



Wheel Fudo PAM 3.0 - System Documentation

Release is not supported

Wheel Systems

September 09, 2021

1	General information	1
1.1	About documentation	1
1.2	System overview	2
1.2.1	PSM	2
1.2.2	Secret manager	3
1.2.3	AAPM (Application to Application Password Manager)	4
1.2.4	Efficiency Analyzer	4
1.2.5	User portal	4
1.3	Data model	5
1.4	Deployment scenarios	6
1.5	User authentication methods and modes	9
1.6	Security measures	10
1.7	Requirements	13
2	Configuration	15
2.1	Hardware overview	15
2.2	System initiation	16
2.2.1	Appliance	16
2.3	Quick start	21
2.3.1	SSH	21
2.3.2	RDP	27
2.3.3	MySQL	35
2.3.4	HTTP	40
2.3.5	Telnet	44
2.3.6	Setting up password changing on a Unix system	50
2.4	Dashboard	53
2.5	Users	54
2.5.1	Adding a user	55
2.5.2	Editing a user	57
2.5.3	Deleting a user	58
2.5.4	Roles	59
2.6	Servers	59
2.7	Listeners	63
2.8	Safes	66
2.9	Accounts	68
2.10	Password changers	73

2.10.1	Password changer policy	73
2.10.2	Custom password changers	75
2.11	Policies	76
3	Sessions	81
3.1	Filtering sessions	82
3.1.1	Defining filters	82
3.1.2	Full text search	84
3.1.3	Managing user defined filter definitions	85
3.2	Reports	86
3.3	Viewing sessions	89
3.4	Viewing live sessions	92
3.5	Pausing connection	92
3.6	Terminating connection	93
3.7	Joining live session	95
3.8	Sharing sessions	95
3.9	Commenting sessions	98
3.10	Exporting sessions	100
3.11	Deleting sessions	102
3.12	OCR processing sessions	102
4	Efficiency analyzer	105
4.1	Overview	105
4.2	Sessions analysis	106
4.3	Activity comparison	108
5	AAPM (Application to Application Password Manager)	109
5.1	Overview	109
5.2	<i>fudopv</i>	109
5.3	API interface	117
6	Administration	119
6.1	System	119
6.1.1	Date and time	119
6.1.2	SSL certificate	121
6.1.3	SSH access	122
6.1.4	Sensitive features	123
6.1.5	System update	124
6.1.5.1	Updating system	125
6.1.5.2	Running update check	125
6.1.5.3	Deleting upgrade snapshot	126
6.1.6	License	126
6.1.7	Diagnostics	127
6.2	Network settings	128
6.2.1	Network interfaces configuration	129
6.2.1.1	Managing physical interfaces	129
6.2.1.2	Defining IP address using system console	132
6.2.1.3	Setting up a network bridge	136
6.2.1.4	Setting up virtual networks (VLANs)	136
6.2.2	Routing configuration	137
6.2.3	DNS servers configuration	139
6.3	Notifications	140

6.4	Trusted timestamping	142
6.5	External authentication	143
6.6	External passwords repositories	145
6.7	Resources	147
6.8	System version restore	148
6.9	System restart	149
6.10	Backups and retention	150
6.11	Exporting/importing system configuration	152
6.11.1	Exporting system configuration	153
6.11.2	Importing system configuration	153
6.12	Cluster configuration	154
6.12.1	Initiating cluster	154
6.12.2	Cluster nodes	155
6.12.3	Redundancy groups	160
6.13	Users synchronization	164
6.14	Events log	167
6.15	Integration with CERB server	169
6.16	System maintenance	179
6.16.1	Monitoring system condition	179
6.16.2	Hard drive replacement	180
7	Reference information	183
7.1	RDP connections broker	183
7.2	Error codes	184
7.3	Wheel Fudo PAM 2.2 to Wheel Fudo PAM 3.0 parameters mapping	188
7.3.1	Connection	188
7.3.2	Server	190
7.4	Data model migration from Wheel Fudo PAM version 2.2 to 3.0	190
7.4.1	Server	190
7.4.2	Safe (previously <i>connection</i>)	191
7.4.3	Account (previously <i>login credentials</i>)	191
7.4.4	Listener (previously <i>bastion</i> or part of a server)	192
7.4.5	Sessions	192
7.5	Supported protocols	192
7.5.1	Citrix StoreFront (HTTP)	192
7.5.2	HTTP	193
7.5.3	ICA	193
7.5.4	Modbus	193
7.5.5	MS SQL (TDS)	193
7.5.6	MySQL	194
7.5.7	Oracle	194
7.5.8	RDP	195
7.5.9	SSH	195
7.5.10	Telnet	195
7.5.11	Telnet 3270	196
7.5.12	Telnet 5250	196
7.5.13	VNC	196
7.5.14	X11	197
8	Troubleshooting	199
8.1	Booting up	199
8.2	Connecting to servers	200

8.3	Logging to administration panel	204
8.4	Session playback	204
8.5	Cluster configuration	205
9	Frequently asked questions	207
10	Glossary	211
	Index	215

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.

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

Disclaimer

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

1.2 System overview

Wheel Fudo PAM is a complete solution for managing remote privileged access. It comprises four modules:

- PSM (Privileged Sessions Management)
- Secret Manager
- AAPM (Application to Application Password Manager)
- Efficiency Analyzer

1.2.1 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

Wheel Fudo PAM supports following protocols:

- *SSH*,
- *RDP*,
- *VNC* - 24-bit (true color) connections only,
- *HTTP/HTTPS*,
- *MySQL*,
- *MS SQL*,
- *Oracle* (client applications: SQLDeveloper 4.1.3.20.78, SQL*Plus: Release 11.2.0.4.0 Production),

Note: *Oracle* protocol support is limited due to its undisclosed specification. Wheel Systems cannot guarantee correct Oracle databases monitoring.

- *Telnet/Telnet 3270*,
- *Citrix*,
- *modbus*.

Detailed information on supported protocols can be found in the *Reference information > Supported protocols* topic.

The PSM module supports following system configurations:

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

1.2.2 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.

1.2.3 AAPM (Application to Application Password Manager)

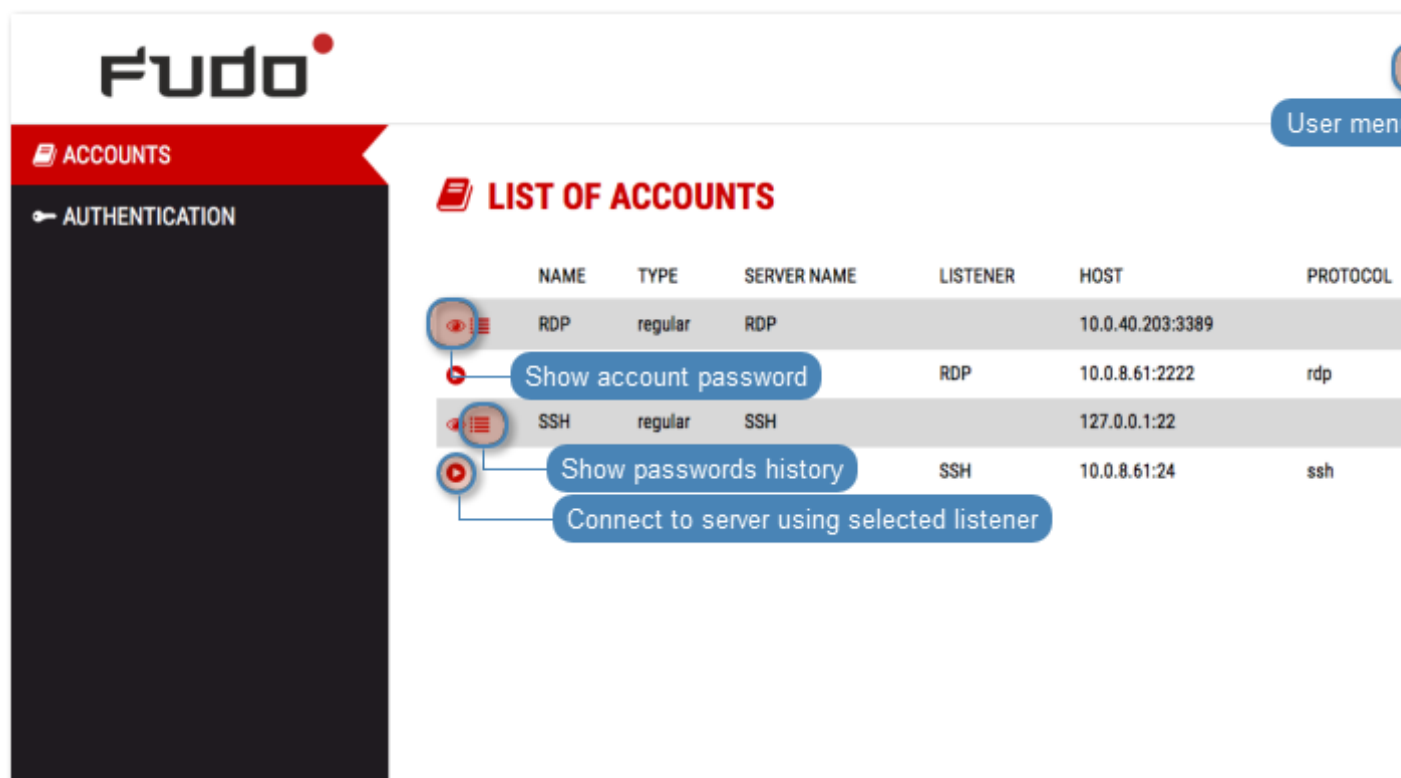
AAPM module enables secure passwords exchange between applications.

1.2.4 Efficiency Analyzer

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

1.2.5 User portal

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



Related topics:

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

1.3 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.

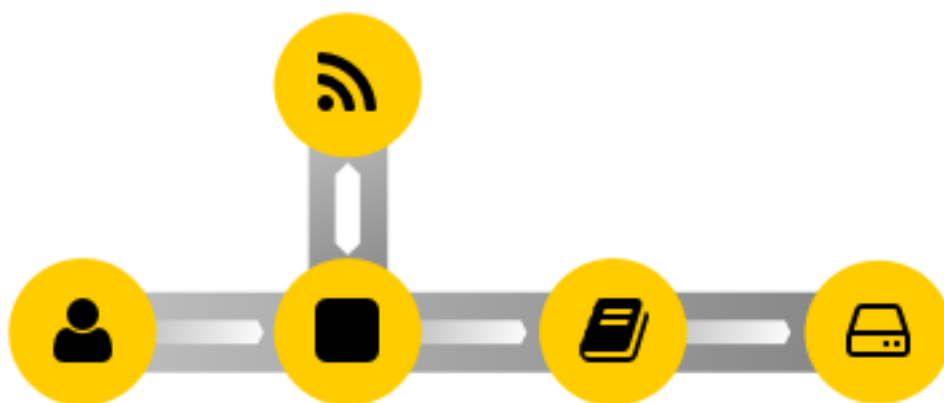
Listener determines server connection mode (proxy, gateway, transparent, bastion) as well as its specifics.

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](#)

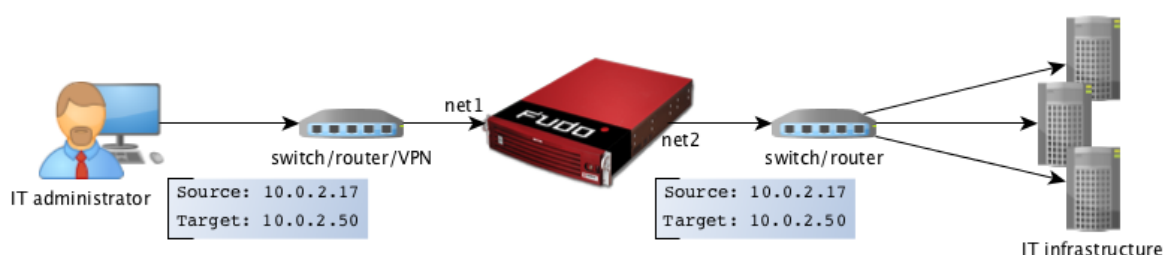
- *Quick start*

1.4 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.



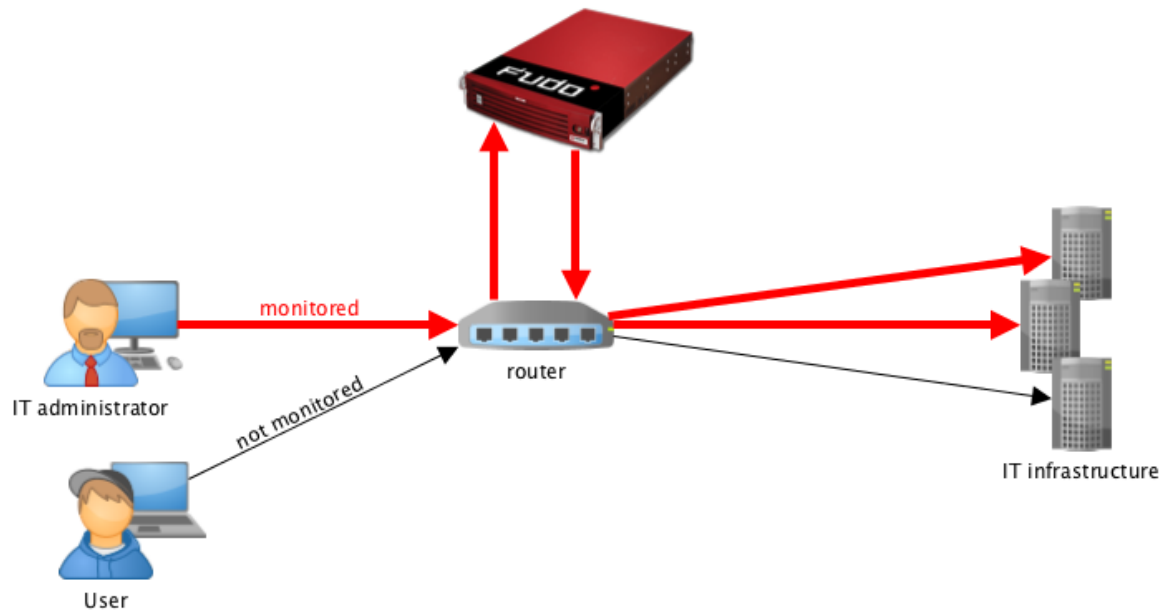
Mediating packages transfer, Wheel Fudo PAM preserves source IP address when forwarding requests to destination servers.

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.

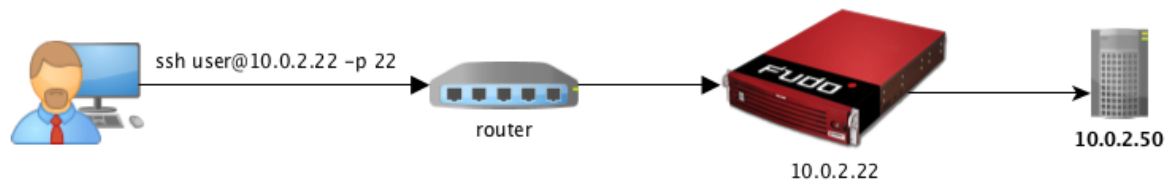


This mode does not require changes in existing network topology and enables network traffic optimization due to separating requests from system administrators and regular users.

Connection modes

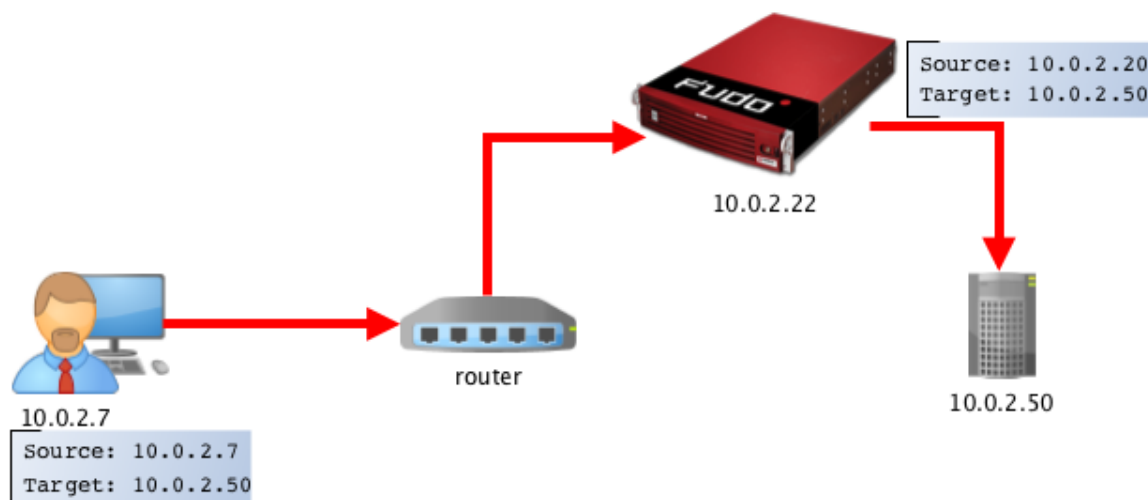
Transparent

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



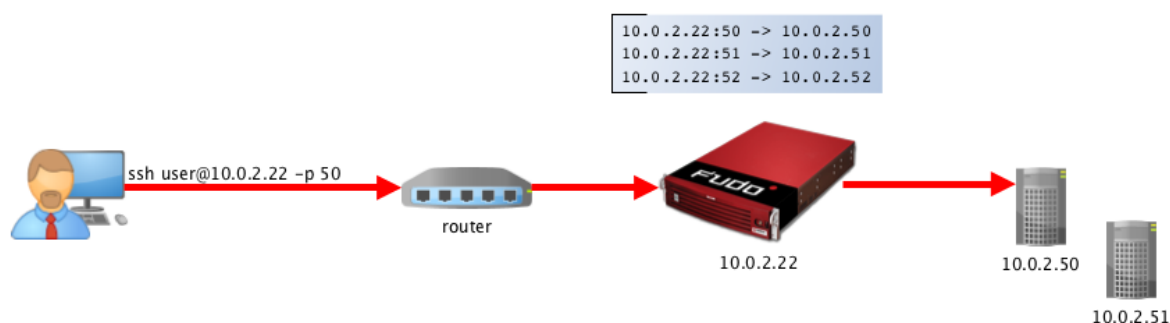
Gateway

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

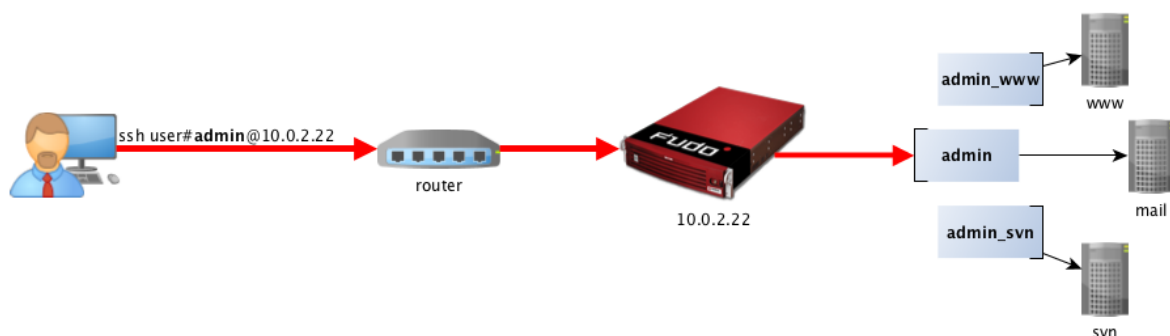
In proxy mode, administrator connects to destination server using combination of Wheel Fudo PAM IP address and unique port number assigned to given server. Uniqueness of this combination enables establishing connection with a particular resource.



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:

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

1.5 User authentication methods and modes

User authentication methods

Before establishing connections with server, Wheel Fudo PAM 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, Wheel Fudo PAM 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, Wheel Fudo PAM 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, Wheel Fudo PAM 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 Wheel Fudo PAM and once again to access the target system.

Related topics:

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

1.6 Security measures

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.

Backups

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

Permissions

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

Role	Access rights
user	Connecting to servers as defined in connections, to which the user has been assigned.
operator	<ul style="list-style-type: none">• logging in to administration panel• browsing objects: servers, users, bastions, connections, to which the user has been assigned sufficient access permissions• blocking/unblocking objects: servers, users, bastions, connections• generating reports on demand and subscribing to periodic reports• activating/deactivating email notifications• converting sessions and downloading converted content
admin	<ul style="list-style-type: none">• logging in to administration panel• managing objects: servers, users, bastions, connections, to which the user has been assigned sufficient access permissions• blocking/unblocking objects: servers, users, bastions, connections• generating reports on demand and subscribing to periodic reports• activating/deactivating email notifications• converting sessions and downloading converted content• managing policies
superadmin	<ul style="list-style-type: none">• full access rights to objects management• full access rights to system configuration options

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.

Reliability

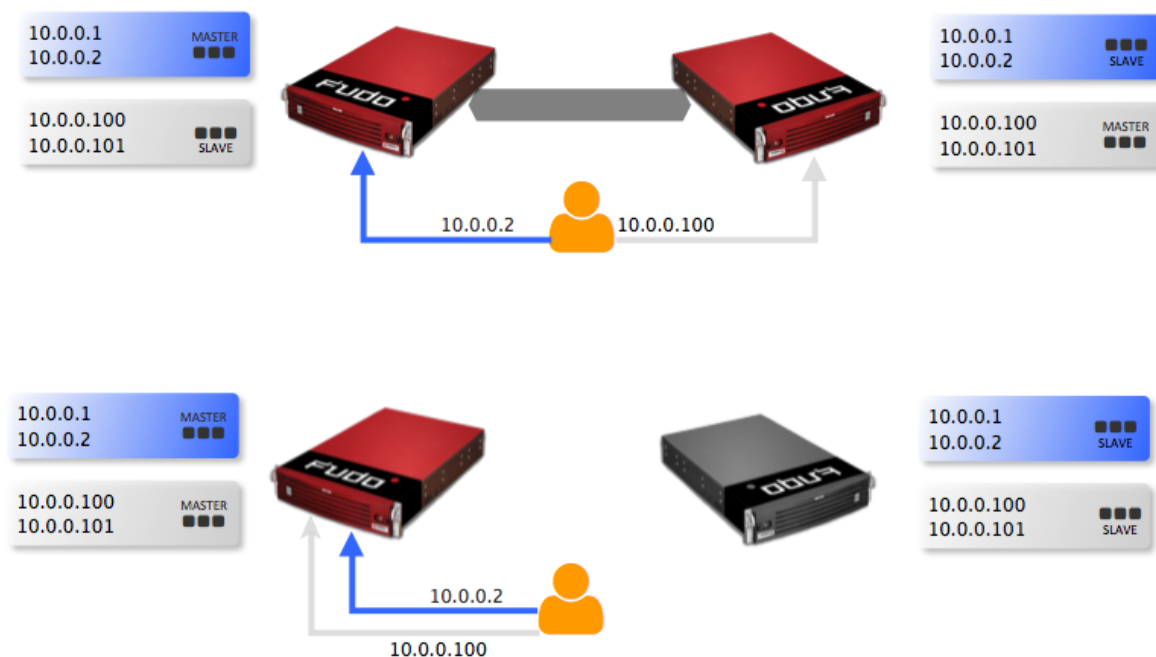
System hardware configuration is optimized to deliver high performance and high availability.

Cluster configuration

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

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

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



Related topics:

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

1.7 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.

2.1 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*

2.2 System initiation

2.2.1 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*

2.3 Quick start

2.3.1 SSH

This chapter contains an example of a basic WHEEL Wheel Fudo PAM 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 Wheel Fudo PAM PAM using an individual login and password combination (*john_smith/john69*). When establishing the connection with the remote server, WHEEL Wheel Fudo PAM 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

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

Parameter	Value
Name	test_server
Blocked	✗
Protocol	SSH
Description	Test server
<i>Permissions</i>	
Granted users	✗
<i>Destination host</i>	
Address	10.0.2.22
Port	22

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

Destination host

Address: 10.0.150.150 Port: 22

Bind address: Any

Server public key: ssh-rsa
 AAAAB3NzaC1yc2EAAAADAQABAAQAC6pbHkib/uemFNLoC49s
 Qss/gWm3Z4w4AMMk1LpD6L3Y9NR6-MGSLB399K-ID7lp4/SVR
 BXrRDC
 WEH/UvAs1CGAX1j21wx88hK3y9m1CzLD0qrupBcz1K2dMxNf/FG
 MQ5HlxOkq6TSkmEBWGLUSosk8tWwE898DwcAk6aD+5BThsTmrGq1I
 BGt0e/Q2M0zQFhkZGOgH55r7CEHWZDWI4YpAv+bU0UrbsqqID6dRLs
 KENtv2sb6Ppkm3700hxjH+p59K880Y9rNmh3lyJv4vCTPx4gF

Download server's public SSH key

Destination server's fingerprint

c9:b9:e8:14:b5:5e:d0:8f:c6:b5:02:96:e7:72:1c:6d:f0:cc:64:36 SHA1

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

Connection

Mode: proxy

Local address: 10.0.150.151 Port: 1022

Fudo public key: Generate FUDO's private SSH key
 Upload FUDO's private SSH key
 Wj+d4nY
 gUF/Cb9
 9SSh0ED9BGcwtowQg+Uo44X5t/1zPAAAFQDa1dZXglBamfYL6okb5
 2MckzjReQAAAIEAgCTQH9PydSERsLwvn0jxkwNro+jVcHJtvKsaj89Fjvrl
 KH3oWBS5rTVMeFx5dC01tkRc/S0RA1Yw1gnEY67JtOLMdUUmakMH
 FOWilvMoDY7NGQqG0DwoC/67L/MnuL+0783ADnYSKgvaQlfdDdT5UN
 AACAIGGYskAACMHEetWsSNDYITaSKAxI
 H5Lm+E3086p9RJ+5BrkRLgbEh8HceD52

FUDO's fingerprint

8b:be:11:c4:e5:dc:96:96:a0:c4:c2:1fa0:bf:aa:bf:9b:1e:cd:15 SHA1

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

6. Click *Save*.

Adding a user

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	john11
Repeat password	john11

4. Click *Save*.

Adding a listener

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

Parameter	Value
Name	ssh_listener
Blocked	✗
Mode	proxy
Local address	10.0.8.64
Port	10050

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

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

Parameter	Value
<i>General</i>	
Name	server_account
Account type	Forward
Session recording	complete
OCR sessions	✓
Delete session data after	61 days
Domain	
Login	administrator
<i>Permissions</i>	
Granted users	✗
<i>Password</i>	
Password change policy	
Replace secret	✓

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

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

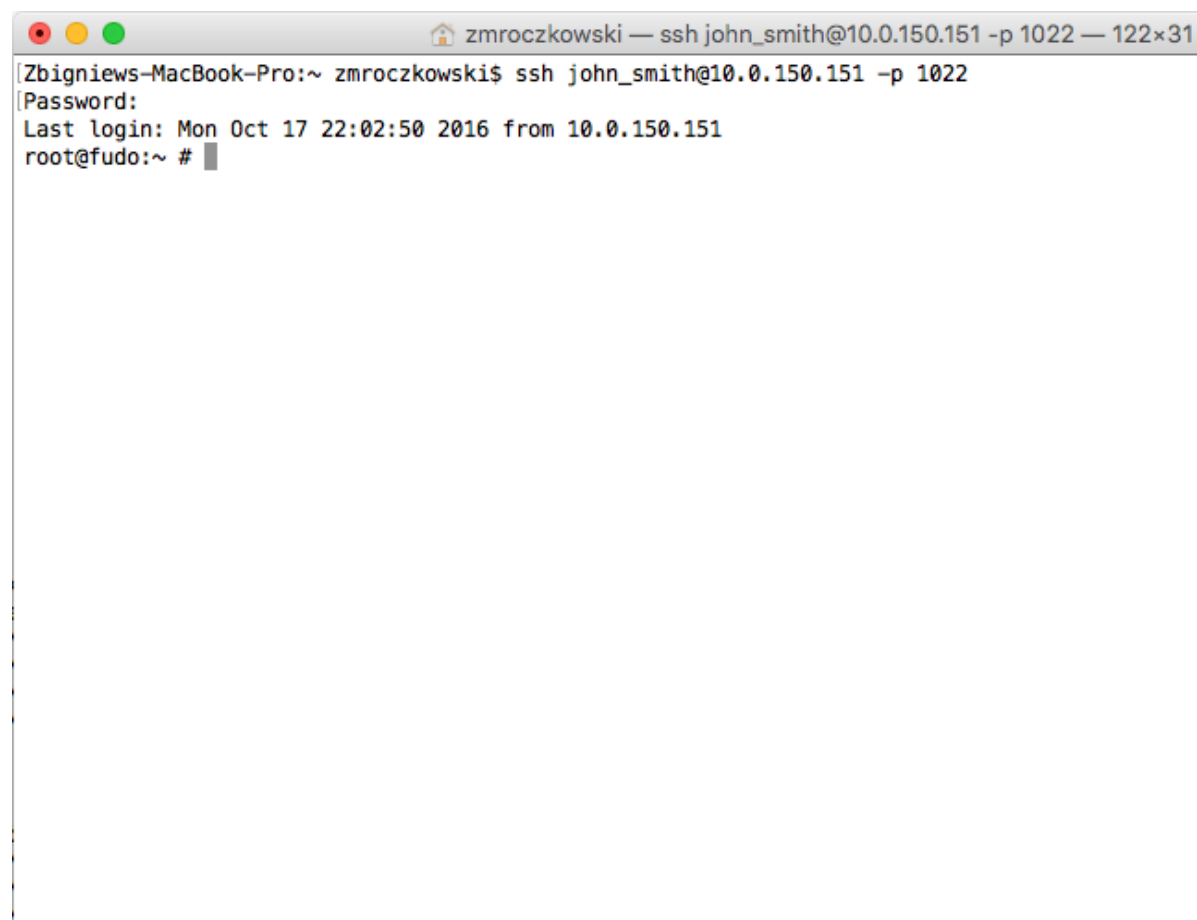
Parameter	Value
<i>General</i>	
Name	the_safe
Notifications	✗
Ask for login reason	✗
Policies	✗
<i>Protocol functionality</i>	
RDP	✗
SSH	✓
VNC	✗
<i>Objects relations</i>	
Users	john_smith
Accounts	server_account
Listeners	ssh_listener

4. Click *Save*.

Establishing connection

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

Example:



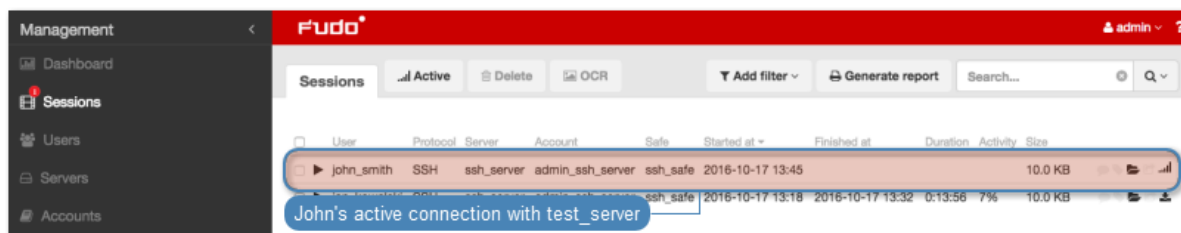
```
zmroczkowski — ssh john_smith@10.0.150.151 -p 1022 — 122x31
Zbigniews-MacBook-Pro:~ zmroczkowski$ ssh john_smith@10.0.150.151 -p 1022
Password:
Last login: Mon Oct 17 22:02:50 2016 from 10.0.150.151
root@fudo:~ #
```

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 Wheel Fudo PAM PAM starts recording user's activities.

Viewing user session

1. Open a web browser and go to the 10.0.8.64 web address.
2. Enter the login and password to login to the WHEEL Wheel Fudo PAM 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](#)

2.3.2 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



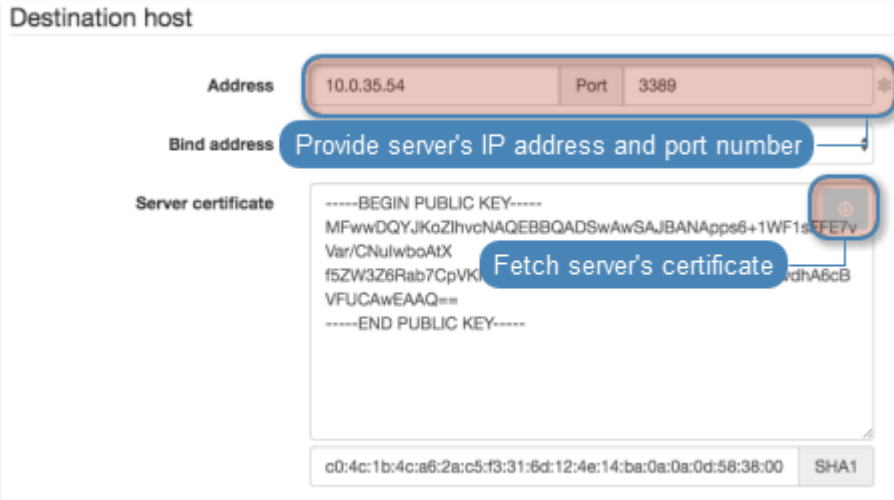
Adding a server

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.



Destination host

Address: 10.0.35.54 Port: 3389

Bind address: Provide server's IP address and port number

Server certificate: Fetch server's certificate

-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANApp6+1WF1s3FE7v
Var/CNulwboAtX
f5ZW3Z8Rab7CpVKI
VFUCAwEAAQ==
-----END PUBLIC KEY-----







c0:4c:1b:4c:a6:2a:c5:f3:31:6d:12:4e:14:ba:0a:0d:58:38:00 SHA1

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.

Connection

Mode: proxy

Local address: 10.0.150.151 Port: 3389

Server public key: MFwWdGf3KozimvChqE8BQd3swW3SdBrFAWt26XtkyubKfP
dA16XJeT1fmg
fLr2W2C0JSDHEXV
CAwEAAQ==
-----END PUBLIC KEY-----

Generate Fudo's private key

Upload Fudo's private key

FUDO's fingerprint

d5:d2:b3:d3:9f:57:59:14:24:20:f4:07:43:29:0a:e4:58:33:ab:e6 SHA1







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	
<i>Protocol functionality</i>	
RDP	
SSH	
VNC	
<i>Objects relations</i>	
Users	john_smith
Accounts	admin_rdp_server
Listeners	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.

The screenshot shows a window titled "Edit Remote Desktops - 10.0.150.151". At the top, there are three tabs: "General" (selected, with a wrench icon), "Session" (with a monitor icon), and "Redirection" (with a folder icon). The "General" tab contains the following fields and options:

- Connection name:** 10.0.150.151
- PC name:** 10.0.150.151
- Gateway:** No gateway configured (dropdown menu)
- Credentials:**
 - User name:** Domain\user
 - Password:** Password
- Resolution:** Native (dropdown menu)
- Colors:** True Color (24 bit) (dropdown menu)
- Full screen mode:** OS X native (dropdown menu)
 - ☒ Start session in full screen
 - ☐ Scale content
 - ☐ Use all monitors

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

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*

2.3.3 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








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

Parameter	Value
Name	mysql_test
Blocked	✗
Protocol	MySQL
Anonymous	✗
Description	MySQL server
<i>Permissions</i>	
Granted users	✗
<i>Destination host</i>	
Address	10.0.35.52
Port	3306
<i>Proxy</i>	
Mode	proxy
Local address	10.0.40.50
Port	3306
Bind address	Any

4. Click *Save*.

Adding a user

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	john11
Repeat password	john11

4. Click *Save*.

Adding a connection

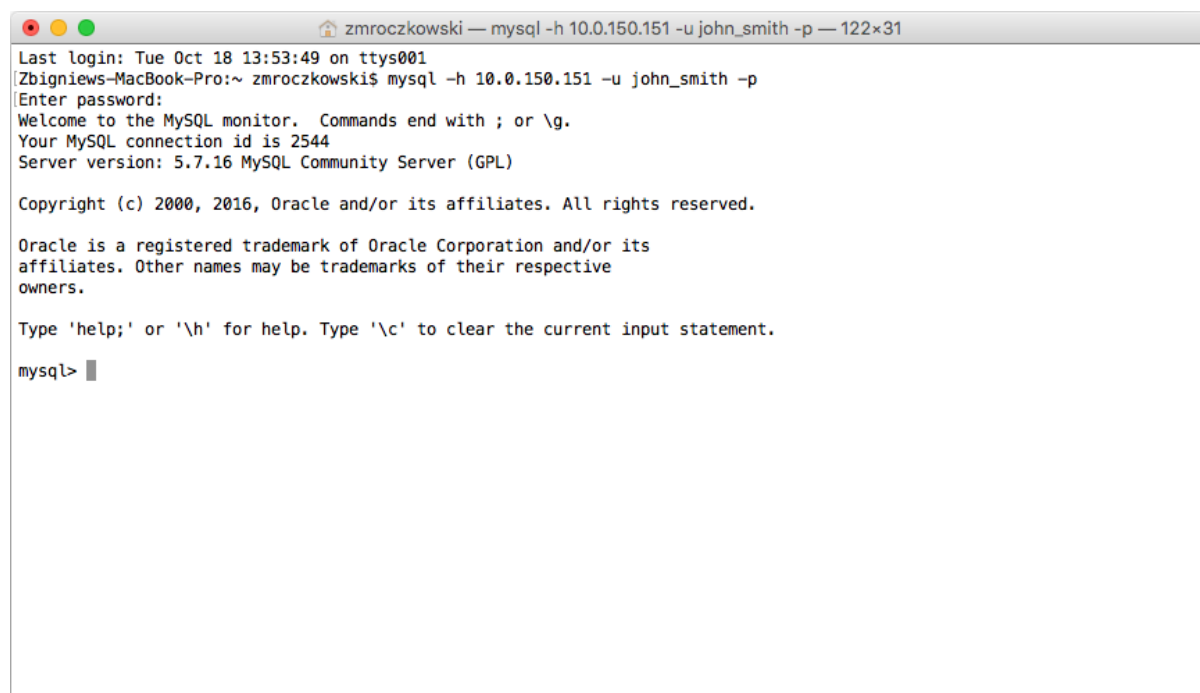
1. Select *Management > Connections* to access the connections configuration page.
2. Click the Add button.
3. Provide connection details:

Parameter	Value
Name	mysql
Blocked	✗
Notifications	✗
Users	john_smith
Sessions recording	Complete
OCR sessions	✗
Delete session data after	10 days
<i>Protocol functionality</i>	
RDP Functionality	default settings
SSH Functionality	default settings
VNC Functionality	default settings
<i>Permissions</i>	
Granted users	✗
<i>Servers</i>	
Server	mysql_test
Policy	✗
Replace user	✓ admin
Replace secret	✓ Replace with password
Password	password
Repeat password	password

4. Click *Save*.

Establishing connection with a MySQL database

1. Launch a command line interface client.
2. Enter `mysql -h 10.0.40.50 -u john_smith -p`, to connect to the database server.
3. Enter the user's password.

A screenshot of a terminal window on a Mac. The title bar shows the user 'zmroczkowski' and the command 'mysql -h 10.0.150.151 -u john_smith -p'. The terminal output shows the last login time, the command being executed, the password prompt, and a successful connection to the MySQL monitor. It displays the MySQL version (5.7.16) and copyright information. The prompt 'mysql>' is visible at the bottom.

```
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.

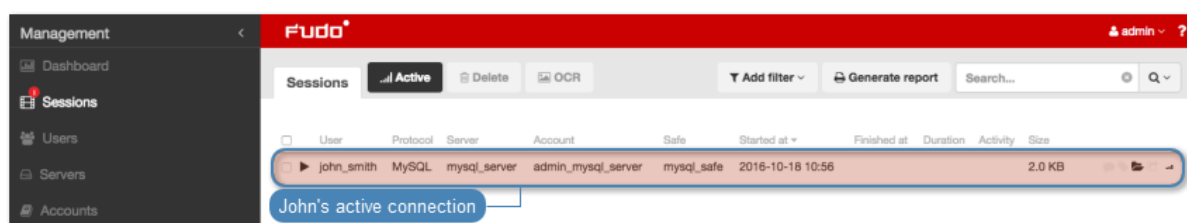
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

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 Terminate

INIT	2016-10-18 10:56:52.032748
<p>Protocol version: 10 Server version: 5.7.16 Connection ID: 2545 Authentication plugin name: mysql_native_password</p> <p>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_FLAG, CLIENT_CONNECT_WITH_DB, CLIENT_FOUND_ROWS, CLIENT_PLUGIN_AUTH_LENENC_CLIENT_DATA, CLIENT_LOCAL_FILES, CLIENT_COMPRESS, CLIENT_MULTI_STATEMENTS, CLIENT_LONG_PASSWORD, CLIENT_ODBC, CLIENT_PS_MULTI_RESULTS, CLIENT_PROTOCOL_41</p>	
OK	2016-10-18 10:56:52.032748
Affected rows: 0 Last inserted_id rows: 0 Status: 2 Warnings: 0 Info:	
COM_QUERY	2016-10-18 10:56:52.034748
<p>Query:</p> <pre>select @@version_comment limit 1</pre>	

00:00:00	00:04:02	Info Share Terminate Pause
----------	----------	--

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*

2.3.4 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








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

Parameter	Value
Name	http_www
Blocked	
Protocol	HTTP
HTTP timeout	900
Anonymous	
Ask for login reason	
Description	Web server
<i>Permissions</i>	
Granted users	
<i>Destination host</i>	
Address	www.wheelsystems.com
Port	80
HTTP host	
Use TLS	
<i>Proxy</i>	
Mode	Proxy
Local address	10.0.40.50
Port	8080

4. Click *Save*.

Adding a user

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	john11
Repeat password	john11

4. Click *Save*.

Adding connection

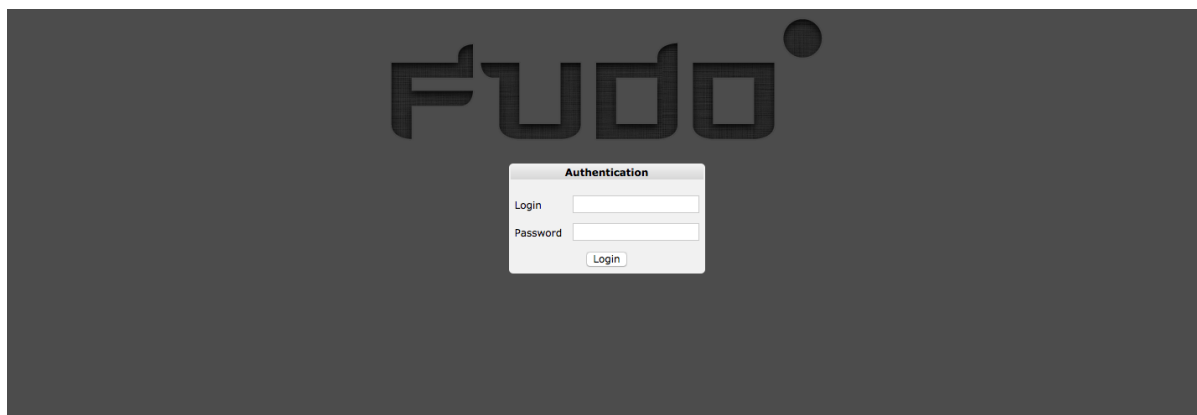
1. Select *Management > Connections*.
2. Click *+ Add*.
3. Provide connection details:

Parameter	Value
Name	http-test
Blocked	✗
Notifications	✗
Users	john_smith
Sessions recording	Complete
OCR sessions	✗
Delete session data after	10 days
<i>Protocol functionality</i>	
RDP Functionality	default settings
SSH Functionality	default settings
VNC Functionality	default settings
<i>Permissions</i>	
Granted users	✗
<i>Servers</i>	
Server	http_www
Policy	✗

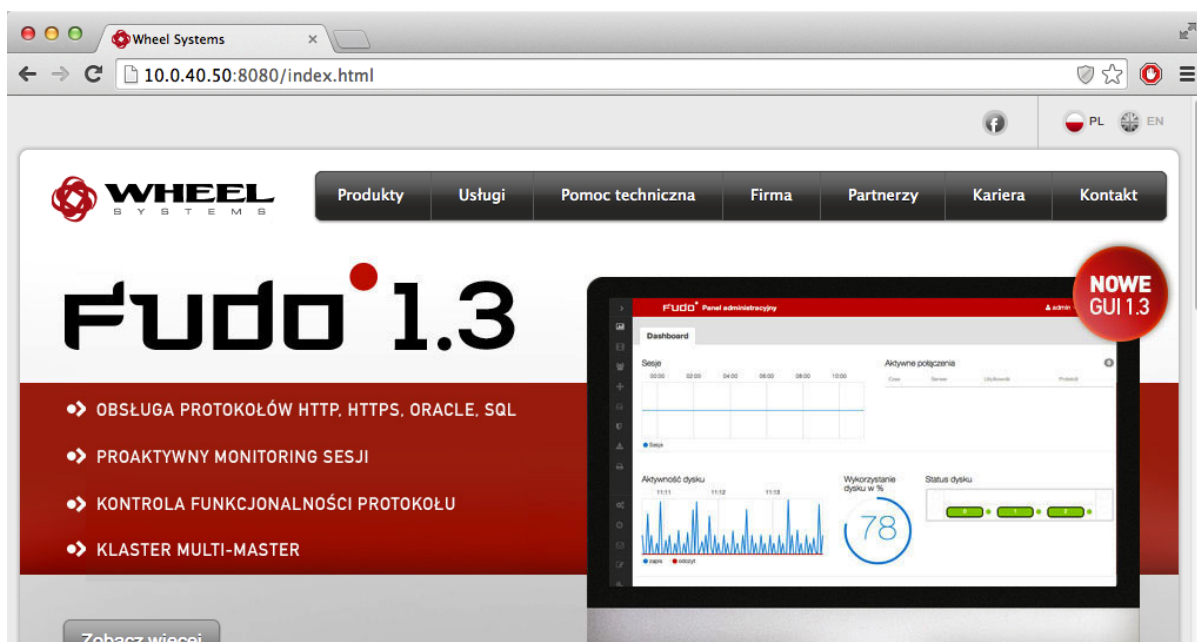
4. Click *Save*.

Connecting to remote resource

1. Launch a web browser.
2. Go to the 10.0.40.50:8080 web address.
3. Enter user login and password and press the [Enter] key or click the *Login* button.

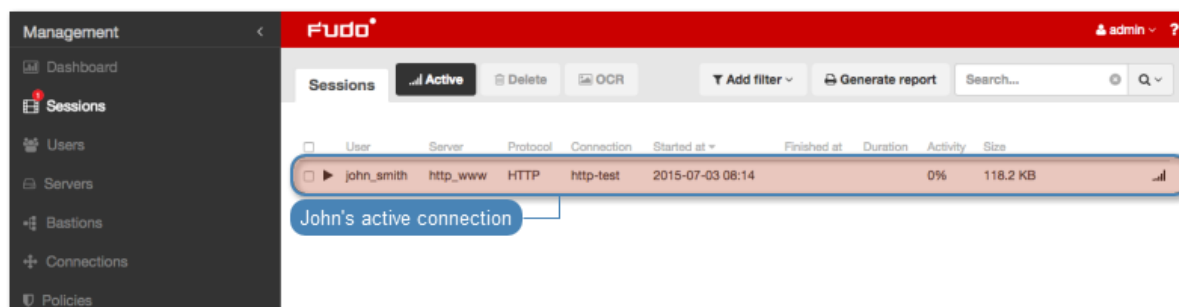





4. Continue browsing the website.



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 848388532111147070

<https://10.0.150.151/sessions/848388532111147070/?i=1&q=on&qc=on&live=2016-10-18+11%3A19%3A02&qo=on>

Session: 848388532111147070, User: john_smith

Terminate

/webman/resources/images/icon_dsm_48.png? v=4398	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	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	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*

2.3.5 Telnet

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



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
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	
Login reason	
Notifications	
Policies	
<i>Protocol functionality</i>	
RDP	
SSH	
VNC	
<i>Permissions</i>	
Granted users	
<i>Objects relations</i>	
Users	john_smith
Accounts	admin_telnet_server
Listeners	telnet_listener

- Click *Save*.

Establishing a telnet connection with the remote host

- Launch telnet client of your choice.
- 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 '^['.
```

- Provide user authentication information defined on Wheel Fudo PAM:

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

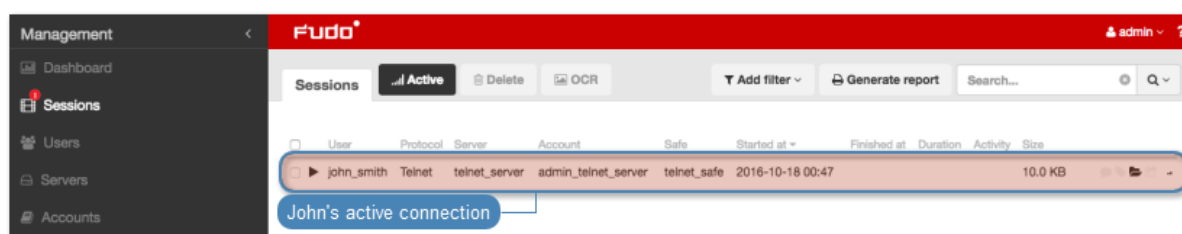
- Provide user authentication information defined on the target host:

```
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*

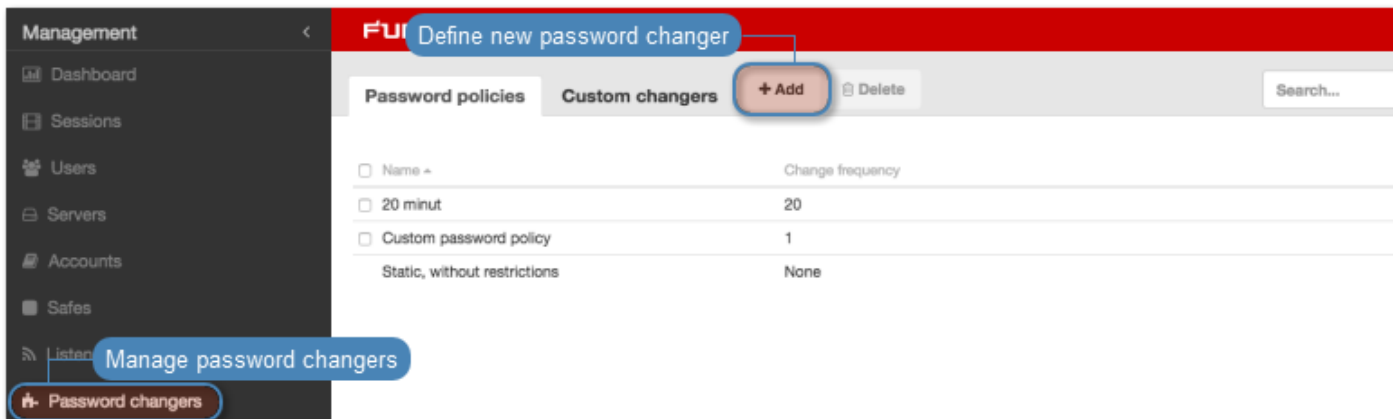
2.3.6 Setting up password changing on a Unix system

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

Configuration

Adding a password change policy

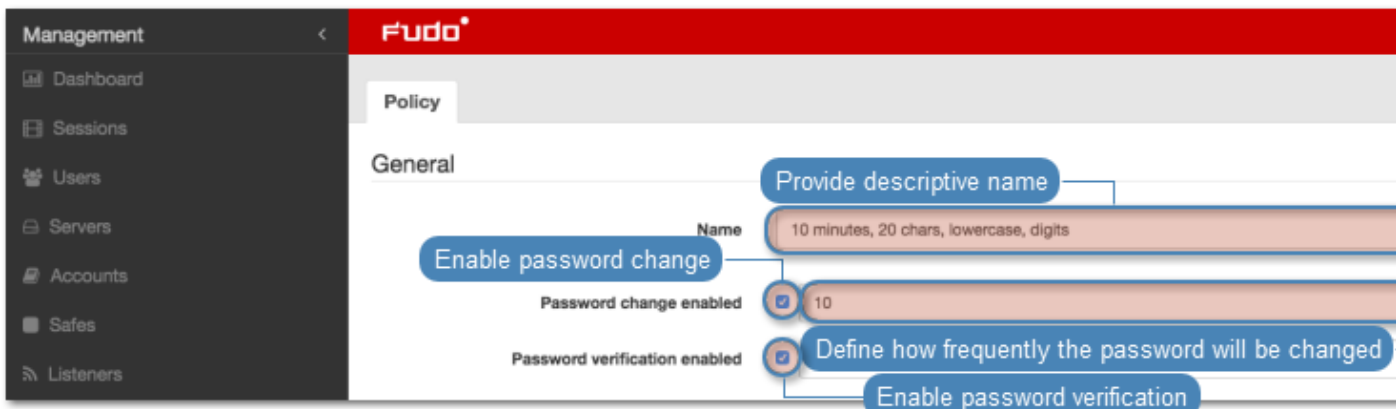
1. Select *Management > Password changers*.
2. Click *+ Add* to create a new password changing policy.



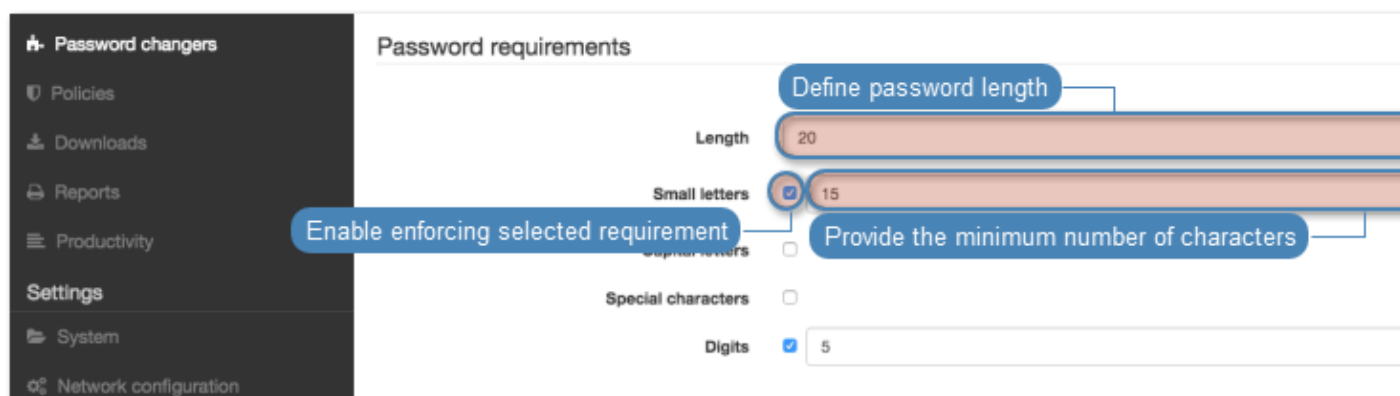
3. Provide password change policy name.

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.



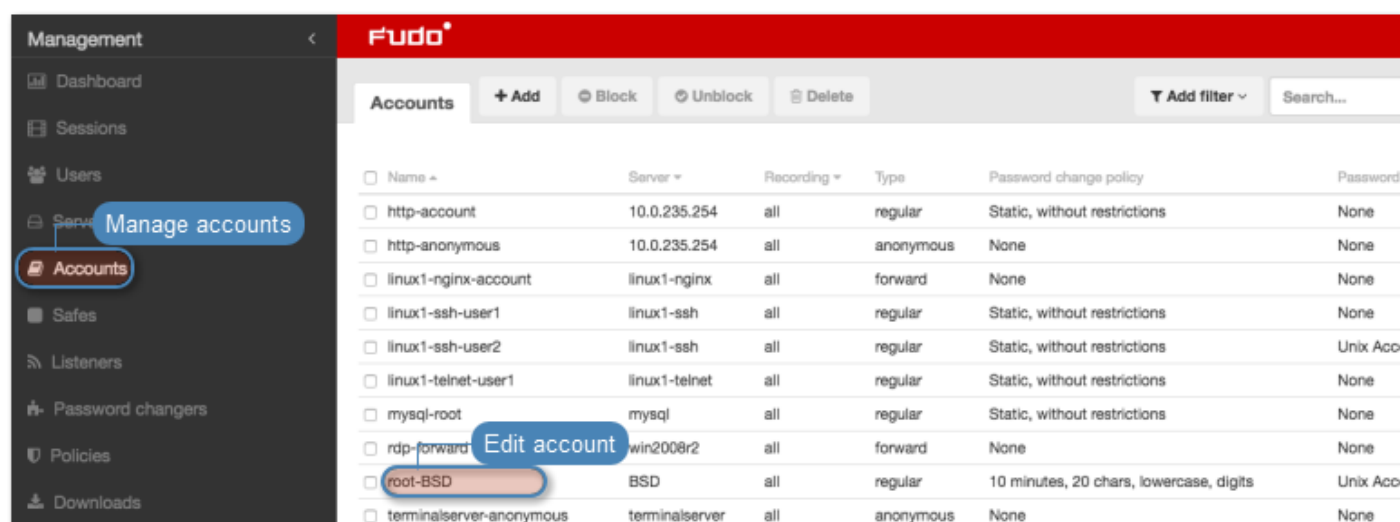
6. Provide the number of characters comprising the password.
7. Select desired password complexity options and provide the minimal number of characters for each.



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](#)

2.4 Dashboard

Wheel Fudo PAM dashboard page enables quick access to essential status information and allows executing shutdown and restart procedures.

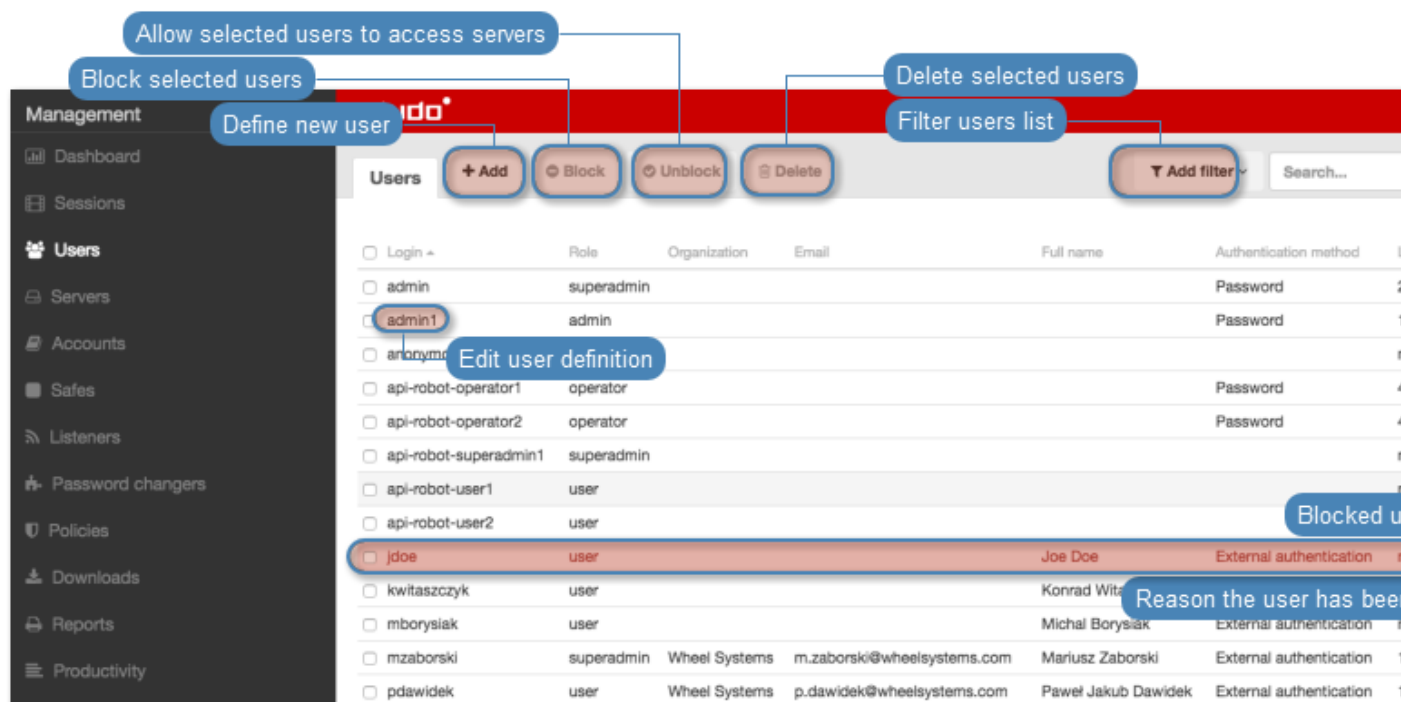


Related topics:

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

2.5 Users

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.



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.

2.5.1 Adding 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*.
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. Define configuration parameters.

Parameter	Description
<i>General</i>	
ID	User unique identifier (<i>applicable only when editing an existing object</i>).
Synchronize with LDAP	Synchronize given user with LDAP service (<i>applicable only when editing an existing object</i>).
Login	Unique user login.
Blocked	Select to disable access to monitored servers.
Account validity	Define account validity period.
Role	Select role determining user access rights.
Preferred language	Select user's preferred language.
Safes	Select safes to grant access to monitored servers.
Note: <ul style="list-style-type: none"> • SSH_safe indicates that the Reveal password option is disabled. • RDP_safe denotes that the Reveal password option is enabled. 	
Full name	User's full name for identification purposes.
Email	User's email address.
Organization	Organization assignment.
Phone	Optional contact information.
AD domain	Active Directory domain to which the user is assigned to.
LDAP base	LDAP base to locate user in the directory service.
<i>Permissions</i>	
Granted users	Users allowed to manage given object.
<i>Authentication</i>	
Type	Select user authentication method.
Password	
Password	Provide static password.
Repeat password	
Delete	Select to delete given authentication method.
External authentication	
External authentication source	Select external authentication source used to verify user's credentials.
SSH Key	
Public key	Paste or upload user's public key.

4. Click *+ Add authentication method* to define more authentication methods.
5. Define time access policy.
 - Click desired safe object.

Preferred language: English

Safes: RDP SSH portal

Full name:

Email:

Click to define access time policy to the safe

Click to enable time policy for the given safe

Reveal password

Allow user to see passwords

Click to define access time interval

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

Access time policy

Enable time policy

Reveal password

00:00 23:59

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Click to enable time policy for the given safe

Click to define access time interval

Cancel OK

- Click *OK*.
6. Click *Save*.

2.5.2 Editing a user

1. Select *Management > Users*.
2. Find desired user definition.
3. Click user's login to access its configuration parameters.
4. Modify configuration parameters as desired.

Note: Unsaved changes are marked with an icon.

General

Unsaved changes

Login john_smith

Blocked ☐

Account validity Indefinite

Role operator

5. Click *Save*.

Blocking and unblocking a user

Warning: Blocking a user will terminate its current connections.

1. Select *Management > Users*.
2. Find and select the desired user definition.
3. Click *Block* to disallow the user to connect to servers or *Unblock* to allow user to connect to servers.
4. Provide a descriptive reason for blocking the given user and click *Confirm*.

2.5.3 Deleting a user

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

1. Select *Management > Users*.
2. Find and select the desired user definition.
3. Click *Delete*.
4. Confirm resource deletion.

2.5.4 Roles

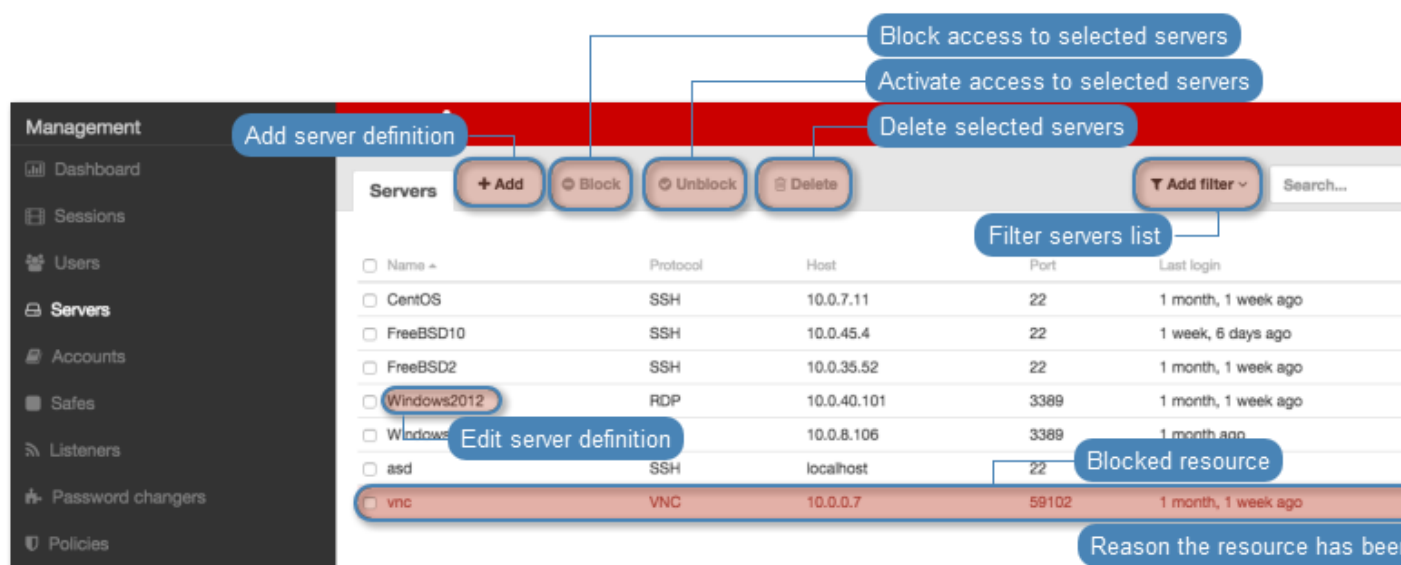
Role	Access rights
user	Connecting to servers as defined in connections, to which the user has been assigned.
operator	<ul style="list-style-type: none">• logging in to administration panel• browsing objects: servers, users, bastions, connections, to which the user has been assigned sufficient access permissions• blocking/unblocking objects: servers, users, bastions, connections• generating reports on demand and subscribing to periodic reports• activating/deactivating email notifications• converting sessions and downloading converted content
admin	<ul style="list-style-type: none">• logging in to administration panel• managing objects: servers, users, bastions, connections, to which the user has been assigned sufficient access permissions• blocking/unblocking objects: servers, users, bastions, connections• generating reports on demand and subscribing to periodic reports• activating/deactivating email notifications• converting sessions and downloading converted content• 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*

2.6 Servers

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



Adding 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.

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. Define server parameters.

Parameter	Description
<i>General</i>	
Name	Object name.
Blocked	Select if defined object should be unavailable after creation.
Login reason	Display prompt requiring users to input login reason.
Protocol	Server communication protocol.
HTTP timeout (<i>HTTP only</i>)	Idle time after which the user will be required to authenticate again.
Enable SSLv2 support (<i>HTTP only</i>)	SSL version 2 support.
Enable SSLv3 support (<i>HTTP only</i>)	SSL version 3 support.
Security (<i>RDP only</i>)	RDP connection's security mode. Enhanced RDP Security (TLS) + MLA allows hiding Wheel Fudo PAM's login screen upon connecting to destination host.
Description	Description helping to identify defined resource.
<i>Permissions</i>	
Granted users	Users allowed to manage given object. The list contains users with the admin or the operator role. For more information on user access rights refer to the <i>Security</i> topic.
<i>Destination host</i>	
Address	IP address of the destination server along with the port number on which the service being monitored is running.
Bind address	
Server certificate (<i>RDP and HTTPS only</i>)	Allows downloading server's SSL certificate for verification purposes.
Server public key (<i>SSH only</i>)	Allows downloading server's SSL certificate for verification purposes.
HTTP host (<i>HTTP only</i>)	Allows providing a specific resource on the server to be monitored.

4. Click *Save*.

Modifying a server definition

1. Select *Management > Servers*.
2. Find desired server definition.
3. Click server name to access server configuration parameters.
4. Modify configuration values as needed.

Note: Unsaved changes are marked with an icon.

General

Unsaved changes

Login john_smith

Blocked ☐

Account validity Indefinite

Role operator

5. Click *Save*.

Blocking and unblocking 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 server definition.
3. Click *Block* to block access to given resource or *Unblock* to allow connecting to selected server.
4. Provide descriptive reason for blocking given resource and click *Confirm*.

Deleting a server definition

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

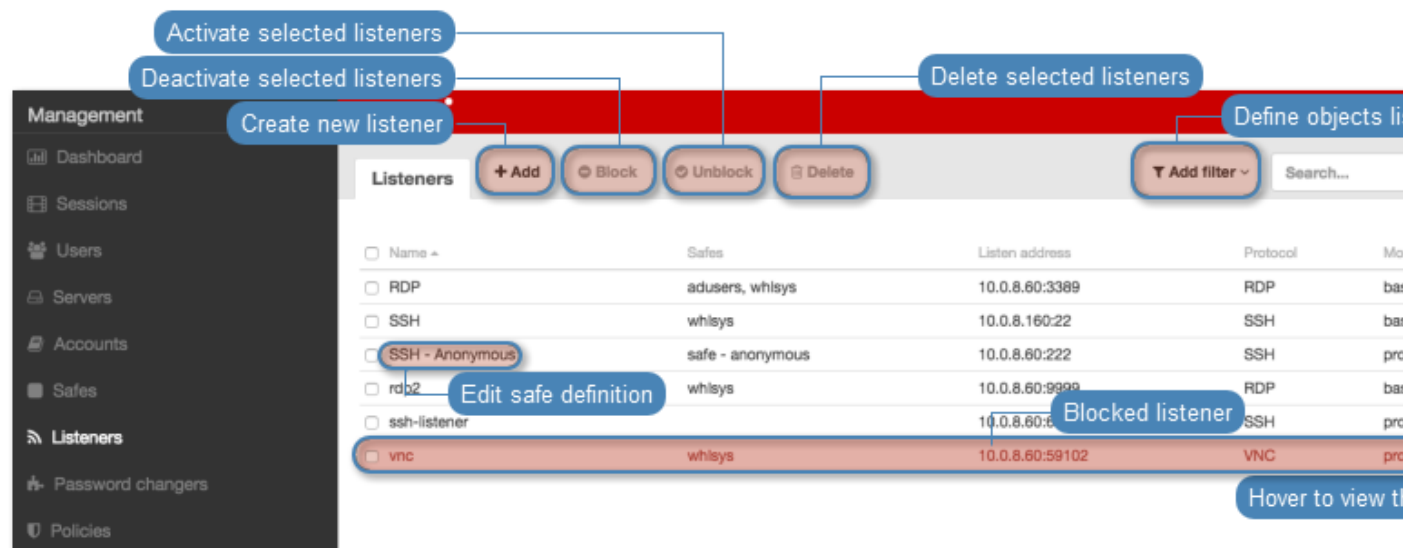
1. Select *Management > Servers*.
2. Find and select desired server definition.
3. Click *Delete*.
4. Confirm deleting selected objects.

Related topics:

- *Data model*
- *System initiation*
- *Servers*
- *Accounts*
- *Listeners*

2.7 Listeners

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



Adding a listener

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

Note:

- A *proxy* type listener can link to only one account to a server with the same protocol through different safes.
- A *bastion* type listener cannot link to an anonymous account on a server with the same protocol as the listener's protocol.
- 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*.

1. Select *Management > Listeners*.
2. Click *+ Add*.
3. Define configuration parameters.

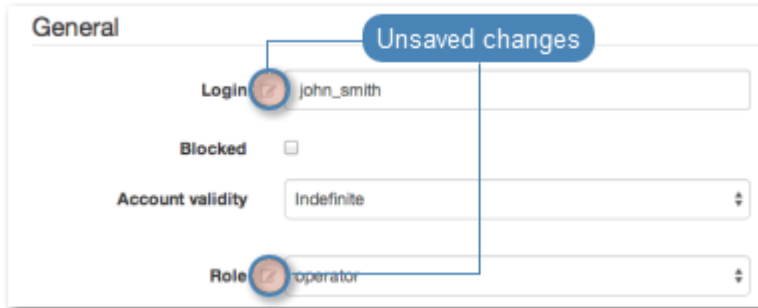
Parameter	Description
<i>General</i>	
Name	Object name.
Blocked	Select if defined object should be unavailable after creation.
Protocol	Server communication protocol.
HTTP timeout (<i>HTTP only</i>)	Idle time after which the user will be required to authenticate again.
Enable SSLv2 support (<i>HTTP only</i>)	SSL version 2 support.
Enable SSLv3 support (<i>HTTP only</i>)	SSL version 3 support.
Security (<i>RDP only</i>)	RDP connection's security mode. Enhanced RDP Security (TLS) + NLA allows hiding Wheel Fudo PAM's login screen upon connecting to destination host.
Announcement (<i>RDP/VNC only</i>)	Local server announcement displayed on user login screen.
<i>Permissions</i>	
Granted users	Users allowed to manage given object.
<i>Connection</i>	
Mode	<p>Select connection mode to determine how the user will connect to target hosts.</p> <ul style="list-style-type: none"> • <i>Transparent</i> - 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 <i>bridge mode</i>. • <i>Proxy</i> - user connects to the target host by providing Wheel Fudo PAM IP address and port number which unambiguously identifies target host. • <i>Gateway</i> - 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 <i>bridge mode</i>. • <i>Bastion</i> - user connects to the target host by including its name in the login string, e.g. <code>ssh john_smith@mail_server@10.0.35.10</code>.
Local address (<i>applicable to bastion and proxy modes</i>)	An IP address and a port number used for connecting to the target host. A unique combination of those parameters allows for unambiguous identification of the target server. For more information on IP address assignment, refer to the <i>Network settings</i> topic.
Interface (<i>applicable to gateway and transparent modes</i>)	Network interface used for communication with monitored servers.
Use HTTPS (<i>HTTP only</i>)	Select this option to have connections to Wheel Fudo PAM encrypted with the SSL protocol.
HTTPS certificate	Wheel Fudo PAM SSL certificate required for establishing secure HTTP connections.
HTTPS private key (<i>HTTPS only</i>)	Wheel Fudo PAM SSL private key required for establishing secure HTTP connections.
TLS certificate (<i>Enhanced Security RDP only</i>)	TLS certificate for RDP connections requiring Enhanced RDP Security.
Server public key (<i>RDP only</i>)	Proxy server's public key.

4. Click *Save*.

Modifying a listener

1. Select *Management > Listeners*.
2. Find and click desired listener to access its configuration parameters.
3. Modify configuration values as needed.

Note: Unsaved changes are marked with an icon.



-
4. Click *Save*.

Blocking and unblocking a listener

Blocking a listener disables access for users using it to connect to servers.

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

1. Select *Management > Listeners*.
2. Find and select desired listener.
3. Click *Block* to disable access to given resource or *Unblock* to enable the access.
4. Provide descriptive reason for blocking given resource and click *Confirm*.

Deleting a server definition

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

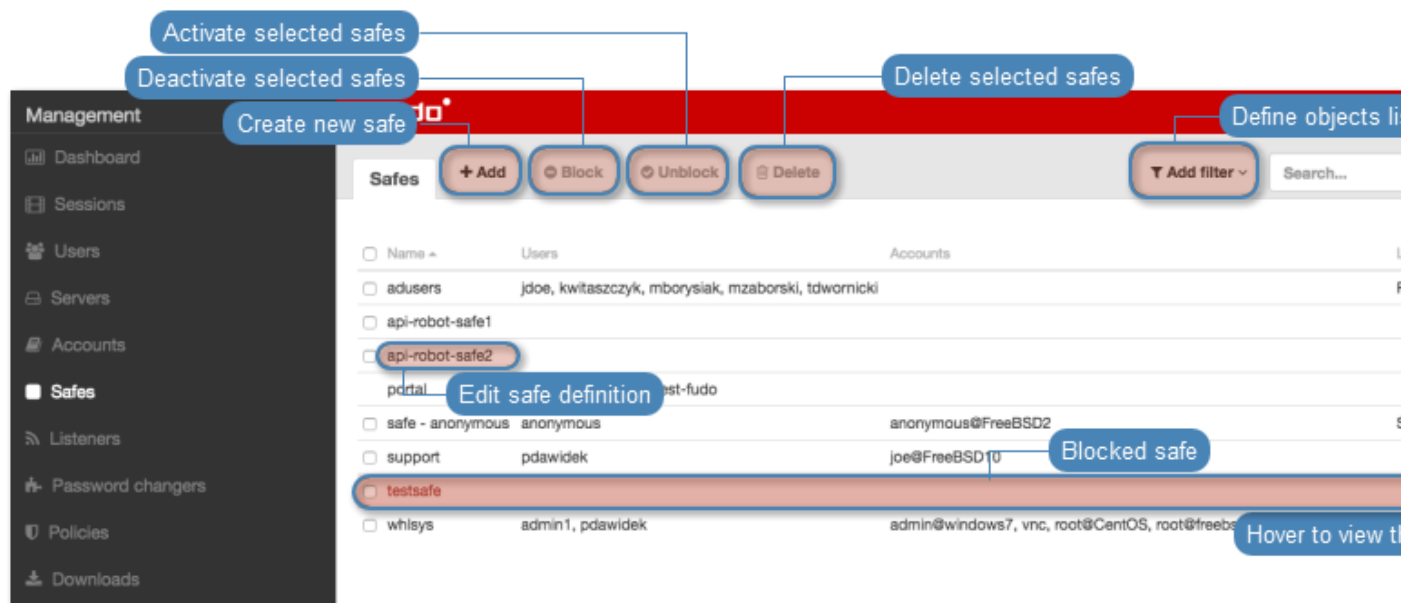
1. Select *Management > Listeners*.
2. Find and select desired listener.
3. Click *Delete*.
4. Confirm deleting selected objects.

Related topics:

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

2.8 Safes

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



Adding 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.

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.

1. Select *Management > Safes*.
2. Click *+ Add*.
3. Define configuration parameters.

Parameter	Description
<i>General</i>	
Name	Object name.
Notifications	Select email notifications sent when a selected event occurs.

Continued on next page

Table 1 – continued from previous page

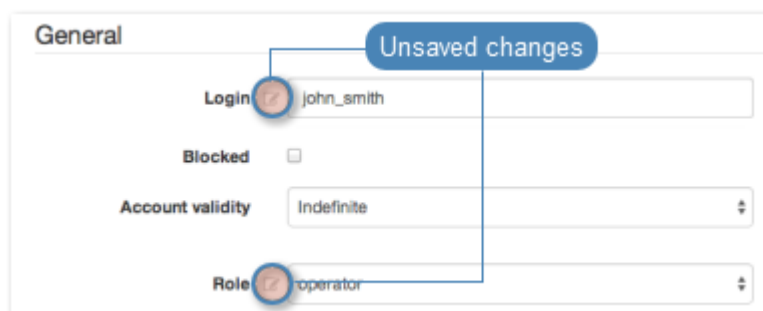
Parameter	Description
Login reason	Prompt the user with a login reason when connecting to the server.
Notifications	Select events triggering email notifications sent to system administrator.
Policies	Assign monitored policies
<p>Note: Policies are definitions of patterns which occurrence can result in terminating connection, blocking given user and notifying system administrator. Refer to the <i>Policies</i> topic for more information on defining patterns and policies.</p>	
<i>Protocol functionality</i>	
<i>RDP Functionality</i>	
Clipboard redirection	Feature allowing to copy and paste text between local computer and remote system using clipboard.
Sound redirection	Allows playing sounds from remote system on local machine.
Device redirection	Enables using devices (printers, CD drives, Plug and Play devices, etc.) connected to remote host as well as accessing mapped network drives.
Dynamic virtual channels	Extensions enabling implementing additional in RDP connections.
Audio input redirection	Local audio input redirection to remote system.
Multimedia redirection	Enables processing media stream on local machine, allowing to lower remote server load and session data transfer.
Maximum RDP sessions resolution	Enables limiting RDP sessions resolution to selected value.
<i>SSH Functionality</i>	
Sessions	Establishing SSH connections with remote servers.
Port forwarding	Local and remote SSH connection tunneling.
Terminal	Establishing SSH connections using terminal.
Environment	Access to remote system's environment.
X11	Running graphical applications on remote host.
SSH Agent forwarding	Forwarding key by the SSH agent in a chain of subsequent SSH connections.
Shell	Ability to execute shell commands.
SCP	Ability to copy files over SSH connection.
<i>VNC Functionality</i>	
Client Cut Text	Clipboard support on client system.
Server Cut Text	Clipboard support on server side.
<i>Object relations</i>	
Users	Assign users allowed to access servers over this object.
Accounts	Define safes to accounts assignment.
Listeners	Select listeners determining server access mode.

4. Click *Save*.

Editing a safe

1. Select *Management > Safes*.
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*.

Deleting a safe

Warning: Deleting a safe definition will terminate all current connections to servers which use selected safe to regulate access to servers.

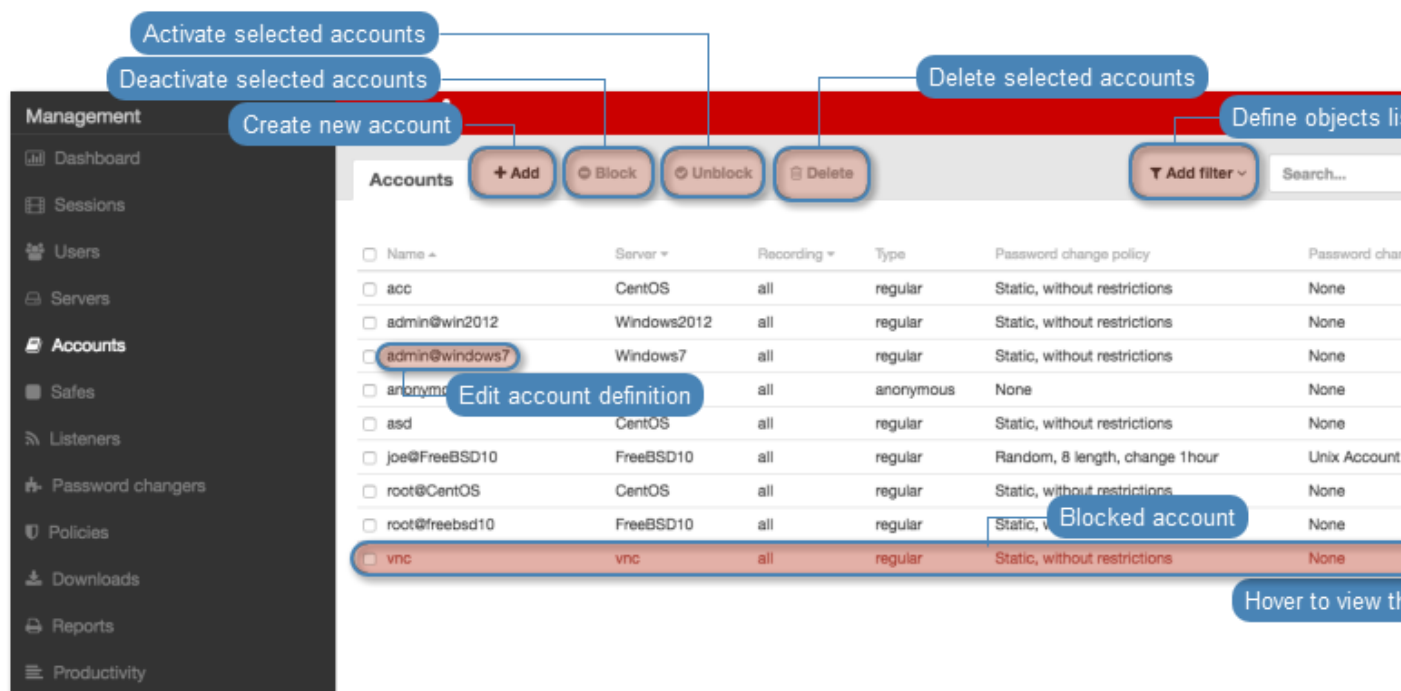
1. Select *Management > Safes*.
2. Find and select desired objects.
3. Click *Delete*.
4. Confirm deletion of selected objects.

Related topics:

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

2.9 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.



Defining 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.

1. Select *Management* > *Accounts*.
2. Click *+ Add*.
3. Define configuration parameters.

Parameter	Description
<i>General</i>	
Name	Object name.
Account type	Select account type: <ul style="list-style-type: none"> • Regular - Password substitution? • Anonymous - When connecting to an anonymous server, Wheel Fudo PAM does not authenticate the user against local database, but forwards login credentials to the destination server and after successful authentication, it continues recording the session. • Forward - User login credentials are forwarded to the target host.
Session recording	Select session recording option.

Continued on next page

Table 2 – continued from previous page

Parameter	Description
<code>all</code>	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.
<code>raw</code>	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.
<code>none</code>	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.
<hr/>	
OCR sessions	Enable RDP sessions content indexing.
OCR language	Select what language the processed content is in.
Delete session data after	Decide how long Wheel Fudo PAM will store session data before deleting it.
<hr/>	
<i>Permissions</i>	
Granted users	Determine users allowed to manage given object.
<hr/>	
<i>Server</i>	
Server	Assign account to a server.
<hr/>	
<i>Credentials</i>	
Domain	Account domain assignment.
<hr/>	
Note: In case of MS SQL connections, providing the <i>domain</i> will result in Wheel Fudo PAM using NTLM authentication mechanism when establishing connections with monitored hosts. Otherwise Wheel Fudo PAM will use the SQL Server Authentication method. SQL Server Authentication is always used to authenticate users initiating connections, whether the <i>domain</i> is set or not.	
<hr/>	
<hr/>	
Login	Login used for authenticating on monitored server.
Replace secret	Select password replacement option.
	<code>with password</code>
Password	Static password.
Repeat password	
	<code>with key</code>
Public key	
	<code>with password from external repository</code>
External passwords repository	Select passwords repository used to manage credentials to selected account.
Password change policy	Select the policy, which determines password change details.
<hr/>	
<i>Password changer</i>	

Continued on next page

Table 2 – continued from previous page

Parameter	Description
Password changer	Select the password changer used for managing password to given account.
Unix Account over SSH	
Privileged user	User login with password changing privileges.
Privileged user password	
Windows account over WMI	
Privileged user	User login with password changing privileges.
Privileged user password	
MySQL User Account on Unix Server over SSH	
SSH user	SSH user login.
SSH password	SSH user password.
SSH server address	SSH server IP address.
SSH server port	SSH server port number.
Privileged user	User login with password changing privileges.
Privileged user password	Privileged user password.
Cisco Account over Telnet	
Privileged mode password	
Privileged user	User login with password changing privileges.
Privileged user password	Privileged user password.
Cisco Enable Password over Telnet	
Privileged mode password	Password used for entering privileged mode.
Privileged user	User login with password changing privileges.
Privileged user password	Privileged user password.
Cisco Account over SSH	
Privileged mode password	
Privileged user	User login with password changing privileges.
Privileged user password	Privileged user password.
Cisco Enable Password over SSH	
Privileged mode password	Password used for entering privileged mode.
Privileged user	User login with password changing privileges.
Privileged user password	Privileged user password.
LDAP	

Continued on next page

Table 2 – continued from previous page

Parameter	Description
Privileged user	User login with password changing privileges.
<hr/>	
Note: <ul style="list-style-type: none">• Privileged user must have the domain included in its name, e.g. <code>domain_name\administrator</code>.• Wheel Fudo PAM allows using full FQDN name as the domain, e.g. <code>domain_name.corp</code>.• Wheel Fudo PAM allows providing privileged user name as <code>administrator@domain_name</code>.	
<hr/>	
Privileged user password	Privileged user password.
LDAP base	Path to the location where the user for which the password is changed is stored.
LDAP server CA certificate	CA public key used for signing the LDAP server's certificate.

Note:

- Server's name (IP address) associated with this account must be the same as it appears in the TLS certificate used by the server. If the server's name in the certificate is `ad.example.com`, then the server's address configured on Fudo must be `ad.example.com`.
 - Active Directory server must have the LDAPS service enabled.
-

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, proceed as follows.

- From the *Type* drop-down list, select **forward**.
 - In the *Credentials* section, select the *Two-fold authentication* option.
-

4. Click *Save*.

Editing an account

1. Select *Management > Accounts*.
 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.

The screenshot shows a 'General' configuration window. At the top right is a blue button labeled 'Unsaved changes'. Below it are four fields: 'Login' with the value 'john_smith', 'Blocked' with an unchecked checkbox, 'Account validity' with the value 'Indefinite', and 'Role' with the value 'operator'. Red circles are drawn around the 'Login' and 'Role' fields. A blue line connects these two circles and extends upwards to the 'Unsaved changes' button, indicating that changes to these fields are not yet saved.

4. Click *Save*.

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:

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

2.10 Password changers

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

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

2.10.1 Password changer policy

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

Defining a password changer policy

1. Select *Management > Password changers*.
2. Click *+ Add*.
3. Define configuration parameters.

Parameter	Description
<i>General</i>	
Name	Object name.
Password change enabled	Enable password changing and determine how often the password should be changed.
Password verification enabled	Enable password verification and specify how often the password should be verified.
<i>Password requirements</i>	
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.

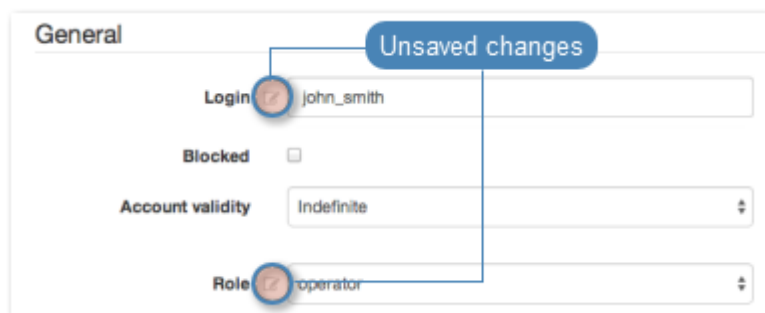
Note: The sum of the enforced password requirements cannot be greater than the specified password length.

4. Click *Save*.

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*.

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.

2.10.2 Custom password changers

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

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%%`).

7. Provide optional comments.
8. Repeat steps 5 through 7 to add additional commands.
9. Repeat steps 5 through 8 and define a password verification commands in the *Password verification commands list* section.

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

10. Click *Save*.

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*.

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:

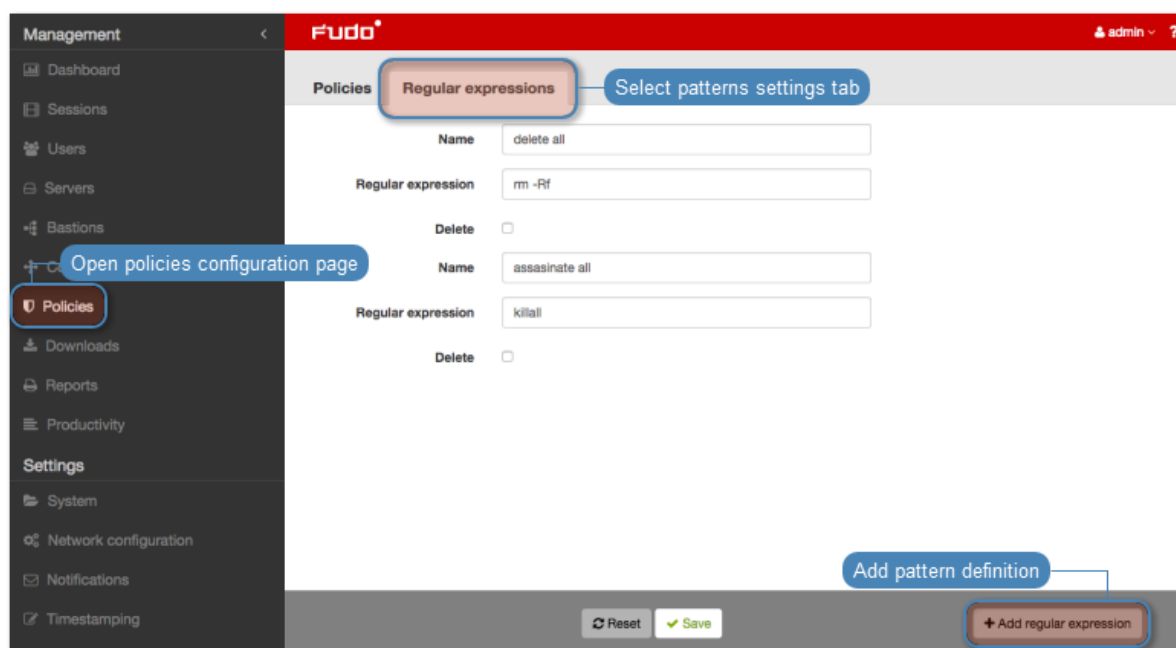
- [Data model](#)
- [System initiation](#)
- [Servers](#)

2.11 Policies

Policies are patterns definitions facilitating proactive session monitoring. In case a defined pattern is detected, Wheel Fudo PAM can automatically pause or terminate given connection, block the user and send notification to Wheel Fudo PAM administrator.

Defining patterns

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



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

Note: Patterns can be defined as regular expressions.

Wheel Fudo PAM does not recognize expressions which use backslash character, e.g. `\d`, `\D`, `\w`, `\W`.

6. Repeat steps 3-5 to define additional patterns.

7. Click Save.

Note: Regular expressions examples

Command `rm`

`(^[^a-zA-Z])rm[:space:]`

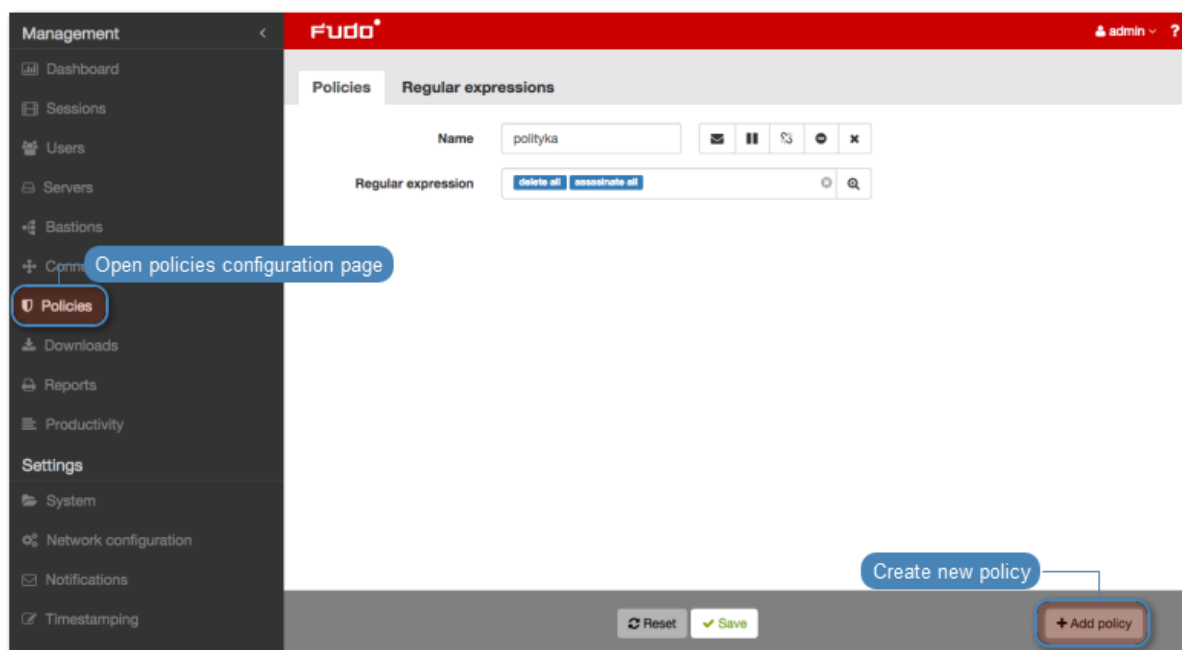
Command `rm -rf` (also `-fr`; `-Rf`; `-fR`)

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

Command `rm file` `(^[^a-zA-Z])rm[:space:]+([[:space:]]+([[:space:]]*)?)?/full/path/to/a/file([[:space:]]|\\;|$(^[^a-zA-Z])rm[:space:]+.*justafilename`





Defining policies

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



3. Enter policy name.

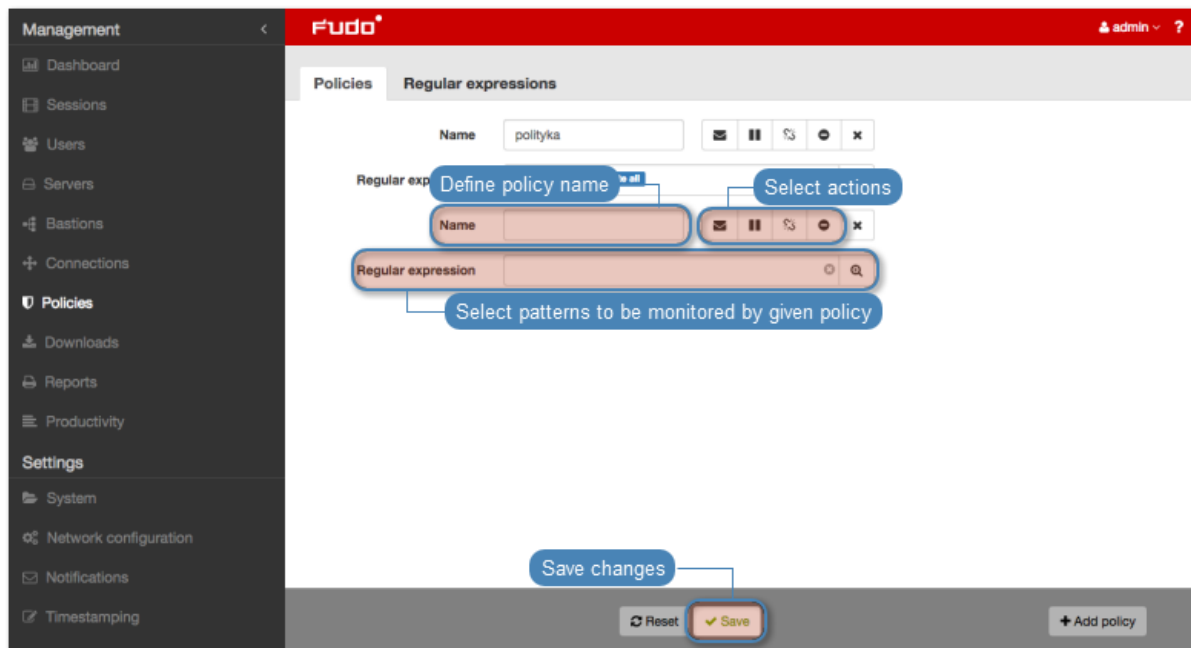
4. Select actions.

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

Note: 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*

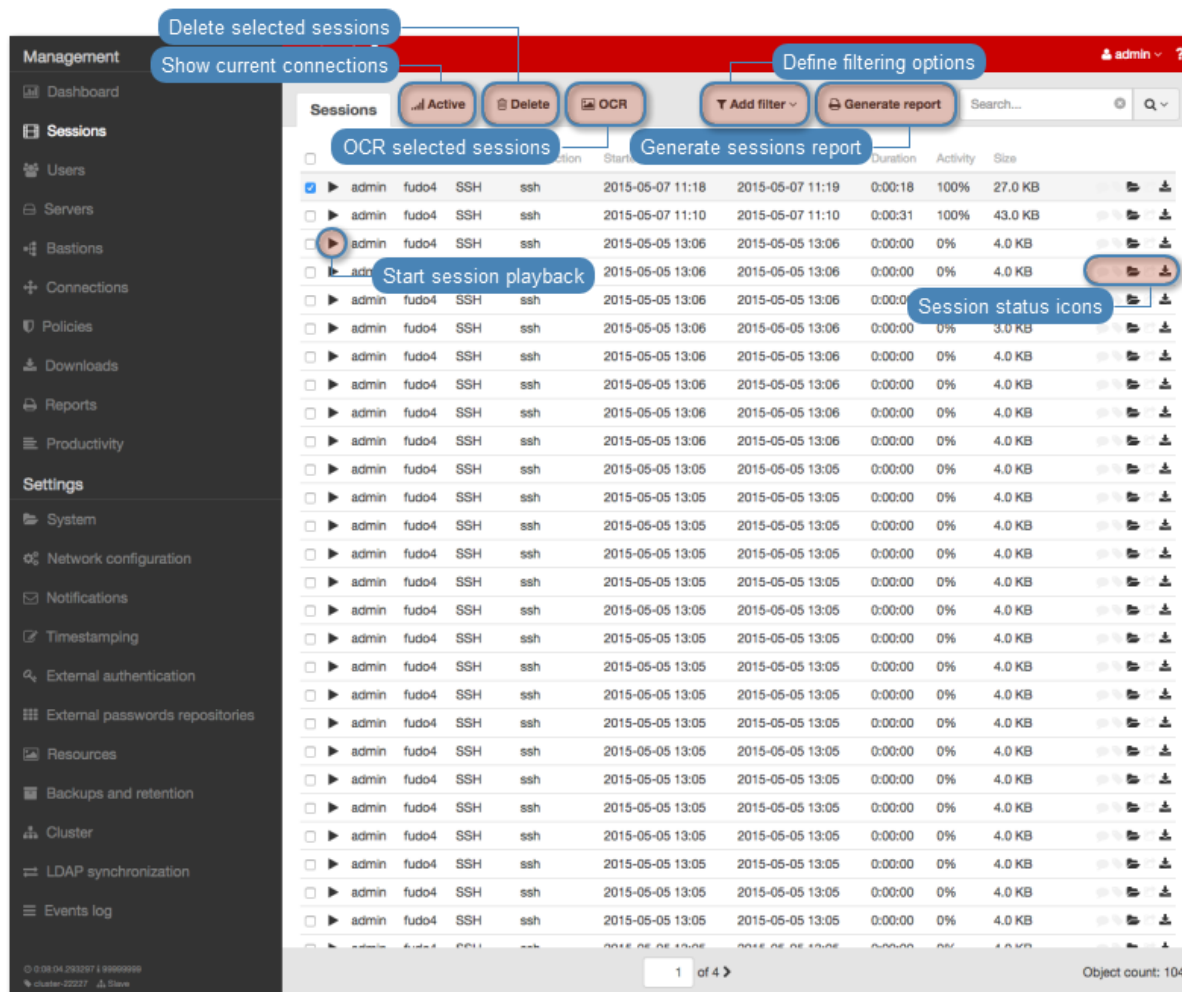
Wheel Fudo PAM stores all recorded servers access sessions, allowing to playback, review, delete and export to one of supported video format.

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.

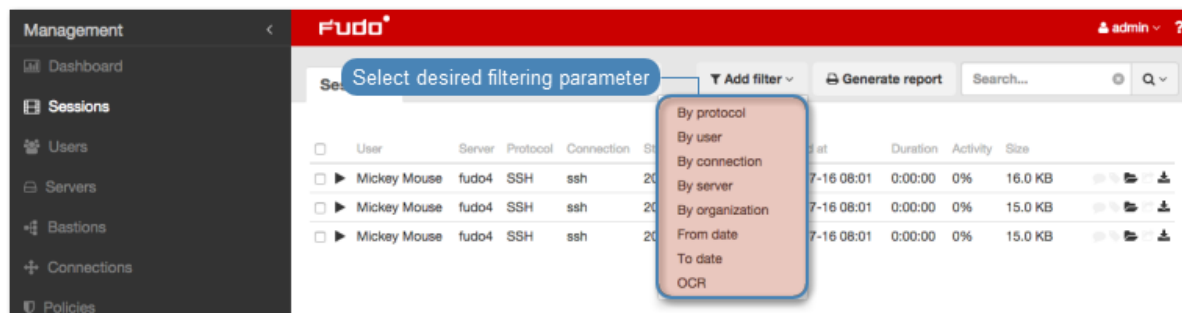


3.1 Filtering sessions

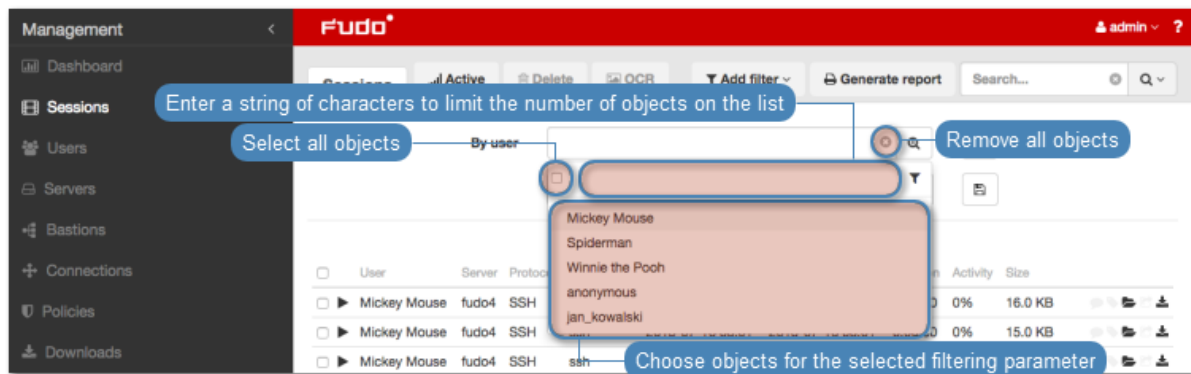
Sessions filtering allows to find desired sessions easily by limiting the number of displayed sessions on the sessions management page.

3.1.1 Defining filters

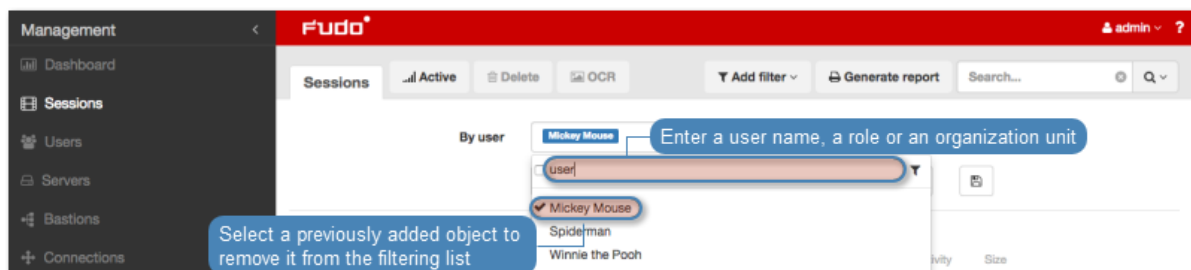
1. Click *Add Filters* and select desired data type from the drop-down list.



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

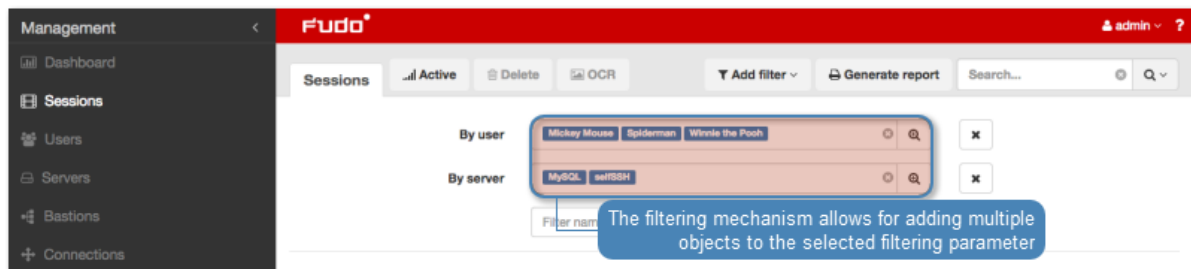


Note: Enter a string of characters to limit the number of the elements on the list. In case of users, the elements on the list can be limited to those who have a given user role assigned or belong to the given organization unit.



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

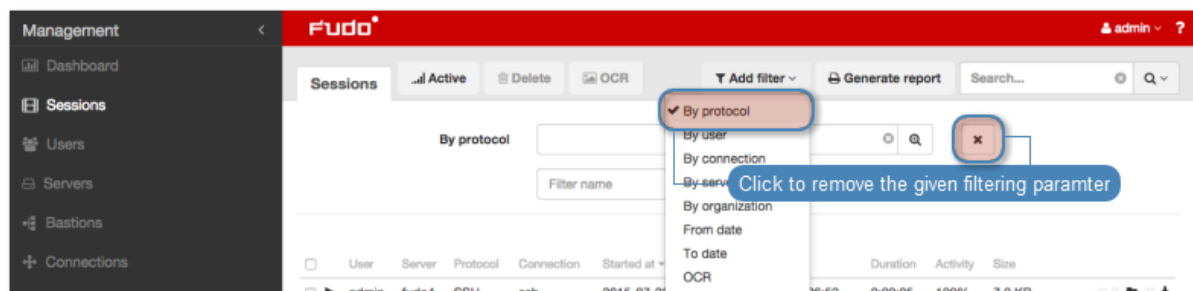
Protocol, user, connection, server and organization parameters allow for selecting multiple objects of the given type.



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

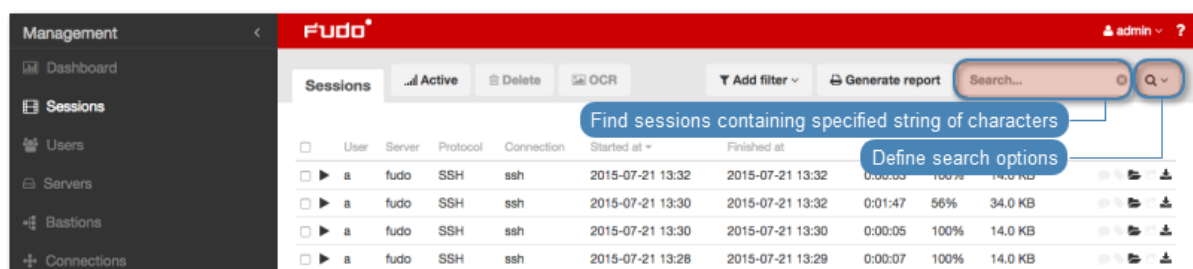
Note: Only sessions which match all defined filtering parameters will be displayed.

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



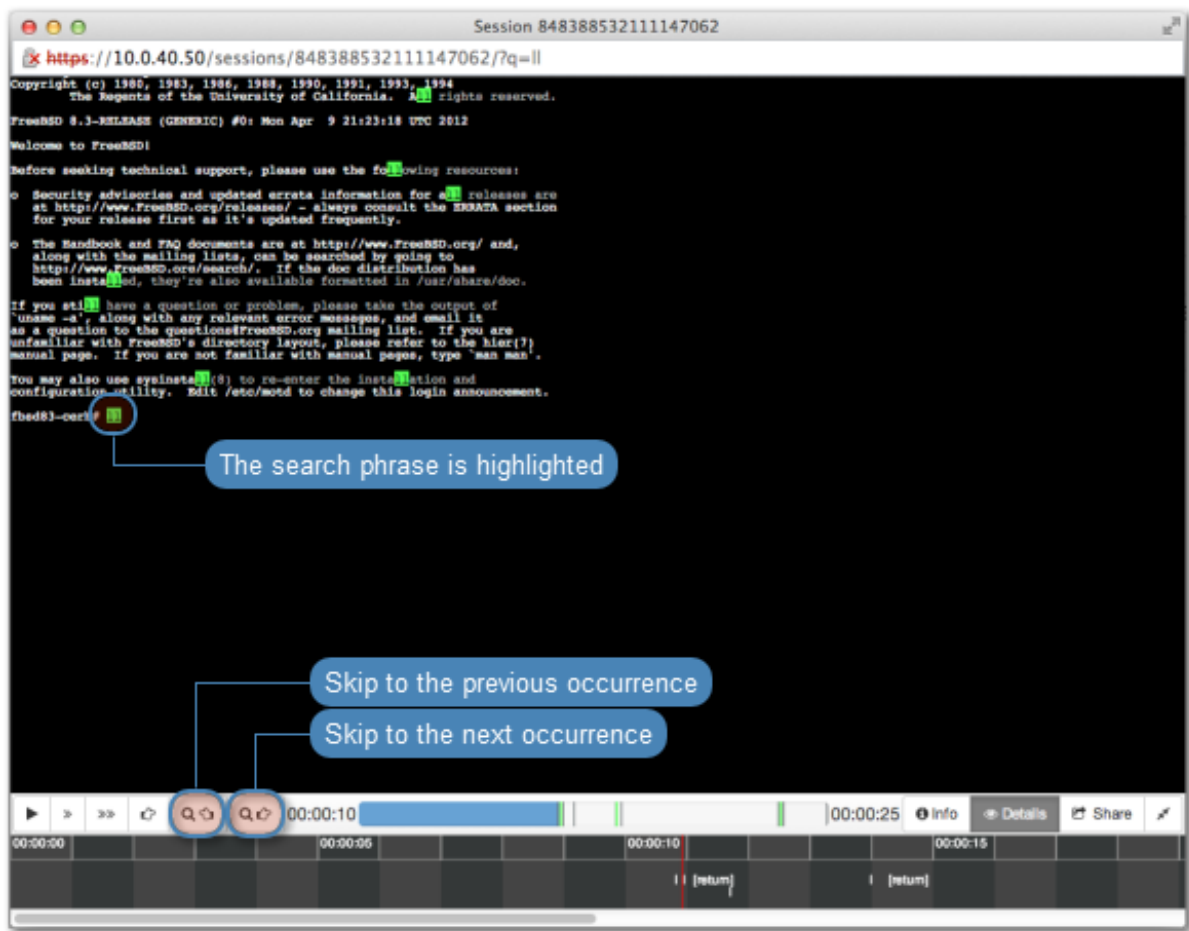
3.1.2 Full text search

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.

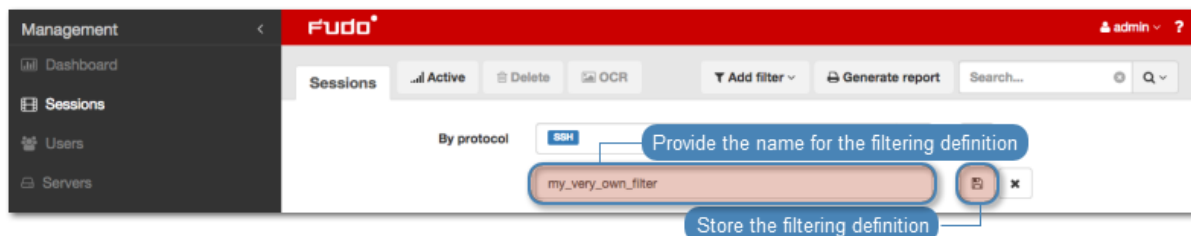


3.1.3 Managing user defined filter definitions

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

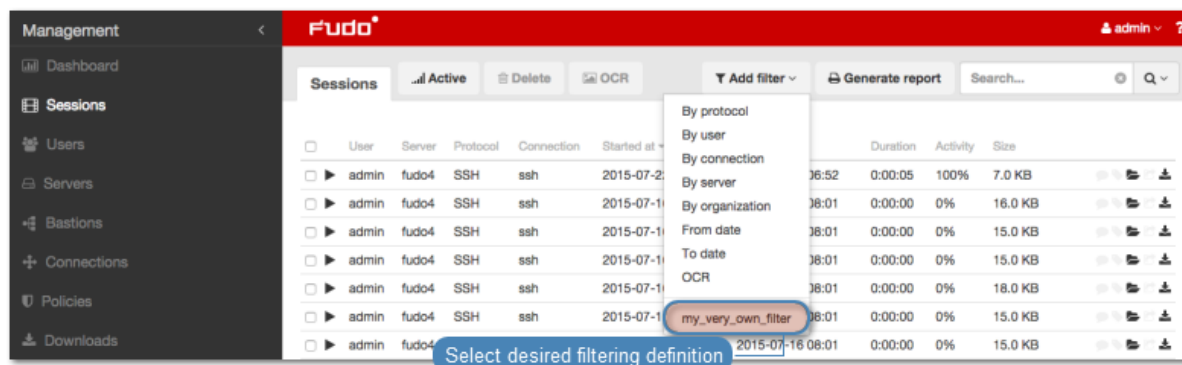
Storing a user defined filter definition

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

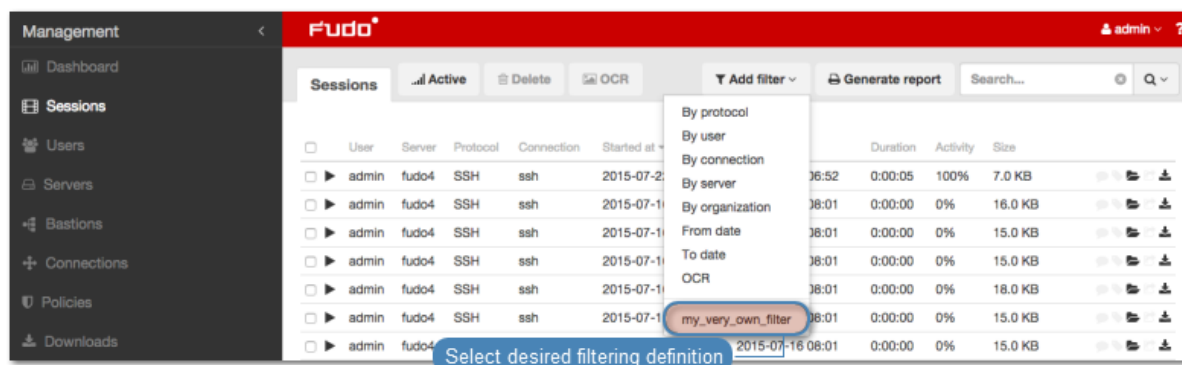
1. Click *Add filter* and select the desired filter definition.



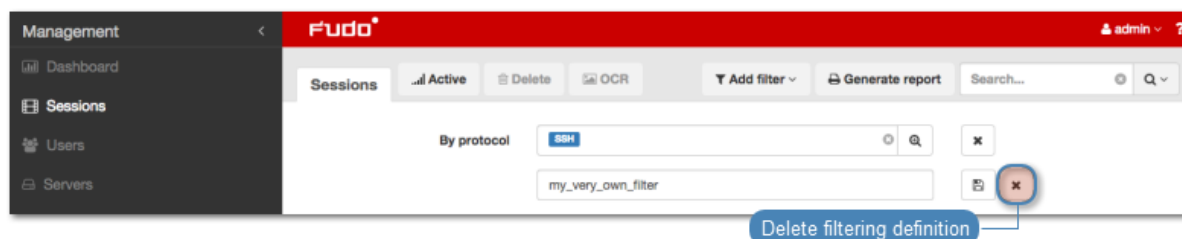
2. Change the filtering parameters as desired.
3. Click the save icon to store changes in the filter definition.

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](#)

3.2 Reports

Reporting service generates detailed statistics of users access sessions.

Full reports are generated periodically (daily, weekly, monthly, quarterly) by the system and can be accessed by users with the `superadmin` role assigned. Reports generated periodically upon

users with **admin** or **operator** requests, will include only information regarding sessions objects which they have access permission assigned to.

In addition to the system default settings, cyclic reports can be also generated based on the user defined *filtering definition*.

Report can also be generated on demand and include data related to specified user sessions.

Subscribing to a periodic report

To enable automatic periodic report generation for the logged in user, proceed as follows.

Note: Periodic reports, generated upon specific user's request, include only sessions, to which given user has sufficient access rights.

1. Select *Management > Reports*.
2. Click *Manage subscriptions*.
3. Select the report definition from the drop-down list.

Note: The list contains system default options and user defined *filtering definitions*.

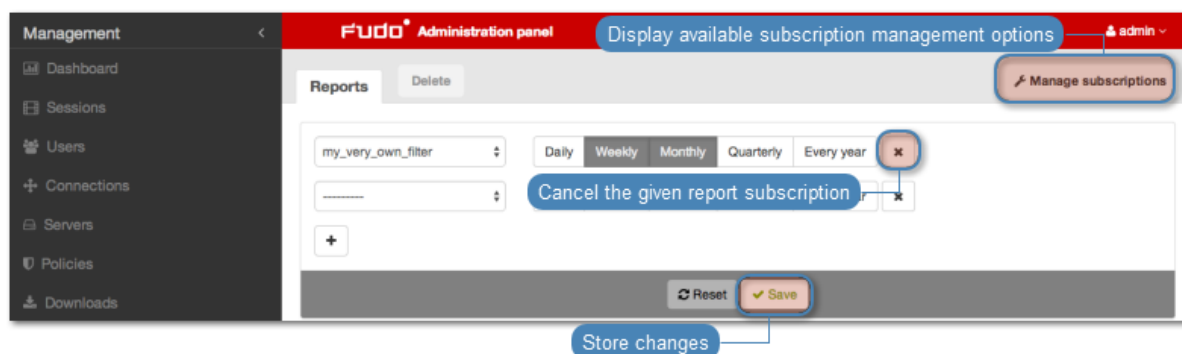
4. Choose how often the given report should be generated.
5. Click *Save*.



Cancelling a periodic report subscription

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

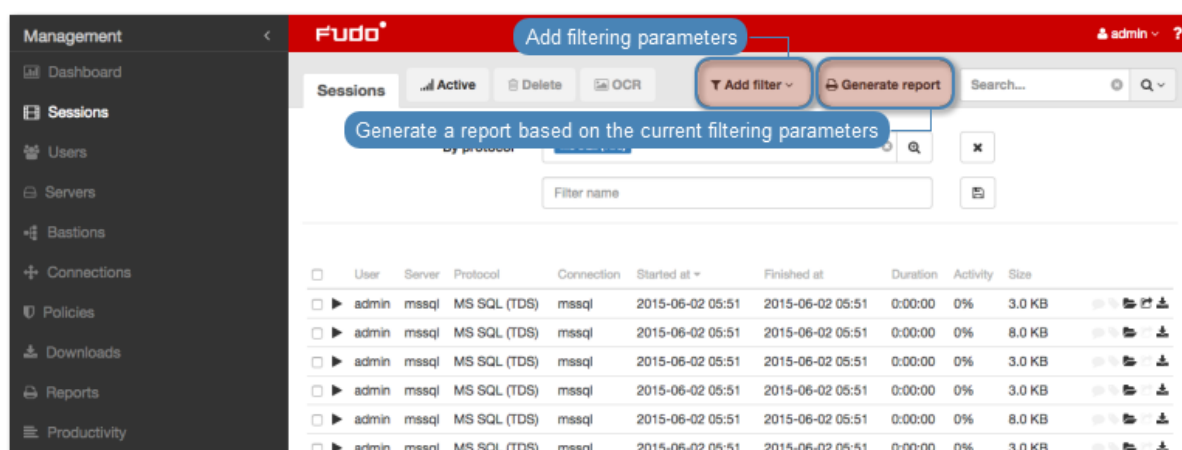
1. Select *Management > Reports*.
2. Click *Manage subscriptions*.
3. Click the report definition removal icon.
4. Click *Save*.



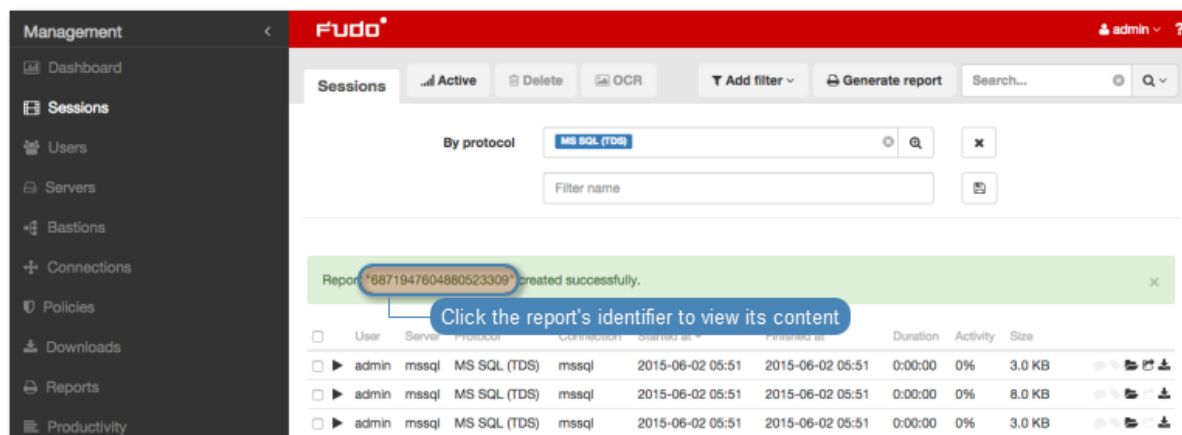
Generating reports on demand

A report can be prepared for a specified subset of user sessions, determined by filtering options.

1. Select *Management > Sessions*.
2. Click *Add filters* and define filtering parameters (for more information on sessions filtering, refer to the *Sessions: Sessions filtering* topic).
3. Click *Generate report*, to have the report generated based on the current filtering criteria.



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

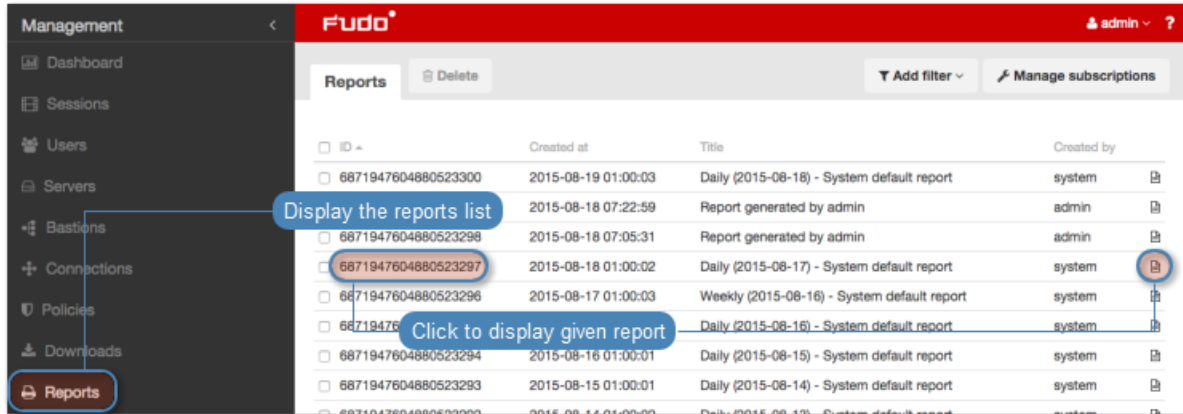


5. Select *Management > Reports*.
6. Find desired report and click the view icon.

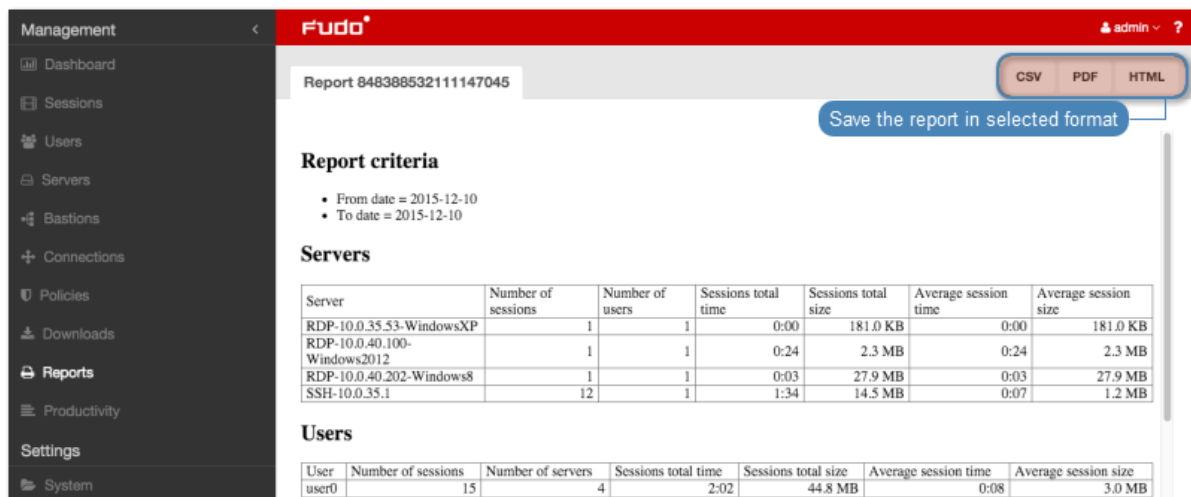
- Click the corresponding button to save the report in selected format.

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.



Deleting reports

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

Related topics:

- [Notifications](#)
- [Filtering sessions](#)

3.3 Viewing sessions

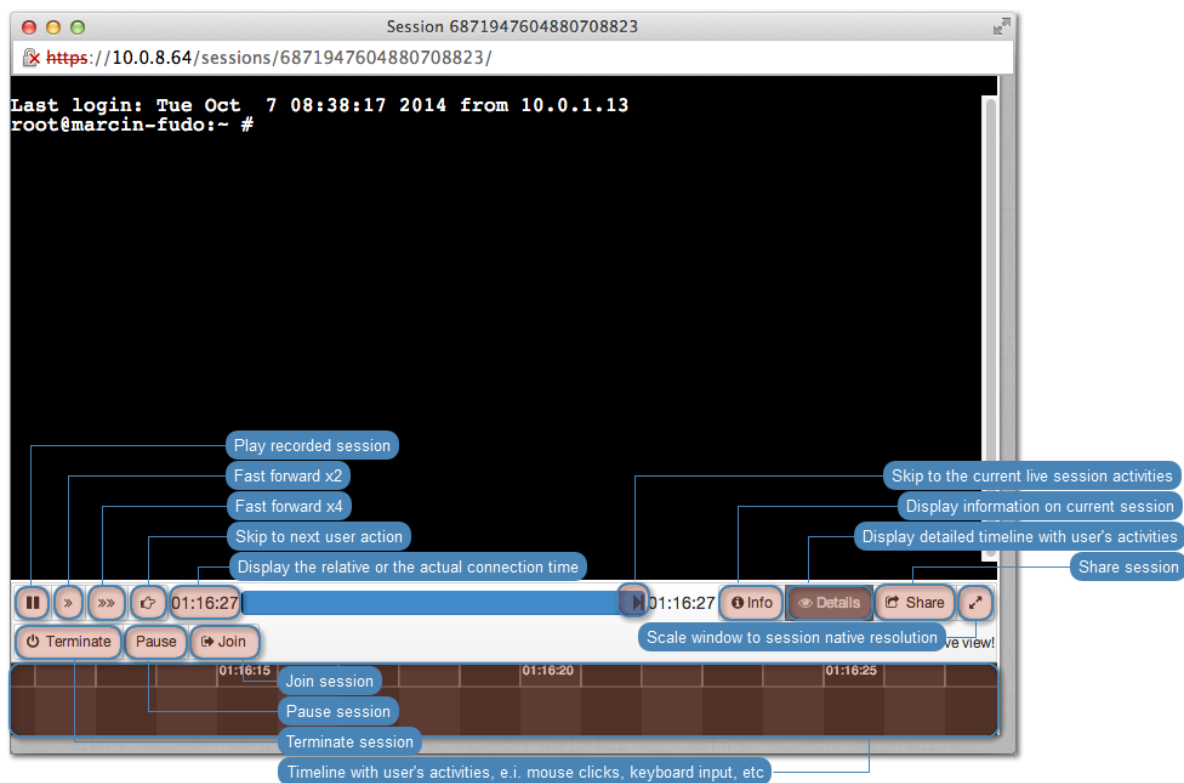
Wheel Fudo PAM allows viewing recorded sessions as well as current user connections.

To view a session, proceed as follows.

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

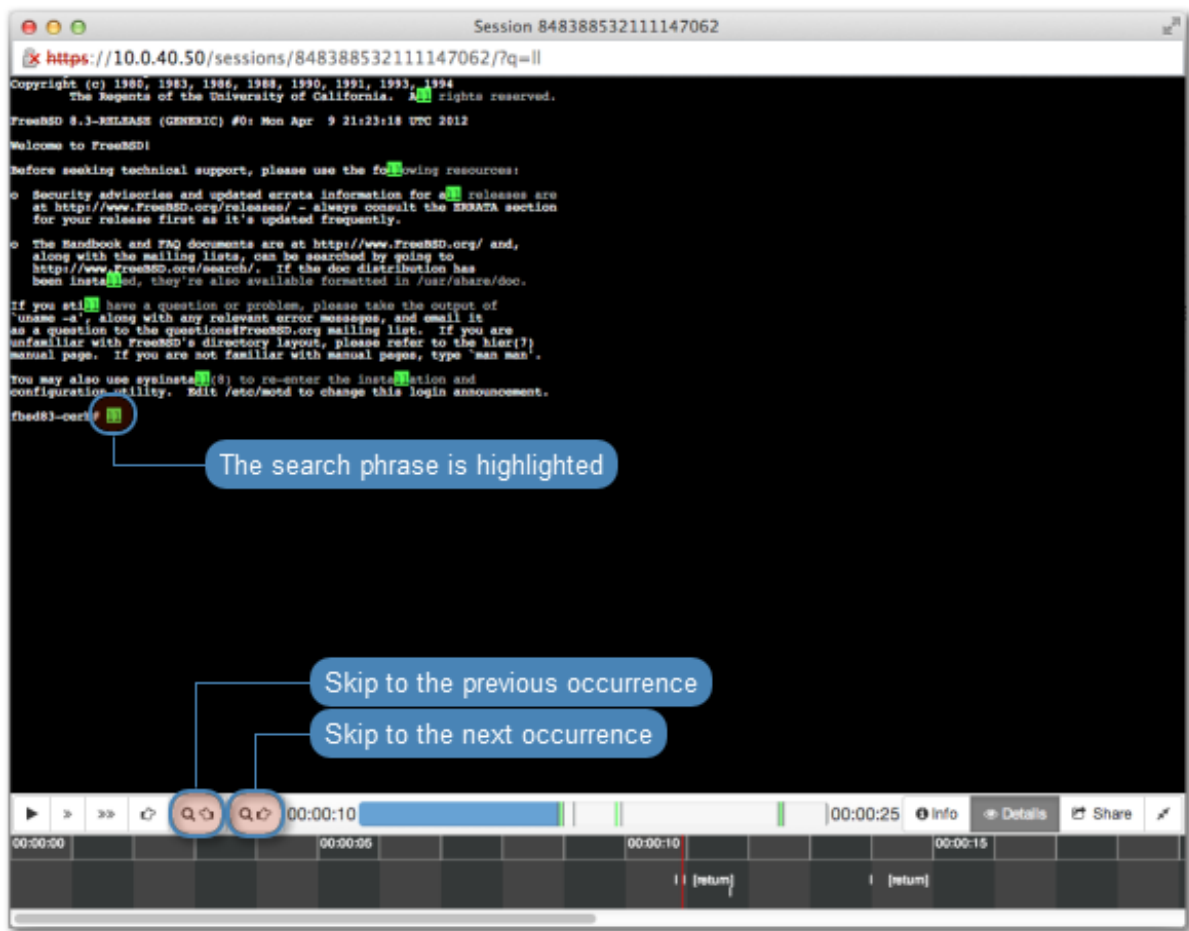
Session player options

Note: Some options are available for live sessions only.

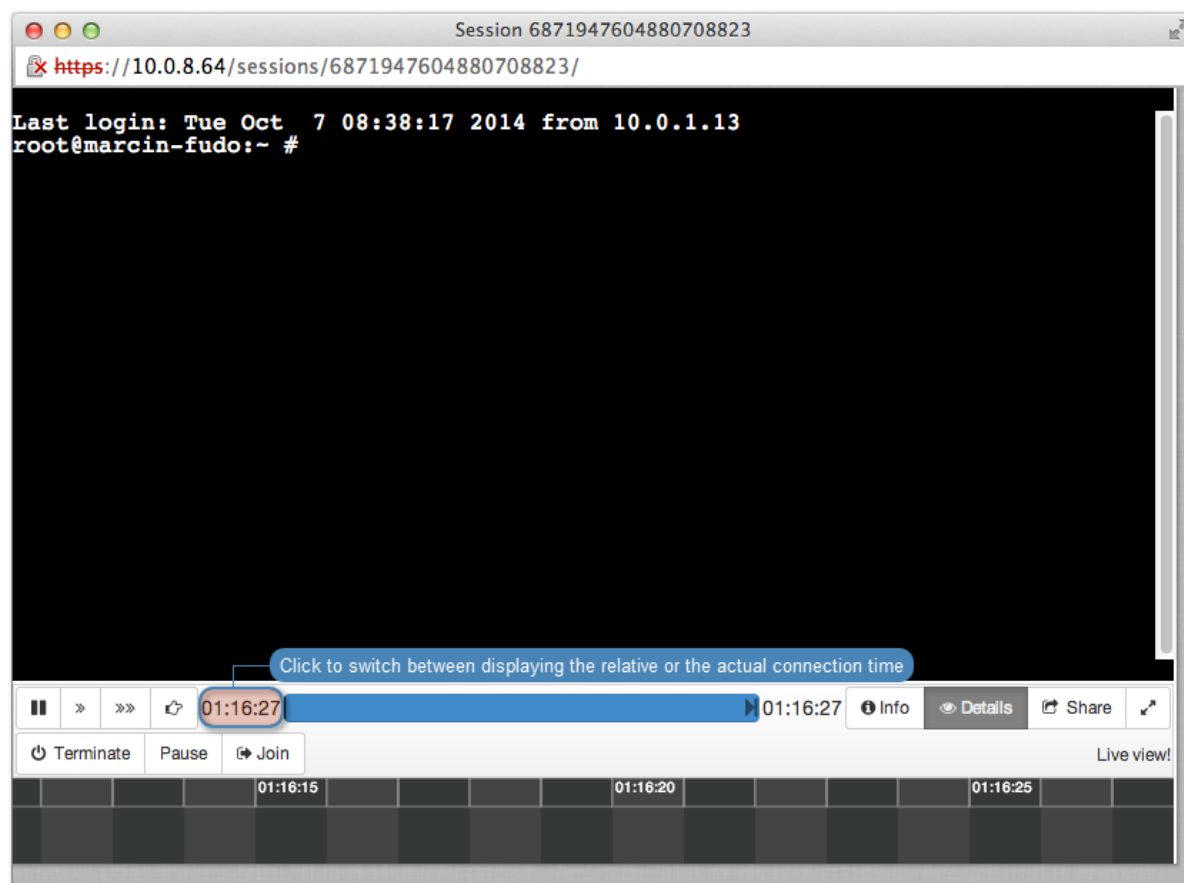


Note: Playing a session containing the specified phrase starts from the moment of its first occurrence.

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*

3.4 Viewing live sessions

Wheel Fudo PAM enables viewing current connection sessions, allowing to supervise user's activities.

1. Select *Management > Sessions*.
2. Click *Active* to display current users' connections.
3. Find desired session and click the play icon to start playback.

Related topics:

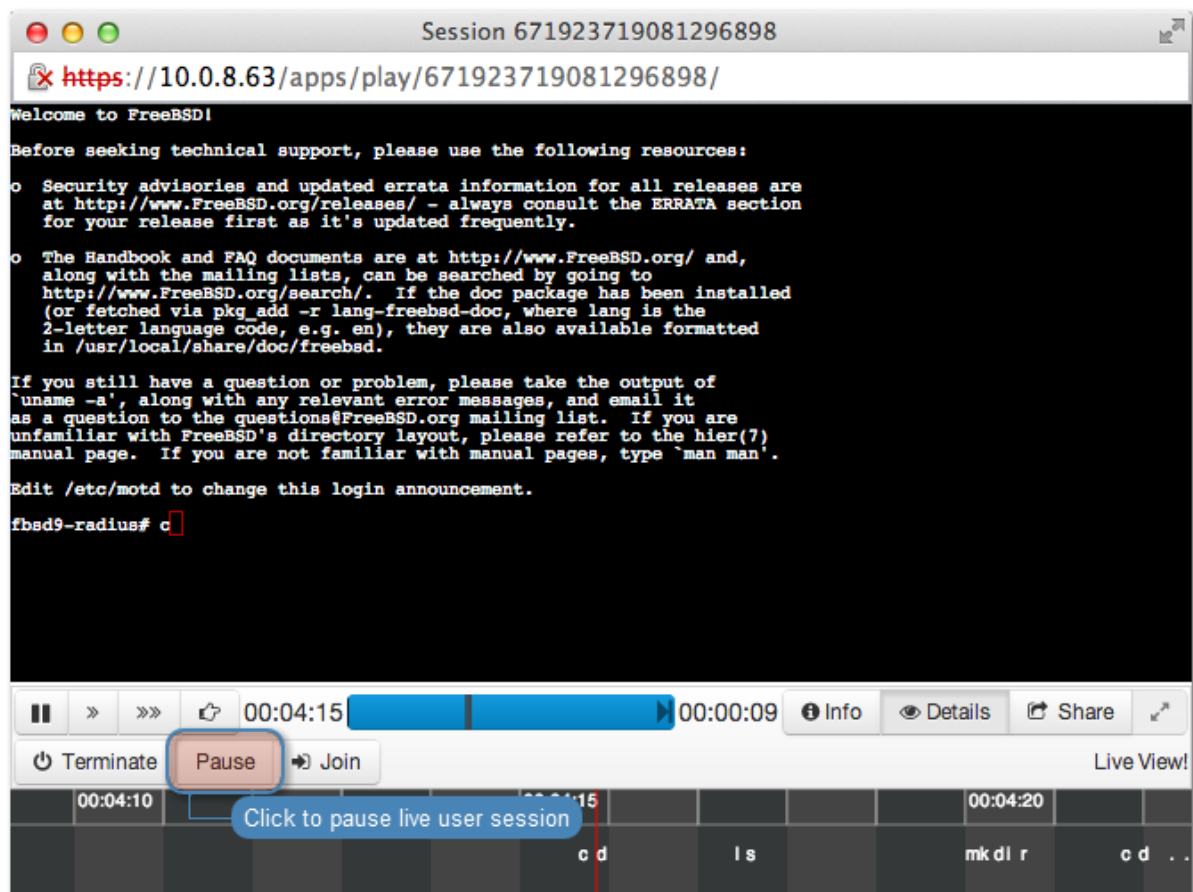
- *Viewing sessions*
- *Terminating connection*

3.5 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 *Active* to display current user connections.
3. Find desired session and and click the play icon to start playback.
4. Click *Pause*.



Related topics:

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

3.6 Terminating connection

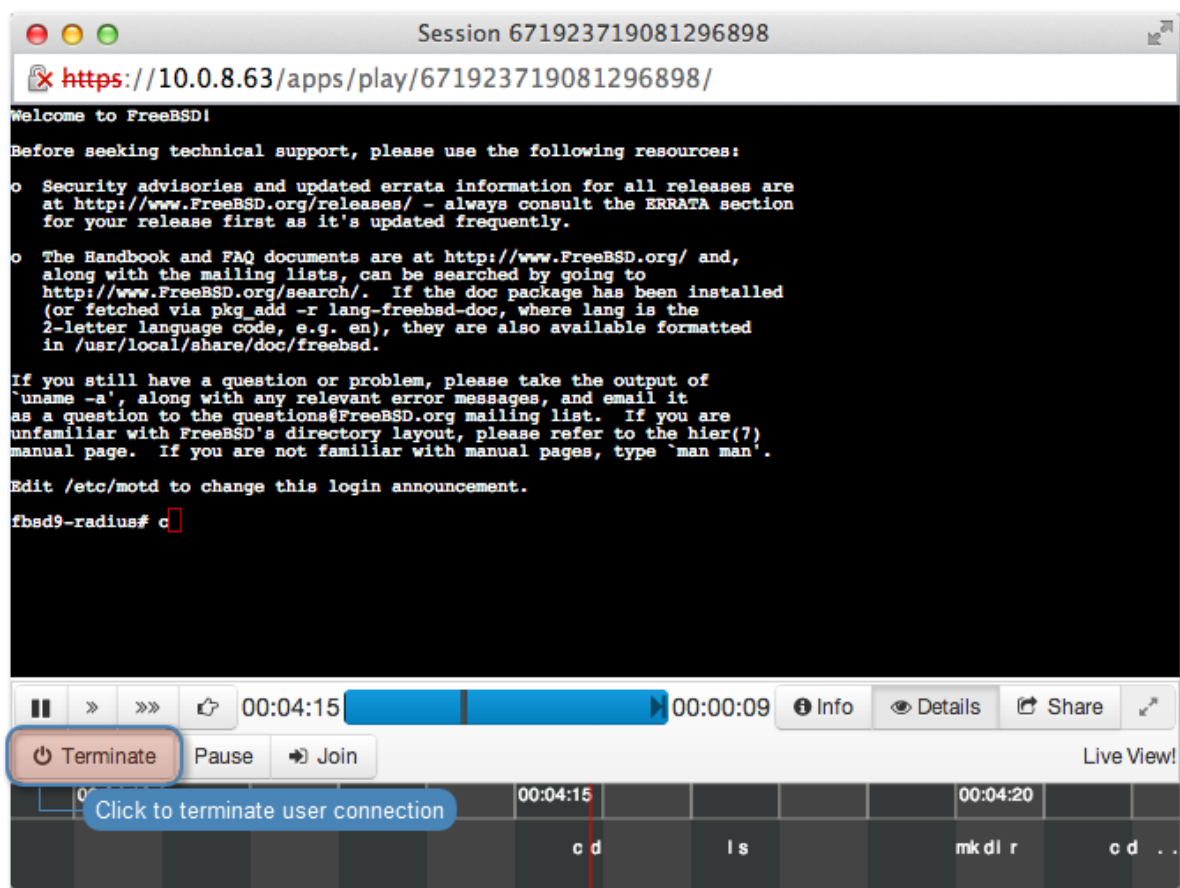
In case the administrator notices access rights misuse, Wheel Fudo PAM allows to terminate the session and automatically block given user.

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 *Active* to display current user connections.
 3. Find desired session and click the playback icon to start playback.
 4. Click *Terminate*.
-

Note: Terminating connection automatically blocks given user.



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

Related topics:

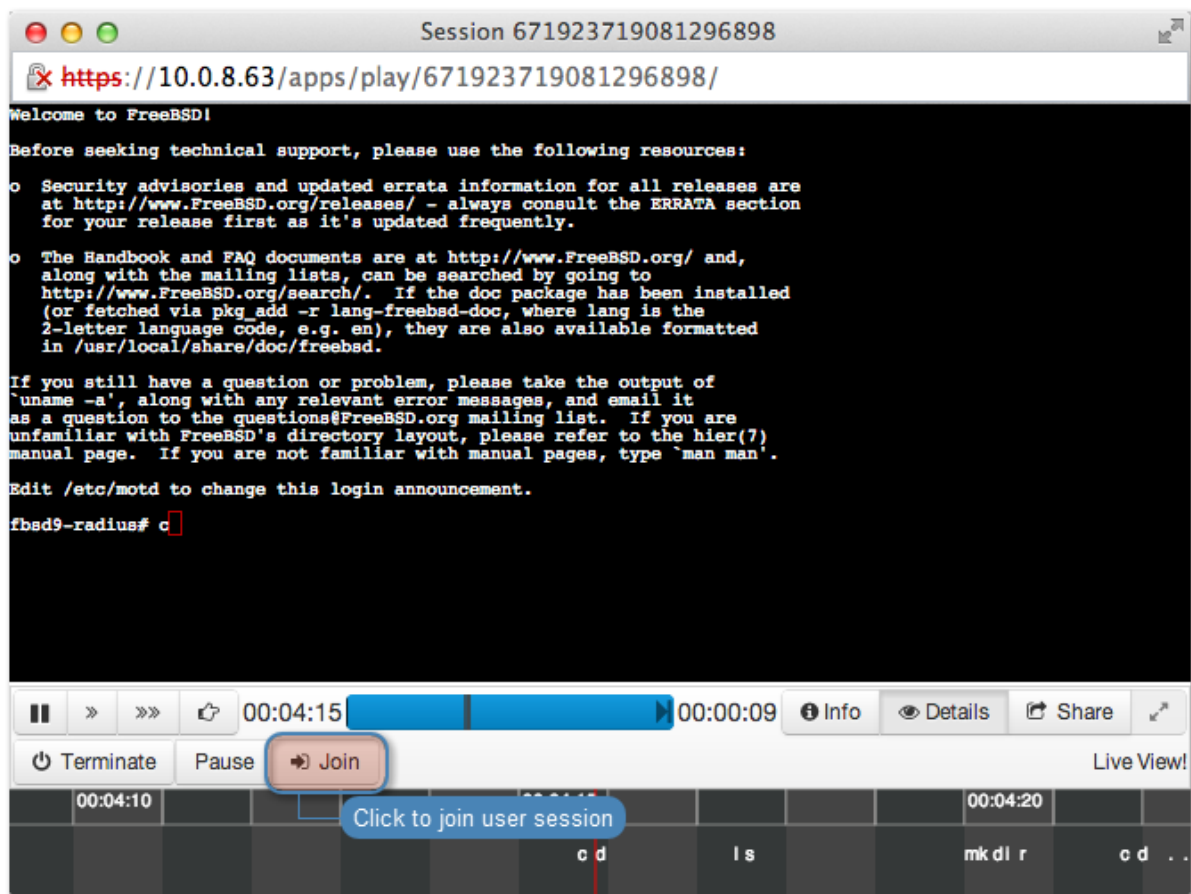
- *Policies*
- *Security measures*
- *Joining live session*
- *Sharing sessions*
- *Filtering sessions*

3.7 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 *Active*.
3. Find desired session and click the play icon to start playback.
4. Click *Join*.



Related topics:

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

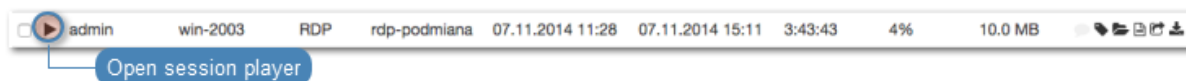
3.8 Sharing sessions

Wheel Fudo PAM enables sharing given session with another user.

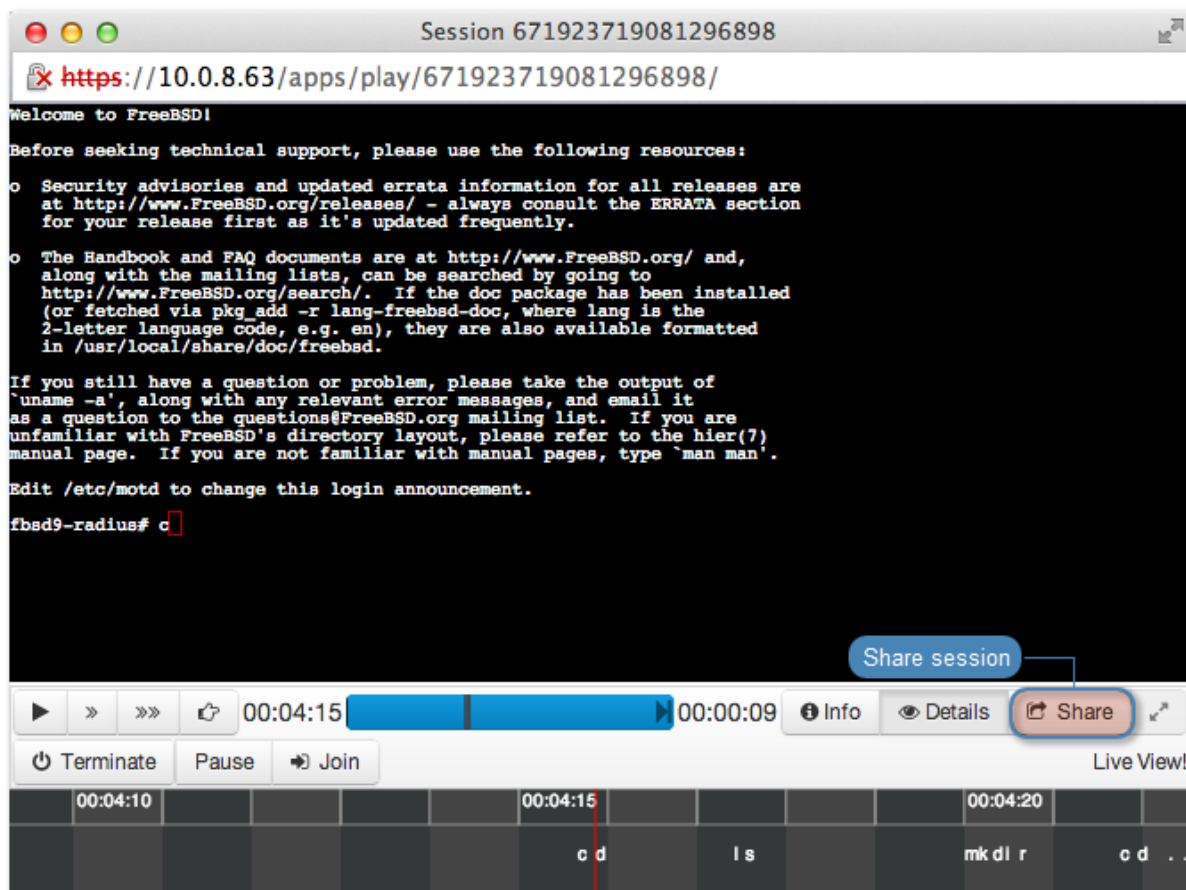
Sharing a session

To share a session, proceed as follows.

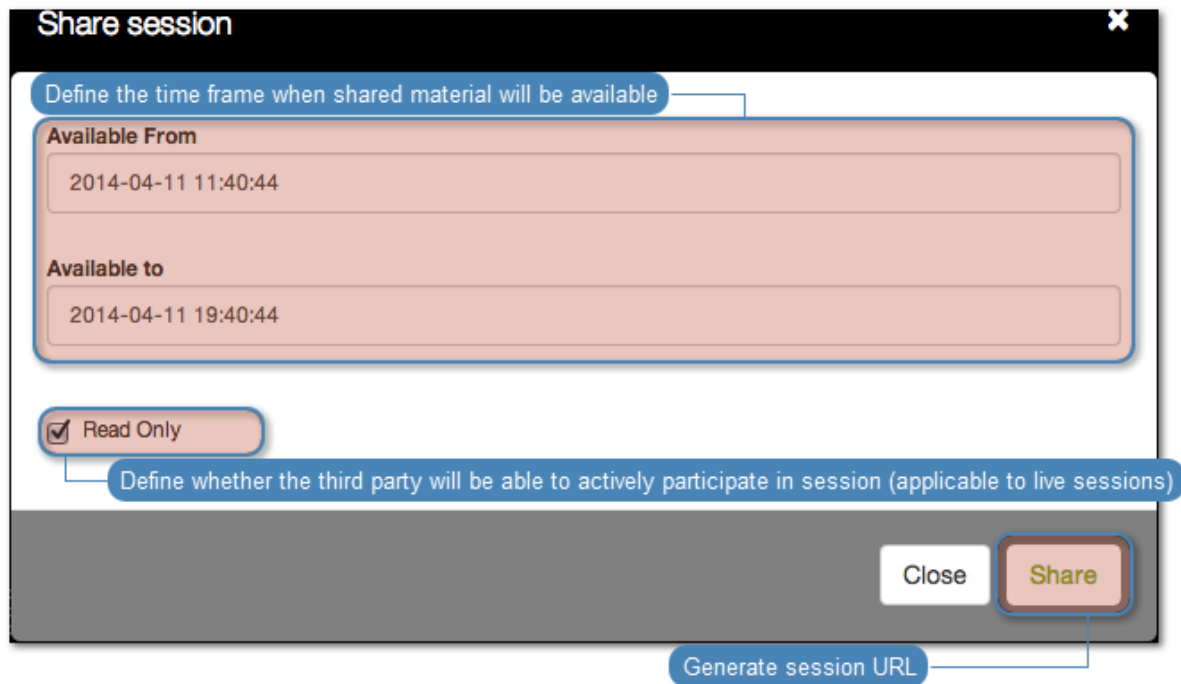
1. Select *Management > Sessions*.
2. Find desired session and click the play icon to start playback.



3. Click *Share*.



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



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

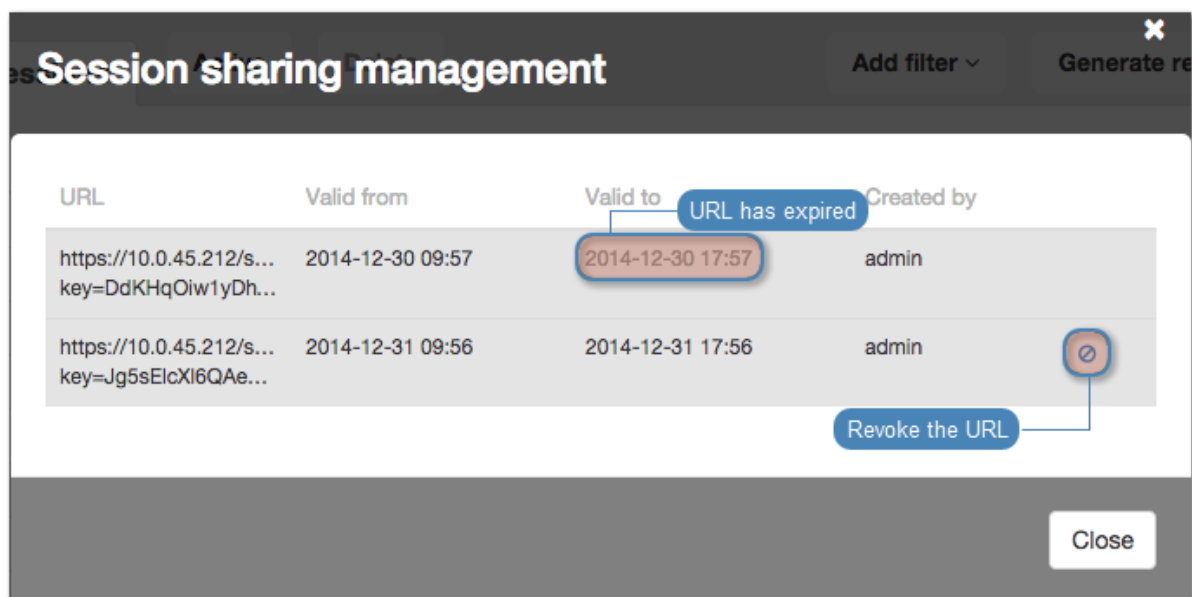
Revoking session URL

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*

3.9 Commenting sessions

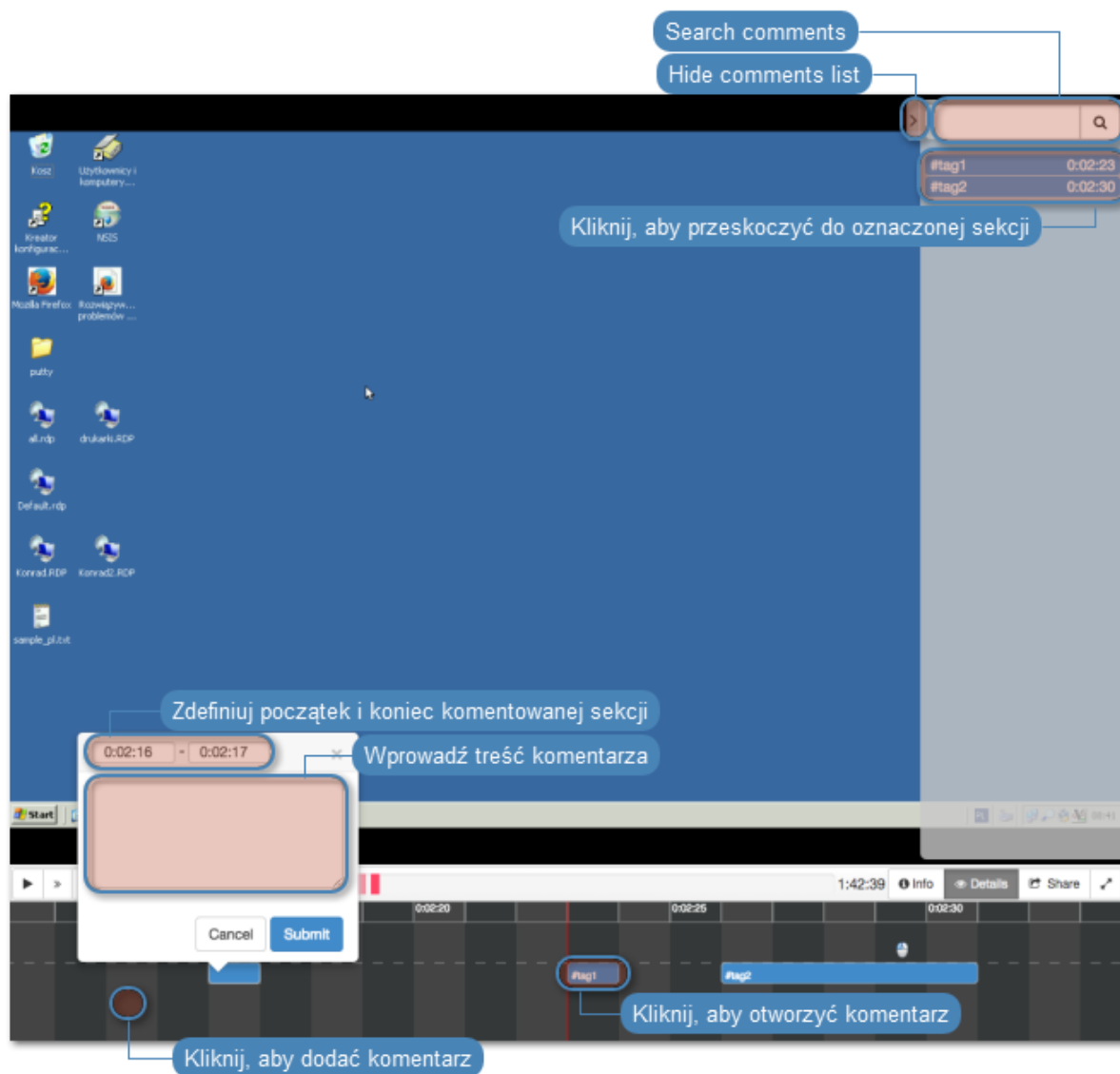
Wheel Fudo PAM enables adding comments and tags to recorded sessions.

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*.



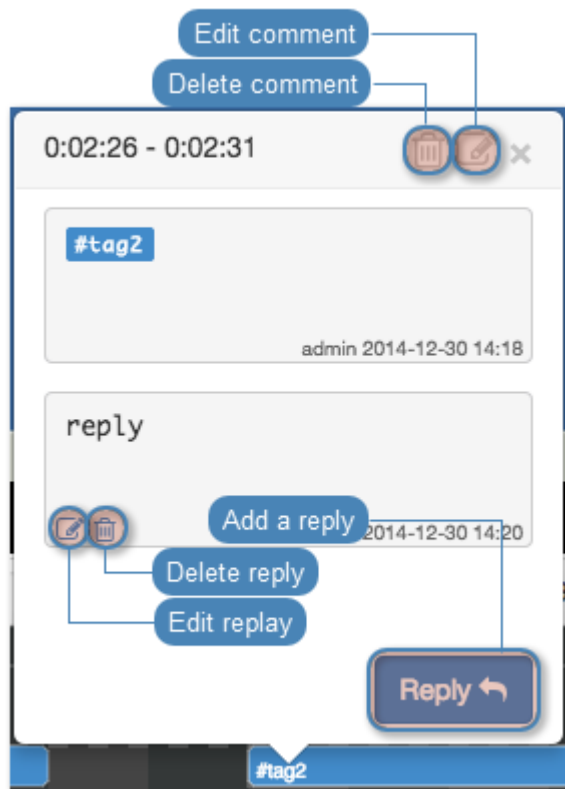
Editing a comment

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:

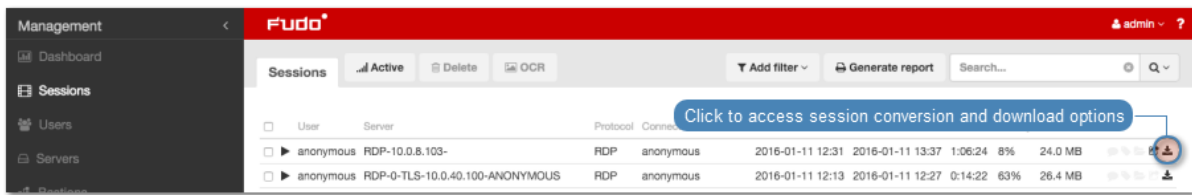
- *Sensitive features*

3.10 Exporting sessions

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

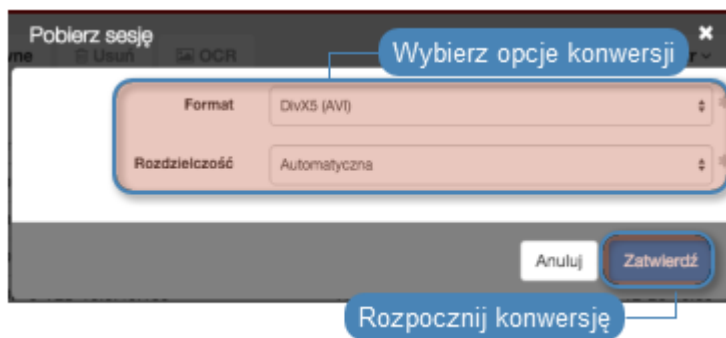
To export a session, proceed as follows.

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.



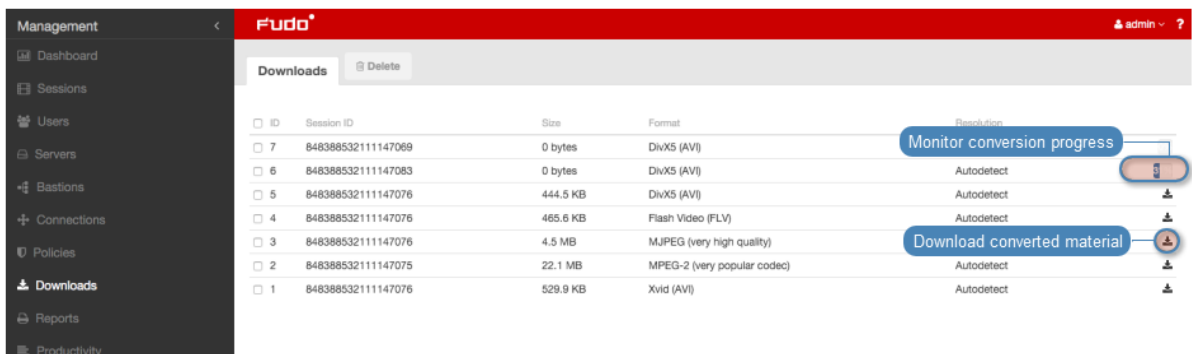
4. Select the video resolution (*not applicable to the text log file format*).

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*

3.11 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*

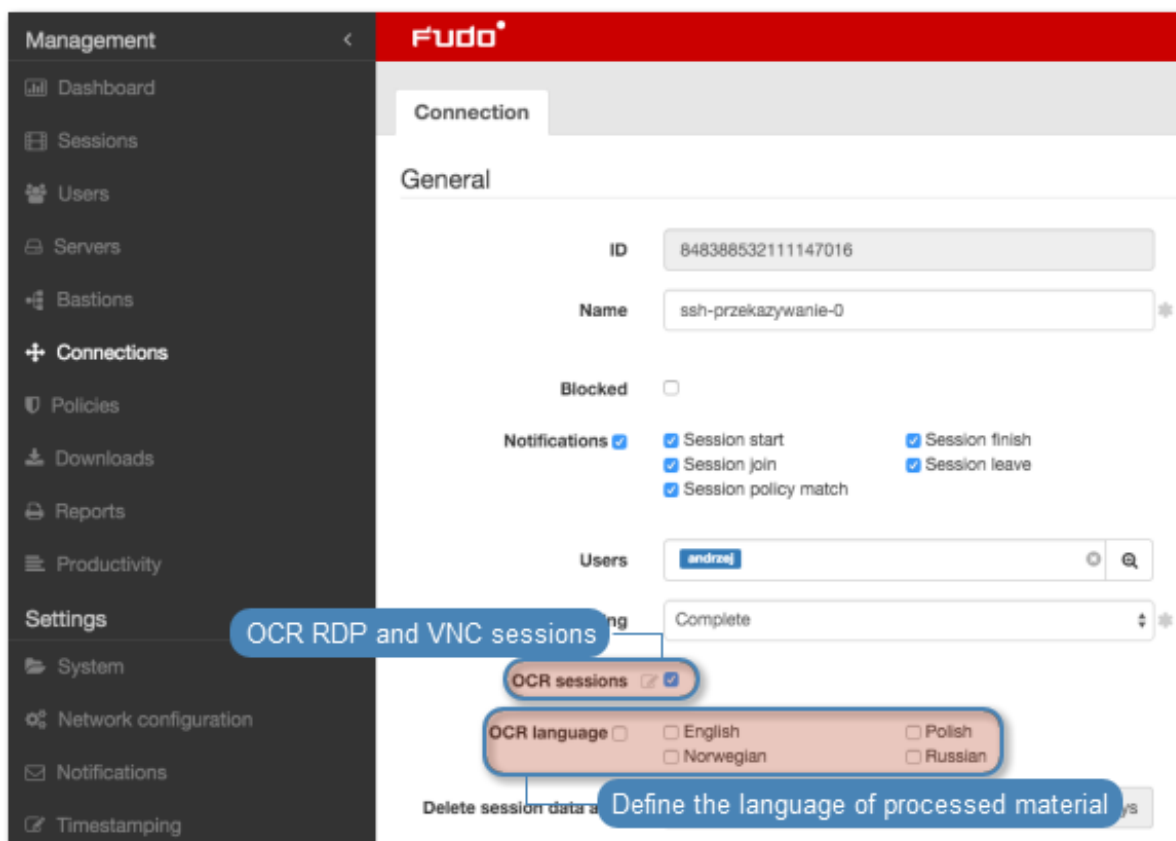
3.12 OCR processing sessions

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.

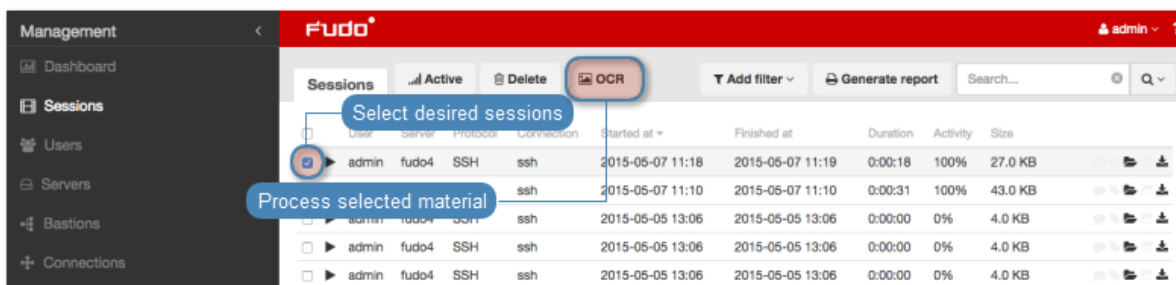


4. Click *Save*.

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*

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

4.1 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.

Management < **Fudo** admin ?

Overview Session analysis Comparison Add filter Generate report

Date from Add a filter, to limit the number of elements on the list

Click to sort table content

Summary

Organization/User	Sessions total time	Active time	Idle time	Productivity	Sessions	Servers
Total	434:56	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
senvis	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

Show users within the given organization

Hide users within the given organization

Management < **Fudo** admin ?

Overview Session analysis Comparison Add filter Generate report

Date from 2014-10-01 to 2014-11-01

Summary

Organization/User	Sessions total time	Active time	Idle time	Productivity	Sessions	Servers
Total	434:56	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
senvis	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

Show users from the given organization only

Show sessions analysis for the given user

Click to display sessions list for the given user/organization

Related topics:

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

4.2 Sessions analysis

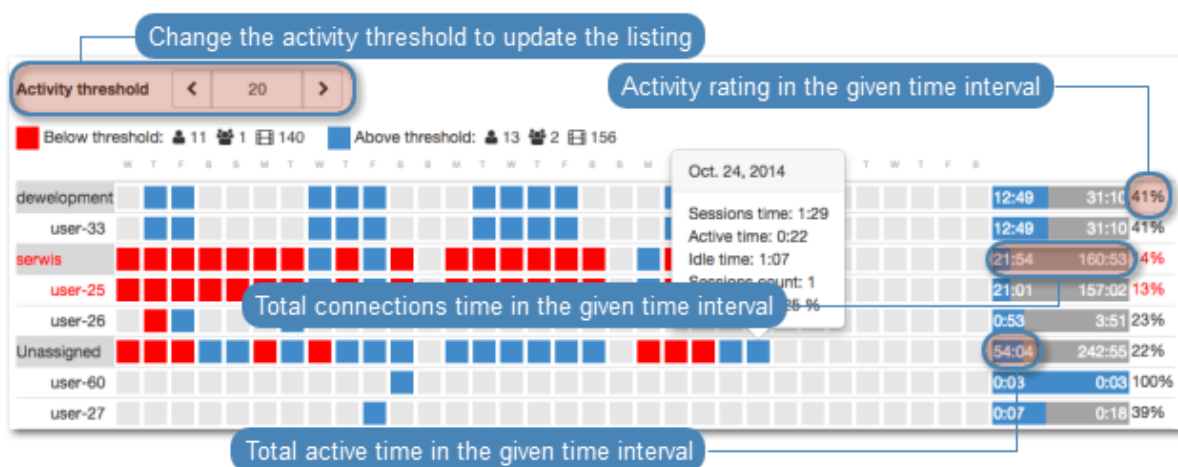
Sessions analysis shows in detail users/organizations productivity in the given time period. The activity threshold parameter allows identifying sessions, users and organisations which do not exceed the required user activity rating and helps establishing the threshold value attainable for a given number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

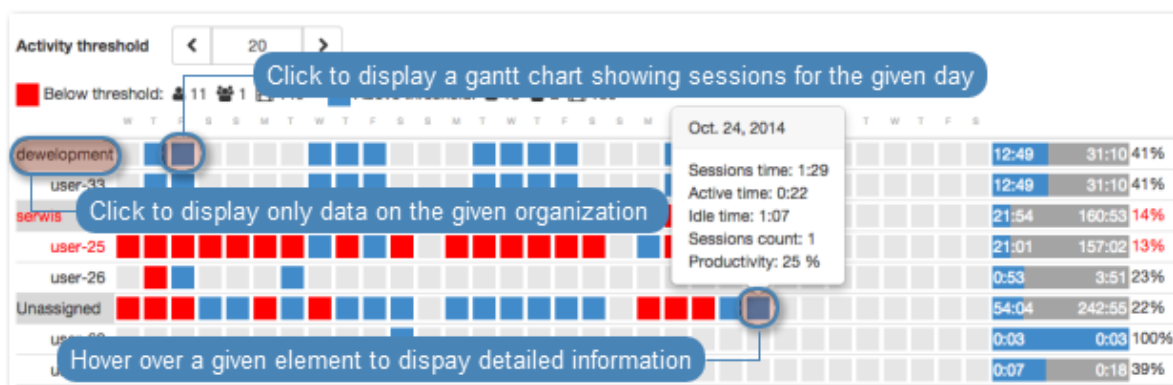


Users activity rating

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](#)

4.3 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](#)

AAPM (Application to Application Password Manager)

5.1 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.

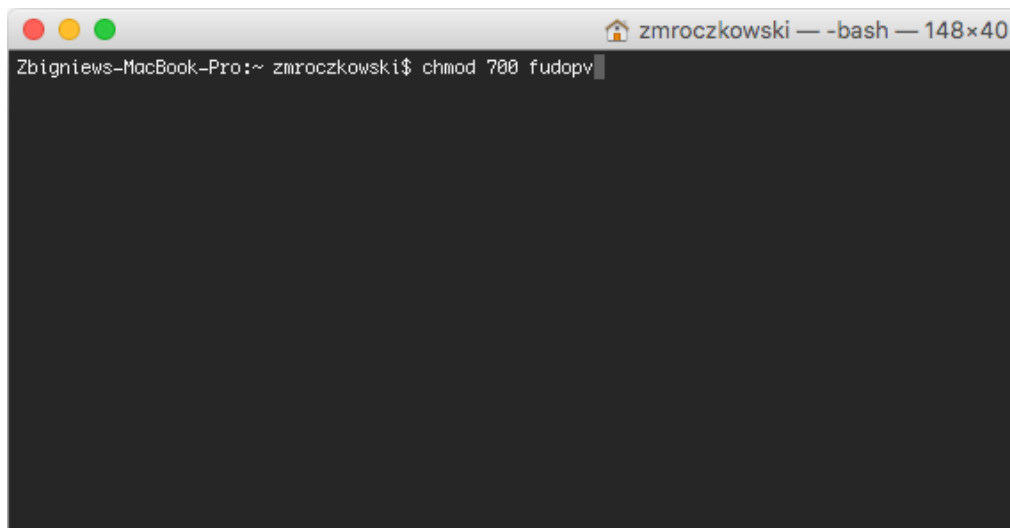
5.2 *fudopv*

Execution parameters

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

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

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

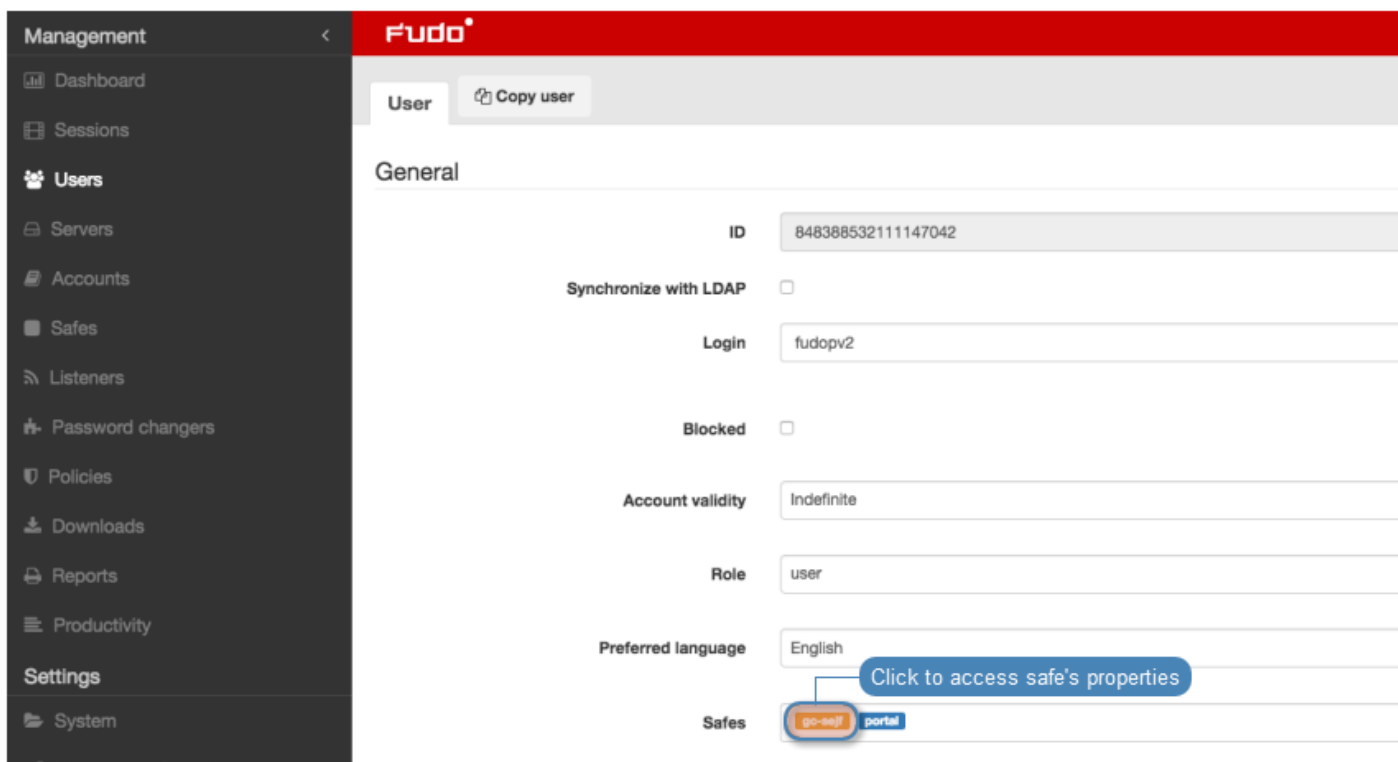
A screenshot of a macOS terminal window. The title bar shows three colored window control buttons (red, yellow, green) on the left, a home icon, the username 'zmroczkowski', the shell '-bash', and the window size '148x40'. The terminal text shows the prompt 'Zbigniews-MacBook-Pro:~ zmroczkowski\$' followed by the command 'chmod 700 fudopv'. The command has been executed, and the prompt is now on a new line.

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

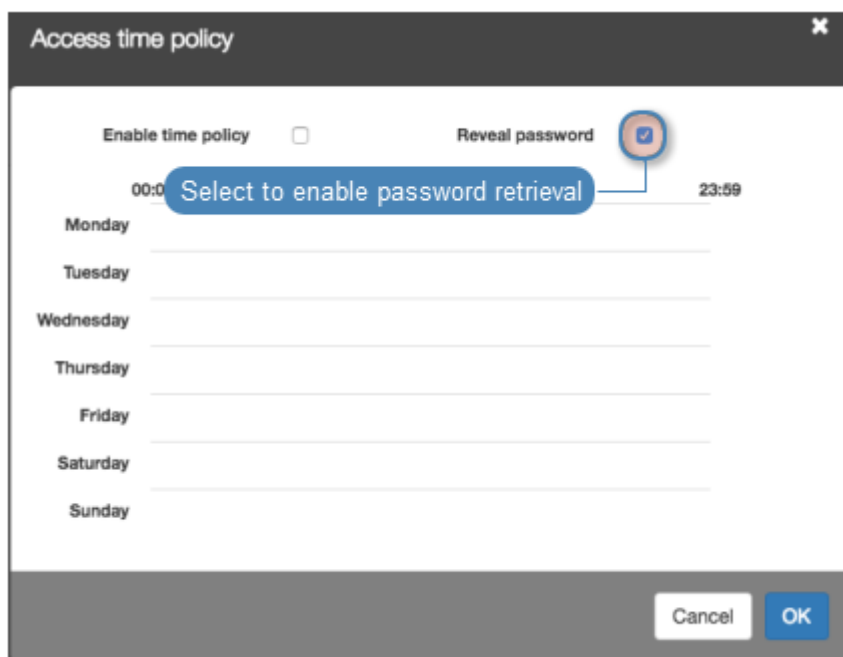
2. Log in to the Wheel Fudo PAM administration panel.
3. Create a user object with **user** role, static or one-time password authentication and server's IP address defined in the *API* section.

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.

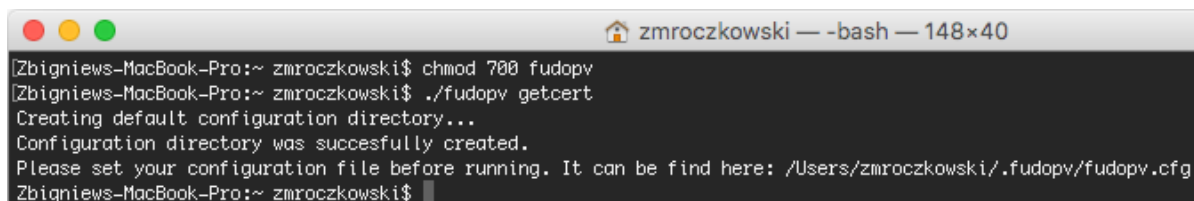


- Select the *Reveal password* option.



- 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*.

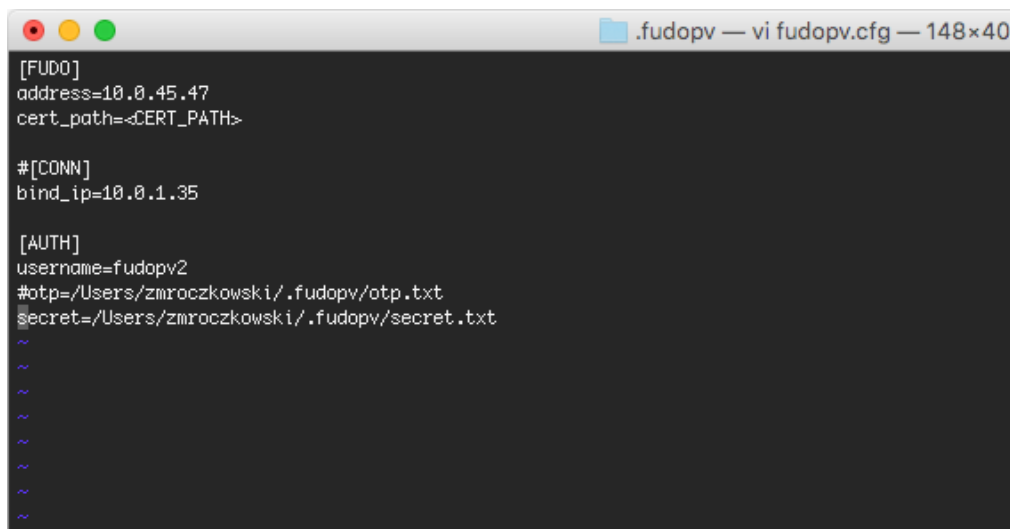
4. Run `fudopv getcert` command to initiate the configuration.



```
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
[FUDOP]
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
cG9ydDEjMCEGA1UEAwRlVETyBUZl1wb3JhenkgQ2VydG lmaW NhdGUxJzAlBgkq
hk iG9w0BCQEWGHN1cHBvcnRAd2h lZWxeXN0ZW1zLmNvbTAeFw0xNjA2MDEwODE4
NDJ0aFw0YnJlMzAwODE4NDJ0aMIHoMQswCQYDVQQGEwJQDEPMA0GA1UEEQwGMDIt
NDk1MRQwEgYDVQQIDAttYXpvd2l lY2tpZTERMA8GA1UEBwwlV2Fyc3phd2ExFjAU
BgNVBAKMdXVsLk9jaG9ja2EgMUYxITAfBgNVBAoMGFdaZWVzIFN5c3R lBXMgU3Au
IHogby5vLjEwMBQGA1UECwwNV2h lZWwgU3VwcG9ydDEjMCEGA1UEAwRlVETyBU
ZW1wb3JhenkgQ2VydG lmaW NhdGUxJzAlBgkqhkiG9w0BCQEWGHN1cHBvcnRAd2h l
ZWxeXN0ZW1zLmNvbTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgcCggIBALc4
dSr7DqZ4kVuJoI7V/jhVIXA0CRpY5IFbckHiNGFXn3vBueNr9opedj/bwF iqb4p+
ZfRcWJ8HbpoVw06qFYKGmPr0esRLR71301Xs0vzNnf smqP2vC9wKHq1LKDwdBMKE
ZqpydVbAcmr0u7ZS ljsFBd2LEfyULme9cIsd3e88SkLY0femZBCcy0++AXvCNhE0
WABvInzUrgbqrvaJKeIU37L tRyHZCa5/o1auxnp+Ew l0ng l0RqwsQxZFoR0w5Rj
j+p0i0XXfYN9cJ3+950QYfupMPSN9dF/0+ lbaThrRnqm5NPXUMxUS5oBdxmcdBjL
dX1bJ/tUyAI7Vdru7Vyn09/uUntcJm7/8nifVda4W lN0aQe43nynMuaAYb3fxJLC
+bs+0ziLarQqMH27MWK6c7XXNd+PDQVhNNK8Q09f0YZYr4UP+7pDFBFFXY0N0qSI
5mv0L2a0CAQNKJJ7D/TtR9vpJBDv9PXV67+p2ZAty9asjAq/Iu6uXmmg8Tb/8MY
3rPQH2nCh6WAW9Cd l4Gx1mxhey0Da5f1EJ0eEwEAX0XzDeGzq/ZR7562Cbwe6he0c
0jbYn2NI9 lCfFC071bGDAKAID lZ2T100uaGSX9tBkTglGdrl lFKrJo7zjWEO400Y
yN/snn45UdwvWzyk9BM84z/0w+Rr7cPj l tYDSzdHAgMBAAGjeDB2MAkGA1UdEwQC
MAAwKQYJYIZIAIYb4QgENBBWgKZVRE8gVGvtcG9yYXJ5J5IEN lcnRpZml jYXR lMB0G
A1UdDgQWBBSXBvJ7BT1XBe8BxZHvQK9 lLSnTbTAfBgNVHSMEGDAWgBSXBvJ7BT1X
Be8BxZHvQK9 lLSnTbTANBgkqhkiG9w0BAQ0FAAOCAGEAqPzZVty1N6UsD5oKUQj7
N5 l3mr2D30nxGBNMaohdTqfZ lLoXRRc5szrzXyhK1Vx l t lJa1andt6BGTqi7eVp
Ur2s9hwABwSKEujr lPnT+rukqgB6EyDvCjuocr3GVub/xs+ssCHjAXHqXxevX7T xn
AMj l0Yi2PTjyo15v9WixQA74 l lJP4nV4ed4N9gSM0cLCceQmEDjaNzv lUW1zZYhs
IfXqFuRs6Xj2zaczYQWnk6RgBL600yngSt5Ey1vScHyTKXSRLuha0Atav51LJmi
rLAXcjdGK+Ag7rPIjIMwz1vxtnrsvrDwjpa80KHndUS9xFgnxG6g3EAE9V802gA
aB5BFJnW/Hhm7GghTMc+vBFT lkt5fxd2+T6dt inZaX7rdkH7JRK9p9G2j8Zrc5HT
li4To1oSTL/3VtbrzVdXqT8QpiLF23IAKMWhDkeqZPwqGmhW0xcnTgSEu3yA1TZe
cwdrUSHy01DZ0A1bHUYzc0G/s9NMasNctqkc29iRypnPuhQAZL fCDxPgiNv/LFx
ZVwKX0TftGZAx3YB0LH0kbQwCzEzwFXdpGBEzwiYE9JFmNGV l m2 l lHz3rdXLkwX
kqdn0QQNKiuojE9KKZTZ42T+32UwUpfJjfkNHzHq4AeQ1FzQ8H5HFzz7uhx7N
yf0IGHrrafLJj9Qg2dtNhJo=
-----END CERTIFICATE-----

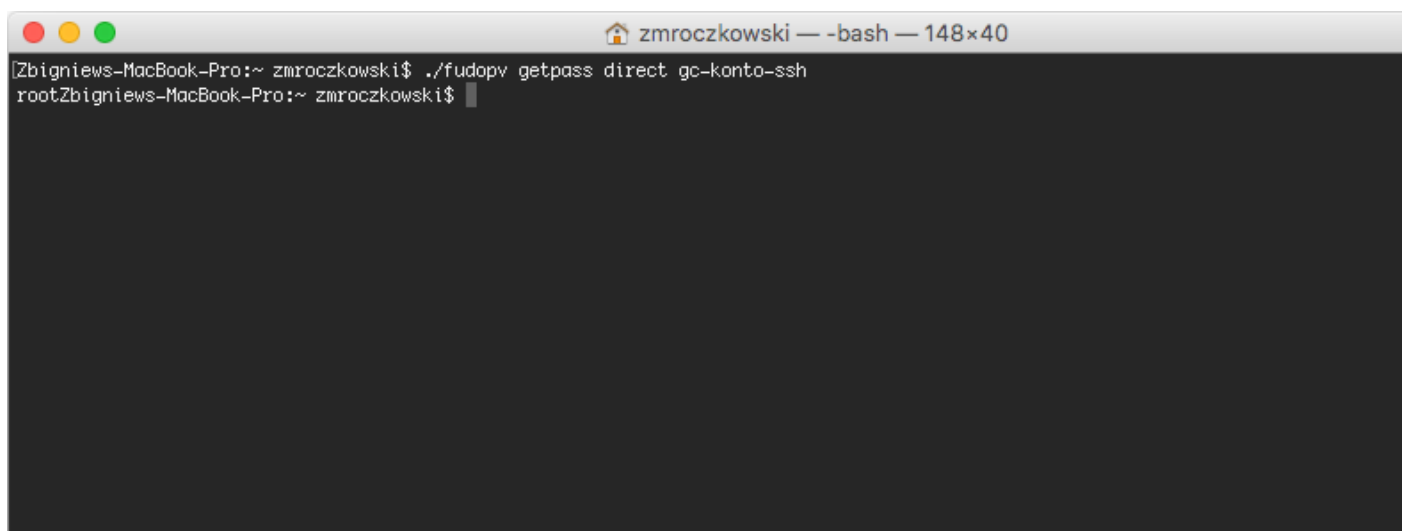
SHA1 Fingerprint: 2cba43a291fdcf71849ae1dfa9e19bcfc2795df8
Do you want to accept this certificate (yes/no)? : yes
Certificate has been successfully downloaded.
Configuration file has been updated.
Zbigniew-MacBook-Pro:~ zmroczkowski$

```

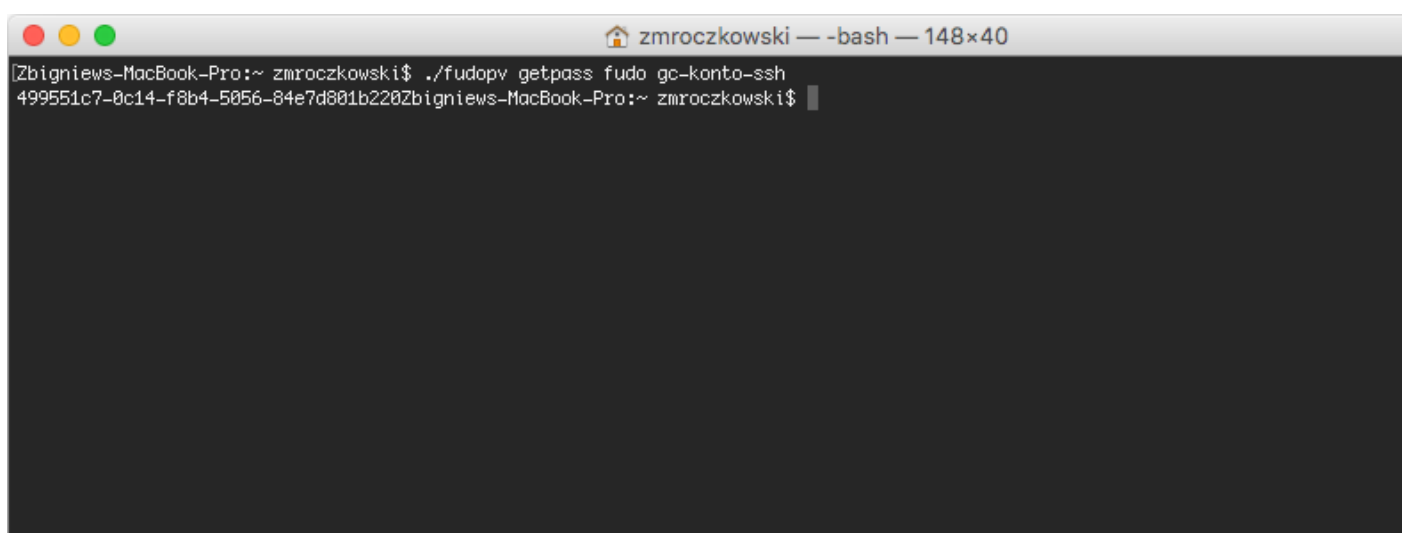
Note: After running the script successfully, the path to the certificate in the configuration file will be automatically updated.

-

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

A terminal window titled 'zmroczkowski — -bash — 148x40' is shown. The prompt is '[Zbigniew-MacBook-Pro:~ zmroczkowski\$]'. The user enters the command './fudopv getpass direct gc-konto-ssh'. The prompt changes to 'rootZbigniew-MacBook-Pro:~ zmroczkowski\$'.

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

A terminal window titled 'zmroczkowski — -bash — 148x40' is shown. The prompt is '[Zbigniew-MacBook-Pro:~ zmroczkowski\$]'. The user enters the command './fudopv getpass fudo gc-konto-ssh'. The prompt changes to '499551c7-0c14-f8b4-5056-84e7d801b220Zbigniew-MacBook-Pro:~ zmroczkowski\$'.

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

The screenshot shows a 'General' configuration window. It contains the following fields and options:

- ID:** 848388532111147017
- Name:** gc-self
- Blocked:** ☐
- Login reason:** ☐ (A blue callout bubble points to this checkbox with the text: "Make sure that the login reason option is disabled")
- Notifications:** ☐
 - ☐ Session start
 - ☐ Session join
 - ☐ Session policy match
 - ☐ Session finish
 - ☐ Session leave
- Policies:** policy

5.3 API interface

AAPM's API interface is described in detail in the *Wheel Fudo PAM 3.0 - API documentation* manual.

Related topics:

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

This section covers Wheel Fudo PAM administration topics.

6.1 System

6.1.1 Date and time

System events registered by Wheel Fudo PAM (sessions, system log events, etc.) are timestamped. Wheel Fudo PAM can obtain the time information either from an NTP server or the system clock.

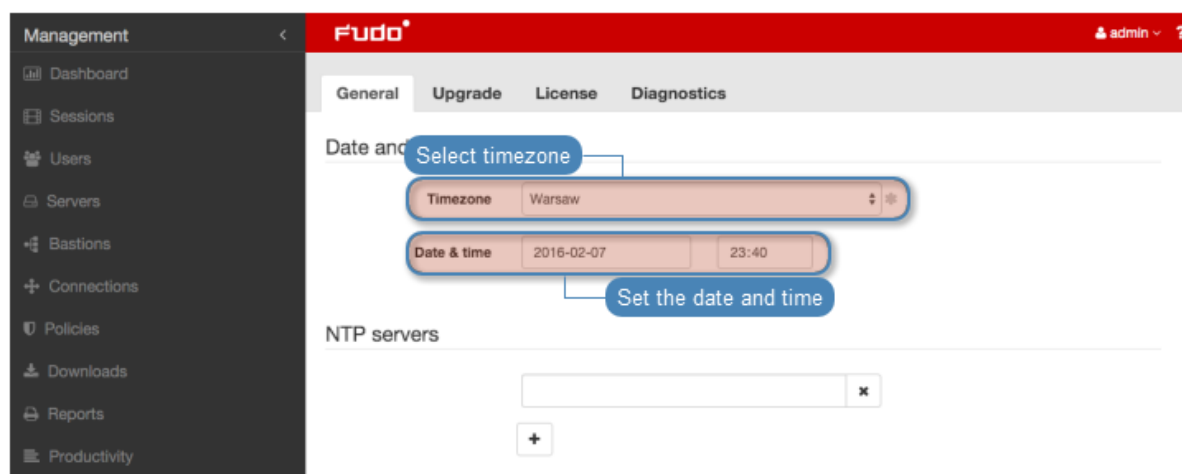
Warning: It is strongly advised for the date and time settings to be obtained from a reliable NTP server. Changing date and time settings manually may result in system malfunction.

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*.

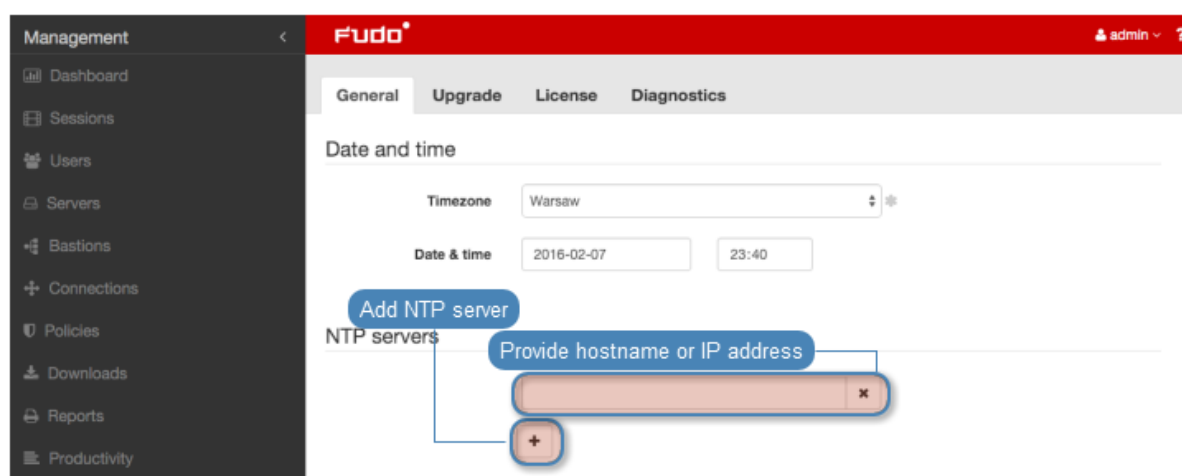
Time servers configuration

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.

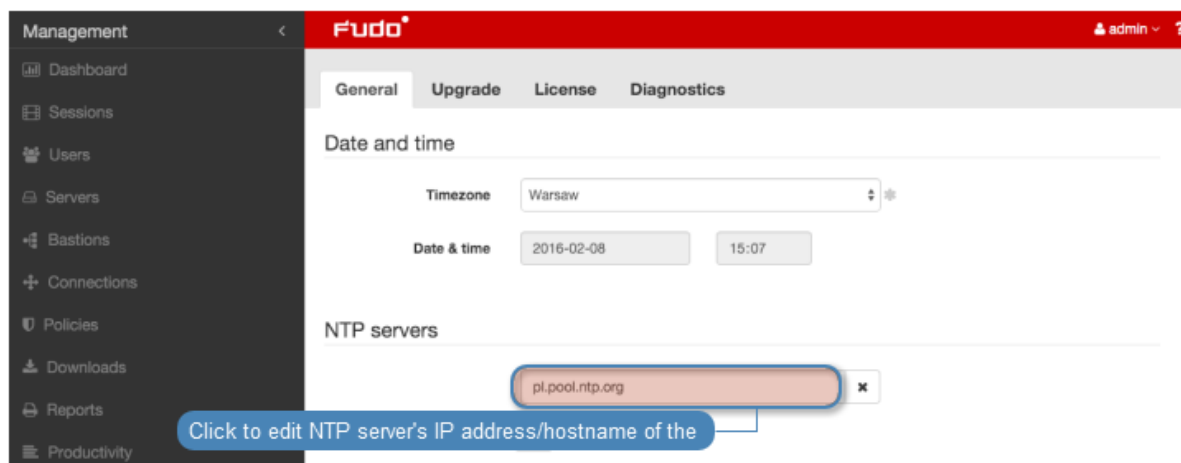


4. Click *Save*.

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.

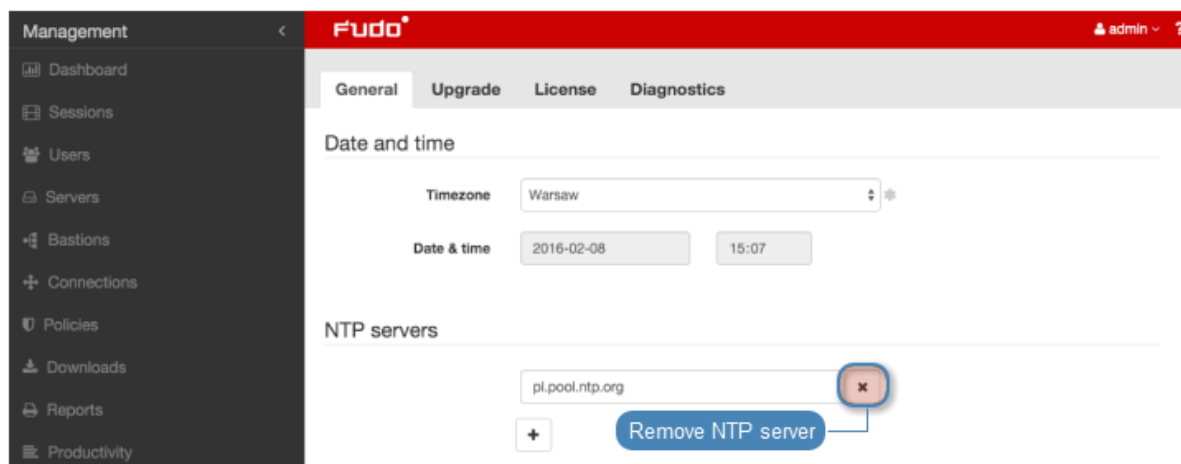


3. Click *Save*.

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*

6.1.2 SSL certificate

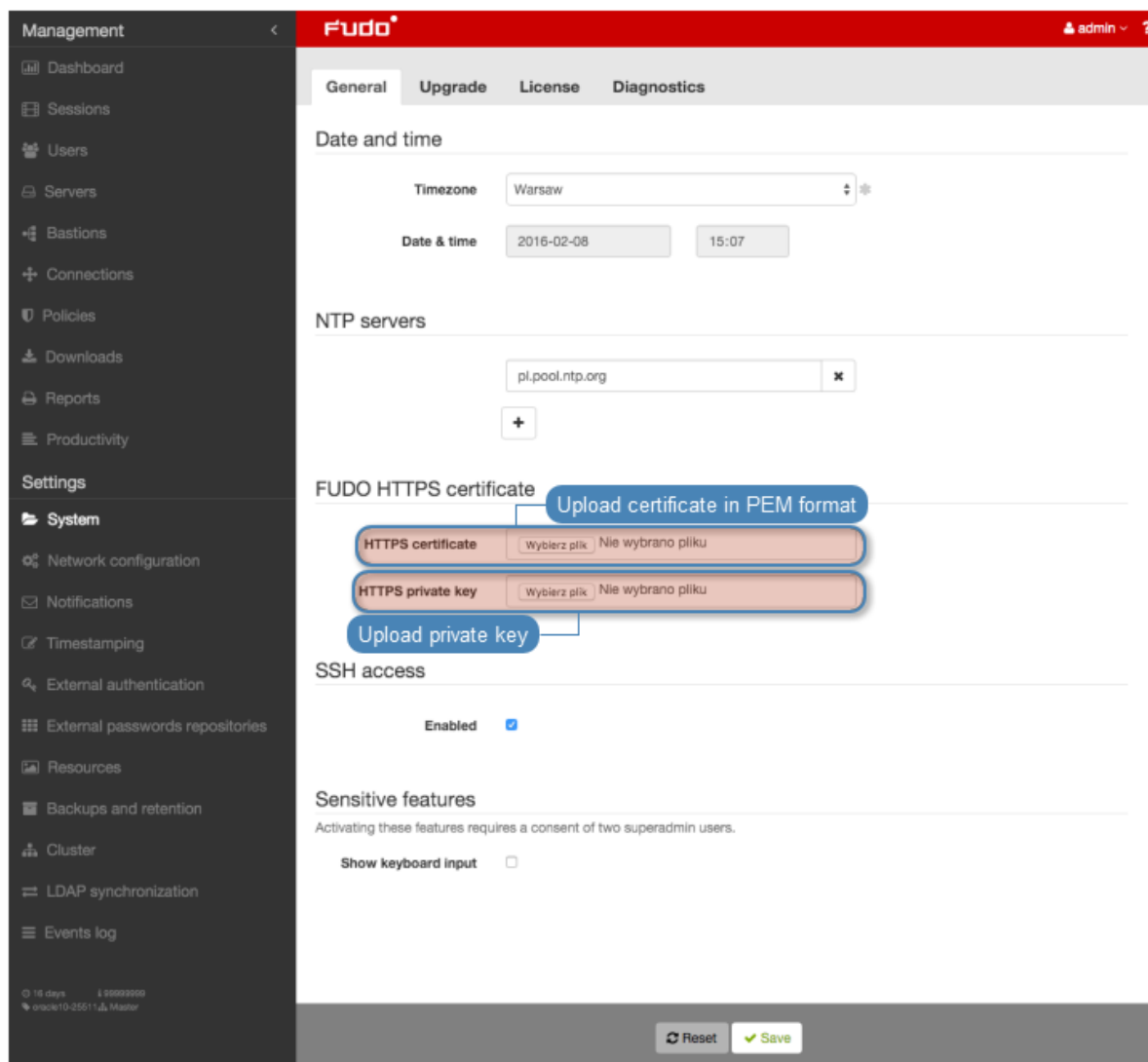
SSL certificate allows prevent phishing attacks.

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.

- Click the *Browse* button next to the *HTTPS Private Key* field and point to the location of the SSL key definition.



- Click *Save*.

Related topics:

- Security measures*
- Servers*

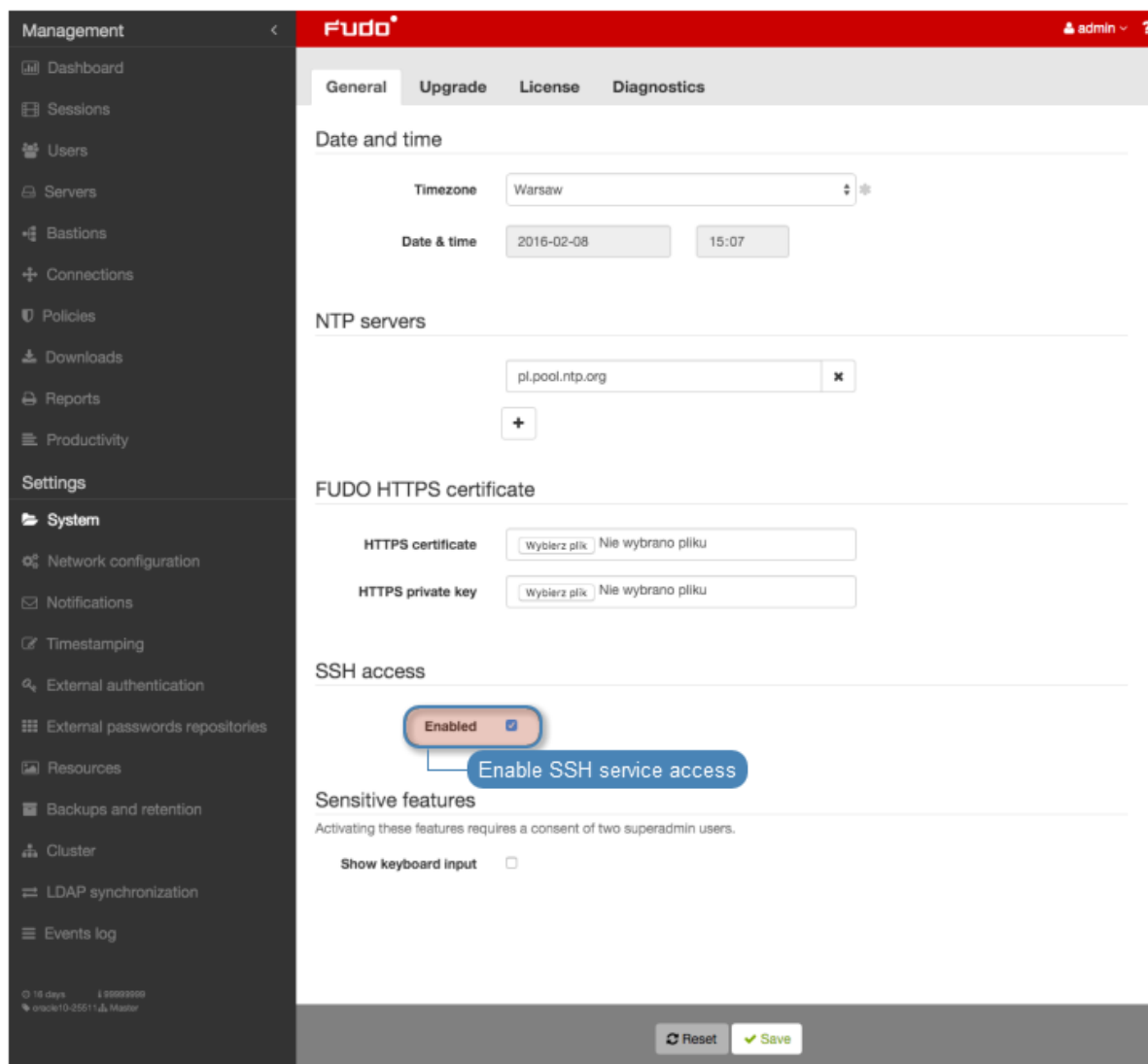
6.1.3 SSH access

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.

- Select *Settings > System*.
- Select *Enable SSH access* option in the *SSH access* section.



3. Click *Save* button.

Related topics:

- *Network interfaces configuration*

6.1.4 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](#)

6.1.5 System update

Note:

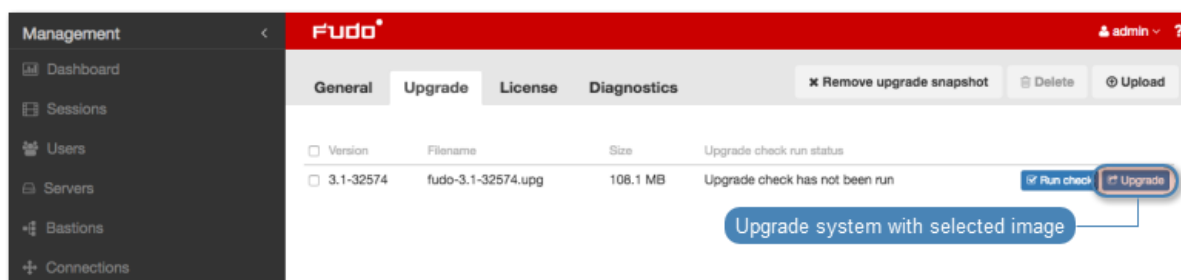
- In addition to the current system version, Wheel Fudo PAM stores the previous revision, allowing for restoring the system to its previous state.
- The system update process does not influence the system configuration or the session data stored on Wheel Fudo PAM.

6.1.5.1 Updating system

Warning:

- Before updating the system it is advised to run a preliminary check to ensure that the current system configuration can be successfully upgraded to new version.
- 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.

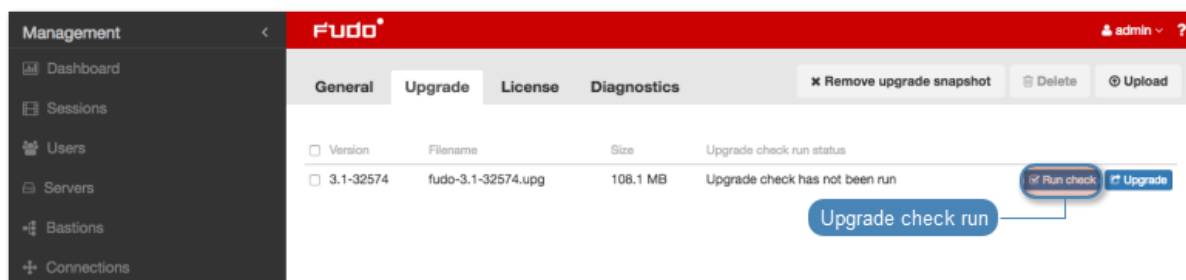
Note: In the event of an unsuccessful system update, Wheel Fudo PAM detects the problem during system restart and restarts itself using the previous system revision.

6.1.5.2 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:

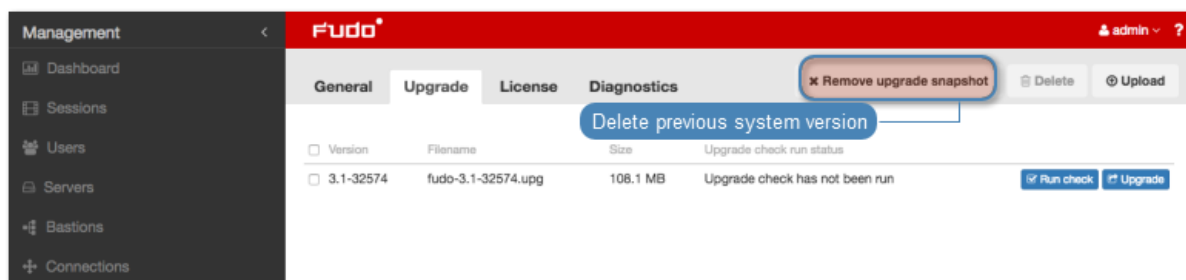
- Click *Cancel check* to stop the preliminary upgrade check.
- Click *Download log* to view the upgrade procedure log along with the information on how long it will take to perform the upgrade.

6.1.5.3 Deleting upgrade snapshot

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

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

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



4. Confirm deleting previous system version.

Related topics:

- *System version restore*
- *Restarting system*

6.1.6 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 shows the Fudo PAM 3.0 web interface. The sidebar on the left has a 'Management' section with links to Dashboard, Sessions, Users, Servers, Bastions, Connections, Policies, Downloads, Reports, and Productivity. Below this is a 'Settings' section with a 'System' subsection containing links to Network configuration, Notifications, Timestamping, External authentication, External passwords repositories, Resources, Backups and retention, Cluster, and LDAP synchronization. The main content area has tabs for General, Upgrade, License, and Diagnostics. The 'License' tab is selected, 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 status bar indicates '11 in use' and '14 available'. An 'Upload' button is in the top right corner. Below the form is a 'Usage statistics' section with a date range from 2015-11-01 to 2016-02-08. A bar chart titled 'Concurrent connections statistics' shows the number of concurrent sessions over time, with a peak of 5.0 on Wed 23.

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

Related topics:

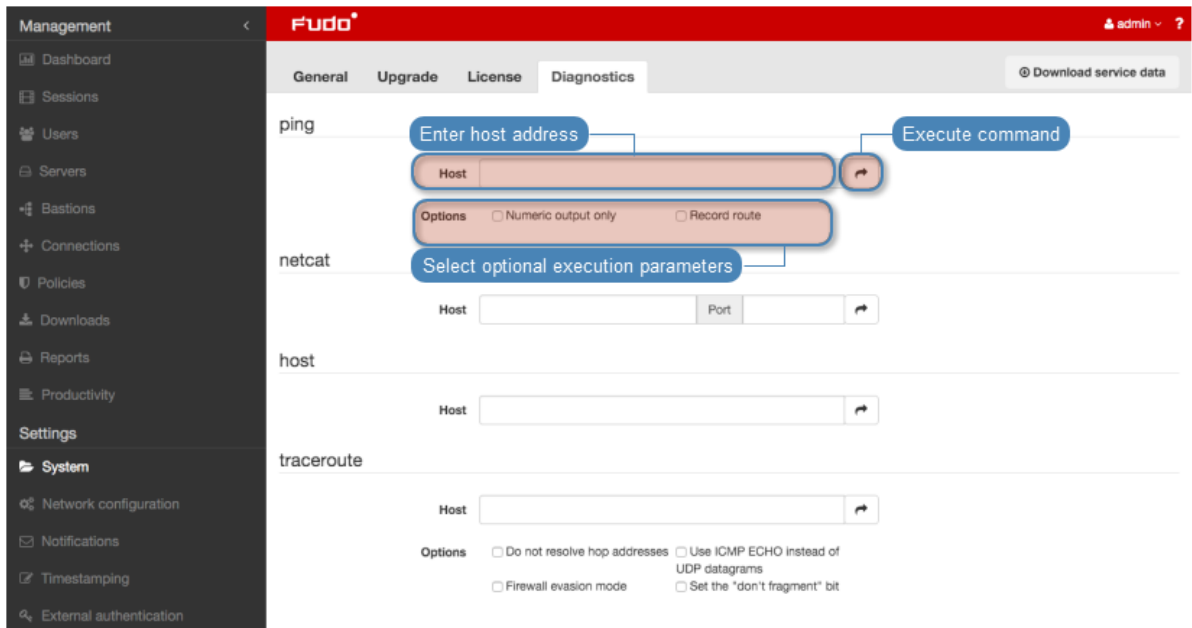
- *System*

6.1.7 Diagnostics

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

To run a diagnostic utility, proceed as follows.

1. Select *Settings* > *System*.
2. Select the Diagnostics tab.
3. Find desired utility, provide necessary parameters and execute the command.



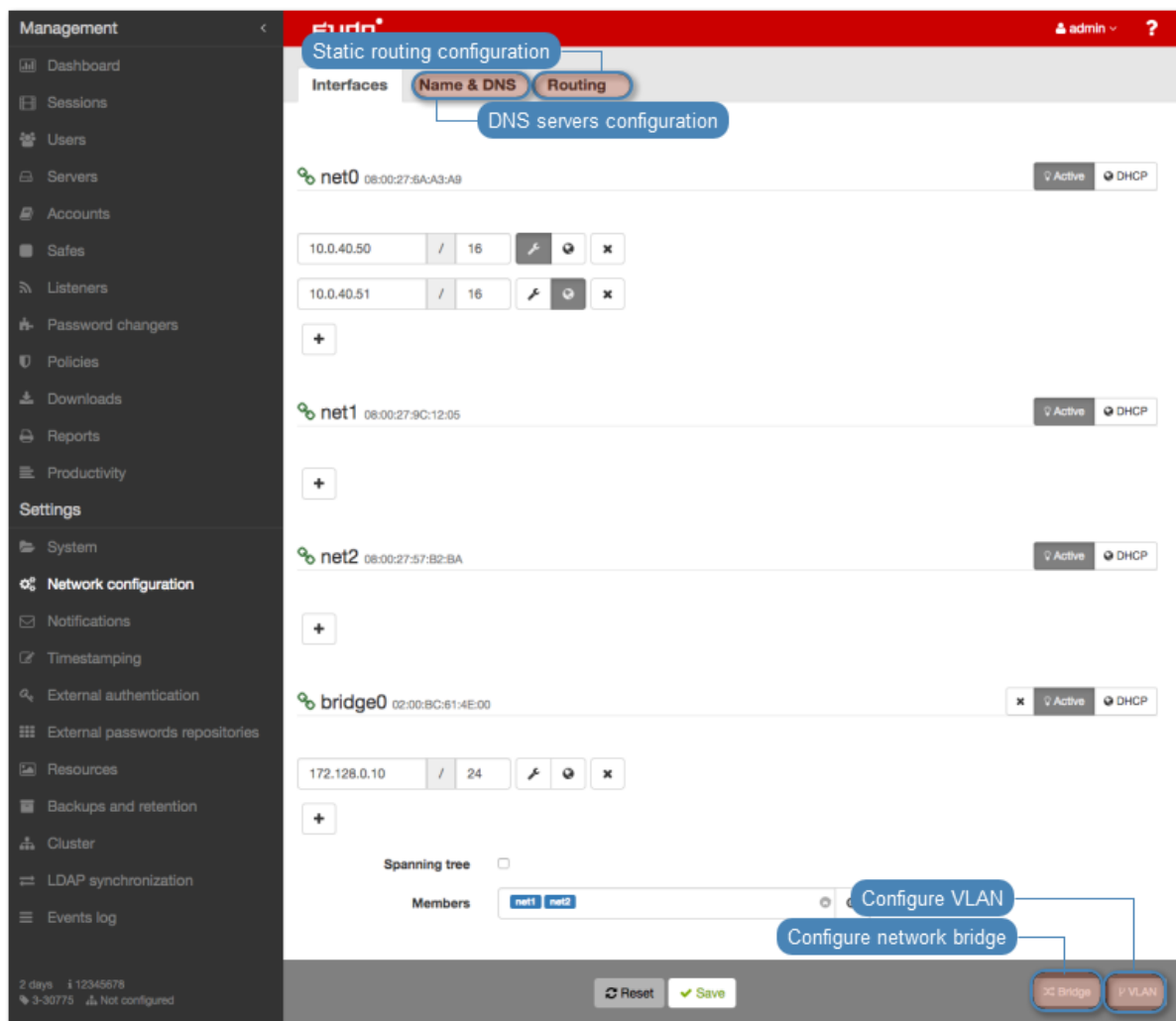
Command/parameter	Description
Ping	Ping sends a sequence of 10 ICMP packets to selected host.
Numeric output only	Does not resolve host's IP address to its mnemonic name.
Record route	Enables tracking packets' route.
netcat	etcat allows establishing connection with remote host on specified port number.
host	host is used to determine if the DNS server correctly resolves mnemonic hostnames.
traceroute	traceroute allows for determining packets' route between Wheel Fudo PAM and the specified host.
Do not resolve hop addresses	Subsequent hop IP addresses are not resolved to mnemonic names.
Use ICMP ECHO instead of UDP datagrams	Enforces traceroute to use UDP packets instead of ICMP.
Firewall evasion mode	Enforces the same port numbers for UDP and TCP packets. Target port is not incremented with each packet sent.
Set the "don't fragment" bit	Disables packet fragmentation in case the packet exceeds defined MTU (Maximum Transmission Unit) value defined for the network. Exceeding the MTU value results in an error.

Related topics:

- [Troubleshooting](#)

6.2 Network settings

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



6.2.1 Network interfaces configuration

6.2.1.1 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.

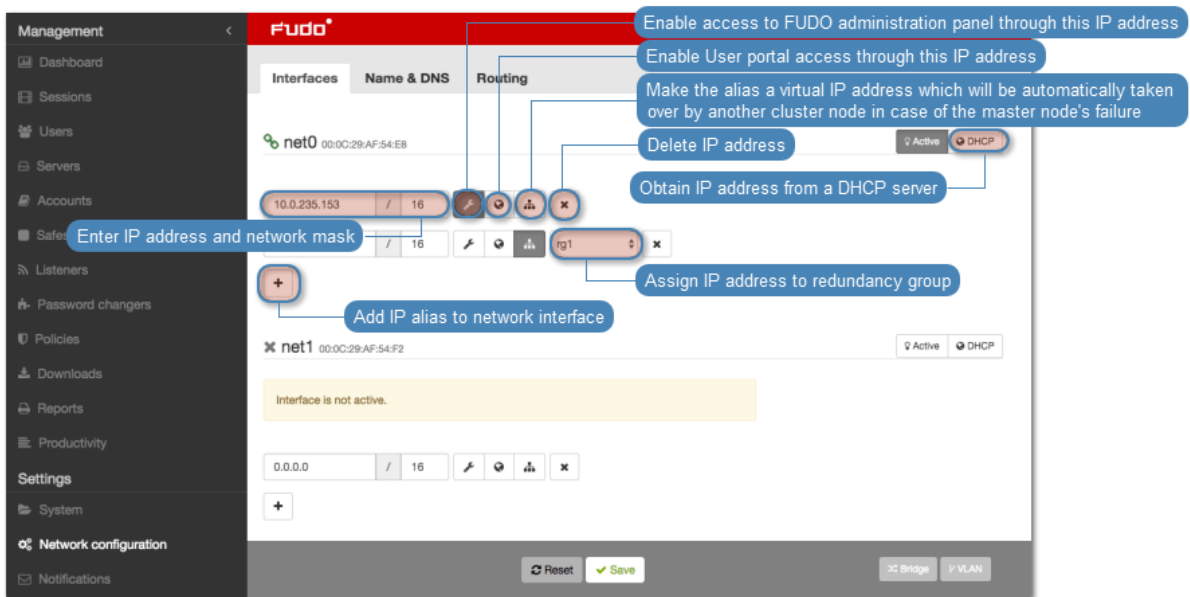
1. Select *Settings > Network configuration*.
2. Click *+* and provide IP address and subnet mask in CIDR format.

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.
	Enable access to <i>User portal</i> on given IP address.

4. Click *Save*.



Note: Current state of each network interface is represented with an icon.

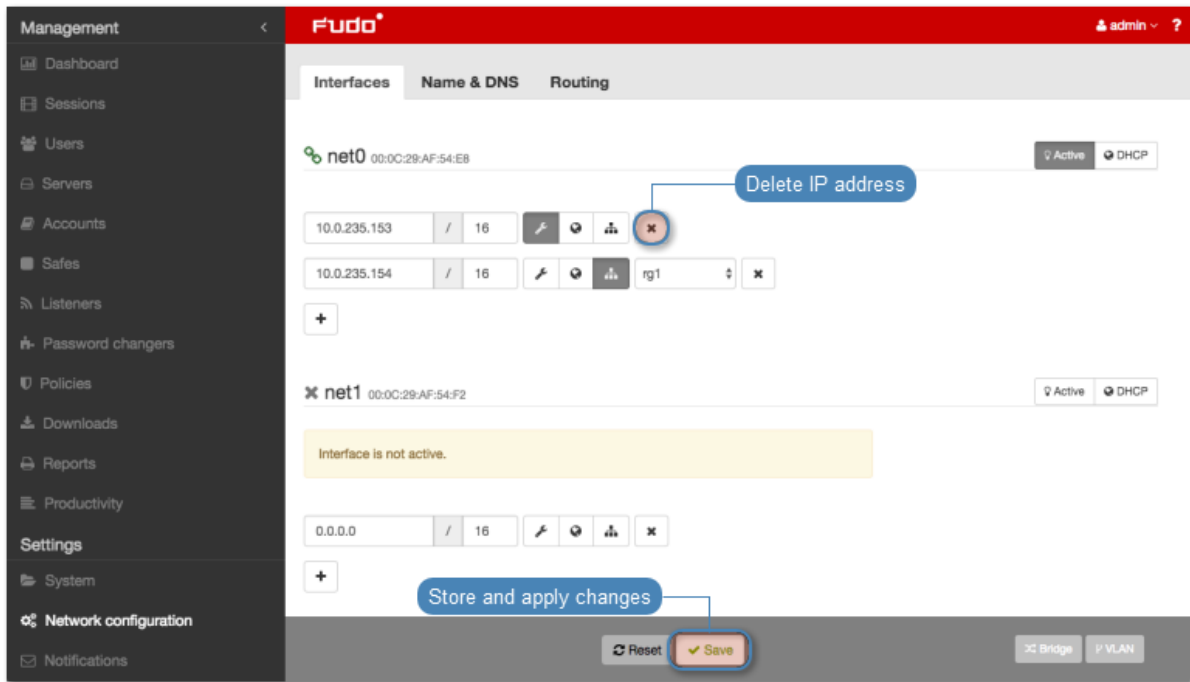
	Interface active and connected.
	Interface active but disconnected.
	Interface disabled.

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.

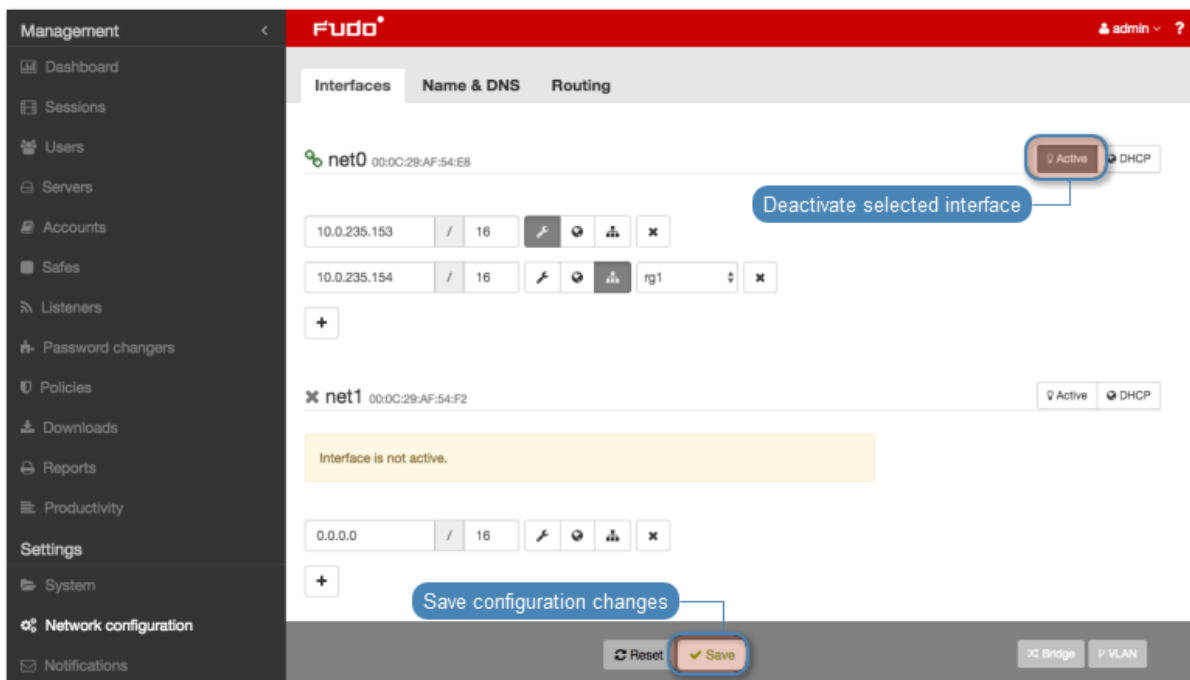
1. Select *Settings > Network configuration*.
2. Select desired IP address assigned to given network interface and click *x*.
3. Click *Save*.



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*.

6.2.1.2 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):
```

6.2.1.3 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*.



6.2.1.4 Setting up virtual networks (VLANs)

VLAN networks allow separating broadcast domains.

To configure a VLAN on , proceed as follows.

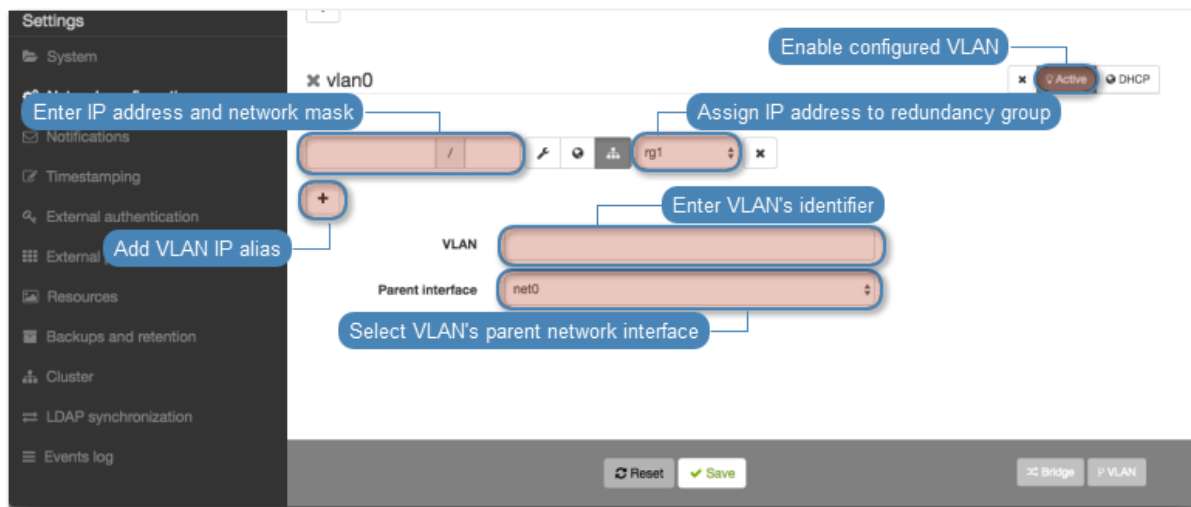
1. Select *Settings > Network configuration*
2. Click *VLAN*.
3. Select the physical interface and define VLAN ID.

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*.



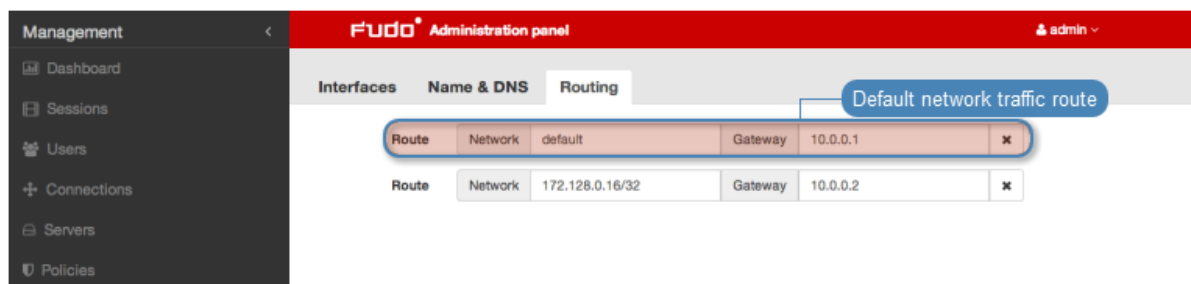
Related topics:

- *Servers management*
- *Accounts*

6.2.2 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

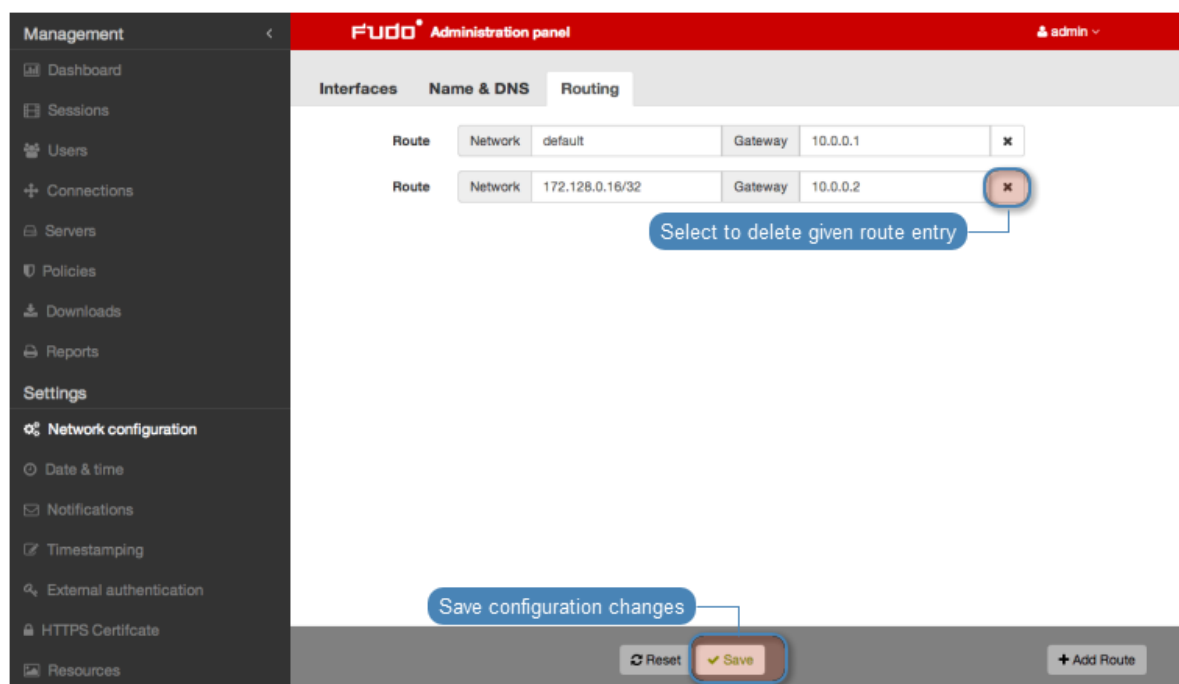
To edit a route, proceed as follows.

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*

6.2.3 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:

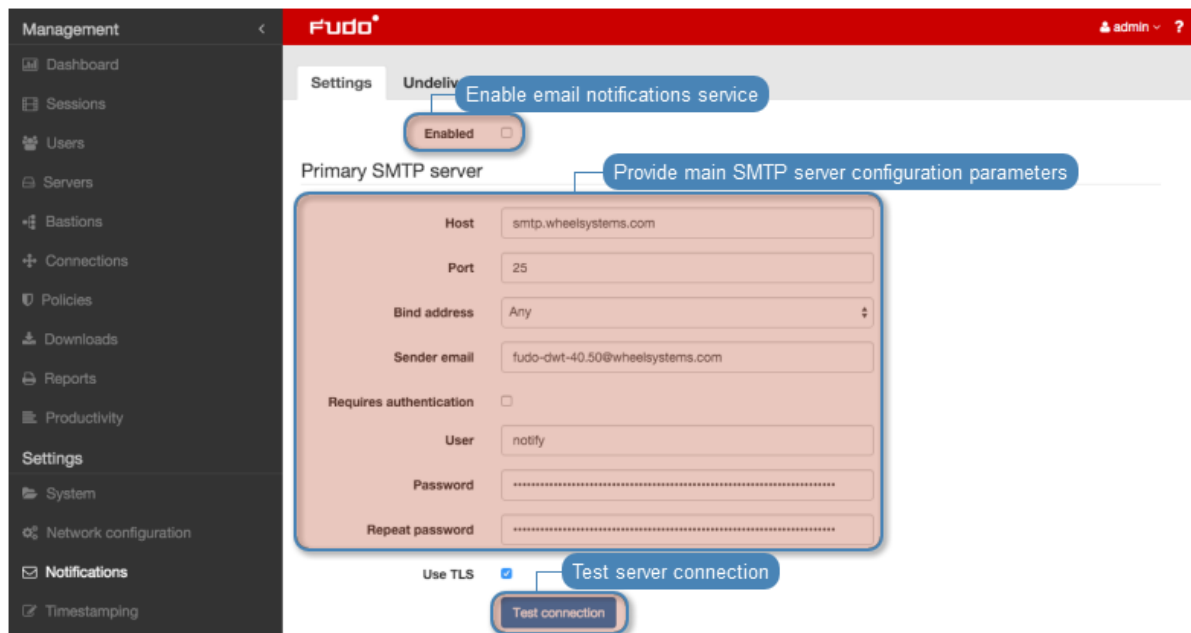
- *Network interfaces configuration*
- *Time servers configuration*

6.3 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.



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

Note: Click *Test connection* to make sure server parameters are correct.

- Optionally, enter configuration parameters for the secondary SMTP server.

Secondary SMTP server

Provide main SMTP server configuration parameters

Host

Port 25

Bind address Any

Sender email noreply@fudo.wheelsystems.com

Requires authentication ☐

User

Password

Repeat password

Use TLS ☐

Test server connection

Test connection

5. Enter server certificate in PEM format.

Secondary SMTP server

Provide main SMTP server configuration parameters

Host

Port 25

Bind address Any

Sender email noreply@fudo.wheelsystems.com

Requires authentication ☐

User

Password

Repeat password

Use TLS ☐

Test server connection

Test connection

6. Click *Save*.

Related Topics:

- [Accounts](#)

6.4 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

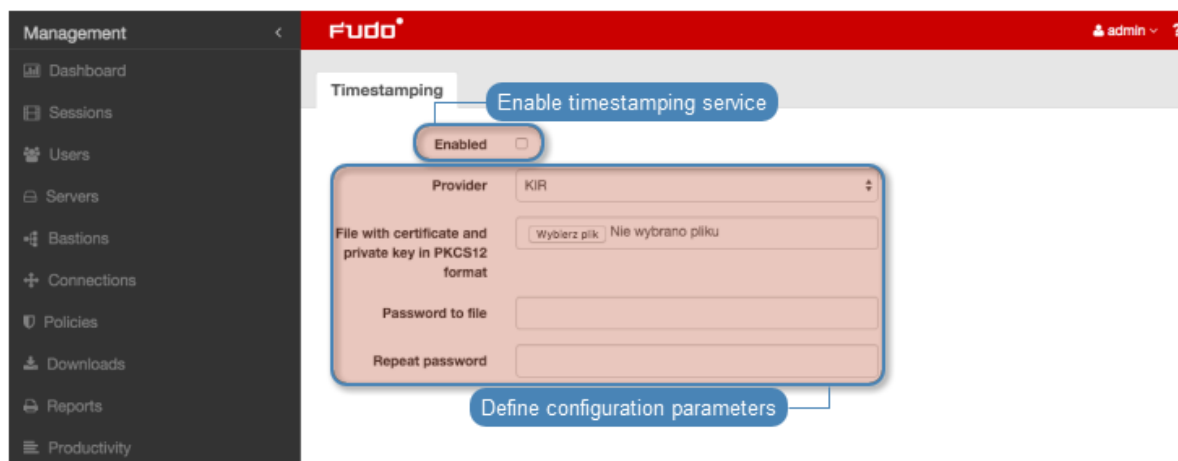
Note: Wheel Fudo PAM will also timestamp sessions recorded before the feature was enabled.

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*

6.5 External authentication

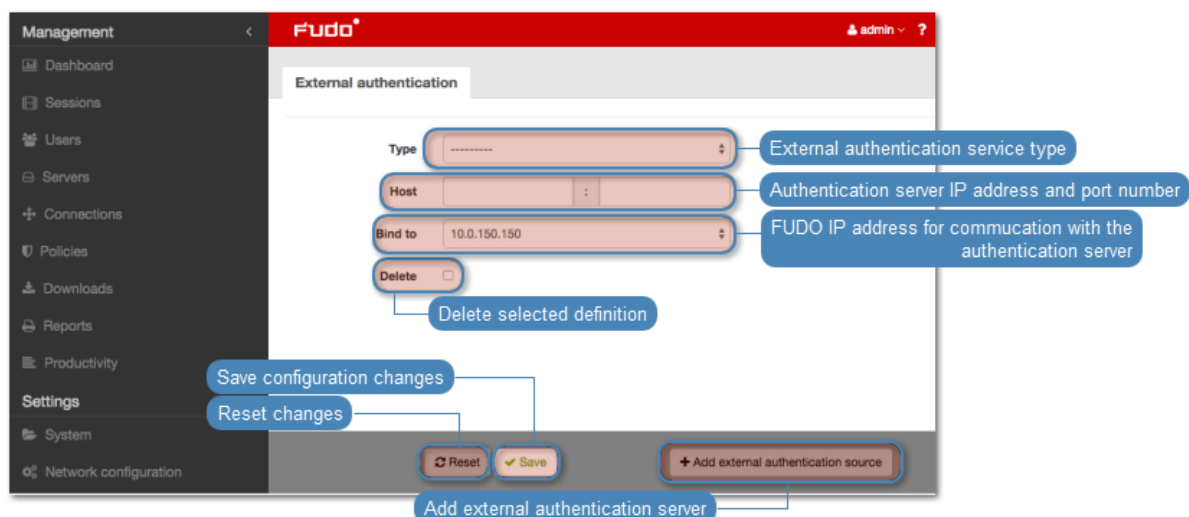
Some of the authentication methods, require defining connections to external authentication servers. These are:

- *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	
IP	Server's IP address.
Secret	Secret used to establish server connection.
Service	CERB service used for authenticating Wheel Fudo PAM users.
RADIUS	
IP	Server's IP address.
Port	Port used to establish connections with given server.
Secret	Secret used to establish server connection.
NAS ID	RADIUS server NAS-Identifier parameter.
LDAP	
IP	Server's IP address.
Port	Port used to establish connections with given server.
User DN template	Template containing a path which will be used to create queries to LDAP server.
Active Directory	
IP	Server's IP address.
Port	Port used to establish connections with given server.
Domain	Domain which will be used for authenticating users in Active Directory.

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](#)

6.6 External passwords repositories

Wheel Fudo PAM supports external passwords repositories for managing passwords to monitored servers.

Adding a new passwords repository

To add a passwords repository definition, proceed as follows.

1. Select *Settings > External passwords repositories*.
2. Click *+ Add server*.
3. Provide configuration parameters.

Parameter	Description
Type	External passwords repository type.
Name	Repository definition name.
URL	URL to the passwords server's API.
Authenticator (applicable to Lieberman ERPM servers)	User's authentication module as defined in the passwords repository.
Login	Login of the user allowed to browse passwords repository contents.
Password	User password.
Repeat password	User password.
Secret format (applicable to Thycotic Secret Server)	Secret string formatting definition used for identifying objects on Thycotic Secret Server.

Management < Fudo[®] admin ?

External passwords repository

Select repository type

Type Lieberman ERPm

Name

URL

Authenticator [Explicit]

Login

Password

Repeat password

Provide configuration parameters

Add passwords repository

Reset Save Add server

Note: For Hitachi ID PAM, the user specified in the configuration must be OTP (One Time Password) type.

Note: Specify the HTTPS protocol in the URL to enforce connection encryption.

Example: `https://10.0.0.2/PWCWeb/`

4. Click *Save*.

4. 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*

6.7 Resources

Wheel Fudo PAM enables customizing RDP and VNC login screen.

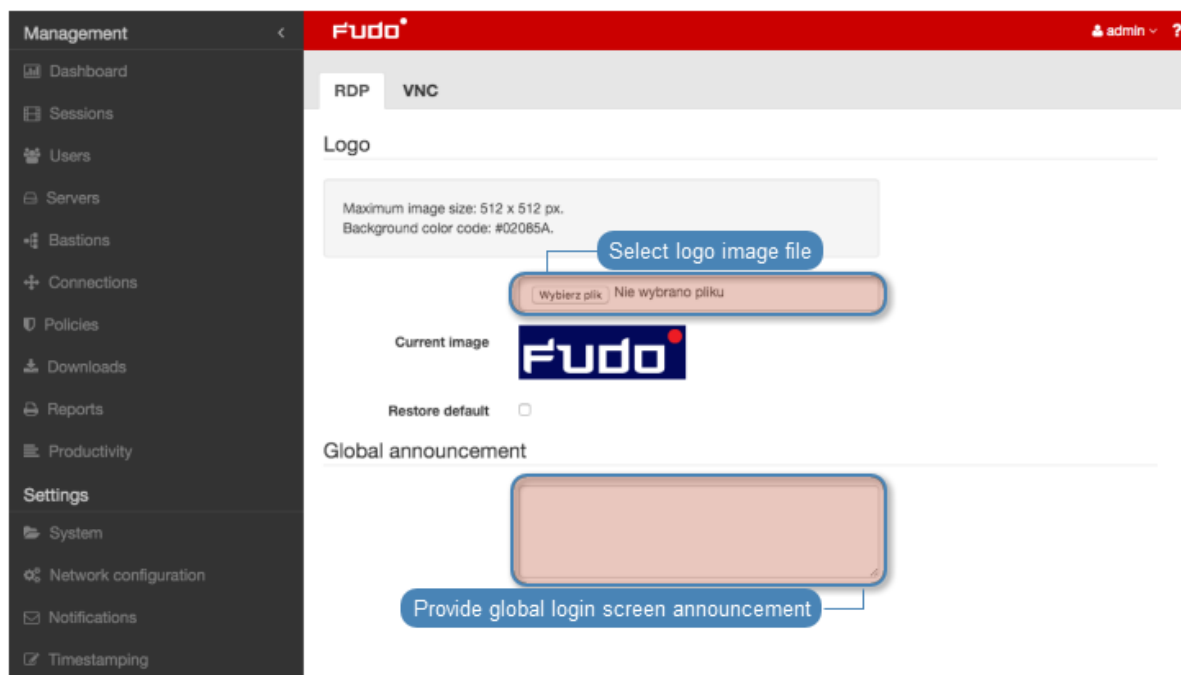


Changing logo

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](#)

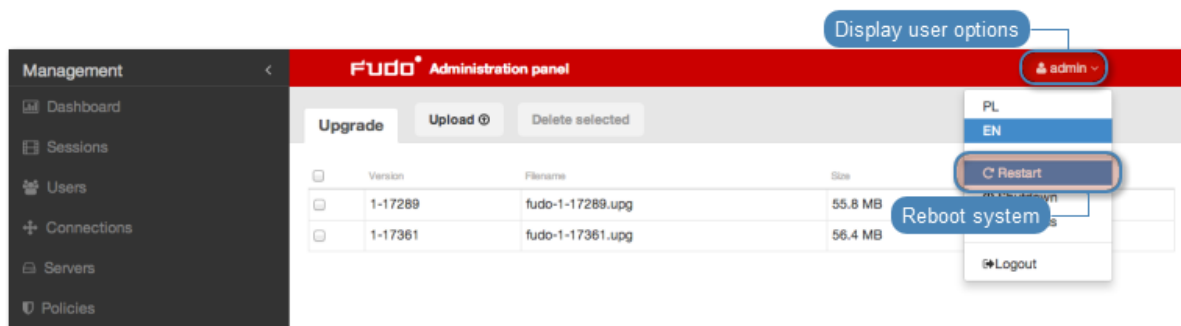
6.8 System version restore

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.

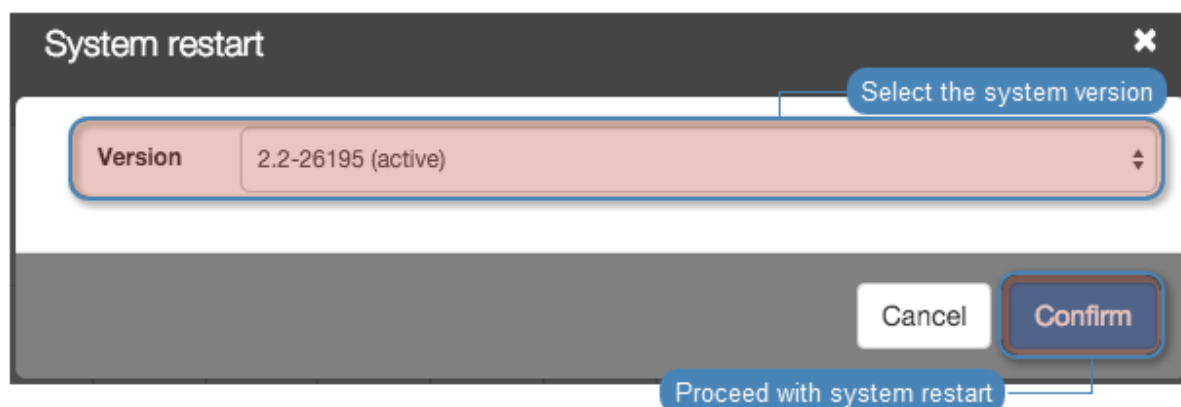
To restore the system to the previous revision, proceed as follows.

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.

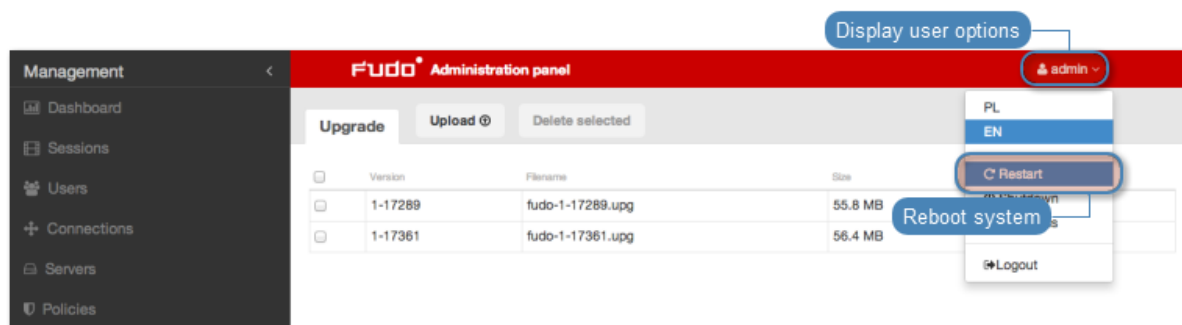
Related topics:

- *System initiation*
- *System update*

6.9 System restart

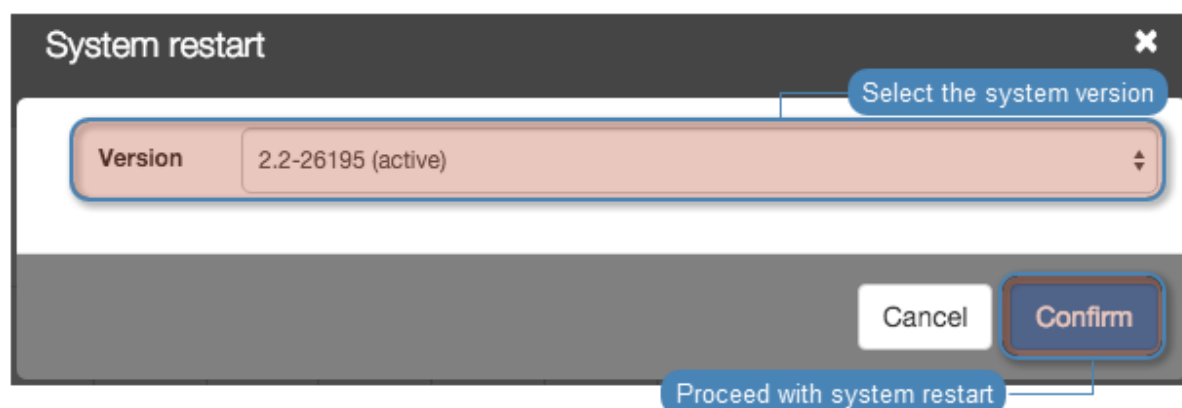
Note: System restart requires USB flash drive with the encryption key connected to the device.

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 version restore*

6.10 Backups and retention

Data retention

Data retention mechanism deletes session data older than the specified number of days.

To enable data retention service, proceed as follows.

1. Select *Settings > Backups and retention*.
2. Select *Enabled* option in the *Data retention* section.
3. Define how long data will be stored before being deleted.

Note: Global retention parameter value has lower priority than the value set in the *accounts*.

4. 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.

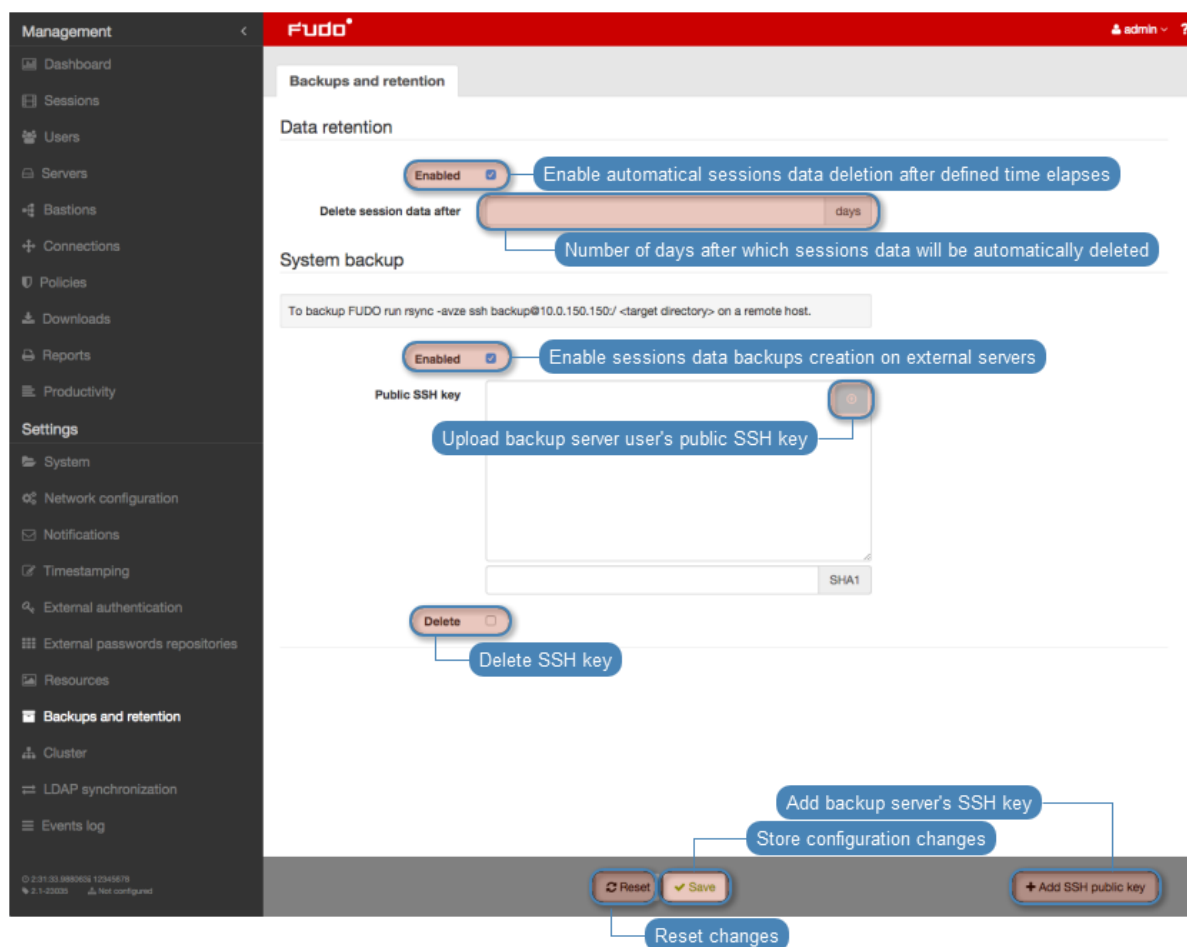
Automated data backup requires configuring **rsync** service on a remote server and granting access rights to data stored on Wheel Fudo PAM by uploading to Wheel Fudo PAM server's public SSH key.

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](#)

6.11 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.

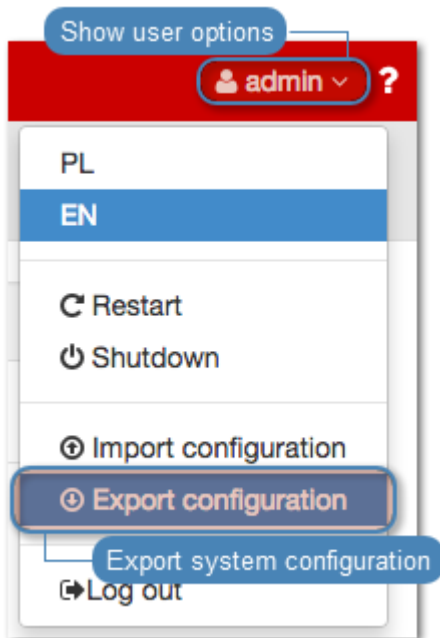
Warning: Exported configuration data contains confidential information.

Note: Configuration export and import options are available only for the *superadmin* users.

6.11.1 Exporting system configuration

To export system configuration, proceed as follows.

1. Select *Export configuration* from the user menu.
2. Save the configuration file.

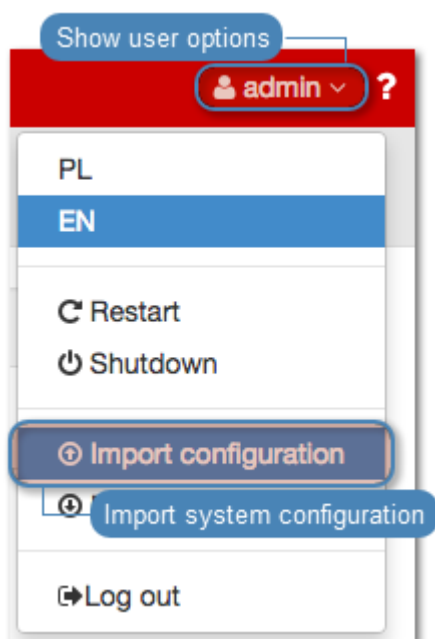


6.11.2 Importing system configuration

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*

6.12 Cluster configuration

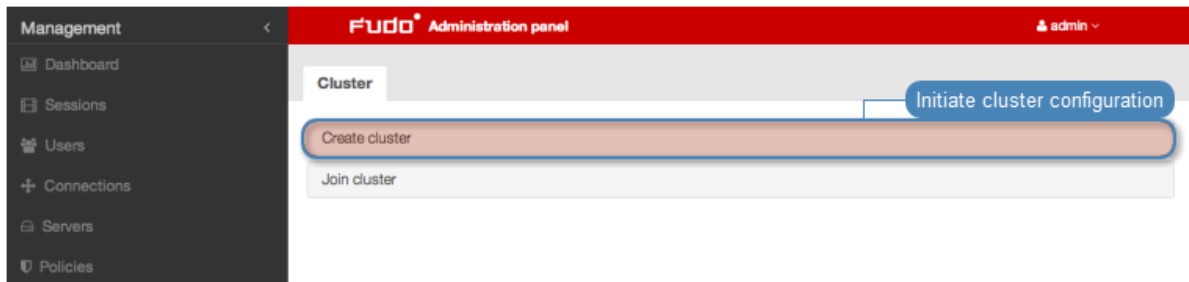
Wheel Fudo PAM cluster ensures uninterrupted access to servers in case of cluster node failure as well as enables implementing static load balancing.

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.

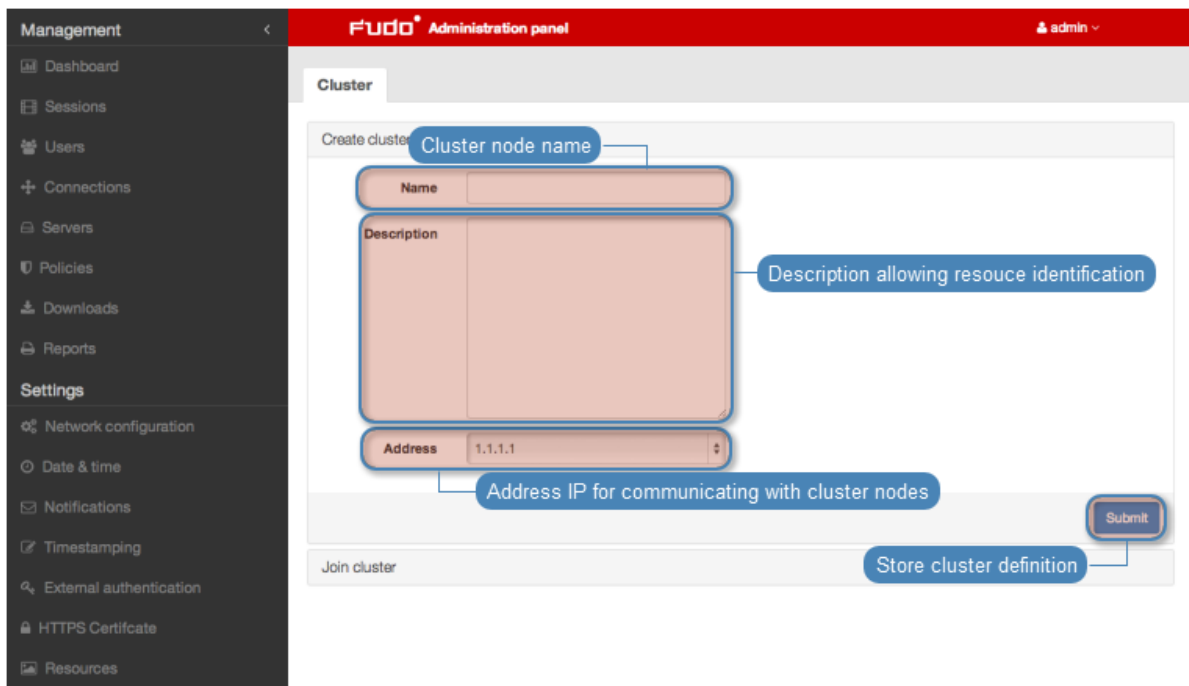
6.12.1 Initiating cluster

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:

- *Security: Cluster configuration*
- *Redundancy groups*
- *Cluster configuration*

6.12.2 Cluster nodes

Adding cluster nodes

Warning:

- Session and configuration data (connections, servers, users, 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.

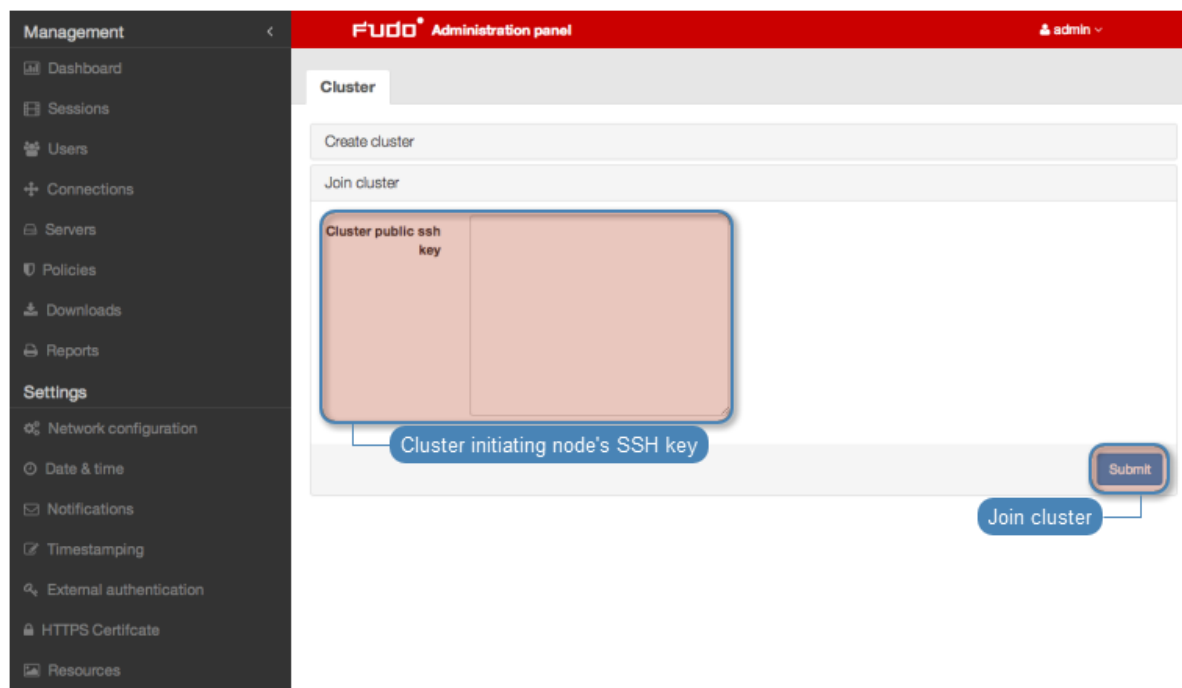
The screenshot displays the 'Fudo Administration panel' with a sidebar menu on the left. The 'Cluster' tab is selected, showing a form for adding a new node. The form includes fields for 'Name' (HACluster), 'Description' (High Availability Cluster), and 'Address' (10.0.8.64). There are checkboxes for 'Force full synchronization' and 'Delete'. A blue callout box points to the 'Initiating cluster node information' header, and another points to the '+ Add Node' button. The bottom of the form has 'Reset' and 'Save' buttons.

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*.



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*.

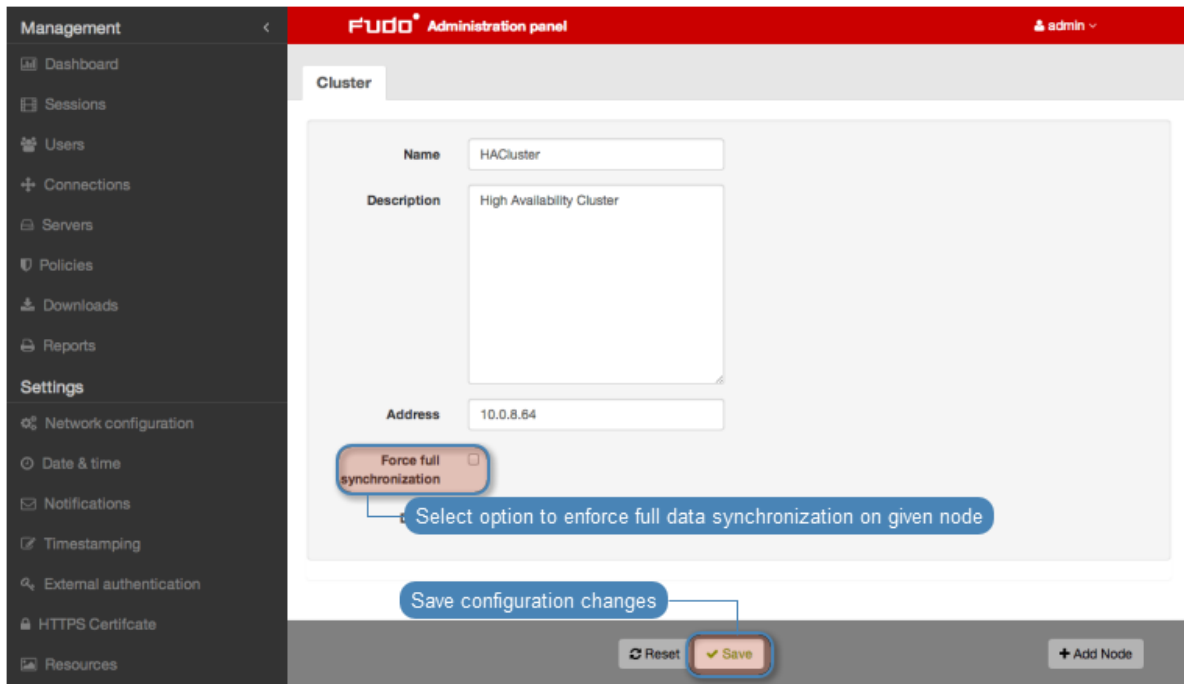
Forcing full data synchronization

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.

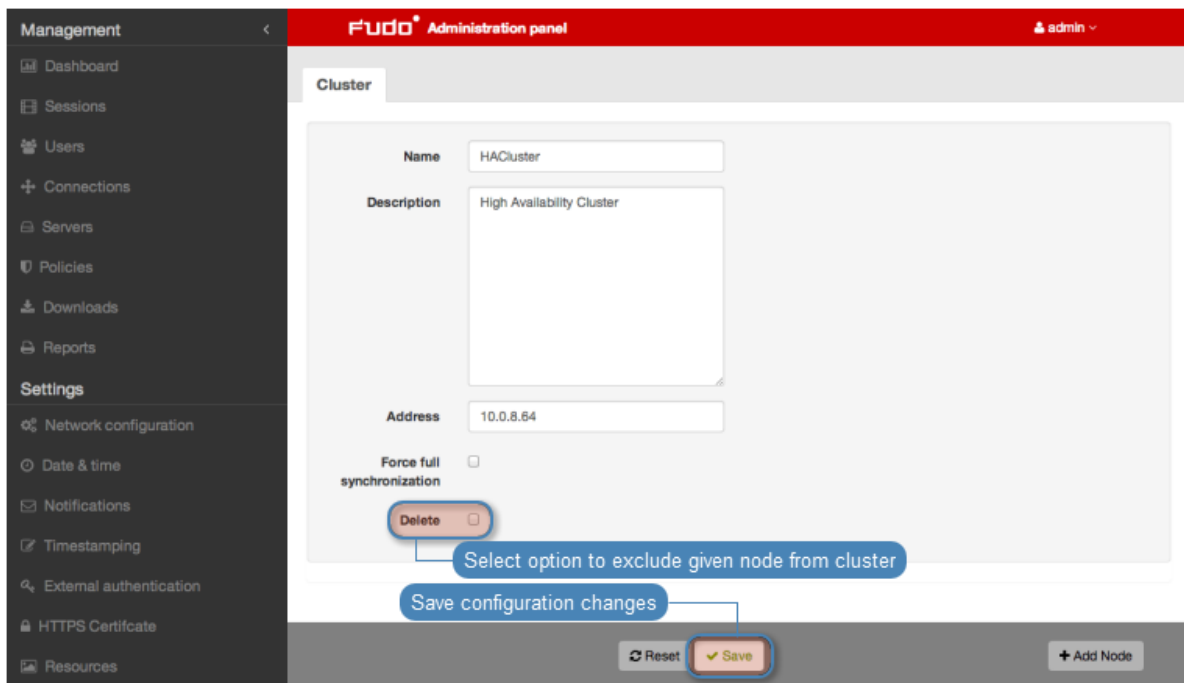
1. Log in to Wheel Fudo PAM administration panel on a node other than the one which requires synchronization.
2. Select *Settings > Cluster*.
3. Find and select node which requires data synchronization.
4. Select *Force full synchronization* option and click *Submit*.



Deleting cluster nodes

To delete a cluster node, proceed as follows.

1. Select *Settings* > *Cluster*.
2. Find desired node and select *Delete*.
3. Click *Submit*.



Related topics:

- *Security: Cluster configuration*

6.12.3 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 one of the remaining nodes with the highest priority defined for given redundancy group.
Interface	Network interface used for communicating with other cluster nodes.

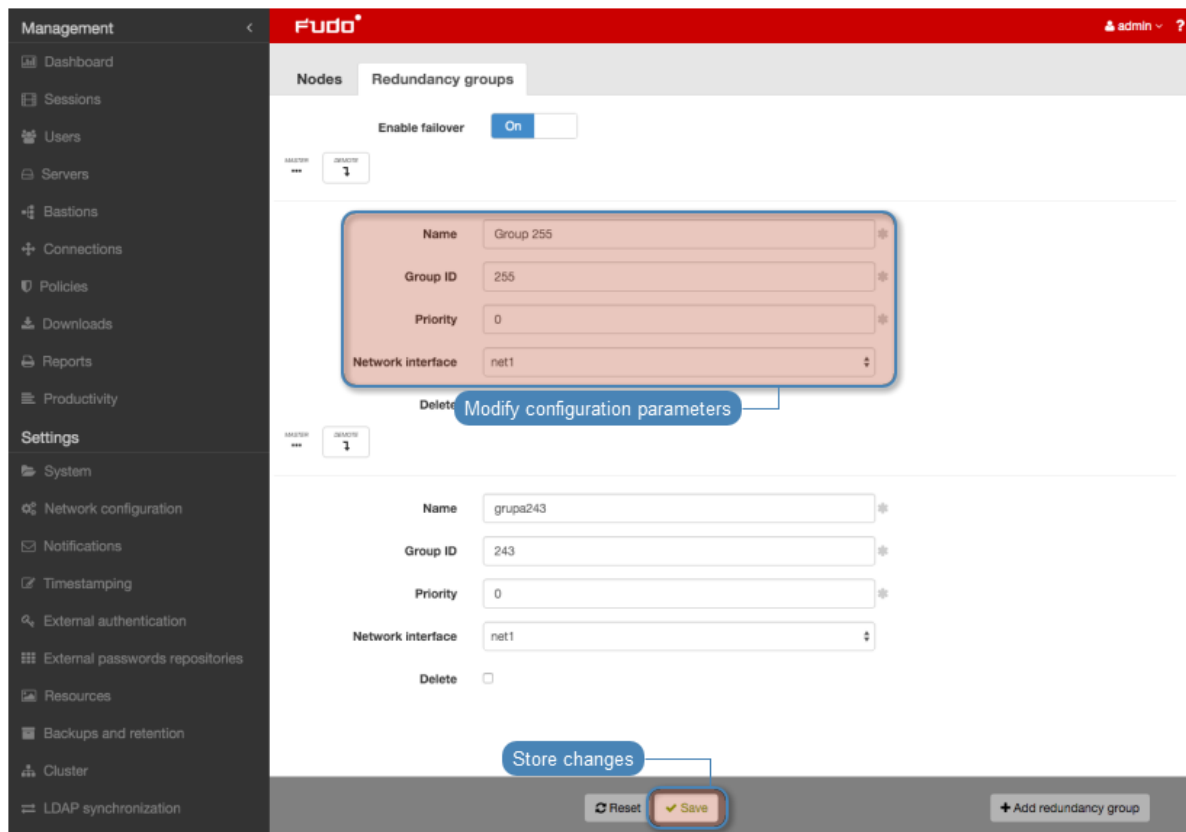


5. Click *Save*.

Editing redundancy groups

To modify a redundancy group, proceed as follows.

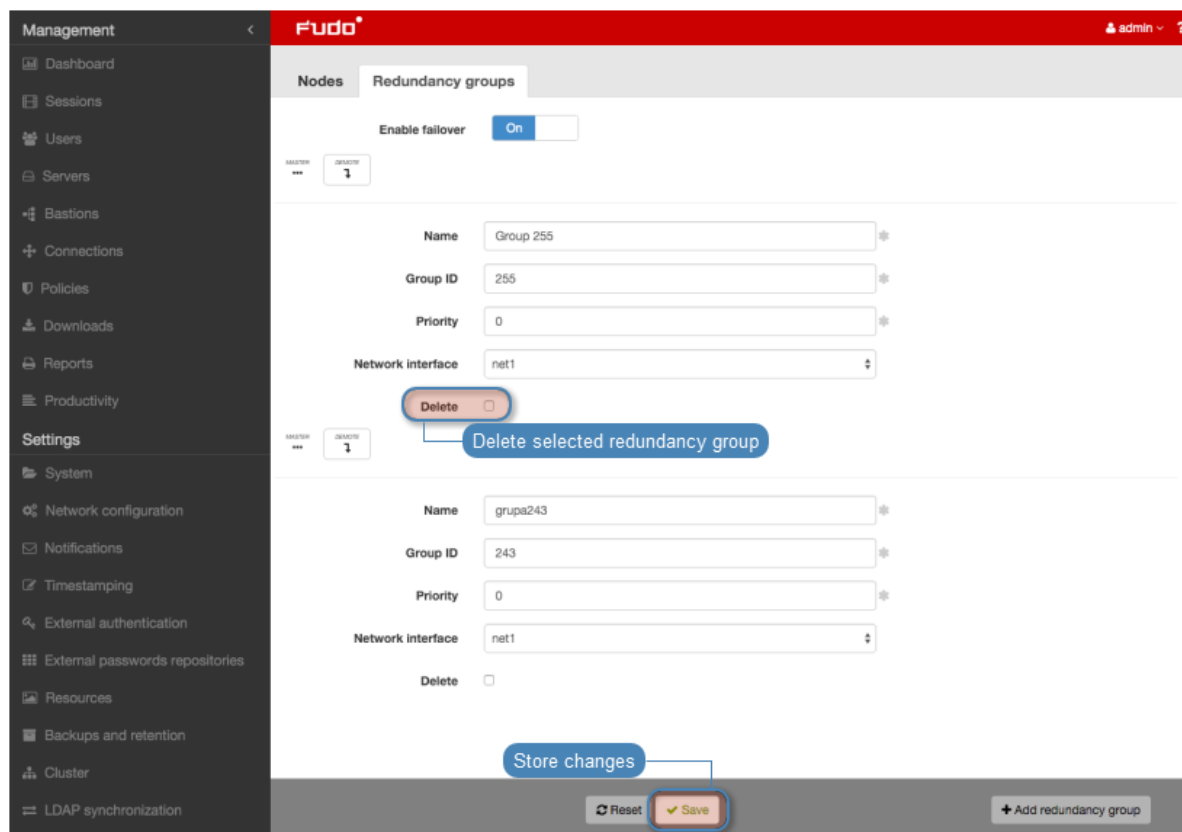
1. Select *Settings > Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Find and edit desired redundancy group definition.
4. Click *Save*.



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*.

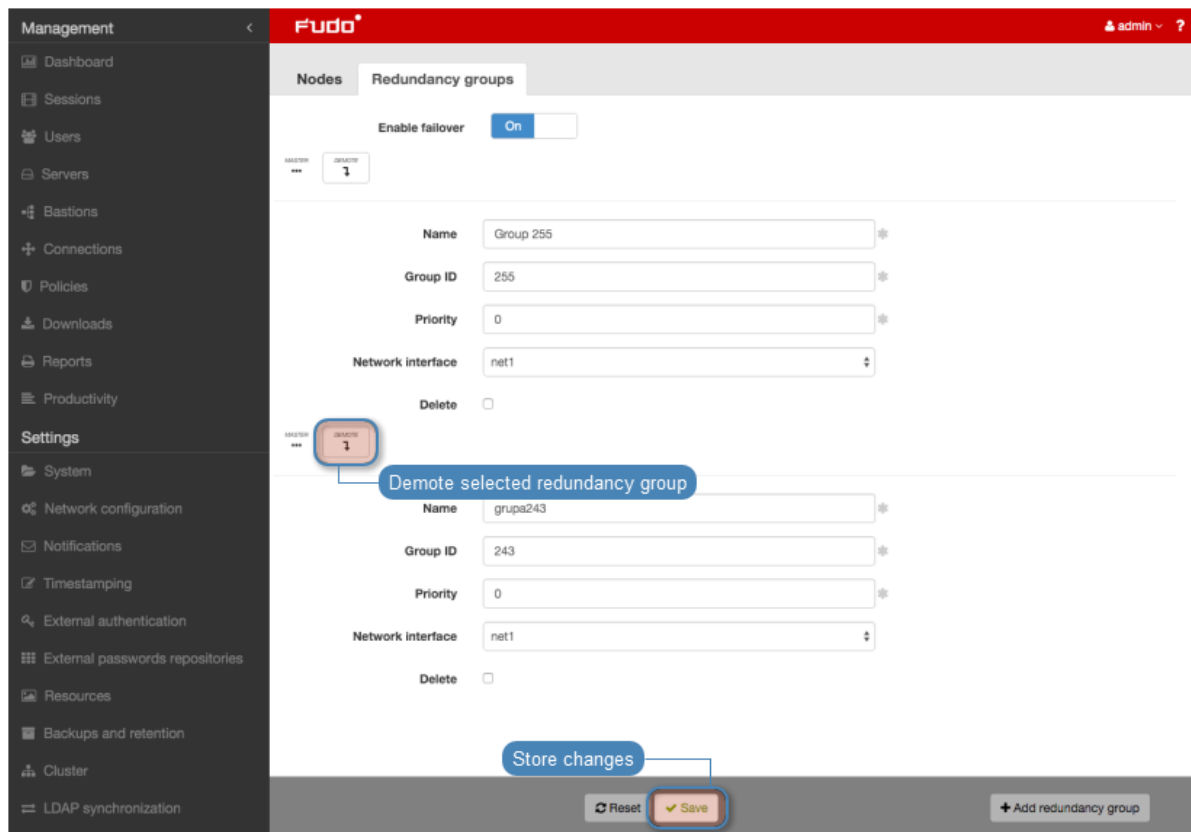


Demoting a redundancy group

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:

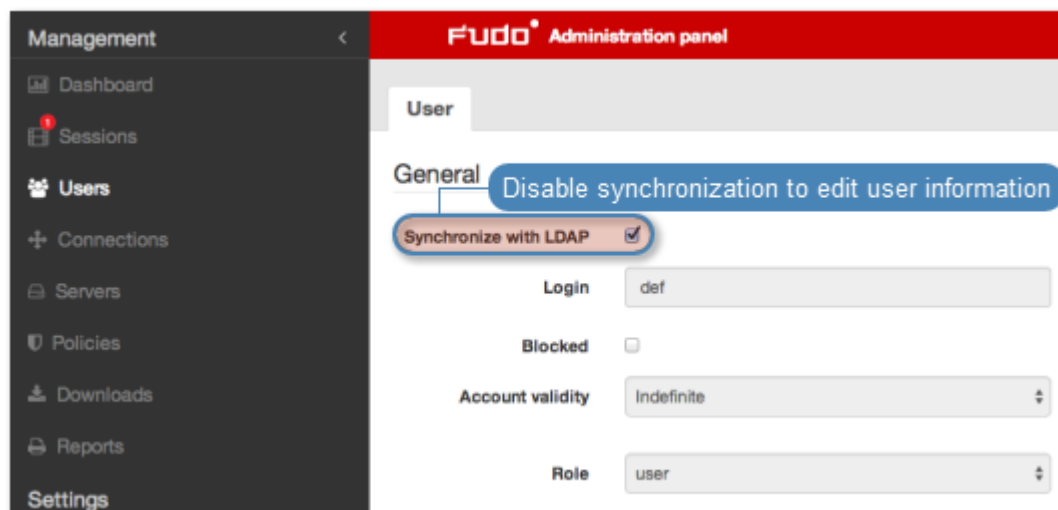
- *Security: Cluster configuration*
- *Initiating cluster*
- *Cluster configuration*

6.13 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. Provide the directory server's IP address and port number.
6. Enter domain name, to which imported users definition belong to.
7. Provide base DN for directory tree (eg. `DC=devel,DC=whl`).

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. 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*.

Attribute	LDAP Attribute
Login	sAMAccountName
Email	mail
Group assignment	memberof
Phone	telephoneNumber
Organization	company
Full name	displayName
Distinguished name	distinguishedName
GUID	objectGUID

External authentication

Define user information mapping for nonstandard attributes names

External authentication source

- ☒ Active Directory 10.0.40.100:389 domain:tech.whl
- ☐ Active Directory 10.0.40.101:389 domain:tech2.whl

Group mappings

+

Reset Save Force full synchronization

11. Select external authentication services which will be automatically assigned to user definitions imported from the directory service.
12. Assign safes to user groups.
13. 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

The screenshot shows the 'Group mappings' interface. It contains two mapping entries. The first entry is for 'Group B' mapped to 'Connection RDP'. Its dropdown menu shows 'CERB' and 'Radius' checked, and 'AD' unchecked. The second entry is for 'Group A' mapped to 'Connection SSH'. Its dropdown menu shows 'CERB' and 'Radius' unchecked, and 'AD' checked. There is a '+' button below the 'Group A' entry and a search icon next to each mapping's dropdown.

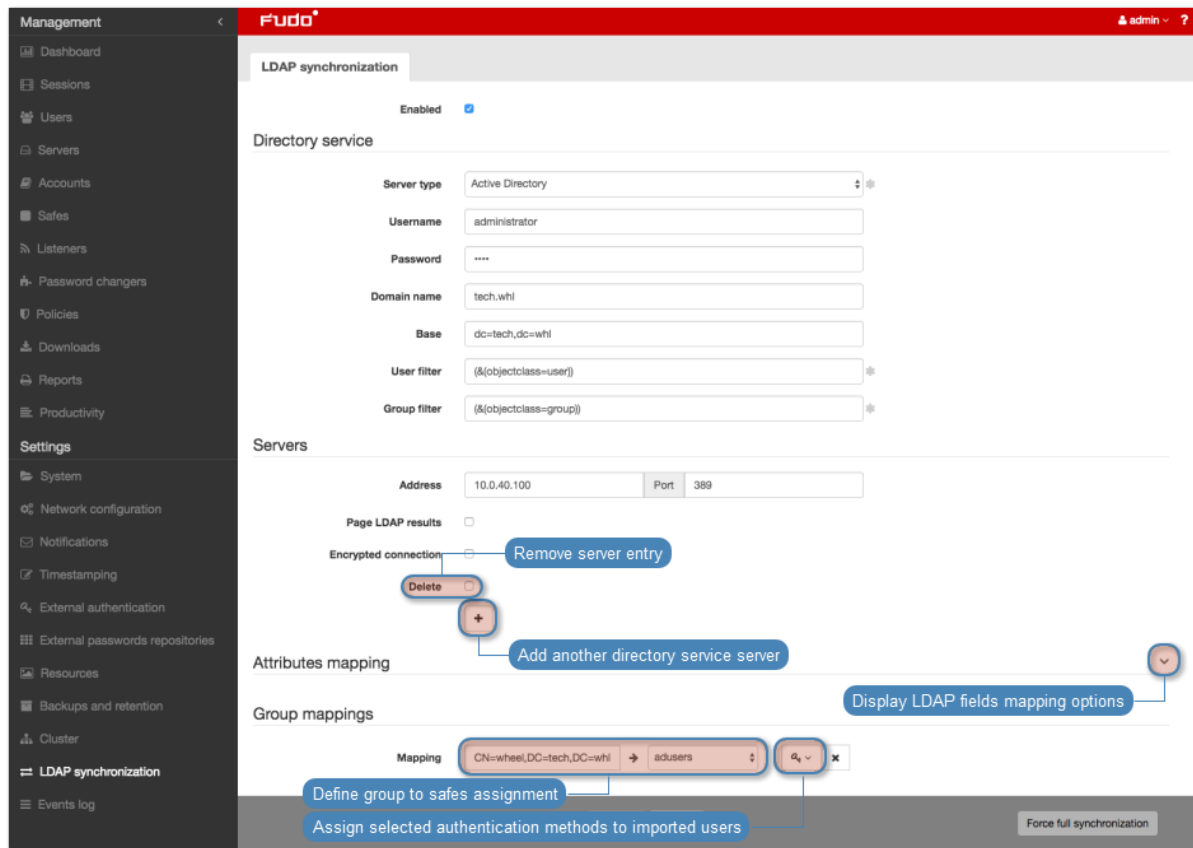
Authenticating a user, Wheel Fudo PAM will send requests to external authentication sources in the following order:

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

-
14. Click *Save*.

Note: The *Force full synchronization* option enables processing changes in directory structures which cannot be processed during periodical synchronization, eg. deleting a defined group or deleting a user.

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



Related topics:

- [Data model](#)
- [Users management](#)
- [Servers management](#)
- [Accounts](#)

6.14 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' section of the management interface. The table contains the following data:

Timestamp	Log level	Component	Message
2014-12-22 14:06:25	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 '[u'2015-01-21'...
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'valid_since' from 'None' to '[u'2014-12-...
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 '[]' to 'SimpleLazyObj...
2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'phone' from '' to '733569593'.
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 't.dwormicki@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	dbrecvd	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: 848388532111147015) (fudo_session:
848388532111147219) (fudo_user: 848388532111147012) (fudo_connection:
848388532111147014) 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:

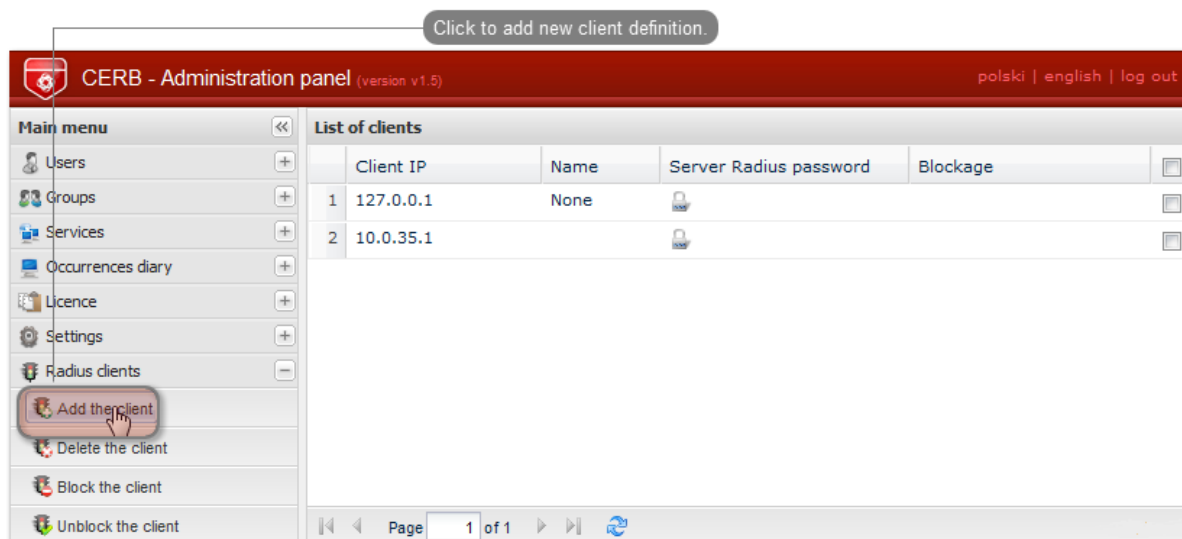
- *Security*
- *Managing servers*

6.15 Integration with CERB server

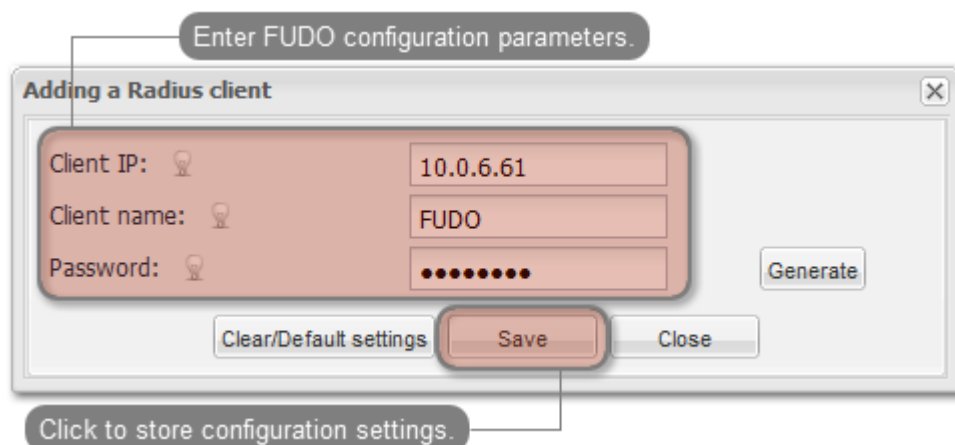
CERB is complete user authorization solution which supports a number of authorization mechanisms (i.e. mobile token, onetime passwords, etc.). The following procedure describes configuration steps required to enable Wheel Fudo PAM to verify users credentials using CERB server.

CERB server configuration

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



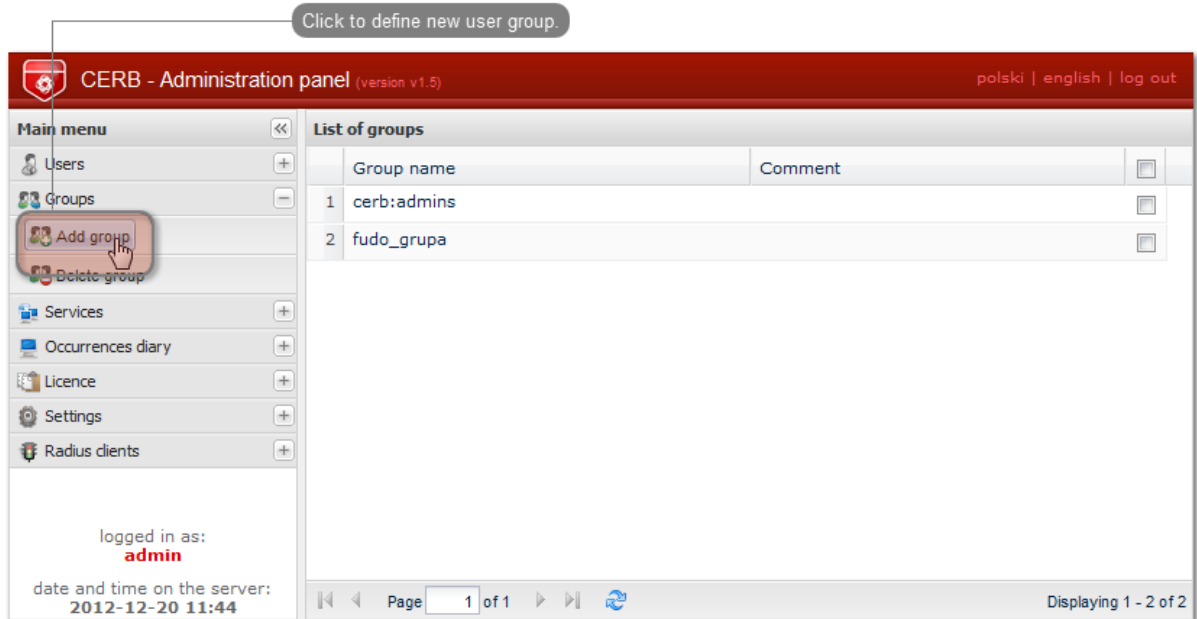
- Provide Wheel Fudo PAM IP address, client's name and password and click *Save*.



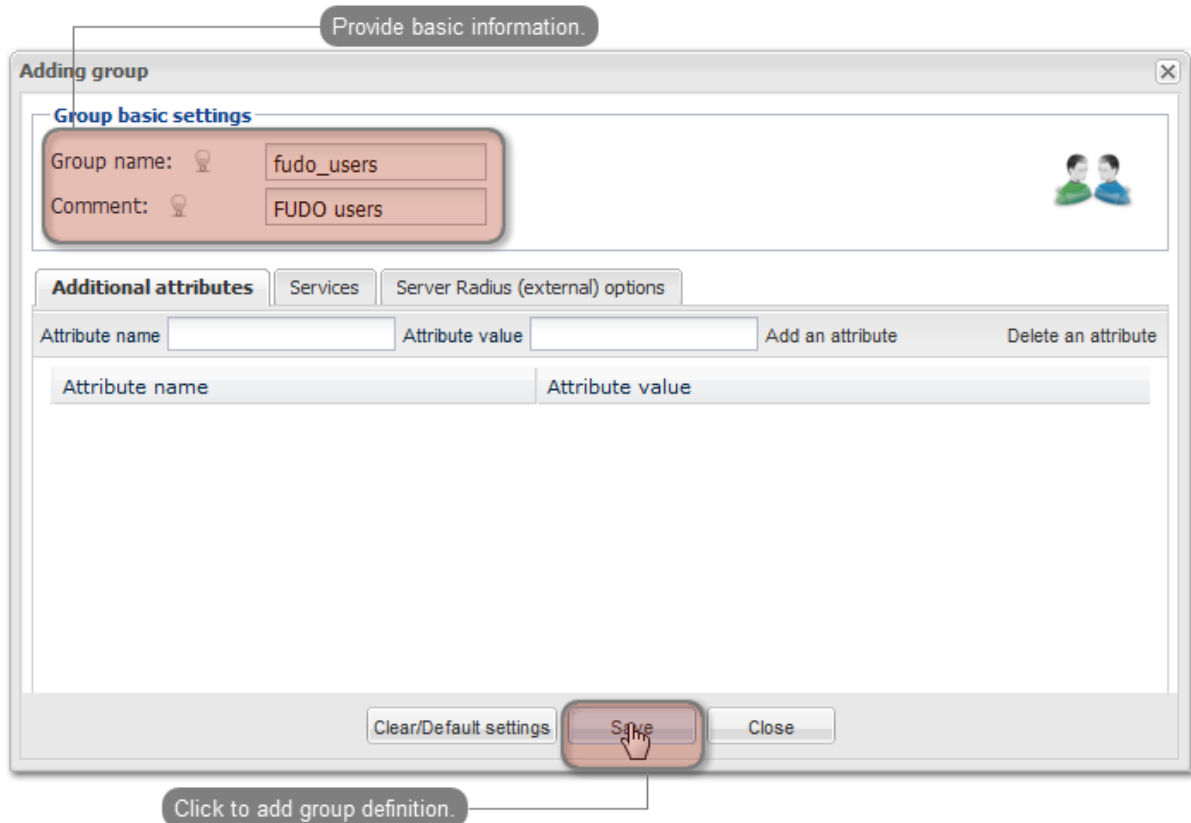
Note: Password will be required to define external authorization server in Wheel Fudo PAM administration panel.

2. Adding user group.

- Select *Groups > Add group* to define Wheel Fudo PAM users who will be authorized by the CERB server.

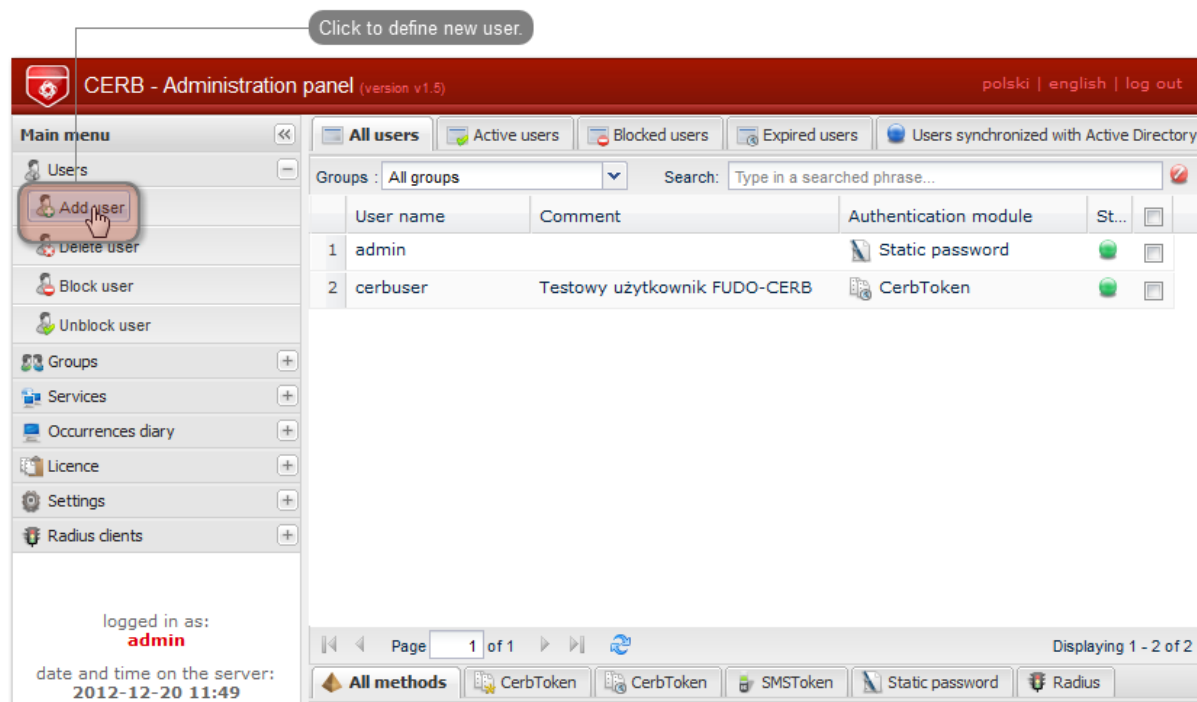


- Enter group's name (**fudo_users**) and click *Save*.

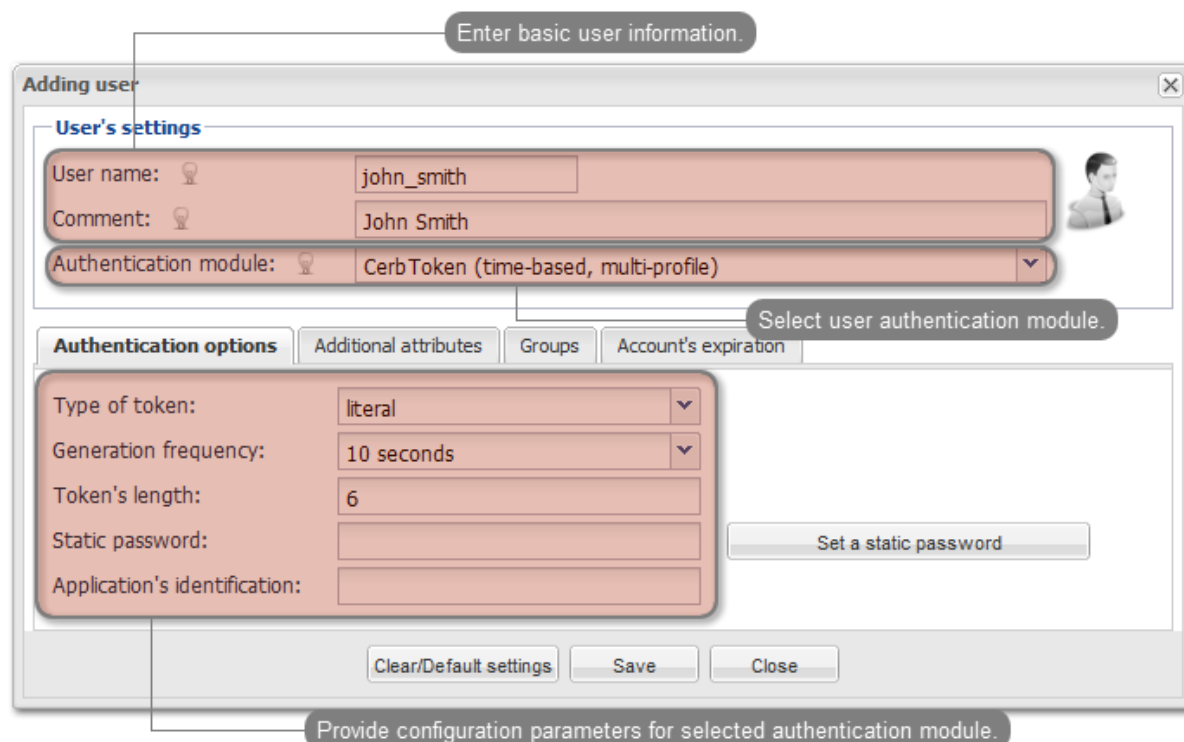


3. Adding user.

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

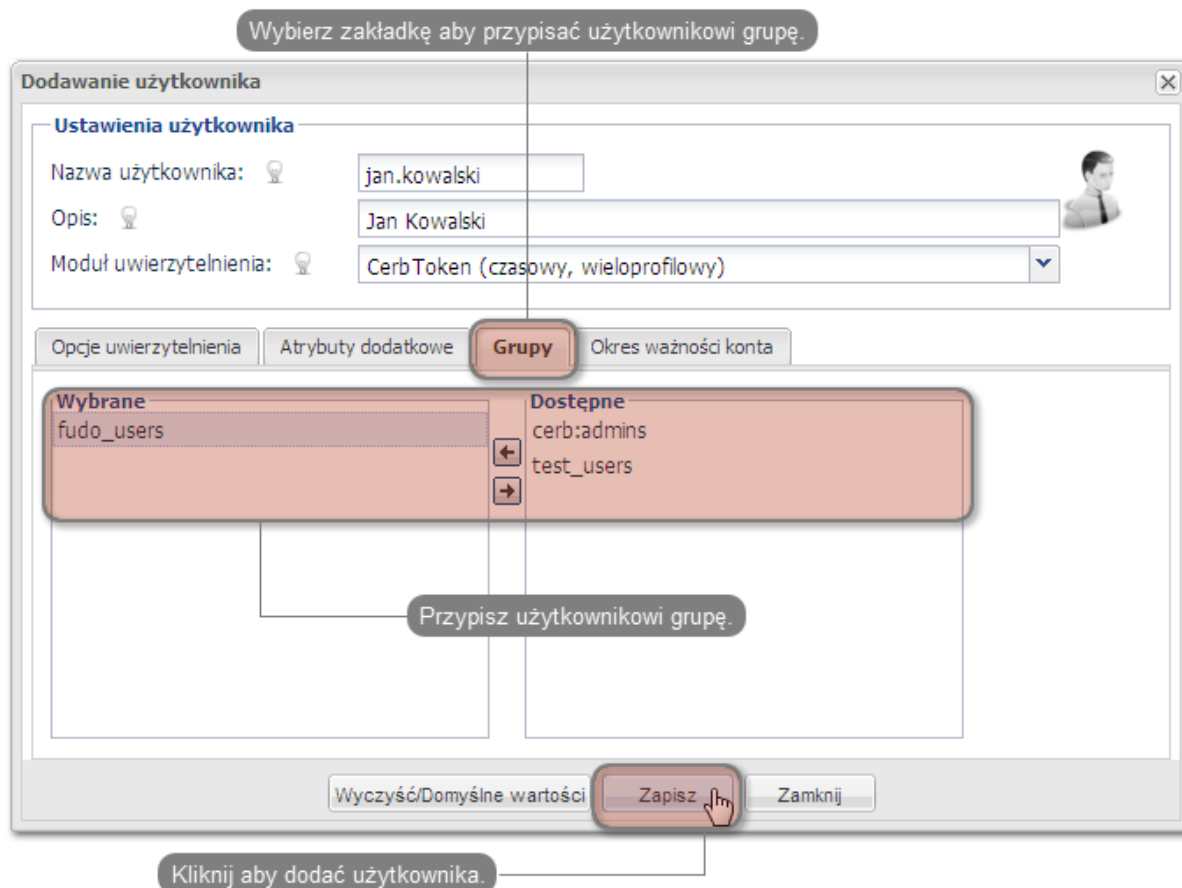


- Provide user name, description and select desired authorization module (refer to CERB server documentation form more information on authorization modules).



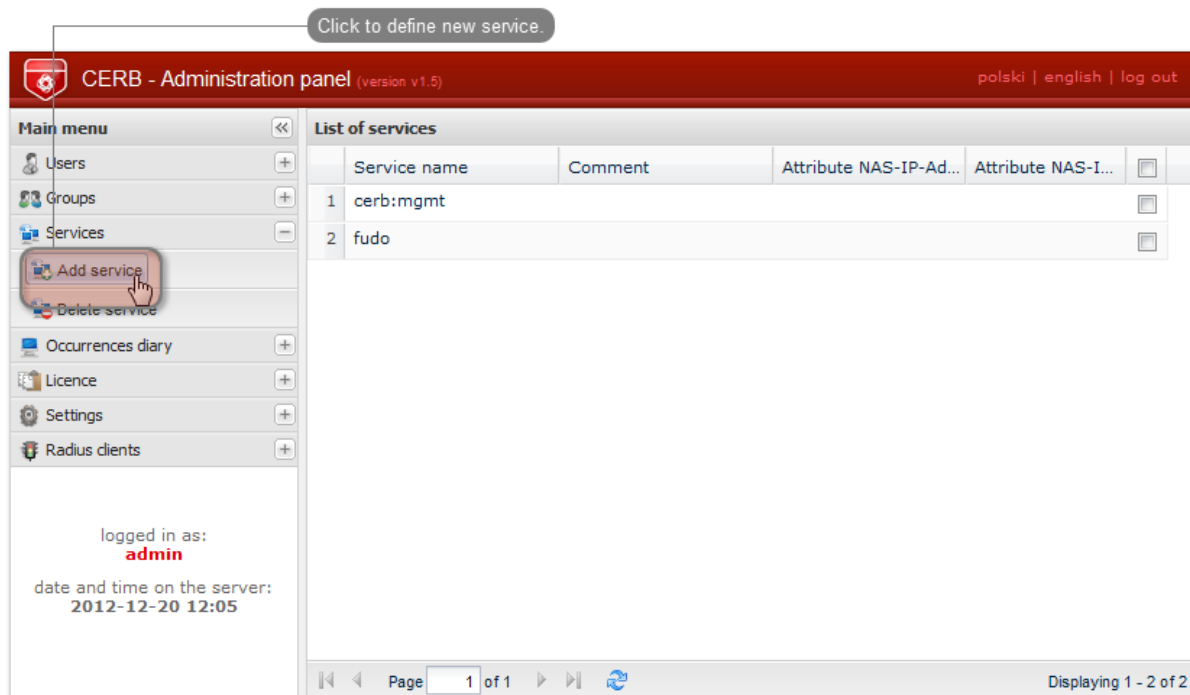
Note: Username is used to authenticate users on Wheel Fudo PAM.

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



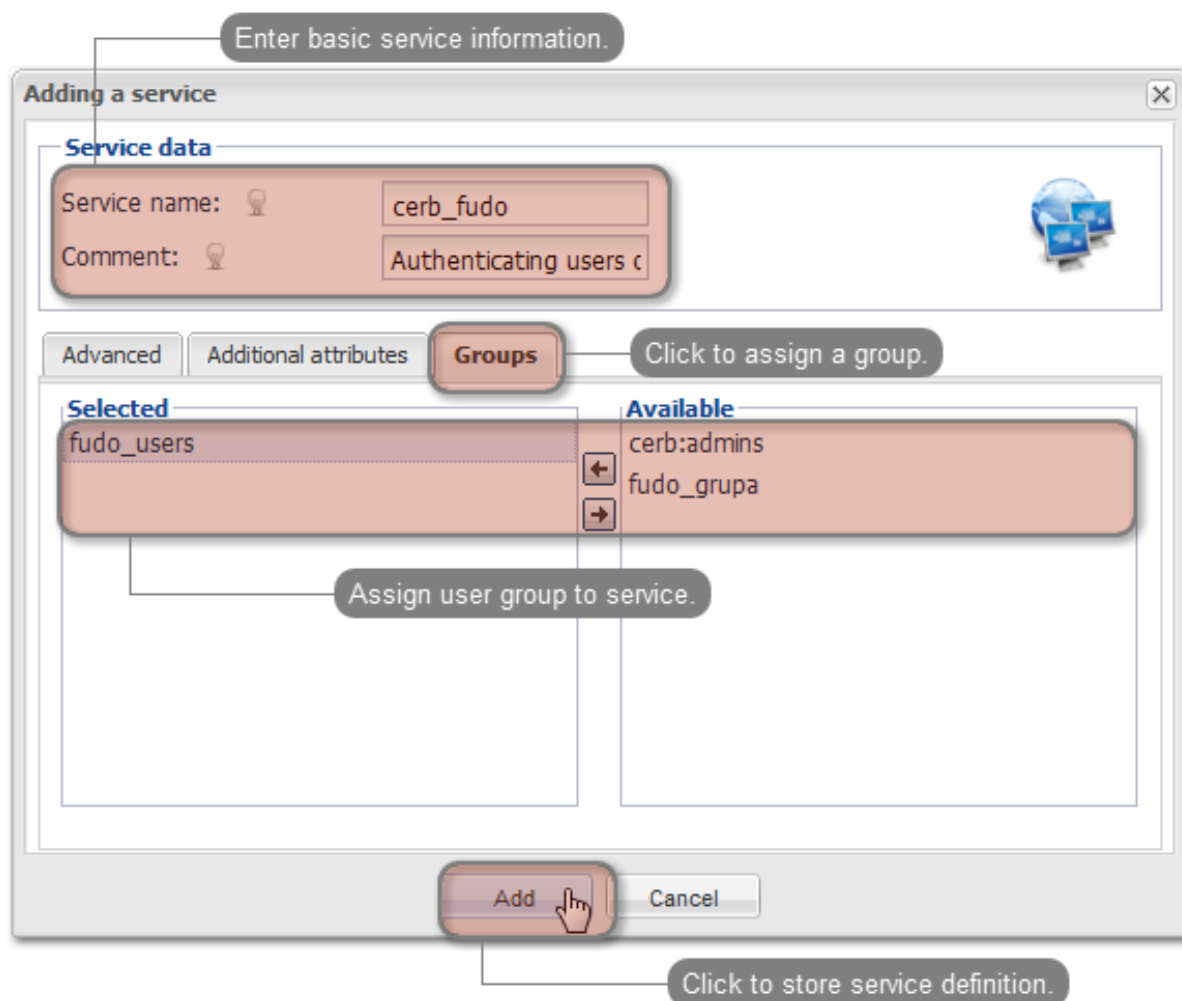
4. Configuring service.

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



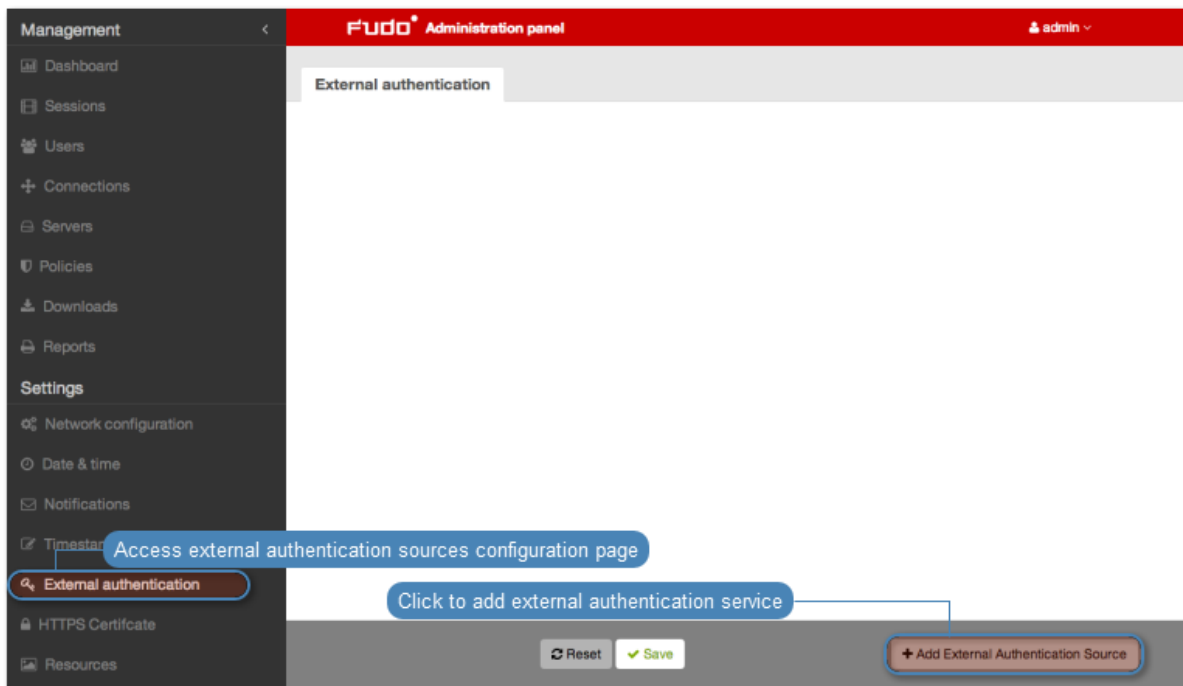
- Provide name identifying authorization service (`cerb_fudo`) and service description.

- 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*.

Open users management page

Add user definition

	Role	Organization	Email	Full Name	Authentication Method	Status
<input type="checkbox"/>	Administrator	user			External Authentication	Active
<input type="checkbox"/>	a2_user1	user	trudny@email.com	a2_user1 a2_user1	External Authentication	Active
<input type="checkbox"/>	ad_admin1	user		ad_admin1 oshogbo ad_admin1	External Authentication	Active
<input type="checkbox"/>	ad_at1	user		ad_at1_display	External Authentication	Blocked
<input type="checkbox"/>	ad_gj1	user		ad_gj1	External Authentication	Active
<input type="checkbox"/>	admin	superadmin		Marcinek	Password	Active
<input type="checkbox"/>	admin2	admin			Password	Active
<input type="checkbox"/>	adminat	admin			Password	Active
<input type="checkbox"/>	adminat2	admin			External Authentication, Password	Active
<input type="checkbox"/>	anonymous	user				Active
<input type="checkbox"/>	asdawdawd	admin				Active
<input type="checkbox"/>	fudo_user1	admin			External Authentication, Password	Active
<input type="checkbox"/>	operator	operator			Password	Active
<input type="checkbox"/>	test	user			Password, SSH Key	Active

- 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

Role

Synchronize with LDAP ☐

Blocked ☐

Full name

Email

Organization

Phone

AD Domain

LDAP Base

Permissions

Granted users

Authentication

Type

External authentication source

Select external authentication option and choose previously added CERB server

Type

Delete ☐

Reset Save

Save user definition

3. Adding connection.

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

The screenshot displays the Fudo Administration panel. The sidebar on the left contains a 'Management' section with links to Dashboard, Sessions, Users, and Connections (highlighted with a red box and a blue callout 'Access connections management page'). Below this is a 'Settings' section with links to Network configuration, Date & time, Notifications, and Timestamping. The main content area has a red header 'Fudo Administration panel' with a user dropdown 'admin'. Below the header is a 'Connections' tab with buttons for 'Add connection' (highlighted with a red box and a blue callout 'Add connection definition'), 'Block', 'Unblock', and 'Delete', and an 'Add filter' dropdown. The main area contains a table of connections:

		Servers	Status	
<input type="checkbox"/>	MYSQL	administrator, user1, user2, user3, user4, user5	root@MYSQL-10.0.35.52	Active
<input type="checkbox"/>	RDP-FORWARD	administrator	RDP-10.0.8.102 , RDP-TLS-10.0.8.103	Active
<input type="checkbox"/>	RDP-REPLACE	user1, user2, user3, user4, user5, z	administrator@RDP-10.0.35.54 , administrator@RDP-TLS-10.0.8.103 , admin@RDP-10.0.40.102-hardening , administrator@RDP-10.0.35.54-15	Active
<input type="checkbox"/>	SSH-REPLACE	fudo_user1, fudo_user2, fudo_user3, fudo_user8, fudo_user9, user1, user2, user3, user4, user5, z	root@10.0.35.52 - SSH	Active
<input type="checkbox"/>	TELNET	admin, administrator, user1, user2, user3, user4, user5	TELNET-10.0.35.52	Active
<input type="checkbox"/>	VNC			Active
<input type="checkbox"/>	anonymous	anonymous	www.ipko.pl , 10.0.35.53	Active
<input type="checkbox"/>	oracle-test	user1	cerb@10.0.7.11 - ORACLE	Active
<input type="checkbox"/>	test		RDP-10.0.35.54	Active

- 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?

Reset **Save** Save connection definition **+ Add Server**

6.16 System maintenance

The following section contains descriptions of maintenance procedures.

6.16.1 Monitoring system condition

Monitoring system condition allows preventing system failures and overloads, ensuring 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*

6.16.2 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

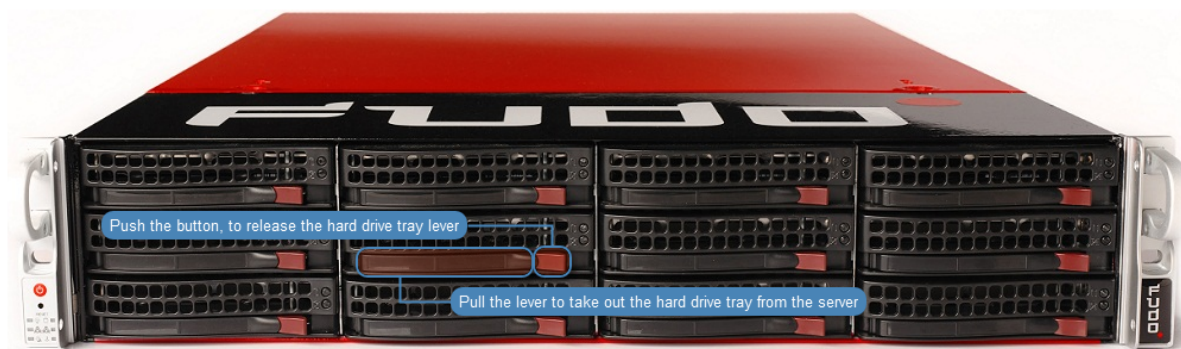
a failure of two hard drives.

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.

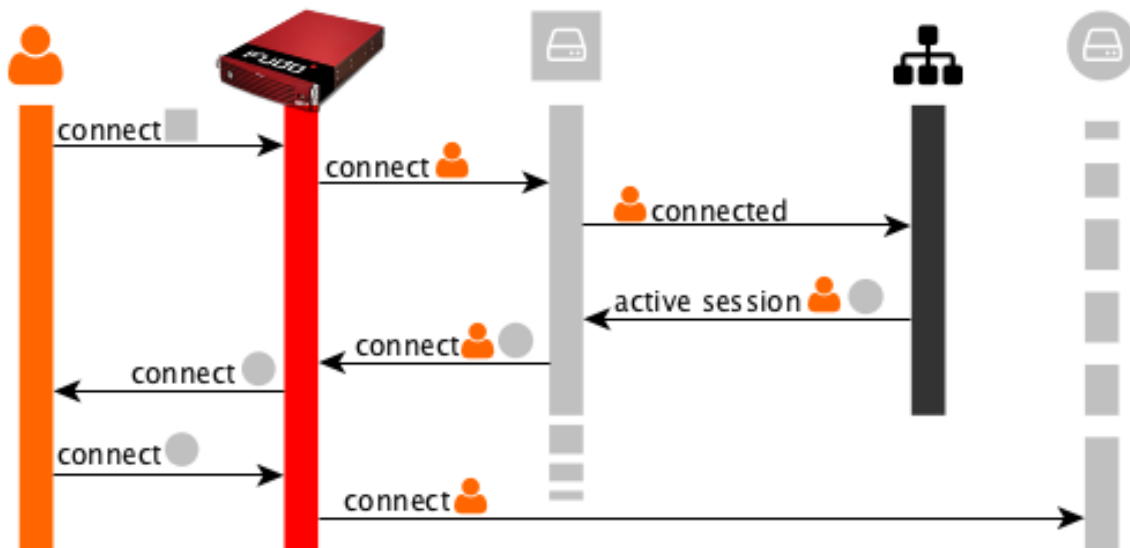
Related topics:

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

7.1 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, listen on default RDP port (3389) and user must be allowed to connect to given server.

Related topics:

- [Data model](#)
- [RDP](#)
- [Servers](#)
- [Accounts](#)

7.2 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 \${disk}.</i> Replace defective drive.
<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 \${disk}.</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 (\${diskserial}) \${disk}.</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 %s than %s FUDO version.</i>
FSE0046	<i>There is no filter called %s.</i>
FSE0048	<i>Error authenticating user over RADIUS.</i>
FUE0057	<i>Authentication method 'password', required by MySQL, requested by the user %s, logging in from IP address %s, was not found.</i>
FUE0058	<i>Authentication method 'password', required by MySQL, requested by the user %s, 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 password or 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

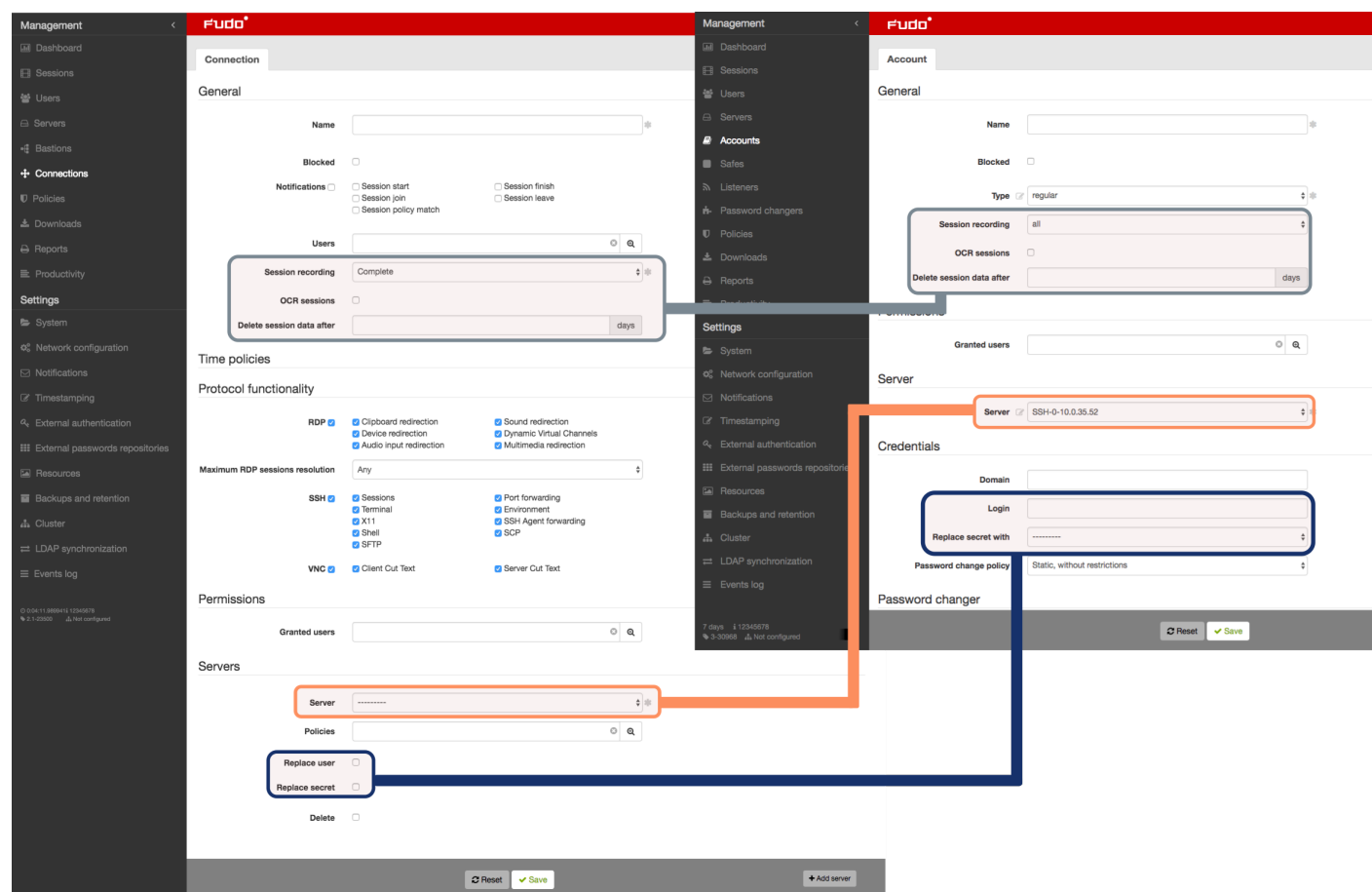
Table 1 – continued from previous page

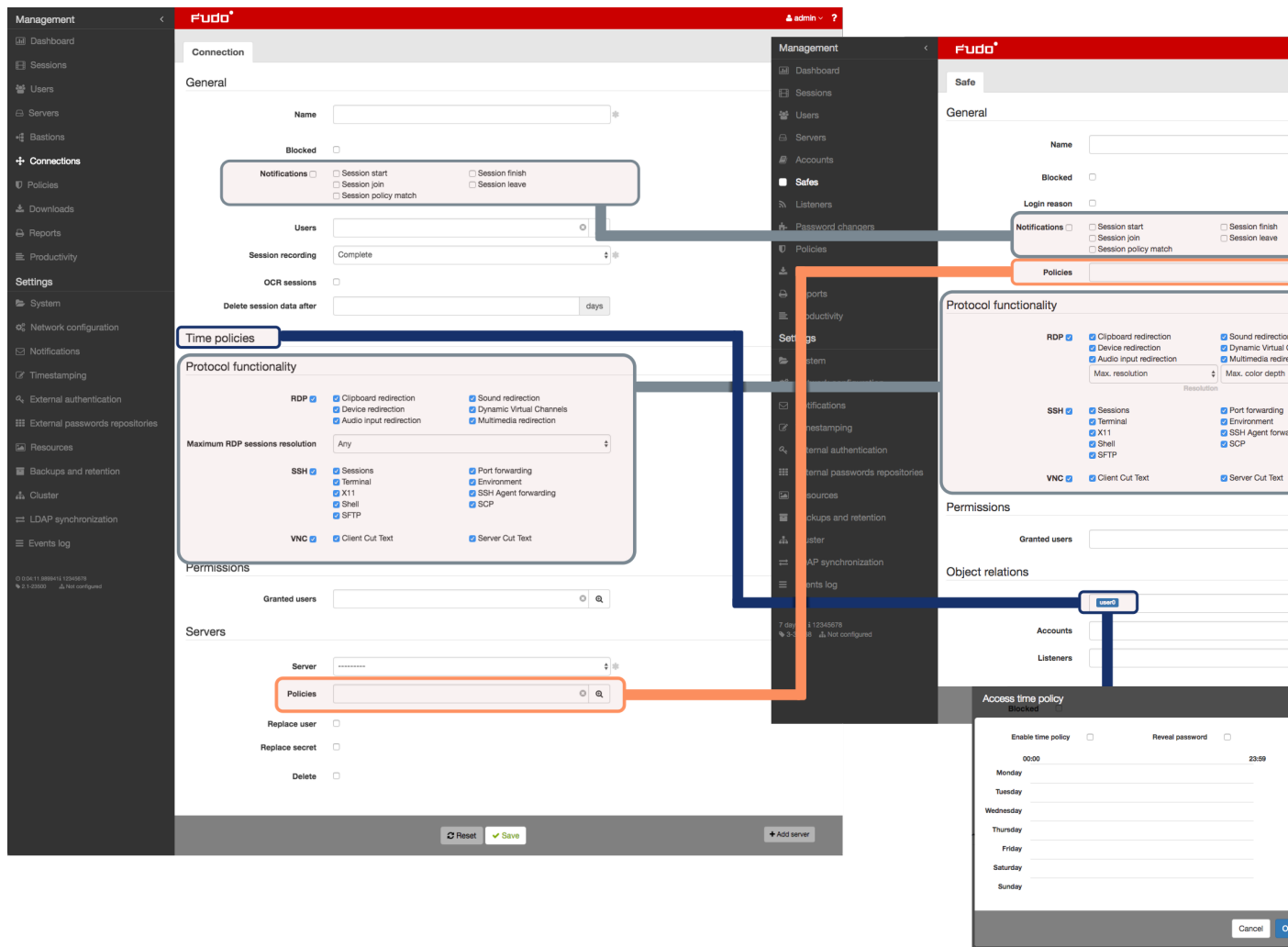
Error code	Error message and description
FUE0318	<i>Unable to fetch SSL certificate.</i>
FSE0330	<i>Bad login field configured on server. Error while processing user %s.</i>
FSE0331	<i>Error while processing userAccountControl value of user %s.</i>
FUE0346	<i>Client sent a packet bigger than %d bytes.</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.

7.3 Wheel Fudo PAM 2.2 to Wheel Fudo PAM 3.0 parameters mapping

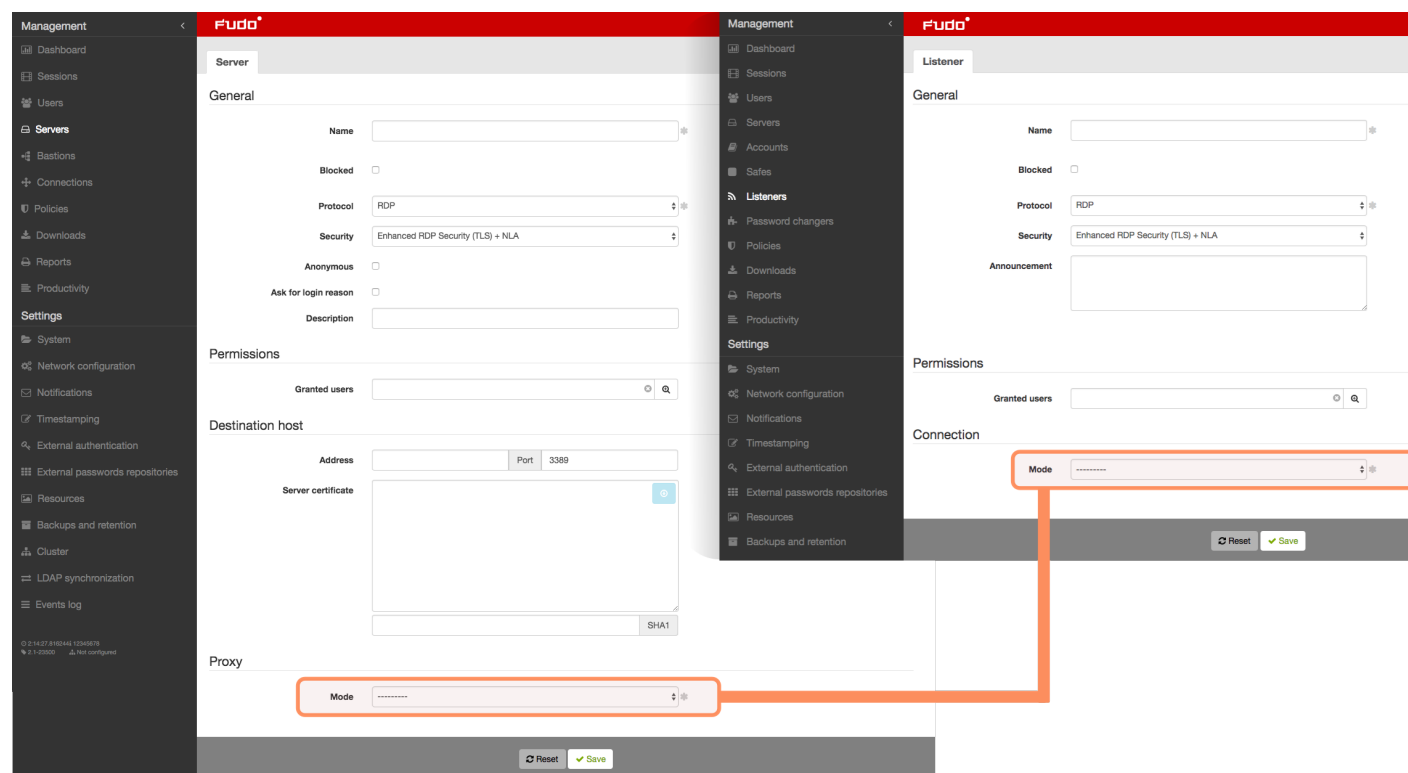
This topic describes how certain parameters from Wheel Fudo PAM 2.2 map to Wheel Fudo PAM 3.0 data model.

7.3.1 Connection





7.3.2 Server



7.4 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.

7.4.1 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.

7.4.2 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.



The screenshot shows a user configuration form with the following fields and controls:

- Preferred language:** A dropdown menu set to 'English' with a star icon on the right.
- Safes:** A section containing three buttons: 'RDP' (highlighted with a red border), 'SSH', and 'portal'. A blue callout bubble points to the 'RDP' button with the text 'Click to define access time policy to the safe'. There are also a gear icon and a magnifying glass icon to the right of the buttons.
- Full name:** An empty text input field.
- Email:** An empty text input field.

-
- After migration, login credentials policies are reflected within the safe.

7.4.3 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.

7.4.4 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.

7.4.5 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.

7.5 Supported protocols

This topic describes in detail Wheel Fudo PAM protocols support.

7.5.1 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.

7.5.2 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.

7.5.3 ICA

Supported connection modes:

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

Supported client applications:

- Citrix Receiver.

7.5.4 Modbus

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Notes:

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

7.5.5 MS SQL (TDS)

Supported connection modes:

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

Supported client applications:

- SQL Server Management Studio,
- sqsh.

7.5.6 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.

7.5.7 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.

7.5.8 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.

7.5.9 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.

7.5.10 Telnet

Supported connection modes:

- Bastion,
- Gateway,
- Proxy,

- Transparent.

Notes:

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

7.5.11 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.

7.5.12 Telnet 5250

Supported connection modes:

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

Notes:

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

Supported client applications:

- IBM Personal Communications,
- tn5250.

7.5.13 VNC

Supported connection modes:

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

Supported client applications:

- TightVNC,
- RealVNC.

7.5.14 X11

X11 protocol is supported within the SSH protocol.

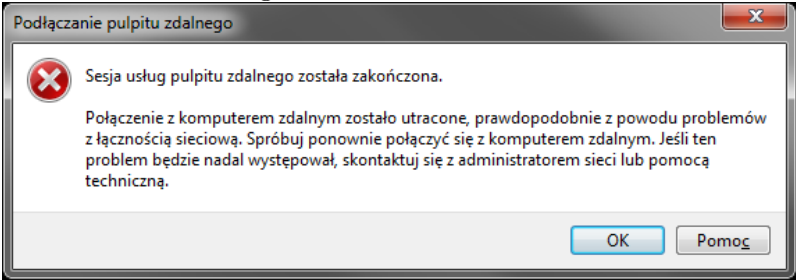
Supported servers:

- Xorg,
- Xming,
- XQuartz.

8.1 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.

8.2 Connecting to servers

Problem	Symptoms and solution
Cannot connect to server	<p>Symptoms:</p> <ul style="list-style-type: none">• User cannot log in.  <ul style="list-style-type: none">• Events log entry: Authentication failed: Invalid username kowalski or password.
	<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.
	<p>Symptoms: events log entry: Unable to establish connection to server zbigniew (10.0.35.53:3399).</p> <p>Cause: incorrect server configuration.</p> <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:
	<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.

Problem	Symptoms and solution
When logging in not all of the users see the Wheel Fudo PAM logon screen.	Cause: <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.
	Symptoms: <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.
	Cause: incorrect login credentials.
	Solution: provide correct login credentials in server configuration.
	Symptoms: <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
	Cause: server has been blocked.
	Solution: log in to Wheel Fudo PAM administration panel and unblock the server.

Problem	Symptoms and solution
Connection is terminated	<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> <div><p>Destination host</p><div><div>Address</div><div>10.0.35.1</div><div>Port</div><div>22</div><div>Click to download server certificate</div></div><div><div>Server public key</div><div>ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAQDTy6vf0NsMYuiOCRfcz/3bEF0tO WKf+bB6wW1XKRu8UqROxZnMEpNpy8cRtZDbpmWE8NN4IM7yosy3gAgD S16TErm6ukVKOjYKIHF4Qqp+8d2OhgKBHtwmXZff4QFyQmMUbA4MhL/cC LTnOJc2du1512cX5xFdh05LUaBB6xbVOhbXLSIQLQUP+/JAs3Qo5lx9m1Wk bJkofQ5AQV7pdsKTU93O6GBO0IDoz3lpPbTKnn/dhNBIfpmHSblPTrgPasO9 C/lhL2PVFiBeqvwwK67CKgW6UrhHPPLquHayA0YulVTjveBumg/CpQ0Zqt7U OUzZ2M2ezQwJxPdvbf6V</div><div>09:de:23:81:72:c1:f7:c7:12:9a:df:6c:cb:cd:ad:d6:f4:50:ac:c0</div><div>SHA1</div></div></div>
	<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>
Cannot connect to server	<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
	Symptoms: <ul style="list-style-type: none"> • After entering username and password, the screen freezes. • Events log entry Terminating session: User user0 (id=848388532111147010) is blocked.
	Cause: user is blocked.
	Solution: log in to Wheel Fudo PAM administration panel and unblock the user in question.
User has to provide login credentials twice	Symptoms: user connecting over RDP protocol enters login credentials and immediately afterwards is asked again for the same login information.
	Cause: server is a part of an infrastructure managed by connections broker which has detected an active user's session on another server.
	Symptoms: user connecting over SSH protocol enters login credentials and immediately afterwards is asked again for login information.
	Cause: in <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.
Cannot connect to server over RDP protocol	Symptoms: <ul style="list-style-type: none"> • User connecting over RDP is disconnected a moment after establishing connection. • Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.
	Cause: connection is redirected to a host which does not listen on port number 3389.
	Solution: configure server in question so it accepts user connections on port number 3389.
	Symptoms: <ul style="list-style-type: none"> • Events log entry: User user0 has no access to host 192.168.0.1:3389
	Cause: connections broker determines an existing user session on another server and redirects user to that host but it is not configured on Wheel Fudo PAM or the user does not have sufficient access rights to connect to given server.
	Solution: <ul style="list-style-type: none"> • Make sure that the server object exists. • Add user to proper <i>connection</i> object.

8.3 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.



8.4 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>

8.5 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.

A

AAPM, [212](#)
account, [212](#)
Active Directory, [211](#)
AD, [211](#)
administration
 configuration export/import, [152](#)
anonymous safe, [212](#)

C

CERB, [211](#)
CIDR, [212](#)
configuration
 Network configuration, [129](#)
 notifications, [140](#)
 users synchronization, [163](#)
connection mode
 bastion, [8](#)
 gateway, [7](#)
 proxy, [8](#)
 transparent, [7](#)

D

data retention, [213](#)
deployment scenario
 bridge, [6](#)
 forced routing, [6](#)

DHCP, [213](#)

DNS, [211](#)

E

Efficiency Analyzer, [212](#)
external authentication server, [213](#)

F

Fingerprint, [211](#)
fudopv, [212](#)

H

heartbeat, [212](#)

hot-swap, [212](#)

L

LDAP, [211](#)
listener, [212](#)

N

Network configuration
 network interface configuration, [129](#)
network configuration
 routing, [137](#)

P

password changer, [212](#)
passwords repository, [213](#)
policy, [212](#)
PSM, [213](#)
PSM (*Privileged Session Management*), [212](#)
Public key, [211](#)

R

RADIUS, [211](#)
RDP, [211](#)
RDP connections broker, [213](#)
RDP connections broker, [183](#)
redundancy group, [213](#)

S

safe, [212](#)
server, [212](#)
servers, [212](#)
sessions
 commenting, [98](#)
 filtering, [82](#)
 play and preview, [89](#)
shared session, [212](#)
SSH, [211](#)
SSH access, [212](#)
Static password, [211](#)

Syslog, [211](#)

T

time policy, [212](#)

timestamp, [213](#)

U

user, [212](#)

users synchronization, [163](#)
 configuration, [163](#)

V

VLAN, [212](#)

VNC, [211](#)