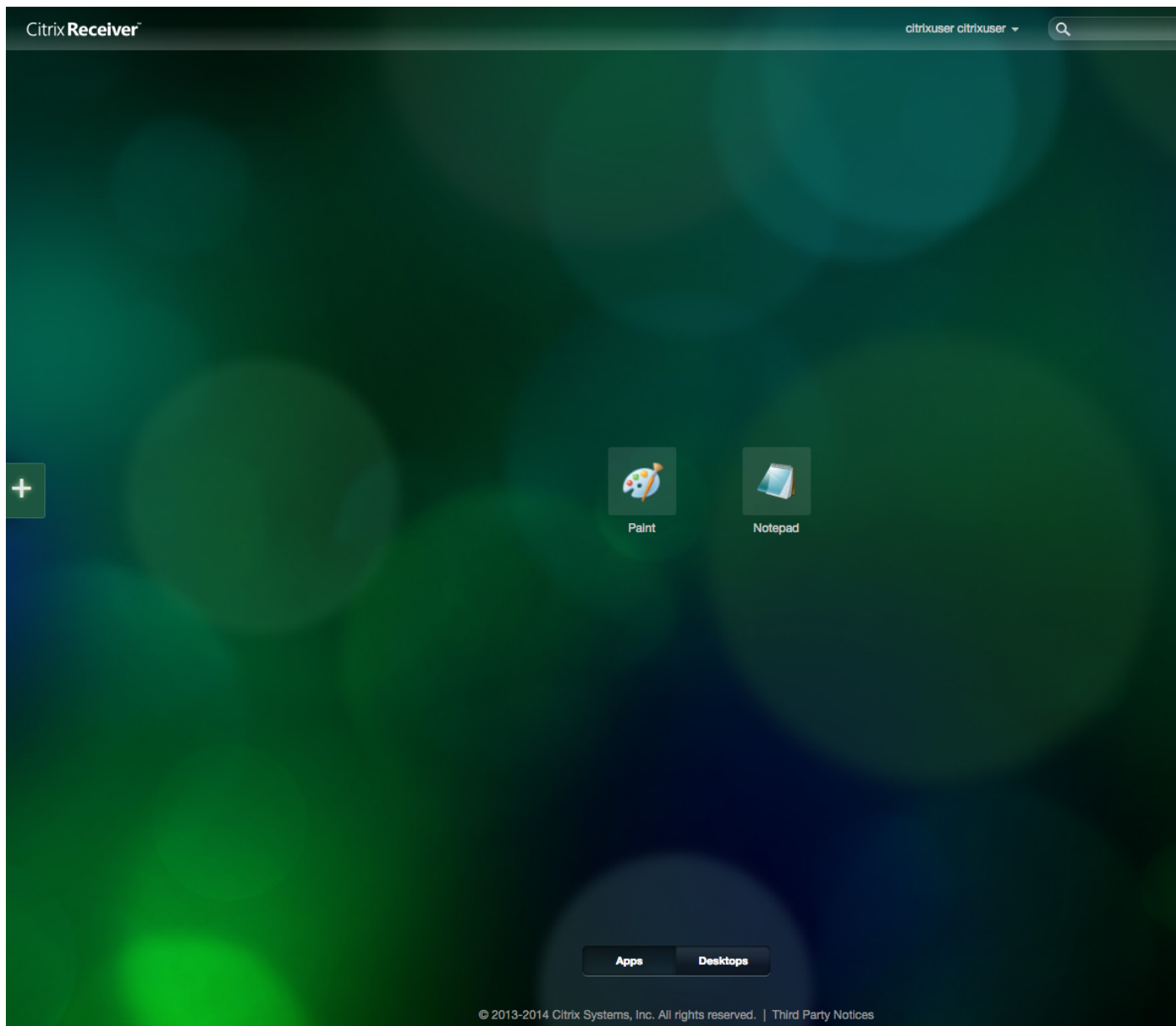
4. Click *Save*.

4.7.2.3 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.



4.7.2.4 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.

User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity
admin	Citrix StoreFront (HTTP)	SF	citrixuser at SF	Citrix	2017-02-16 15:12			0%
		ICA	forward@ICA	Citrix	2017-02-16 14:56	2017-02-16 14:57	0:00:32	0%
		ICA	forward@ICA	Citrix	2017-02-16 14:54	2017-02-16 14:55	0:00:42	0%
admin	ICA	ICA	citrixuserICA	Citrix-BASTION	2017-02-16 14:49	2017-02-16 14:49	0:00:11	100%
admin	ICA	ICA	citrixuserICA	Citrix-BASTION	2017-02-16 14:49	2017-02-16 14:49	0:00:14	100%
admin	ICA	ICA	forward@ICA	Citrix	2017-02-16 14:48	2017-02-16 14:48	0:00:26	100%

Related topics:

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

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

The screenshot shows the 'Users' management interface in Wheel Fudo PAM. The interface includes a sidebar with navigation options and a main content area with a table of users. Callouts highlight various actions:

- Define new user**: Points to the '+ Add' button.
- Block selected users**: Points to the 'Block' button.
- Allow selected users to access servers**: Points to the 'Unblock' button.
- Delete selected users**: Points to the 'Delete' button.
- Filter users list**: Points to the 'Add filter' button.
- Edit user definition**: Points to the 'admin1' user row.
- Blocked u**: Points to the 'jdoe' user row, which is highlighted in red.
- Reason the user has been**: Points to the 'jdoe' user row.

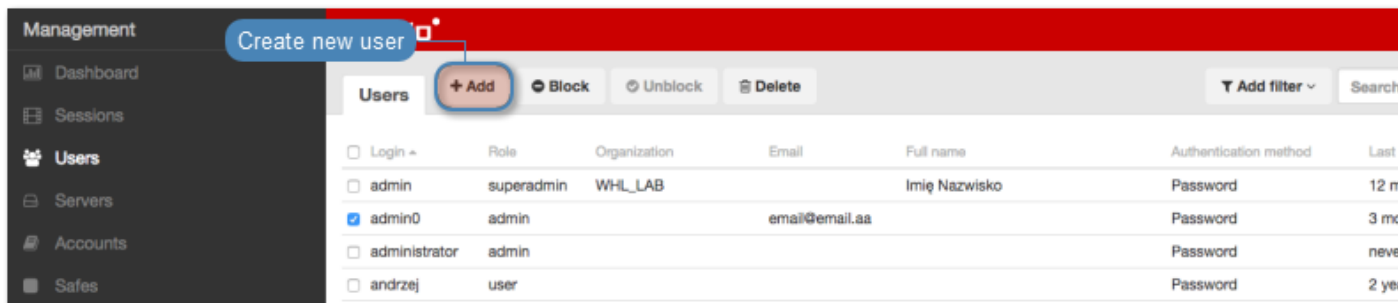
Login	Role	Organization	Email	Full name	Authentication method
<input type="checkbox"/> admin	superadmin				Password
<input type="checkbox"/> admin1	admin				Password
<input type="checkbox"/> anonym					
<input type="checkbox"/> api-robot-operator1	operator				Password
<input type="checkbox"/> api-robot-operator2	operator				Password
<input type="checkbox"/> api-robot-superadmin1	superadmin				
<input type="checkbox"/> api-robot-user1	user				
<input type="checkbox"/> api-robot-user2	user				
<input checked="" type="checkbox"/> jdoe	user			Joe Doe	External authentication
<input type="checkbox"/> kwitaszczyk	user			Konrad Witaszczyk	
<input type="checkbox"/> mborysiak	user			Michal Borysiak	External authentication
<input type="checkbox"/> mزابorski	superadmin	Wheel Systems	m.zaborski@wheelsystems.com	Mariusz Zaborski	External authentication
<input type="checkbox"/> pdawidek	user	Wheel Systems	p.dawidek@wheelsystems.com	Pawel Jakub Dawidek	External authentication

Note: Wheel 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.

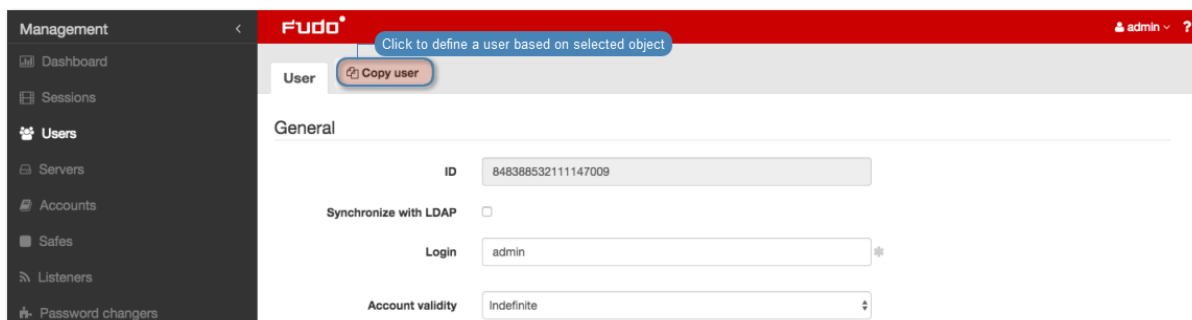
5.1 Creating a user

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.

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



Note: Wheel 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 a unique user login.

Note: The *Login* field is not case sensitive.

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

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

Role	Access rights
user	<ul style="list-style-type: none"> • Connecting to servers through assigned safes. • Loggin to the User Portal (requires adding the user to the <code>portal</code> safe) • Fetching servers' passwords (requires additional access right).
service	Accessing SNMP information.
operator	<ul style="list-style-type: none"> • Logging in to the administration panel. • Browsing objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permissions. • Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permissions. • Generating reports on demand and subscribing to periodic reports. • Activating/deactivating email notifications. • Viewing live and archived sessions involving objects (user, safe, account, listener, server), to which the user has been assigned sufficient access permissions. • Converting sessions and downloading converted content involving objects (user, safe, account, listener, server), to which the user has been assigned sufficient access permissions.
admin	<ul style="list-style-type: none"> • Logging in to the administration panel. • Managing objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permissions. • Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permissions. • Generating reports on demand and subscribing to periodic reports. • Activating/deactivating email notifications. • Viewing live and archived sessions involving objects (user, safe, account, listener, server), to which the user has been assigned management privileges. • Converting sessions and downloading converted content involving objects (user, safe, account, listener, server), to which the user has been assigned sufficient access permissions. • Managing policies.
superadmin	<ul style="list-style-type: none"> • Full access rights to objects management. • Full access rights to system configuration options.

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

Note:

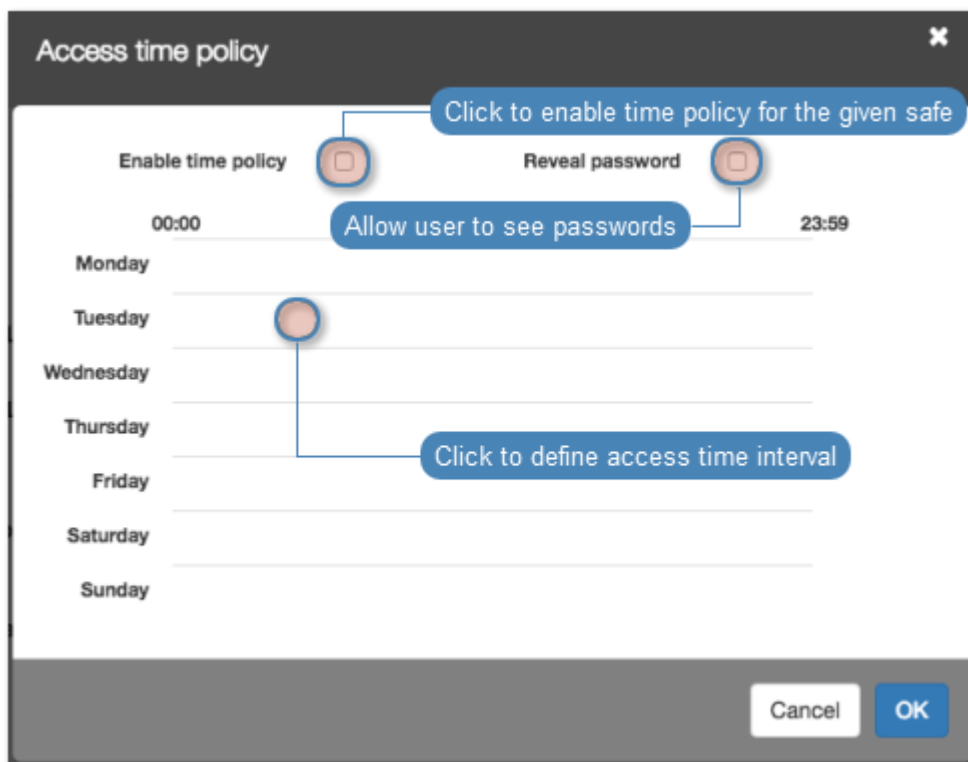
- Przeciągnij i upuść sejf, żeby określić kolejność użycia danych przechowywanych w sejfach przy zestawianiu połączenia.
- SSH_sejf wskazuje, że opcja Pokaż hasło jest wyłączona.
- RDP_sejf oznacza, że opcja Pokaż hasło jest włączona.

9. Define time access policy.

- Click desired safe object.



- Select the *Enable time policy* option.
- Click the weekly calendar to define time interval.



- Click *OK*.

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.
 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.
17. In the *Authentication* section, 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.

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.

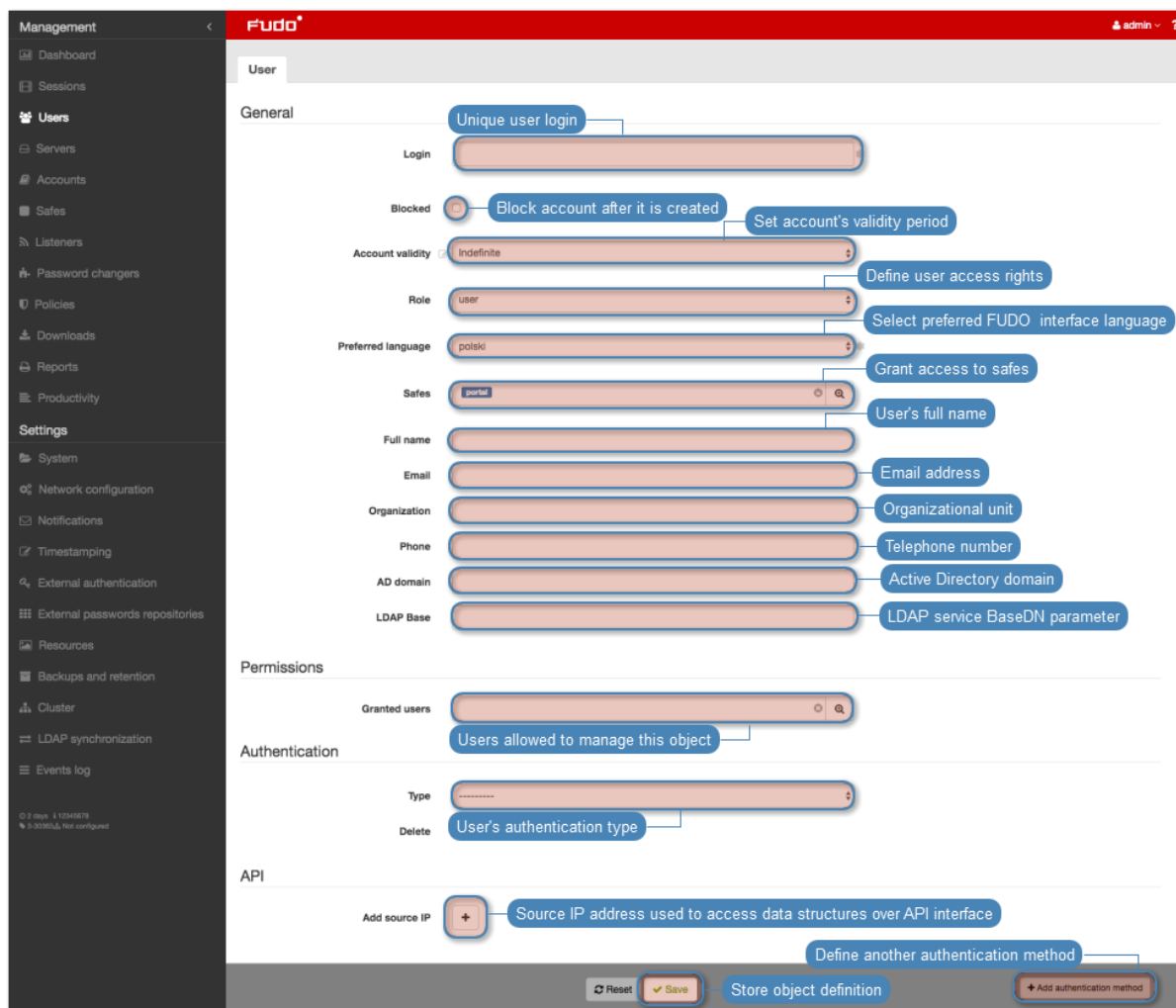
One-time password

<p>Warning: One-time passwords are used for implementing <i>AAPM</i> use case scenarios.</p>

- Select **One-time password** from the *Type* drop-down list.
18. Click *+ Add authentication method* to define more authentication methods.
-

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

19. Click *Save*.

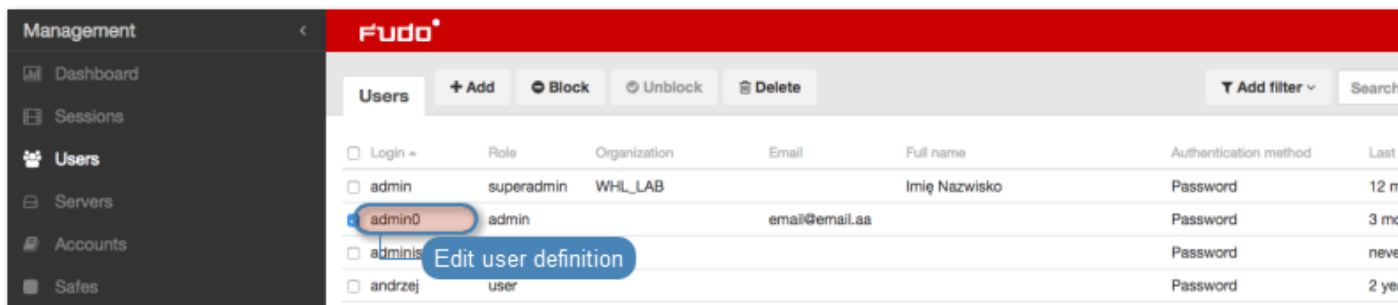


Related topics:

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

5.2 Editing a user

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

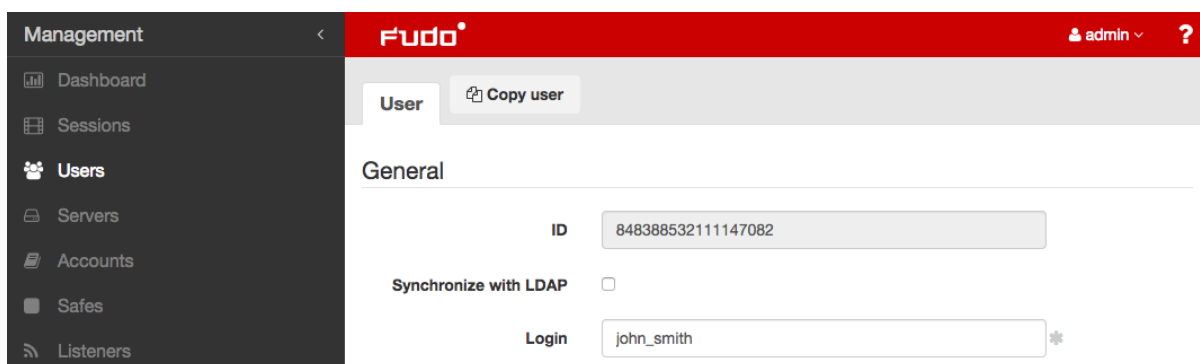


Note: Define filters to limit the number of objects displayed on the list.

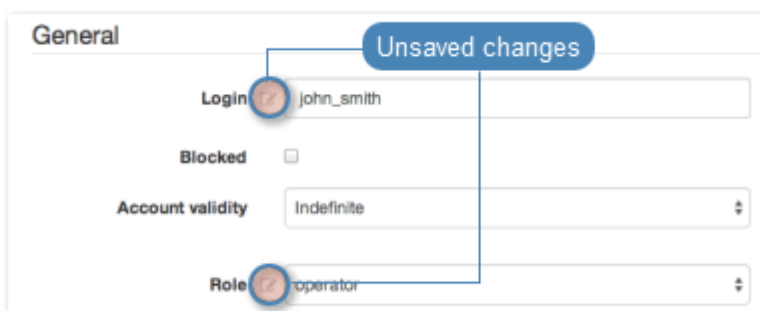
3. Modify configuration values as needed.

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*

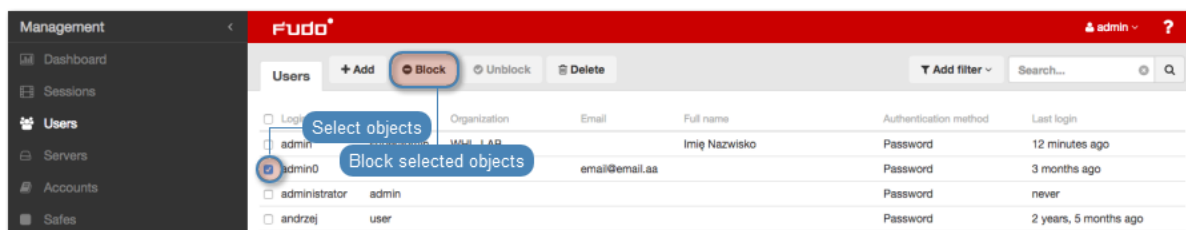
5.3 Blocking a user

Warning: Blocking a user will terminate its current connections.


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

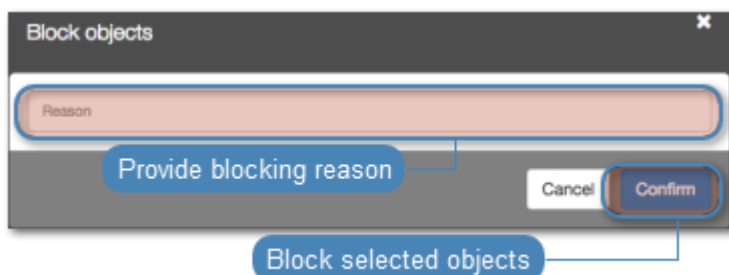
Note: Define filters to limit the number of objects displayed on the list.

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:

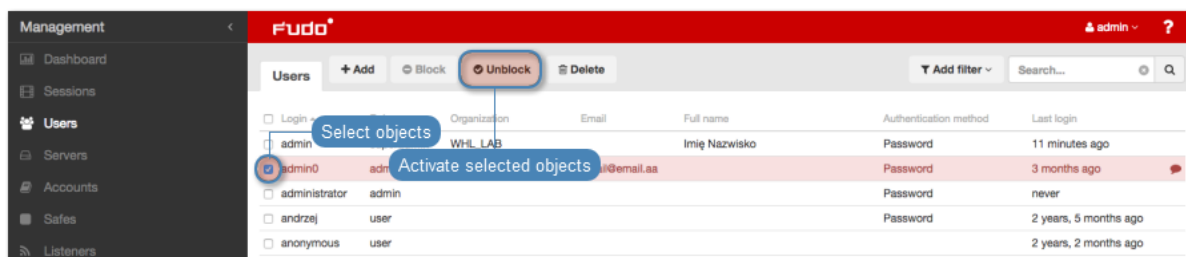
- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*
- *Accounts*

5.4 Unblcoking 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*

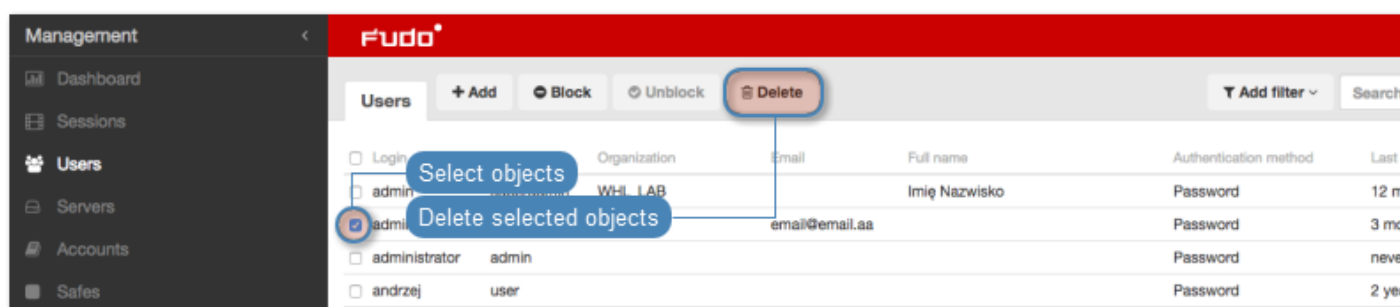
5.5 Deleting a user

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

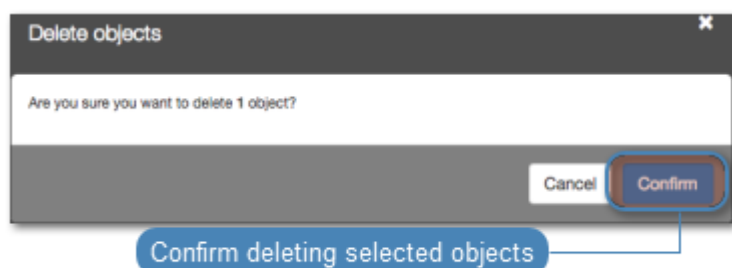
1. Select *Management > Users*.
2. Find and select desired object.

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 Roles

Role	Access rights
user	<ul style="list-style-type: none">• Connecting to servers through assigned safes.• Loggin to the User Portal (requires adding the user to the portal safe)• Fetching servers' passwords (requires additional access right).
service	Accessing SNMP information.
operator	<ul style="list-style-type: none">• Logging in to the administration panel.• Browsing objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permissions.• Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permissions.• Generating reports on demand and subscribing to periodic reports.• Activating/deactivating email notifications.• Viewing live and archived sessions involving objects (user, safe, account, listener, server), to which the user has been assigned sufficient access permissions.• Converting sessions and downloading converted content involving objects (user, safe, account, listener, server), to which the user has been assigned sufficient access permissions.
admin	<ul style="list-style-type: none">• Logging in to the administration panel.• Managing objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permissions.• Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permissions.• Generating reports on demand and subscribing to periodic reports.• Activating/deactivating email notifications.• Viewing live and archived sessions involving objects (user, safe, account, listener, server), to which the user has been assigned management privileges.• Converting sessions and downloading converted content involving objects (user, safe, account, listener, server), to which the user has been assigned sufficient access permissions.• Managing policies.
superadmin	<ul style="list-style-type: none">• Full access rights to objects management.• Full access rights to system configuration options.

Related topics:

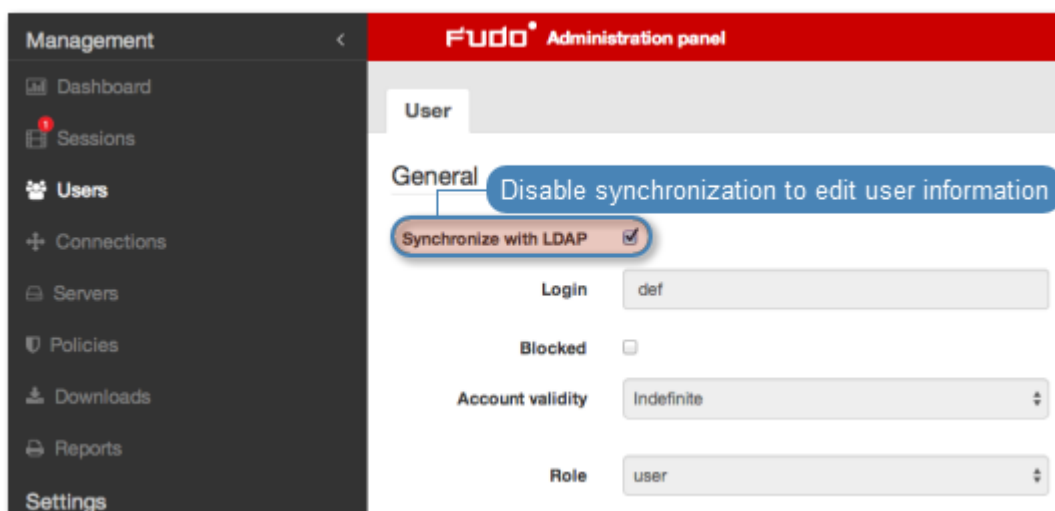
- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*
- *Accounts*

5.7 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.

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: 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. Select the data source type from the *Server type* drop-down list.
4. Provide the user authentication information to access user data on given server.
5. Enter domain name, to which imported users definition belong to.

6. In the *Base user* field, provide base DN for directory tree where users' definitions are stored (eg. `DC=tech,DC=wh1`).
7. In the *Base group* field, provide base DN for directory tree where groups' definitions are stored (eg. `DC=tech,DC=wh1`).

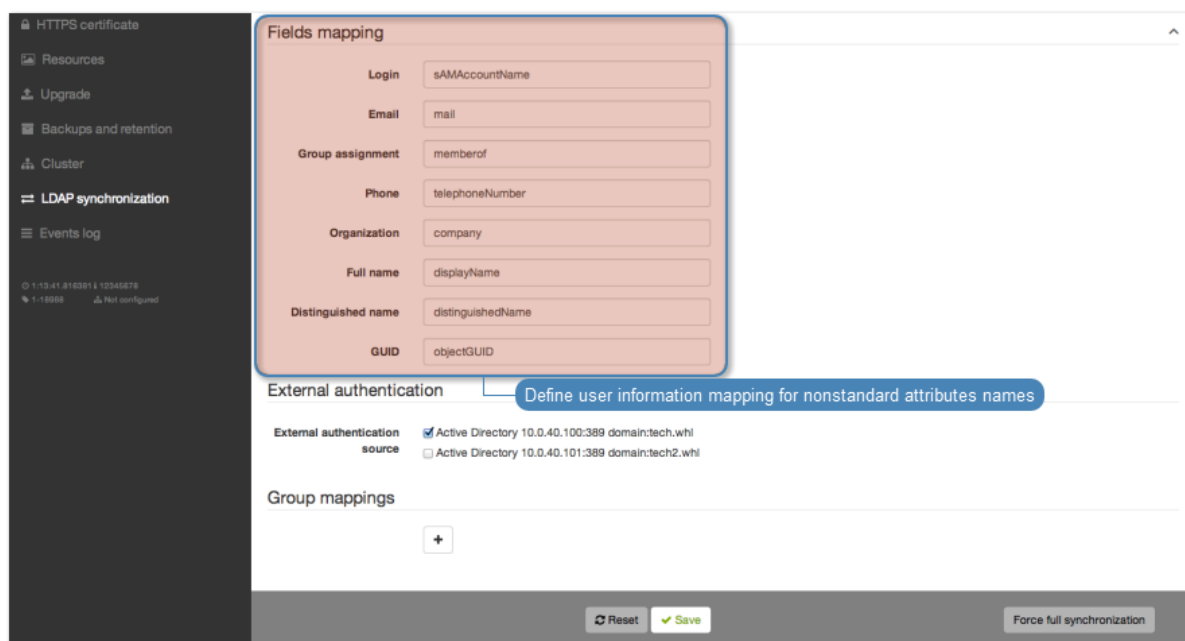
Note: DN parameter should not contain any white space characters.

8. Define filter for user records, which are subject to synchronization.
9. Define filter for user groups, which are subject to synchronization.
10. In the *Servers* section, provide the directory server's IP address and port number.

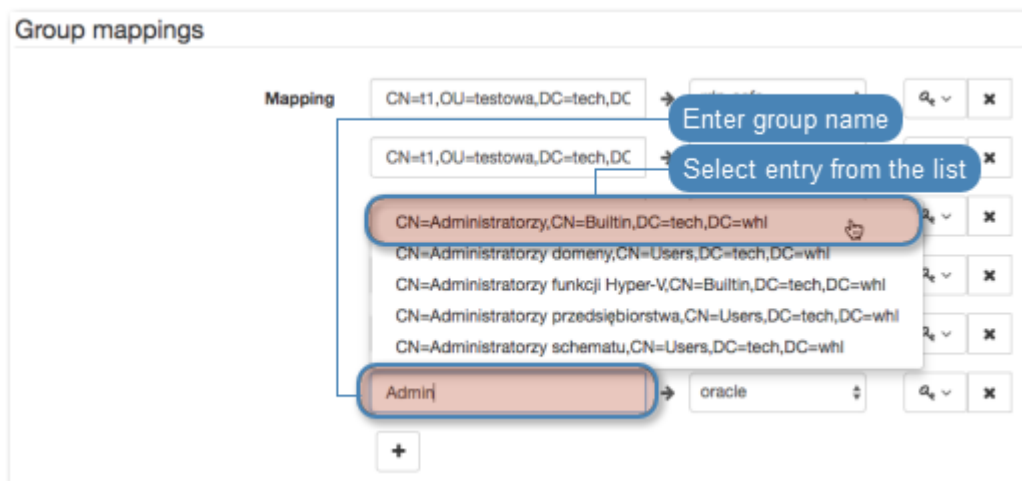
Note: Click *+* to add more directory servers.

11. Select the *Page LDAP results* option to enable paging.
12. Select the *Encrypted connection* option to enable encryption.
13. 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*.



14. Click *+* to add users group mapping.
15. Type in user group and select desired entry.



16. Assign safes to user groups.

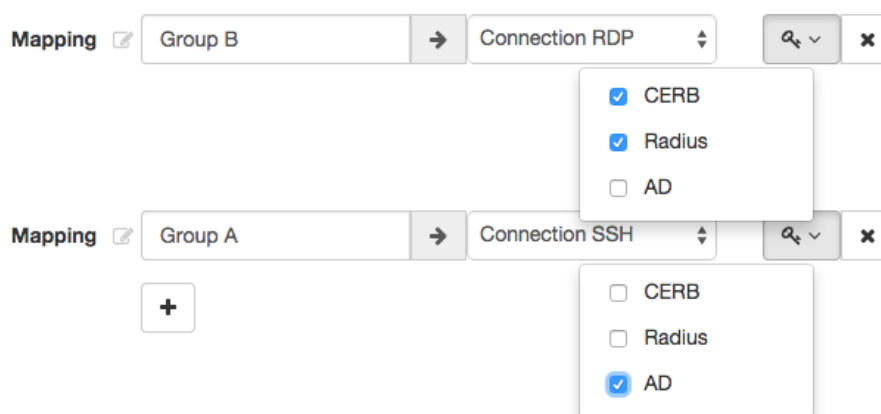
17. Assign external authentication sources to user groups.

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.

Group mappings



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

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

18. 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.

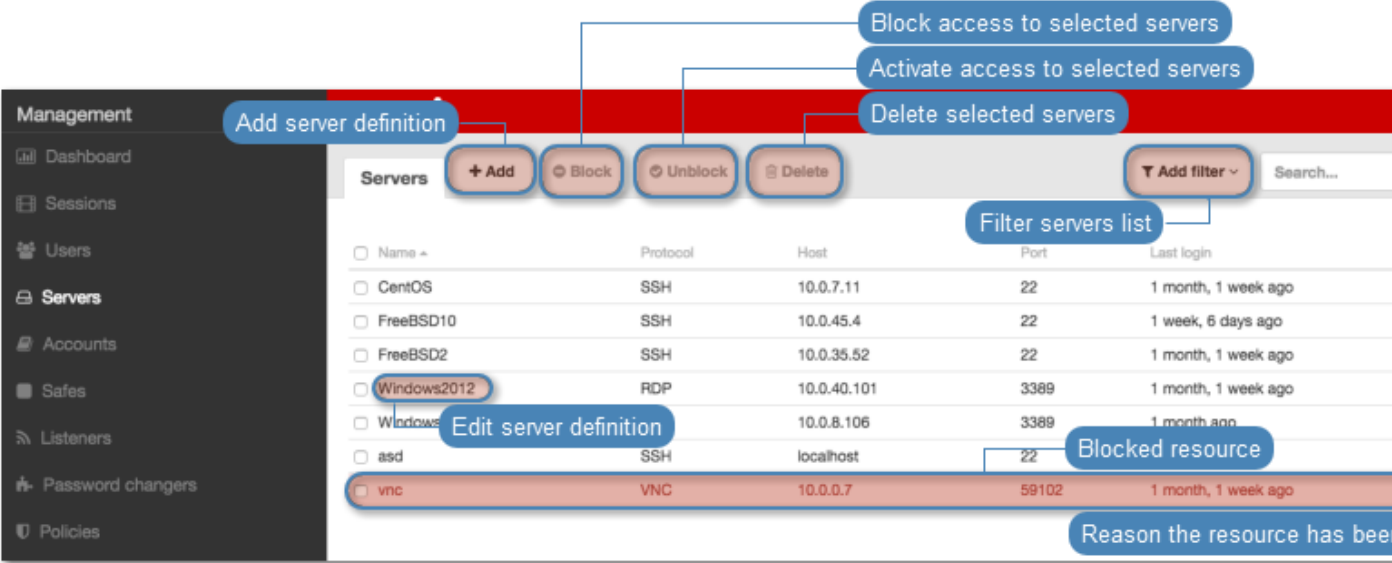
The full synchronization process is triggered automatically once a day at 00:00, or can be triggered manually.

The screenshot shows the Fudo web interface for LDAP synchronization configuration. The left sidebar contains navigation options like Management, Settings, and LDAP synchronization. The main content area is titled 'LDAP synchronization' and is currently 'Enabled'. Under 'Directory service', the configuration is set for 'Active Directory' with the following details: Username: Administrator, Password: [redacted], Domain name: tech.whl, Base user: dc=tech,dc=whl, Base group: dc=tech,dc=whl, User filter: (&(objectclass=user)), and Group filter: (&(objectclass=group)). The 'Servers' section shows an address of 10.0.40.160 on port 636, with 'Encrypted connection' checked. A CA certificate is displayed in a text area. Below the servers list, there are buttons for 'Remove server entry', 'Delete', and 'Add another directory service server'. The 'Attributes mapping' section includes a search bar and a dropdown menu. At the bottom, there are 'Reset', 'Save', and 'Force full synchronization' buttons.

Related topics:

- *Data model*
- *Users management*
- *Servers management*
- *Accounts*

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



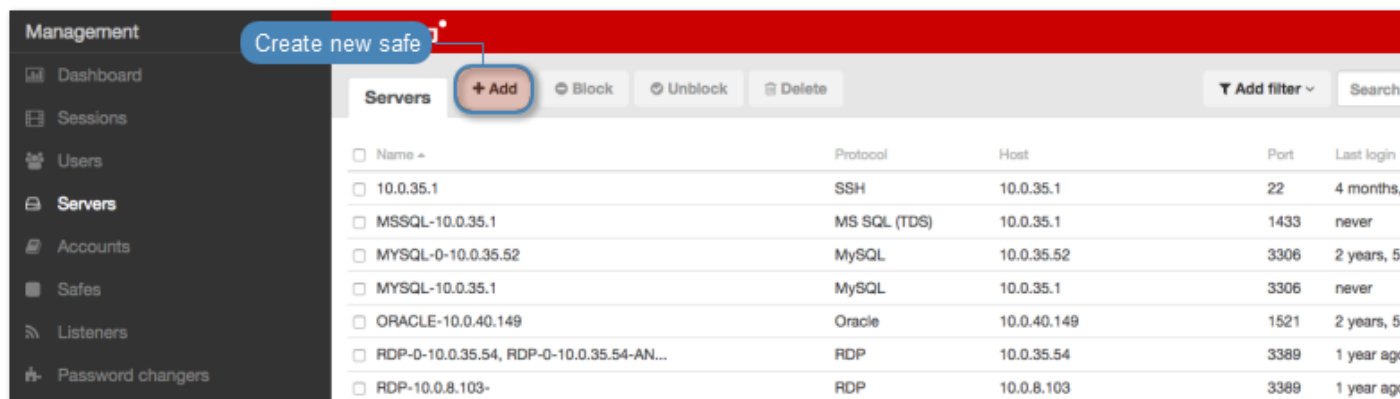
6.1 Creating a server

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.

6.1.1 Static server

6.1.1.1 Creating a Citrix server

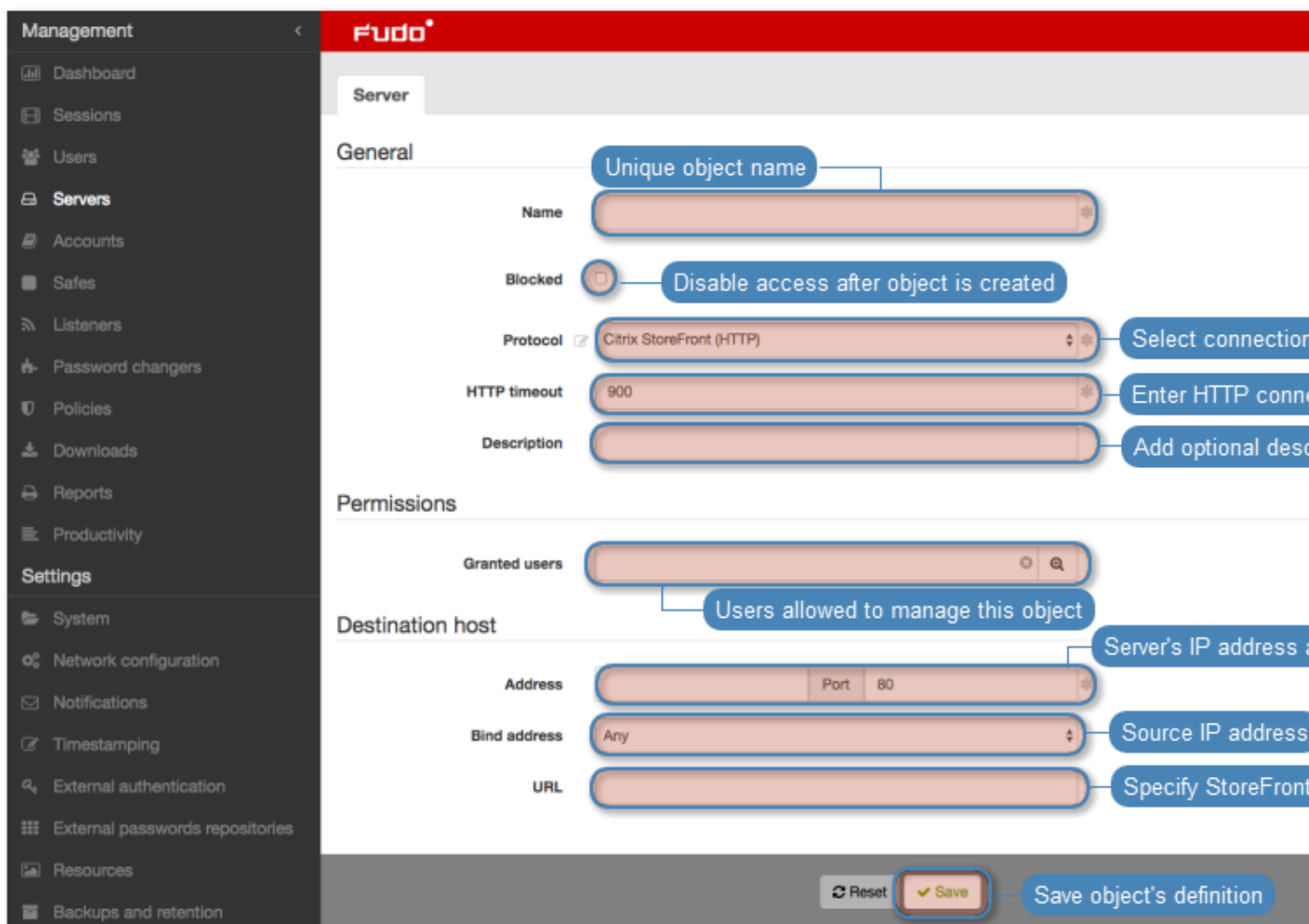
1. Select *Management* > *Servers*.
2. Click *+ Add*.



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. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

11. In the URL field, enter Citrix StoreFront base URL.
12. Click *Save*.



Related topics:

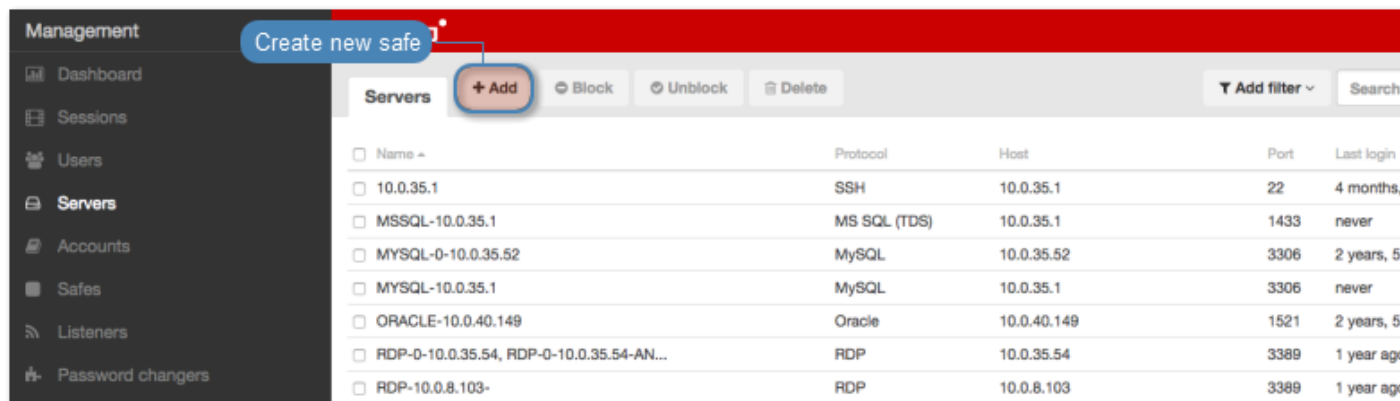
- *Data model*
- *Creating a Citrix listener*
- *ICA via Citrix StoreFront*
- *Citrix StoreFront (HTTP)*
- *ICA*
- *ICA configuration file*

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.

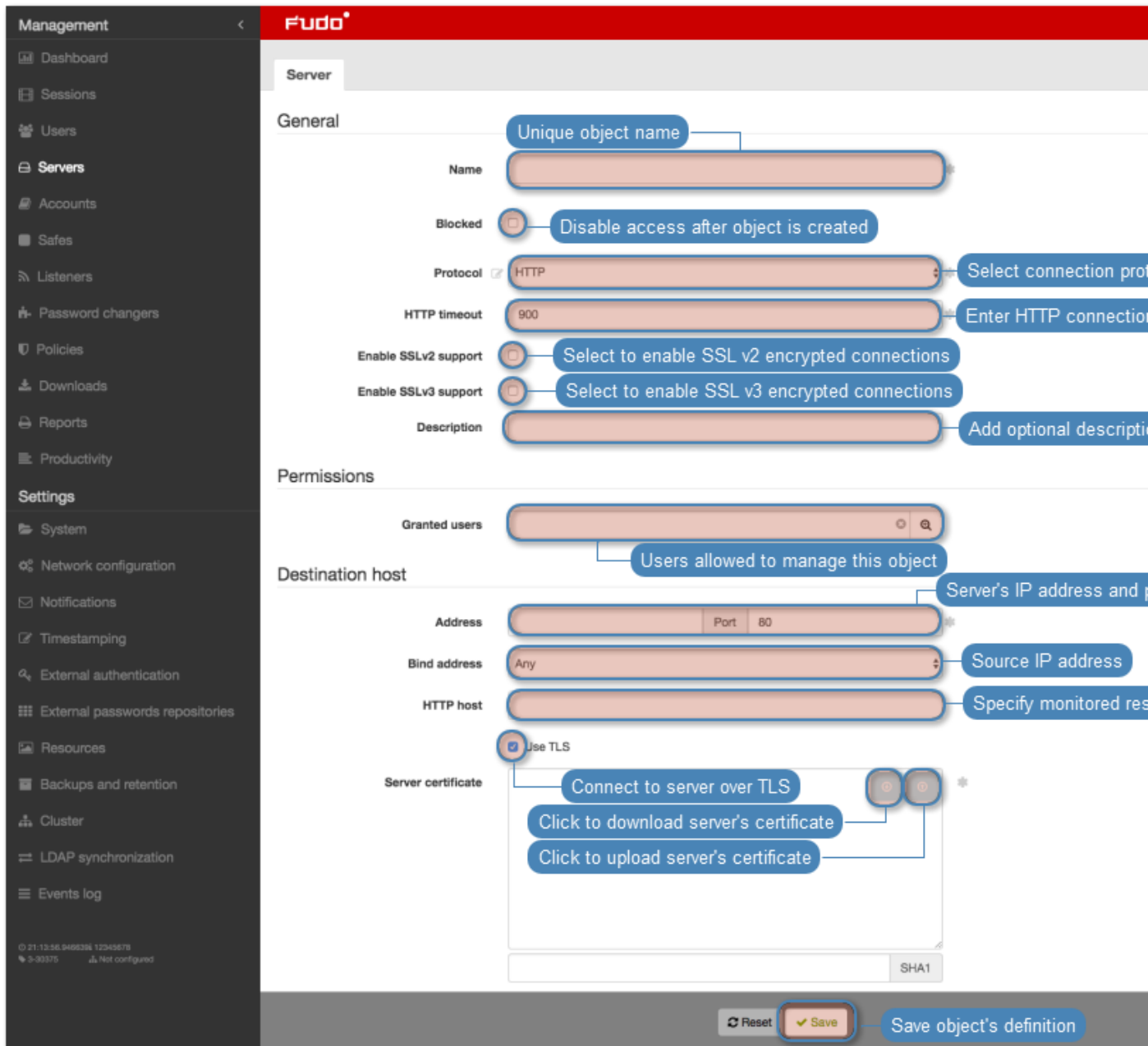
1. Select *Management > Servers*.
2. Click *+ Add*.



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. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
8. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
9. Enter optional description, which will help identifying this server object.
10. In the *Permissions* section, add users allowed to manage this object.
11. In the *Destination host* section, enter server's IP address and port number.
12. 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.

13. Specify the monitored resource in the *HTTP host* field.
14. Select the *Use TLS* options to connect to monitored server over TLS.
15. Click the certificate download icon to fetch server's certificate, or the certificate upload icon to upload a certificate.
16. Click *Save*.



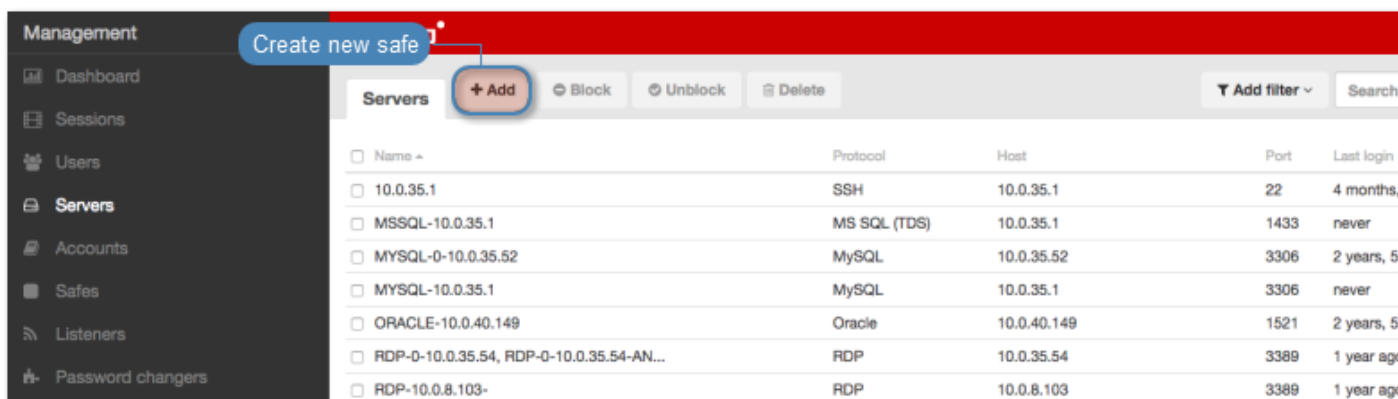
Related topics:

- *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. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

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 certificate download icon to fetch server's certificate, or the certificate upload icon to upload a certificate.
14. Click *Save*.

The screenshot shows the 'Server' configuration page in the Fudo web interface. The page is divided into three main sections: General, Permissions, and Destination host. Each field has a blue callout box explaining its function.

- General:**
 - Name:** Unique object name
 - Blocked:** Disable access after object is created
 - Protocol:** Select connection protocol (ICA is selected)
 - Description:** Add optional description
- Permissions:**
 - Granted users:** Users allowed to manage this object
- Destination host:**
 - Address:** Server's IP address and port number
 - Bind address:** Source IP address
 - Use TLS:** Connect to server over TLS
 - Enable SSLv2 support:** Select to enable SSL v2 encrypted connections
 - Enable SSLv3 support:** Select to enable SSL v3 encrypted connections
 - Server certificate:**
 - Click to download server's certificate
 - Click to upload server's certificate

At the bottom of the page, there are 'Reset' and 'Save' buttons. The 'Save' button is highlighted with a blue callout box: 'Save object's definition'.

Related topics:

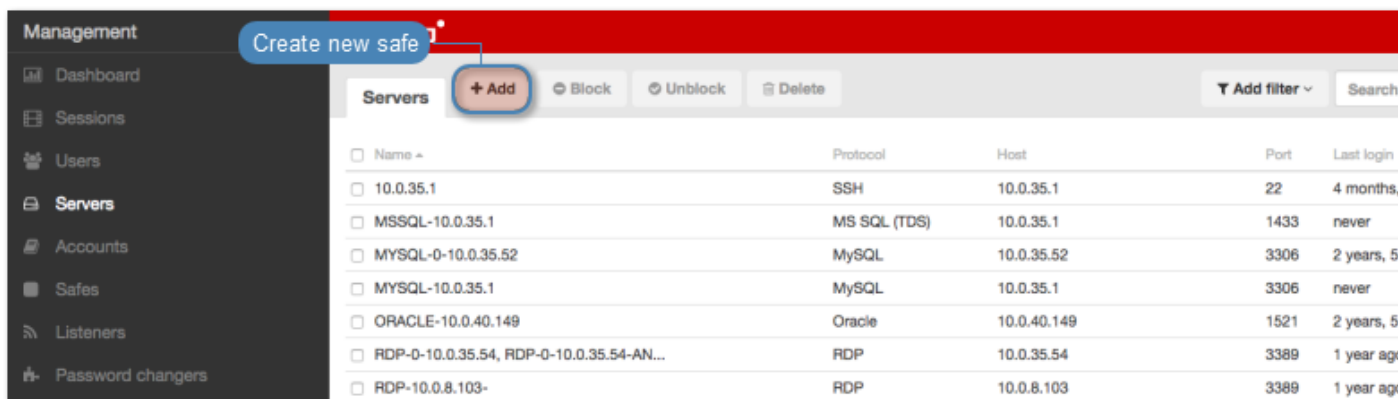
- *Data model*
- *ICA*
- *Creating an ICA listener*
- *ICA configuration file*
- *ICA*

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.
-

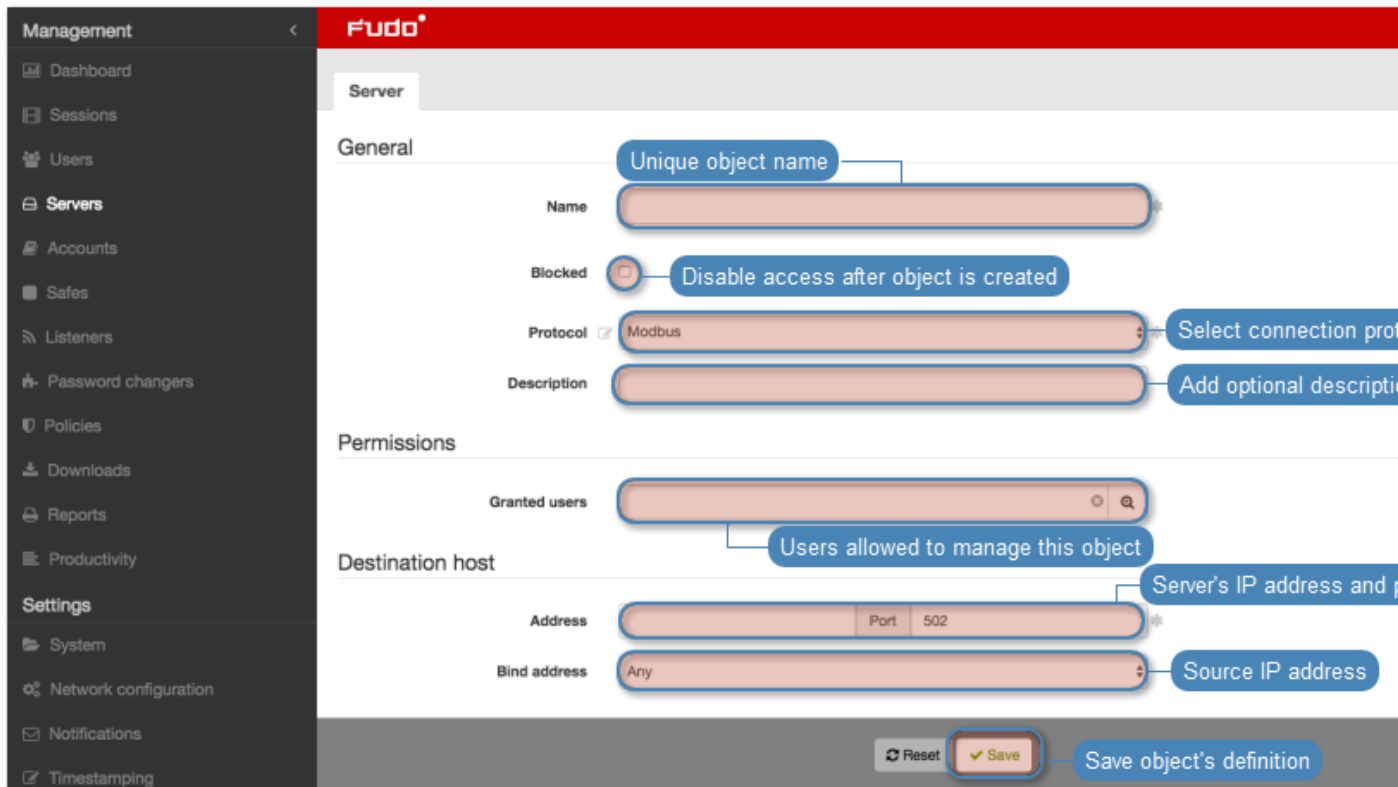
1. Select *Management > Servers*.
2. Click *+ Add*.



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. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

10. Click *Save*.



Related topics:

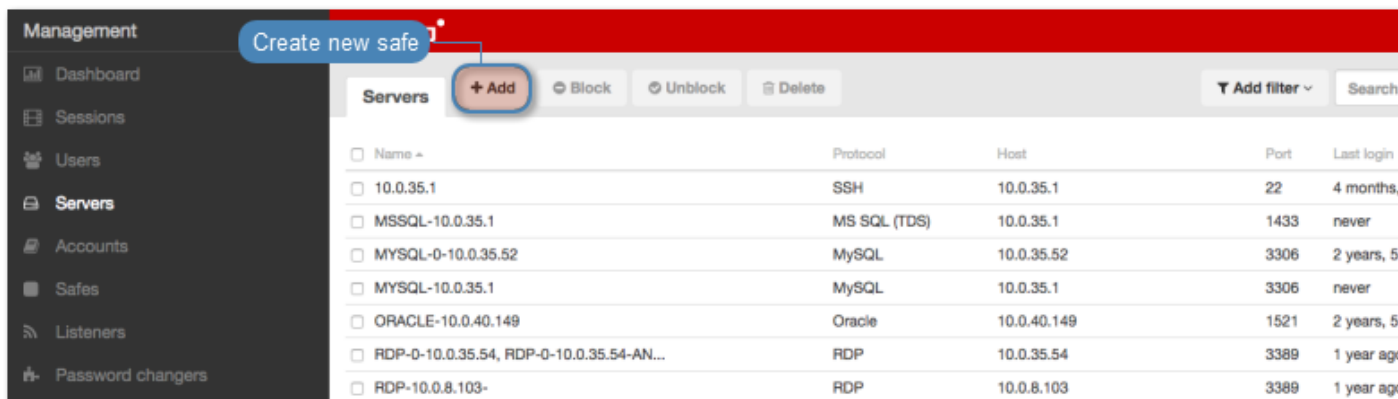
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

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.

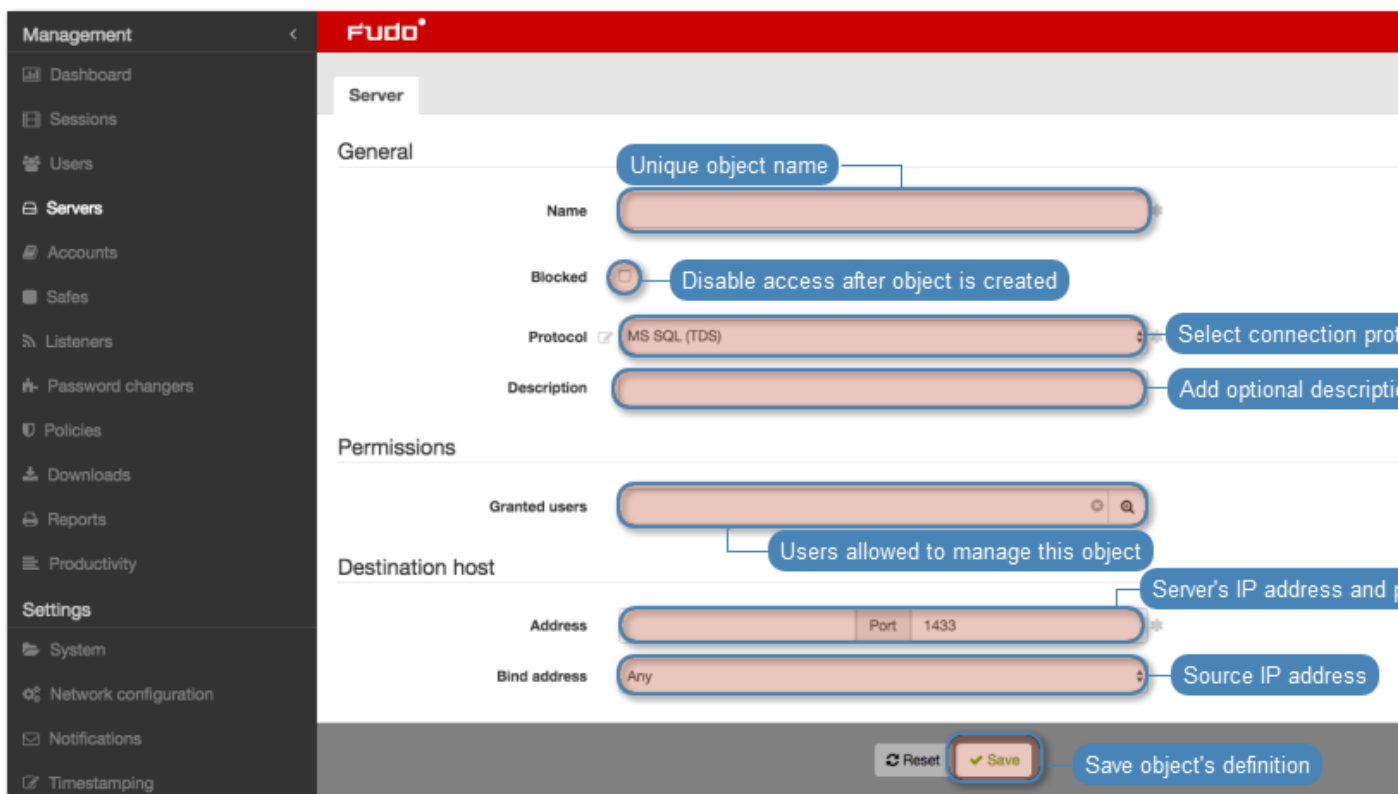
1. Select *Management > Servers*.
2. Click *+ Add*.



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. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

10. Click *Save*.



Related topics:

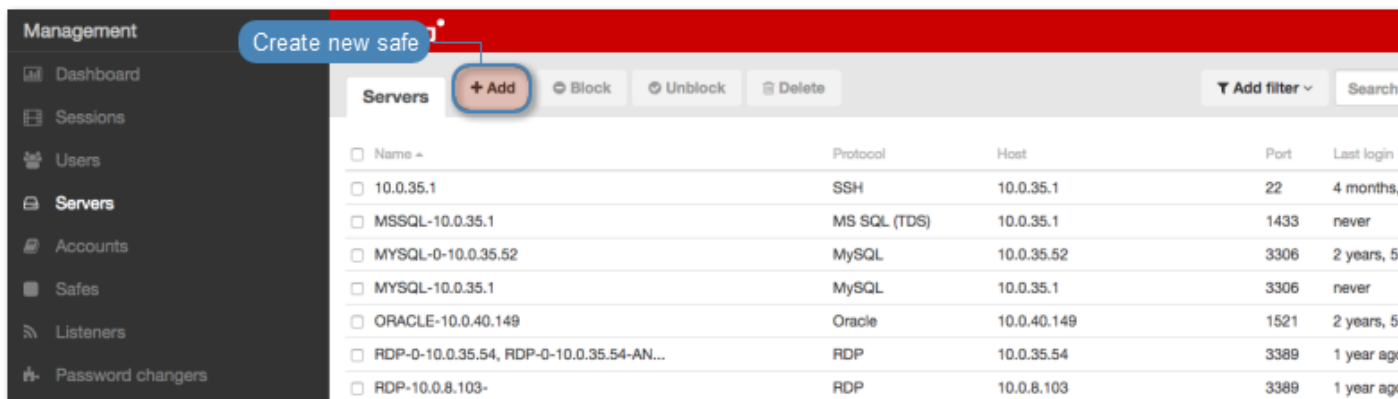
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

6.1.1.6 Creating a MySQL server

Note:

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

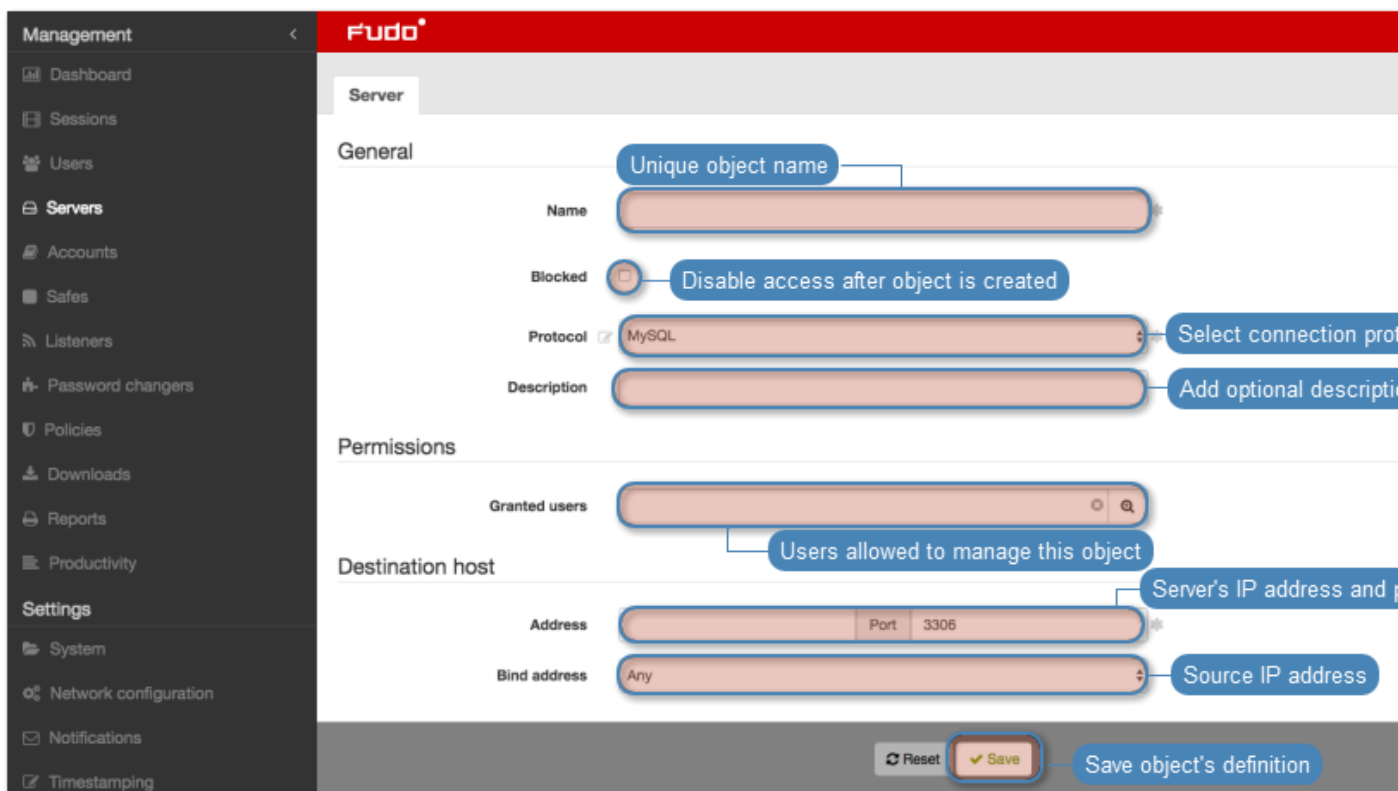
1. Select *Management > Servers*.
2. Click *+ Add*.



3. Enter server's unique name.
4. Select *Blocked* option to disable access to server after it's created.
5. Select 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. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

10. Click *Save*.



Related topics:

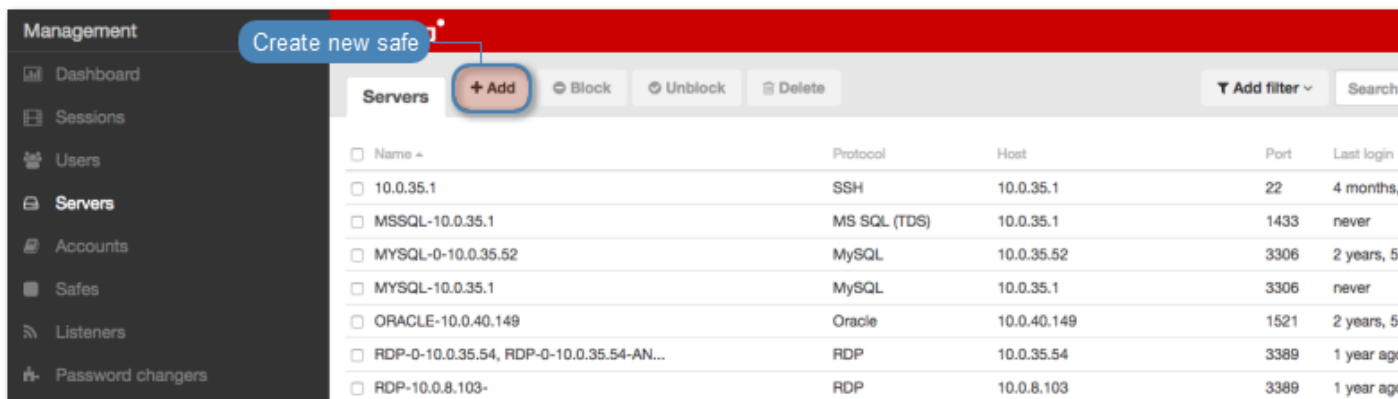
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

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.

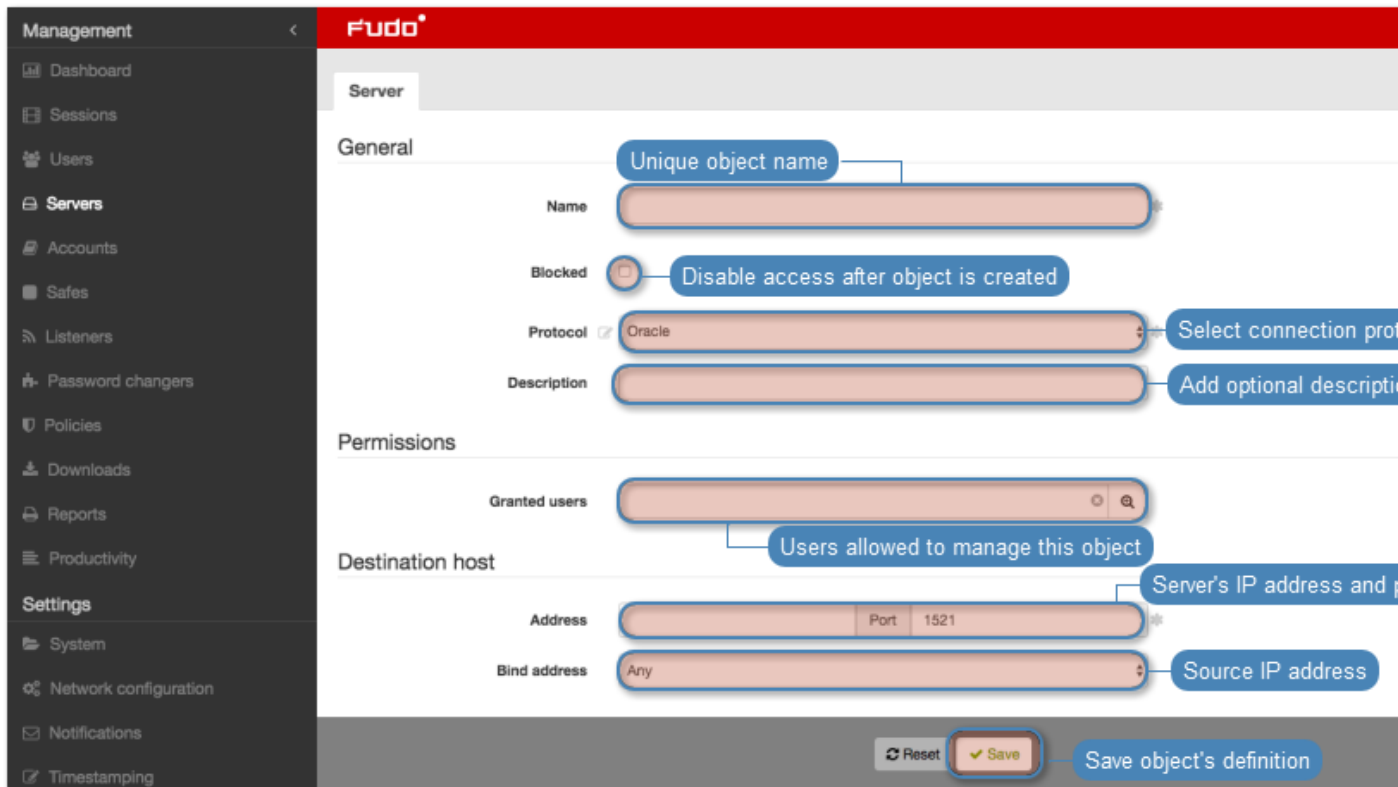
1. Select *Management > Servers*.
2. Click *+ Add*.



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. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

10. Click *Save*.



Related topics:

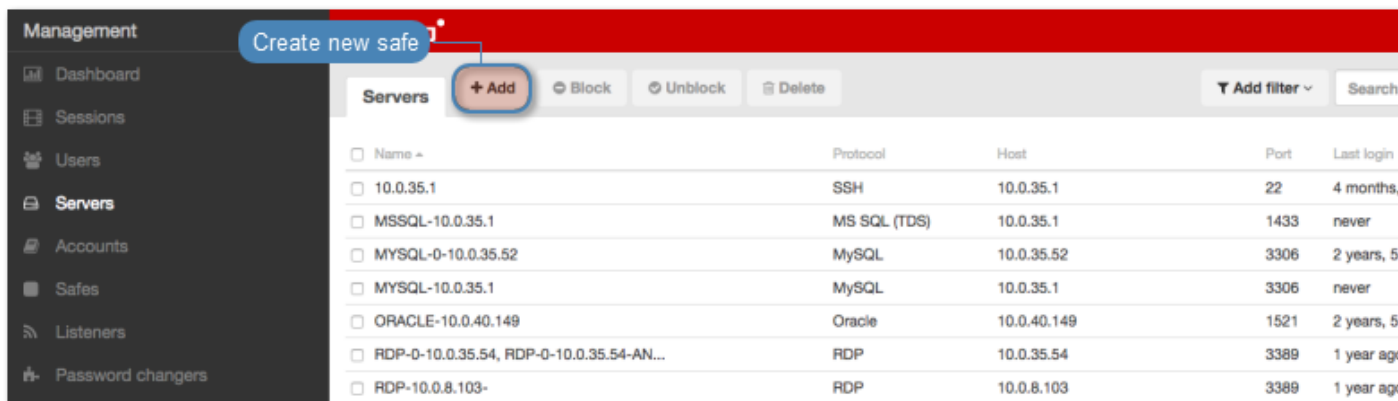
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

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.

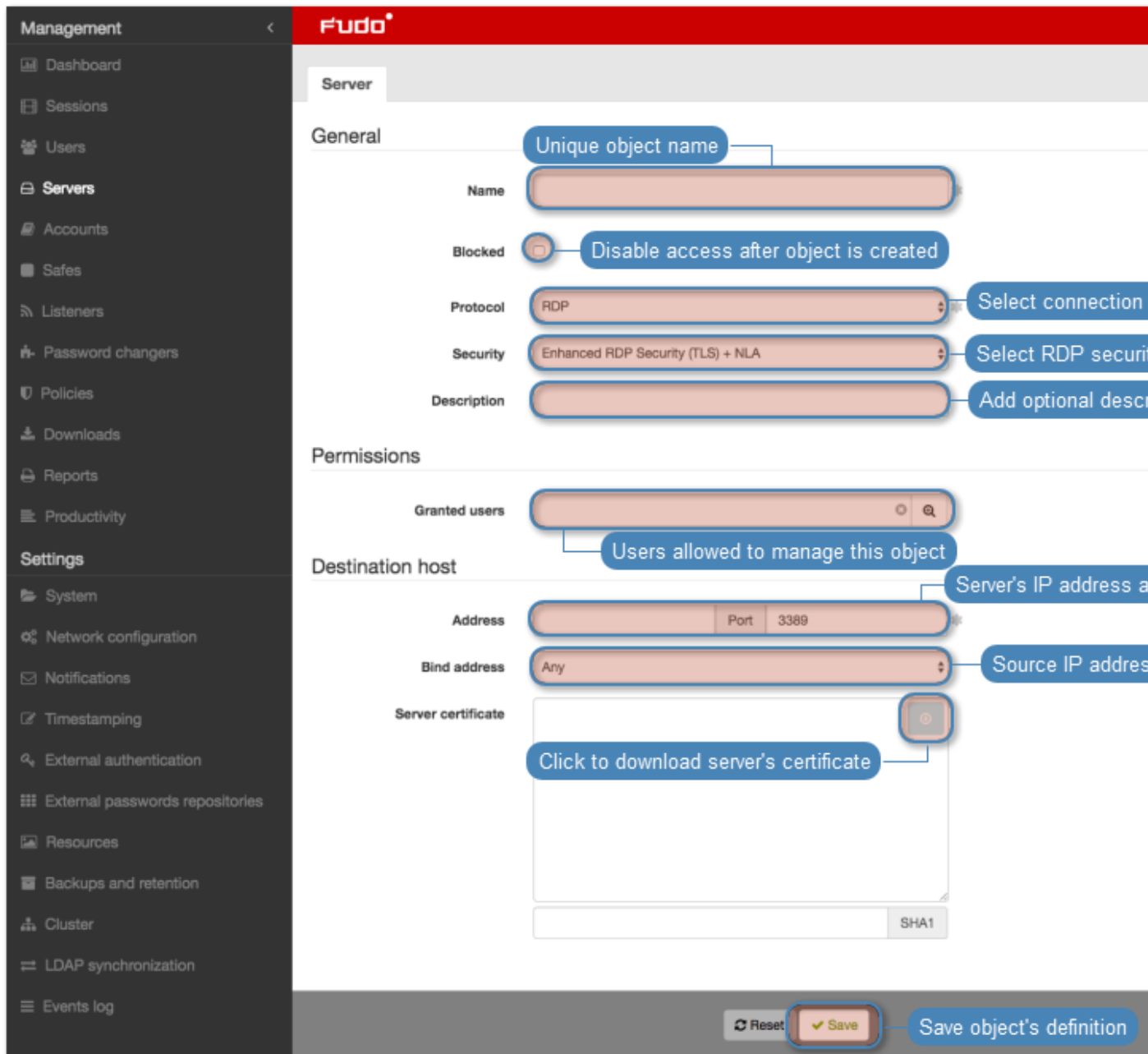
1. Select *Management > Servers*.
2. Click *+ Add*.



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. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

10. Click the fetch key icon to download server's certificate.
11. Click *Save*.



Related topics:

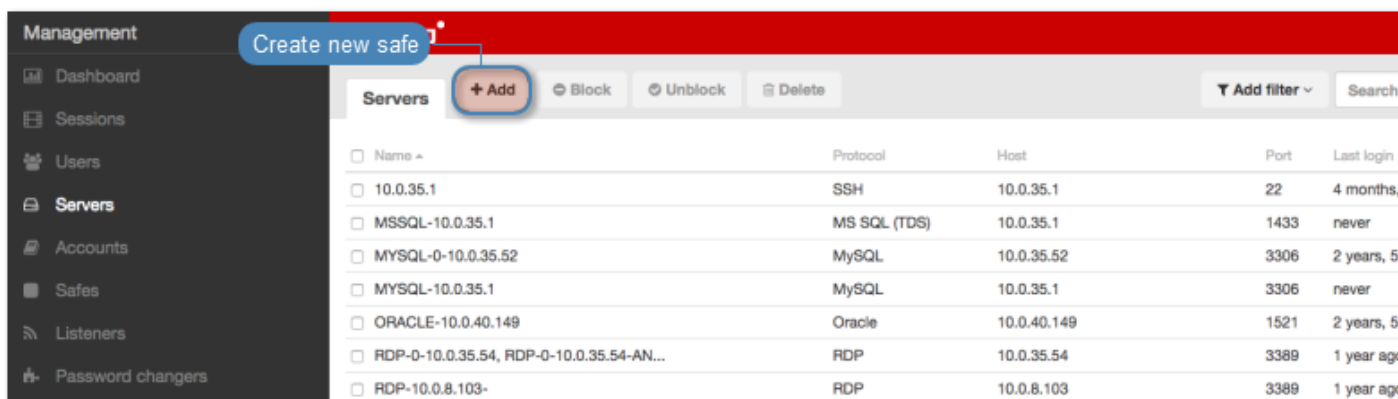
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

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.
-

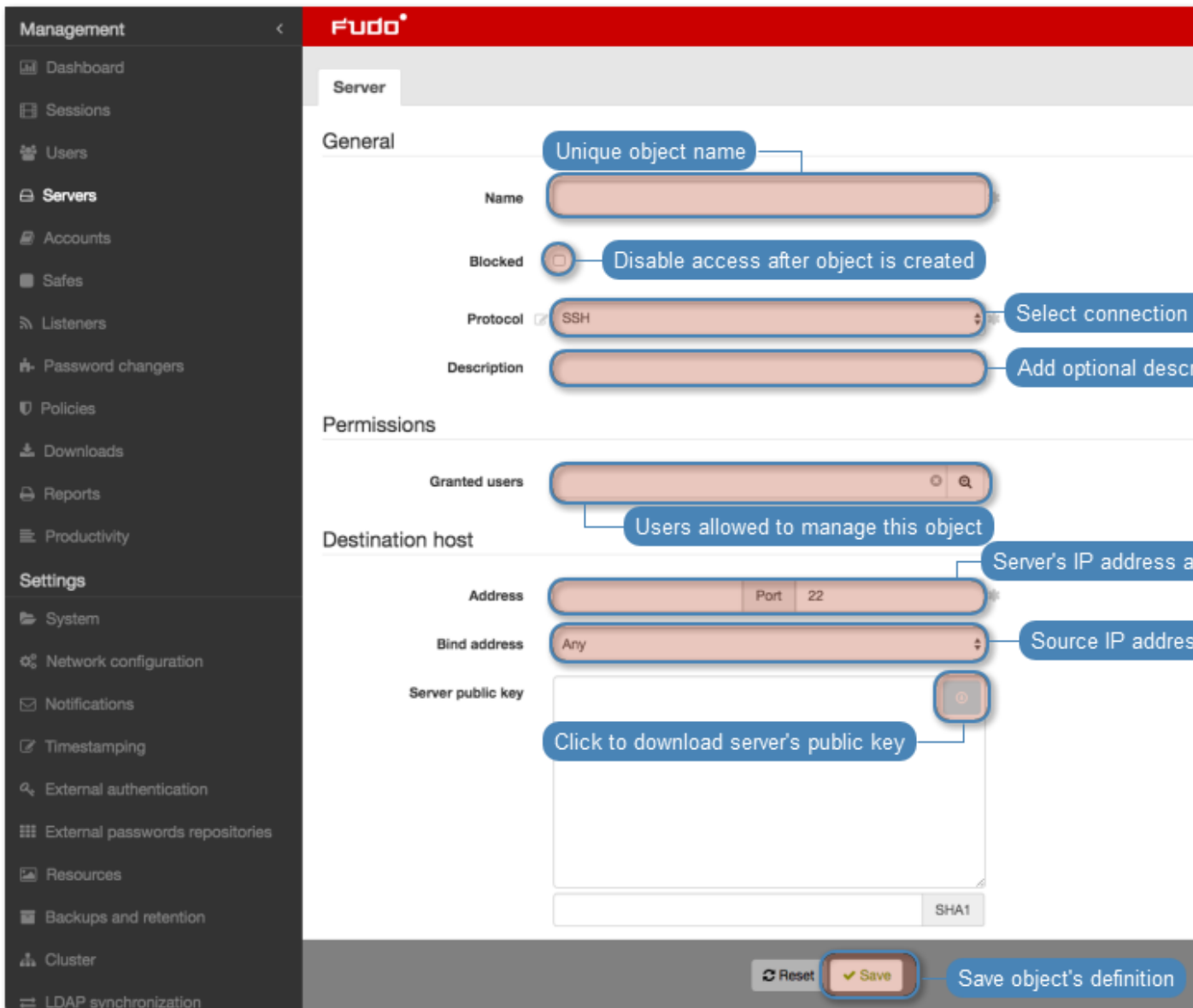
1. Select *Management > Servers*.
2. Click *+ Add*.



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. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

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*

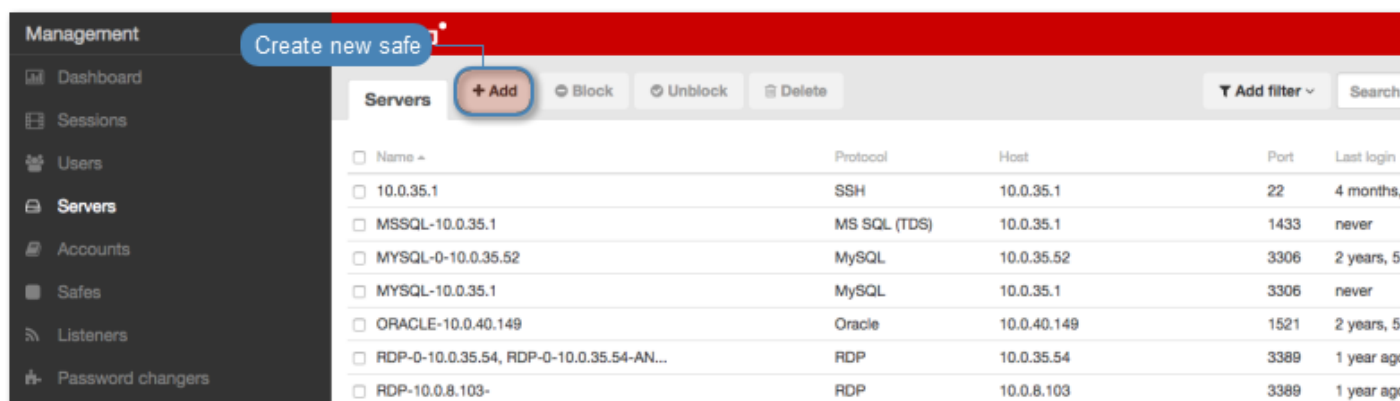
6.1.1.10 Creating a Telnet server

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.
-

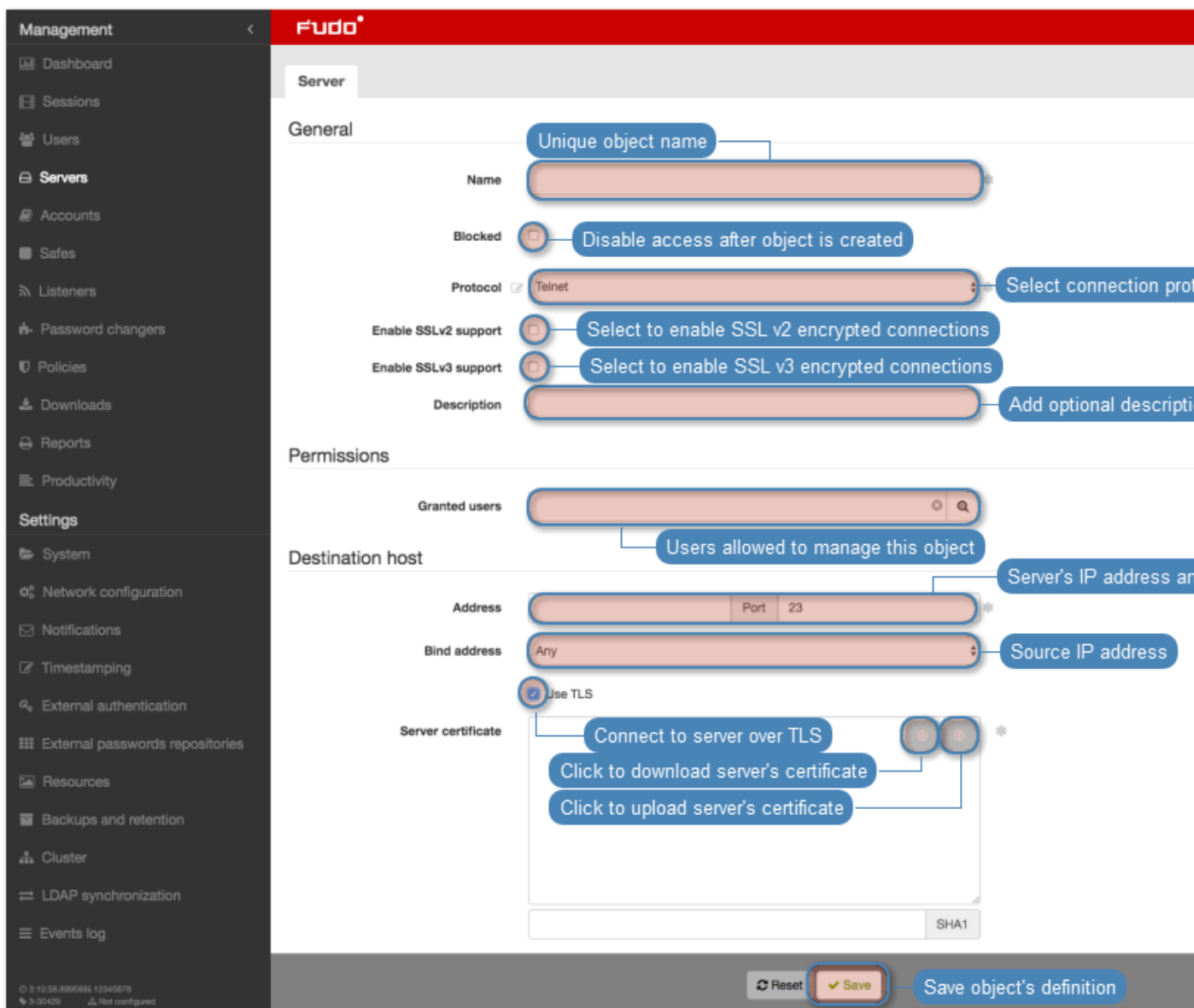
1. Select *Management > Servers*.
2. Click *+ Add*.



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. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
 7. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
 8. Enter optional description, which will help identifying this server object.
 9. In the *Permissions* section, add users allowed to manage this object.
 10. In the *Destination host* section, enter server's IP address and port number.
 11. 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.

12. Select the *Use TLS* options to connect to monitored server over TLS.
13. Click the certificate download icon to fetch server's certificate, or the certificate upload icon to upload a certificate.
14. Click *Save*.



Related topics:

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

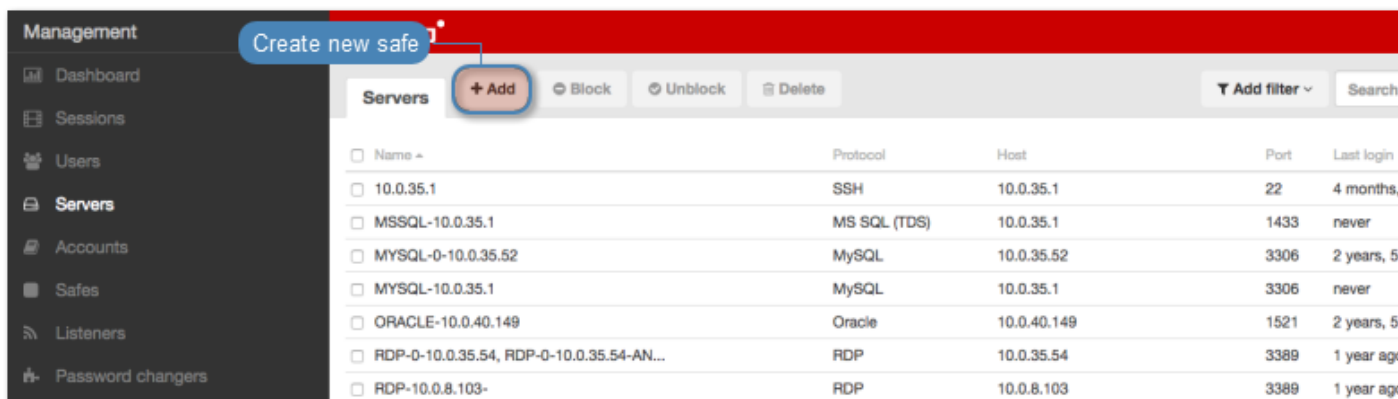
6.1.1.11 Creating a Telnet 3270 server

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.
-

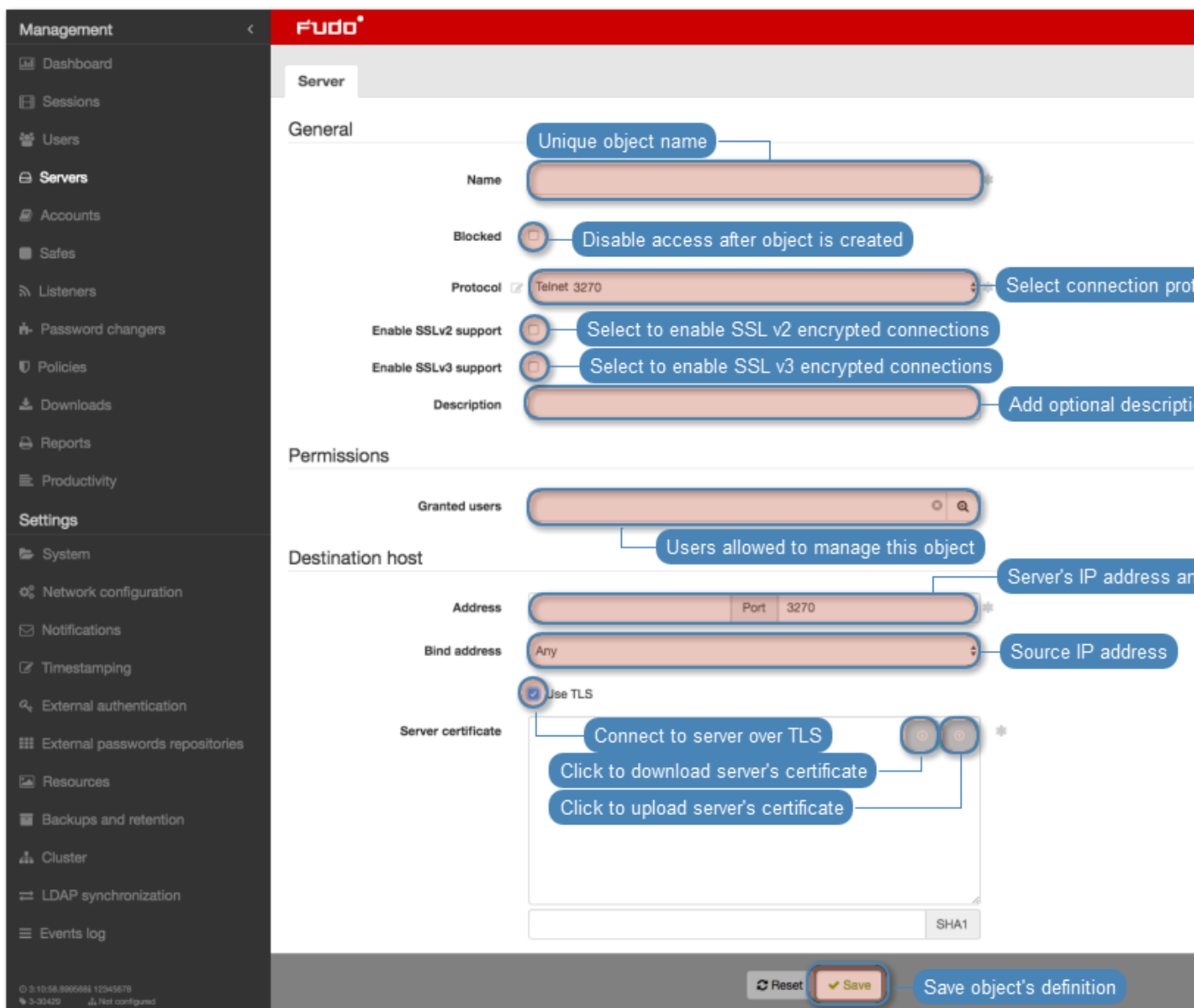
1. Select *Management > Servers*.
2. Click *+ Add*.



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. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
 7. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
 8. Enter optional description, which will help identifying this server object.
 9. In the *Permissions* section, add users allowed to manage this object.
 10. In the *Destination host* section, enter server's IP address and port number.
 11. 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.

12. Select the *Use TLS* options to connect to monitored server over TLS.
13. Click the certificate download icon to fetch server's certificate, or the certificate upload icon to upload a certificate.
14. Click *Save*.



Related topics:

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

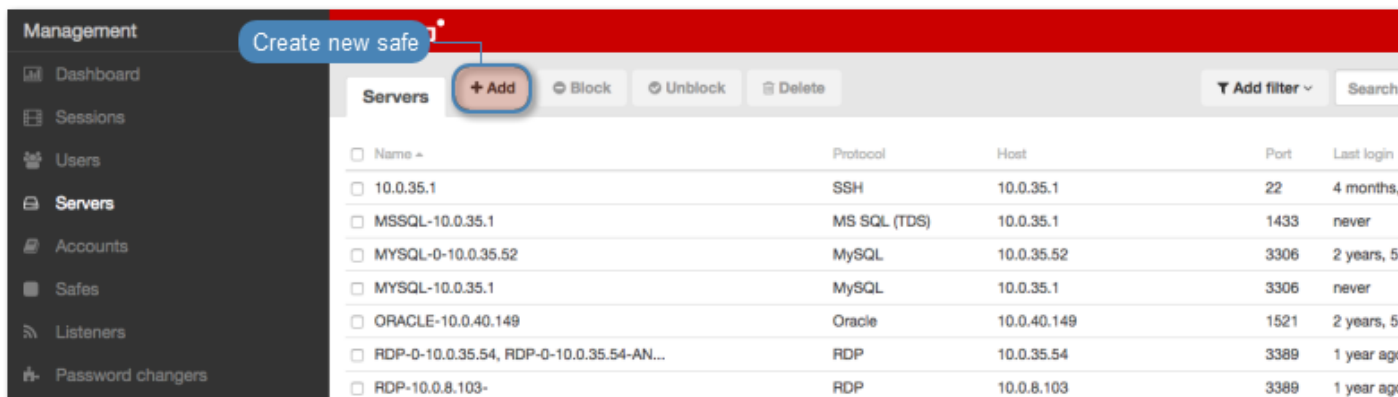
6.1.1.12 Telnet 5250 server

Adding an 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. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
7. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
8. Enter optional description, which will help identifying this server object.
9. In the *Permissions* section, add users allowed to manage this object.
10. In the *Destination host* section, enter server's IP address and port number.
11. 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.

12. Select the *Use TLS* options to connect to monitored server over TLS.
13. Click the certificate download icon to fetch server's certificate, or the certificate upload icon to upload a certificate.
14. Click *Save*.

Related topics:

- *Data model*

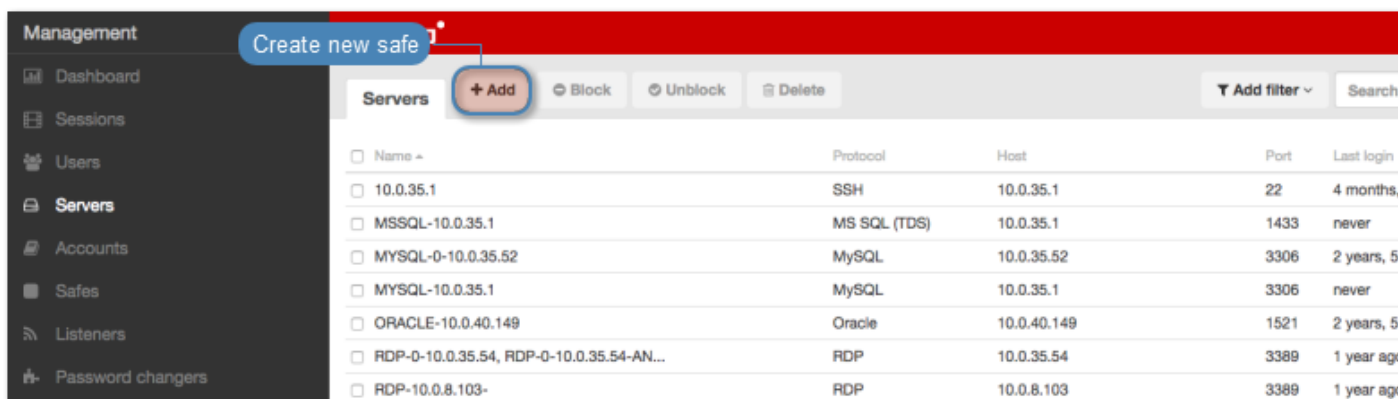
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

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. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

10. Click *Save*.

The screenshot shows the Fudo web interface for configuring a server. The left sidebar contains a navigation menu with categories like Management, Settings, and System. The main content area is titled 'Server' and is divided into three sections:

- General:**
 - Name:** A text input field with a callout 'Unique object name'.
 - Blocked:** A checkbox with a callout 'Disable access after object is created'.
 - Protocol:** A dropdown menu with 'VNC' selected and a callout 'Select connection protocol'.
 - Description:** A text input field with a callout 'Add optional description'.
- Permissions:**
 - Granted users:** A text input field with a search icon and a callout 'Users allowed to manage this object'.
- Destination host:**
 - Address:** A text input field with a 'Port' dropdown set to '5900' and a callout 'Server's IP address and port'.
 - Bind address:** A dropdown menu with 'Any' selected and a callout 'Source IP address'.

At the bottom right, there are 'Reset' and 'Save' buttons, with a callout 'Save object's definition' pointing to the Save button.

Related topics:

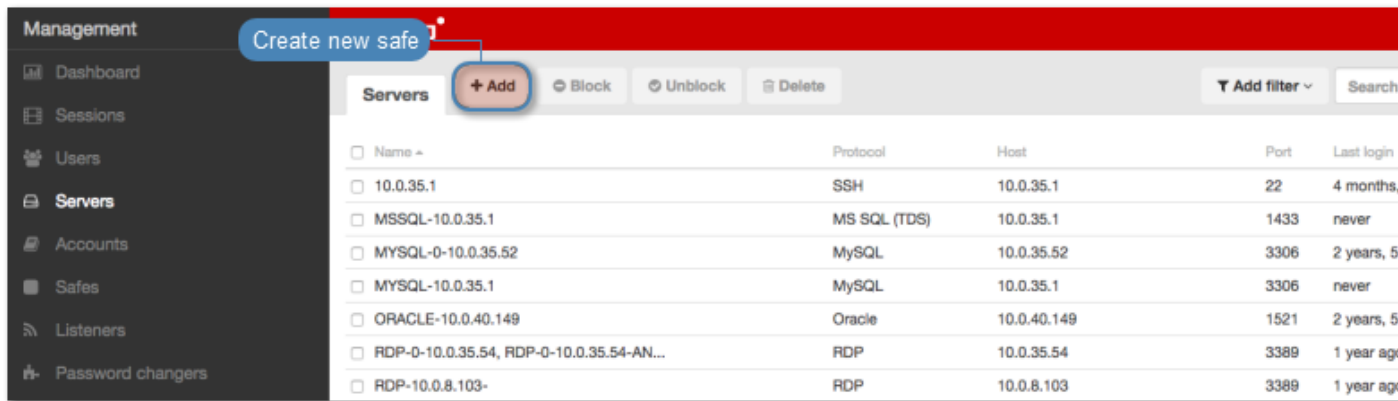
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

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.

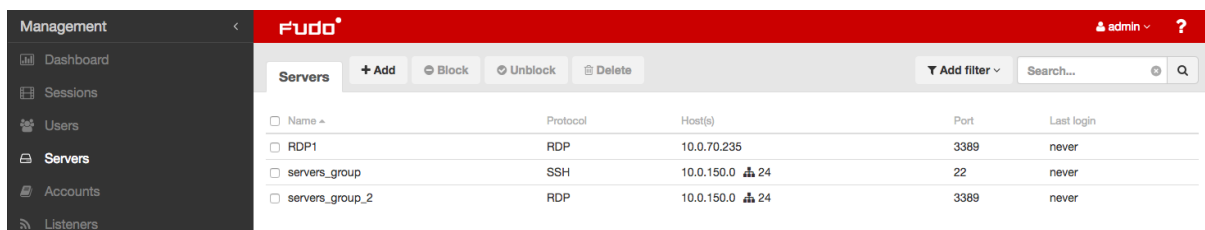
Note: The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu. Refer to *Network interfaces configuration* for more information on managing physical interfaces.

8. Click the **|icon-upload-key|** 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-servers-group|** icon.



3. Click *+ Add host*.
4. Provide server's IP address.

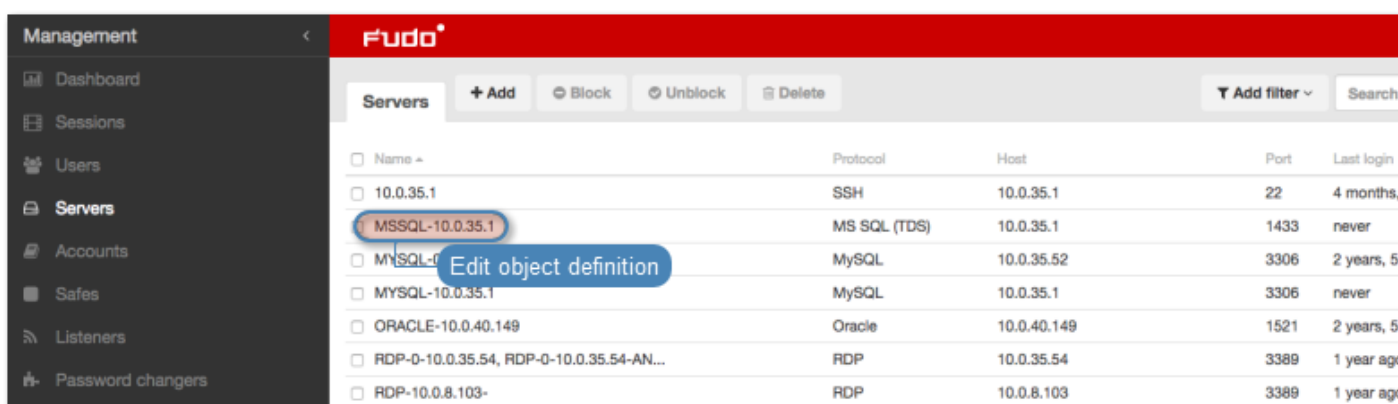
5. Click the  icon to download server's certificate.
6. Click *Save*.

Related topics:

- *Data model*
- *Static server*


6.2 Editing a server

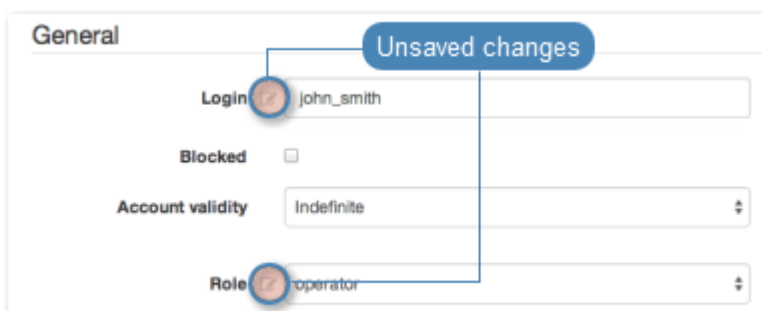
1. Select *Management > Servers*.
2. Find and click desired object to open its configuration page.



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

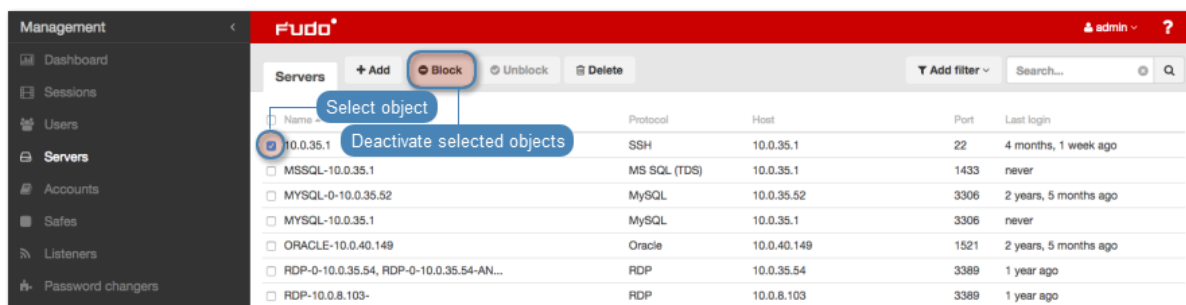
Wheel Fudo PAM allows blocking access to given server for all users.

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

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

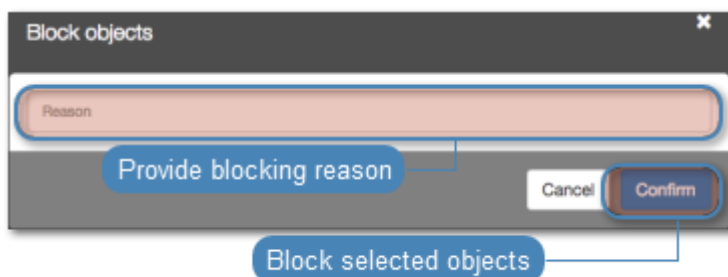
Note: Define filters to limit the number of objects displayed on the list.

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*

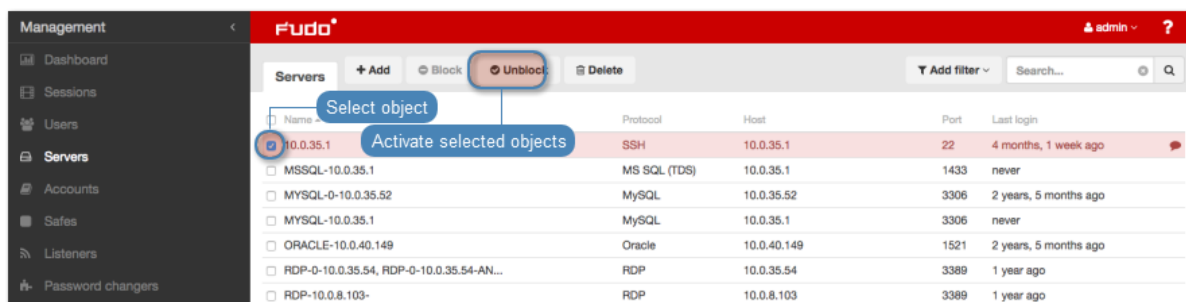
6.4 Unblocking a server

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

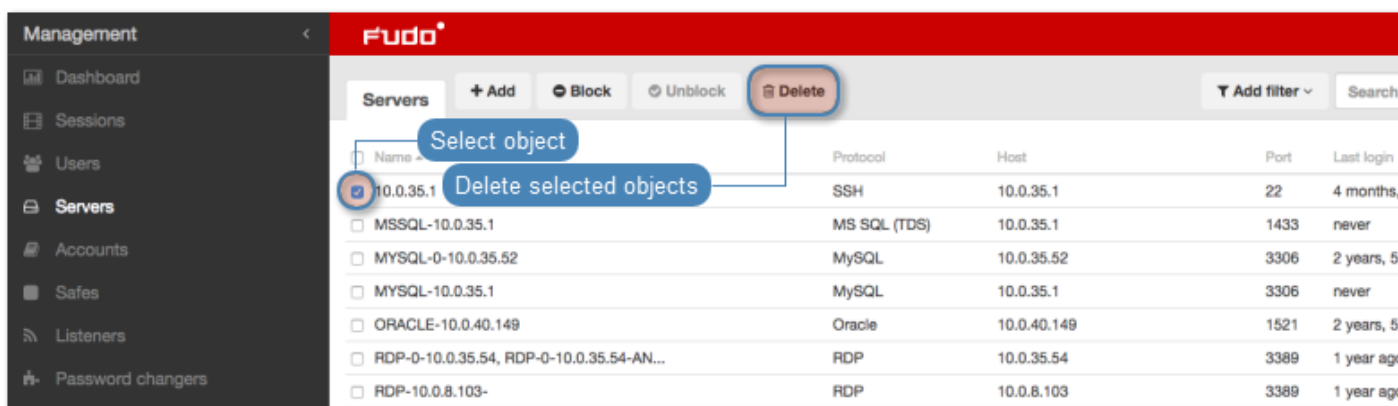
Warning: Deleting a server definition will terminate current connections with the given server.

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*.

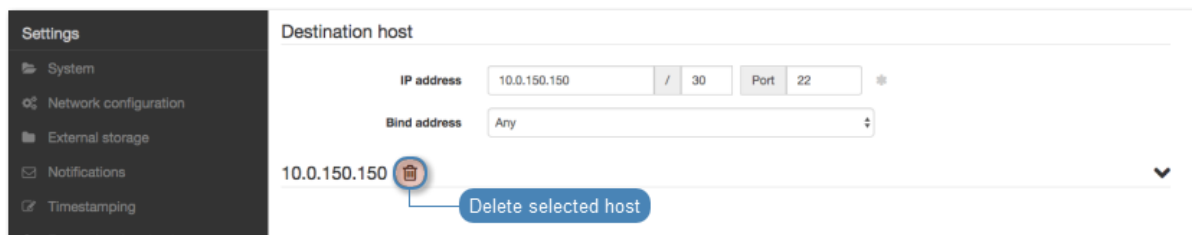


4. Confirm deletion of selected objects.



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*

CHAPTER 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.

The screenshot shows a web interface for managing accounts. A sidebar on the left contains a 'Management' menu with items like Dashboard, Sessions, Users, Servers, Accounts, Safes, Listeners, Password changers, Policies, Downloads, Reports, and Productivity. The main area is titled 'Accounts' and features a table of account entries. Above the table are buttons for '+ Add', 'Block', 'Unblock', and 'Delete', along with an 'Add filter' dropdown and a search box. A red bar at the top of the interface contains buttons for 'Activate selected accounts', 'Deactivate selected accounts', and 'Delete selected accounts'. A 'Create new account' button is also visible. The table lists accounts with columns for Name, Server, Recording, Type, Password change policy, and Password char. The 'admin@windows7' account is highlighted with a blue callout 'Edit account definition'. The 'vnc' account is highlighted with a blue callout 'Blocked account'. A 'Hover to view th' callout is also present at the bottom right.

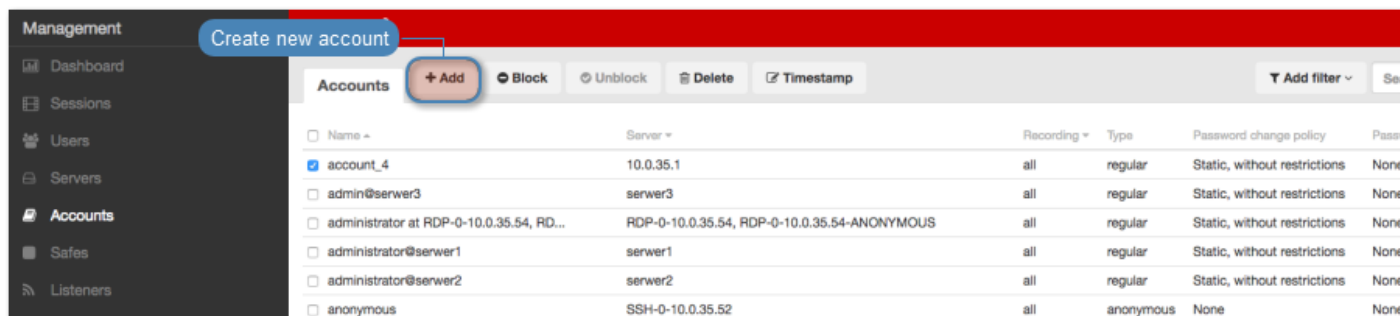
Name	Server	Recording	Type	Password change policy	Password char
acc	CentOS	all	regular	Static, without restrictions	None
admin@win2012	Windows2012	all	regular	Static, without restrictions	None
admin@windows7	Windows7	all	regular	Static, without restrictions	None
anonymous		all	anonymous	None	None
asd	CentOS	all	regular	Static, without restrictions	None
joe@FreeBSD10	FreeBSD10	all	regular	Random, 8 length, change 1 hour	Unix Account
root@CentOS	CentOS	all	regular	Static, without restrictions	None
root@freebsd10	FreeBSD10	all	regular	Static, without restrictions	None
vnc	vnc	all	regular	Static, without restrictions	None

7.1 Creating an account

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

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** - Wheel Fudo PAM records network traffic allowing for future session playback, using the built in session player, as well as converting session material to a selection of video file formats.
 - **raw** - Wheel Fudo PAM keeps records of the data exchanged between the user and the monitored server. The raw data can be downloaded later on but the session cannot be played back using the built in session player.
 - **none** - Wheel Fudo PAM only takes note of the fact that the give session took place but does not record the data exchanged between the user and the server.
7. Select the *OCR sessions* option to fully index RDP and VNC sessions contents.
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 be 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*.

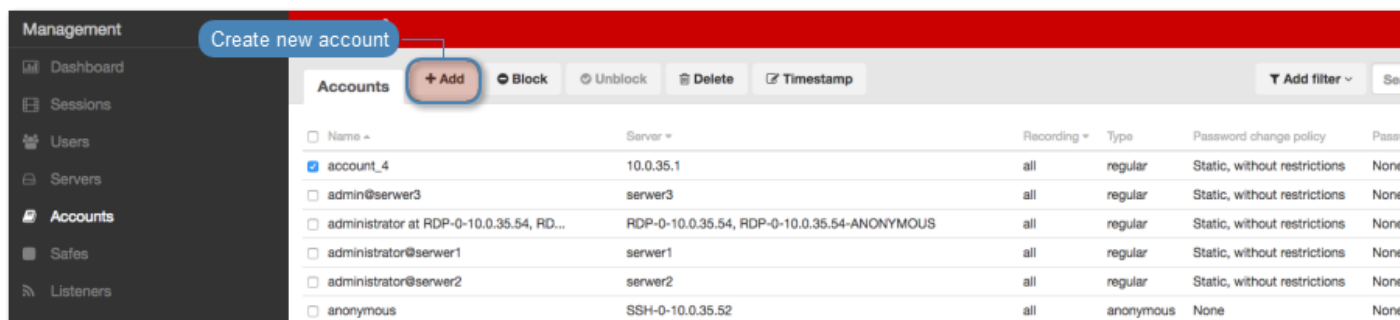
The screenshot shows the 'Account' configuration page in the Fudo PAM 3.5 interface. The page is organized into three main sections: General, Permissions, and Server. The 'General' section contains several configuration options, each with a callout box explaining its function. The 'Permissions' section includes a field for 'Granted users'. The 'Server' section includes a field for 'Server'. At the bottom right, there are 'Reset' and 'Save' buttons, with the 'Save' button highlighted and a callout box indicating its purpose.

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** - Wheel Fudo PAM records network traffic allowing for future session playback, using the built in session player, as well as converting session material to a selection of video file formats.
 - **raw** - Wheel Fudo PAM keeps records of the data exchanged between the user and the monitored server. The raw data can be downloaded later on but the session cannot be played back using the built in session player.
 - **none** - Wheel Fudo PAM only takes note of the fact that the give session took place but does not record the data exchanged between the user and the server.
7. Select the *OCR sessions* option to fully index RDP and VNC sessions contents.
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.

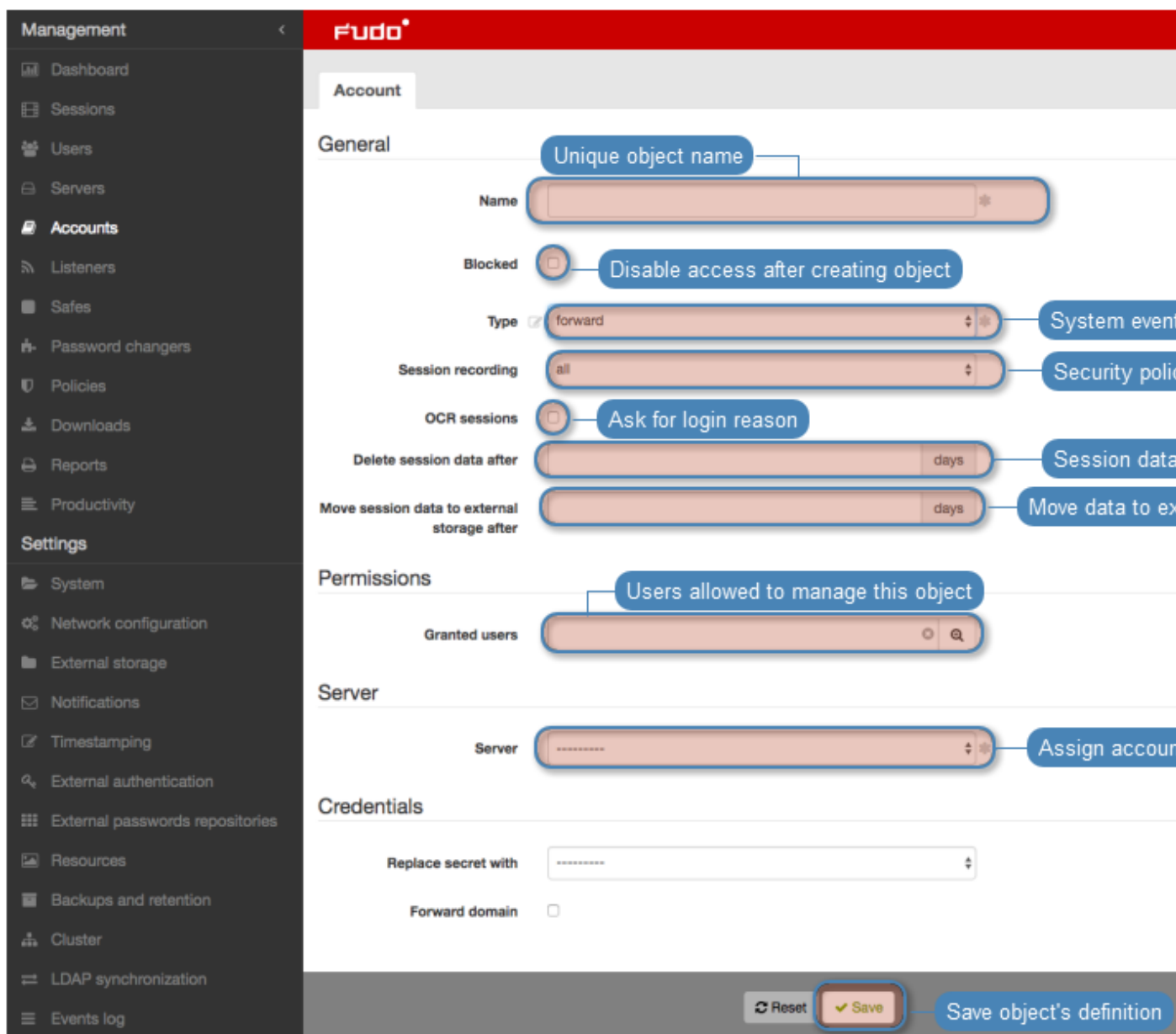
Note: *Two-fold authentication*

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

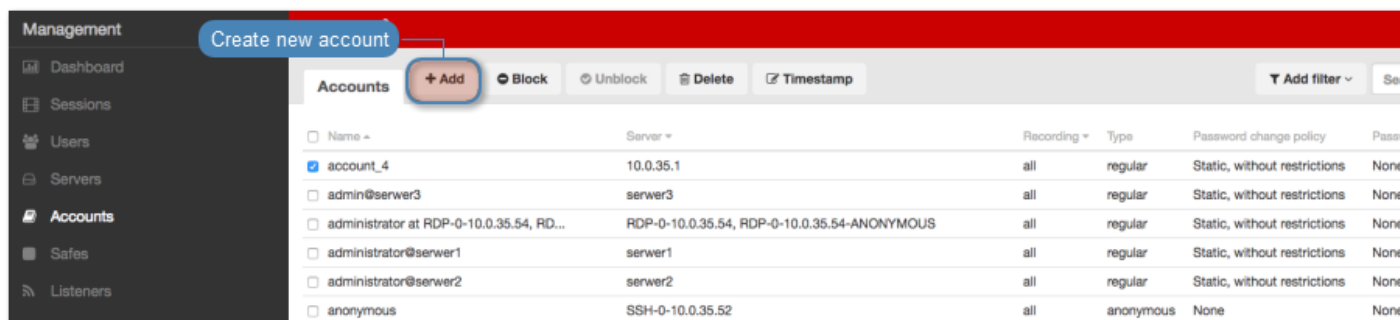


Related topics:

- *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* - Wheel Fudo PAM records network traffic allowing for future session playback, using the built in session player, as well as converting session material to a selection of video file formats.
 - *raw* - Wheel Fudo PAM keeps records of the data exchanged between the user and the monitored server. The raw data can be downloaded later on but the session cannot be played back using the built in session player.
 - *none* - Wheel Fudo PAM only takes note of the fact that the give session took place but does not record the data exchanged between the user and the server.
7. Select the *OCR sessions* option to fully index RDP and VNC sessions contents.



Note: Indexing sessions enables full-text content searching.

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 be 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.

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.

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 poprzez SSH

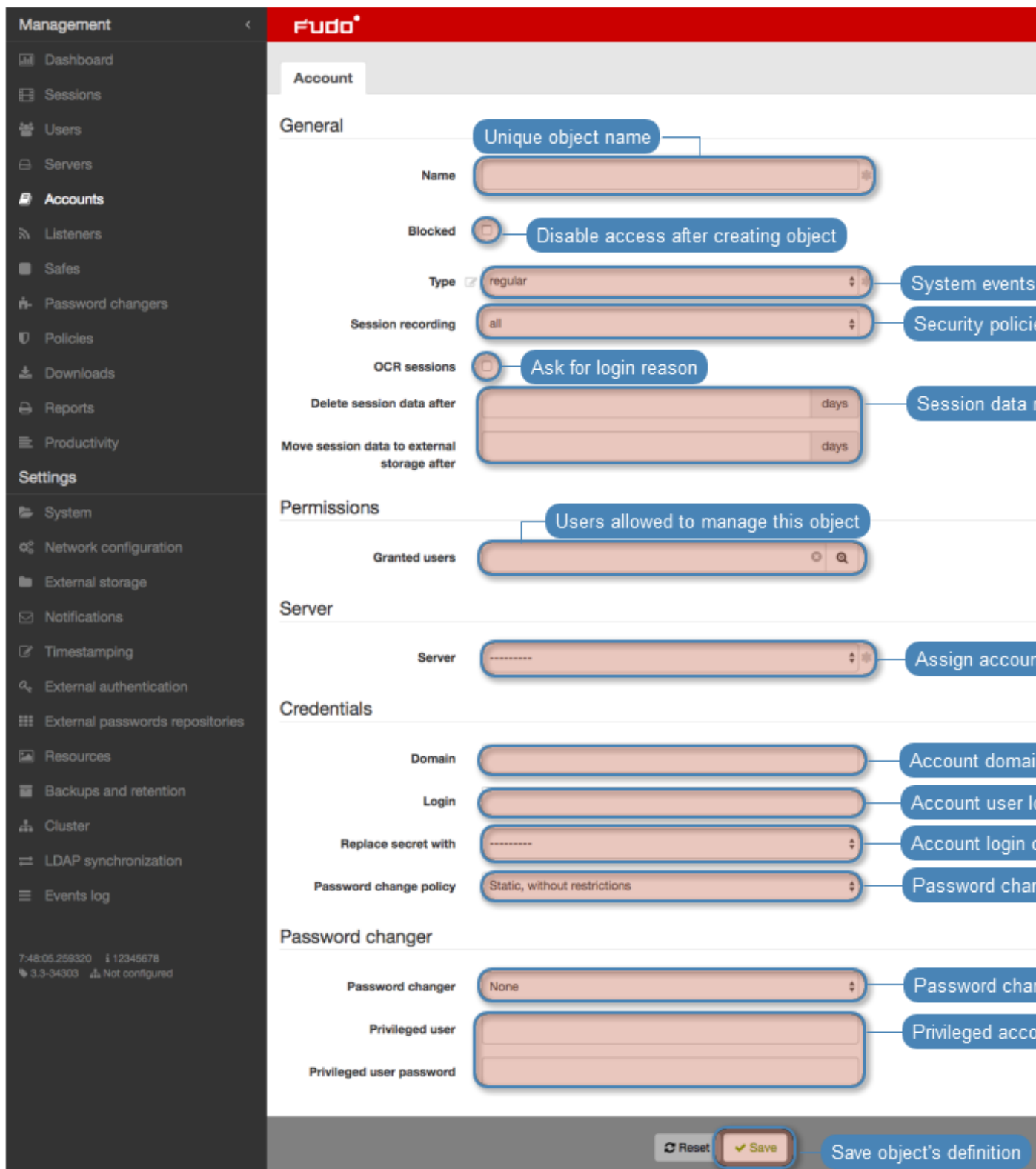
- Provide privileged mode password.
- Enter privileged user name.
- Enter privileged user password.

LDAP

- Enter privileged user name.
- Enter privileged user password.
- Wprowadź parametr bazowy LDAP (LDAP base).
- Wgraj certyfikat CA serwera LDAP.

Note: Privileged user account is used for changing the password when system detects that password has been changed in an unauthorized way.

18. Click *Save*.



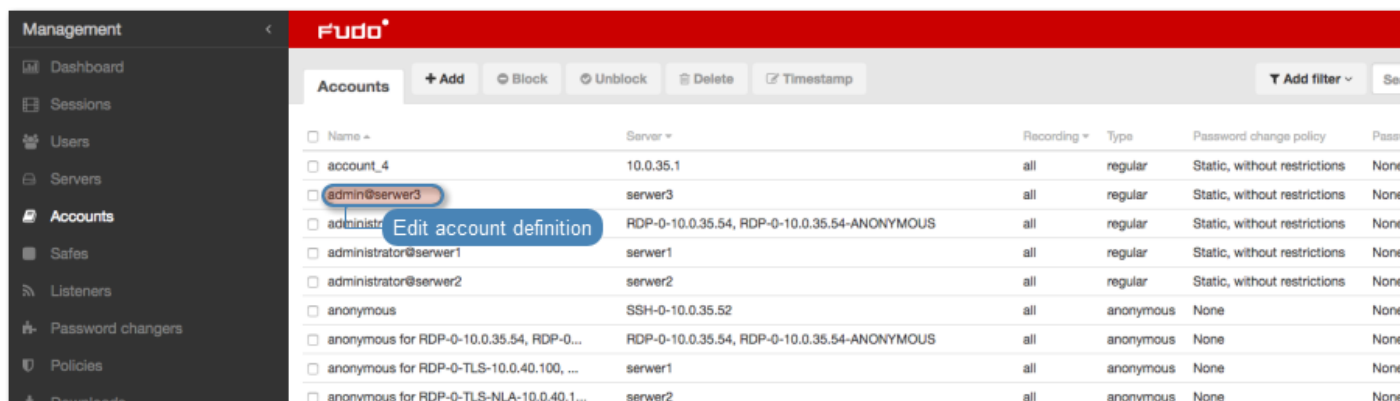
Related topics:

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

- *Unblocking an account*
- *Deleting an account*


7.2 Editing an account

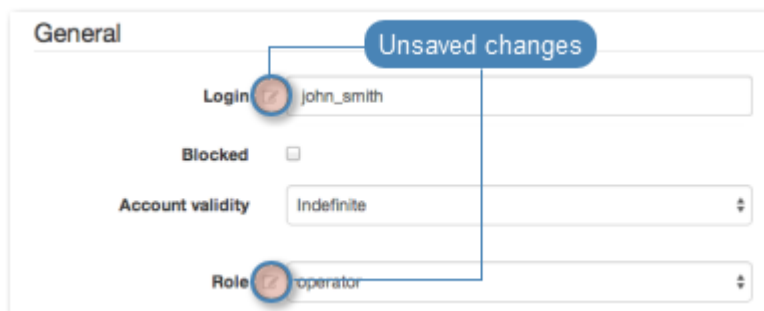
1. Select *Management > Accounts*.
2. Find and click desired object to open its configuration page.



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*.

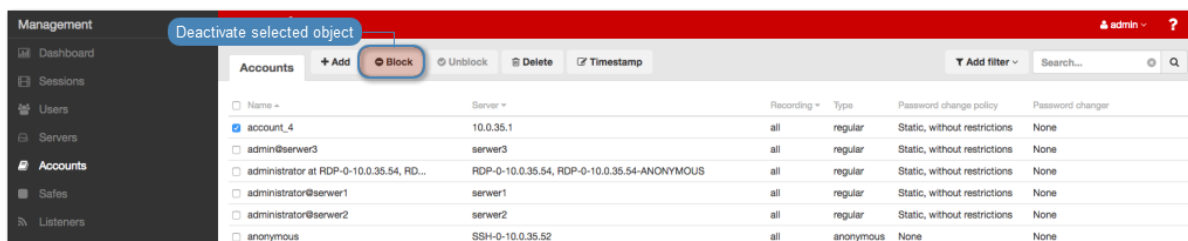
Related topics:

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


7.3 Blocking an account

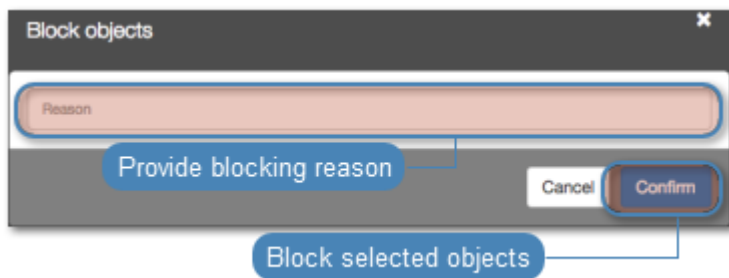
Warning: Blocking an account definition will terminate all current connections to servers which use selected account for accessing those servers.

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.

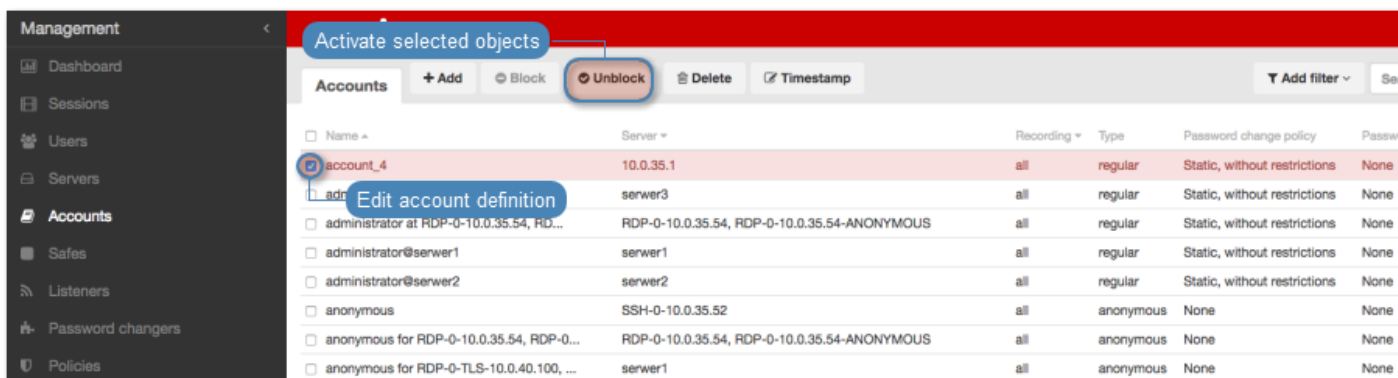


Related topics:

- *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.



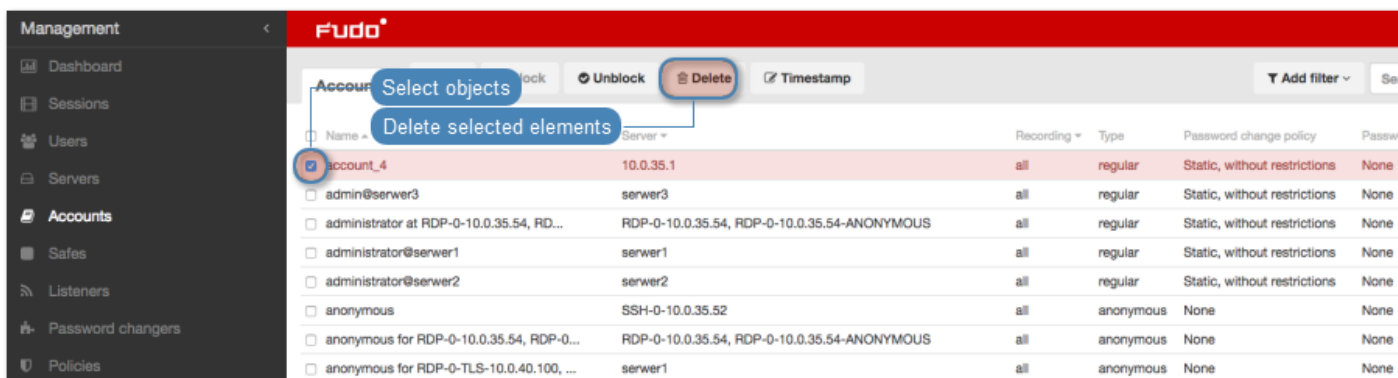
Related topics:

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

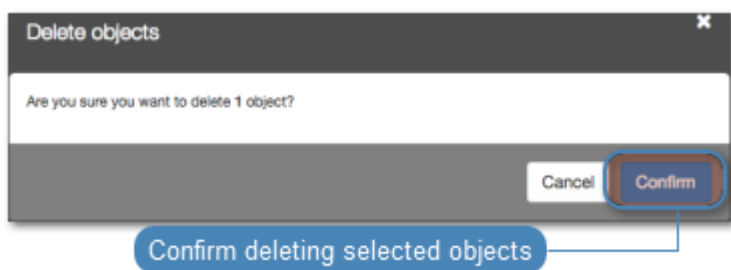
7.5 Deleting an account

Warning: Deleting an account 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*.



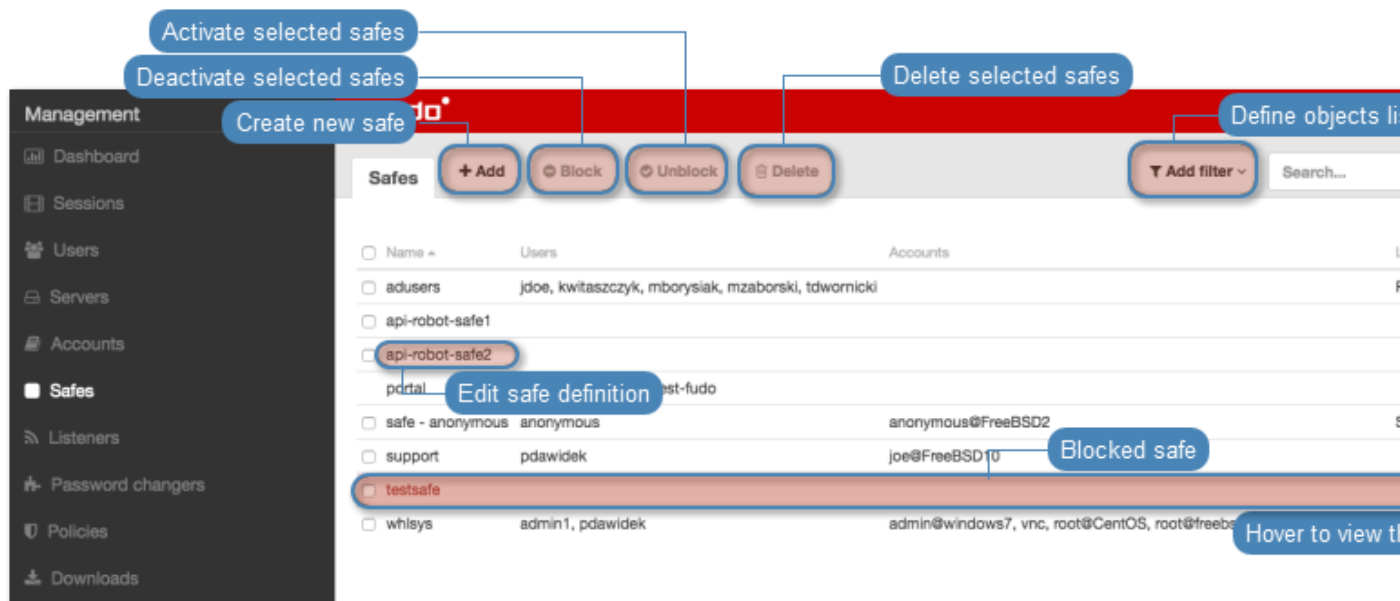
4. Confirm deletion of selected objects.



Related topics:

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

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



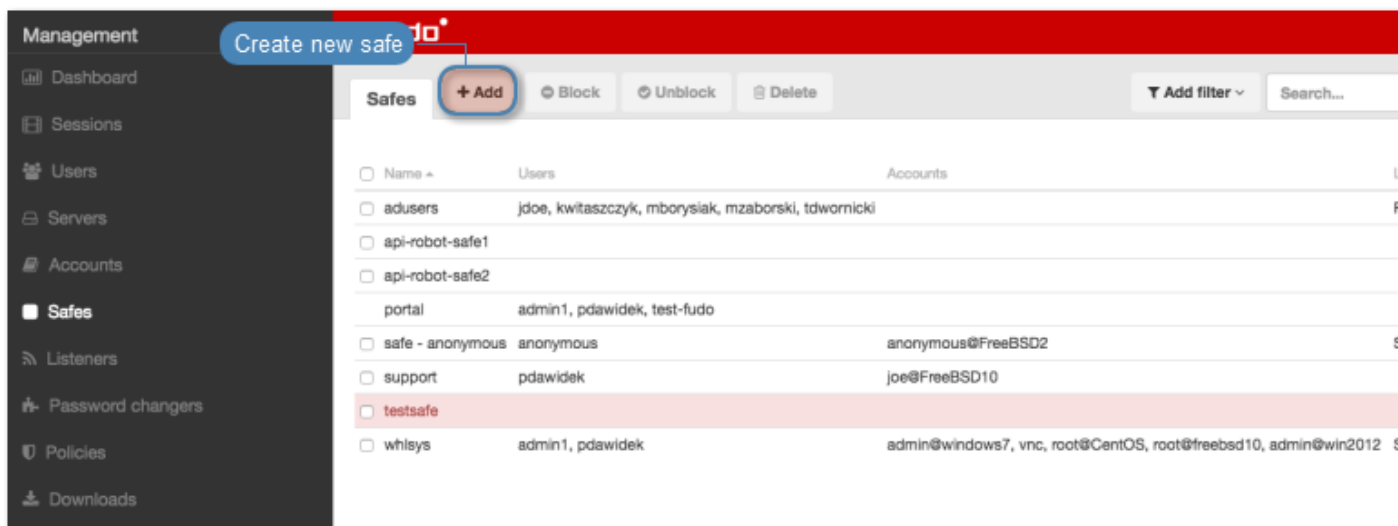
Note:

- 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

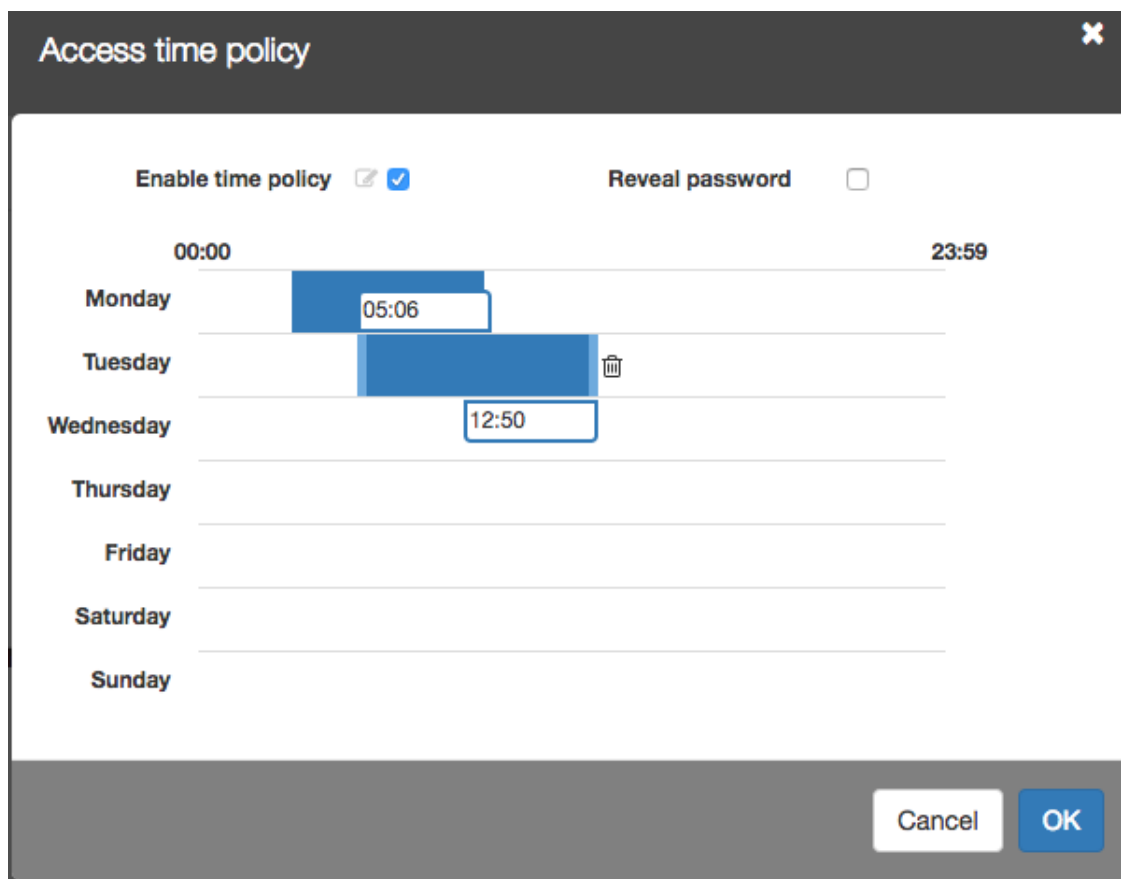
Warning: Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances must not be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.


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 *Notifications* option and choose notifications sent out to Wheel Fudo PAM administrator.
7. Assign *security policies* in the *Policies* field.
8. 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.



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

Management

- Dashboard
- Sessions
- Users
- Servers
- Accounts
- Listeners
- Safes**
- Password changers
- Policies
- Downloads
- Reports
- Productivity

Settings

- System
- Network configuration
- External storage
- Notifications
- Timestamping
- External authentication
- External passwords repositories
- Resources
- Backups and retention
- Cluster
- LDAP synchronization
- Events log

6 days | 00000002
head-33959 | Not configured

Safe

General

Name

Blocked

Login reason

Notifications

- Session start
- Session join
- Session policy match
- Session finish
- Session leave

Policies

Users

Protocol functionality

RDP

- Clipboard redirection
- Device redirection
- Audio input redirection
- Sound redirection
- Dynamic Virtual Channels
- Multimedia redirection

Max. resolution Resolution Max. color depth Color depth

SSH

- Sessions
- Terminal
- X11
- Shell
- SFTP
- Port forwarding
- Environment
- SSH Agent forwarding
- SCP

VNC

- Client Cut Text
- Server Cut Text

Management permissions

Granted users

Accounts

Account#1 ssh0 ssh2 ssh1

Account#2

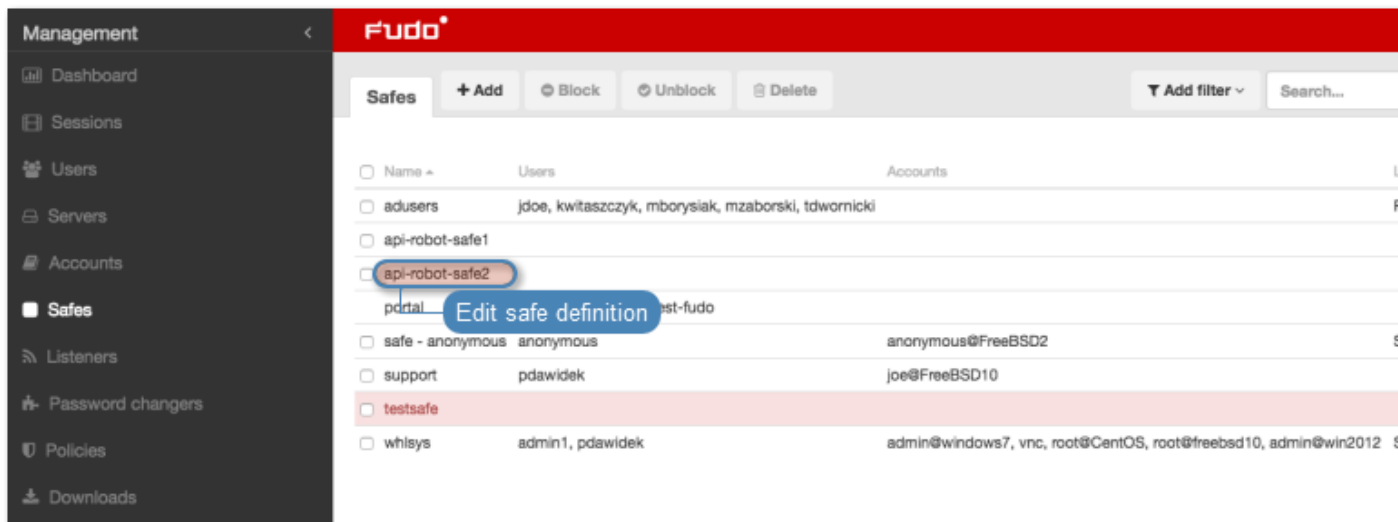
Select account Add listeners...

Related topics:

- [Data model](#)
- [Editing a safe](#)
- [Blocking a safe](#)
- [Deleting a safe](#)


8.2 Editing a safe

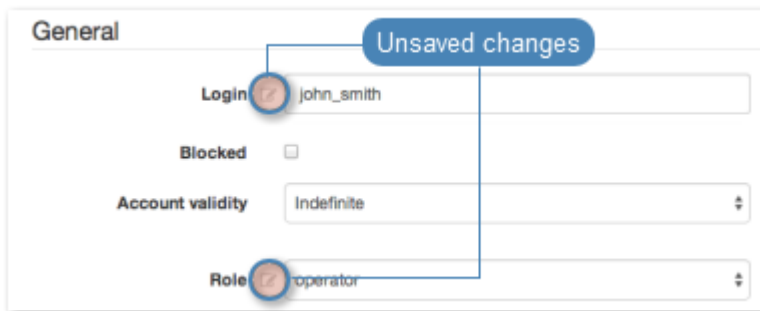
1. Select *Management* > *Safes*.
2. Find and click desired object to open its configuration page.



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*

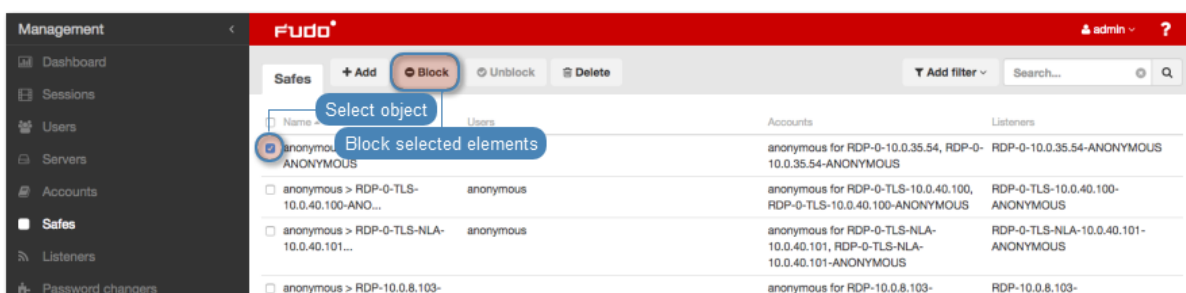
8.3 Blocking a safe

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.

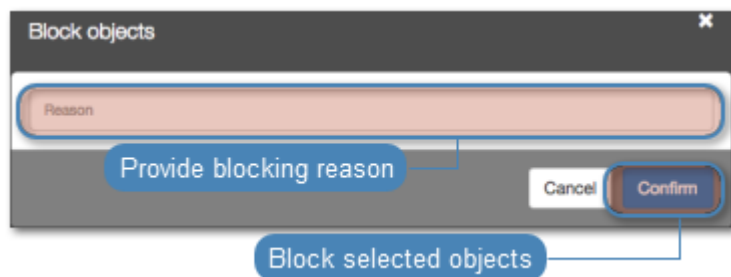
Note: Define filters to limit the number of objects displayed on the list.

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*

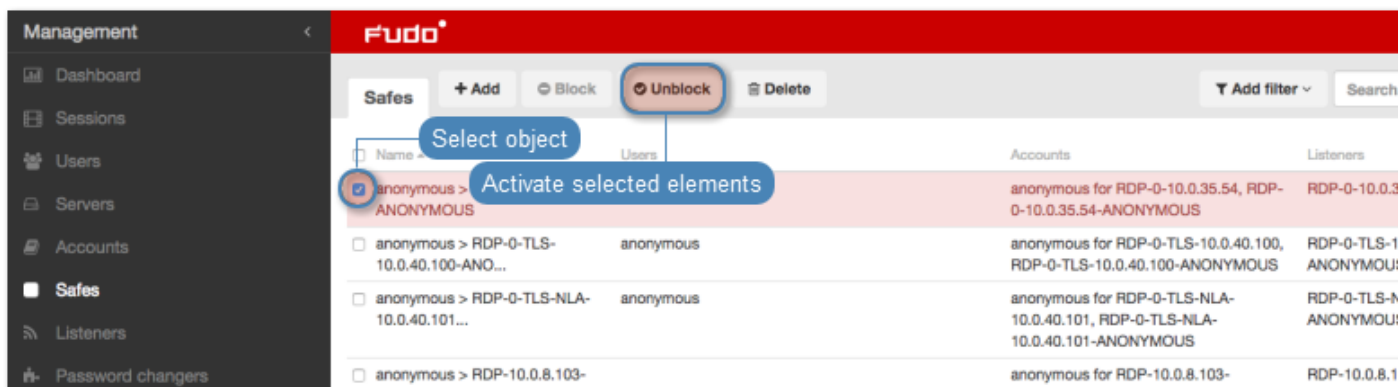
8.4 Unblocking a safe

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*

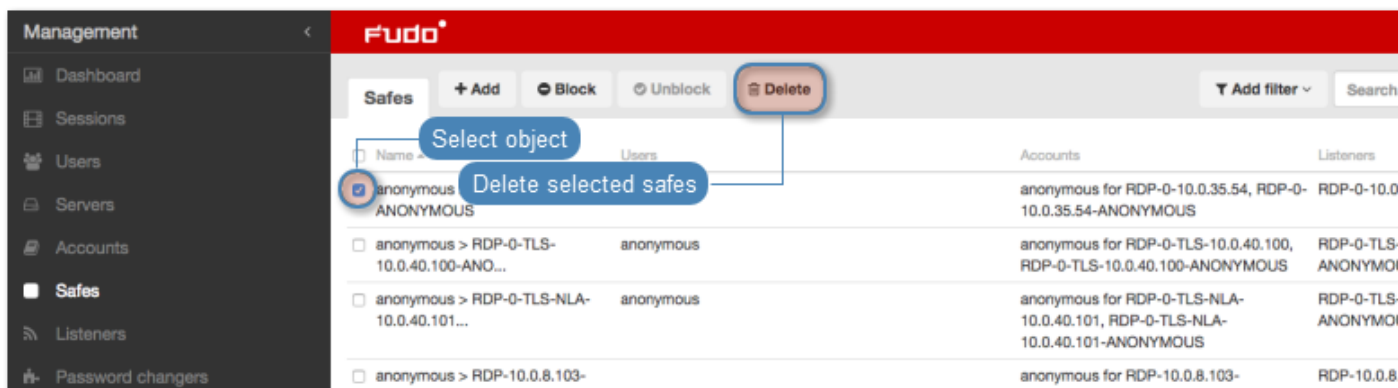
8.5 Deleting a safe

Warning: Deleting a safe definition will terminate all current connections that use accounts assigned to this safe to connect to servers.

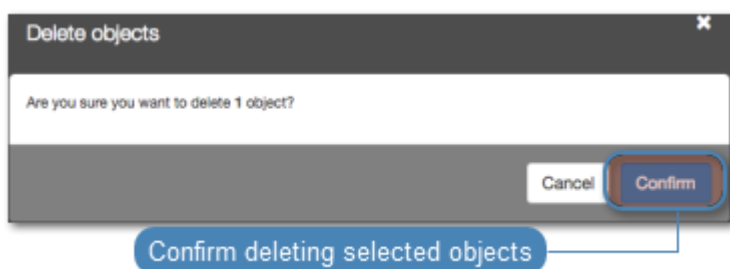
1. Select *Management > Safes*.
2. Find and select desired objects.

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*

Listeners

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

The screenshot shows the 'Listeners' management interface. A red bar at the top contains buttons for '+ Add', 'Block', 'Unblock', and 'Delete'. Below this is a table of listeners. Callouts point to various elements: 'Activate selected listeners' points to the 'Block' button; 'Deactivate selected listeners' points to the 'Unblock' button; 'Create new listener' points to the '+ Add' button; 'Delete selected listeners' points to the 'Delete' button; 'Define objects li' points to the 'Add filter' button; 'Edit safe definition' points to the 'SSH - Anonymous' row; 'Blocked listener' points to the 'vnc' row; and 'Hover to view t' points to the 'vnc' row.

Name	Safes	Listen address	Protocol	Mo
<input type="checkbox"/> RDP	adusers, whlsys	10.0.8.60:3389	RDP	ba
<input type="checkbox"/> SSH	whlsys	10.0.8.160:22	SSH	ba
<input type="checkbox"/> SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	pro
<input type="checkbox"/> rdp2	whlsys	10.0.8.60:9999	RDP	ba
<input type="checkbox"/> ssh-listener		10.0.8.60:6	SSH	pro
<input checked="" type="checkbox"/> vnc	whlsys	10.0.8.60:59102	VNC	pro

Note:

- A listener cannot link to an account that is assigned to a server with a different protocol than 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*.
-

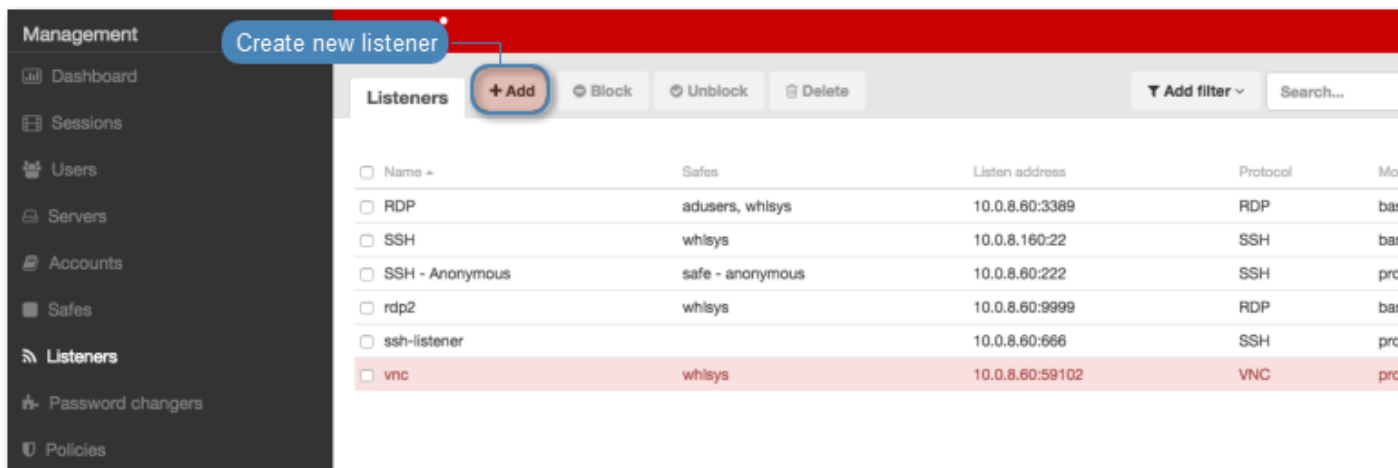
9.1 Creating a listener

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.

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.

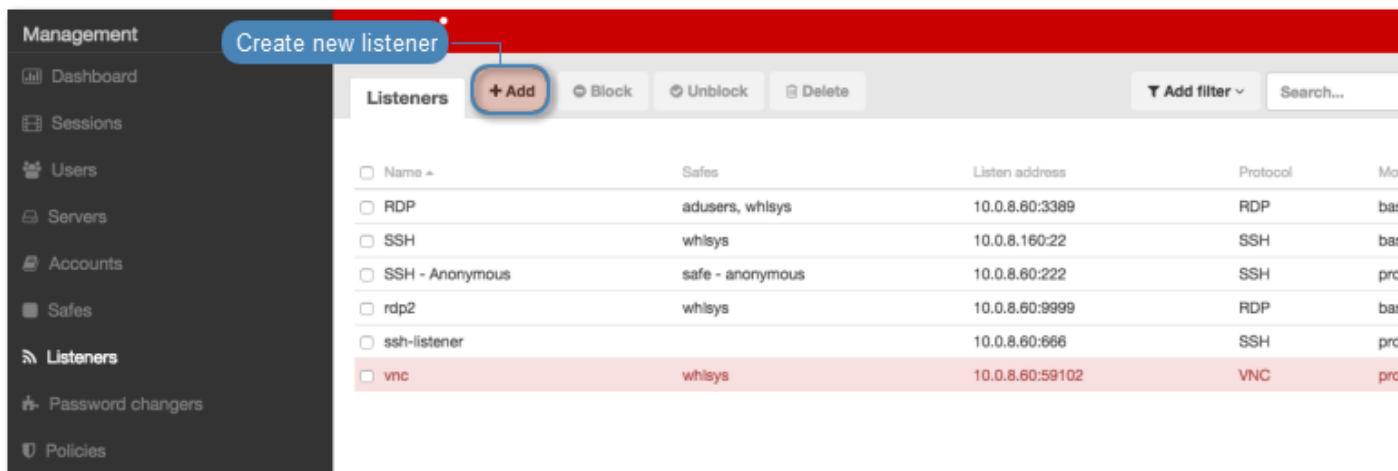
6. Click *Save*.

Related topics:

- *Data model*
- *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.

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. Click the generate certificate icon to generate certificate, or the certificate upload icon to upload a certificate.
 10. Click *Save*.

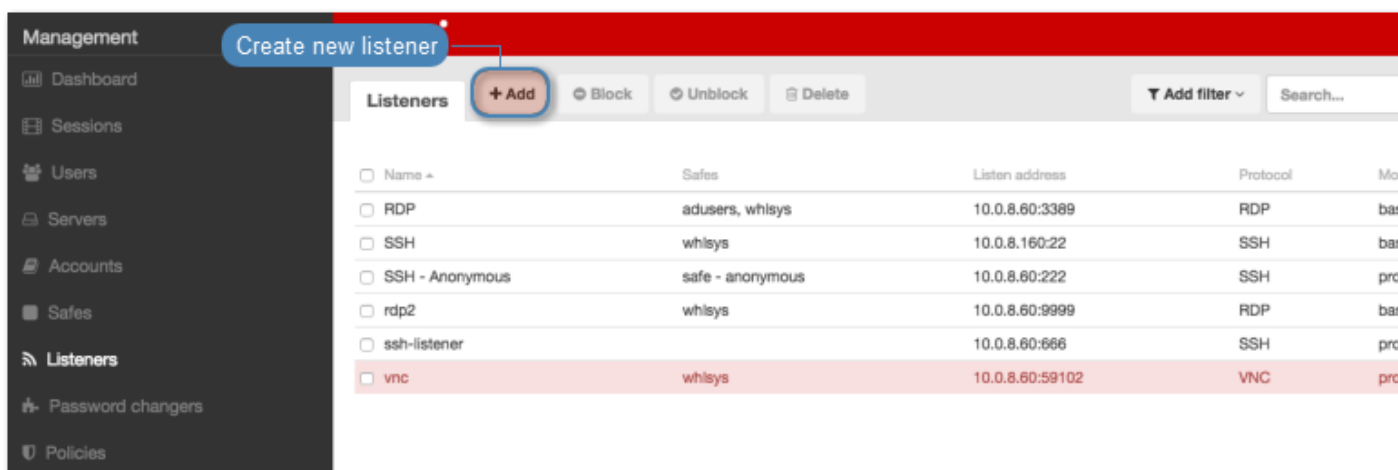
Related topics:

- *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.

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*.

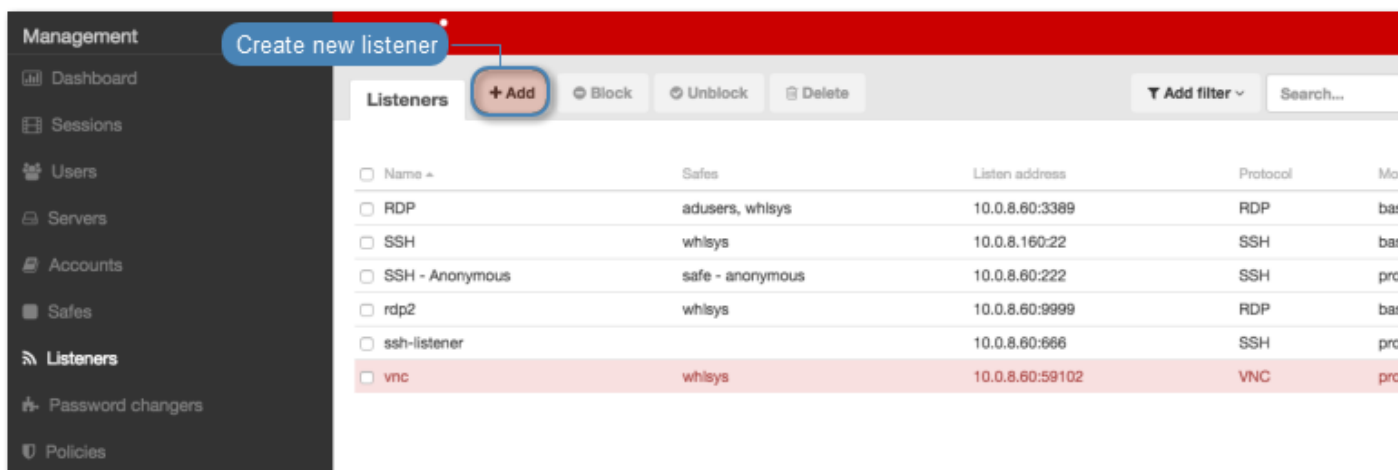
- Select **transparent** from the *Mode* drop-down list.
 - Select the network interface used for handling connections over this listener.
6. Click *Save*.

Related topics:

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

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.

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*.

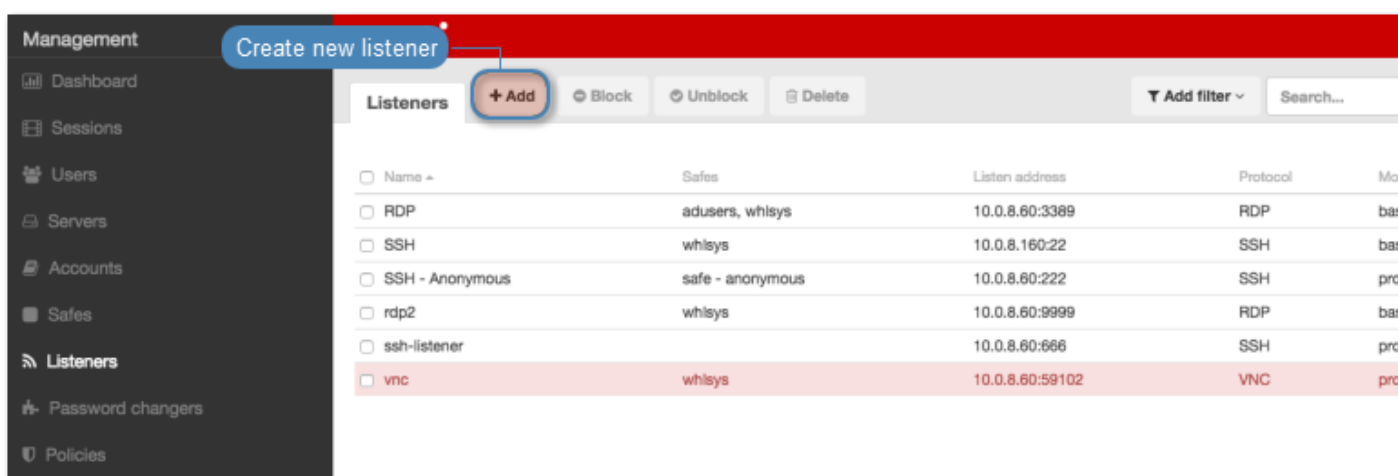
- Select `transparent` from the *Mode* drop-down list.
 - Select the network interface used for handling connections over this listener.
6. Click *Save*.

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.

`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*.

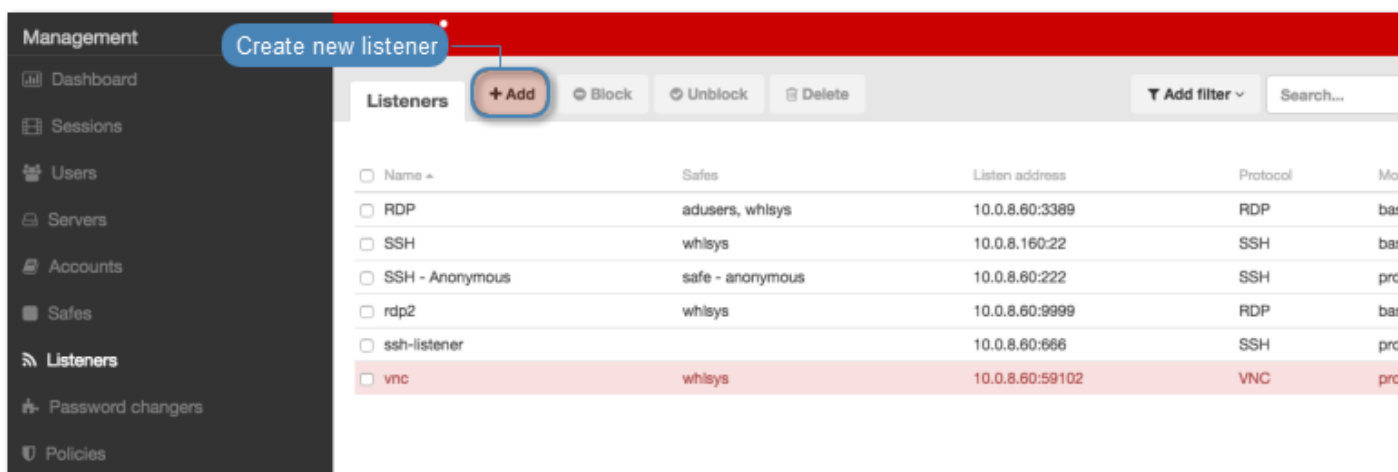
- Select `transparent` from the *Mode* drop-down list.
 - Select the network interface used for handling connections over this listener.
6. Click *Save*.

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.

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*.

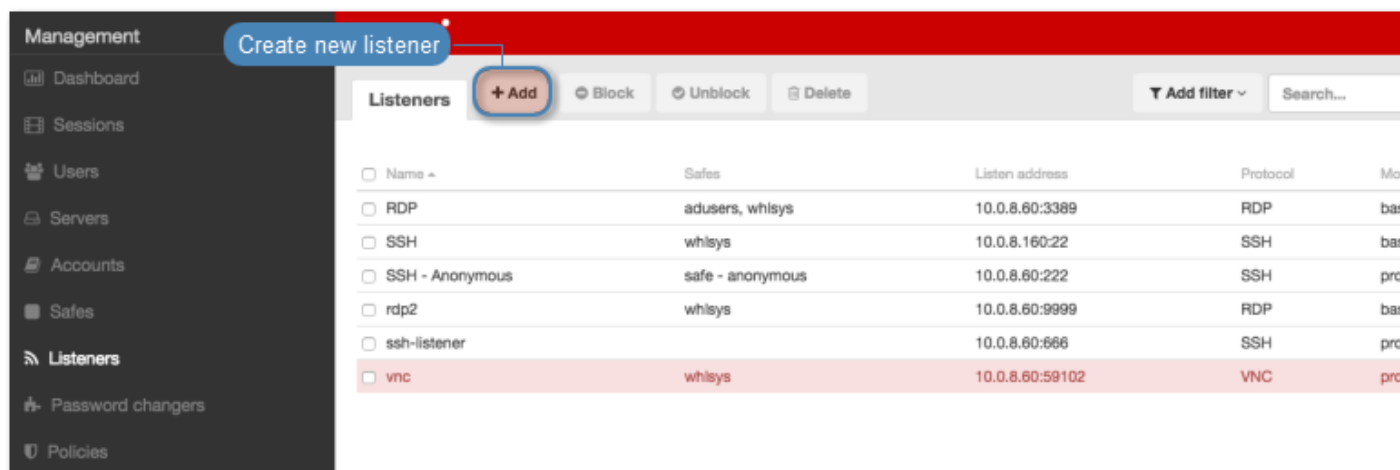
- Select **transparent** from the *Mode* drop-down list.
 - Select the network interface used for handling connections over this listener.
6. Click *Save*.

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.

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.

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*.

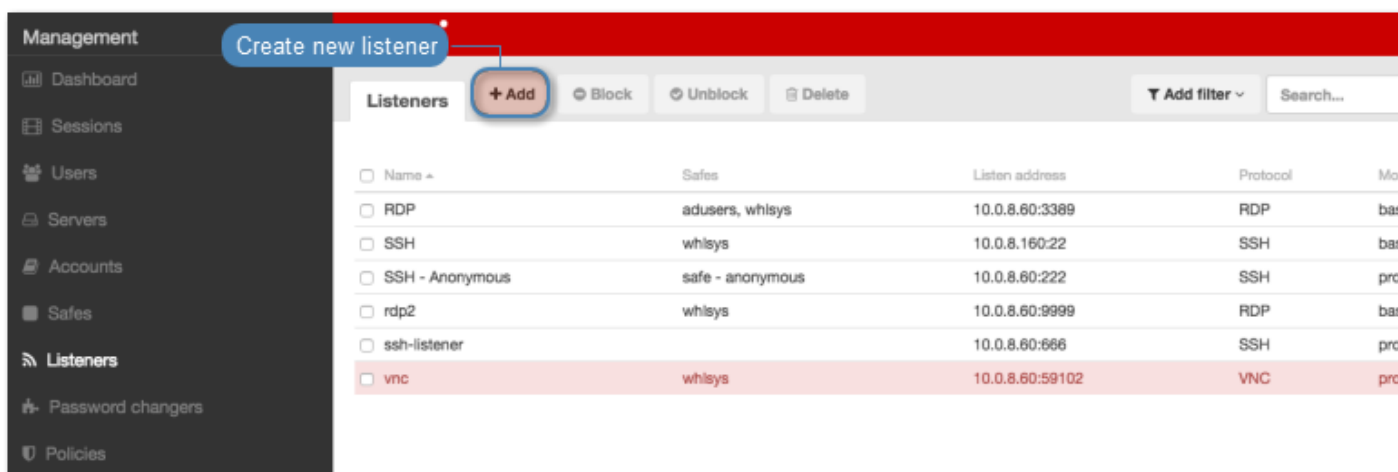
- Select **transparent** from the *Mode* drop-down list.
 - Select the network interface used for handling connections over this listener.
8. In the *TLS certificate* field, click the generate certificate icon to generate certificate, or the certificate upload icon to upload a certificate.
 9. Click *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.

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.

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 the generate certificate icon to generate certificate, or the certificate upload icon to upload a certificate.
 7. Click *Save*.

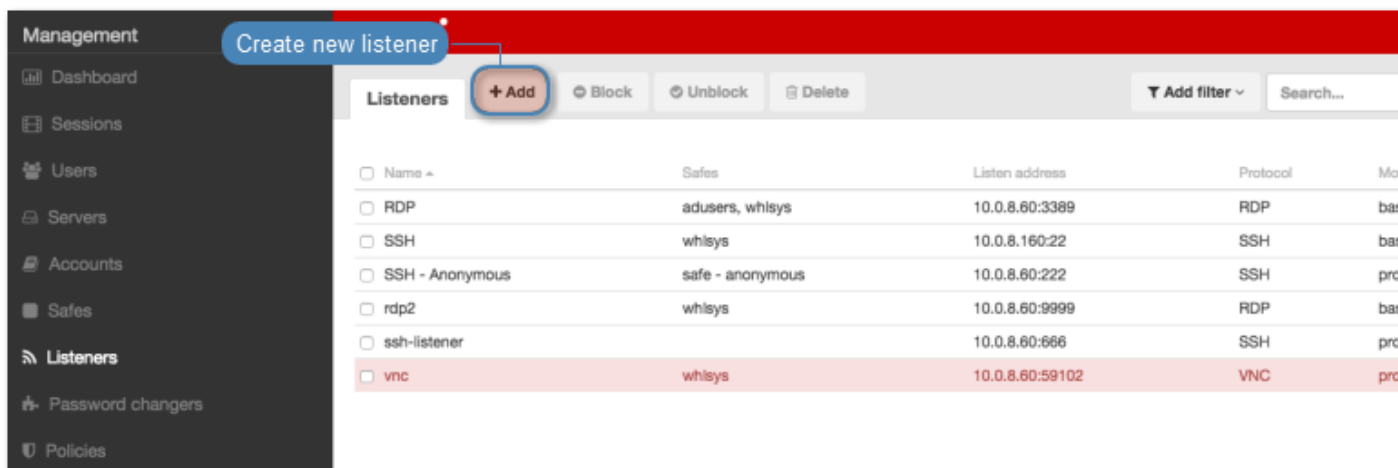
Related topics:

- *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.

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*.

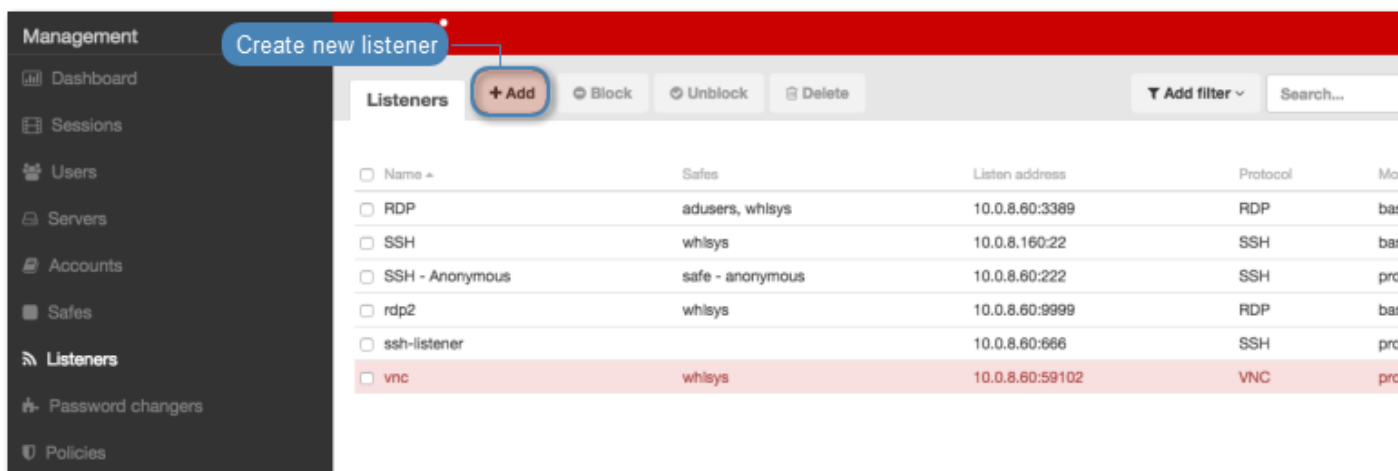
- Select **transparent** from the *Mode* drop-down list.
 - Select the network interface used for handling connections over this listener.
6. Click *Save*.

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.

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*.

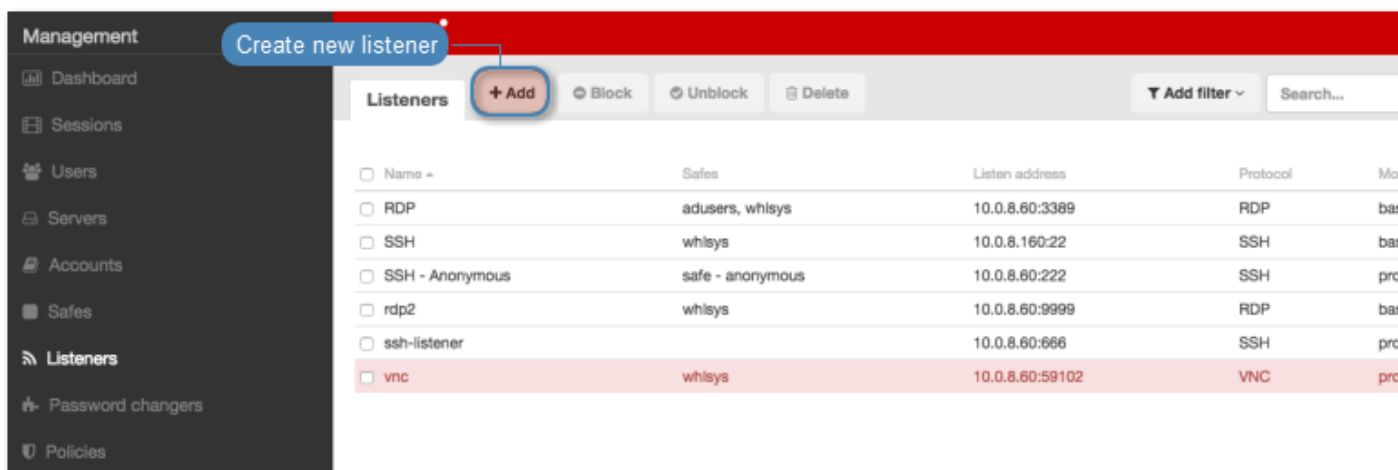
- Select **transparent** from the *Mode* drop-down list.
 - Select the network interface used for handling connections over this listener.
6. Select the *Use TLS* option to enable encryption.
 7. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
 8. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
 9. Click the generate certificate icon to generate certificate, or the certificate upload icon to upload a certificate.
 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.

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.

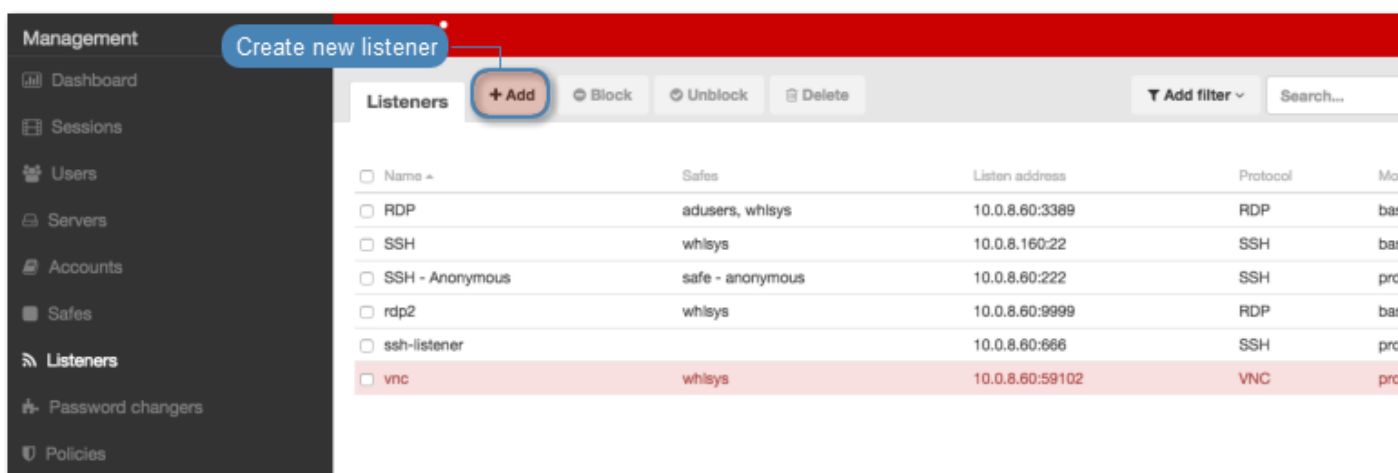
7. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
8. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
9. Click the generate certificate icon to generate certificate, or the certificate upload icon to upload a certificate.
10. Click *Save*.

Related topics:

- [Data model](#)
- [Editing a listener](#)
- [Deleting a listener](#)
- [Blocking a listener](#)
- [Unblocking a listener](#)

9.1.12 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.

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.

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.

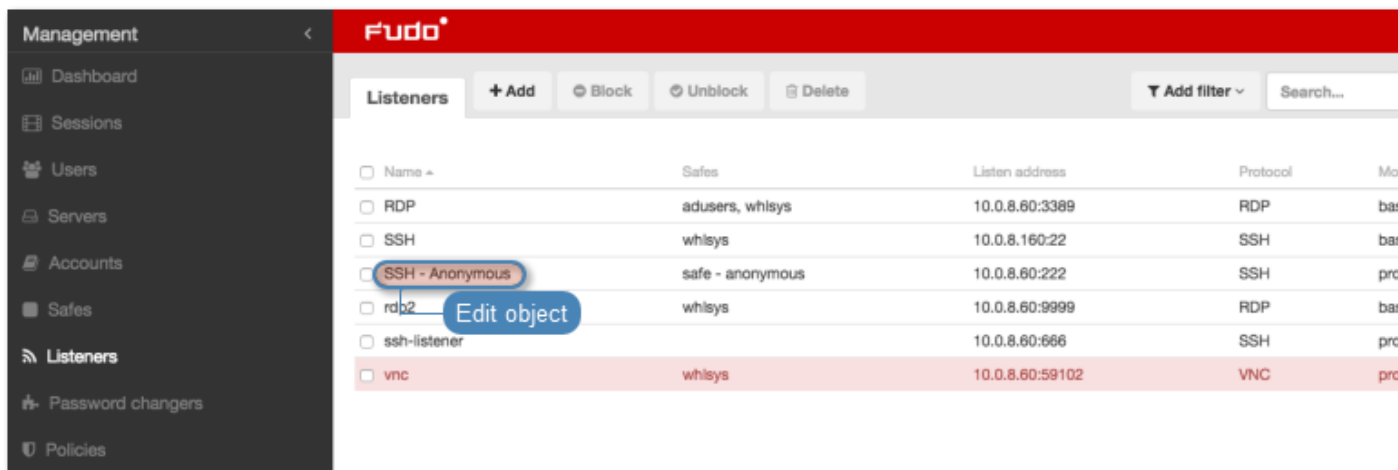
7. Click *Save*.

Related topics:

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

9.2 Editing a listener

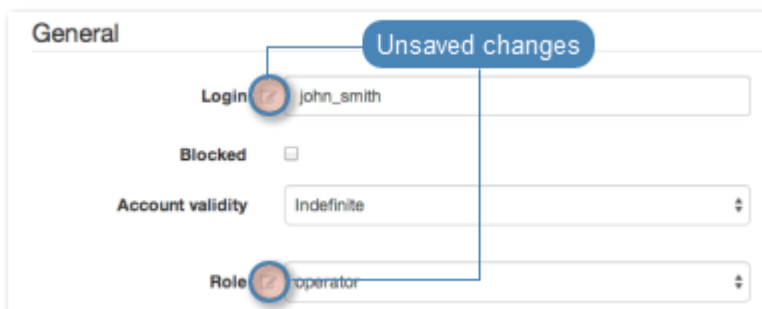
1. Select *Management > Listeners*.
2. Find and click desired listener to access its configuration parameters.



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*

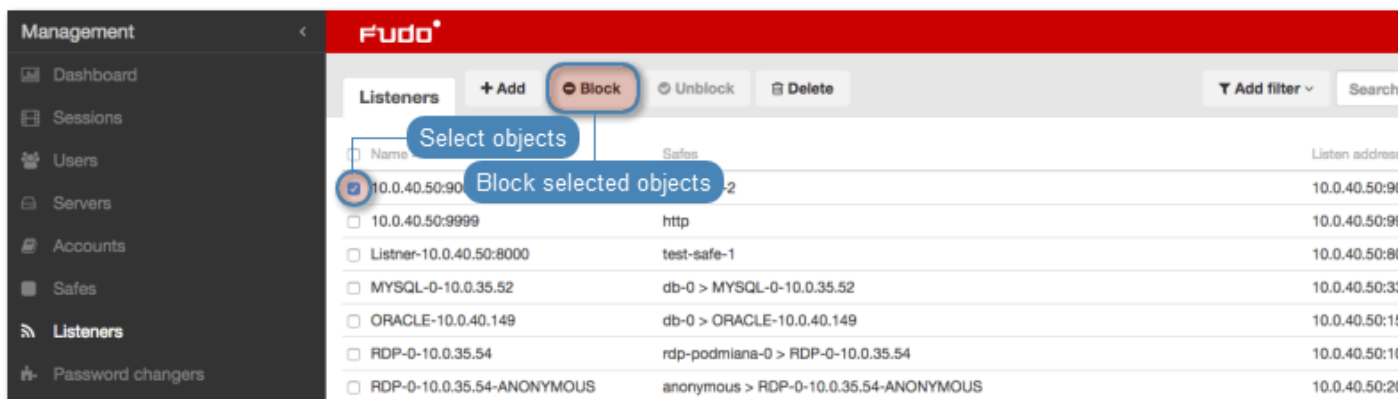
9.3 Blocking a listener

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:

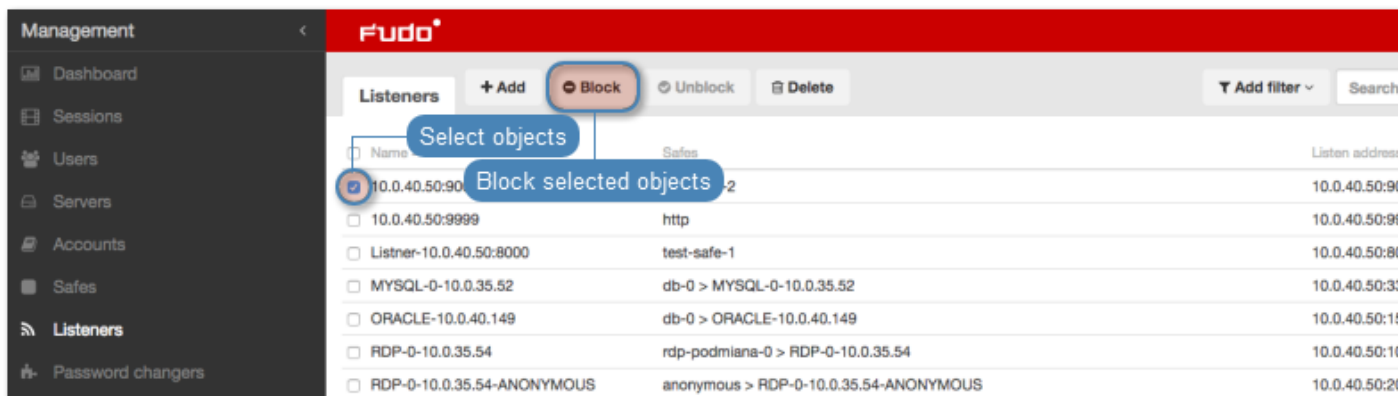
- [Data model](#)
- [System initiation](#)
- [Servers](#)

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*

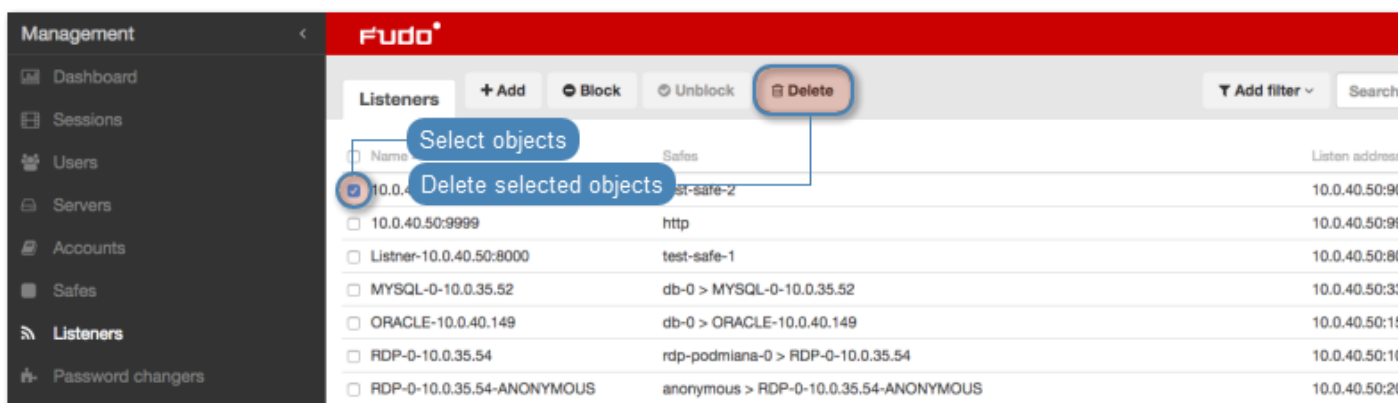
9.5 Deleting a listener

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*

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

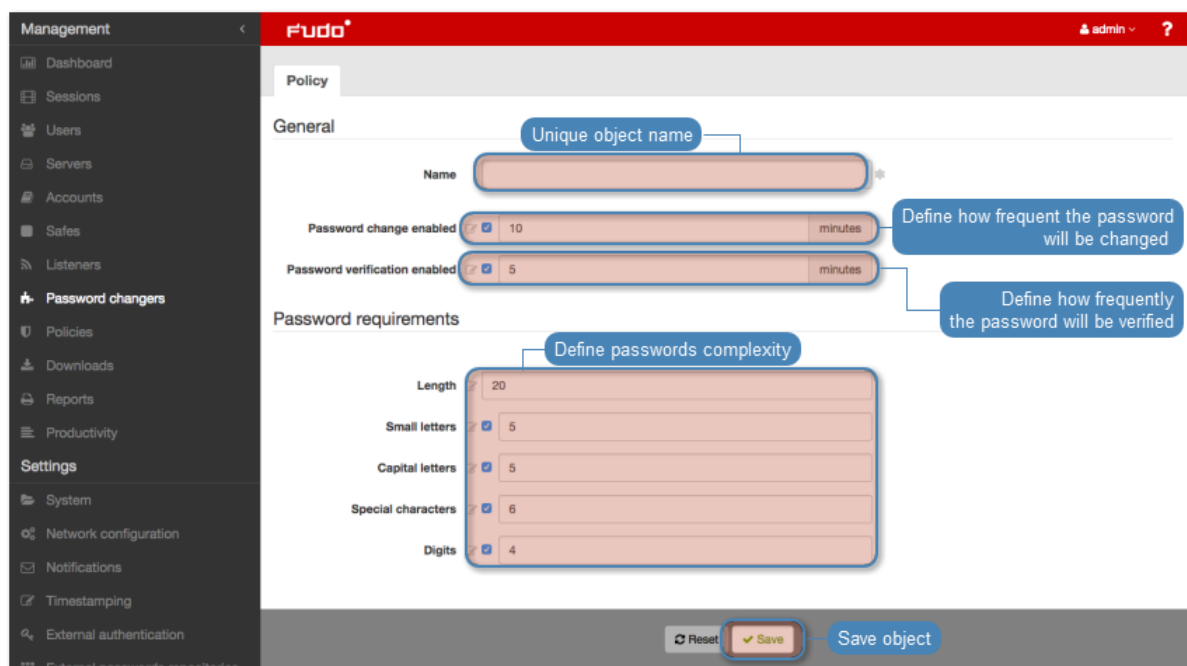
1. Select *Management > Password changers*.
2. Click *+ Add*.
3. Enter object name.
4. Select the *Password change enabled* option and specify the time interval between each password change.

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.

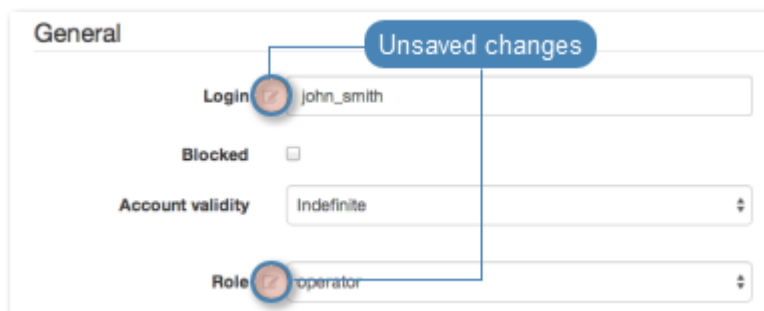
7. Click *Save*.



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 `%%` characters 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:

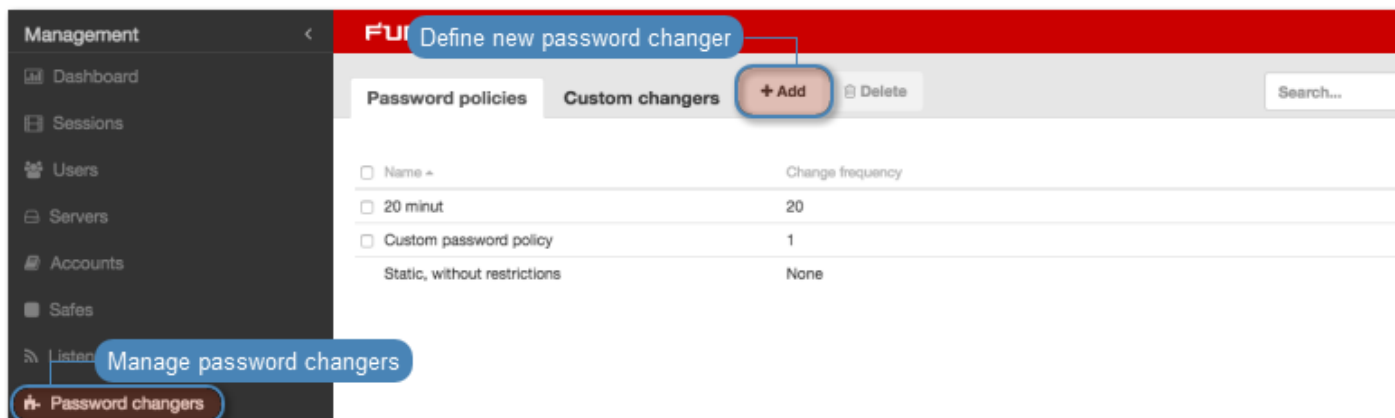
- *Data model*
- *Accounts*
- *Password changer policy*
- *Setting up password changing on a Unix system*

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

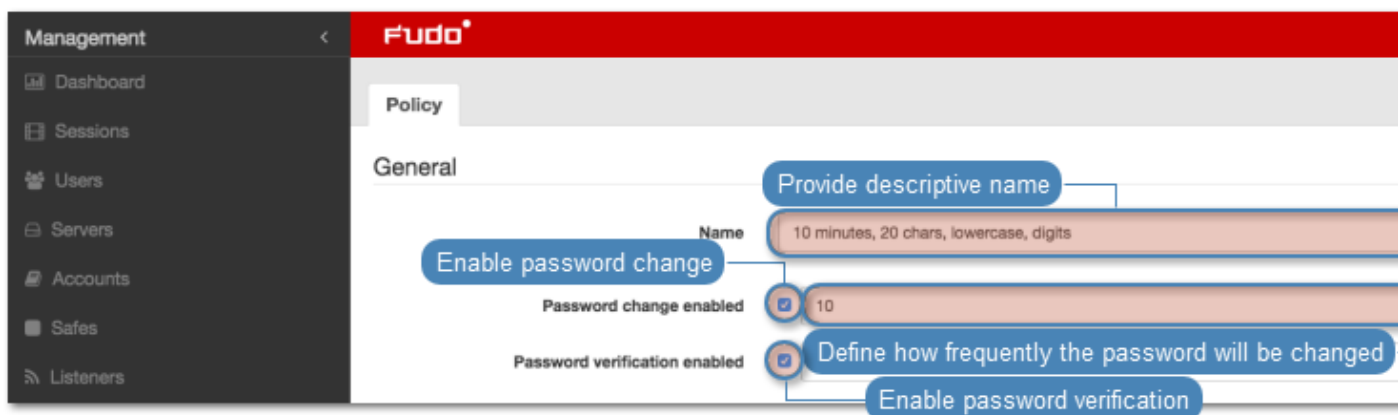
1. Select *Management > Password changers*.
2. Click *+ Add* to create a new password changing policy.



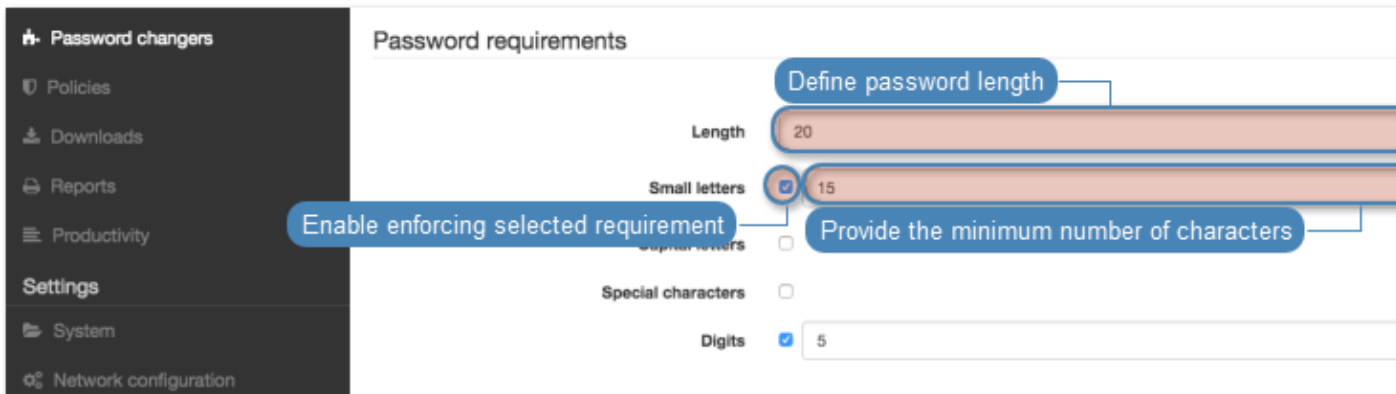
3. Provide password change policy name.

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 other way but the Secret Manager itself.



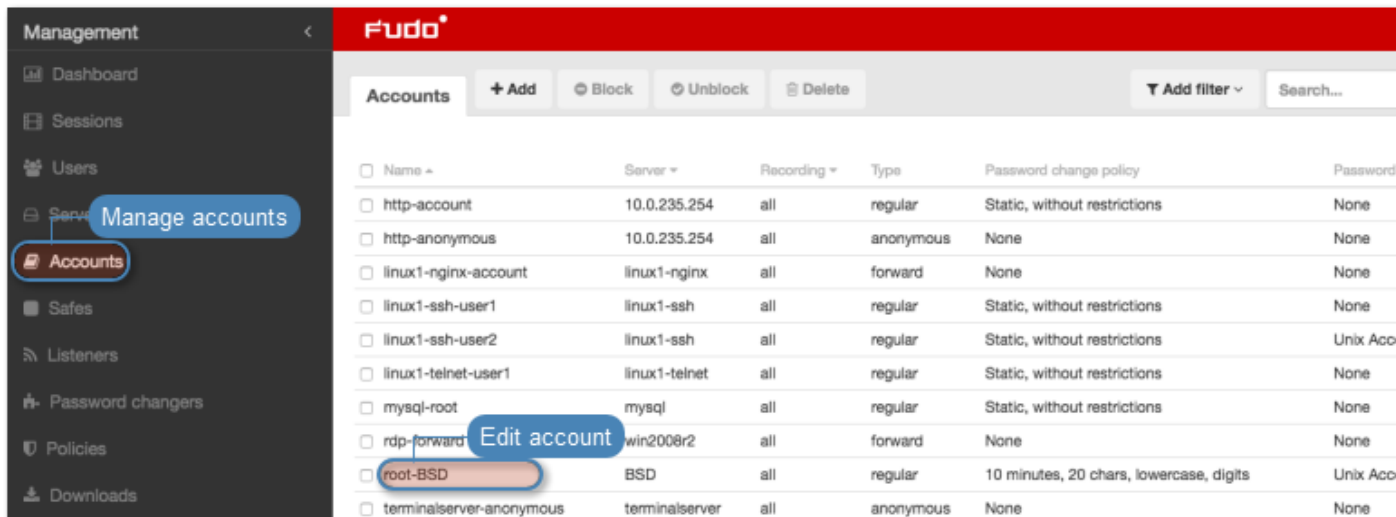
6. Provide the number of characters comprising the password.
7. Select desired password complexity options and provide the minimal number of characters for each.



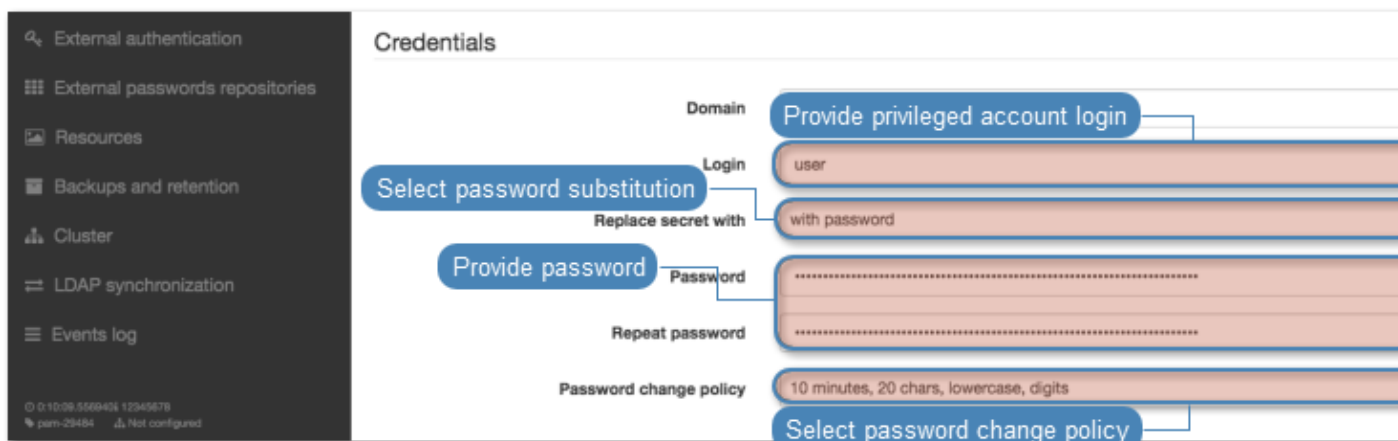
8. Click *Save* to store password changer policy.

Assigning password changer to the privileged account

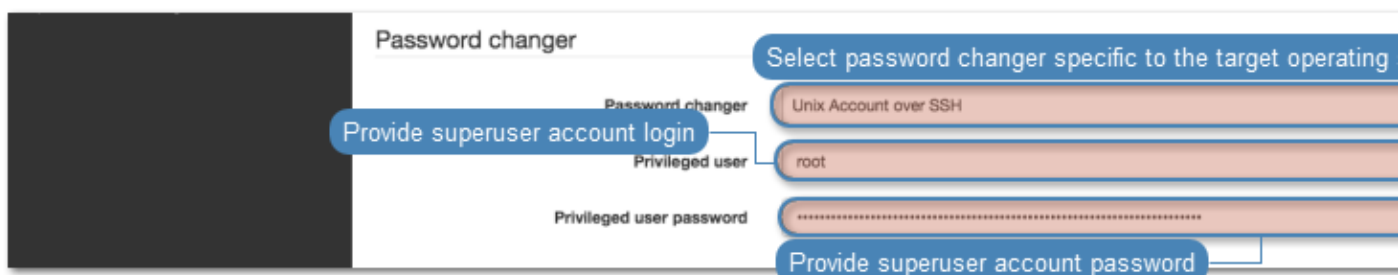
1. Select *Management* > *Accounts*.
2. Find and click desired account object.



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*.

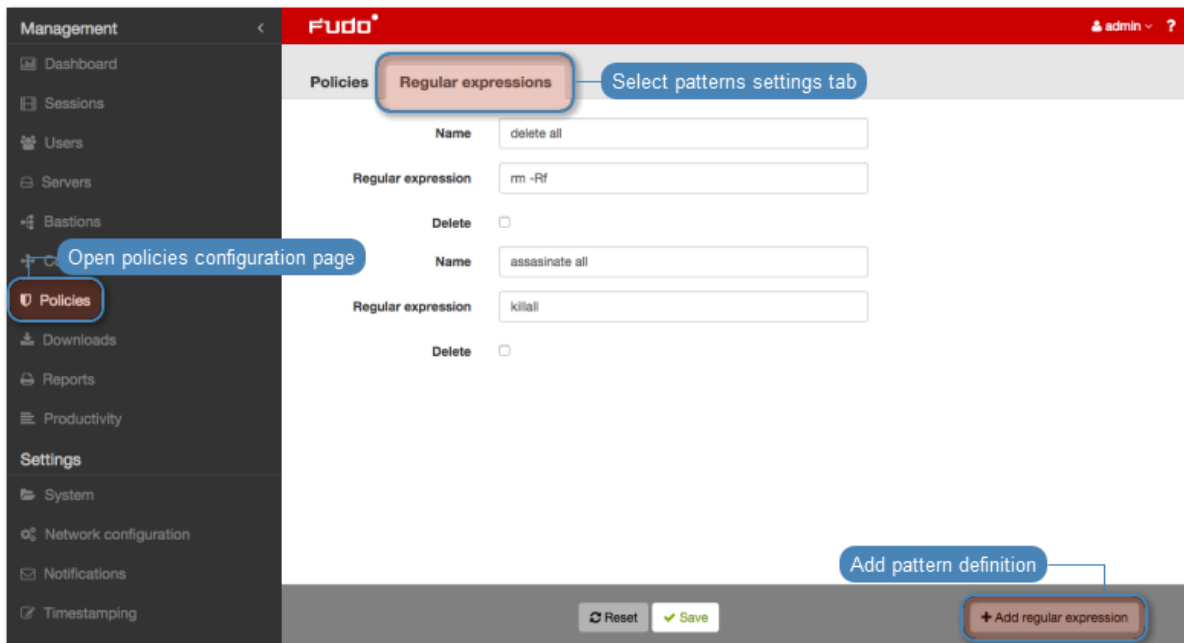
Related topics:

- *Requirements*
- *Data model*
- Configuration

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

1. Select *Management* > *Policies*.
2. Select *Regular expressions* tab.
3. Click *+ Add regular expression*.

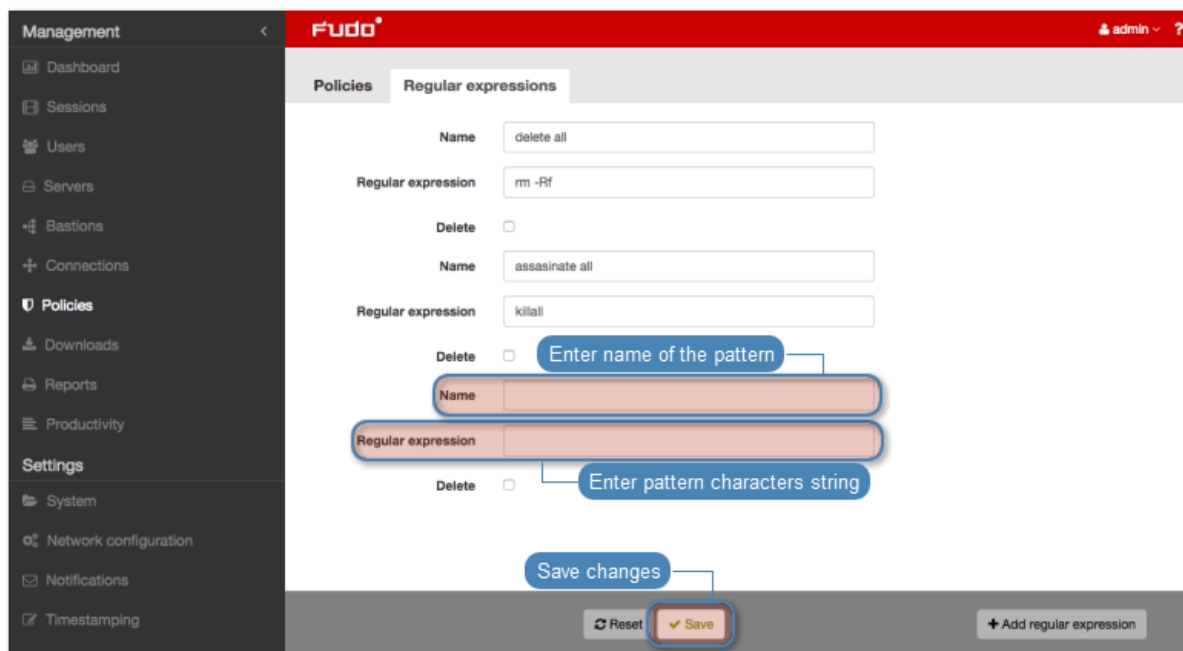


4. Enter pattern name.
5. Define the pattern itself.

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:]`

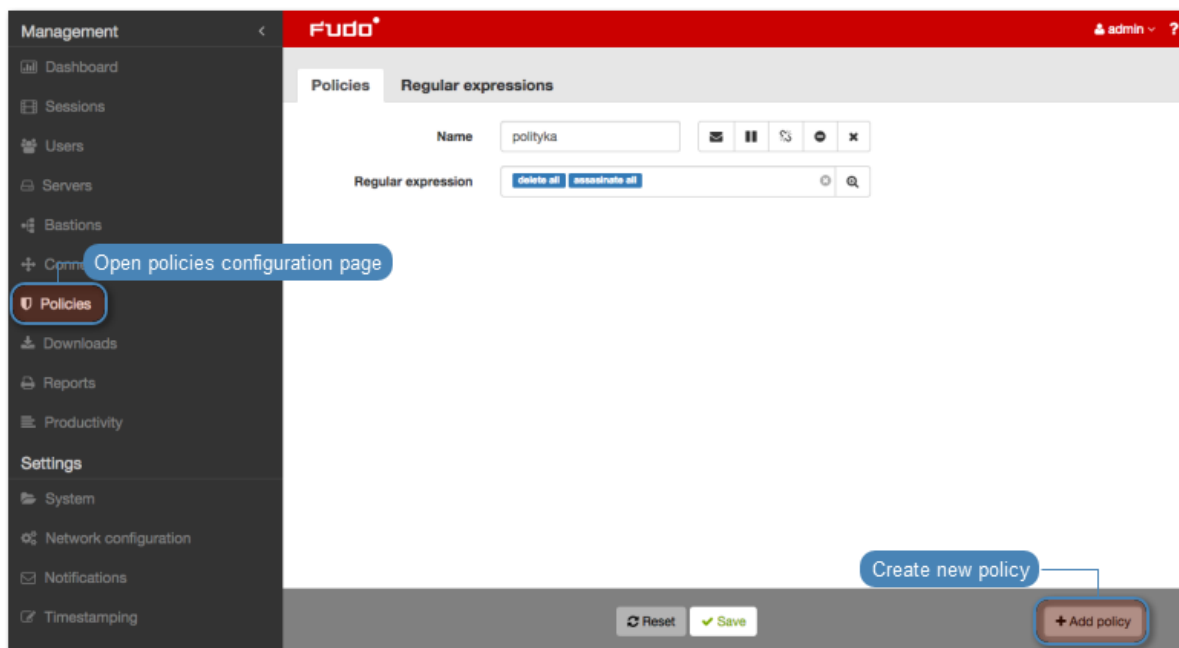
Command `rm -rf` (also `-fr`; `-Rf`; `-fR`)

`(^[^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:]+.*justfilename`





Defining policies

1. Select *Management > Policies*.
2. Click Add policy.



3. Enter policy name.

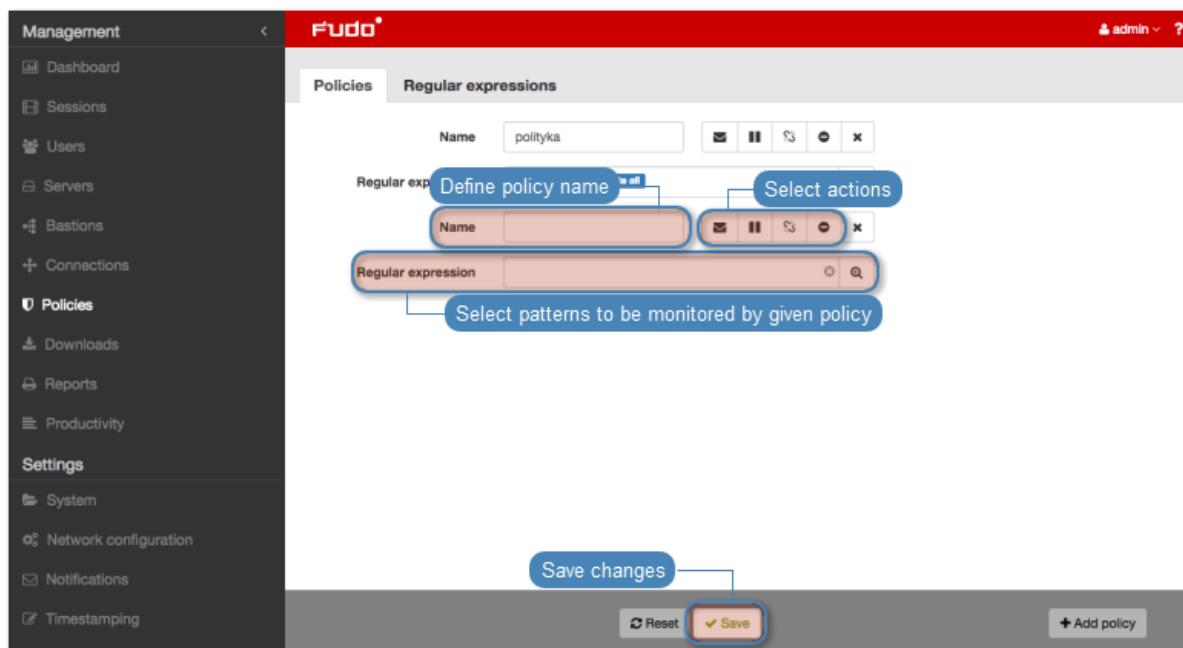
4. Select actions.

	Send email notification to system administrator.
	Pause connection.
	Terminate connection.
	Block user.

Note: Note that terminating connection also blocks the user account and vice versa - blocking user automatically terminates user's connections.

5. Select monitored patterns.

6. Click Save.



Note: After defining a policy, you can assign it to a particular server configured in connection.

Deleting patterns

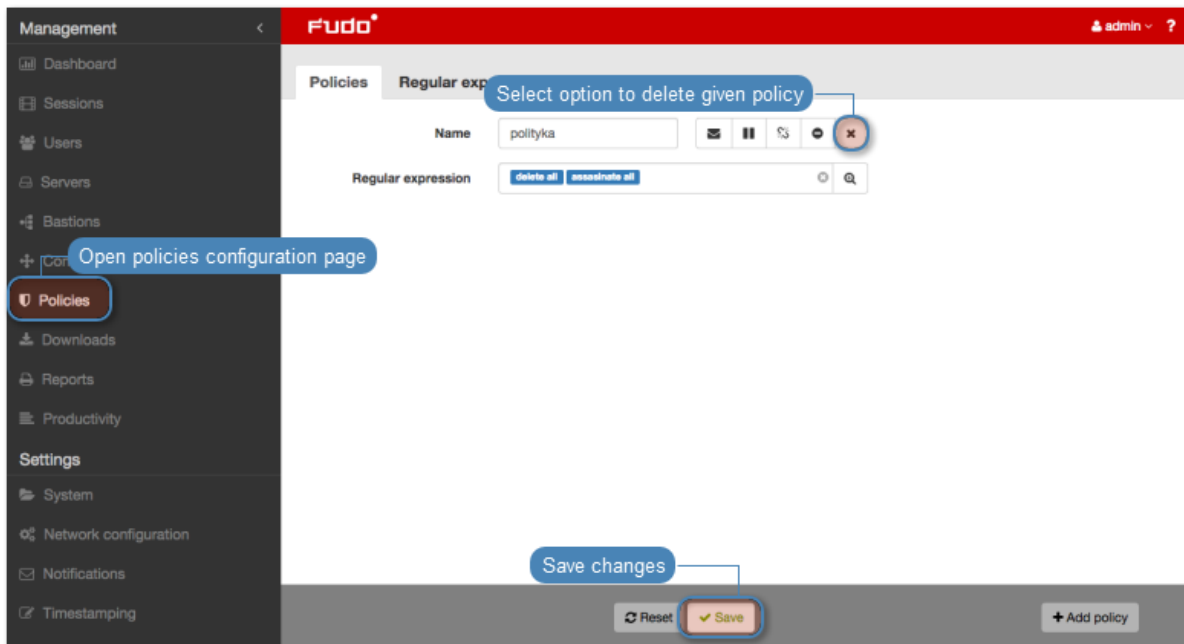
1. Select *Management* > *Policies*.
2. Select the *Regular expressions* tab.
3. Find desired pattern definition and select the *Delete* option.
4. Click *Save*.



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:

- *Terminating connection*
- *Notifications*
- *Accounts*
- *Security*

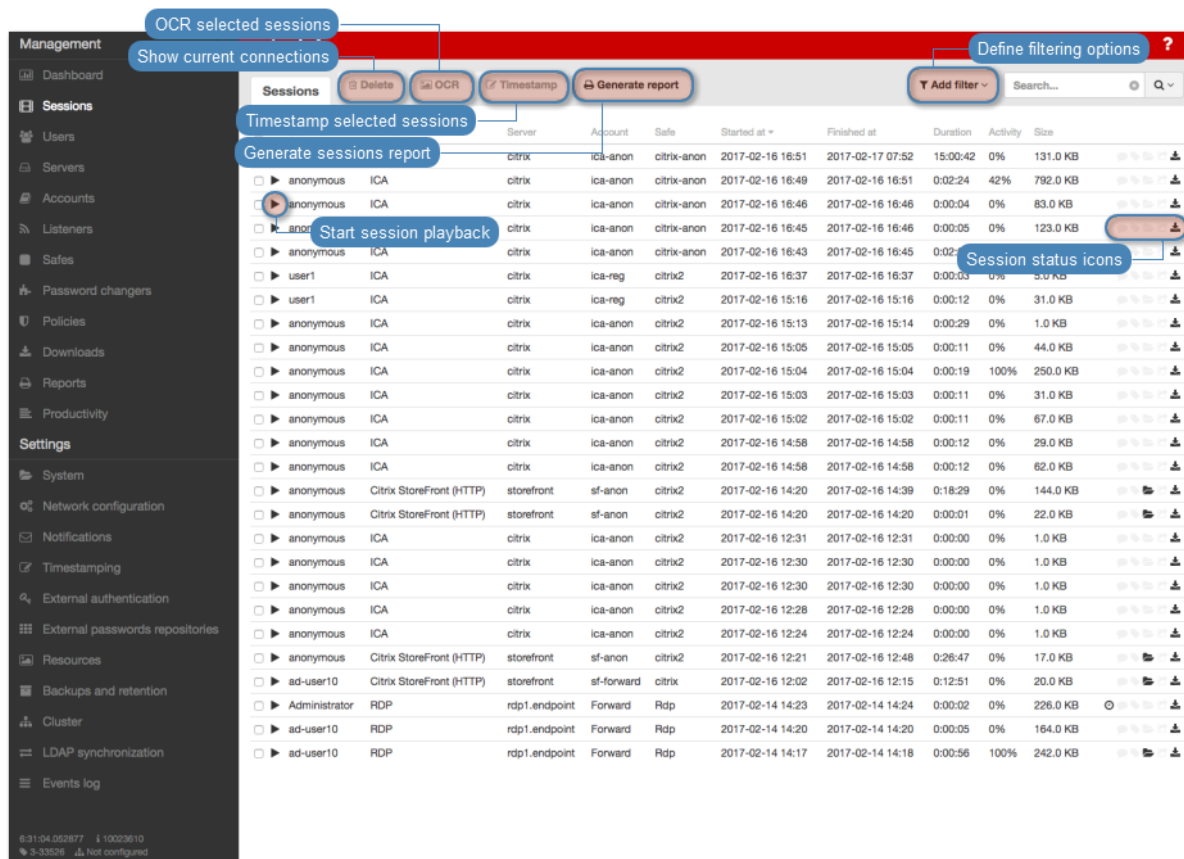
Wheel Fudo PAM stores all recorded servers access sessions, allowing to playback, review, delete and export to one of supported video format.

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.

Icon	Description
	Start session playback (<i>applicable to sessions with the entire traffic recording option selected in connection properties</i>).
	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 (<i>applicable to sessions with either complete or raw traffic recording option selected in connection properties</i>).
	User activity monitor (<i>applicable to live sessions</i>).

To open sessions management page, select *Management > Sessions*.

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

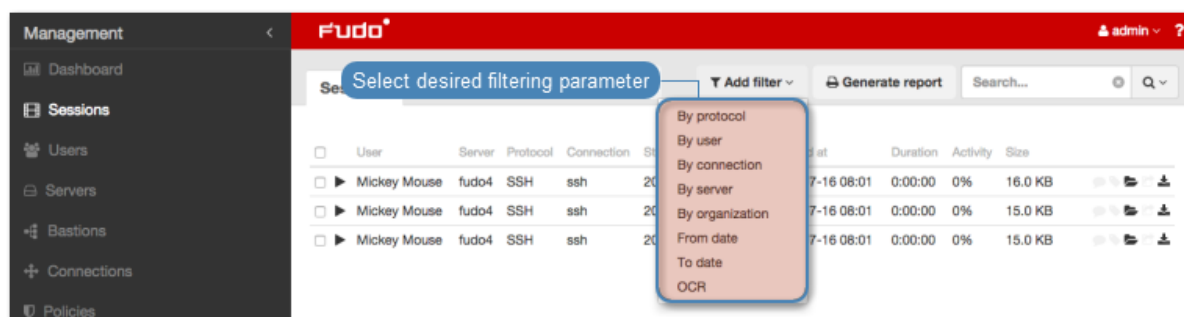


12.1 Filtering sessions

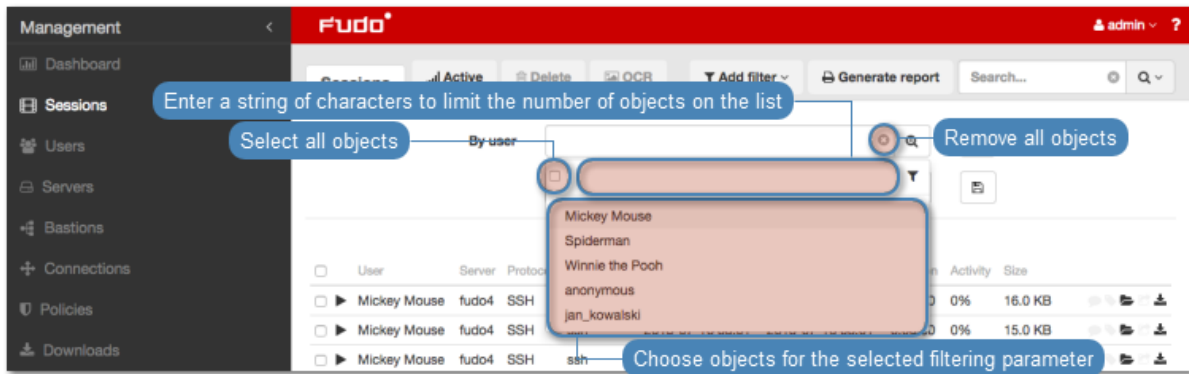
Sessions filtering allows to find desired sessions easily by limiting the number of displayed sessions on the sessions management page.

12.1.1 Defining filters

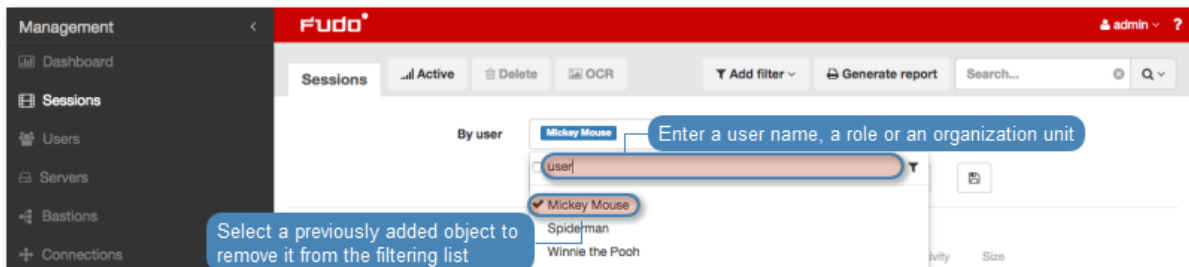
1. Click *Add Filters* and select desired data type from the drop-down list.



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.

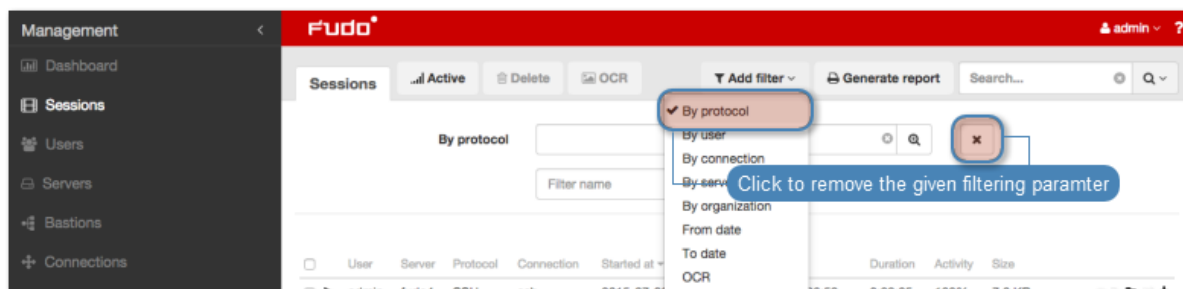
Protocol, user, connection, server and organization parameters allow for selecting multiple objects of the given type.



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

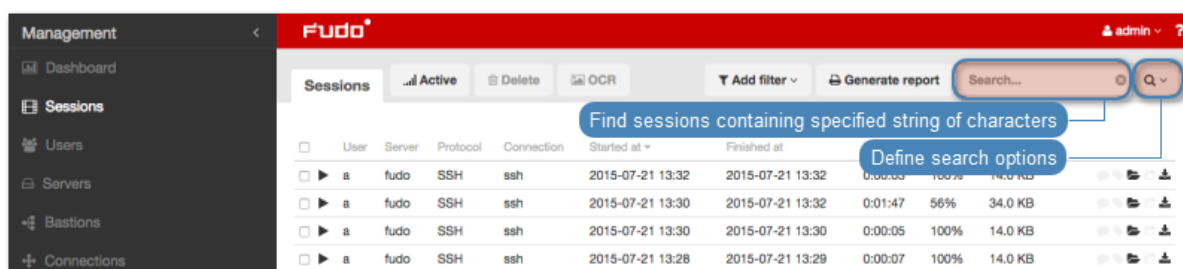
Note: Only sessions which match all defined filtering parameters will be displayed.

4. Click *Add Filter* and select previously added filtering parameter to disable given filter.



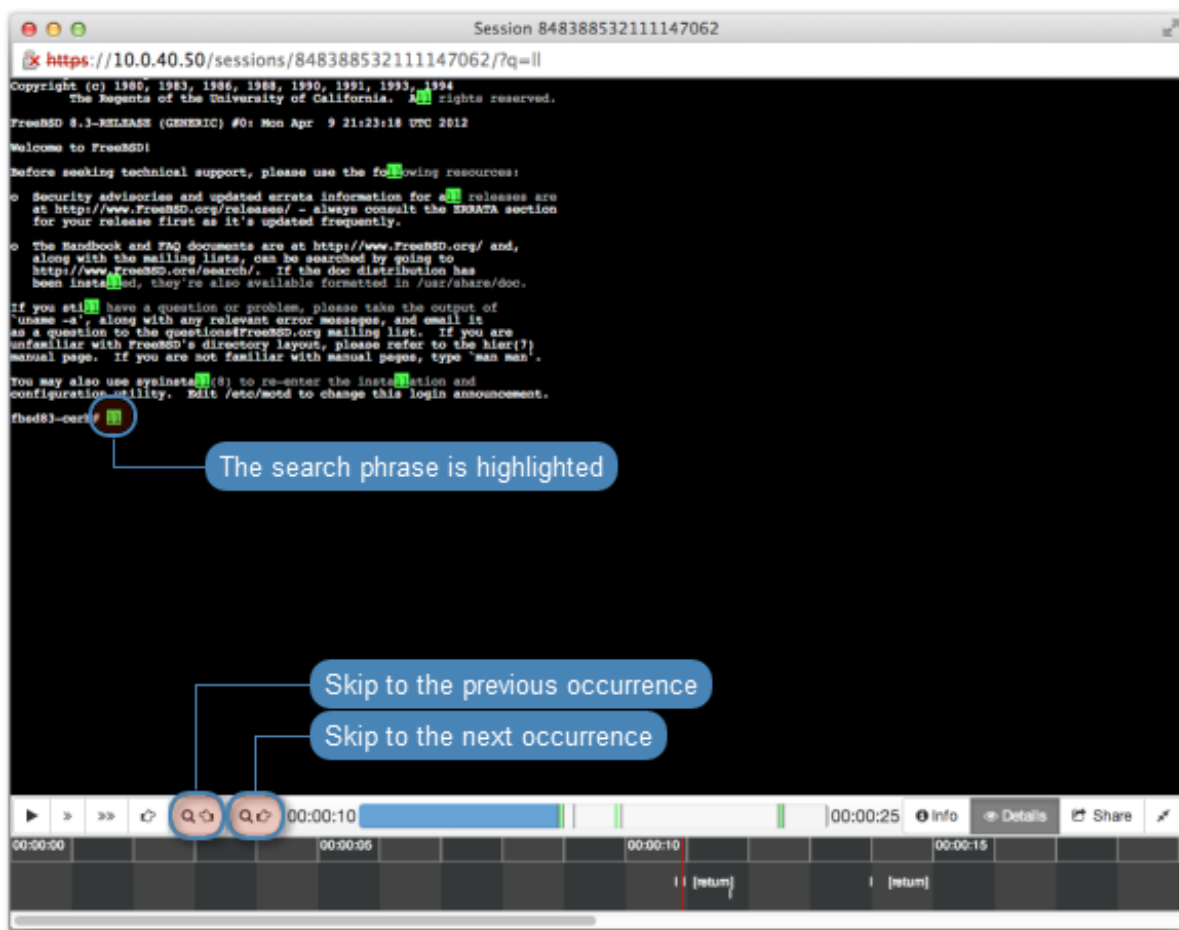
12.1.2 Full text search

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.

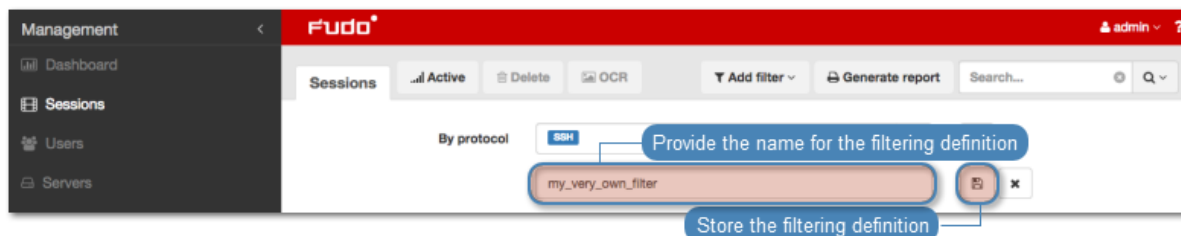


12.1.3 Managing user defined filter definitions

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

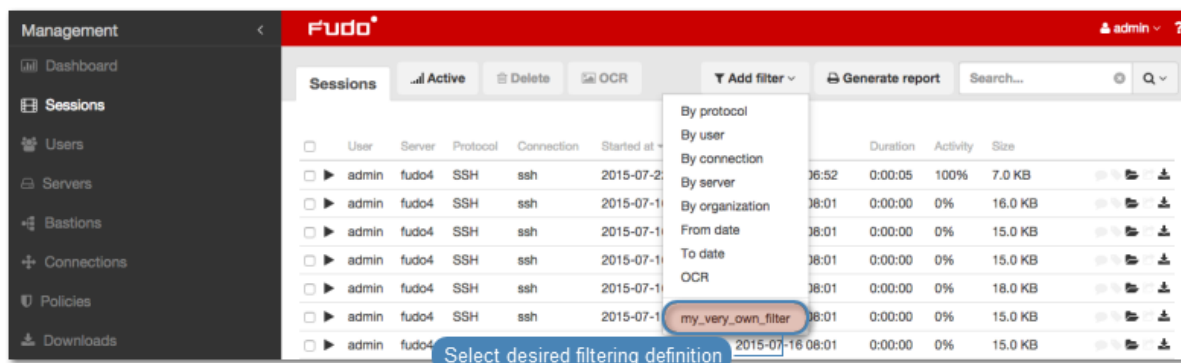
Storing a user defined filter definition

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

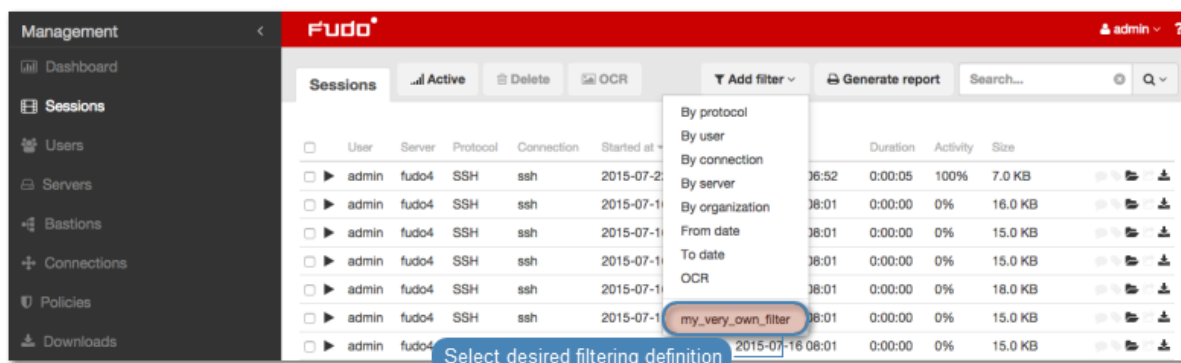
1. Click *Add filter* and select the desired filter definition.



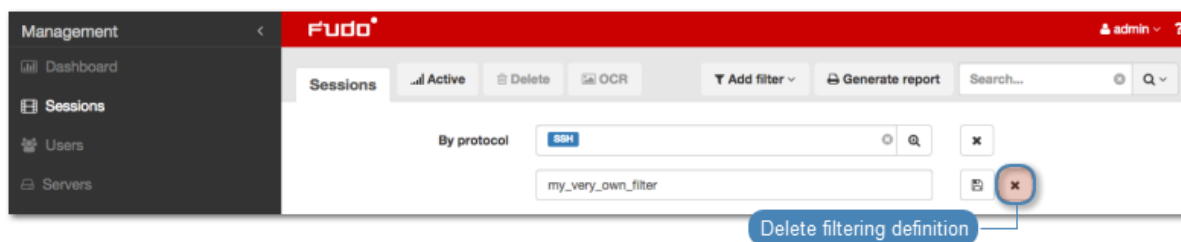
2. Change the filtering parameters as desired.
3. Click the save icon to store changes in the filter definition.

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

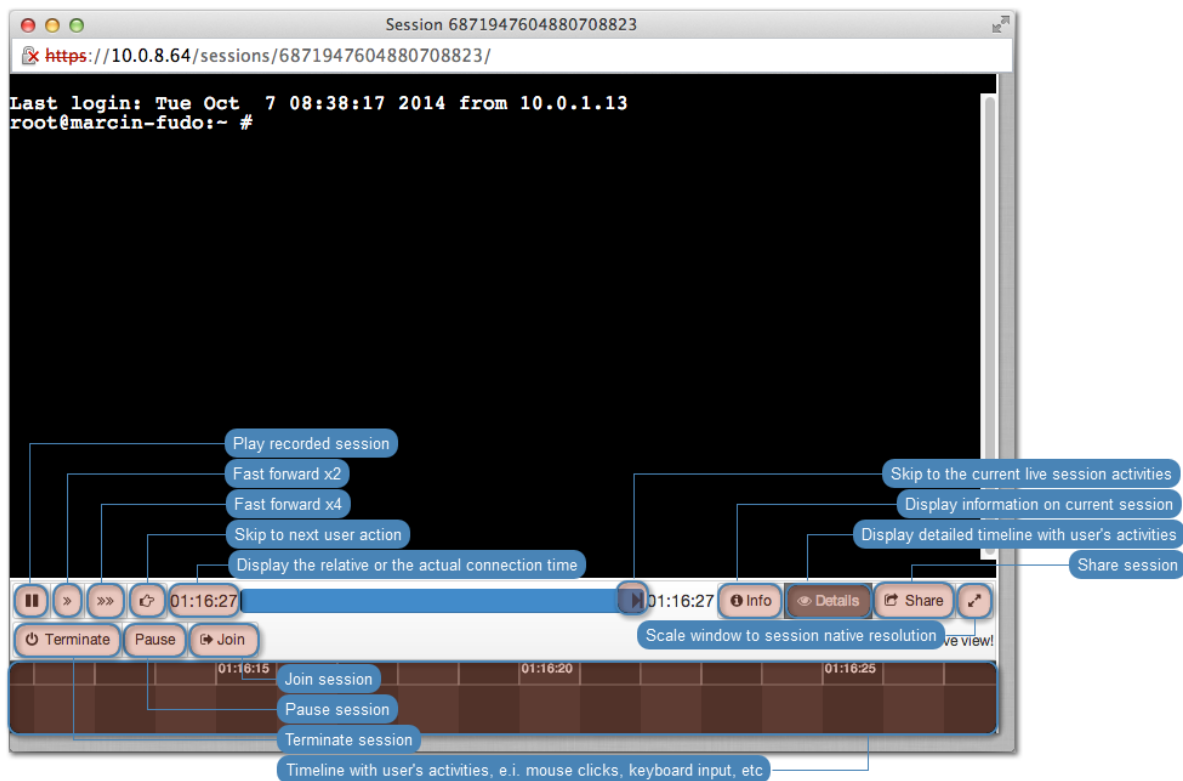
Wheel Fudo PAM allows viewing recorded sessions as well as current user connections.

To view a session, proceed as follows.

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

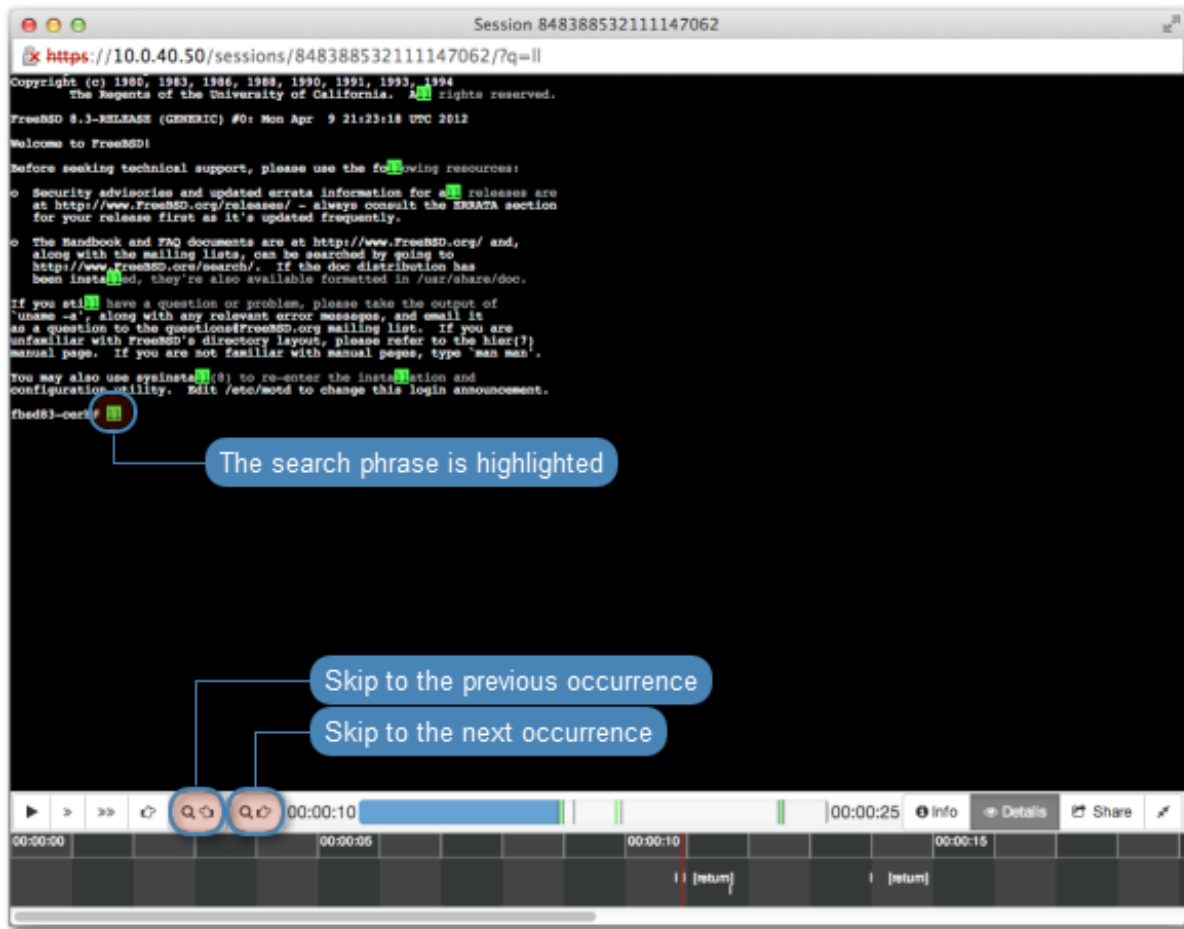
Session player options

Note: Some options are available for live sessions only.

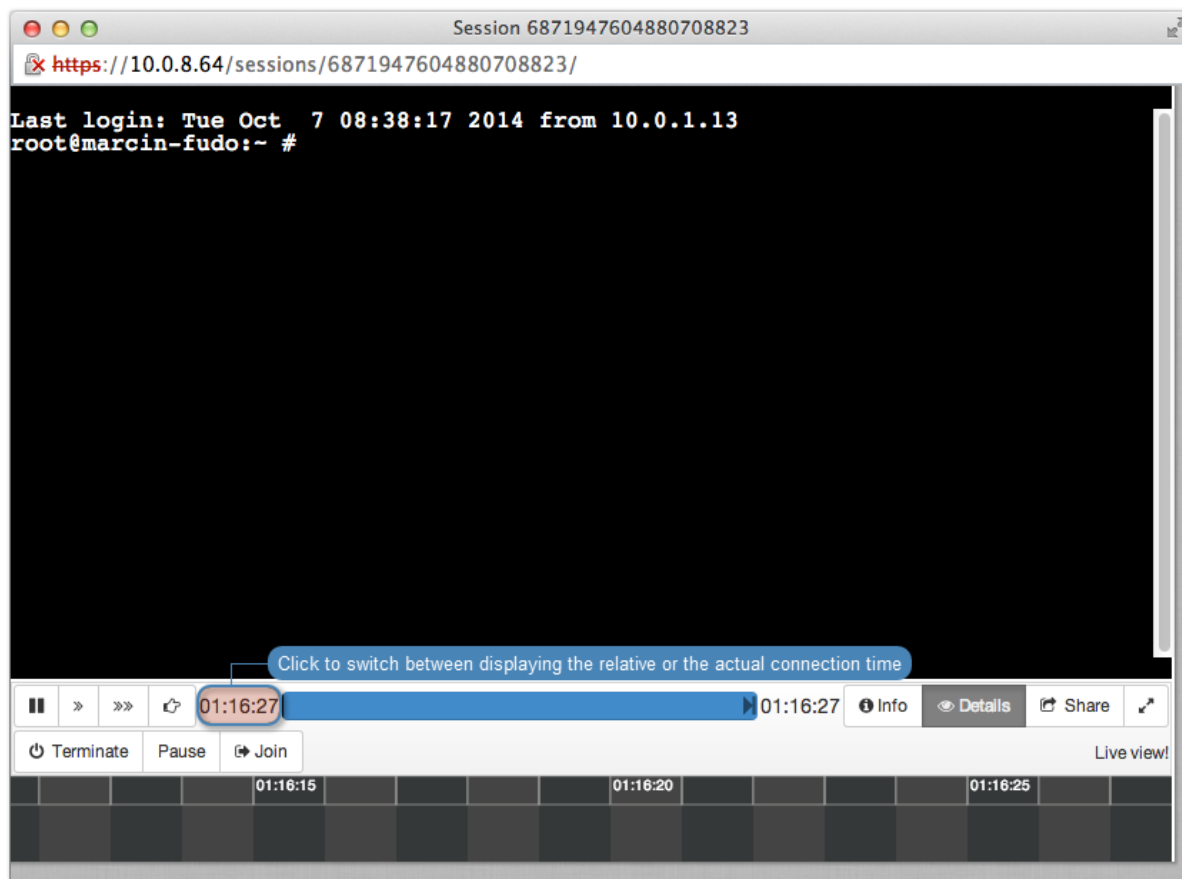


Note: Playing a session containing the specified phrase starts from the moment of its first occurrence.

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*

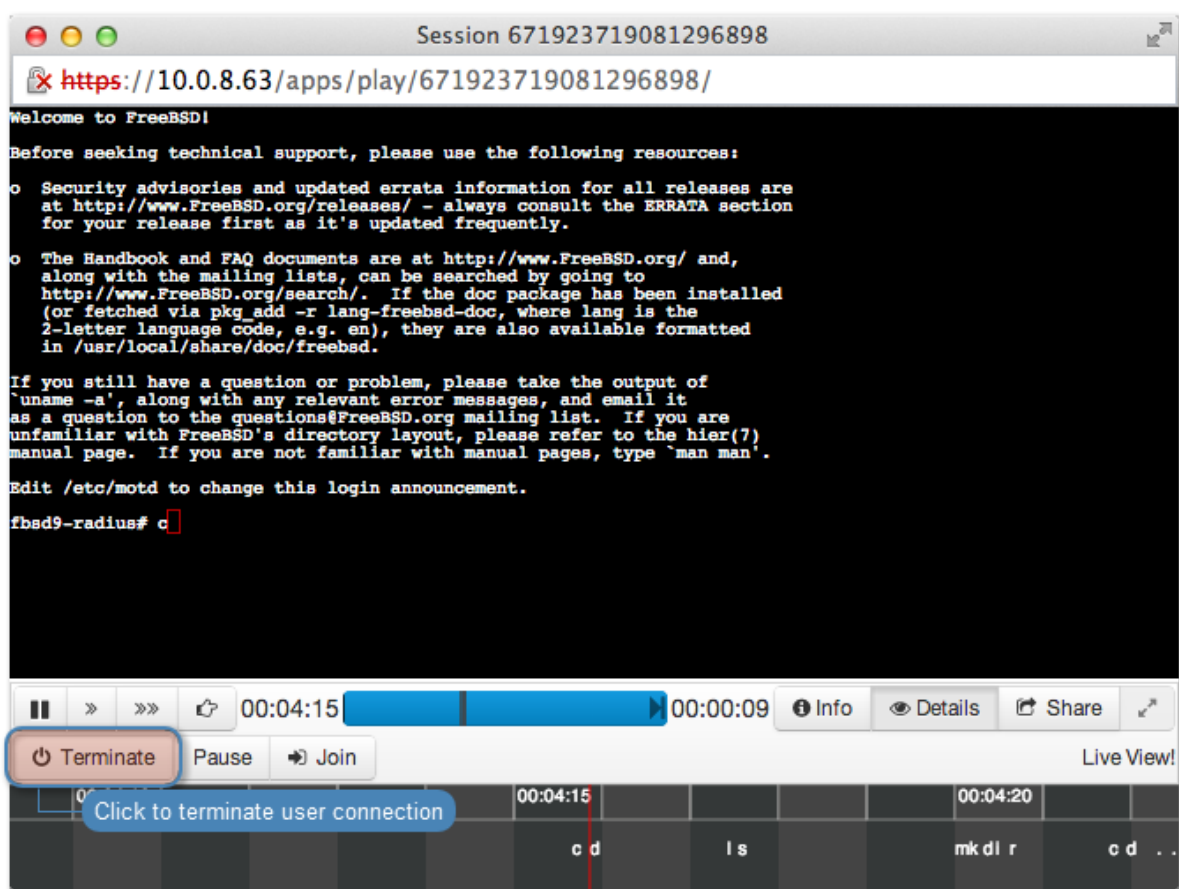
12.5 Terminating connection

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:

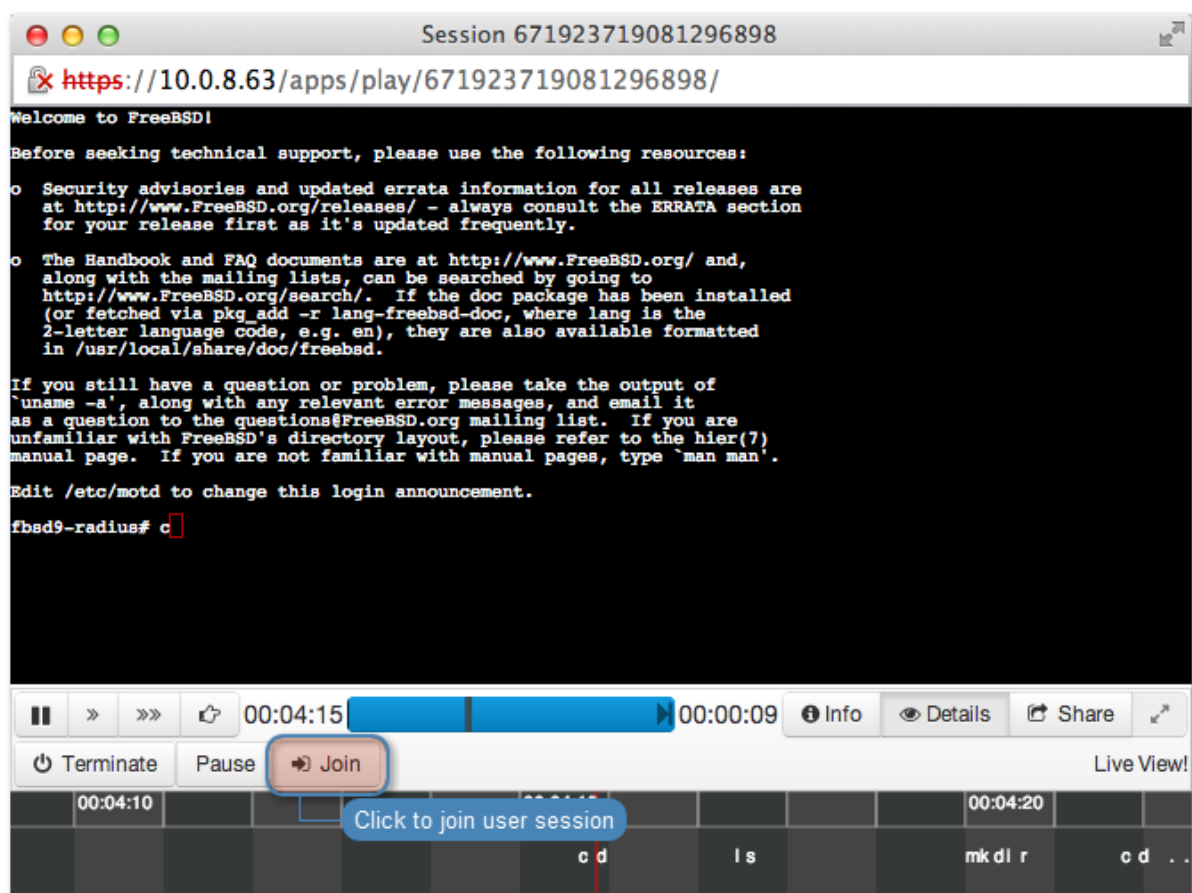
- *Policies*
- *Security measures*
- *Joining live session*
- *Sharing sessions*
- *Filtering sessions*

12.6 Joining live session

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

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 click the play icon to start playback.
5. Click *Join*.



Related topics:

- *Replaying sessions*
- *Sharing sessions*
- *Filtering sessions*

12.7 Sharing sessions

Wheel Fudo PAM enables sharing given session with another user.

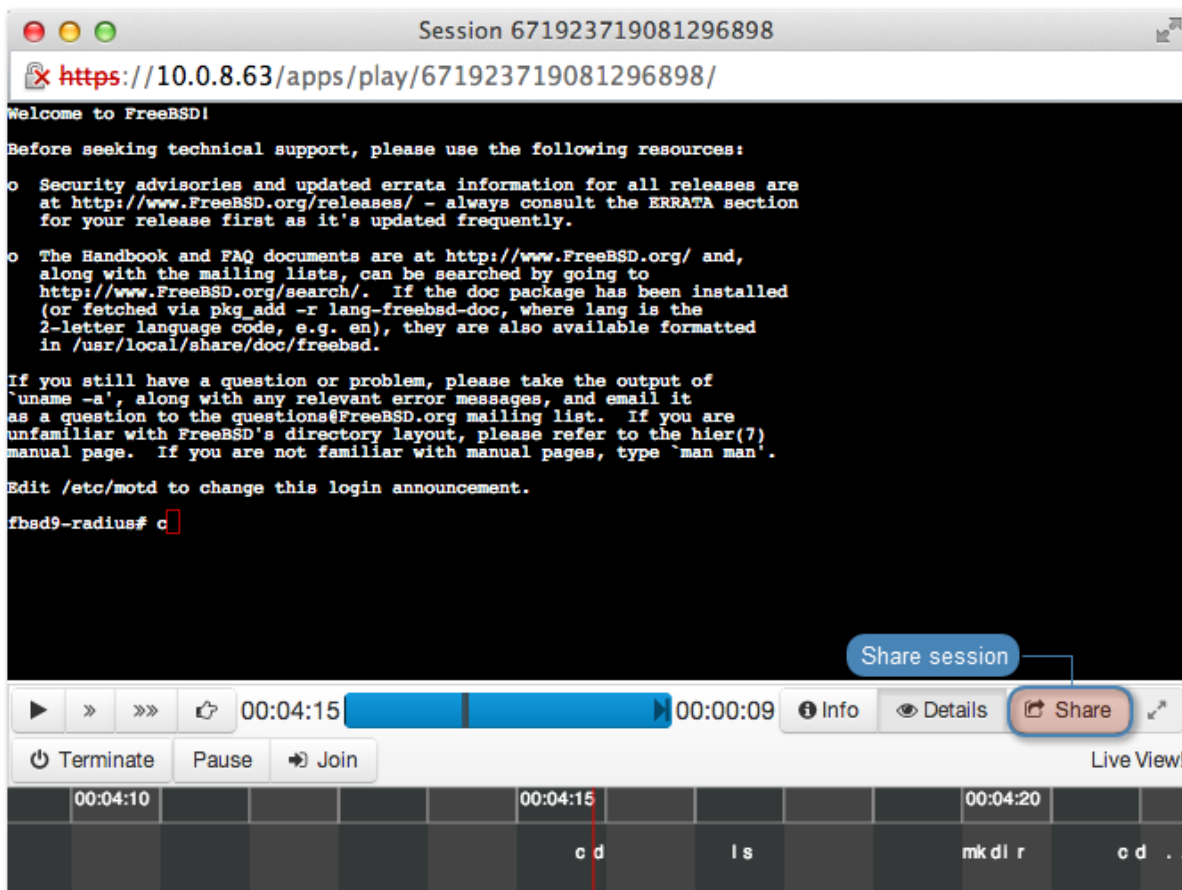
Sharing a session

To share a session, proceed as follows.

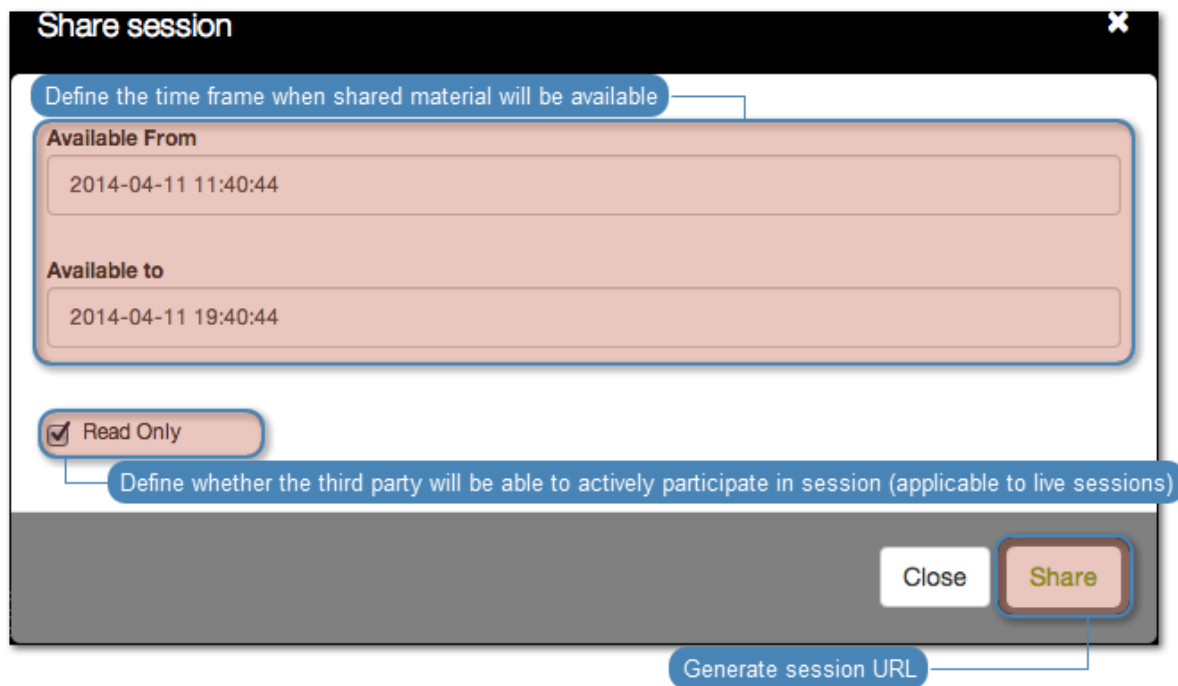
1. Select *Management > Sessions*.
2. Find desired session and click the play icon to start playback.



3. Click *Share*.



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



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

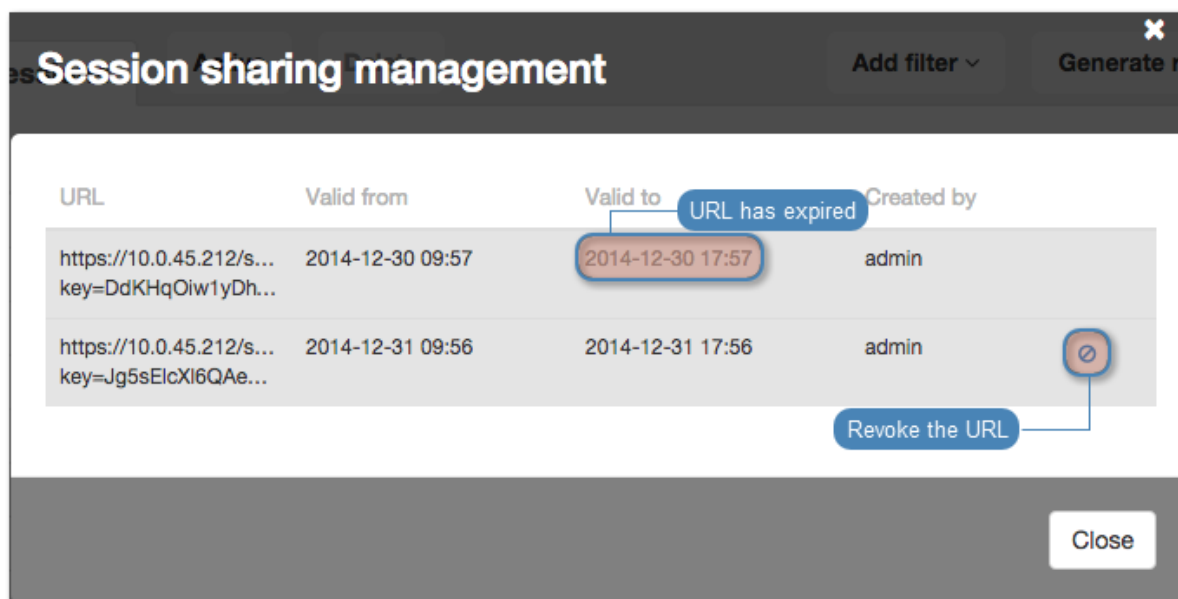
Revoking session URL

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

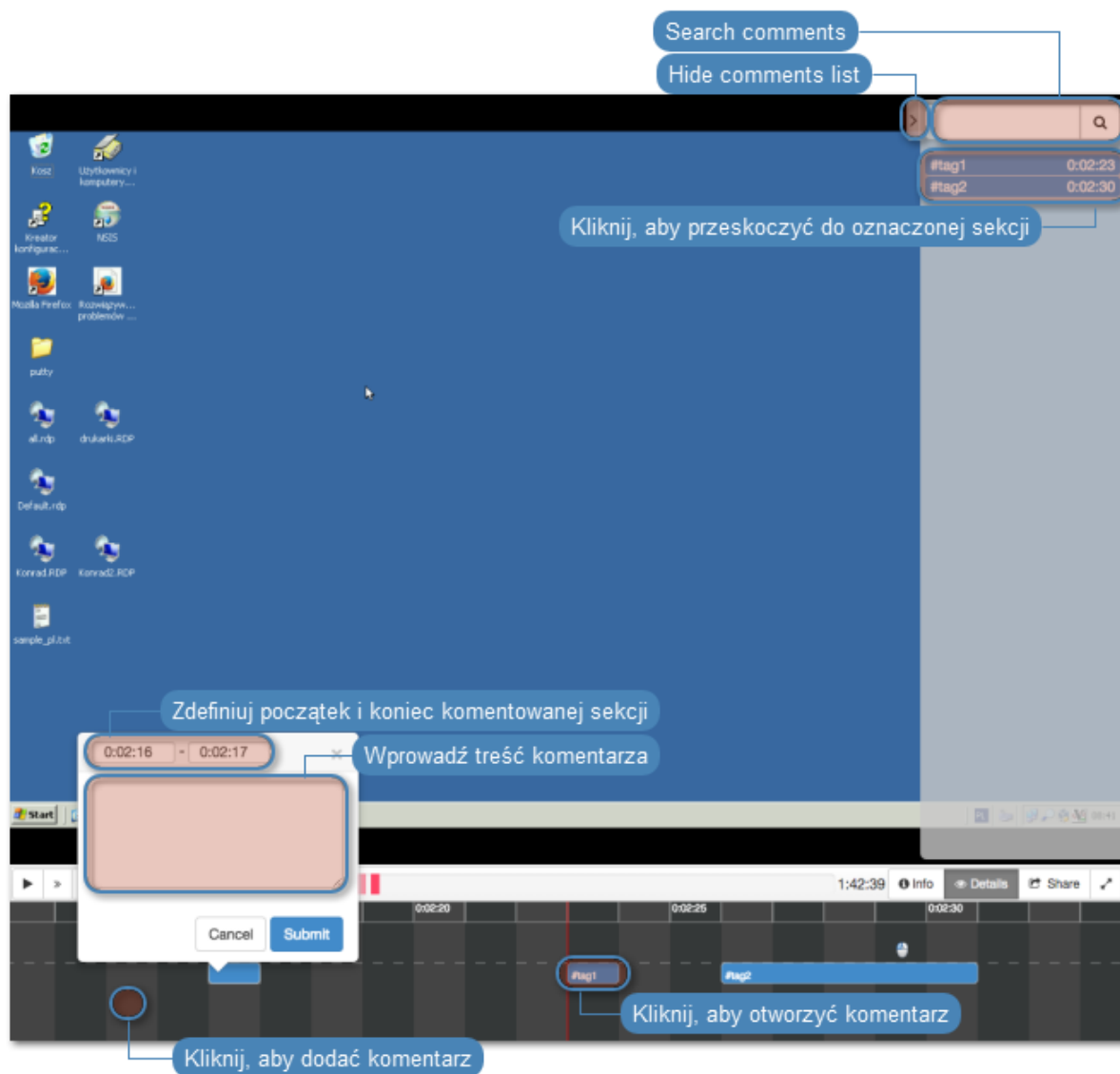
Wheel Fudo PAM enables adding comments and tags to recorded sessions.

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*.



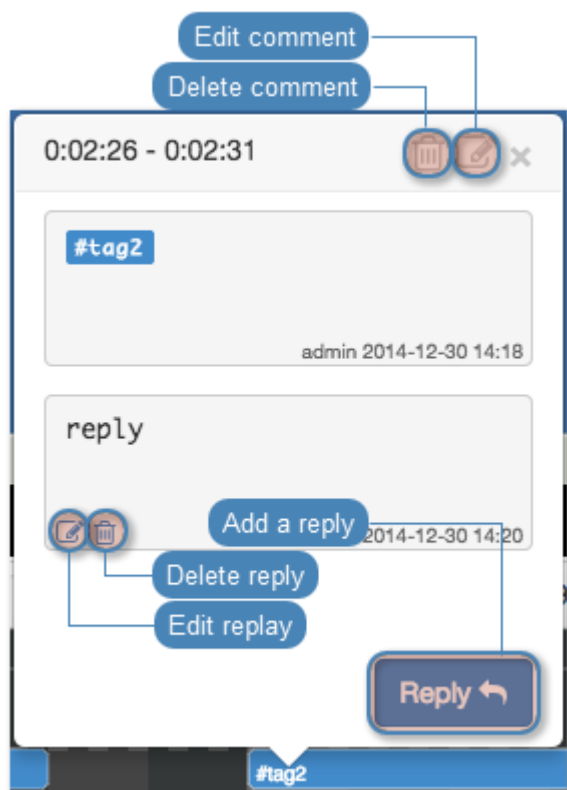
Editing a comment

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.

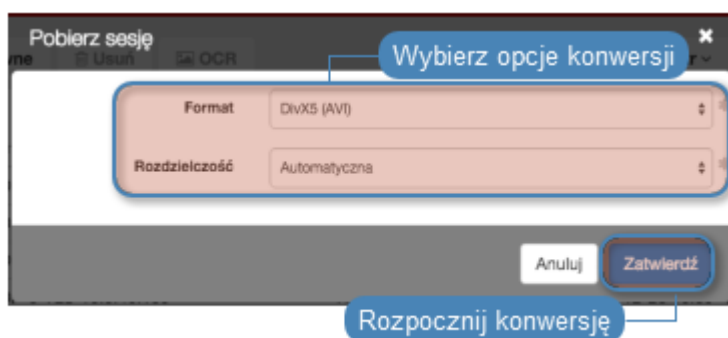
To export a session, proceed as follows.

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.



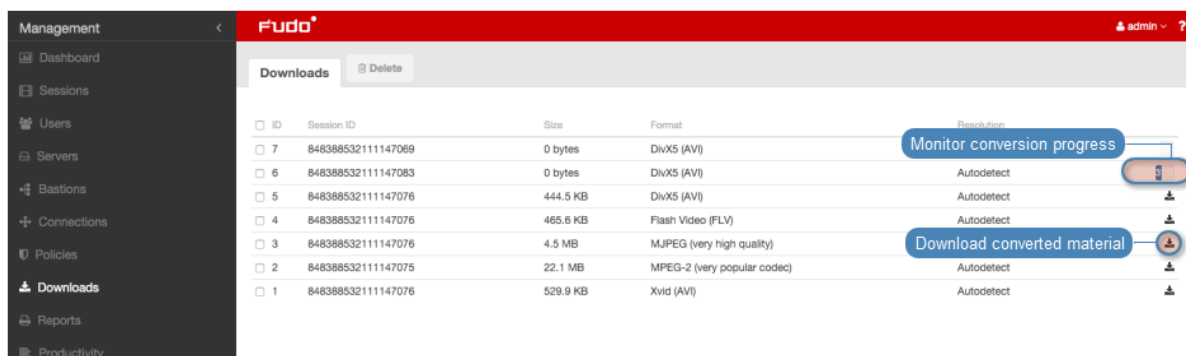
4. Select the video resolution (*not applicable to the text log file format*).

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*

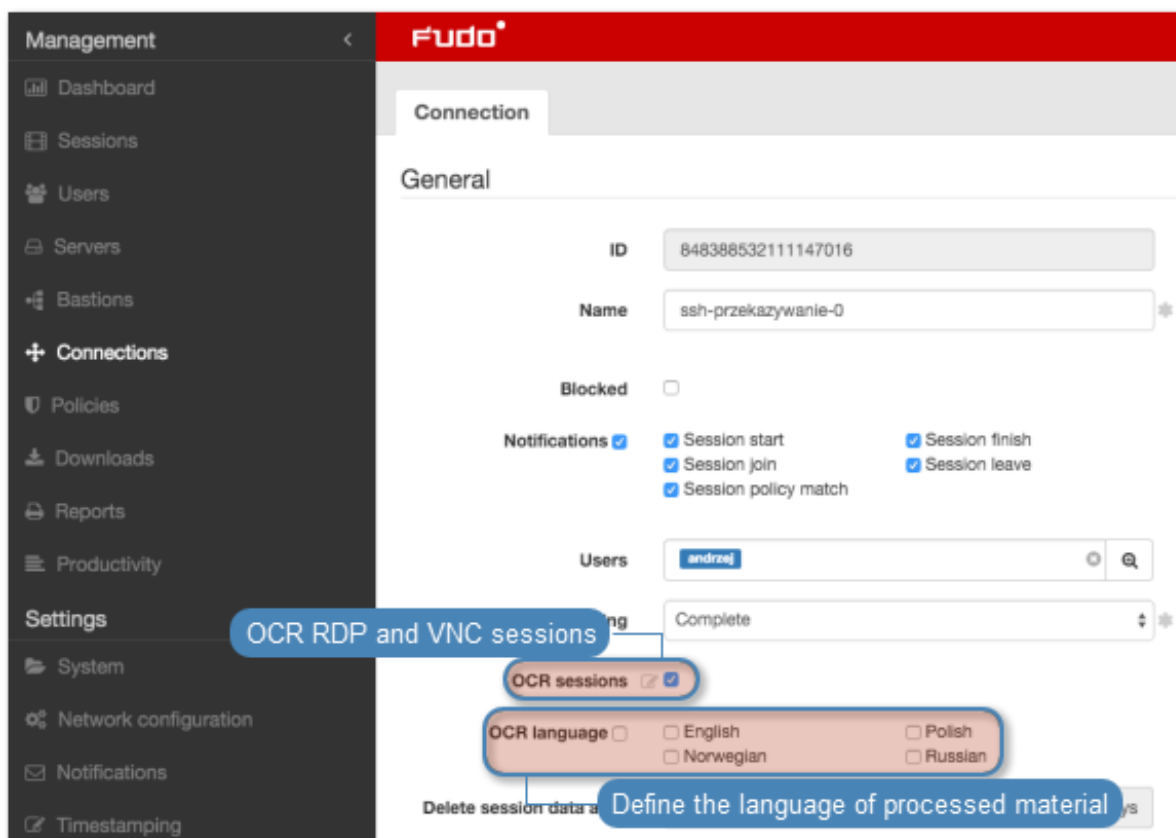
12.11 OCR processing sessions

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

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.

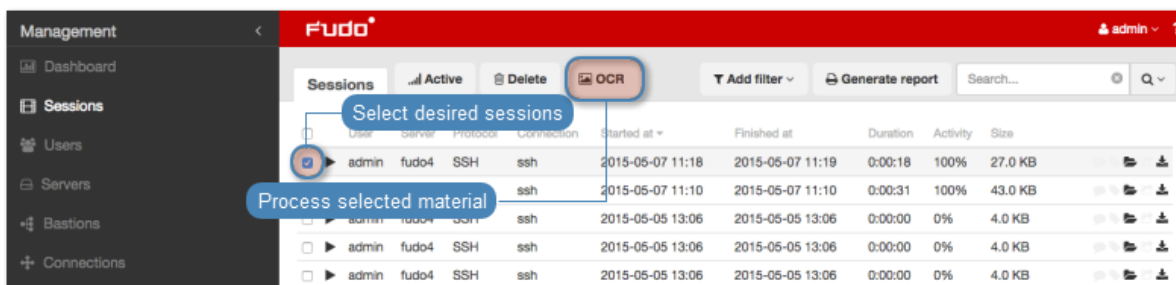


4. Click *Save*.

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.

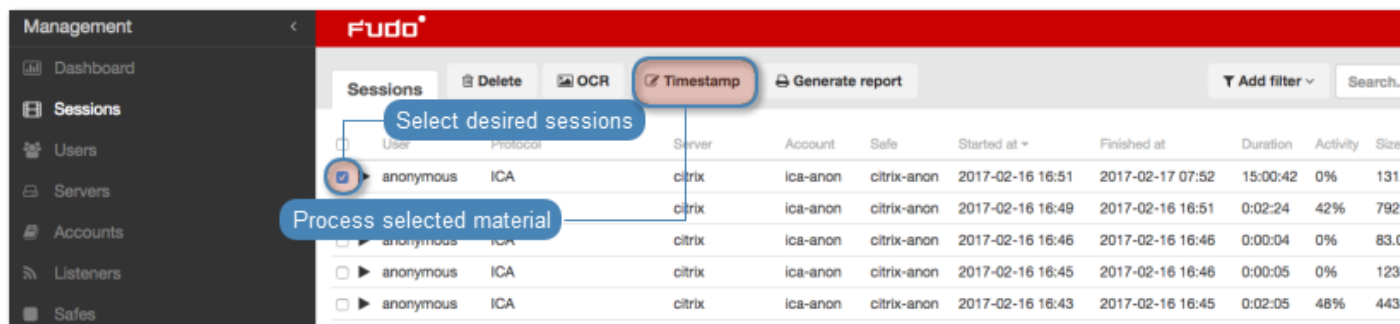
Related topics:

- *Filtering sessions*
- *Accounts*

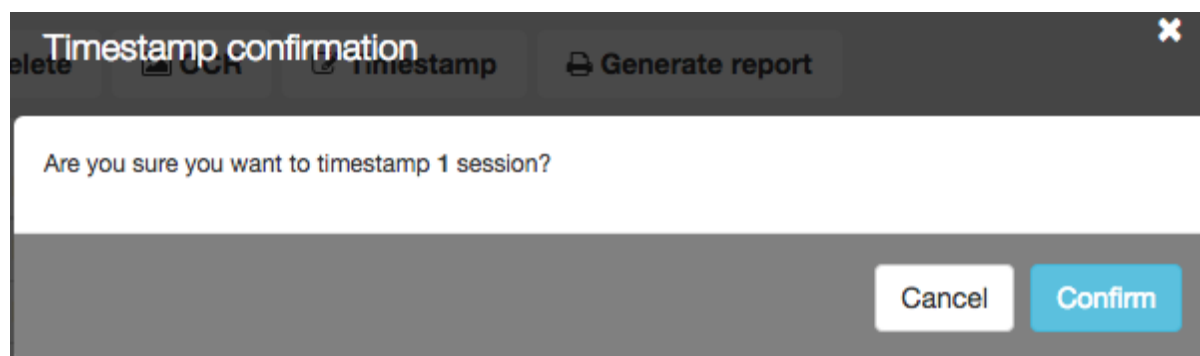
12.12 Timestamping selected sessions

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*

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*.

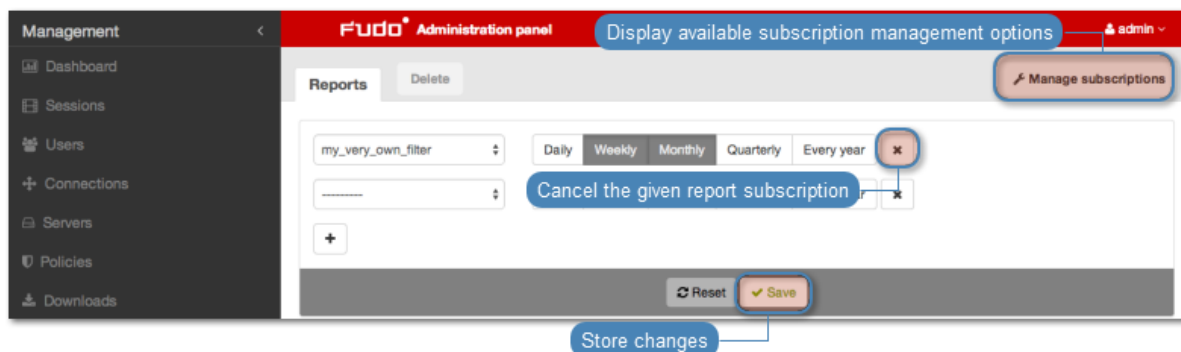
4. Choose how often the given report should be generated.
5. Click *Save*.



Canceling a periodic report subscription

To cancel a subscription to a cyclic report, proceed as follows.

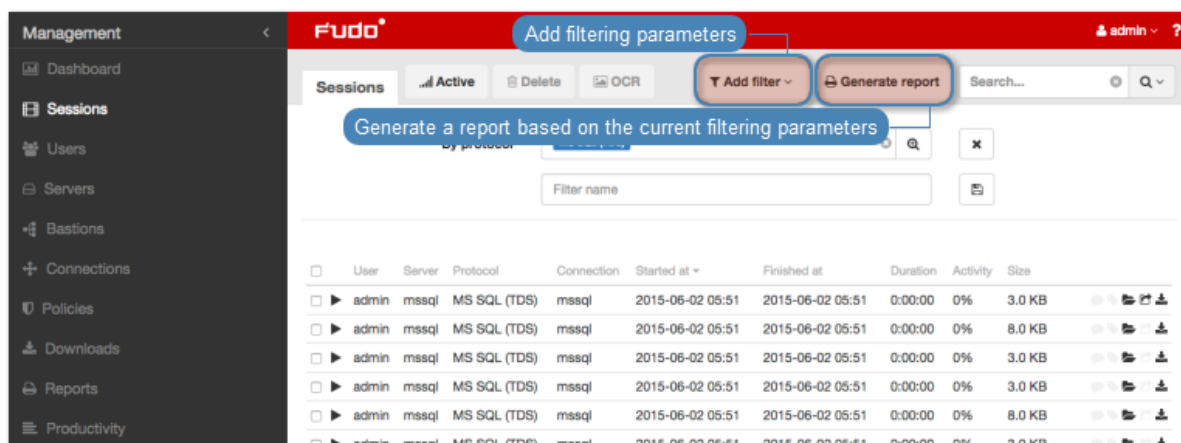
1. Select *Management > Reports*.
2. Click *Manage subscriptions*.
3. Click the report definition removal icon.
4. Click *Save*.



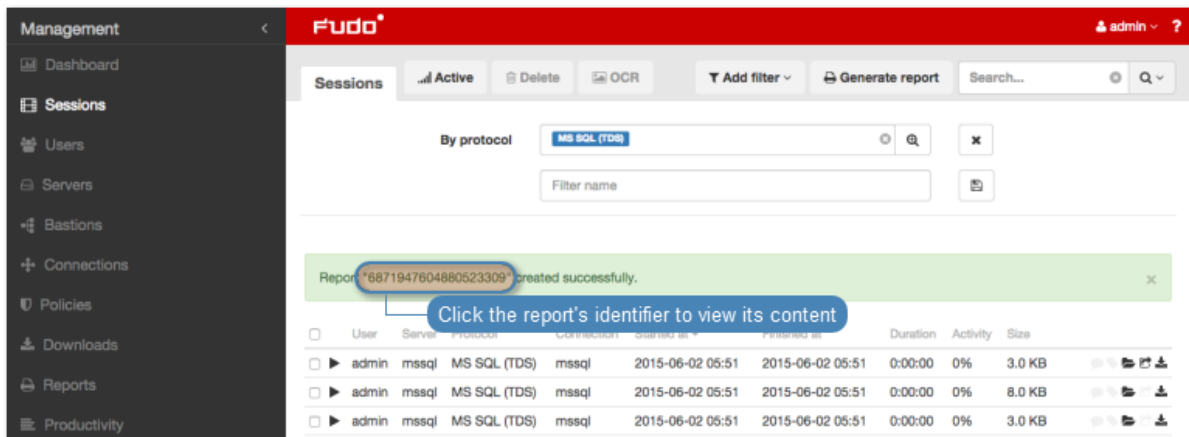
Generating reports on demand

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.



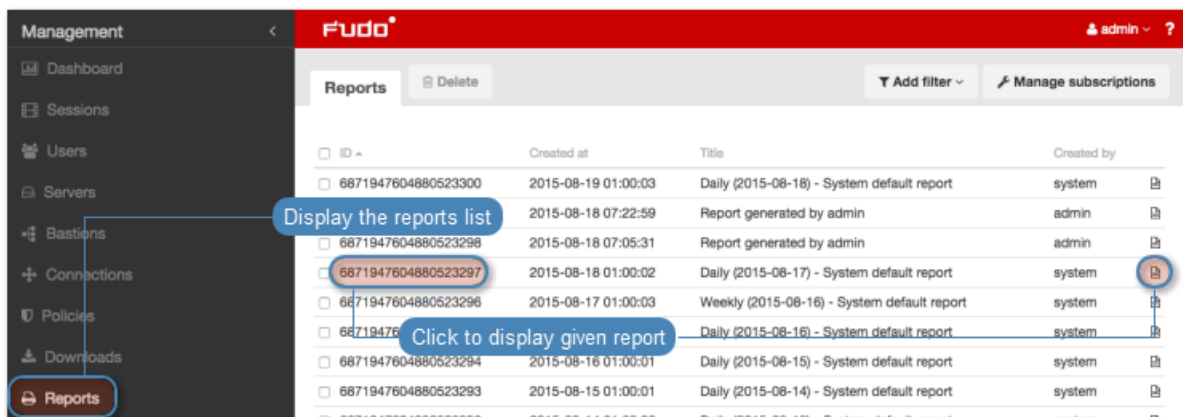
- Note your report's identifier or click it to display the report.



- Select *Management > Reports*.
- Find desired report and click the view icon.
- Click the corresponding button to save the report in selected format.

Opening and downloading reports

- Select *Management > Reports*.
- Find desired report and click the view icon.



- Click the corresponding button to save the report in selected format.

Management < Fudo admin ?

Report 848388532111147045 CSV PDF HTML

Save the report in selected format

Report criteria

- From date = 2015-12-10
- To date = 2015-12-10

Servers

Server	Number of sessions	Number of users	Sessions total time	Sessions total size	Average session time	Average session size
RDP-10.0.35.53-WindowsXP	1	1	0:00	181.0 KB	0:00	181.0 KB
RDP-10.0.40.100-Windows2012	1	1	0:24	2.3 MB	0:24	2.3 MB
RDP-10.0.40.202-Windows8	1	1	0:03	27.9 MB	0:03	27.9 MB
SSH-10.0.35.1	12	1	1:34	14.5 MB	0:07	1.2 MB

Users

User	Number of sessions	Number of servers	Sessions total time	Sessions total size	Average session time	Average session size
user0	15	4	2:02	44.8 MB	0:08	3.0 MB

Deleting reports

1. Select *Management > Reports*.
2. Find, select desired reports and click *Delete*.
3. Confirm deleting selected reports.

Related topics:

- *Notifications*
- *Filtering sessions*

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.

The screenshot shows the 'Session analysis' tab in the Fudo PAM interface. The 'Date from' field is highlighted with a callout: 'Add a filter, to limit the number of elements on the list'. Below the table, a callout points to the 'Sessions total time' header: 'Click to sort table content'. Another callout points to the 'development' organization dropdown: 'Hide users within the given organization'. A third callout points to the 'Unassigned' organization dropdown: 'Show users within the given organization'.

Organization/User	Sessions total time	Active time	Idle time	Productivity	Sessions	Servers
Total	434:58	88:47	346:11	20%	296	19
Unassigned	188:51	54:04	188:51	22%	181	16
development	18:21	12:49	18:21	41%	31	1
user-33	31:10	12:49	18:21	41%	31	1
serwis	160:53	21:54	138:59	13%	84	2
user-25	157:02	21:01	136:01	13%	80	1
user-26	3:51	0:53	2:58	22%	4	1

The screenshot shows the 'Session analysis' tab with date filters set to '2014-10-01' to '2014-11-01'. Callouts include: 'Show users from the given organization only' pointing to the 'development' dropdown, 'Show sessions analysis for the given user' pointing to the 'user-25' row, and 'Click to display sessions list for the given user/organization' pointing to the '13%' productivity value in the 'user-25' row.

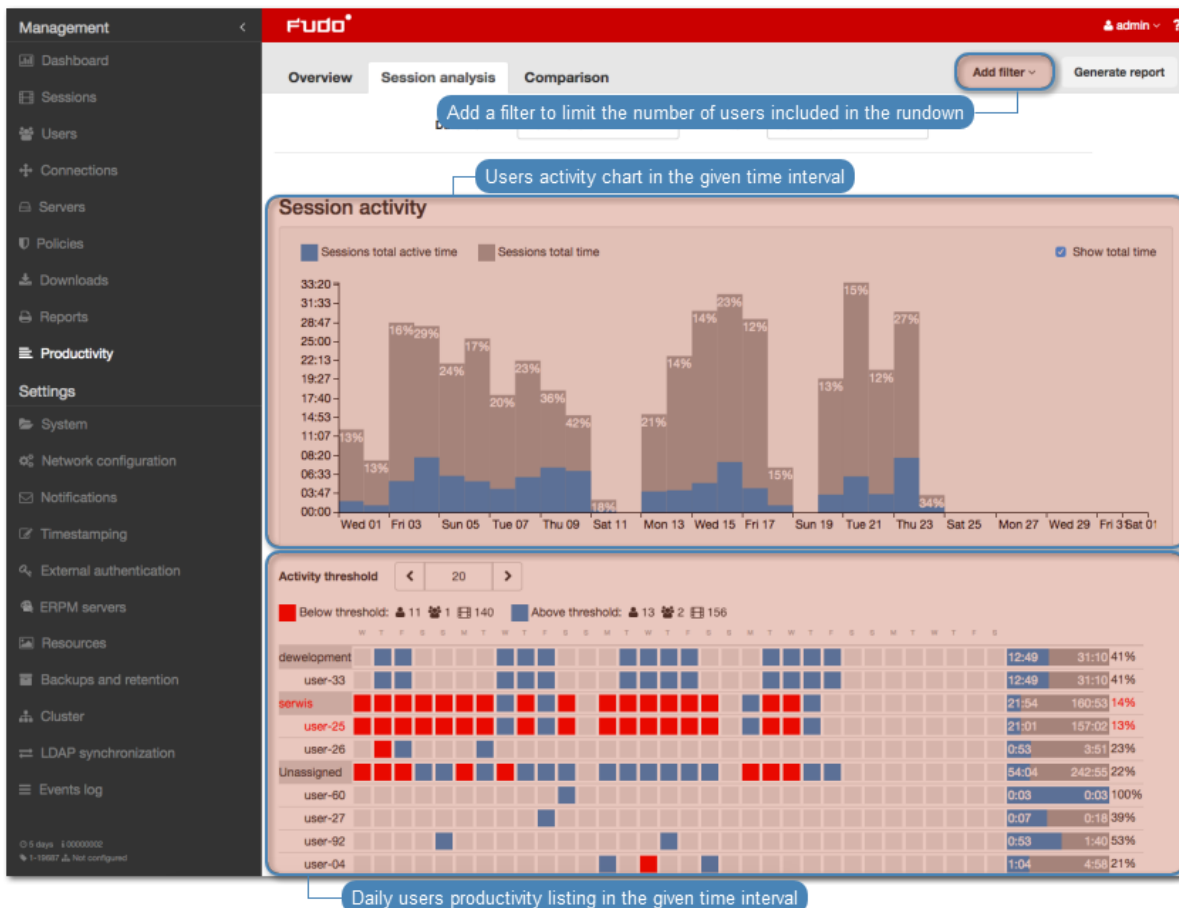
Organization/User	Sessions total time	Active time	Idle time	Productivity	Sessions	Servers
Total	434:58	88:47	346:11	20%	296	19
Unassigned	242:55	54:04	188:51	22%	181	16
development	31:10	12:49	18:21	41%	31	1
user-33	31:10	12:49	18:21	41%	31	1
serwis	160:53	21:54	138:59	13%	84	2
user-25	157:02	21:01	136:01	13%	80	1
user-26	3:51	0:53	2:58	22%	4	1

Related topics:

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

14.2 Sessions analysis

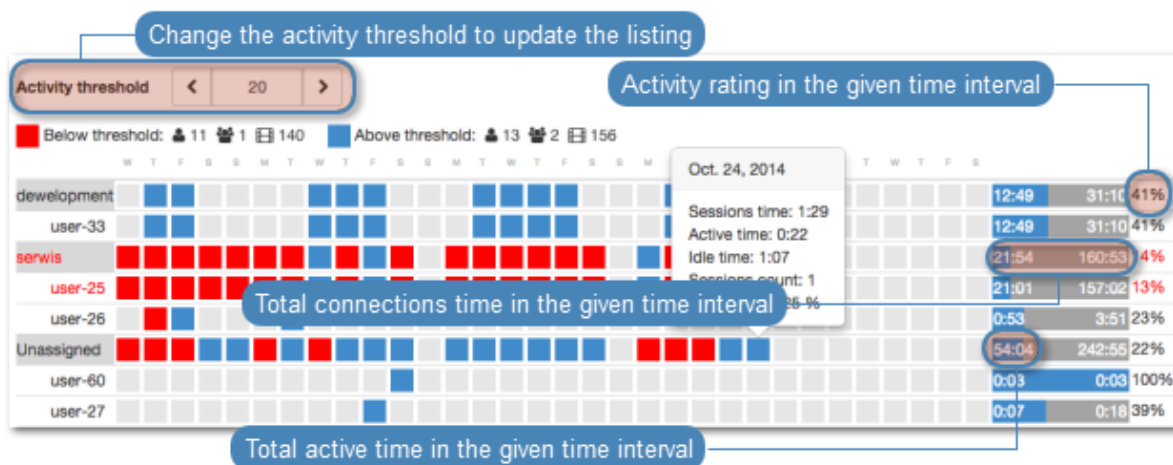
Sessions analysis shows in detail users/organizations productivity in the given time period. The activity threshold parameter allows identifying sessions, users and organisations which do not exceed the required user activity rating and helps establishing the threshold value attainable for a given number of users or sessions.

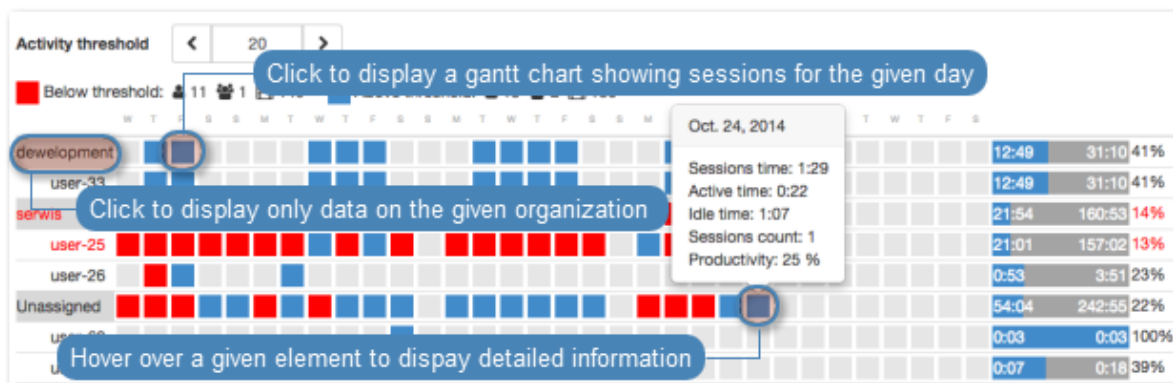


Users activity rating

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*

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.

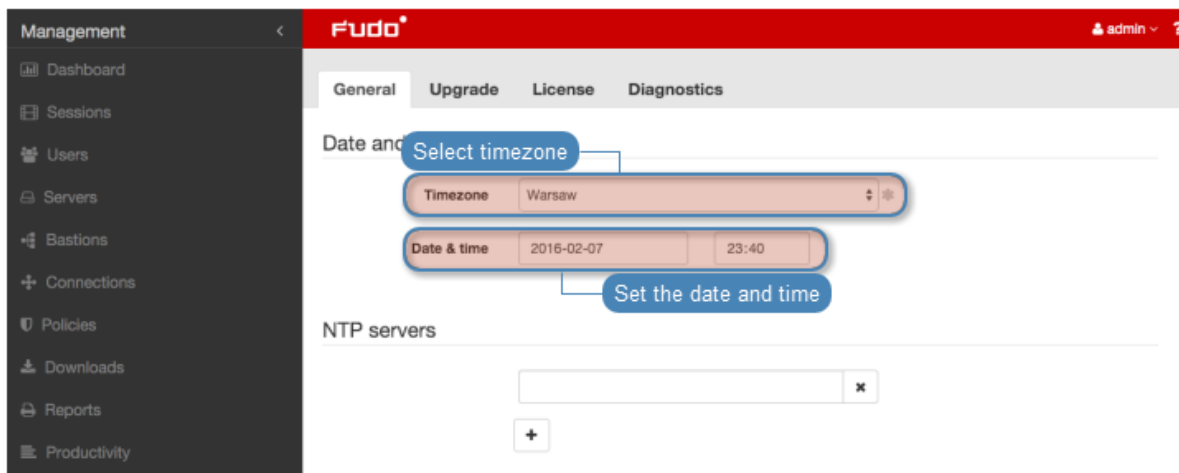
<p>Warning: It is strongly advised for the date and time settings to be obtained from a reliable NTP server. Changing date and time settings manually may result in system malfunction.</p>

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*.

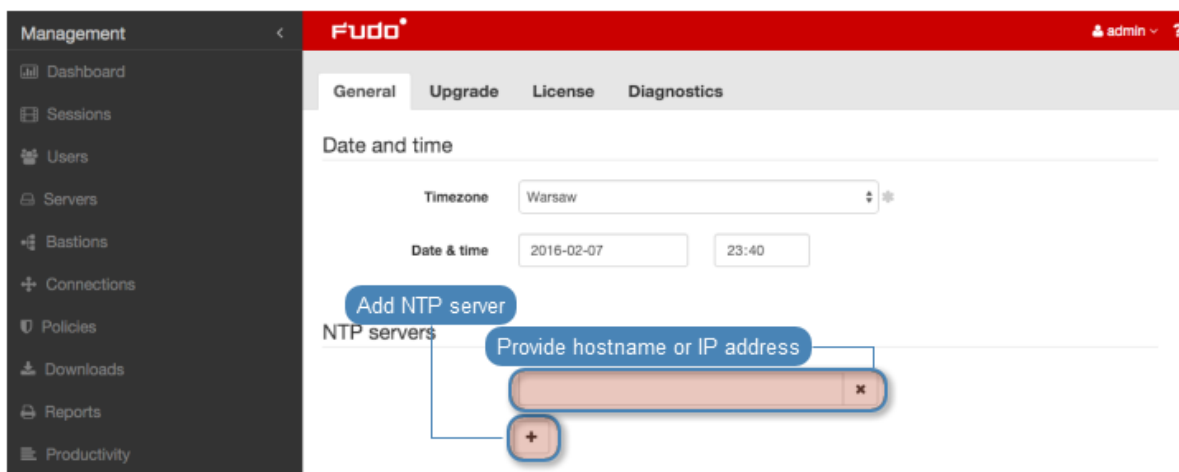
Time servers configuration

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.

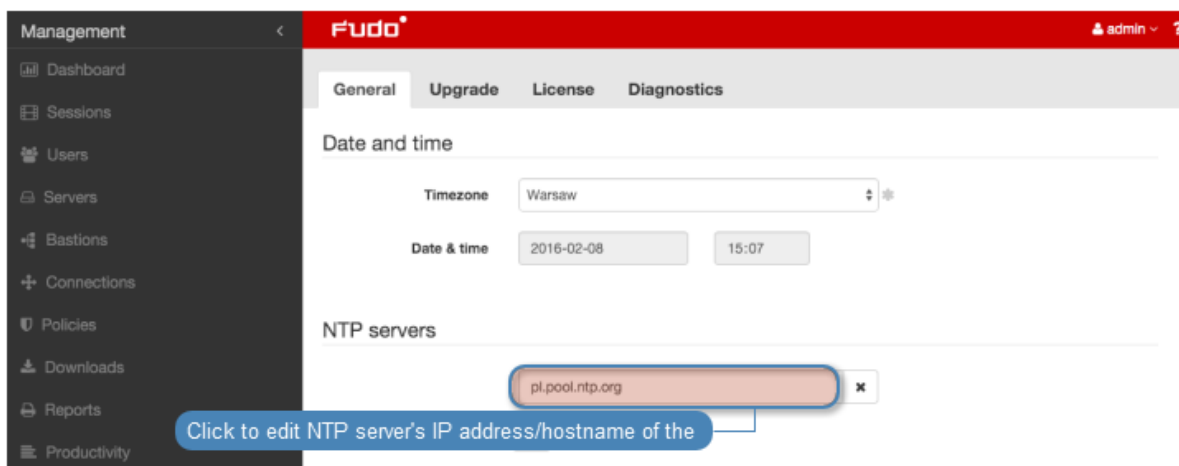


4. Click *Save*.

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.

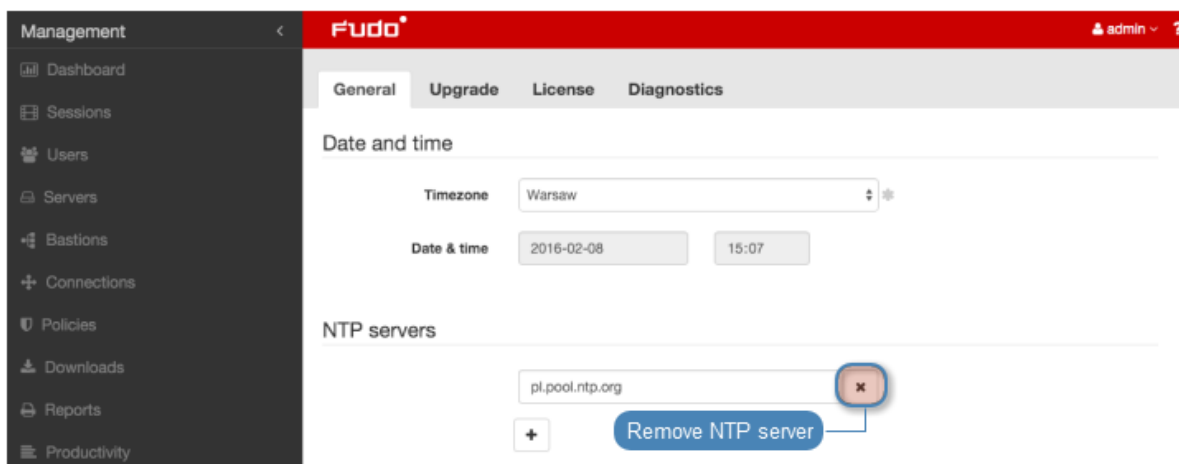


3. Click *Save*.

Deleting an NTP server definition

To remove an 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 certificate

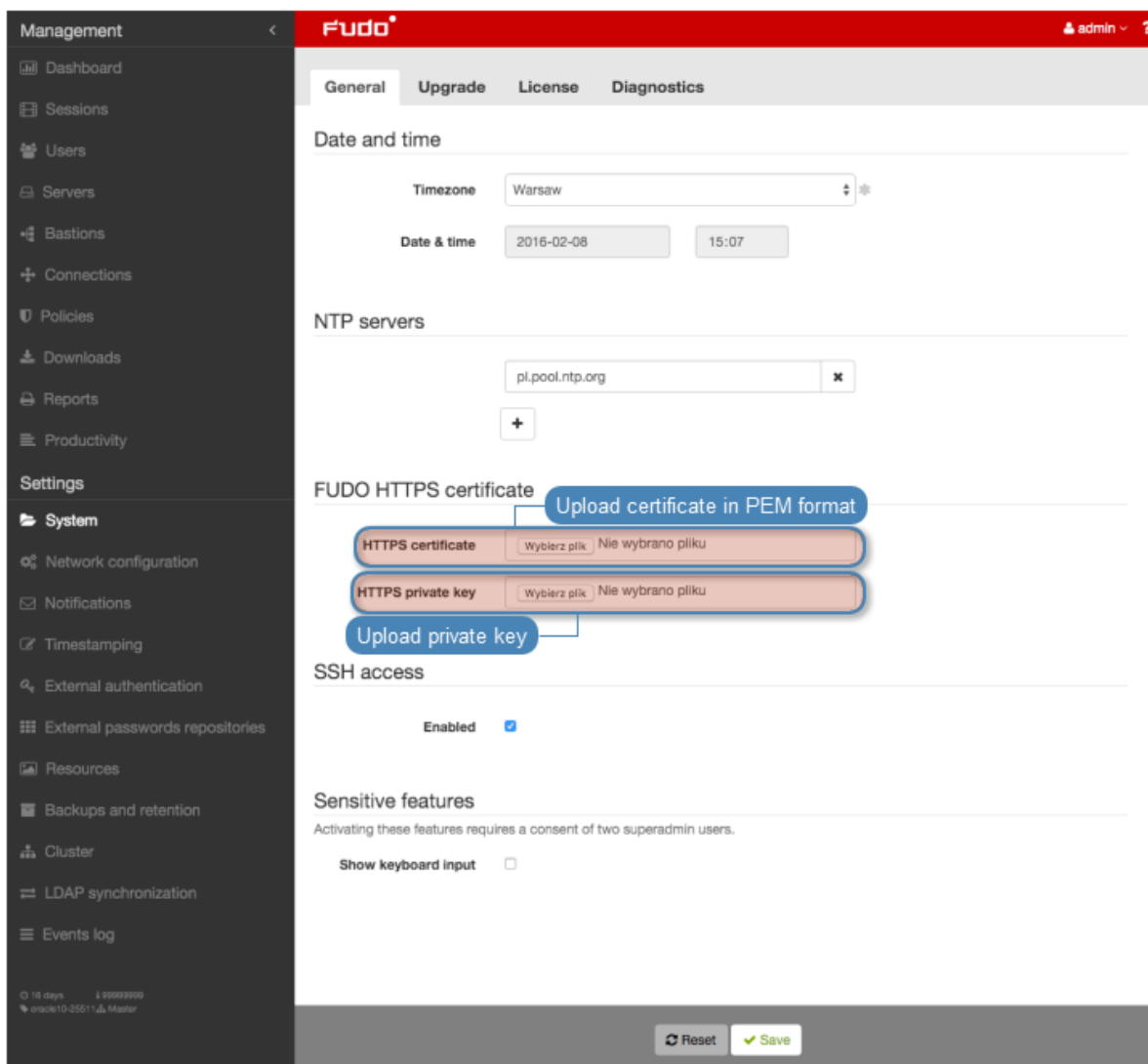
SSL certificate allows prevent phishing attacks.

Configuring SSL certificate

To configure SSL certificate, proceed as follows.

1. Select *Settings > System*.
2. Click the *Browse* button next to the *HTTPS Certificate* field in the *FUDO 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*

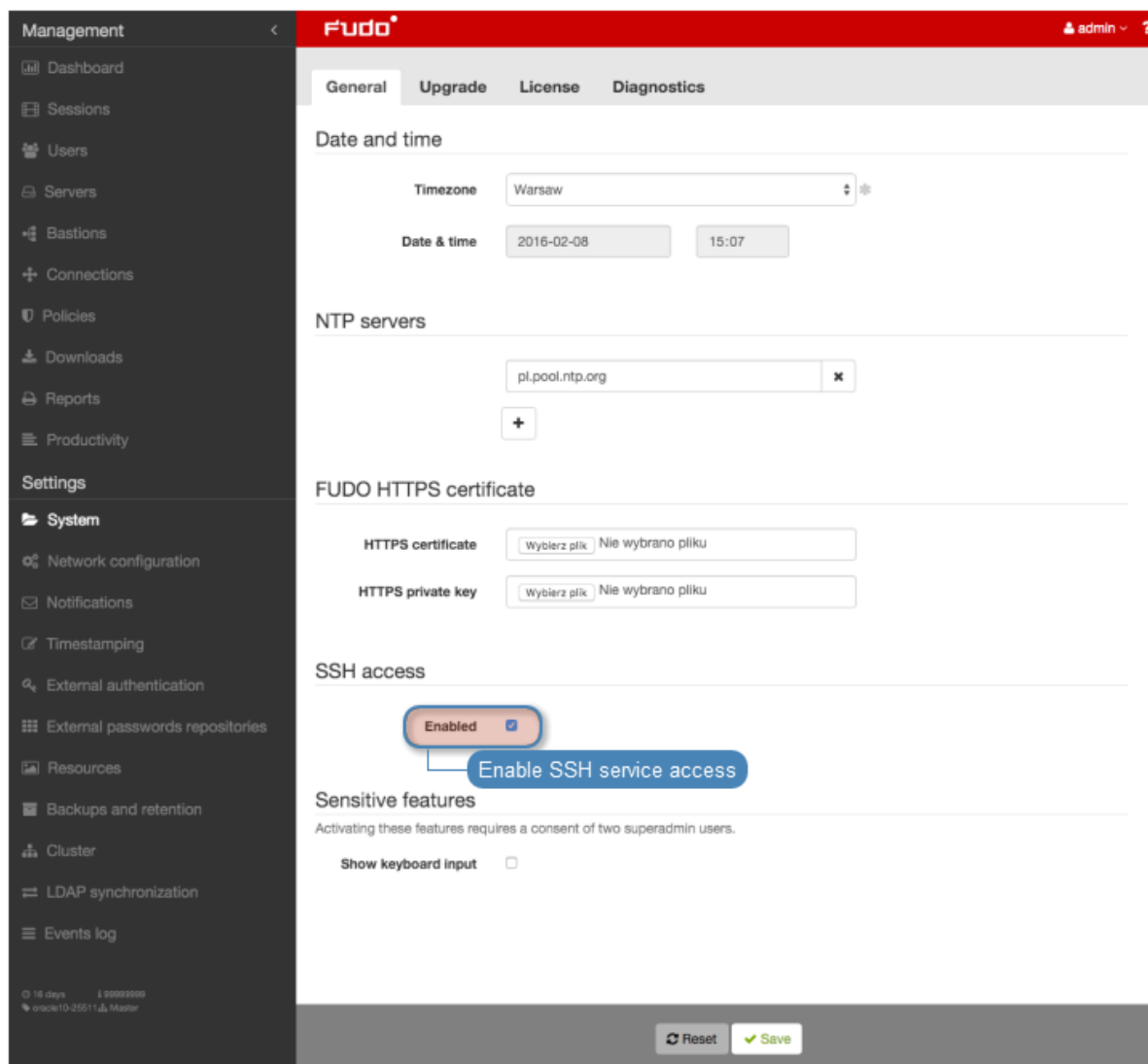
15.1.4 SSH access

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

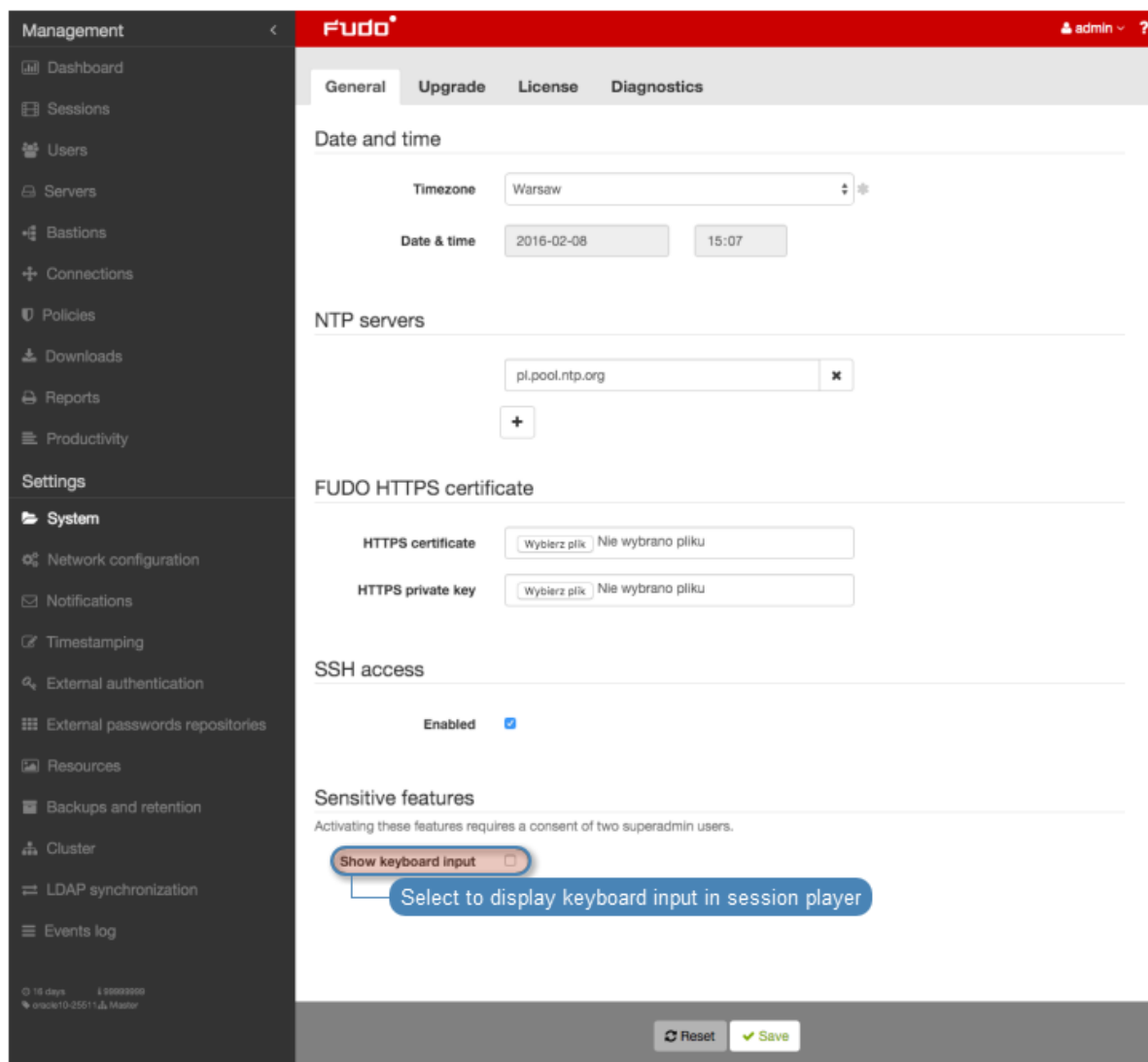
Sensitive features is a set of options enabling which requires a consent from two **superadmin** users.

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:

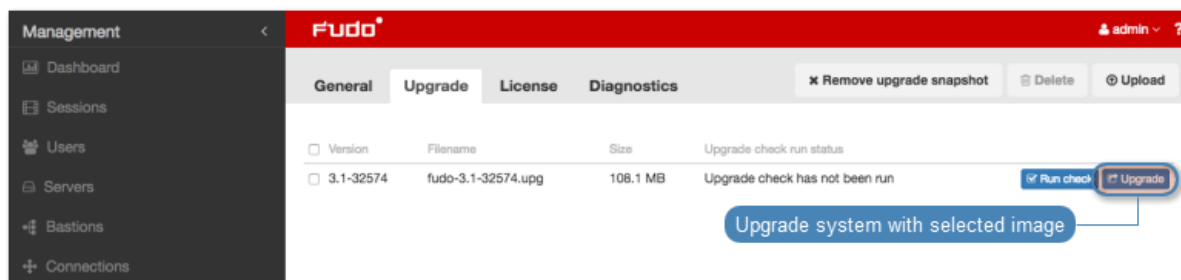
- In addition to the current system version, Wheel Fudo PAM stores the previous revision, allowing for restoring the system to its previous state.
- The system update process does not influence the system configuration or the session data stored on Wheel Fudo PAM.
- The storage usage may temporarily increase during system update.

15.1.7.1 Updating system

Warning:

- Before updating the system it is advised to run a preliminary check to ensure that the current system configuration can be successfully upgraded to new version.
- If the storage usage on the system being updated exceeds 85%, contact Wheel System 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 in the system settings menu.

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 *Upgrade*.



Warning: After running system update, Wheel Fudo PAM will restart automatically.

Rebooting Wheel Fudo PAM requires the encryption key. Connect the USB flash drive containing the encryption key to the USB port before proceeding.

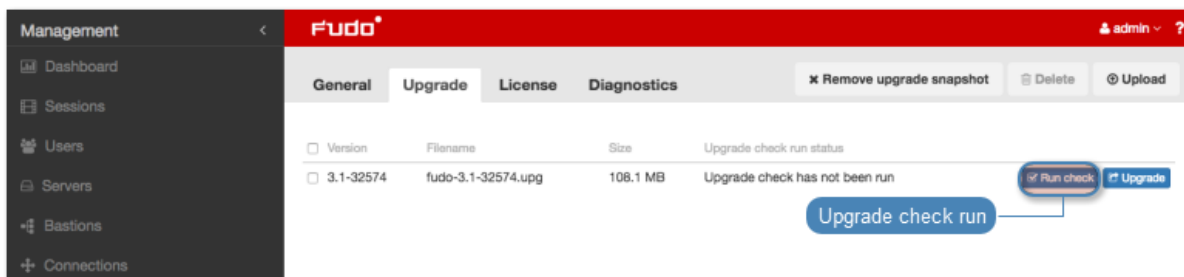
Note: In the event of an unsuccessful system update, Wheel Fudo PAM detects the problem during system restart and restarts itself using the previous system revision.

15.1.7.2 Running update check

Before updating the system it is advised to run a preliminary check to ensure that the current system configuration can be successfully upgraded to new version. The preliminary upgrade check also estimates the time it will take to perform the 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 *Run check*.



Note:

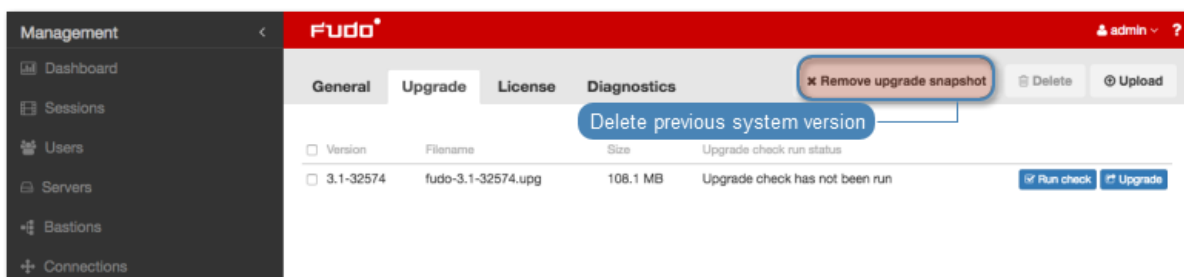
- Click *Cancel check* to stop the preliminary upgrade check.
- Click *Download log* to view the upgrade procedure log along with the information on how long it will take to perform the upgrade.

15.1.7.3 Deleting upgrade snapshot

Deleting upgrade snapshot will free the storage space occupied by previous system version.

Warning: After deleting the upgrade snapshot it will not be possible to restore the system to previous version.

1. Select *Settings > System*.
2. Select the *Upgrade* tab.
3. Click *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*.

The screenshot displays the Fudo web interface. On the left is a sidebar with 'Management' and 'Settings' sections. The 'License' tab is active, showing a form with the following fields: Serial number (12345678), Expiration date (2016-03-31), License owner (Wheel Systems sp. zoo), License type (test), Accounting mode (host,port), Cluster nodes limit (1), and Number of servers (25). A progress bar indicates 11 servers in use and 14 available. Below the form is a 'Usage statistics' section with a date range from 2015-11-01 to 2016-02-08 and a bar chart titled 'Concurrent connections statistics' showing the number of concurrent sessions over time.

4. Browse the file system to find the license file and click *OK* to upload and replace current license definition.

Related topics:

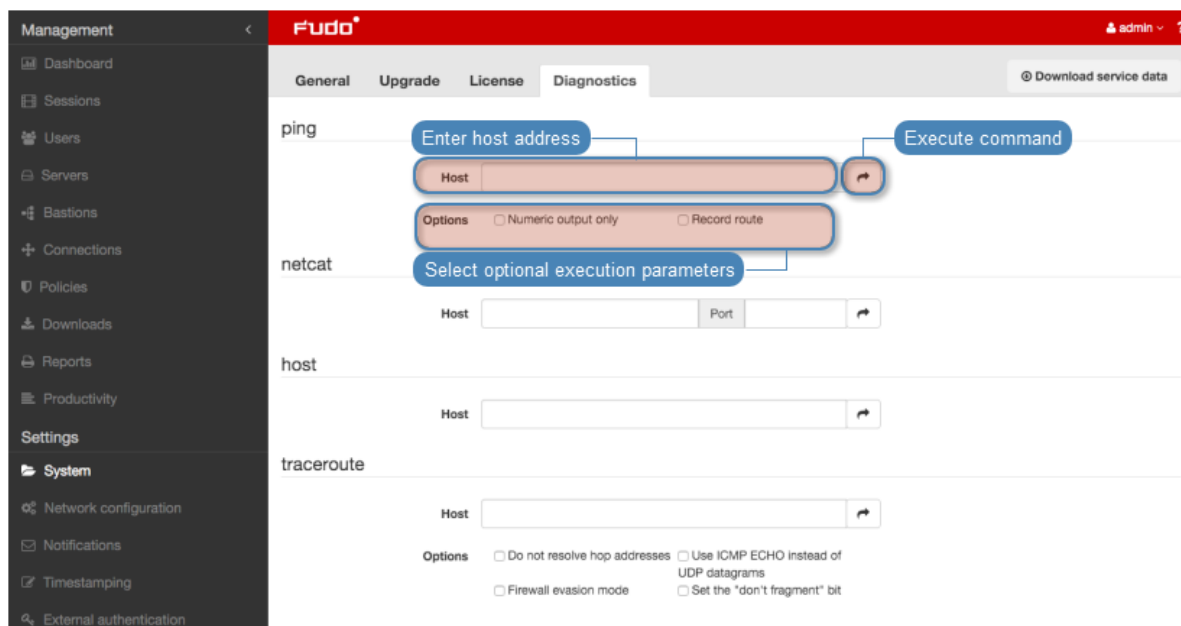
- *System*

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.



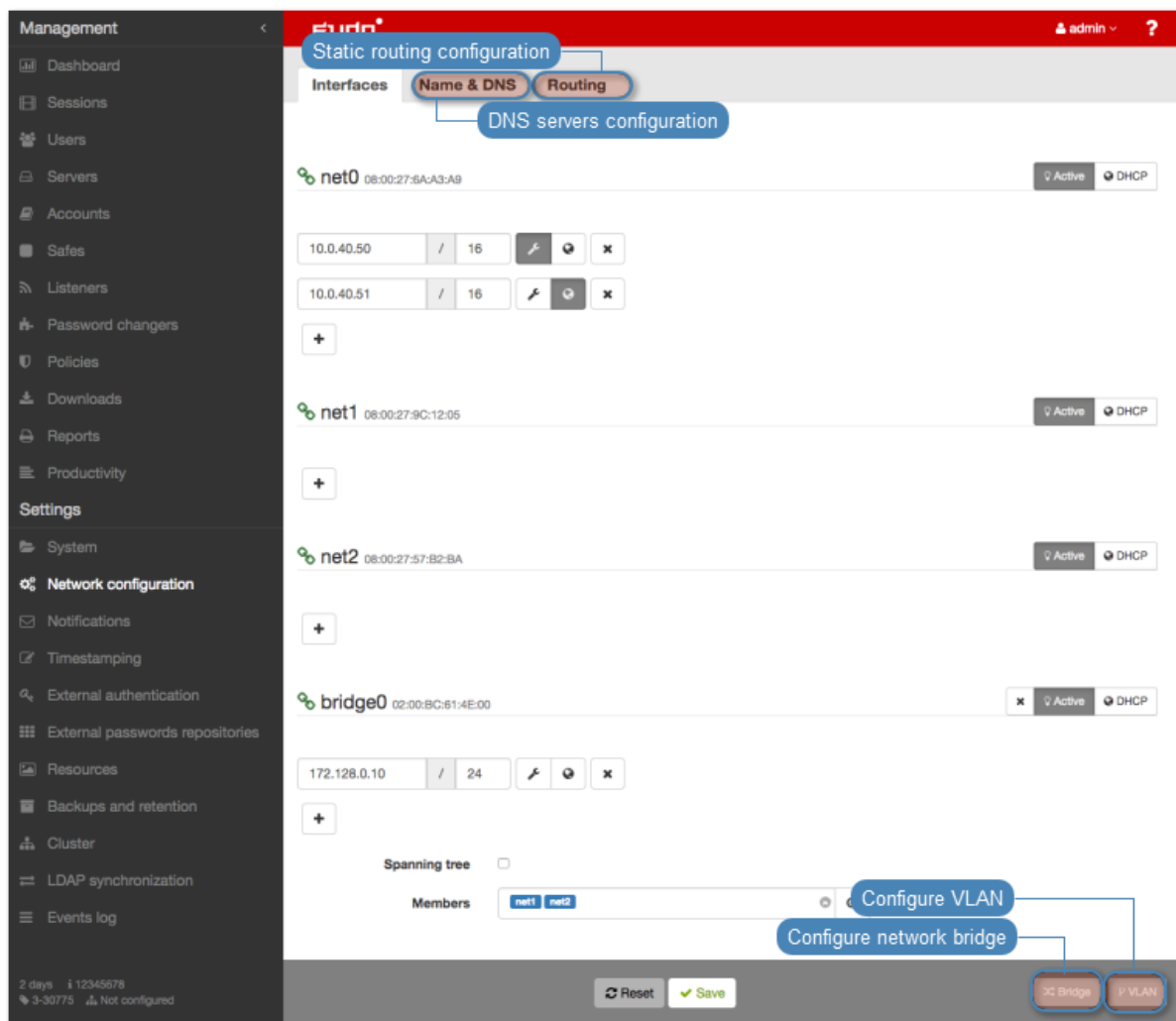
Command/parameter	Description
Ping	Ping sends a sequence of 10 ICMP packets to selected host.
Numeric output only	Does not resolve host's IP address to its mnemonic name.
Record route	Enables tracking packets' route.
netcat	<code>etcat</code> allows establishing connection with remote host on specified port number.
host	<code>host</code> is used to determine if the DNS server correctly resolves mnemonic hostnames.
traceroute	<code>traceroute</code> 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 <code>traceroute</code> 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](#)

15.2 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 there 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.

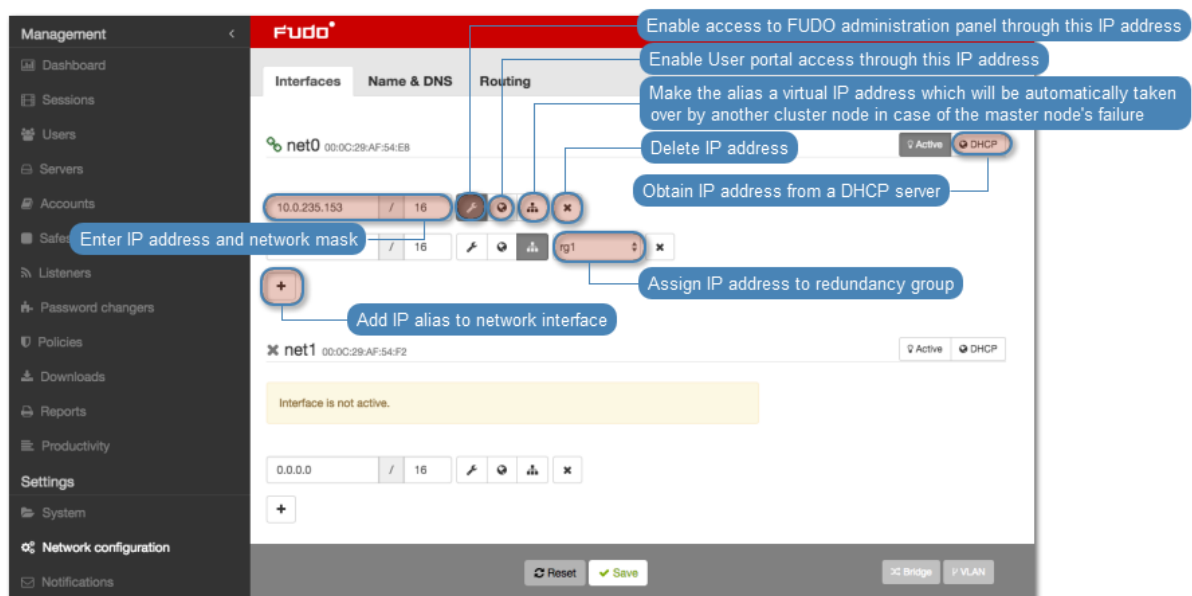
 Enable access to administration panel on given IP address. Note that the management IP address is also used for replicating data between cluster nodes.

 Make the alias a virtual IP address which will be take over by another cluster node in case of the master node's failure.




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.

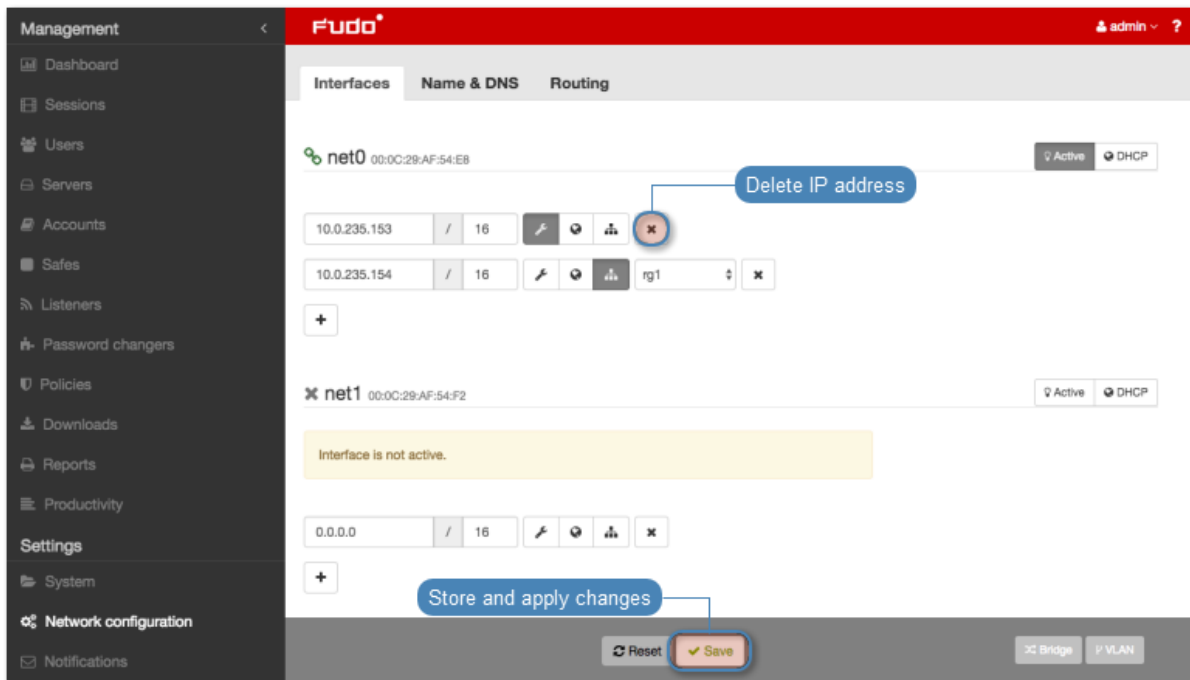
-  Interface active and connected.
-  Interface active but disconnected.
-  Interface disabled.

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.

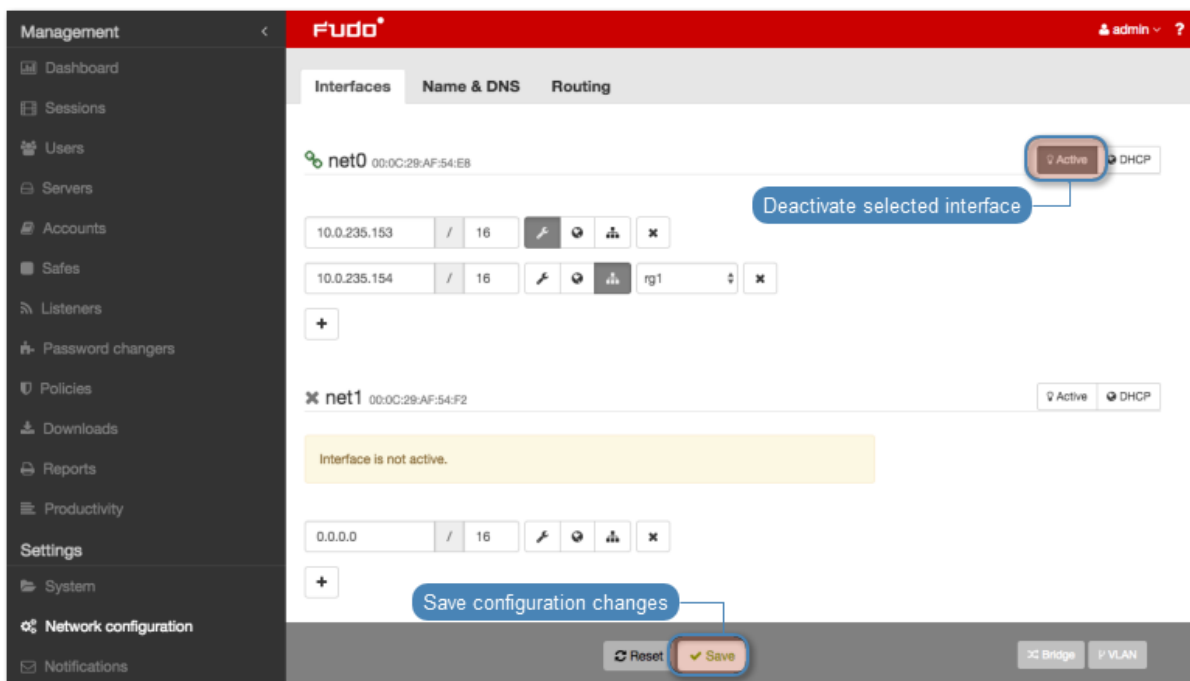
1. Select *Settings* > *Network configuration*.
2. Select desired IP address assigned to given network interface and click *x*.
3. Click *Save*.



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*.

```
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: █
```

3. Enter administrator account password 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:
```

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*.

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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0

*** FUDO configuration utility ***

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

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

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

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.

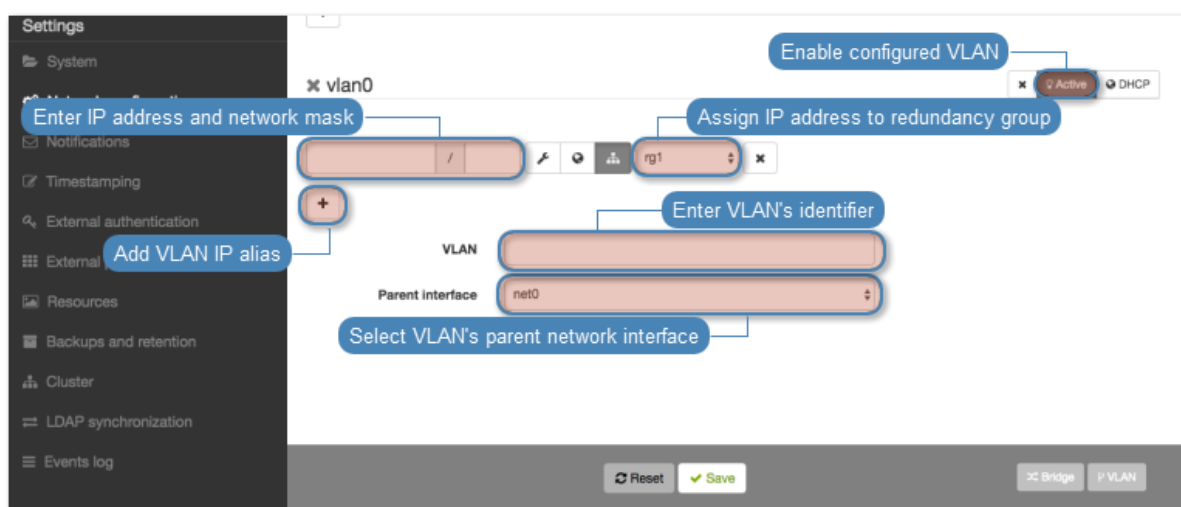
1. Select *Settings > Network configuration*
2. Click *VLAN*.
3. Select the physical interface and define VLAN ID.

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*.

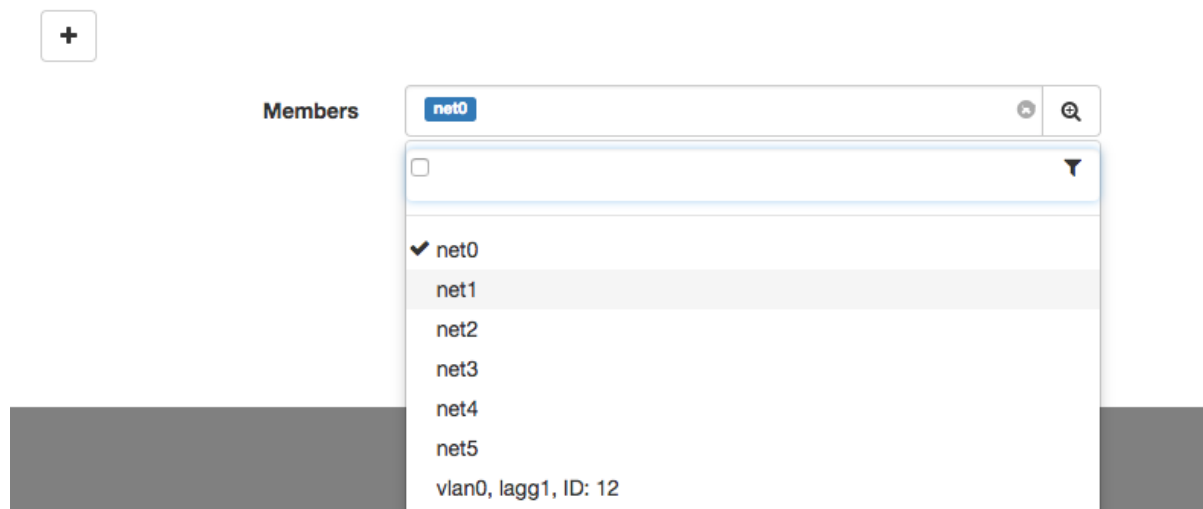


15.2.1.5 Setting up LACP link aggregation

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 and thus are replicated throughout cluster's nodes. 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.

Destination host

The screenshot shows a configuration form for a destination host. It includes fields for IP address (10.0.1.35), Port (22), Bind address (Any), and Server public key. A dropdown menu for Bind address is open, showing a list of labeled IP addresses: label_1 [10.0.150.153], label_2 [10.0.0.6], label_3 [10.0.150.151], and label_4 [10.0.150.152]. Below the dropdown is a text area for the server public key and a SHA1 hash field containing the value a0:5f:e4:a3:31:b0:9f:f4:e8:72:d9:d5:ee:4d:5a:c7:d9:54:29:57.

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*.

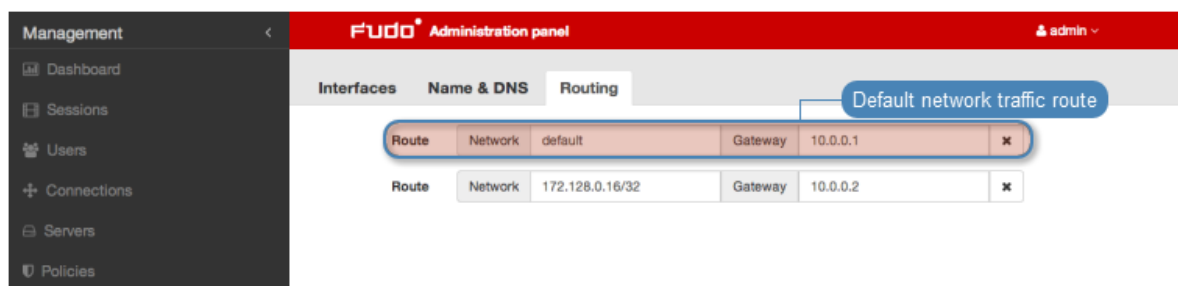
Related topics:

- *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.

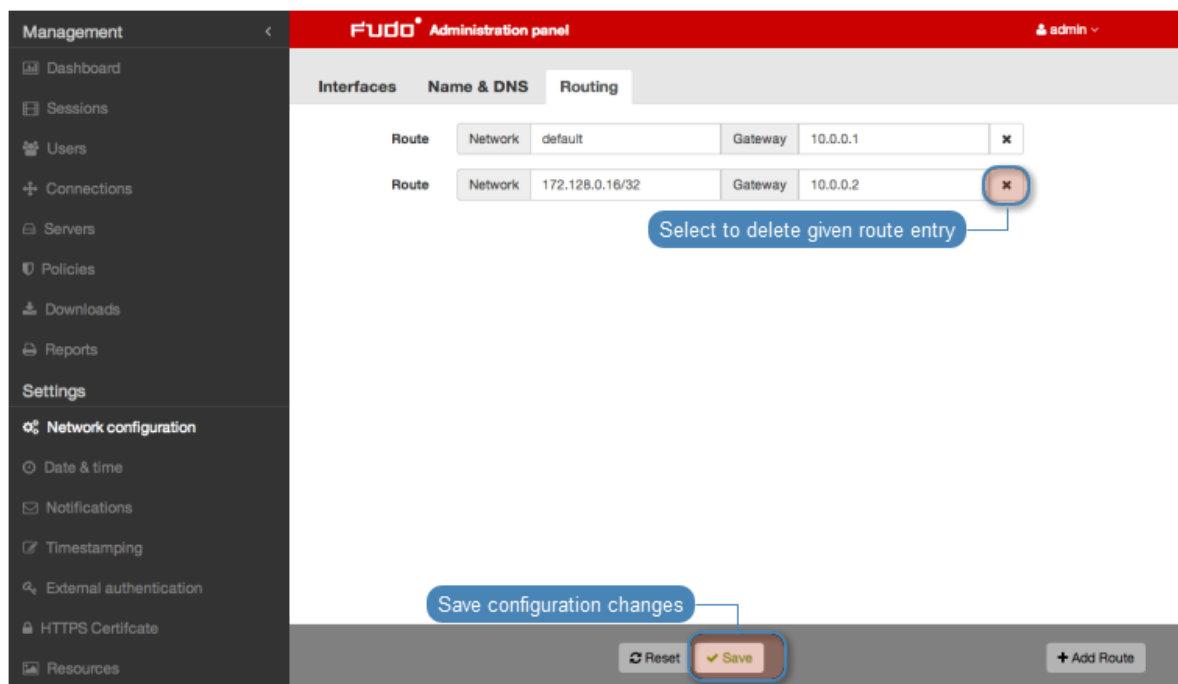
1. Select *Settings > Network configuration*.
2. Select *Routing* tab.
3. Find and edit desired route entry.

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*.

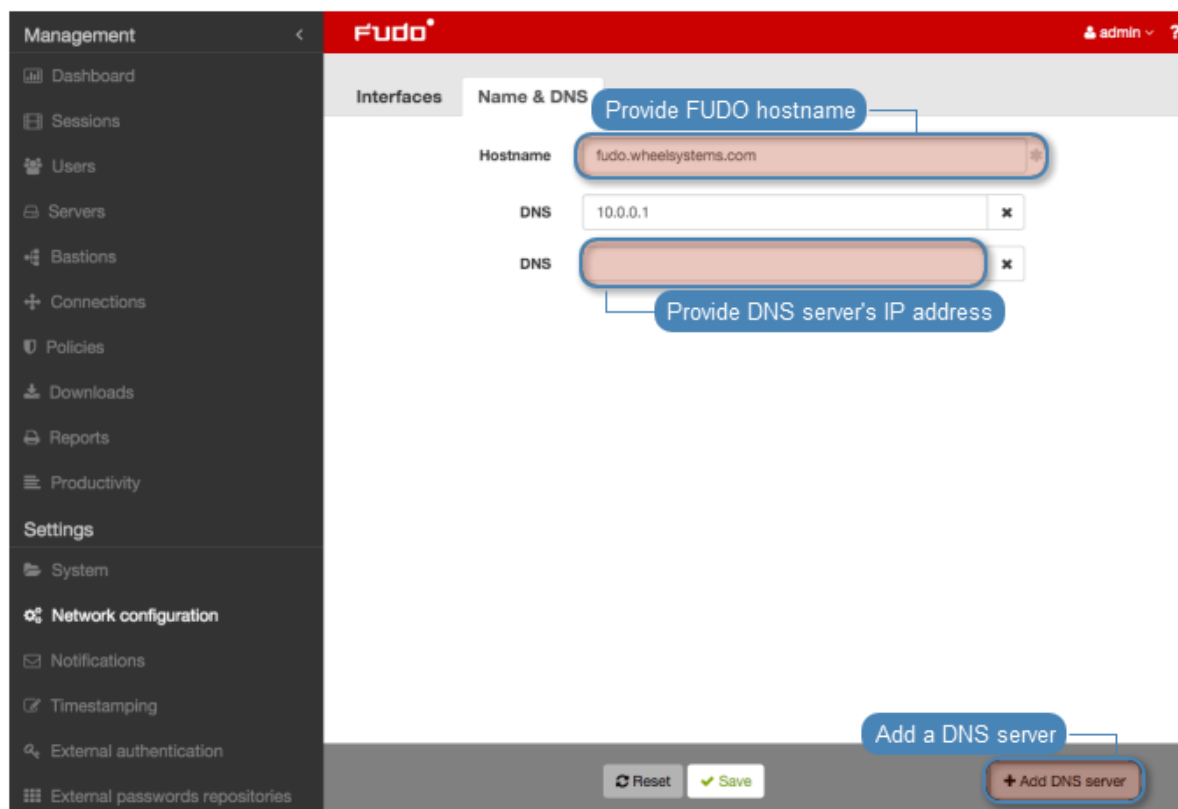


Related topics:

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

15.2.5 DNS servers configuration

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



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*

15.3 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. 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.

The screenshot displays the 'Settings' page for 'Notifications' in the Wheel Fudo PAM interface. The left sidebar shows the navigation menu with 'Notifications' selected. The main content area shows the 'Notifications' settings, where the 'Enabled' checkbox is checked. Below this, the 'Primary SMTP server' configuration form is shown, with the following fields and values:

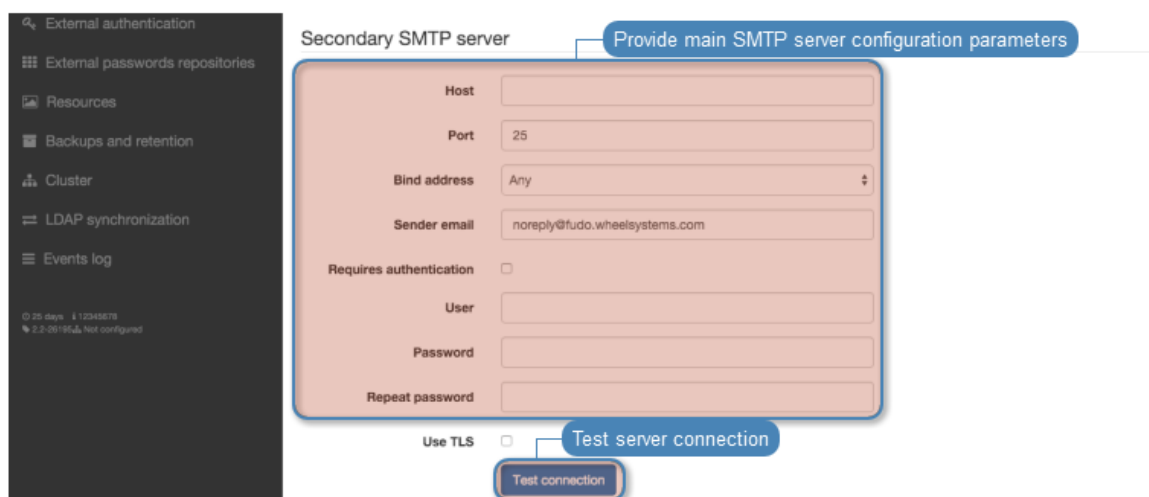
- Host: smtp.wheelsystems.com
- Port: 25
- Bind address: Any
- Sender email: fudo-dwt-40.50@wheelsystems.com
- Requires authentication:
- User: notify
- Password: [Redacted]
- Repeat password: [Redacted]

At the bottom of the form, the 'Use TLS' checkbox is checked, and a 'Test connection' button is visible. Blue callout boxes highlight the 'Enabled' checkbox, the 'Primary SMTP server' section, and the 'Test connection' button.

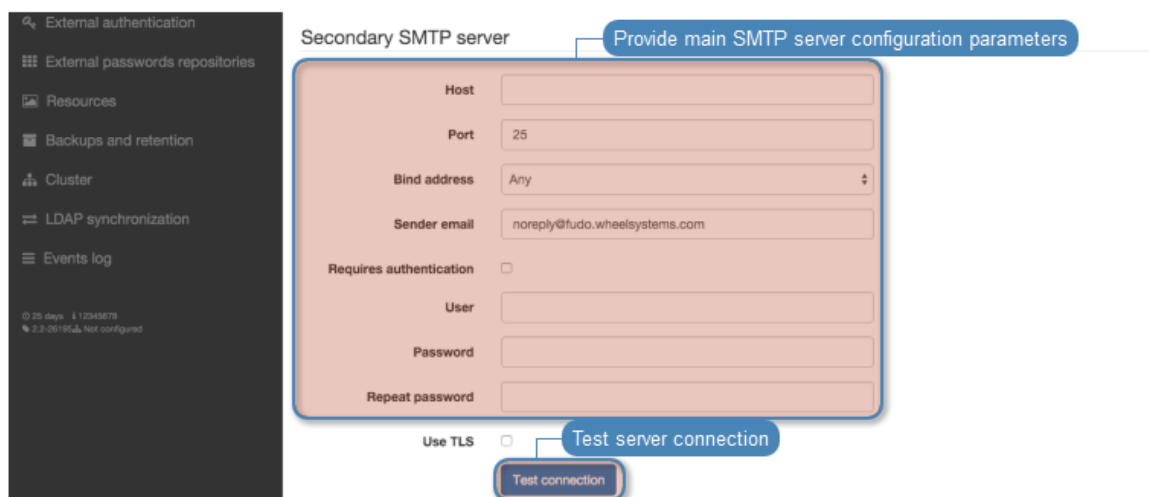
Parameter	Description
Address	SMTP server IP address.
Port	SMTP service port number.
Sender email	Email address from which the emails will be sent.
Requires authentication	Select if the SMTP server requires authentication.
User	User name for authentication on SMTP server.
Password	User password for authentication on SMTP server.
Use secure connection (<i>TLS</i>)	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 timestamping

A trusted timestamp makes recorded session a more convincing evidence in court.

Note: Trusted timestamping feature requires signing a contract with an institution providing timestamping services.

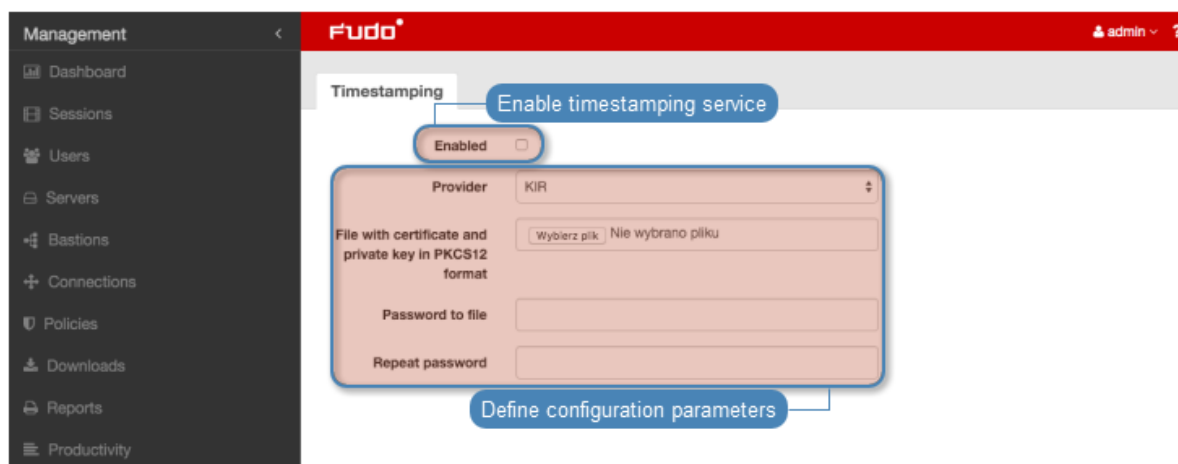
Enabling and configuring trusted timestamping

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 timestamping services.
4. Provide the certificate and the private key of the timestamping service.

Note: You should receive these information from your timestamping service provider.

5. Click *Save*.



Related topics:

- *Security measures*

15.5 External authentication

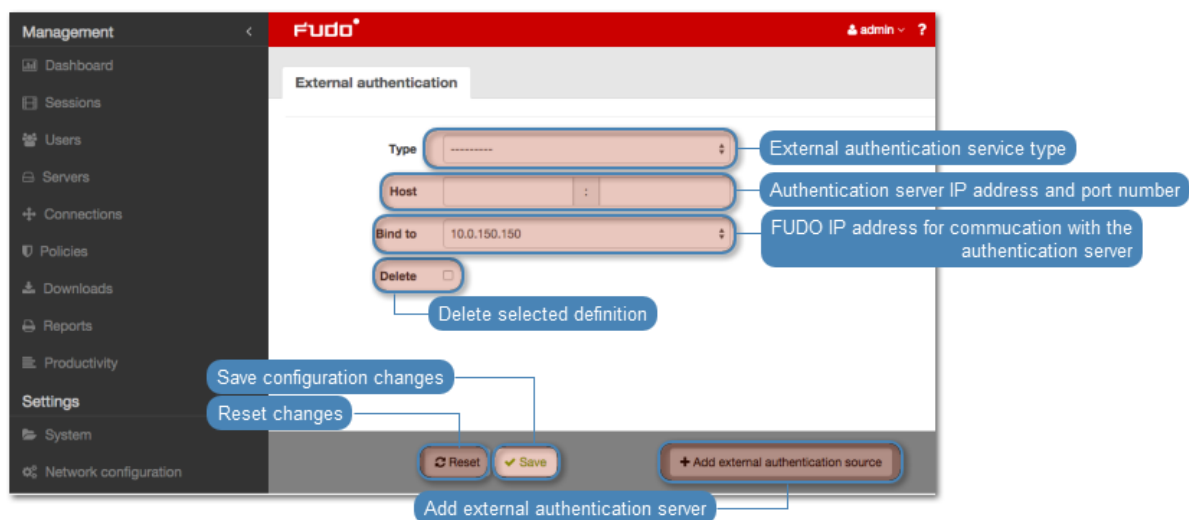
Some of the authentication methods, require defining connections to external authentication servers. These are:

- *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 give 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 give 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 give 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 give 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*.

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 passwords 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*.

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 passwords server's API.
6. Define authentication 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.
9. 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 passwords 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.
9. 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:

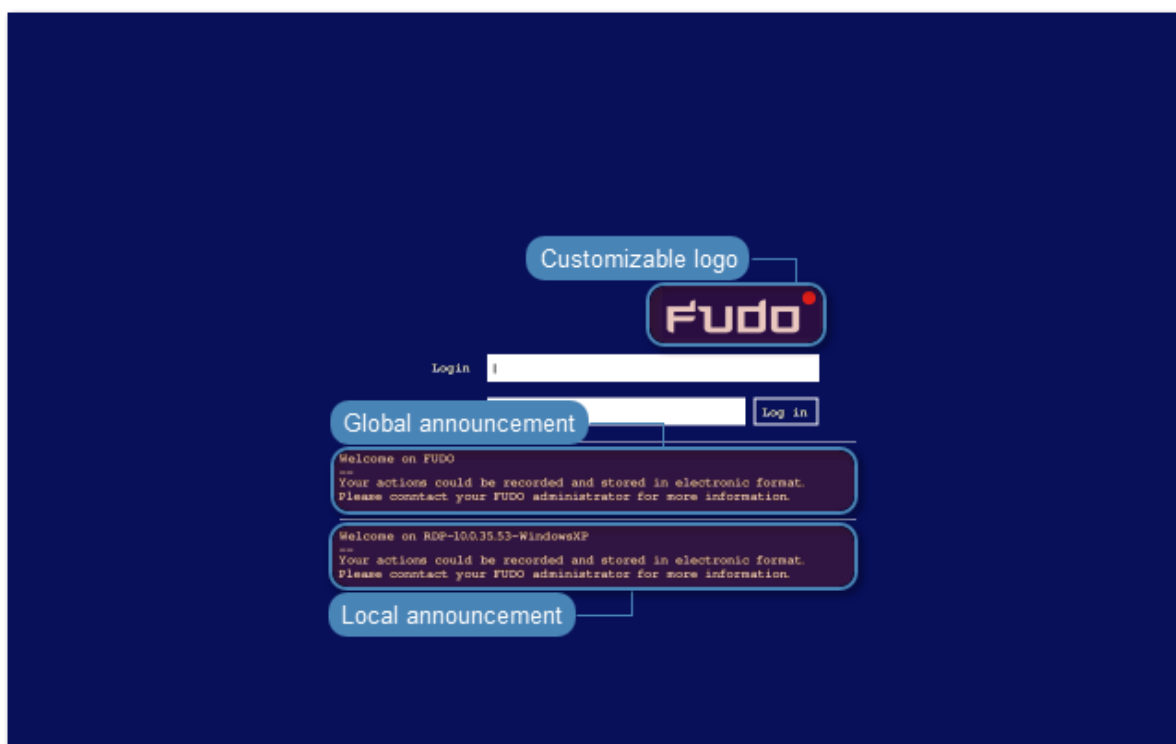
- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

15.7 Resources

Wheel Fudo PAM enables customizing RDP and VNC login screen.



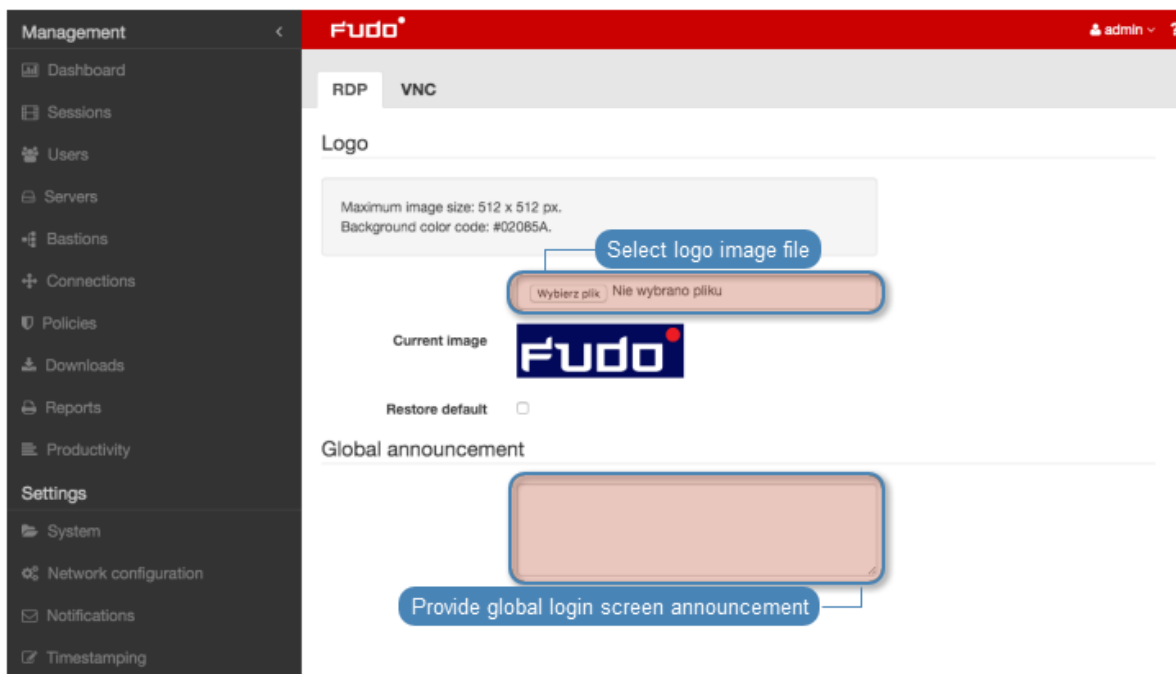
Changing logo

1. Select *Settings > Resources*.
2. Select the *RDP* or the *VNC* tab.

3. 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* or *VNC* tab.
3. 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* or *VNC* tab.
3. Enter desired message in the *Global announcement* section.
4. Click *Save*.

Related topics:

- *Quickstart - RDP*

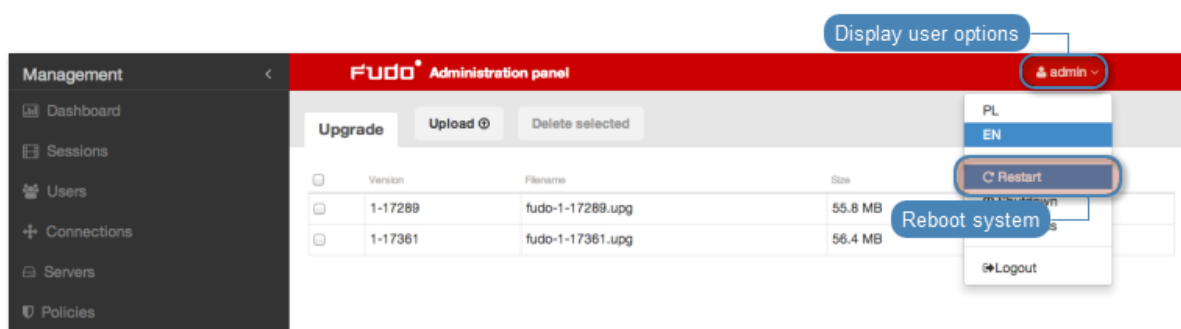
15.8 System version restore

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.

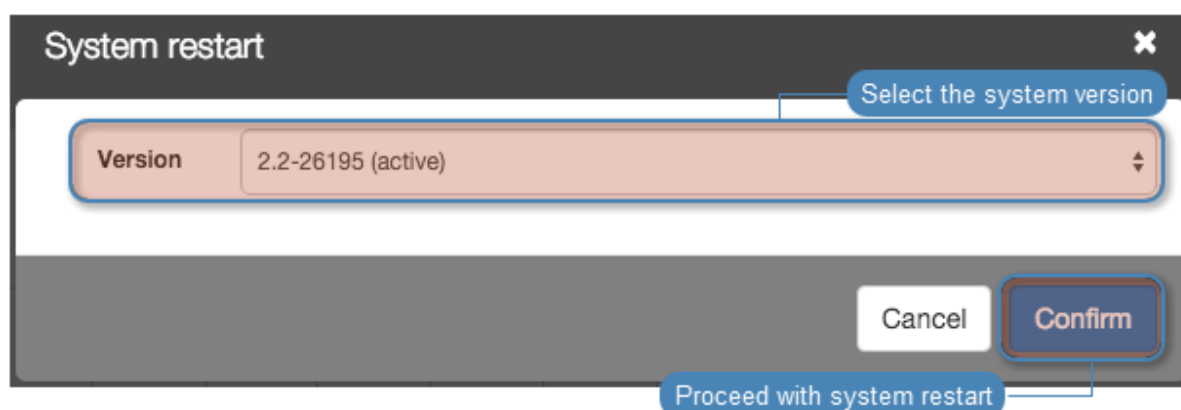
To restore the system to the previous revision, proceed as follows.

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*

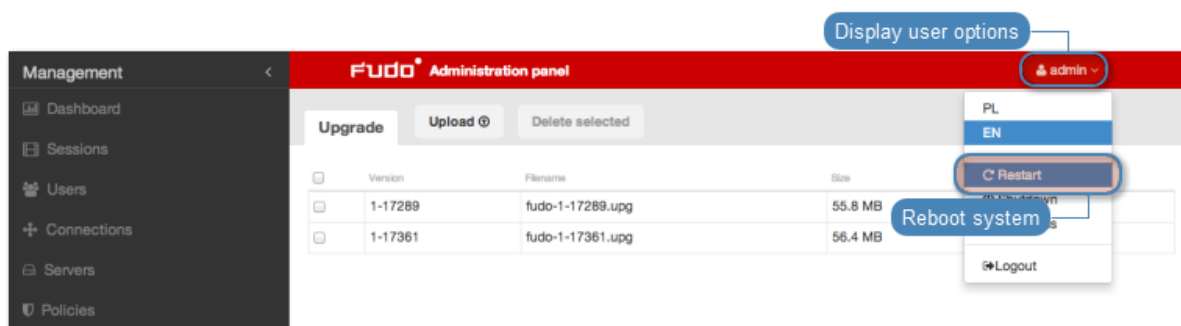
- *System update*

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. Click *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 Wheel Fudo PAM specific SNMP extensions

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, Counter32, enterprises FROM SNMPv2-
↪SMI;

wheel MODULE-IDENTITY
    LAST-UPDATED "201702140000Z"    -- 14 February 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      "201702140000Z"
    DESCRIPTION
        "First draft"
    ::= { enterprises 24410 }

products OBJECT IDENTIFIER ::= { wheel 1 }

fudo OBJECT IDENTIFIER ::= { products 1 }

sessionTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SessionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The table of active sessions on Fudo."
    ::= { fudo 1 }
```

(continues on next page)

(continued from previous page)

```
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
    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.

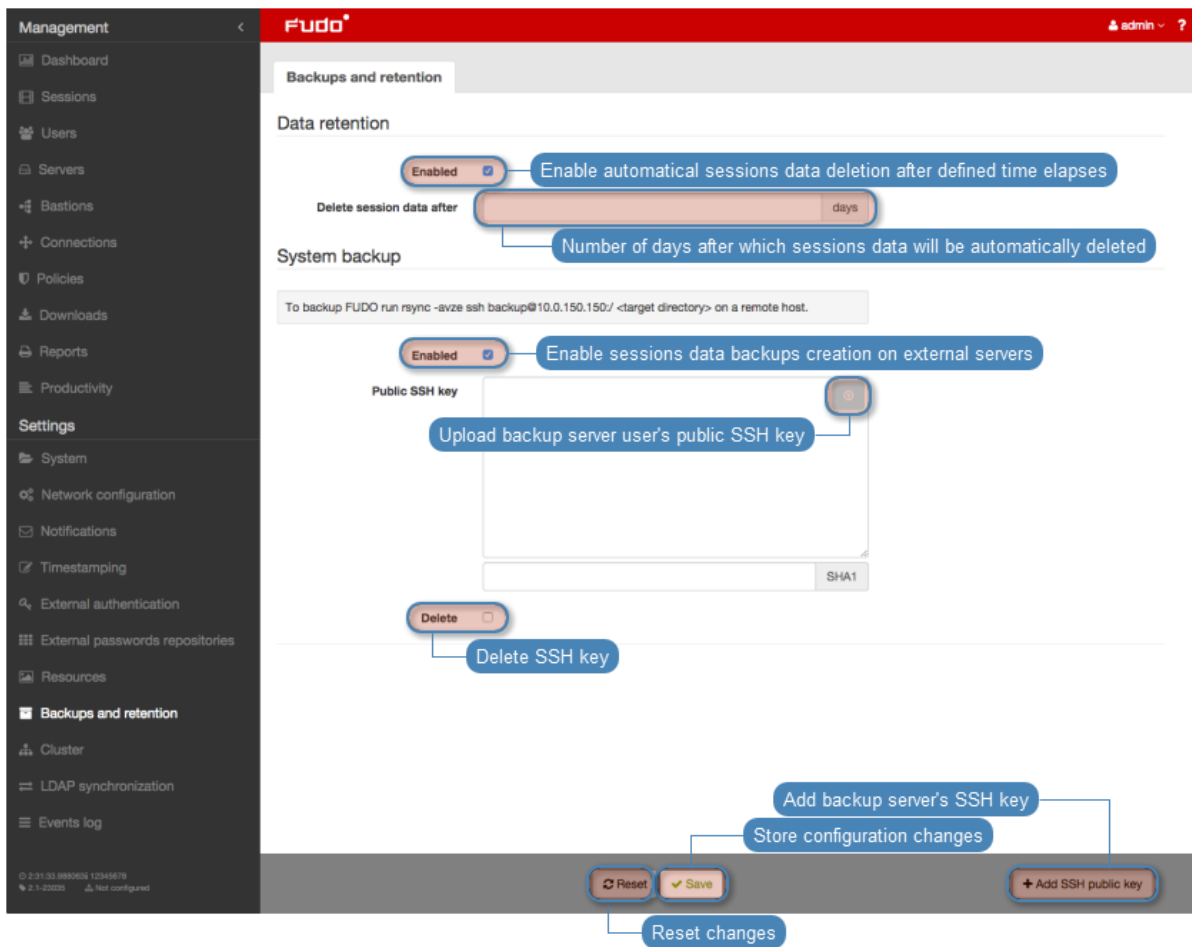
Automated data backup requires configuring `rsync` service on a remote server and granting access rights to data stored on Wheel Fudo PAM by uploading to Wheel Fudo PAM server's public SSH key.

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.

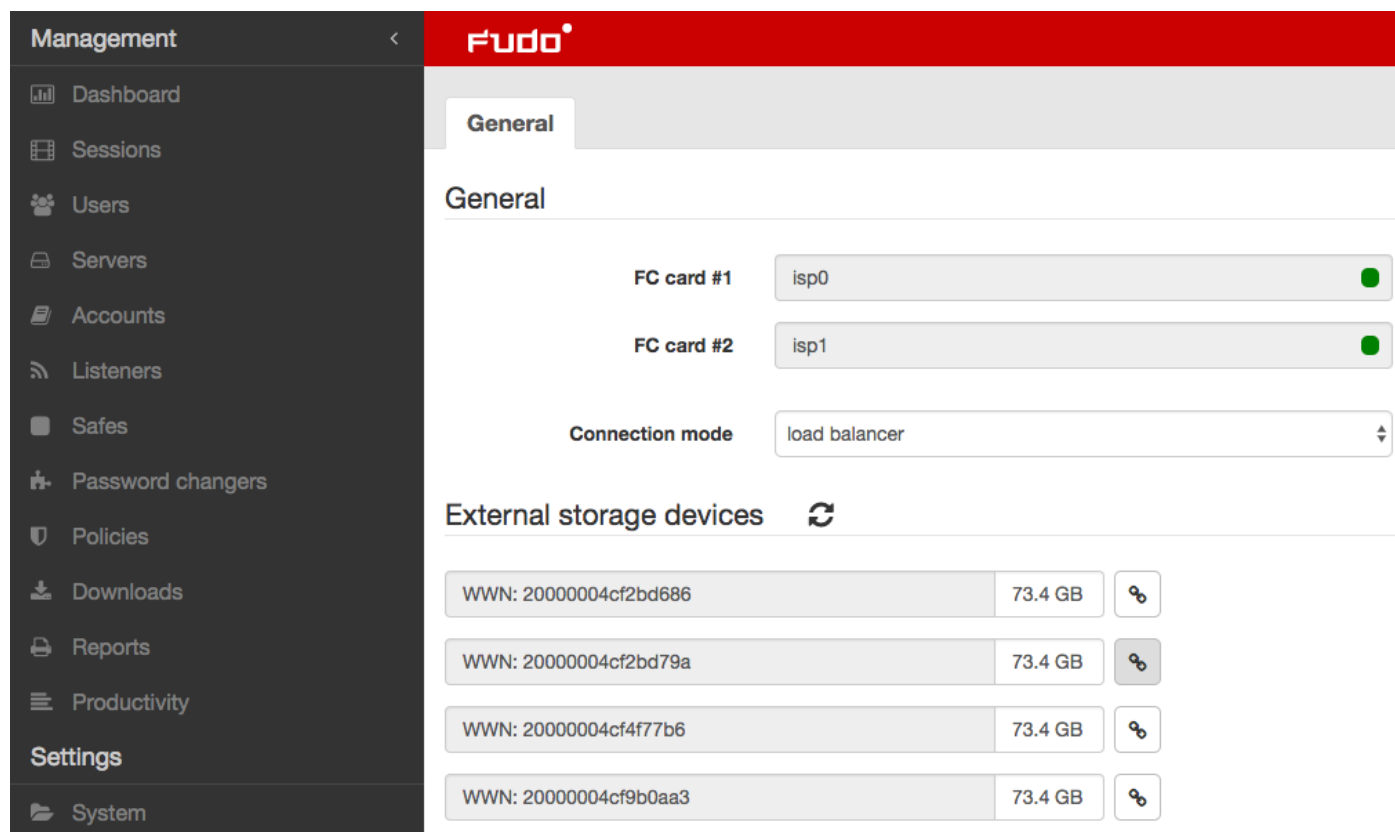
-  - both fiber channel cards are operational.
-  - external storage volume is degraded - one of the fiber channel card is down.
-  - both fiber channel cards are down.

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*.



The screenshot shows the Fudo management interface. On the left is a dark sidebar with a 'Management' menu containing items like Dashboard, Sessions, Users, Servers, Accounts, Listeners, Safes, Password changers, Policies, Downloads, Reports, Productivity, and Settings. The main content area has a red header with the 'FUDO' logo and a 'General' tab selected. Under the 'General' section, there are three configuration items: 'FC card #1' set to 'isp0' with a green status indicator, 'FC card #2' set to 'isp1' with a green status indicator, and 'Connection mode' set to 'load balancer'. Below this is the 'External storage devices' section, which has a refresh icon and a table of four storage devices. Each device entry shows its WWN, a 73.4 GB capacity, and a refresh icon.

WWN	Capacity	Action
20000004cf2bd686	73.4 GB	
20000004cf2bd79a	73.4 GB	
20000004cf4f77b6	73.4 GB	
20000004cf9b0aa3	73.4 GB	

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*.

The screenshot displays the 'General' configuration page for a WWN object. The left sidebar contains a 'Management' menu with items like Dashboard, Sessions, Users, Servers, Accounts, Safes, Listeners, Password changers, Policies, Downloads, Reports, Productivity, and a 'Settings' section with a 'System' item. The main content area shows the 'General' settings for the WWN object. It includes two 'FC card' fields, both containing the value '12345678', and a 'Connection mode' dropdown set to 'failover'. Below this, the WWN ID is displayed as '20000004cf2bd686'. A warning message is shown in a light gray box: 'The mounted resource has been resized to 11 GB, click Expand to enlarge the volume. Note that after expanding the volume it cannot be down-sized.' A 'Volume usage' bar indicates '2GB in use' and '8GB free'. An 'Expand' button is located at the bottom right of the settings area.

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.

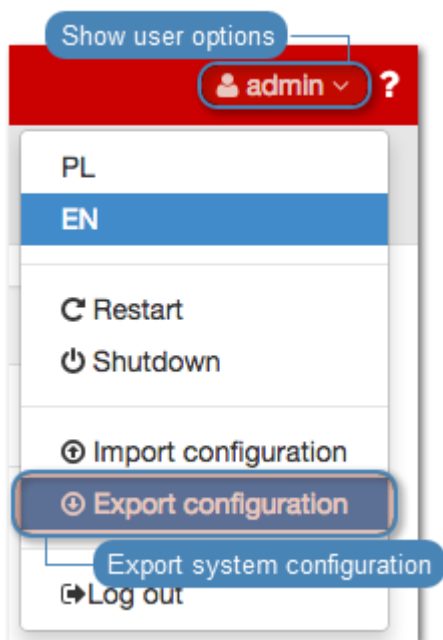
Warning: Exported configuration data contains confidential information.

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.

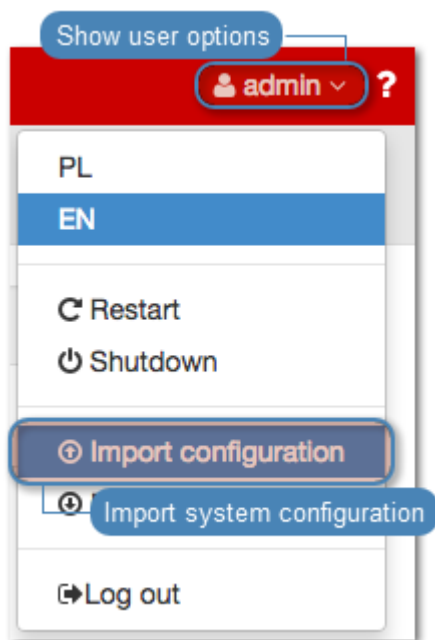


15.13.2 Importing system configuration

Warning: 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.

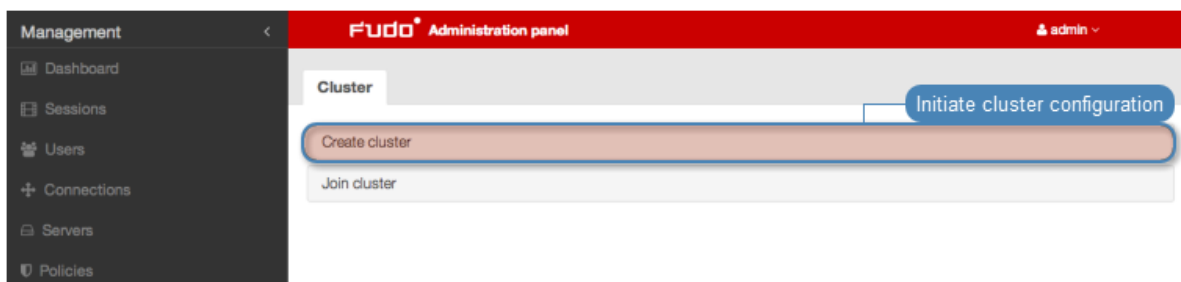
Warning: Cluster configuration does not facilitate data backup. If session data is deleted on one of the cluster nodes, it is also deleted from other nodes.

15.14.1 Initiating cluster

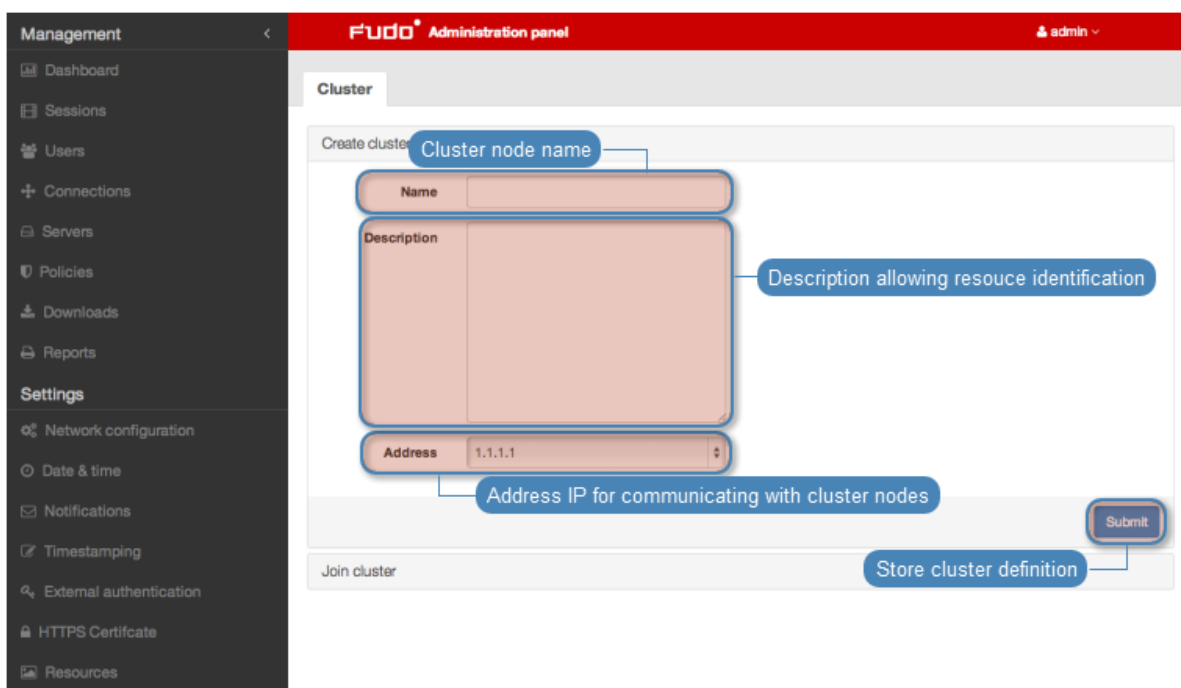
Warning: In cluster configuration all cluster nodes must have *NTP server configured*.

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*
- *Forcing full data synchronization*
- *Security: Cluster configuration*
- *Redundancy groups*
- *Cluster configuration*

15.14.2 Adding cluster nodes

Warning:

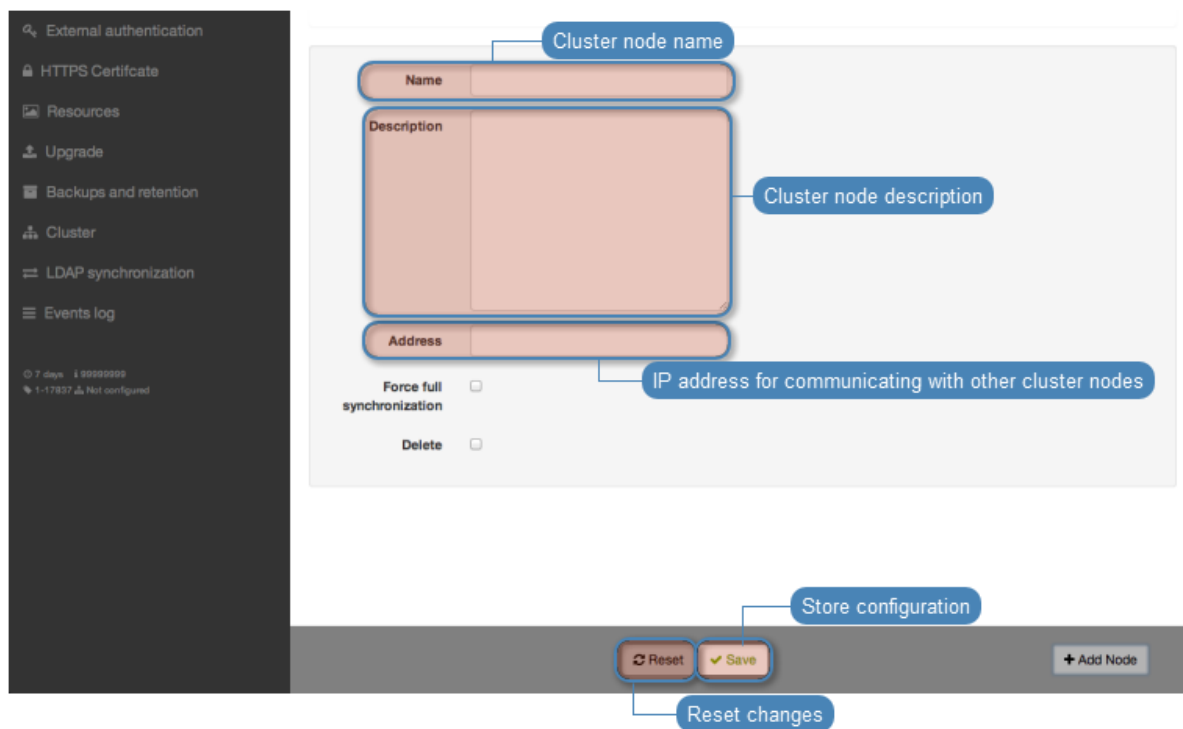
- Session and configuration data (servers, users, safes, accounts, listeners, external authentication servers) of the joining node are deleted and initiated with data replicated from the cluster.
- Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster 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.

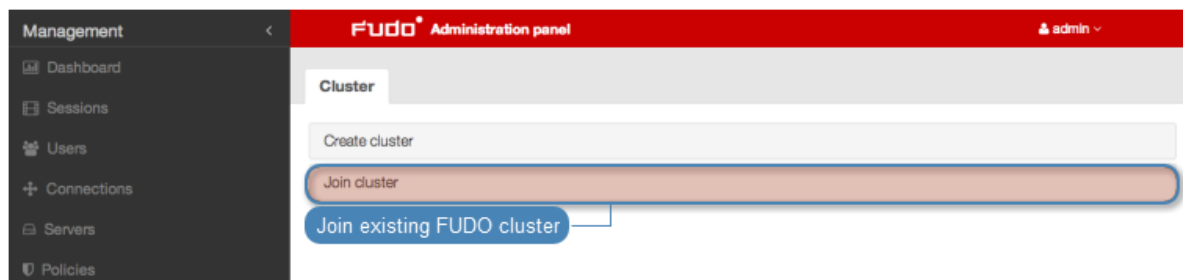
1. Log in to the Wheel Fudo PAM administration panel where the cluster has been *initiated*.
2. Select *Settings > Cluster*.
3. Click *Add node* to display new node configuration parameters.

4. Provide node's name and optional description.
5. Provide node's IP address.

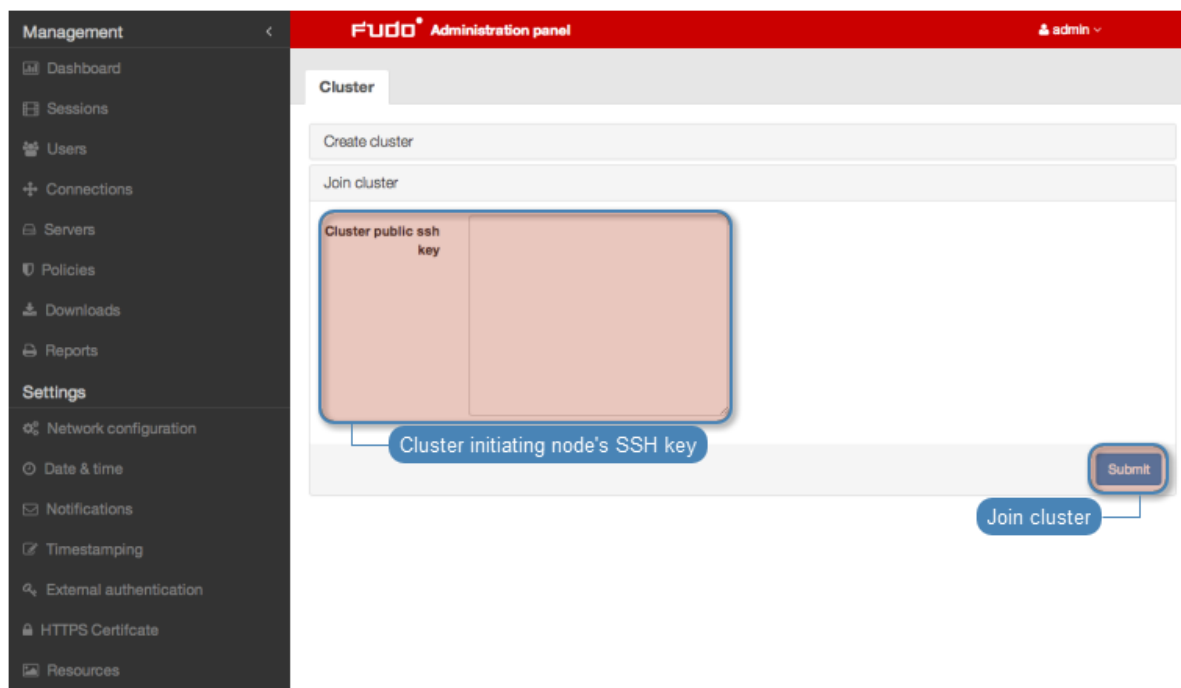
Note: Management option has to be enabled on given network interface. Refer to *Network settings: Network interfaces configuration* for details on configuring network interfaces.



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*.



Related topics:

- *Editing cluster nodes*
- *Deleting cluster nodes*
- *Forcing full data synchronization*
- *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:

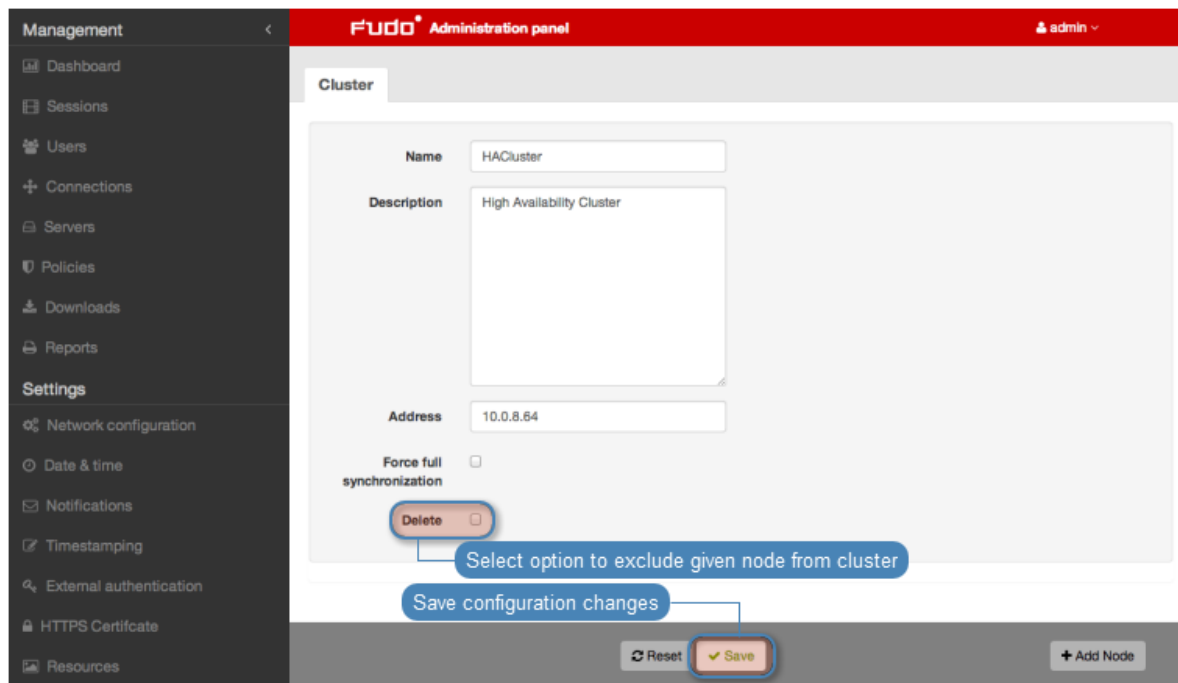
- *Adding cluster nodes*
- *Deleting cluster nodes*
- *Forcing full data synchronization*
- *Security: Cluster configuration*

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*
- *Forcing full data synchronization*
- *Security: Cluster configuration*

15.14.5 Forcing full data synchronization

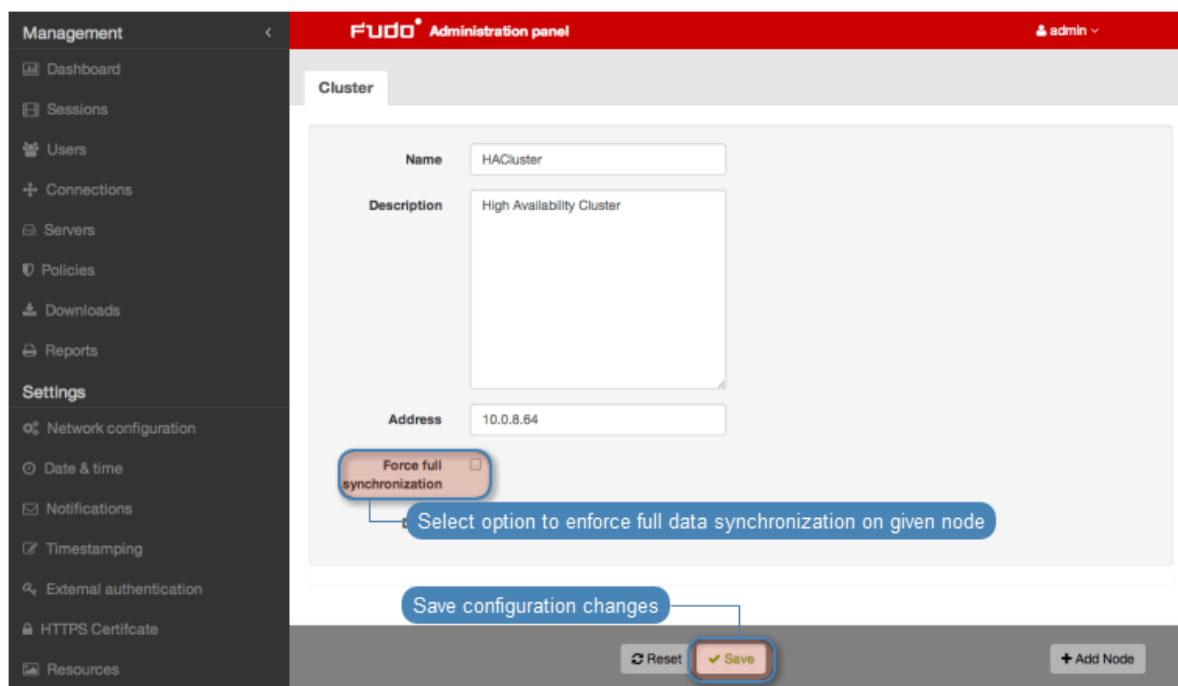
Warning: Before enforcing full data synchronization contact Wheel Systems' technical support.

In case data stored on a certain cluster node gets desynchronized, it is necessary to perform forced data synchronization on given node.

To force data synchronization on a certain node, proceed as follows.

1. Log in to Wheel Fudo PAM administration panel on a node other than the one which requires synchronization.
2. Select *Settings > Cluster*.
3. Find and select node which requires data synchronization.

4. Select *Force full synchronization* option and click *Submit*.



Related topics:

- [Adding cluster nodes](#)
- [Editing cluster nodes](#)
- [Deleting cluster nodes](#)
- [Security: Cluster configuration](#)

15.14.6 Redundancy groups

Redundancy groups aggregate IP addresses assigned to network interfaces enabling implementing static load balancing scenarios while fully preserving high availability features.

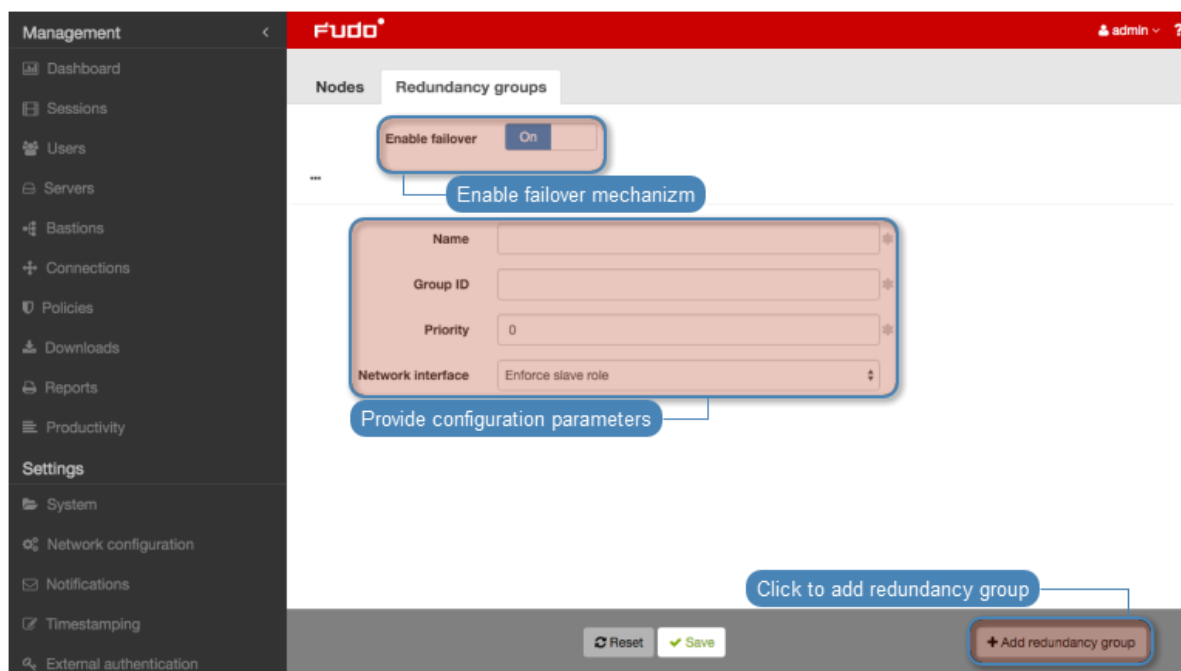
Note: Redundancy groups configuration options are available only after initializing the cluster.



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 <i>master</i> 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*.

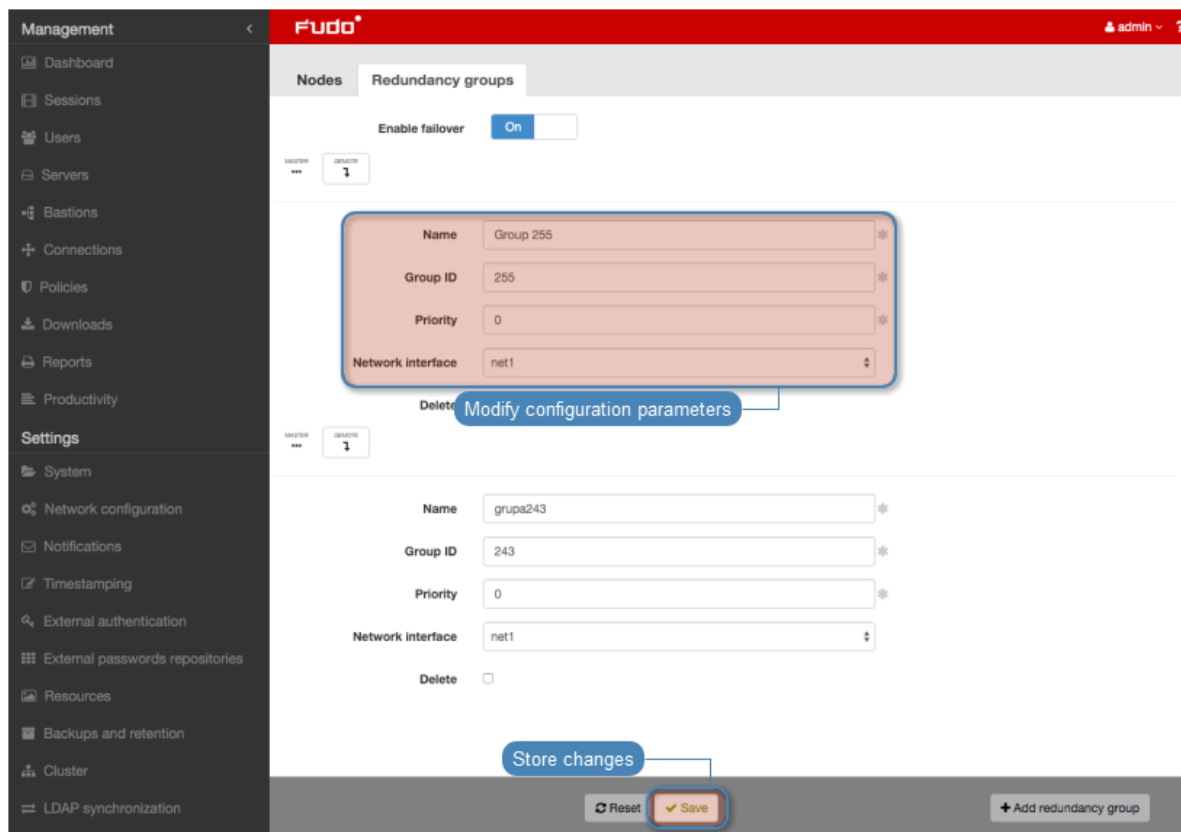


Note: Cluster IP address DNS must be defined on every cluster node.

Editing redundancy groups

To modify a redundancy group, proceed as follows.

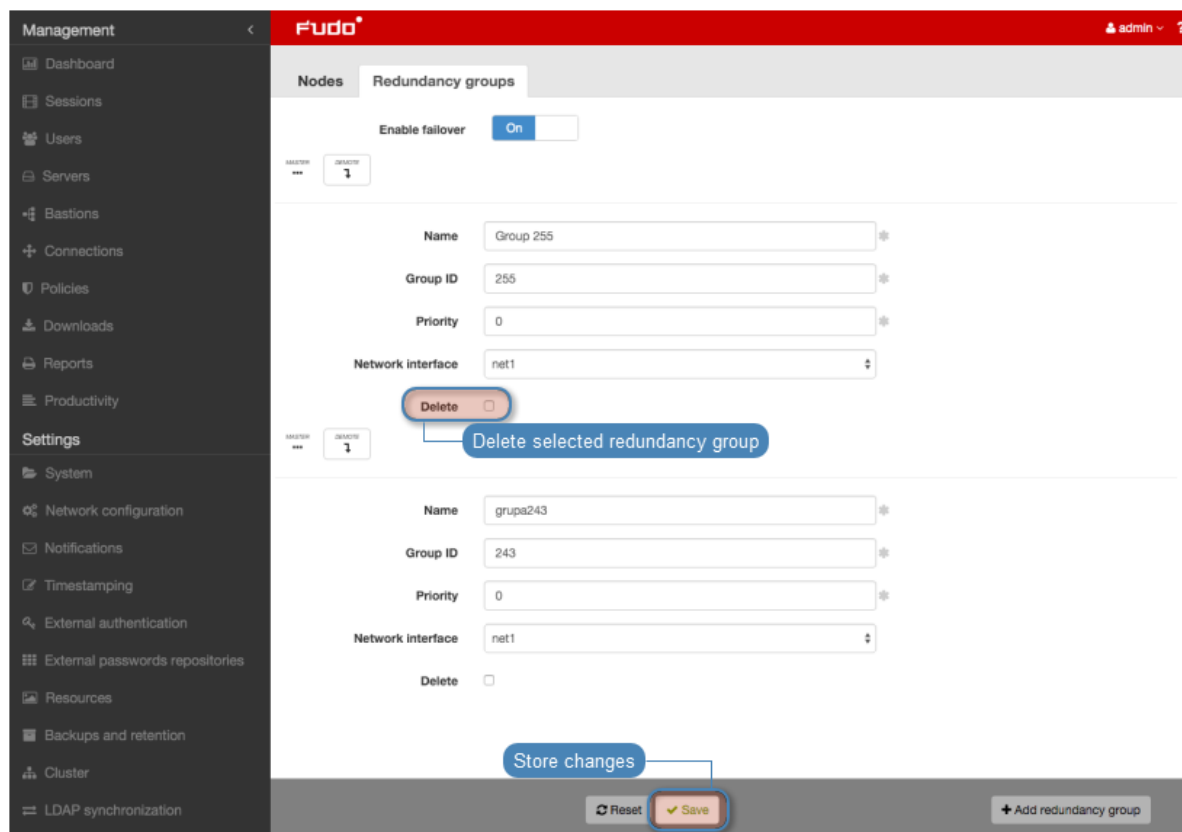
1. Select *Settings > Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Find and edit desired redundancy group definition.
4. Click *Save*.



Deleting a redundancy group

To delete a redundancy group, proceed as follows.

1. Select *Settings > Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Select *Delete* next to the desired redundancy group.
4. Click *Save*.

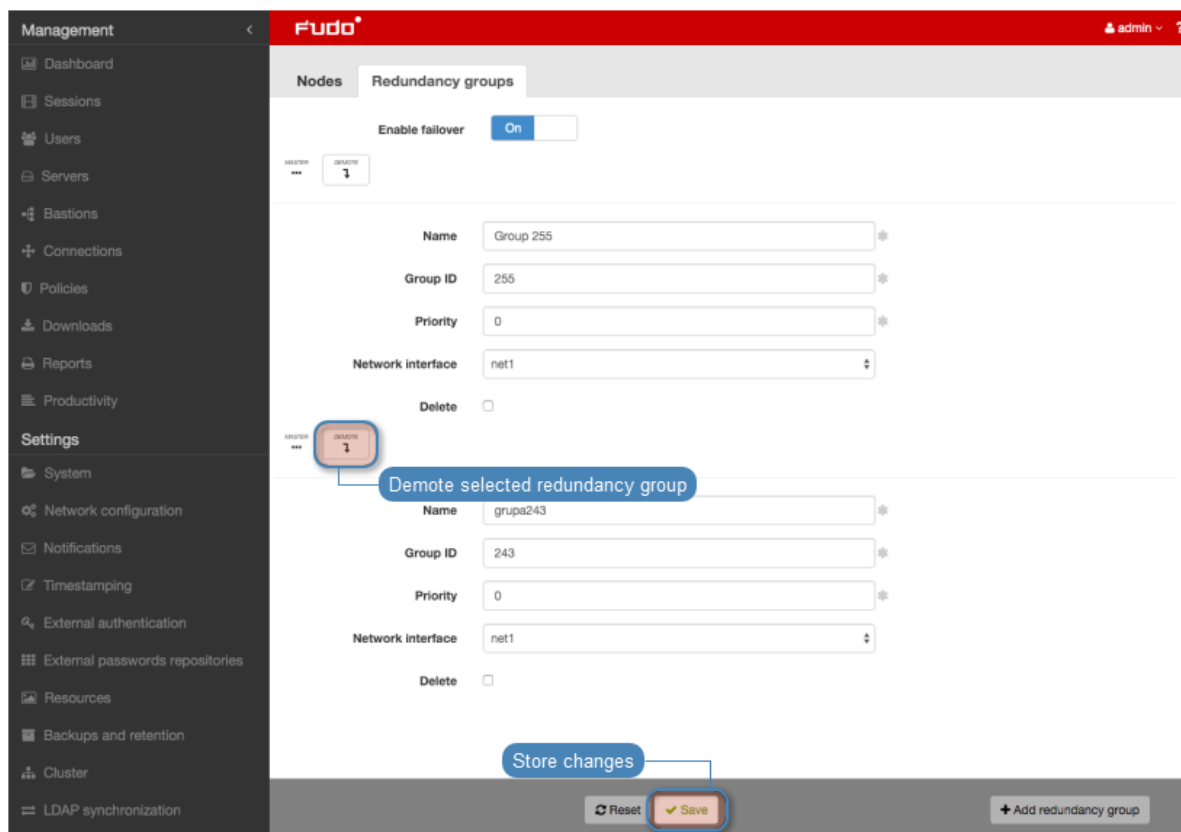


Demoting a redundancy group

Note: Demoting redundancy group transfers the master role for given group to another cluster node. The master role is assumed by one of the remaining nodes, on which the given redundancy group has the highest priority defined.

To demote a redundancy group, proceed as follows.

1. Select *Settings > Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Click *Demote* next to the desired redundancy group.
4. Click *Confirm*.



Note: If after demoting a redundancy group no other node assumes the master role for the given group, it will be reassigned to the node which previously had this role.

Enforcing a slave role

Note: Enforcing a permanent slave role on a redundancy group ensures that the given node will not assume master role on given redundancy group despite the state that other nodes are in. It's recommended for directing all traffic to other nodes before performing maintenance tasks on given cluster node.

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.

The screenshot shows the 'Events log' page in the Wheel Fudo PAM 3.5 interface. The page has a sidebar on the left with 'Management' and 'Settings' sections. The 'Events log' page displays a table of log entries. The table has columns for Timestamp, Log level, Component, and Message. The log entries show various system events, including user authentication, configuration changes, and network interface settings. Callouts highlight the 'Add filter' button, 'Export logs' button, 'Configure syslog' button, and the 'External syslog servers configuration' link.

Timestamp	Log level	Component	Message
2014-12-22 14:08:25	Info	fudoauth	User admin authenticated using password logged in from IP address: 10.0.1.35.
2014-12-22 14:07:29	Info	fudoauth	User admin authenticated using password logged in from IP address: 10.0.1.36.
2014-12-22 12:59:39	Info	fudoauth	User admin authenticated using password logged in from IP address: 10.0.1.36.
2014-12-22 12:06:10	Info	gui	User admin created connection RDP (771109632230817793).
2014-12-22 12:05:45	Info	fudod	Reloading configuration.
2014-12-22 12:05:45	Info	gui	User admin created server WINDOWS 2000 (771109632230817793).
2014-12-22 12:02:20	Info	gui	User admin created user "tomek" (771109632230817794).
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'granted_to_users' from '[77110963223...
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'language' from 'en' to 'pl'.
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'valid_to' from 'None' to '[u2015-01-21]...
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'valid_since' from 'None' to '[u2014-12-...
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'account_validity' from 'None' to '30'.
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'granted_users' from '['-SimpleLazyObjje...
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'phone' from '' to '733568993'.
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'organization' from 'None' to 'Wheel Sys...
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'full_name' from '' to 'TD'.
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'email' from '' to 'Ldwornicki@wheelsyst...
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'name' from '' to 'tomek'.
2014-12-22 12:00:59	Info	fudoauth	User admin authenticated using password logged in from IP address: 10.0.1.36.
2014-12-22 12:00:48	Info	gui	User admin changed network interfaces settings.
2014-12-22 12:00:48	Info	gui	User admin deleted address 192.168.1.1 from interface net0
2014-12-22 12:00:48	Info	fudod	Reloading configuration.
2014-12-22 11:59:51	Info	gui	User admin changed network interfaces settings.
2014-12-22 11:59:51	Info	gui	User admin added address 10.0.45.90/16 to interface net0 with enabled management and disabled cluster address
2014-12-22 11:59:51	Info	fudod	Reloading configuration.
2014-12-22 11:59:20	Info	fudoauth	User admin authenticated using password logged in from IP address: 192.168.1.150.
2014-12-22 11:59:02	Info	fudocord	Started successfully.
2014-12-22 11:58:59	Info	eventd	Started successfully.
2014-12-22 11:58:59	Info	otbrecvd	Started successfully.

External syslog servers

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: 84838853211147015) (fudo_session:
84838853211147219) (fudo_user: 84838853211147012) (fudo_connection:
84838853211147014) User user0 authenticated using password logged in from IP
address: 10.0.40.101.
```

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*.

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:

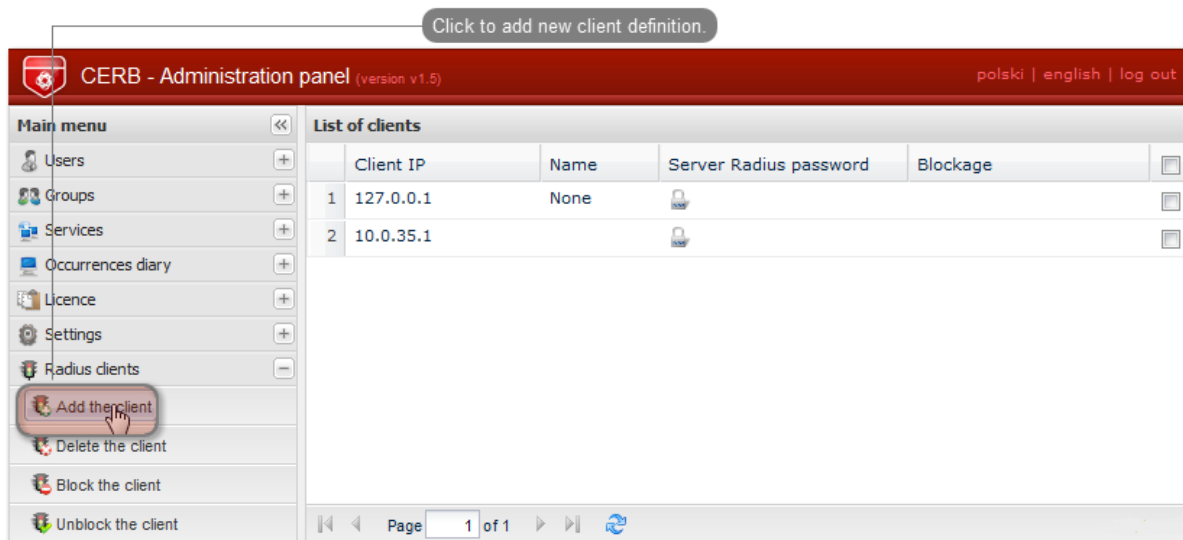
- *Security*
- *Managing servers*

15.16 Integration with CERB server

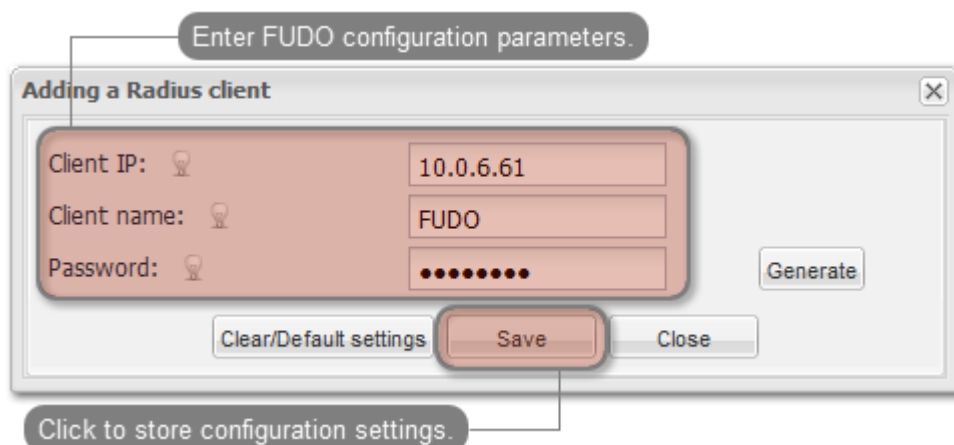
CERB is complete user authorization solution which supports a number of authorization mechanisms (i.e. mobile token, onetime passwords, etc.). The following procedure describes configuration steps required to enable Wheel Fudo PAM to verify users credentials using CERB server.

CERB server configuration

1. Adding RADIUS client.
 - Select *RADIUS clients > Add client* to add Wheel Fudo PAM as a RADIUS client.



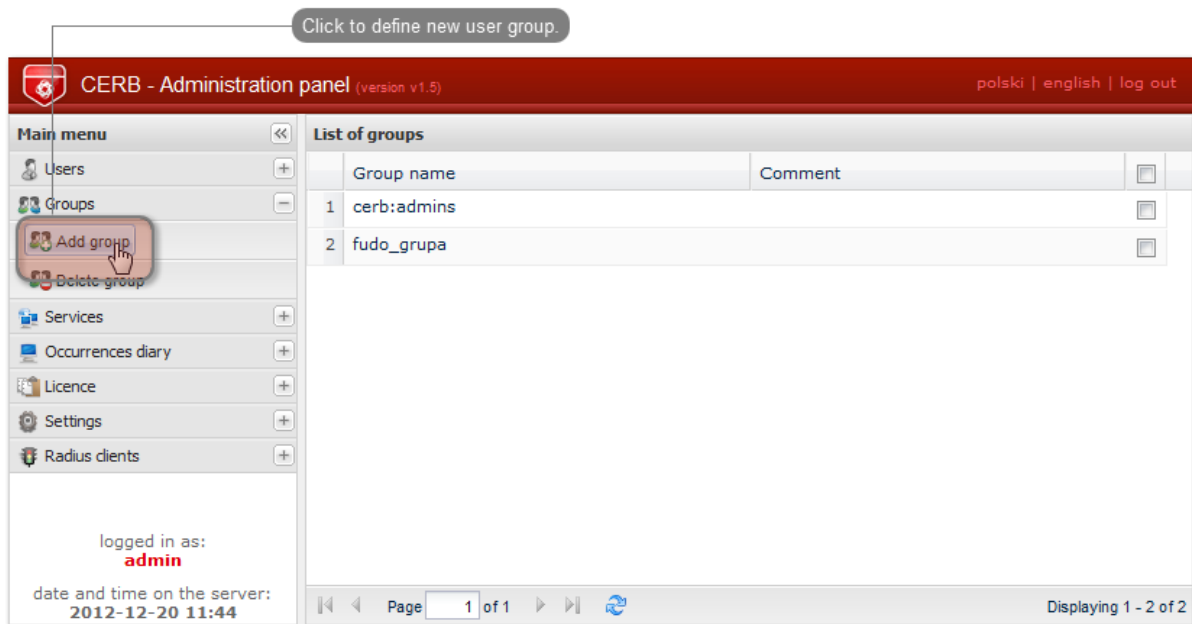
- Provide Wheel Fudo PAM IP address, client's name and password and click *Save*.



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.

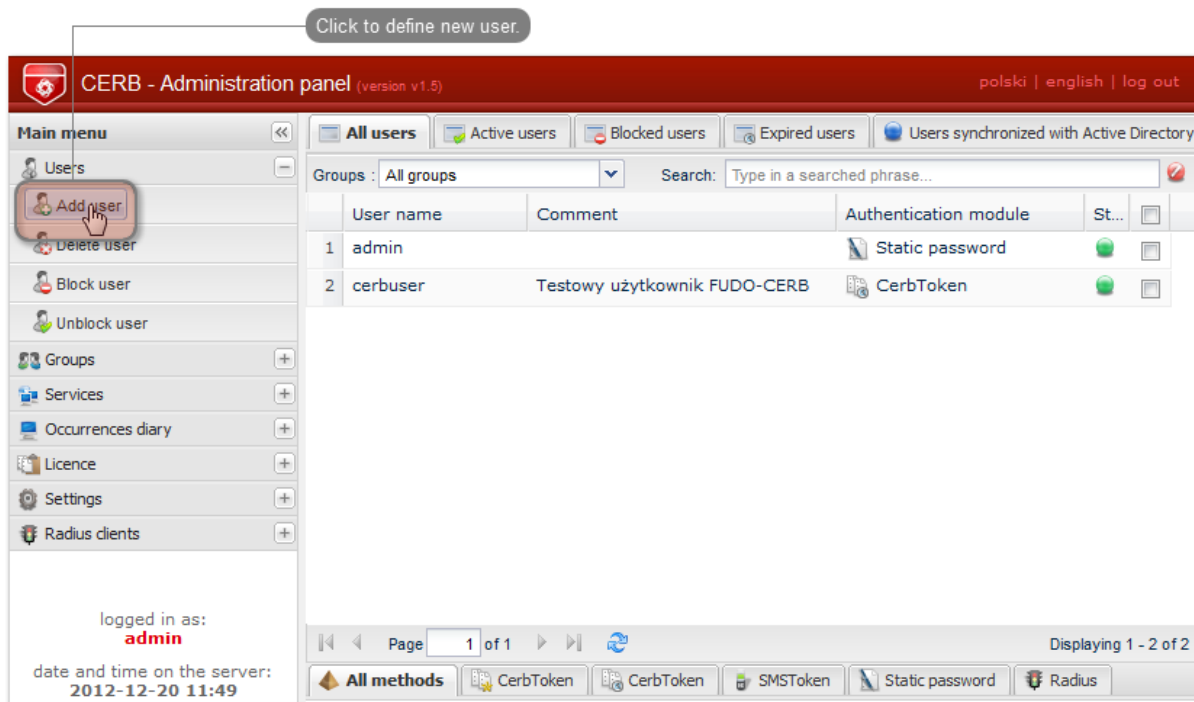


- Enter group's name (`fudo_users`) and click *Save*.

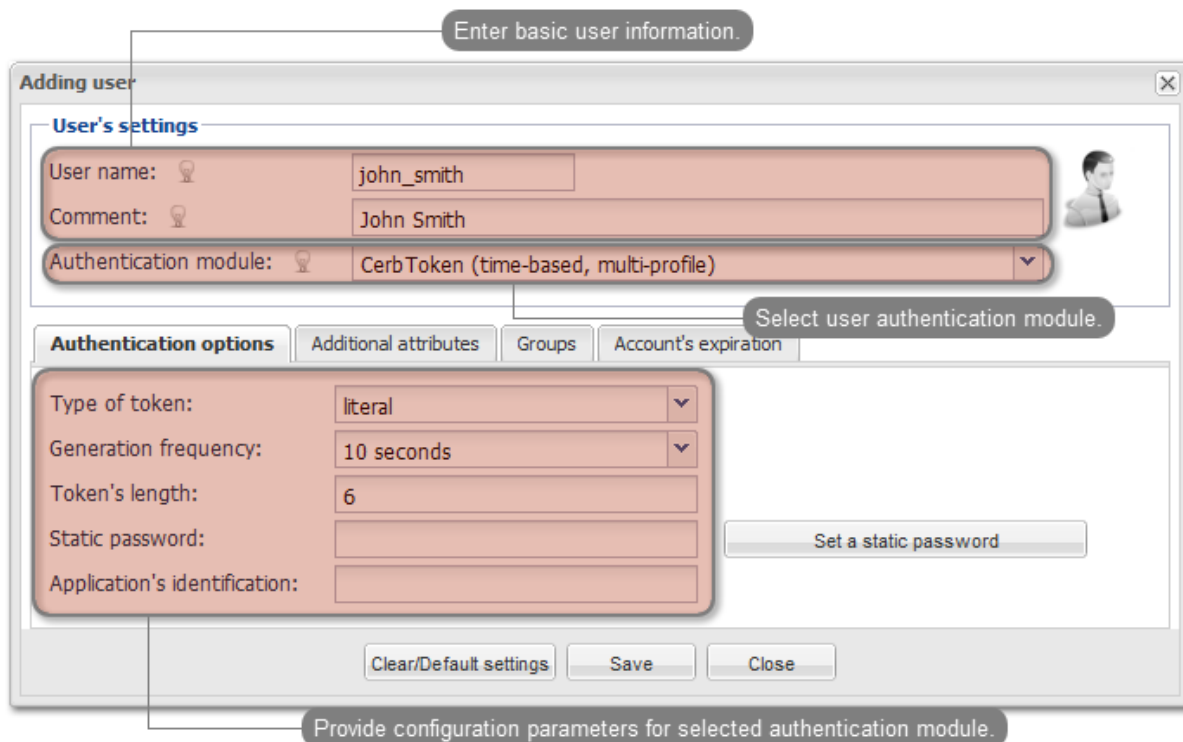


3. Adding user.

- Select *Users* > *Add user* to open new user definition window.

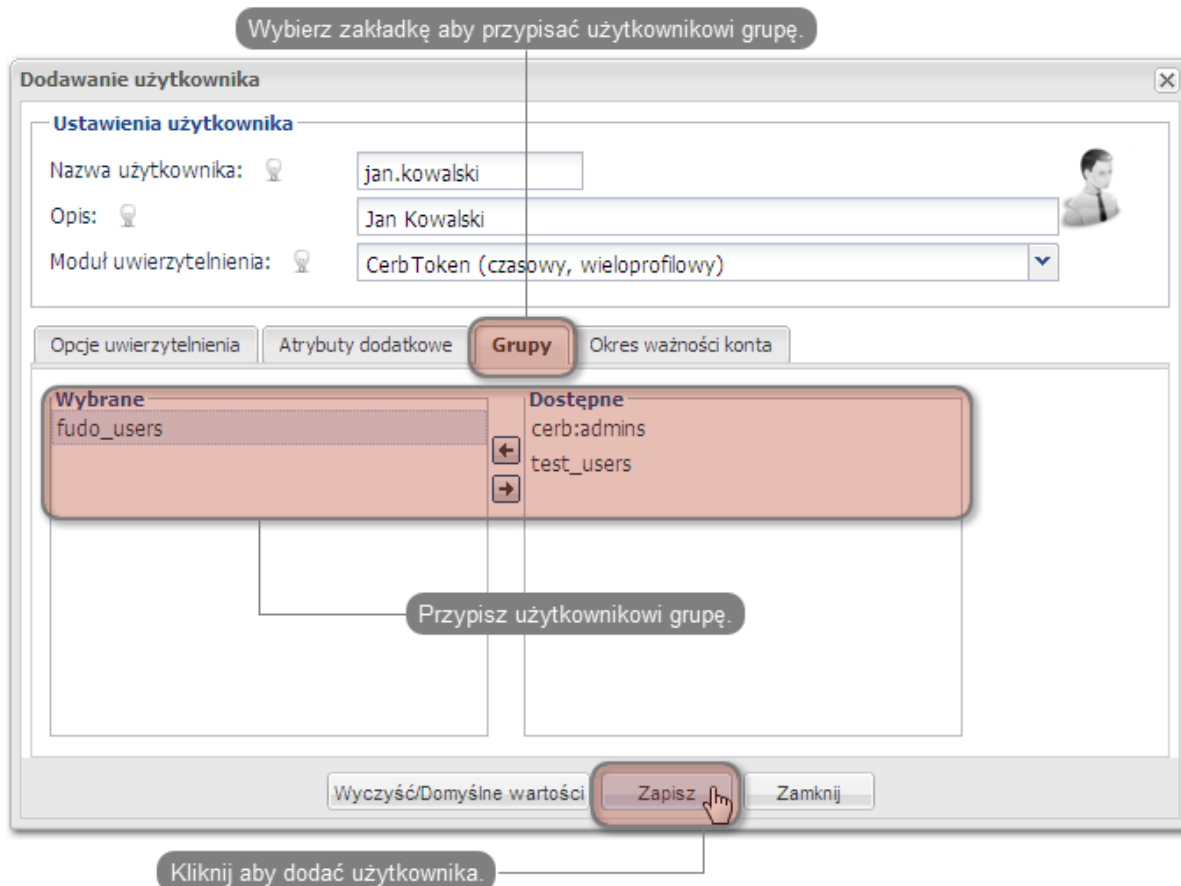


- Provide user name, description and select desired authorization module (refer to CERB server documentation form more information on authorization modules).



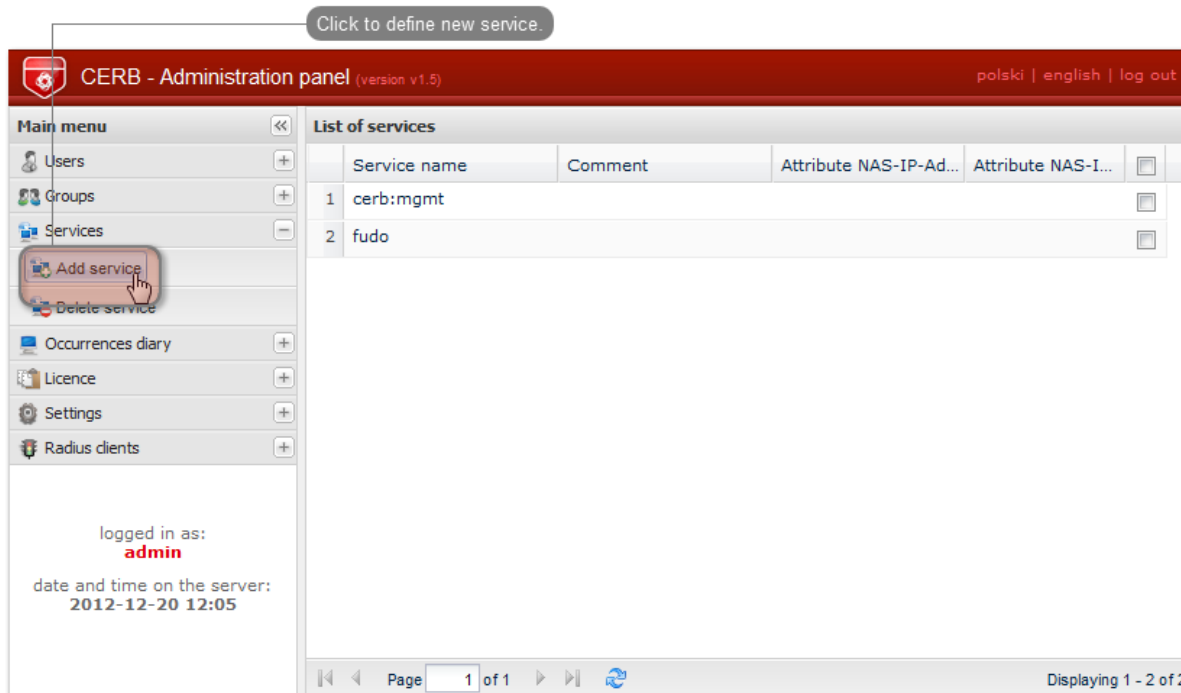
Note: Username is used to authenticate users on Wheel Fudo PAM.

- Assign user to previously created `fudo_users` group and click *Save*.



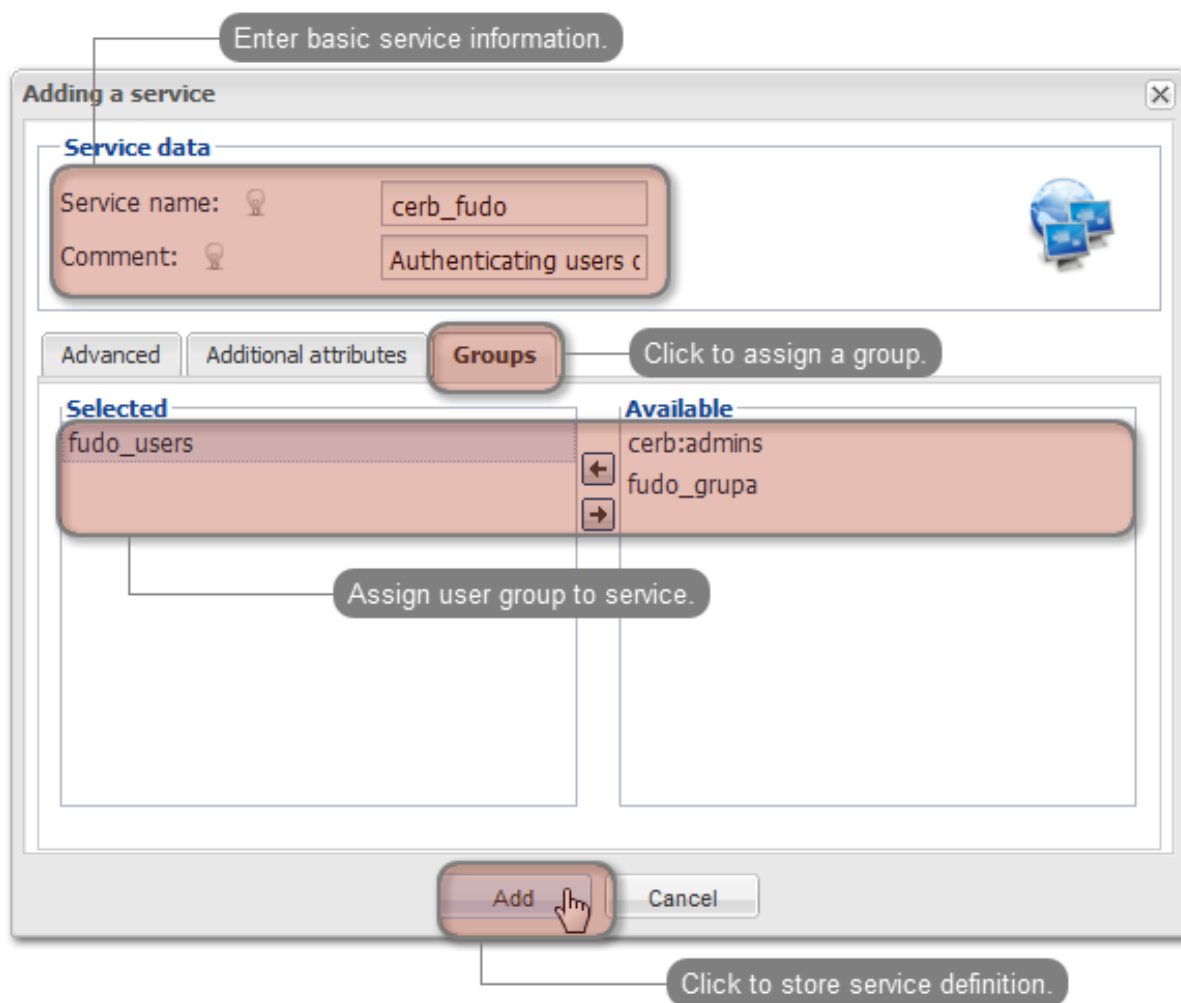
4. Configuring service.

- Select *Services* > *Add service* to open new service definition window.



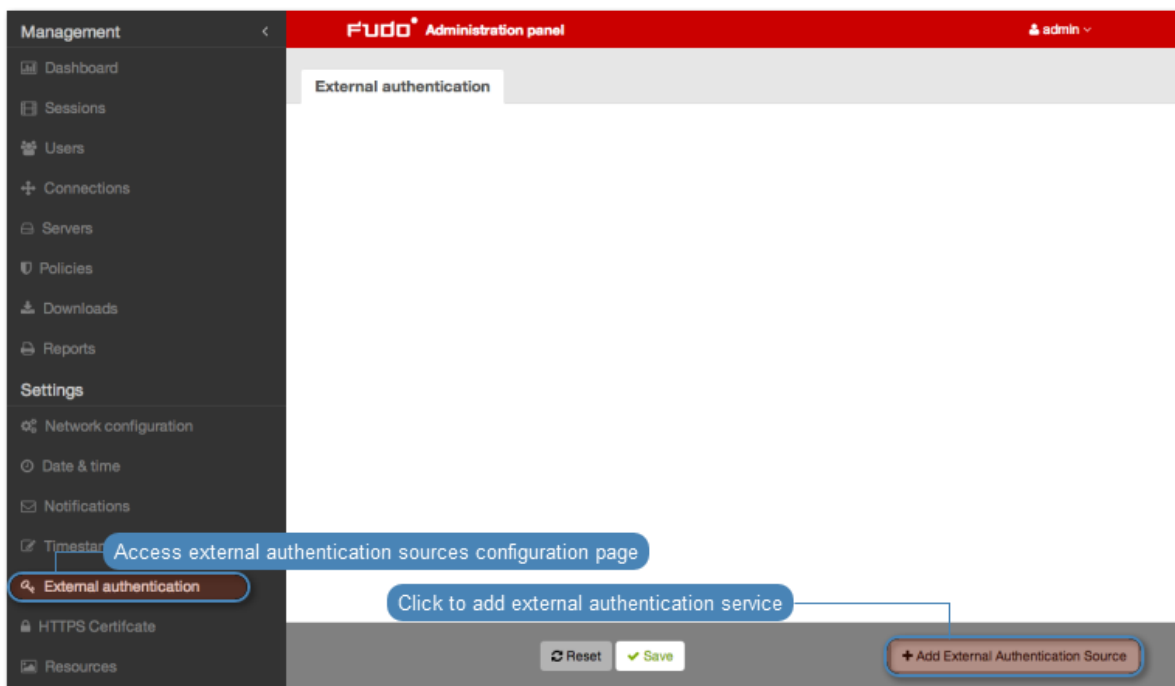
- Provide name identifying authorization service (`cerb_fudo`) and service description.

- Add fudo_users group to service and click *Add*.



Wheel Fudo PAM server configuration

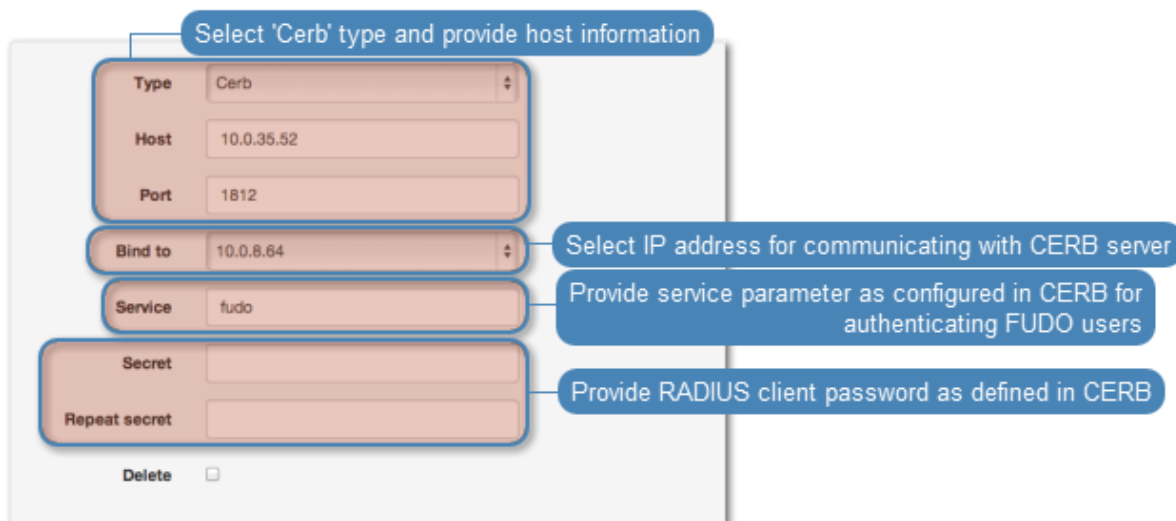
1. Adding CERB external authorization server.
 - Select *Settings > External authentication*.
 - Click *Add external authentication source* to add CERB server definition.



- Provide CERB server IP address, *secret* and service name identifying authorization service.

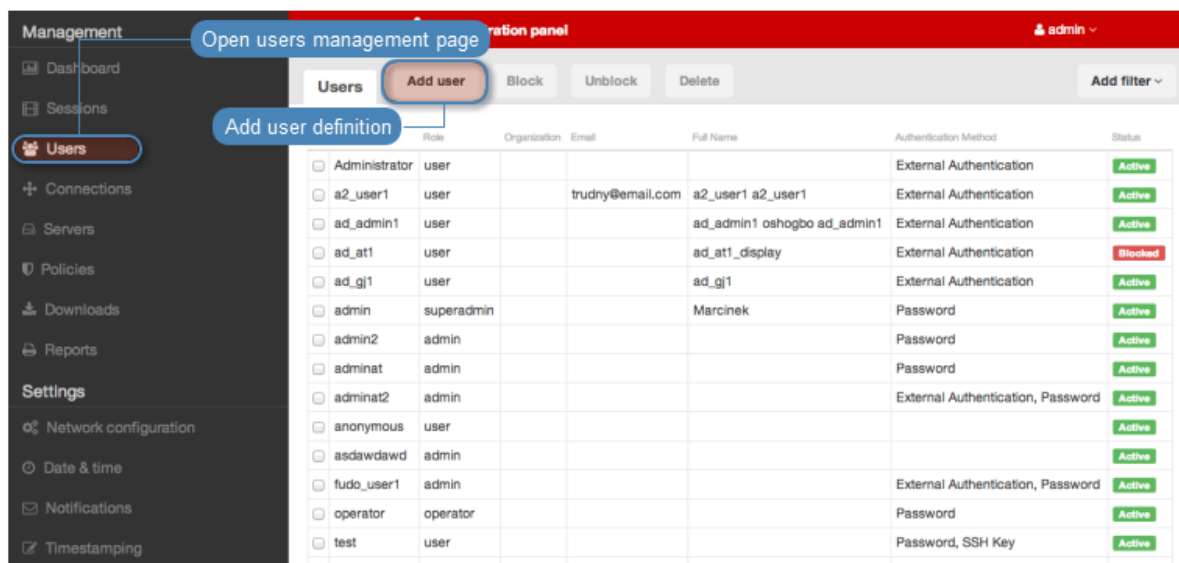
Note: Secret must match the RADIUS client password on CERB server. Service name must match the service name on CERB

- 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.

- Select CERB from the drop-down list as authorization method and select previously added authorization server.
- Click *Save*.

Create user

Provide user information

General

Username: jan.kowalski

Role: user

Synchronize with LDAP:

Blocked:

Full name: Jan Kowalski

Email: jan@kowalski.pl

Organization:

Phone:

AD Domain:

LDAP Base:

Permissions

Granted users:

Authentication

Type: External Authentication

External authentication source: Cerb 10.0.35.52 service:fudo

Type:

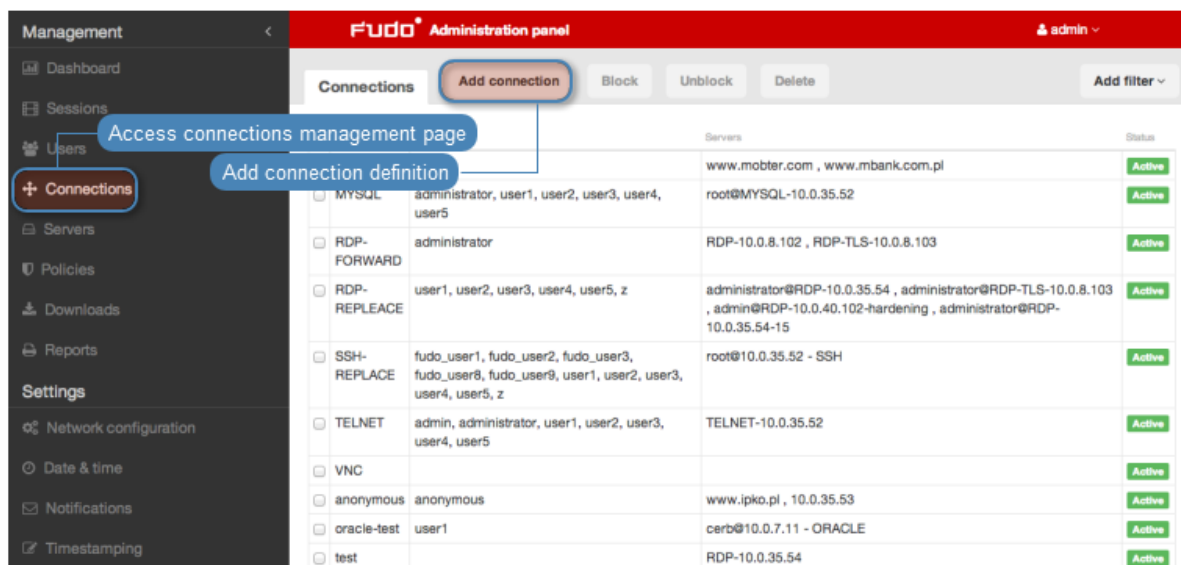
Delete:

Reset Save

Save user definition

3. Adding connection.

- Select *Management > Connections*.
- Click *+ Add*.



- Provide basic connection parameters.
- Select previously defined user.
- Select target server to enable user access within given connection.
- Select user authorization mode (*User authorization mode*).
- Click *Save*.

Create connection

General

Name: Provide connection name

Notifications: Session start Session finish Session inject open Session inject close Session policy match Select administrator notification options

Users: Assign user to connection

Retention time (in days): Define session data retention

RDP Functionality Clipboard redirection Sound redirection Device redirection
 Dynamic Virtual Channels Audio input redirection Multimedia redirection

SSH Functionality Sessions Port forwarding Terminal Environment X11 SSH Agent forwarding
 Shell SCP

VNC Functionality Client Cut Text Server Cut Text

Permissions

Granted users: Search

Servers

Server: Select server and choose user authentication mode

Policy:

Replace user?:

Replace secret?:

Save connection definition

15.17 System maintenance

The following section contains descriptions of maintenance procedures.

15.17.1 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.

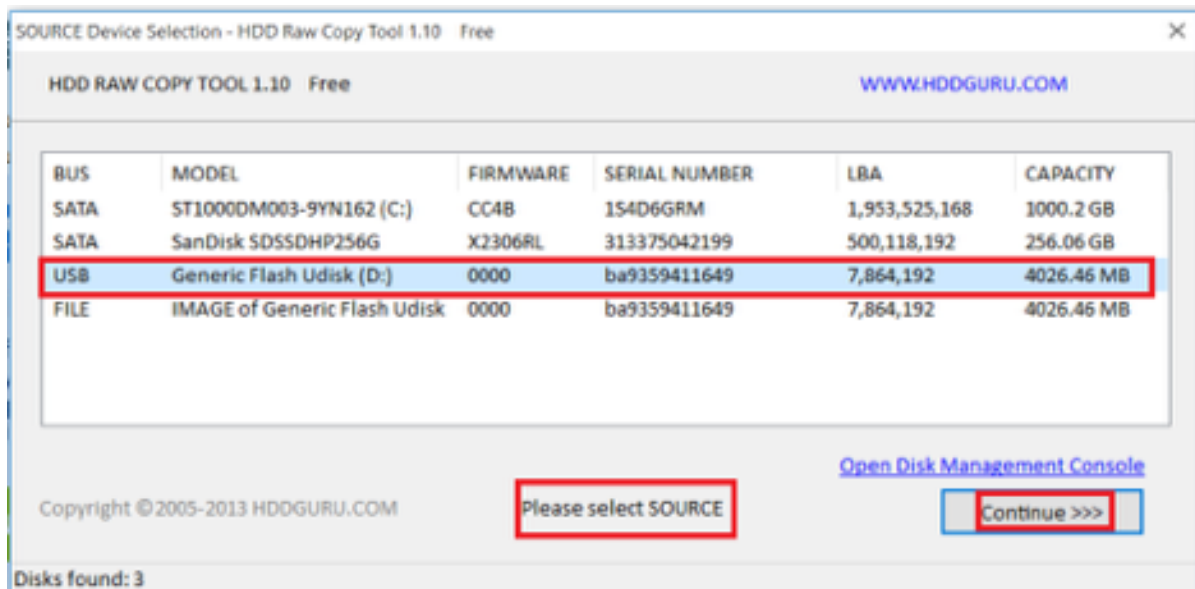
Microsoft Windows

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.

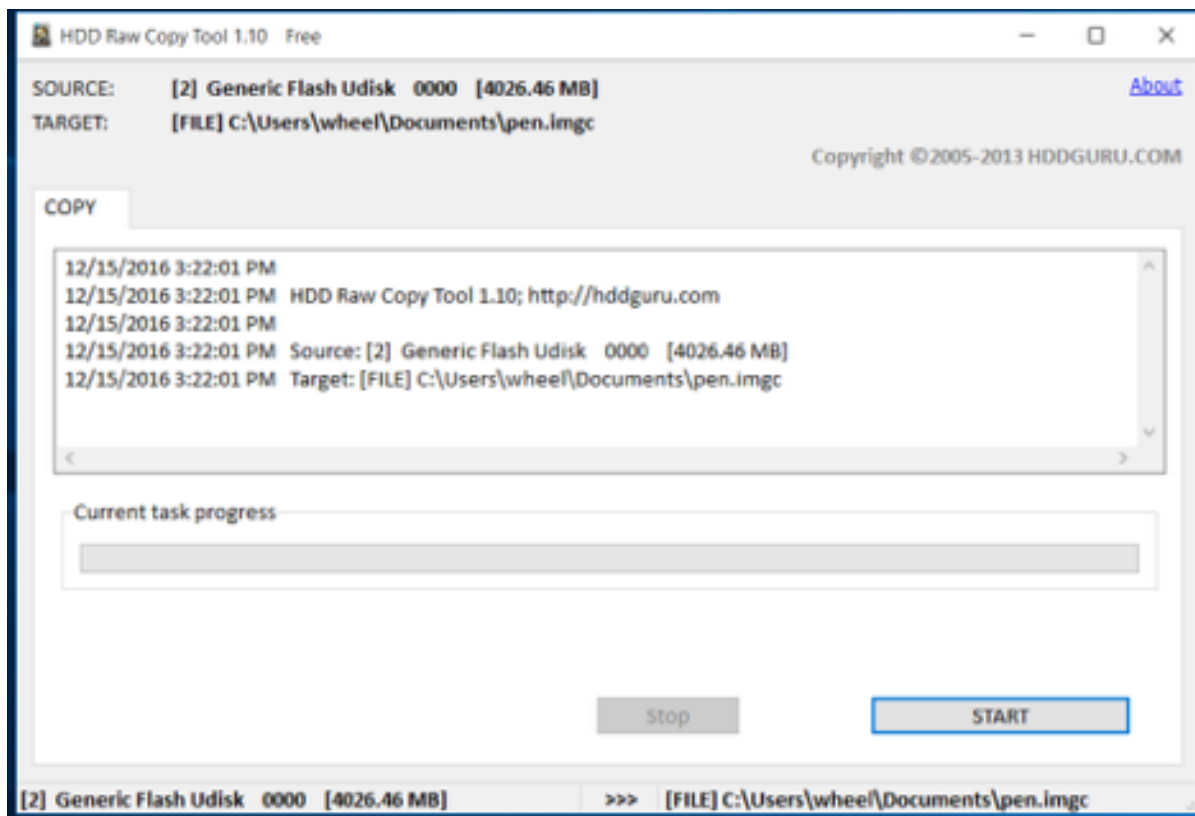
1. Download and install *HDD Raw Copy Tool*.

<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 encryption key and click *Continue*.

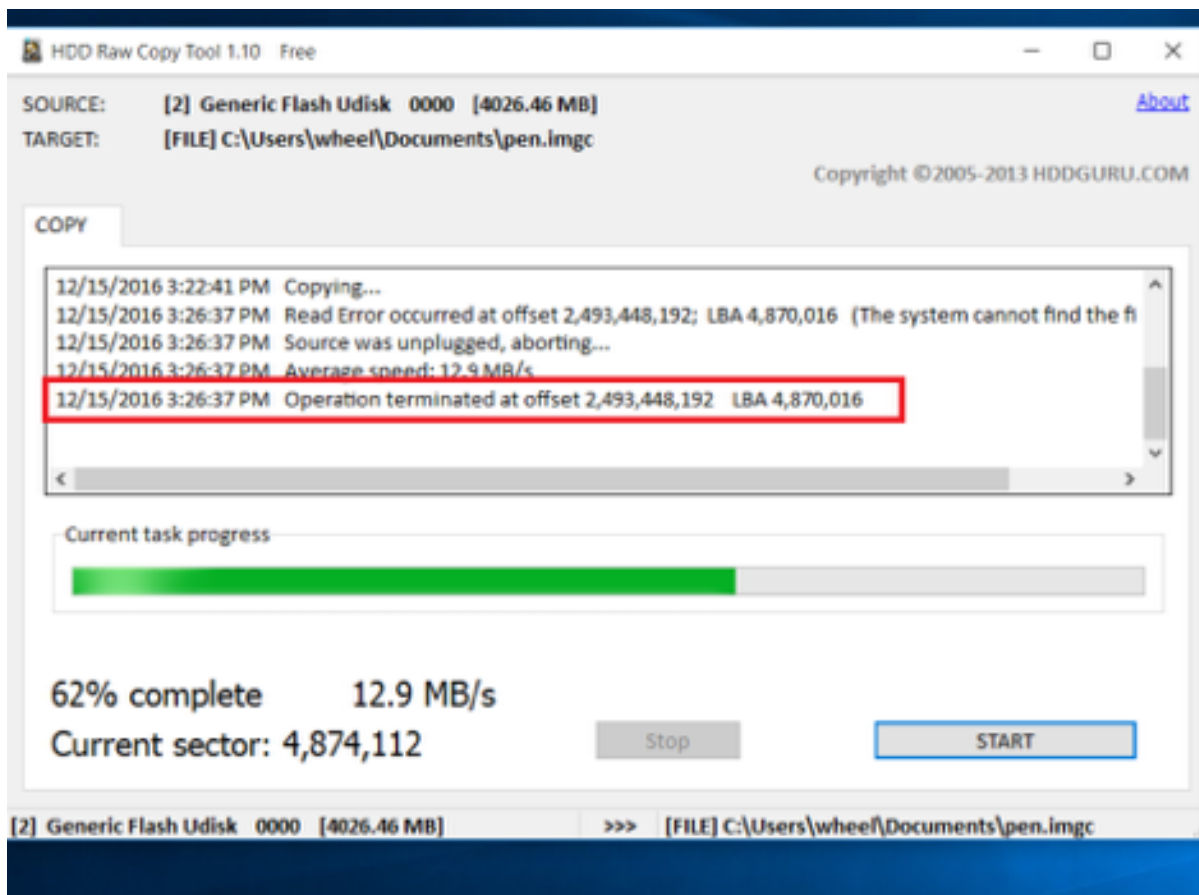


4. Click *FILE* twice, select the target image file and click *Continue*.
5. Click *START* to proceed with copying data.

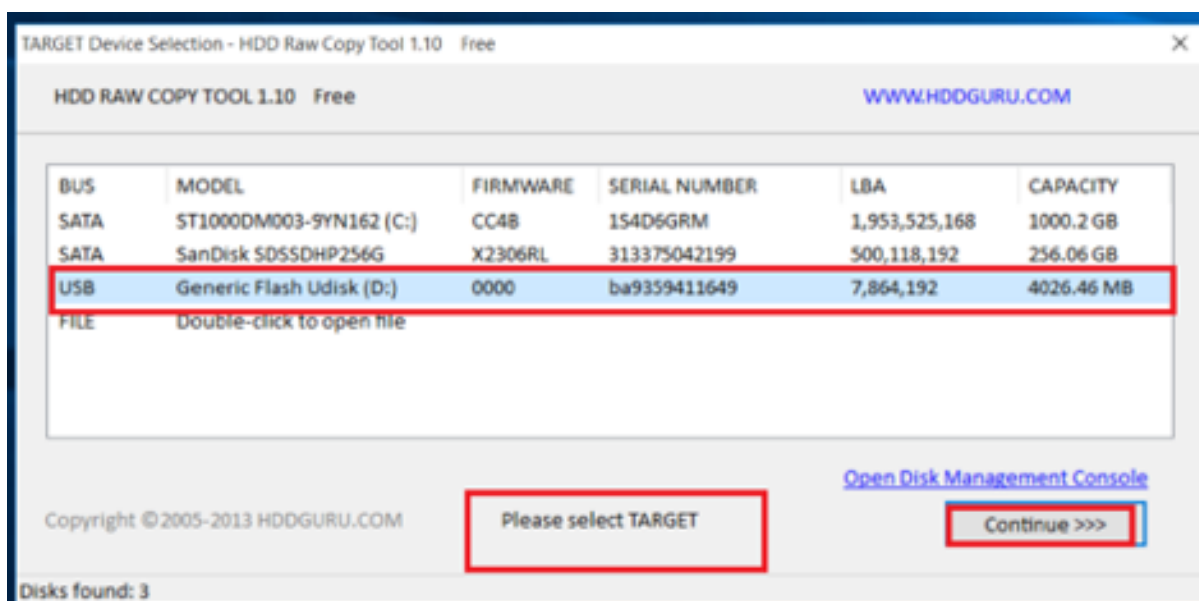


6. Once the following message occurs

Operation terminated at offset... close the application and disconnect the USB drive.



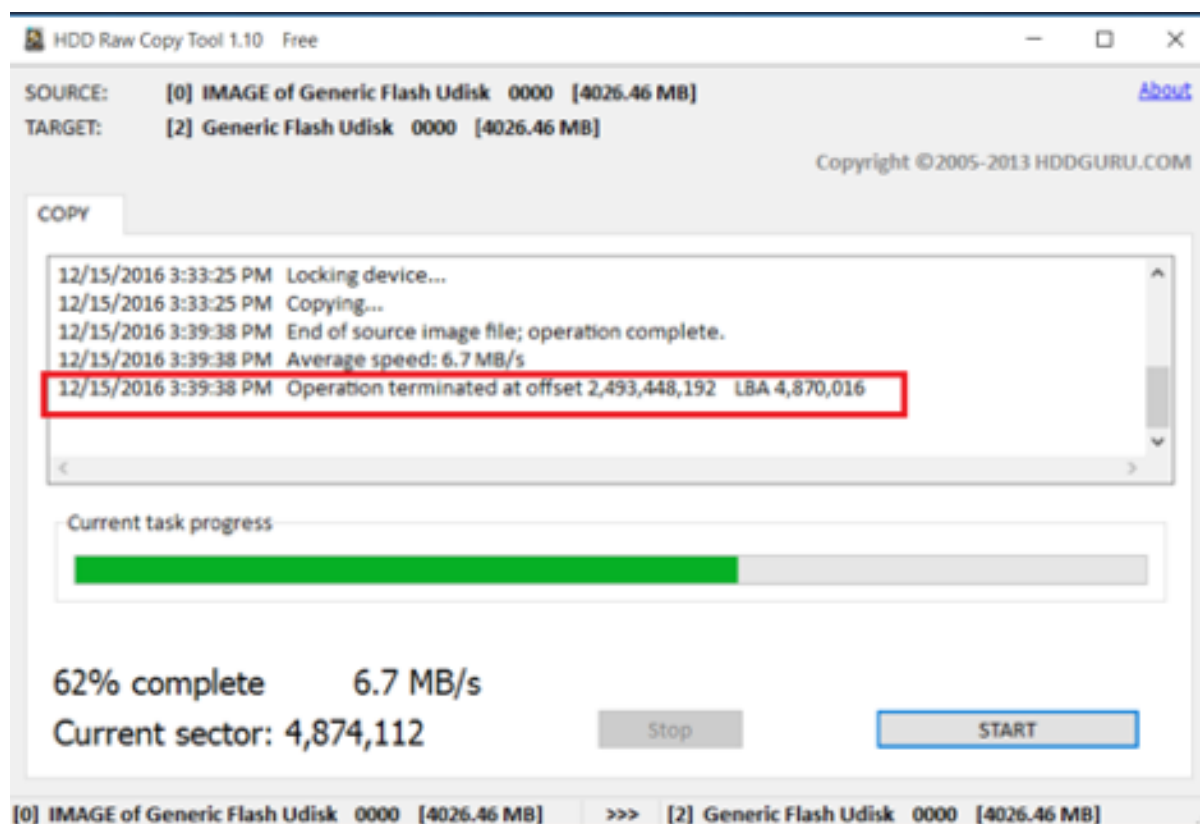
7. Connect another USB drive and start *HDD Raw Copy Tool*.
8. On the source drive selection screen select *FILE* and browse the file system to find the encryption keys image file.
9. Select the newly connected USB flash drive as a target device and click *Continue*.



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*

15.17.2 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*

15.17.3 Hard drive replacement

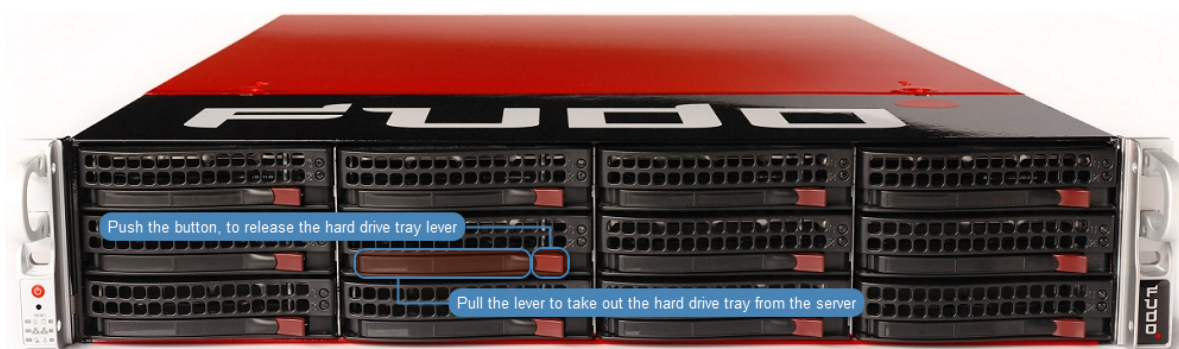
In default configuration, Wheel Fudo PAM’s storage array comprises 12 hard drives in RAIDZ2 configuration running ZFS file system allowing the system to remain fully operational in case of a failure of two hard drives.

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.

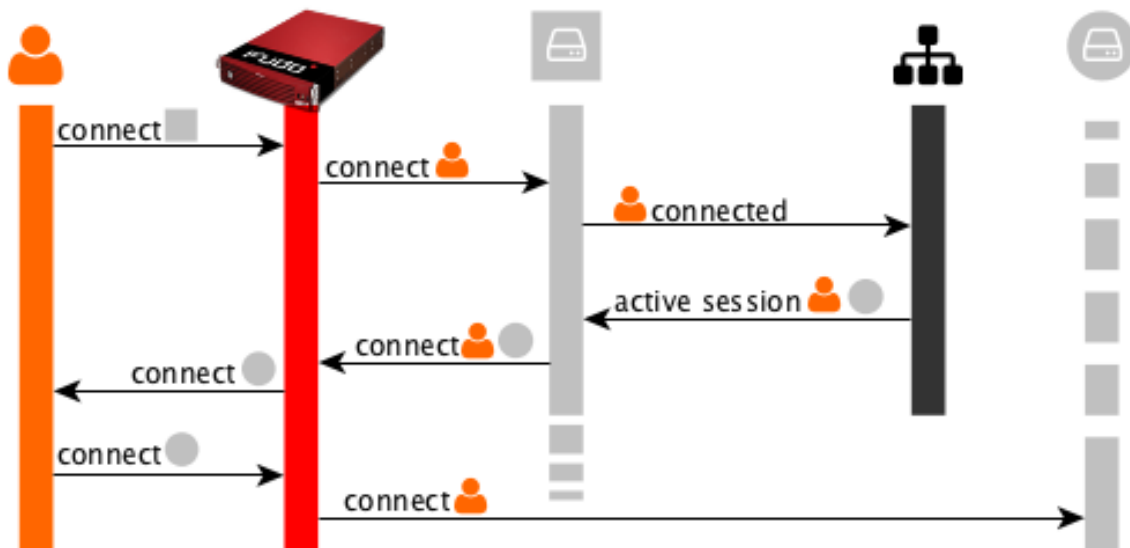
Related topics:

- [*Hardware overview*](#)
- [*Frequently asked questions*](#)

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 successfully 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 Error codes

Error code	Error message and description
FSE0001	<i>Internal system error</i>
FSE0002	<i>FUDO certificate error.</i>
FSE0003	<i>Unable to change configuration settings.</i>
FSE0004	<i>Configuration import error</i>
FSE0005	<i>Unable to initialize <code>{disk}</code>. Replace defective drive.</i>
<hr/> Note: Hard drives numbering starts from 0. If there is a problem with the hard drive number 1, physically it's the second drive in the top row. <hr/>	
FSE0006	<i>Invalid license</i>
FSE0007	<i>Unable to find license file</i>
FSE0008	<i>Unable to attach hard drive <code>{disk}</code>.</i>
FSE0009	<i>Upgrade failed.</i>
FSE0010	<i>License expired.</i>
FSE0020	<i>System backup error.</i>
FSE0024	<i>Hard drive belongs to another FUDO (<code>{diskserial}</code>) <code>{disk}</code>.</i>
FSE0026	<i>Cluster communication error.</i>
FSE0028	<i>Unable to join node to cluster.</i>
FSE0031	<i>Timestamping service communication error.</i>
FSE0032	<i>Unable to timestamp session.</i>
FSE0033	<i>Unknown timestamping service provider.</i>
FSE0040	<i>Cluster communication error. Local FUDO version is <code>%s</code> than <code>%s</code> FUDO version.</i>
FSE0046	<i>There is no filter called <code>%s</code>.</i>
FSE0048	<i>Error authenticating user over RADIUS.</i>
FUE0057	<i>Authentication method 'password', required by MySQL, requested by the user <code>%s</code>, logging in from IP address <code>%s</code>, was not found.</i>
FUE0058	<i>Authentication method 'password', required by MySQL, requested by the user <code>%s</code>, was not found.</i>
FSE0061	<i>Incorrect password repository configuration: login is empty.</i>
FSE0062	<i>Incorrect password repository configuration: password is empty.</i>
FSE0063	<i>Incorrect server configuration: ERPM namespace is empty.</i>
FSE0064	<i>Incorrect server configuration: ERPM name is empty.</i>
FSE0065	<i>License configuration error.</i>

Continued on next page

Table 1 – continued from previous page

Error code	Error message and description
FSE0066	<i>Unable to block user %jd.</i>
FSE0067	<i>Error connecting to Lieberman ERPM server %s: incorrect URL in configuration.</i>
FSE0068	<i>Error connecting to Lieberman ERPM server %s: incorrect protocol specified.</i>
FSE0069	<i>Error fetching password from Lieberman ERPM server %s: unable to get sessid for user %s.</i>
FSE0070	<i>Error fetching password from Lieberman ERPM server %s: unable to get password for user %s for the %s/%s server.</i>
FSE0076	<i>Unable to establish connection, could not find specified transparent server (tcp://%s:%u).</i>
FSE0077	<i>LDAP authentication error.</i>
FSE0078	<i>LDAP authentication error: unable to connect from %s to %s.</i>
FUE0079	<i>Authentication timeout after %ju key attempt%s and %ju password attempt%s.</i>
FUE0080	<i>Authentication timeout after %lu key attempt%s.</i>
FUE0081	<i>Authentication timeout after %lu password attempt%s.</i>
FSE0082	<i>Unable to establish connection to server %s (%s).</i>
FSE0083	<i>Unable to establish connection from %s to server %s (%s).</i>
FUE0089	<i>Authentication timeout.</i>
FSE0090	<i>Unable to connect to the passwords repository server %s.</i>
FSE0091	<i>Unable to add server %s.</i>
FSE0092	<i>Passwords repository server %s communication error.</i>
FSE0093	<i>Error connecting to Thycotic server %s: incorrect URL in configuration.</i>
FSE0094	<i>Error connecting to Thycotic server %s: incorrect protocol specified.</i>
FSE0095	<i>Error fetching password from Thycotic server %s: unable to get sessid for user %s.</i>
FSE0096	<i>Error fetching password from Thycotic server %s.</i>
FSE0097	<i>Error fetching password from Thycotic server %s: unable to get secretid for server %s.</i>
FSE0098	<i>Error fetching password from Thycotic server %s: unable to get password for user %s for the %s server.</i>
FUE0099	<i>Connection terminated.</i>
FUE0101	<i>Unable to find matching HTTP connection.</i>
FUE0103	<i>HTTP connection error.</i>
FUE0106	<i>Authentication failed: %s.</i>
FUE0108	<i>MySQL connection error.</i>
FUE0110	<i>Oracle connection error.</i>
FUE0112	<i>RDP connection error.</i>
FUE0113	<i>TLS Security configured, but missing TLS private key.</i>
FUE0114	<i>TLS Security configured, but missing TLS certificate.</i>
FUE0115	<i>Standard RDP Security configured, but missing private key.</i>
FUE0116	<i>TLS certificate verification failed.</i>
FUE0117	<i>RSA key verification failed.</i>
FUE0124	<i>SSH connection error.</i>
FUE0125	<i>User %s failed to authenticate after %d attempts, disconnecting.</i>
FUE0127	<i>Invalid authentication method: expected passwordor sshkey, got %s.</i>

Continued on next page

Table 1 – continued from previous page

Error code	Error message and description
FUE0129	<i>Failed to authenticate against the server as user %s using %s.</i>
FUE0130	<i>Failed to authenticate against the server as user %s using %s (received %s).</i>
FUE0132	<i>Client requested incorrect terminal dimensions (%dx%d).</i>
FUE0133	<i>MSSQL connection error.</i>
FUE0134	<i>TN3270 connection error.</i>
FUE0135	<i>Unknown TN3270 command: %02x.</i>
FUE0136	<i>Telnet connection error.</i>
FSE0137	<i>Unable to read private key.</i>
FSE0138	<i>Server's certificate does not match configured certificate.</i>
FUE0139	<i>VNC connection error.</i>
FUE0140	<i>Client version: %s is higher than the client integrated in FUDO: %s.</i>
FUE0141	<i>VNC connection error. Client answered with unsupported security type: %hhu.</i>
FUE0142	<i>VNC connection error. Server version: %s is lower than client version: %s.</i>
FUE0144	<i>User %s failed to authorize logging in from IP address: %s.</i>
FUE0145	<i>User %s failed to authorize.</i>
FUE0146	<i>User %s failed to authenticate logging in from IP address: %s.</i>
FUE0147	<i>User %s failed to authenticate.</i>
FSE0148	<i>Listening on %s:%u failed while adding bastion %s.</i>
FAE0153	<i>Session indexing failure.</i>
FAE0154	<i>Session conversion failure for session %s.</i>
FAE0165	<i>Error authenticating user <user_name>.</i>
FAE0189	<i>Error saving NTP servers: <server_name>.</i>
FAE0232	<i>MySQL session playback error.</i>
FAE0267	<i>Error generating report %d: %s.</i>
FSE0283	<i>Unable to process pattern: %s.</i>
FSE0285	<i>Unable to read certificate.</i>
FSE0286	<i>No peer certificate received.</i>
FSE0290	<i>Unable to add server %s because %s is listening on same IP address and port.</i>
FUE0305	<i>Client connection closed: encryption is not available.</i>
FUE0306	<i>Client connection closed.</i>
FSE0307	<i>Error fetching password from HiPAM server %s: unable to get sessid for user %s.</i>
FSE0308	<i>HiPAM server internal error.</i>
FSE0309	<i>Error fetching password from HiPAM server %s: unable to get sessdat for user %s.</i>
FSE0310	<i>Incorrect server configuration: HiPAM name is empty.</i>
FSE0311	<i>Unable to fetch password from HiPAM.</i>
FSE0312	<i>Error connecting to HiPAM server %s: incorrect URL in configuration.</i>
FSE0313	<i>Error connecting to HiPAM server %s: incorrect protocol specified.</i>
FUE0314	<i>Invalid pixel format.</i>
FUE0315	<i>Unable to fetch standard RDP certificate.</i>
FUE0316	<i>Protocol security negotiation failure.</i>
FUE0317	<i>Unable to establish connection to server %s.</i>

Continued on next page

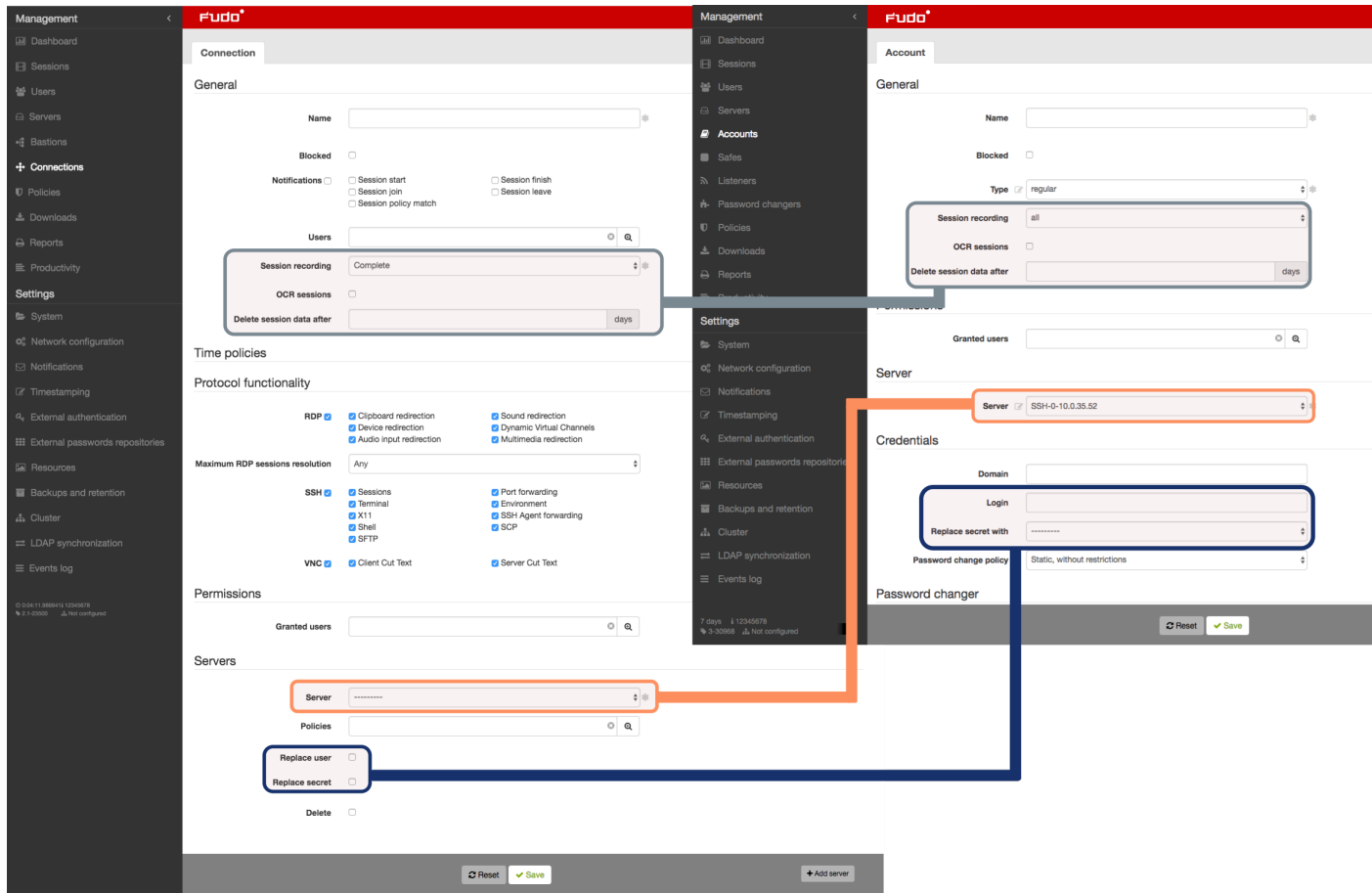
Table 1 – continued from previous page

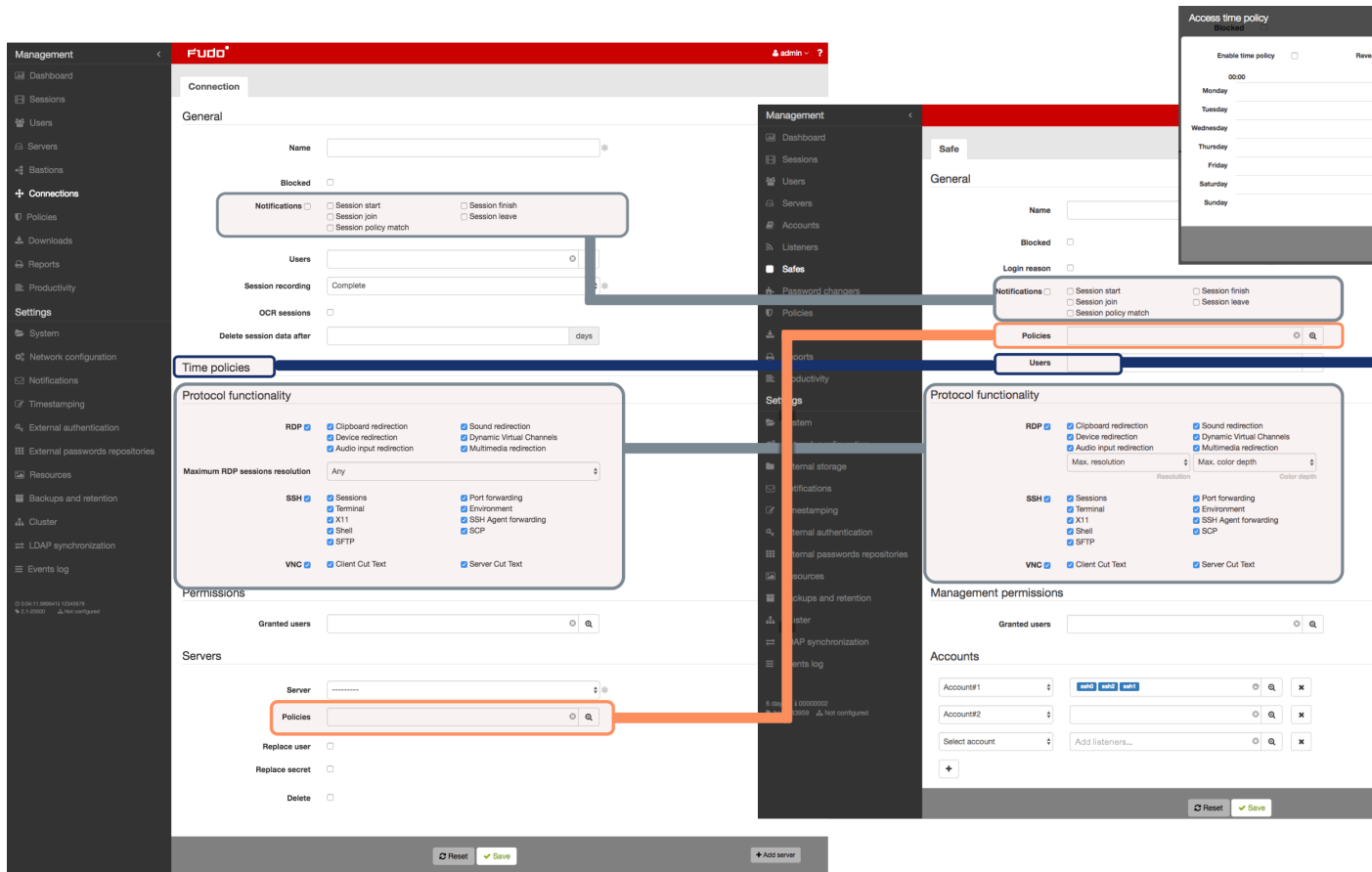
Error code	Error message and description
FUE0318	<i>Unable to fetch SSL certificate.</i>
FSE0330	<i>Bad login field configured on server. Error while processing user %s.</i>
FSE0331	<i>Error while processing userAccountControl value of user %s.</i>
FUE0346	<i>Client sent a packet bigger than %d bytes.</i>
FSE0347	<i>Cluster communication error. Local FUDO version: \${lversion}, remote FUDO version: \${rversion}.</i>
FSE0348	<i>Unable to get configuration settings.</i>
FUE0351	<i>Client sent unsupported NTLM v1 response.</i>
FSE0352	<i>Bastion requires login and server delimited with one of '%s' (%s).</i>
FSE0355	<i>Inconsistent data, starting recovery replication to node \${name}.</i>
FUE0359	<i>Server rejected X11 connection: %.*s.</i>
FUE0360	<i>Server requires unsupported X11 authentication: %.*s.</i>
FSE0362	<i>Unable to propagate ARP.</i>
FUE0363	<i>User %s has no access to host %s:%u.</i>
FUE0365	<i>RDP server %s:%u has to listen on the default RDP port in order to redirect sessions.</i>
FSE0366	<i>Error connecting to CyberArk server %s: incorrect URL in configuration.</i>
FSE0367	<i>Error connecting to CyberArk server %s: incorrect protocol specified.</i>
FSE0368	<i>Error fetching password from CyberArk server %s.</i>
FSE0369	<i>Error fetching password from CyberArk server %s: unable to get password for user %s for server %s.</i>
FSE0372	<i>Unable to invalidate OTP password %jd.</i>
FSE0375	<i>Unable to add listener %s.</i>
FSE0376	<i>Unable to add listener %s because %s is listening on same IP address and port.</i>
FSE0377	<i>Bastion requires login and server delimited with a '%s' character (login: %s).</i>
FSE0378	<i>Unable to establish connection, could not find a server (login: %s).</i>
FSE0379	<i>Unable to establish connection, could not find specified transparent server (tcp://%s:%u) (login: %s).</i>
FSE0380	<i>Unable to authenticate user %s: server is blocked.</i>
FSE0381	<i>Unable to authenticate user %s: account not found.</i>
FSE0382	<i>Unable to authenticate user %s: account is blocked.</i>
FSE0383	<i>Unable to authenticate user %s: user not found.</i>
FSE0384	<i>Unable to authenticate user %s: user is blocked.</i>
FSE0385	<i>Unable to authenticate user %s: safe not found.</i>
FSE0386	<i>Unable to authenticate user %s: safe is blocked.</i> Unblock the safe in question to allow users to connect to servers which use this safe.
FSE0420	<i>Unable to authenticate user %s against server %s.</i>
FSE0461	<i>Invalid data from AD server.</i>
FAE0464	<i>User %s is not allowed to login from address %s.</i> Add the specified IP address in the user object configuration in the <i>API</i> section.

16.3 Fudo 2.2 to Fudo 3.0 parameters mapping

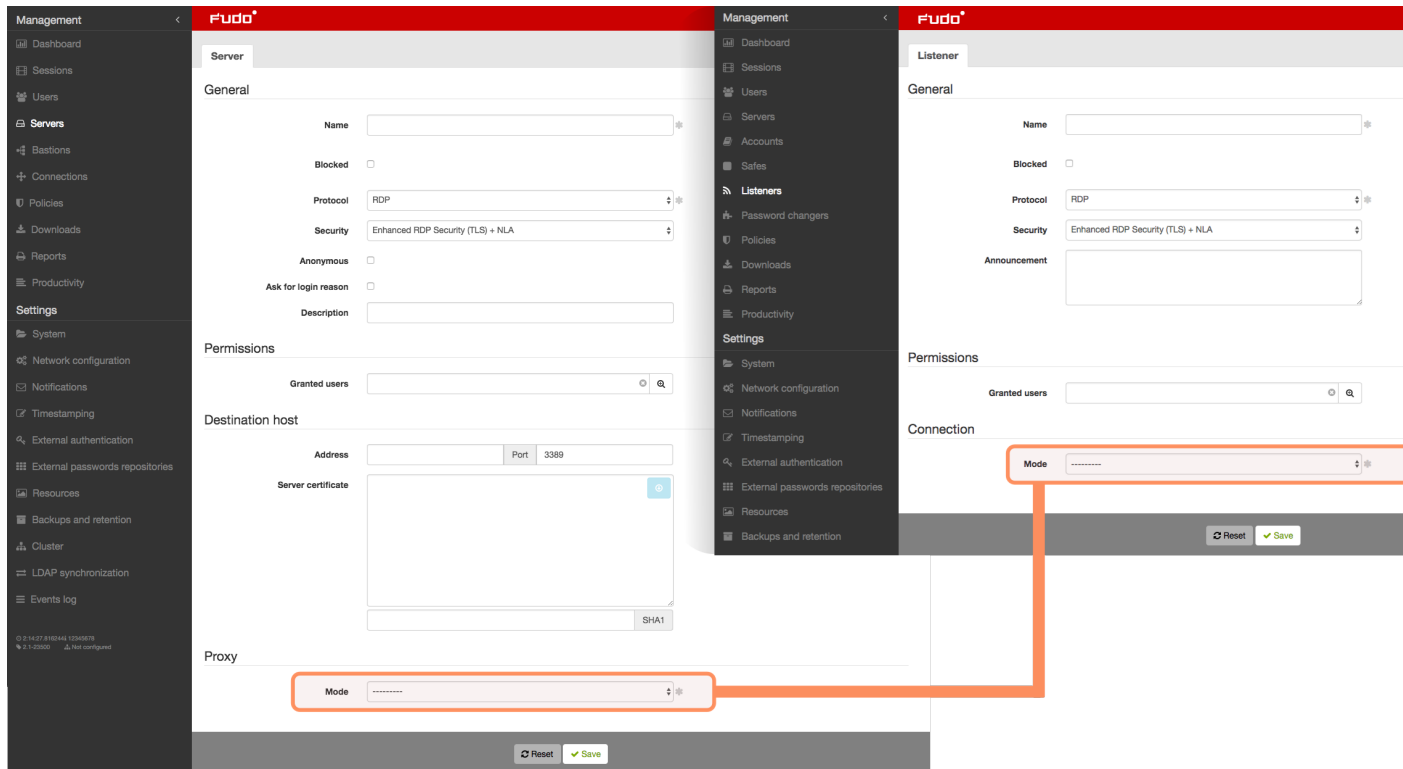
This topic describes how certain parameters from Fudo 2.2 map to Fudo 3.0 data model.

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 events 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 repository, 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 login 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 Supported protocols

This topic describes in detail Wheel Fudo PAM protocols support.

16.5.1 Citrix StoreFront (HTTP)

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Notes:

- 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.

16.5.2 HTTP

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Notes:

- 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.

16.5.3 ICA

Supported connection modes:

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

Supported client applications:

- Citrix Receiver.

16.5.4 Modbus

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Notes:

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

16.5.5 MS SQL (TDS)

Supported connection modes:

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

Supported client applications:

- SQL Server Management Studio,
- sqsh.

16.5.6 MySQL

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Supported client applications:

- Official MySQL client,

- PyMySQL libraries for Python.

Notes:

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

16.5.7 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:

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

16.5.8 RDP

Supported connection modes:

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

Supported client applications:

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

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.
- RemoteApp support is in development.

16.5.9 SSH

Supported connection modes:

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

Supported features:

- Connections multiplexing,
- SCP,
- Ports redirection.

Notes:

- SFTP sessions playback is not supported,
- SSH keys forwarding is not supported.

16.5.10 Telnet

Supported connection modes:

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

Notes:

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

16.5.11 Telnet 3270

Supported connection modes:

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

Notes:

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

Supported client applications:

- IBM Personal Communications,
- c3270.

16.5.12 Telnet 5250

Supported connection modes:

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

Notes:

- User must authenticate twice - first against Fudo and then against the target host.
- It is not possible to join a Telnet 5250 session.

Supported client applications:

- IBM Personal Communications,
- tn5250.

16.5.13 VNC

Supported connection modes:

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

Supported client applications:

- TightVNC,
- RealVNC.

16.5.14 X11

X11 protocol is supported within the SSH protocol.

Supported servers:

- Xorg,
- Xming,
- XQuartz.

16.6 ICA configuration file

The `.ica` configuration file defines connection parameters for establishing connections with remote host over the ICA protocol.

16.6.1 Plik ICA do połączeń bez TLS

```
[ApplicationServers]
<connection name>=

[<connection name>]
ProxyType=SOCKSV5
ProxyHost=<host>:<port>
ProxyUsername=*
ProxyPassword=*
Address=<login użytkownika>
Username=<login użytkownika>
ClearPassword=<hasło>
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

Note: <connection name> służy do celów informacyjnych i może być dowolnym ciągiem znaków.

16.6.2 Plik ICA do połączeń bez TLS

```
[ApplicationServers]
<connection name>=

[<connection name>]
ProxyType=SOCKSV5
ProxyHost=<host>:<port>
ProxyUsername=*
ProxyPassword=*
Address=<login użytkownika>
Username=<login użytkownika>
ClearPassword=<hasło>
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

Note: <connection name> służy do celów informacyjnych i może być dowolnym ciągiem znaków.

Tematy pokrewne:

- [ICA](#)
- [Model danych](#)

AAPM (Application to Application Password Manager)

17.1 Overview

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.

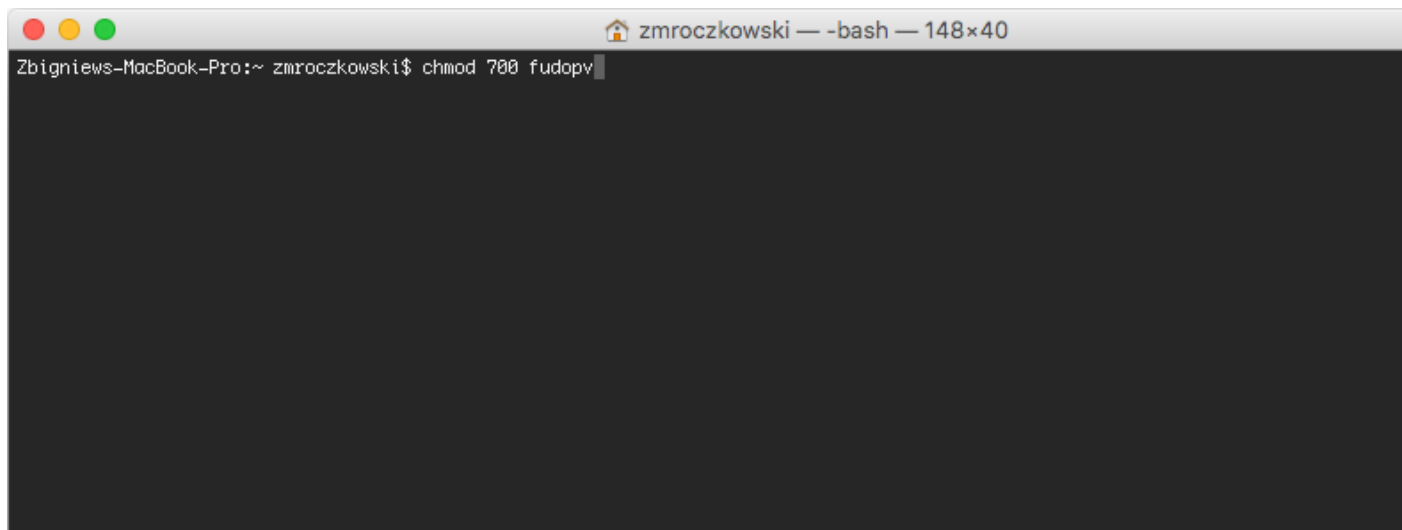
17.2 `fudopv`

Execution parameters

```
fudopv [<options>] <command> [<parameters>]
```

Command/option/parameter	Description
<i>Commands</i>	
<code>getcert</code>	Fetch Wheel Fudo PAM SSL certificate.
<code>getpass <type> <account></code>	Fetch password to selected account. type: <ul style="list-style-type: none"> • <code>direct</code> - direct, unmonitored connection; • <code>fudo</code> - connection monitored by the <i>PSM</i> module
<i>Options</i>	
<code>-c <path></code>	Use configuration file from provided path.
<code>--cfg <path></code>	
<code>-h, --help</code>	Show options and parameters list.

1. Upload `fudopv` script to the server and change its access rights to allow execution.

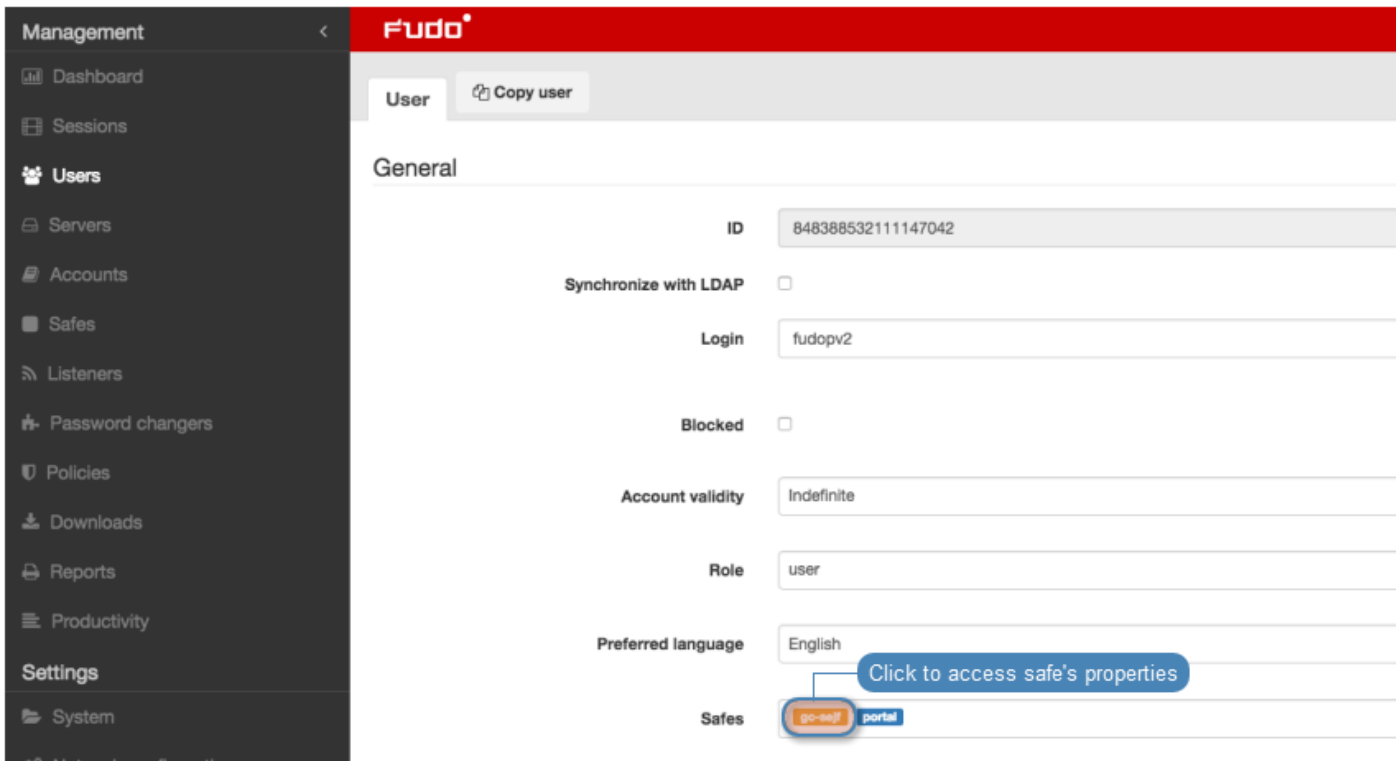
A terminal window with a dark background and a light gray title bar. The title bar contains three colored window control buttons (red, yellow, green) on the left and the text 'zmroczkowski — -bash — 148x40' on the right. The terminal content shows the prompt 'Zbigniews-MacBook-Pro:~ zmroczkowski\$' followed by the command 'chmod 700 fudopv' and a cursor at the end of the line.

```
Zbigniews-MacBook-Pro:~ zmroczkowski$ chmod 700 fudopv
```

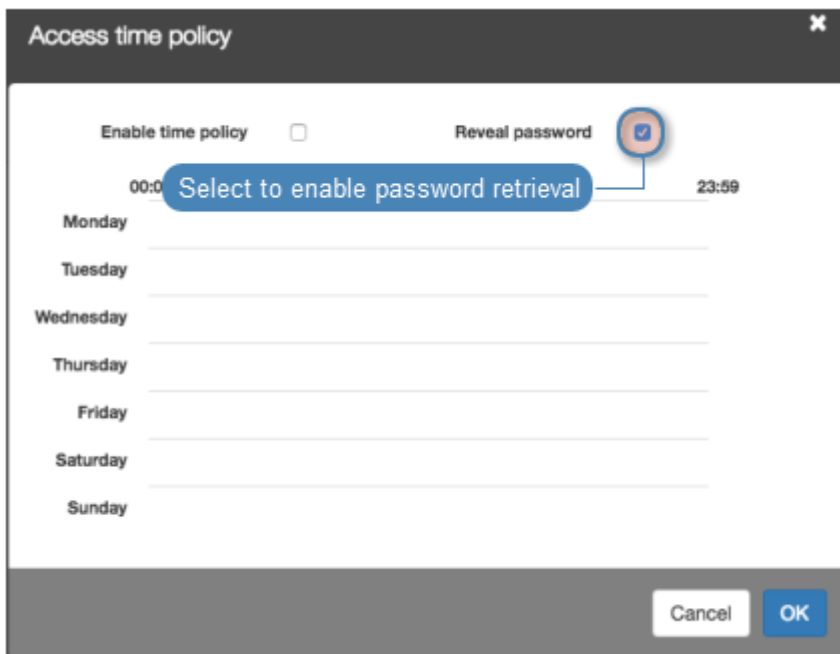
2. Log in to the Wheel Fudo PAM administration panel.
3. Create a user object with **user** role, static or one-time password authentication and server's IP address defined in the *API* section.

Note:

- 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.

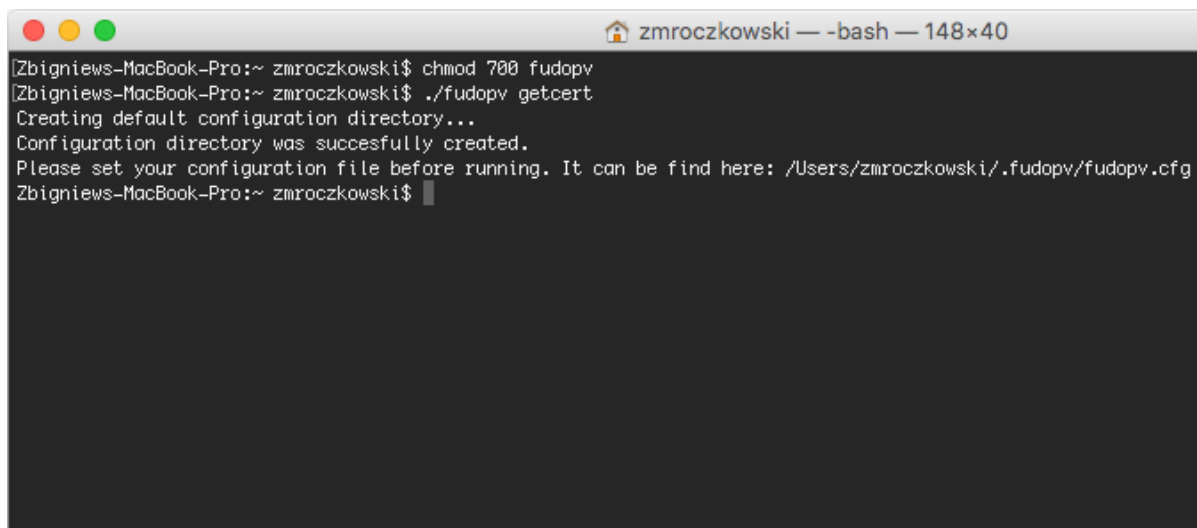


- Select the *Reveal password* option.



- 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*.

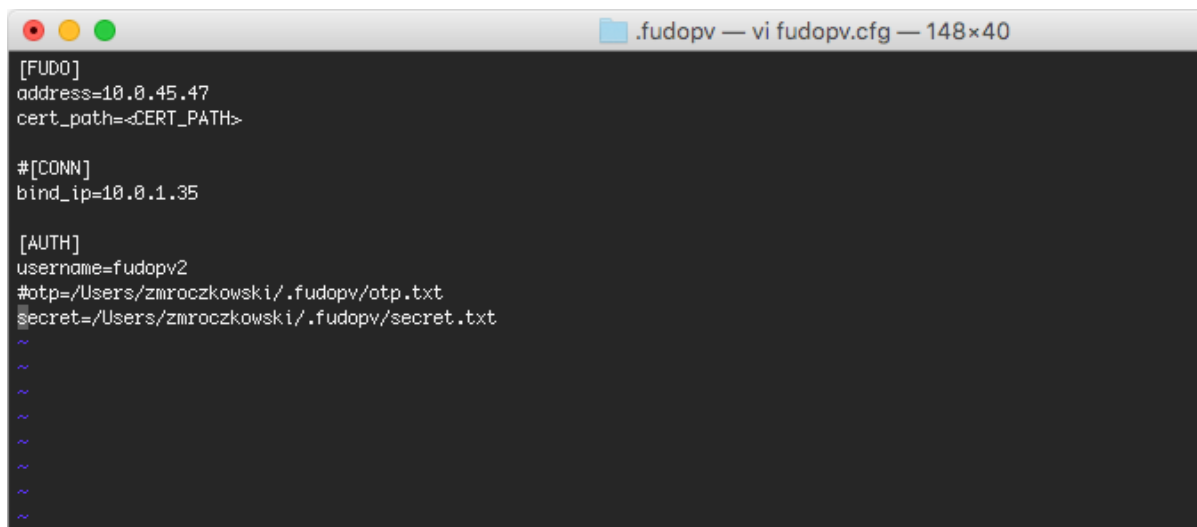
4. Run `fudopv getcert` command to initiate the configuration.



```
zmroczkowski — -bash — 148x40
[Zbigniew-MacBook-Pro:~ zmroczkowski$ chmod 700 fudopv
[Zbigniew-MacBook-Pro:~ zmroczkowski$ ./fudopv getcert
Creating default configuration directory...
Configuration directory was successfully created.
Please set your configuration file before running. It can be find here: /Users/zmroczkowski/.fudopv/fudopv.cfg
Zbigniew-MacBook-Pro:~ zmroczkowski$
```

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.



```
.fudopv — vi fudopv.cfg — 148x40
[FUDO]
address=10.0.45.47
cert_path=<CERT_PATH>

#[CONN]
bind_ip=10.0.1.35

[AUTH]
username=fudopv2
#otp=/Users/zmroczkowski/.fudopv/otp.txt
secret=/Users/zmroczkowski/.fudopv/secret.txt
~
~
~
~
~
~
~
```

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 <code>fudopv</code> script. The IP address must be the same as the IP address defined in the <i>API</i> section in user configuration.
[AUTH]	
username	User login as defined in step 3.
otp	Path to the <code>otp.txt</code> file containing the one time password.
secret	Path to the <code>secret.txt</code> 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.

```

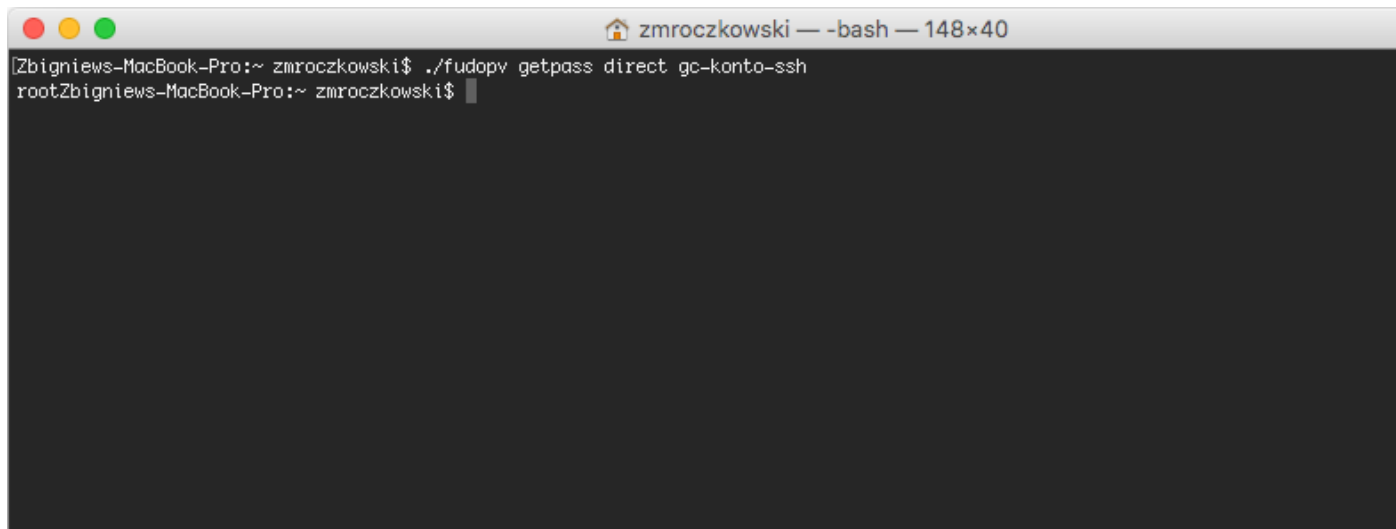
zmroczkowski — -bash — 148x40
cG9ydDEjMCEGA1UEAwwaRlVETyBUZWI1wb3JhenkgQ2VydG lmaW NhdGUxJzA lBglkq
hk iG9w0BCQEwGHN1cHBvcnRAd2h lZWxzexN0ZW1zLmNvbTAeFw0xNjA2MDEwODE4
NDJmFw0yNjA1MzAwODE4NDJmIHoMQSwCQYDVQQGEWJQTEPMA0GA1UEEQwGMDIt
NDk1MRQwEgYDVQQIDAttYXpvd2l lY2tpZTERMA8GA1UEBwwlV2Fyc3phd2EzXjAU
BgnVBAKMdXVsLk9jaG9ja2EgMUYxITAfBgnVBBAoMGFdoZWVzIFN5c3R lBxMgU3Au
IHogby5vLjEwMBQGA1UECwwuNV2h lZWwgU3VwcG9ydDEjMCEGA1UEAwwaRlVETyBU
ZW1wb3JhenkgQ2VydG lmaW NhdGUxJzA lBglkqhk iG9w0BCQEwGHN1cHBvcnRAd2h l
ZWxzexN0ZW1zLmNvbTCCA i lWdQYJKoZIhvcNAQEBBQADggIPADCCAgcCggIBALc4
dSr7DqZ4kVuJoI7V//jhVIXA0CRpY5IFbcKH iNGFXn3vBueNr9opedj /bwF iqb4p+
ZfRcWJ8HbpoVWo6gFYKGmPr0esRLR71301Xs0vzNnf smqP2vc9wKHq1LKDwdBMKE
ZqpydVbAcmr0u7ZS ljsFBd2LEFyULme9cIsd3e80SkLY0femZBCcy0++AXvCNhE0
WABvInzUrgbqrvaJKeIU37L tRyHZCa5 /o1auxnp+Ew l0ng l0RqwoS0x2FoR0w5Rj
j+p0i0XxfYN9cJ3+950QYfupMPSN9dF /0+ lbaThrRnqm5NPXUMxUS5oBdxmcd bJL
dX1bJ/tUyA17Vdru7Vyn09 /uUNtcJm7 /8nifVda4W lNOaQe43nynMuaAYb3fxJLC
+bs+0z iLarQgMH27MwK6c7XxNd+PDqVhNNK0Q09f0YZYr4UP+7pDFBFFXY0N0qSI
5mv0L2a0CAQNKJJ7D /TtR9vpJBDv9PXV67+p2ZA ty9asjAq /Iu6uXmmg8Tb /8MY
3rPQH2nC6WAW9Cd l4GX1mxhey0Da5f1EJ0eEwEAX0XzDeGzq /ZR7562Cbwe6he0c
0jbyN2NI9 lCfFC071bGDAKAID lZ2T100ua6SX9tBkTgLGdr l lFKrJo7zjWEo400Y
yN /snn45UdwvWzyk9BM84z /0w+Rr7cPj l tYDSzdHAgMBAAGjeDB2MAkGA1UdEwQC
MAAwKQYJYIZIAyB4QgENBBWwGKZVRE8gVGVtcG9yYXJ5J5IEN lcnRpZm l jYXR lMB0G
A1UdDgQWBBSXBvJ7BT1XBe8BxZHvQK9 lLsnTbTafBgnVHSMEGDAWgBSXBvJ7BT1X
Be8BxZHvQK9 lLsnTbTANBglkqhk iG9w0BAQ0FAA0CAgEAqPzZVty1N6UsD5oKUQj7
N5 l3mr2D30nxGBNMaohdTqfZ lLoXRRc5szrzXyhK1Vx l t lJa1andt6BGtqi7eVp
Ur2s9hwABwSKEUjr lPnT+rukqgB6EyDvcjuCr3GVub /xe+ssChjAXHqXxevX7Txn
AMj l0Y i2PTjyo15v9WixQA74 l lJP4nV4ed4N9gSM0cLCceQmEDjaNzV lUW1zZYhs
IfXdqFuRs6XjZzaczYQWnk6RgBL600yngSt5Ey1vScHyTKXSRLuha0Atav51LJm i
rLAXcjdGK+Ag7rPI jIMwz1vxtnrysvrDwjpg80KhNdUS9xFgnxG6g3EAE9V802gA
aB5BFJnW /Hhm7GghTMc+vbFT lkt5fxd2+TGdt inZaX7rdkH7JRK9p9G2j8Zrc5HT
li4To1oSTL /3VtbrzVdXqT8Qp lLF23IAKMWhDkeqZPwqGmhW0xcnTgSEu3yA1TZe
cwdrsUSHy01DZ0A1bHUyzc0G /s9NMasNctqkc29iRyprPuhQAZL fCDxPgiNv /LFX
ZVwKX0TftGZAx3YB0LH0kbQwCzEzwFXdpGBEzwiYE9JFmNGV l m2 l lHz3rdXLkwx
kqdnq0QQNKiuojE9KkZT242t+32UwUpfJjfkhhNazHq4AeQ1FzQ8H5HFzz7uhx7N
yf0IGHrrafLJj9qg2dtNhJo=
-----END CERTIFICATE-----

SHA1 Fingerprint: 2cba43a291fdcf71849ae1dfa9e19bcfc2795df8
Do you want to accept this certificate (yes/no)? : yes
Certificate has been successfully downloaded.
Configuration file has been updated.
Zbigniew-MacBook-Pro:~ zmroczkowski$

```

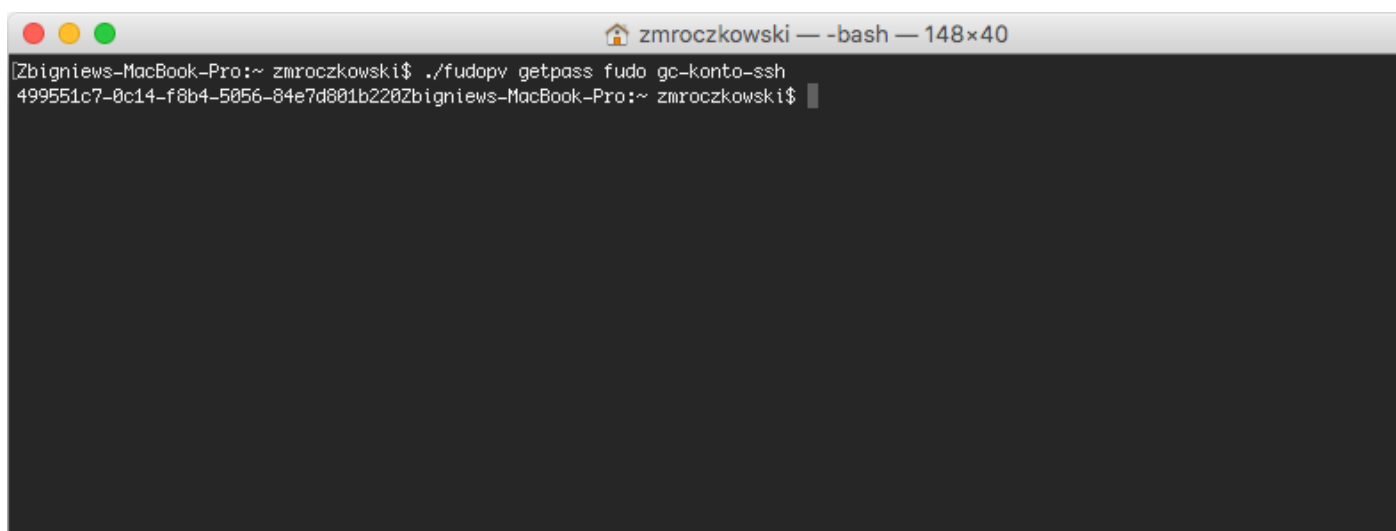
Note: After running the script successfully, the path to the certificate in the configuration file will be automatically updated.

- `fudopv getpass direct <account_name>`, to fetch password to connect directly to the server.



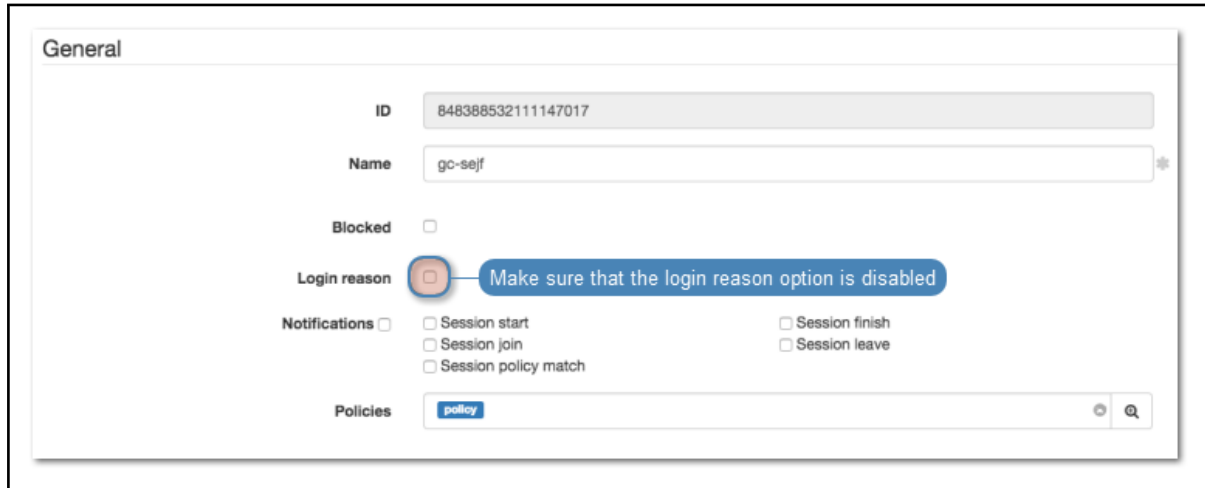
```
zmroczkowski — -bash — 148x40
[Zbigniew-MacBook-Pro:~ zmroczkowski$ ./fudopv getpass direct gc-konto-ssh
root[Zbigniew-MacBook-Pro:~ zmroczkowski$
```

- `fudopv getpass fudo <account_name>`, to fetch password to establish monitored connection with the target host.



```
zmroczkowski — -bash — 148x40
[Zbigniew-MacBook-Pro:~ zmroczkowski$ ./fudopv getpass fudo gc-konto-ssh
499551c7-0c14-f8b4-5056-84e7d801b220[Zbigniew-MacBook-Pro:~ zmroczkowski$
```

Warning: Correct operation of the `fudopv` script requires disabling the login reason prompt option in the safe's properties.



17.3 API interface

AAPM's API interface is described in detail in the *Wheel Fudo PAM - API documentation* manual.

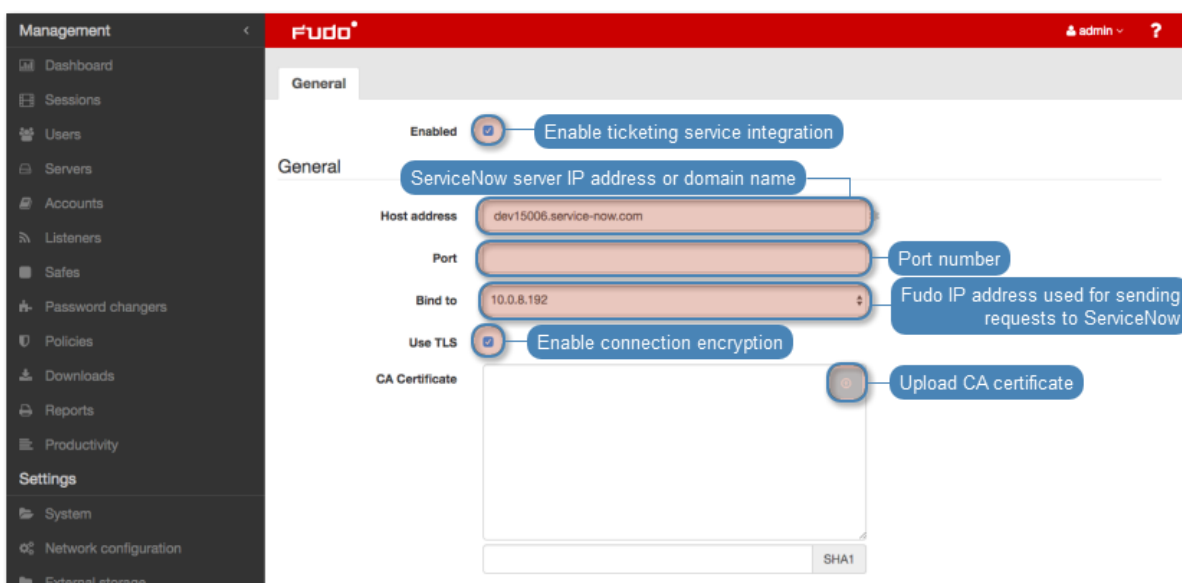
Related topics:

- *Data model*
- *System overview*
- *Setting up password changing on a Unix system*

18.1 Configuration

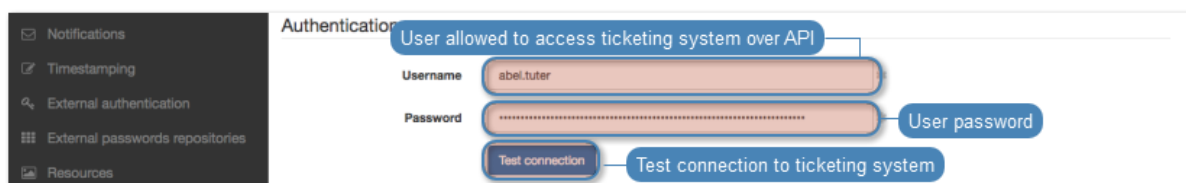
To configure *ServiceNow*, proceed as follows.

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.

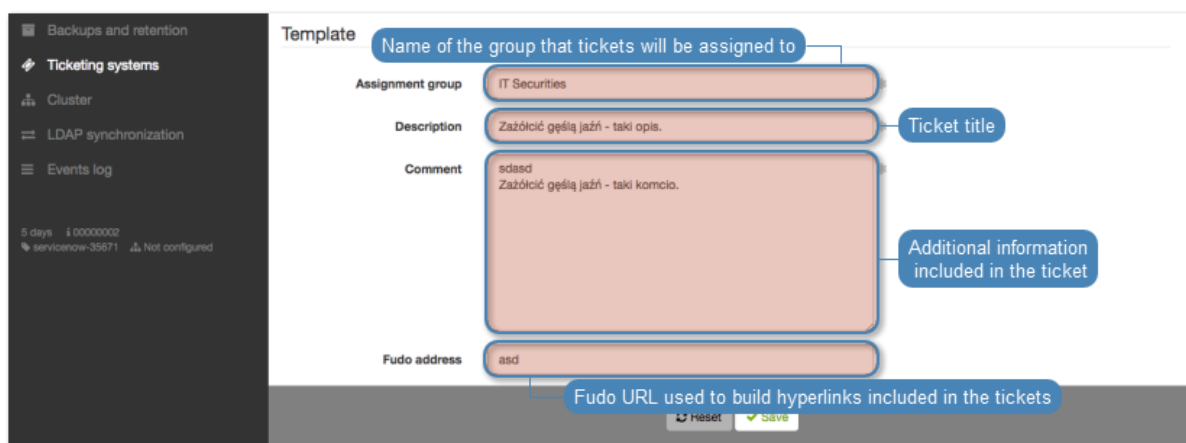


6. In the *Authentication* section, provide user credentials allowed to access *ServiceNow* over defined REST API.

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:

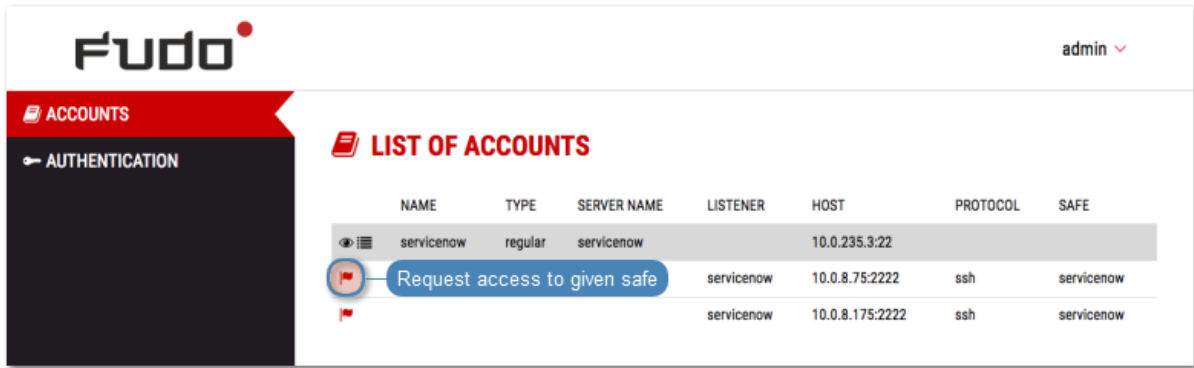
- *Requesting access to safe*
- *Granting access*

18.2 Requesting access to safe

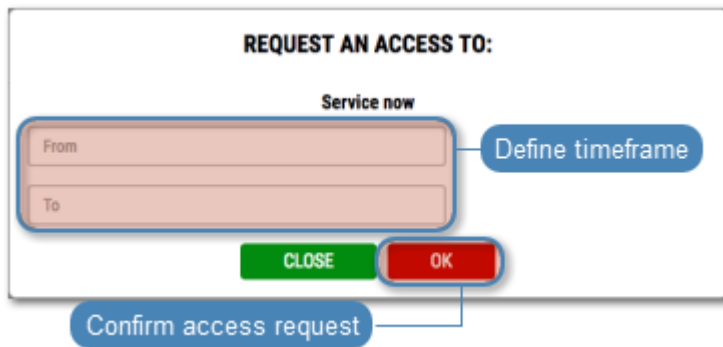
Note: Usernames on Wheel Fudo PAM and *ServiceNow* must be the same to ensure correct requests processing.

To request access to safe, proceed as follows.

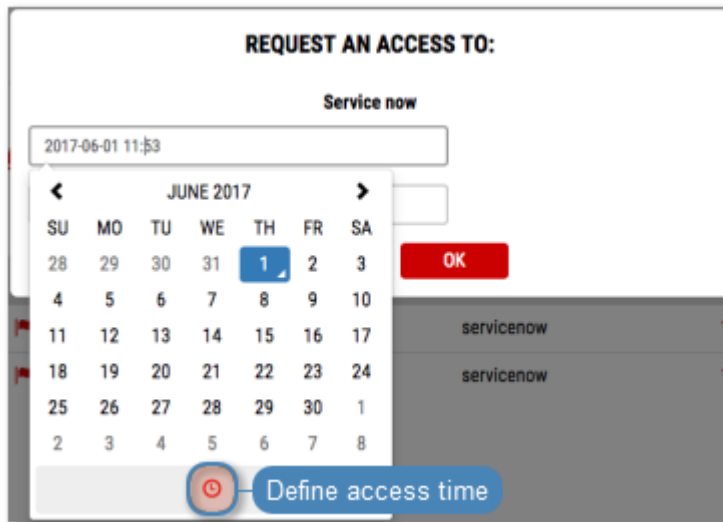
1. Log in to *User Portal*.
2. Find desired safe and click .



3. Define time period and click *OK*.



Note: Click the  icon to access time settings.




Related topics:

- *Configuration*
- *Granting access*

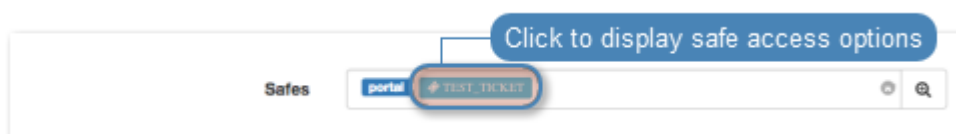
18.3 Granting access

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*

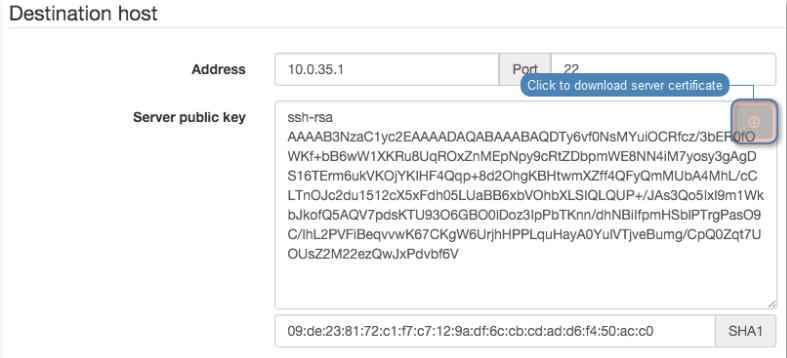
19.1 Booting up

Problem	Symptoms and solution
Wheel Fudo PAM does not boot up	<ul style="list-style-type: none">• Make sure that both power supplies are connected to power outlets. Not connecting both power supplies will result in sound alarm.• Make sure that encryption key is properly connected.• In case the problem is a result of unsuccessful system update, wait a few minutes. During that time, Wheel Fudo PAM will detect the problem and will restore previous system revision.

19.2 Connecting to servers

Problem	Symptoms and solution
Cannot connect to server	<p>Symptoms:</p> <ul style="list-style-type: none">• User cannot log in.• Events log entry: <code>Authentication failed: Invalid username kowalski or password.</code> <hr/> <p>Solution:</p> <ul style="list-style-type: none">• Verify that user definition exists in Wheel Fudo PAM database.• Make the login credentials are correct.• Make sure that the client software does not have outdated credentials stored. <hr/>
	<p>Symptoms: events log entry: <code>Unable to establish connection to server zbigniew (10.0.35.53:3399).</code></p> <hr/> <p>Cause: incorrect server configuration.</p> <hr/> <p>Solution:</p> <ul style="list-style-type: none">• Verify that the server in question is properly configured (IP address, port number).• Check if the server is reachable from Wheel Fudo PAM: <hr/> <ol style="list-style-type: none">1. Log in to Wheel Fudo PAM administration panel.2. Select <i>Settings > System, Diagnostics</i> tab.3. Enter server address in the <i>Ping</i> section and execute command and test host's availability. <hr/> <hr/>

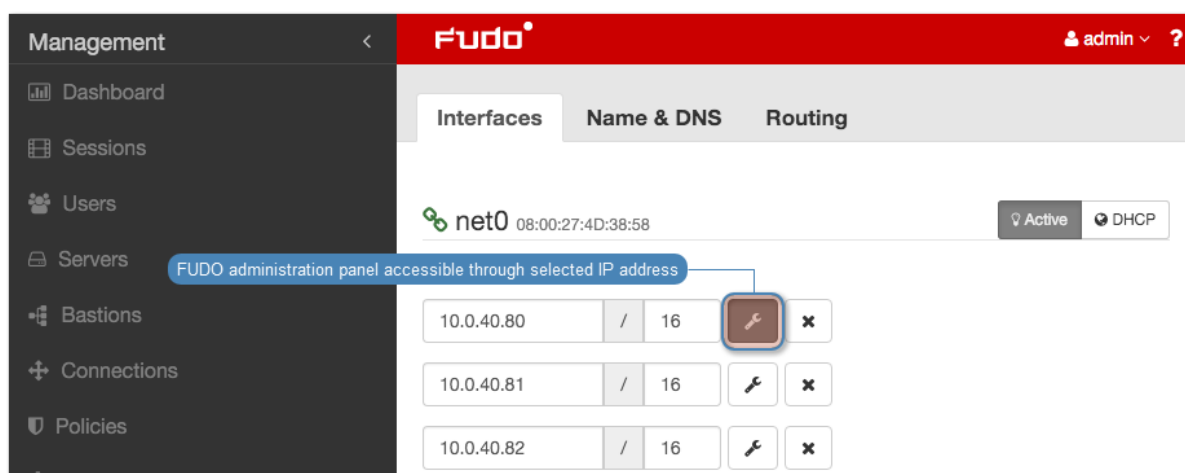
Problem	Symptoms and solution
When logging in not all of the users see the Wheel Fudo PAM logon screen.	<p>Cause:</p> <ul style="list-style-type: none"> • Credentials stored in RDP client result in users being automatically logged in to remote host. • Credentials stored in RDP client, user is successfully authenticated against credentials stored so the 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.
	<p>Symptoms:</p> <ul style="list-style-type: none"> • Client software message: Connection closed by remote host. • Events log entry: Failed to authenticate against the server as user root using password.
	<p>Cause: incorrect login credentials.</p>
	<p>Solution: provide correct login credentials in server configuration.</p>
	<p>Symptoms:</p> <ul style="list-style-type: none"> • RDP client message: Connection refused. • SSH client message: ssh: connect to host 10.0.1.111 port 10011: Connection refused
	<p>Cause: server has been blocked.</p>
	<p>Solution: log in to Wheel Fudo PAM administration panel and unblock the server.</p>

Problem	Symptoms and solution
<p>Connection is terminated</p>	<p>Symptoms:</p> <ul style="list-style-type: none"> • User tries to log in to server monitored by Wheel Fudo PAM, after entering username and password session is immediately terminated. • Events log entry: TLS certificate verification failed.
	<p>Solution:</p>
	<p>Download new target host certificate in the <i>Target host</i> section.</p>
	
	<p>Symptoms:</p> <ul style="list-style-type: none"> • After entering username and password the connection is terminated. • Events log entry: RDP connection error.
	<p>Solution: check if in the <i>General</i> tab in TCP-Rdp properties, the <i>Encryption level</i> option is not set to FIPS Compliant.</p>
<p>Cannot connect to server</p>	<p>Symptoms:</p> <ul style="list-style-type: none"> • Cannot log in to server with error message User user0 not allowed to connect to server. • Events log entry: Authentication failed: User user0 not allowed to connect to server.
	<p>Cause: user is not assigned to proper connection.</p>
	<p>Solution: add user to appropriate connection object.</p>

Problem	Symptoms and solution
	<p>Symptoms:</p> <ul style="list-style-type: none"> • After entering username and password, the screen freezes. • Events log entry <code>Terminating session: User user0 (id=848388532111147010) is blocked.</code> <hr/> <p>Cause: user is blocked.</p> <hr/> <p>Solution: log in to Wheel Fudo PAM administration panel and unblock the user in question.</p>
<p>User has to provide login credentials twice</p>	<p>Symptoms: user connecting over RDP protocol enters login credentials and immediately afterwards is asked again for the same login information.</p> <hr/> <p>Cause: server is a part of an infrastructure managed by connections broker which has detected an active user's session on another server.</p>
	<p>Symptoms: user connecting over SSH protocol enters login credentials and immediately afterwards is asked again for login information.</p> <hr/> <p>Cause: in <i>connection</i> 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.</p>
<p>Cannot connect to server over RDP protocol</p>	<p>Symptoms:</p> <ul style="list-style-type: none"> • User connecting over RDP is disconnected a moment after establishing connection. • Events log entry: <code>RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</code> <hr/> <p>Cause: connection is redirected to a host which does not listen on port number 3389.</p> <hr/> <p>Solution: configure server in question so it accepts user connections on port number 3389.</p>
	<p>Symptoms:</p> <ul style="list-style-type: none"> • Events log entry: <code>User user0 has no access to host 192.168.0.1:3389</code> <hr/> <p>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.</p>
	<p>Solution:</p> <ul style="list-style-type: none"> • Make sure that the server object exists. • Add user to proper <i>connection</i> object.

19.3 Logging to administration panel

Problem	Symptoms and solution
Cannot log in to administration panel	<ul style="list-style-type: none"> • Make sure that Wheel Fudo PAM IP address is correct. • Set Wheel Fudo PAM IP address from the console as described in the <i>Wheel Fudo PAM System documentation</i> in the <i>Network interfaces configuration</i> topic. • Make sure that the IP address in question has the management access option enabled.



19.4 Session playback

Problem	Symptoms and solution
Cannot playback exported video	<p>Cause: required video codecs are missing.</p> <p>Solution: install correct video codecs.</p>
Administrator user does not see sessions	<p>Symptoms: session list does not contain expected entries.</p> <p>Cause: insufficient access rights.</p> <p>Solution: grant access rights to specific user, server and connection objects.</p>
Cannot playback session in session player	<p>Symptoms: message: Could not find session data.</p> <p>Cause: recording has been disabled in connection properties when given session transpired.</p> <p>Solution: enable session recording to be able to playback session material in future.</p>

19.5 Cluster configuration

Problem	Symptoms and solution
Data model objects are not replicated to other nodes	Symptoms: Objects created on a node are not copied to other cluster nodes. Solution: Contact technical support department.

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?*

1. How many user sessions can be stored on Wheel Fudo PAM at once?

Wheel Fudo PAM is delivered with 20TB of hard drive space dedicated to storing users sessions. Size of the stored session is determined by user's activity. A minute of recorded connection takes on average:

RDP	1 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	50 kB active session.

Given that assumptions, 20TB of disk space allows recording:

- approximately 36 years of RDP sessions;
- approximately 760 years of SSH sessions.

Note: 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 keystrokes in the session player requires a consent from two `superadmin` users. Refer to the *Sensitive features* topic for the details on enabling this functionality.

11. Can I deactivate a session URL?

Active session URL can be deactivated anytime. URL revoking procedure is described in the *Sessions sharing* topic.

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, 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 Wheel 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 Wheel 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.

A

AAPM, **348**
account, **348**
Active Directory, **347**
AD, **347**
administration
 configuration export/import, **271**
anonymous safe, **348**
API
 users, **90**

C

CERB, **347**
CIDR, **348**
Citrix
 servers, **106**
configuration
 Network configuration, **239, 248, 249**
 notifications, **253**
 users synchronization, **100**
connection mode
 bastion, **14**
 gateway, **13**
 proxy, **13**
 transparent, **13**
creating
 servers, **106**

D

data retention, **349**
deleting
 servers, **135**
deployment scenario
 bridge, **12**
 forced routing, **12**
DHCP, **349**
DNS, **347**
dynamic
 servers, **130**

E

editing
 servers, **132**
Efficiency Analyzer, **348**
external authentication server, **349**

F

Fingerprint, **347**
fudopv, **348**

H

heartbeat, **348**
hot-swap, **348**
HTTP
 servers, **107**

I

ICA
 servers, **109**

L

LDAP, **347**
listener, **348**

M

Modbus
 servers, **112**
MS SQL
 servers, **113**
MySQL
 servers, **115**

N

Network configuration
 IP labels, **248**
 network bypass configuration, **249**
 network interface configuration, **239**
network configuration
 routing, **250**

O

Oracle
servers, 117

P

password changer, 348
passwords repository, 349
policy, 348
PSM, 349
PSM (*Privileged Session Management*), 348
Public key, 347

R

RADIUS, 347
RDP, 347
RDP
servers, 119
RDP connections broker, 349
RDP connections broker, 303
redundancy group, 349

S

safe, 348
server, 348
servers, 348
servers
Citrix, 106
creating, 106
deleting, 135
dynamic, 130
editing, 132
HTTP, 107
ICA, 109
Modbus, 112
MS SQL, 113
MySQL, 115
Oracle, 117
RDP, 119
ssh, 121
Telnet, 123
Telnet 3270, 125
Telnet 5250, 127
VNC, 129
sessions
commenting, 211
filtering, 198
play and preview, 202
shared session, 348
SSH, 347
ssh
servers, 121

SSH access, 348
Static password, 347
Syslog, 347

T

Telnet
servers, 123
Telnet 3270
servers, 125
Telnet 5250
servers, 127
time policy, 348
timestamp, 349

U

user, 348
users
access rights, 90
API, 90
roles, 90
users synchronization, 100
configuration, 100

V

VLAN, 348
VNC, 347
VNC
servers, 129

W

WWN, 349