Fudo PAM 4.4 - System Documentation

Release is not supported

Fudo Security

June 08, 2022

Contents

CHAPTER 1

About documentation

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

Documentation Structure

1. General information

This chapter contains information on documentation.

2. System overview

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

3. System deployment

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

4. Quick start

This chapter contains typical configuration examples.

5. Users

This chapter covers users management topics.

6. Servers

This chapter covers servers management topics.

7. Accounts

This chapter covers accounts management topics.

8. Safes

This chapter covers safes management topics.

9. Listeners

This chapter covers listeners management topics.

10. Password changers

This chapter contains information on automated password changing feature.

11. Policies

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

12. Sessions

This chapter contains information on stored access sessions.

13. Reports

This chapter contains topics related to generating reports.

14. Efficiency analyzer

This chapter describes Fudo PAM's efficiency analyzer module.

15. Administration

This chapter contains administration procedures.

16. Reference information

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

17. AAPM (Application to Application Password Manager)

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

18. Service Now

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

19. Client applications

This chapter contains client applications configuration instructions for selected protocols.

20. Troubleshooting

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

21. Frequently asked questions

This chapter contains frequently requested information about Fudo PAM.

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

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.

CHAPTER 2

Introduction

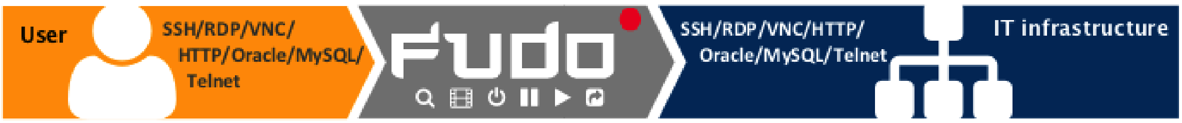
2.1 System overview

Fudo PAM is a complete solution for managing remote privileged access. Fudo PAM comprises four modules each dedicated to different aspects of remote access management:

- *Privilege Session Monitoring (PSM)*
- *Secret Manager*
- *Efficiency Analyzer*
- *Application to Application Password Manager (AAPM)*

PSM

PSM module enables facilitating constant monitoring of remote access sessions to IT infrastructure. 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.

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

The PSM module supports following system configurations:

- Linux,
- FreeBSD,
- Mac OS X

- Microsoft Windows Server,
- Microsoft Windows,
- TightVNC,
- Solaris.

Secret manager

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.

For more information on the Secret Manager module, refer to the *Password changers* topic.

Efficiency Analyzer

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

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

Application to Application Password Manager (AAPM)

AAPM module enables secure passwords exchange between applications.

AAPM supported operating systems:

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

For more information on the AAPM module, refer to the *AAPM (Application to Application Password Manager)* topic.

Related topics:

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

2.2 Supported protocols

2.2.1 Citrix StoreFront (HTTP)

Supported connection modes:

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

Notes:

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

2.2.2 HTTP

Supported connection modes:

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

Supported OCR languages for the rendered HTTP session:

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

Notes:

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

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

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

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

Additionally, in the non-rendered mode:

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

Additionally, in the rendered mode:

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

2.2.3 ICA

Supported connection modes:

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

Supported client applications:

- Citrix Receiver.

Supported encryption algorithms:

- Basic,
- TLS.

Supported OCR languages:

- English
- German
- Norwegian

- Ukrainian
- Polish
- Hungarian
- Russian

Notes:

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

2.2.4 Modbus

Supported connection modes:

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

Notes:

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

2.2.5 MS SQL (TDS)

Supported connection modes:

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

Supported client applications:

- SQL Server Management Studio,
- sqsh.

Notes:

- Session joining is not supported.

2.2.6 MySQL

Supported connection modes:

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

Supported client applications:

- Official MySQL client,
- PyMySQL libraries for Python.

Notes:

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

2.2.7 RDP

Supported connection modes:

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

Supported client applications:

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

Supported OCR languages:

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

Notes:

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

- When authenticating Fudo users against AD (or other external source) the TLS+NLA (Network Level Authentication) is not supported; TLS mode is used instead. NLA mode on server side is supported.
- In case of *Enhanced RDP Security (TLS) + NLA*, Fudo PAM requires NTLM protocol version 2 or newer. To properly handle NLA authentication connections, enable option to only send NTLMv2 response both on client and server side.
  1. Click *Start > All Programs > Accessories > Run*.
  2. Type `secpol.msc` in the *Open* input field and click *OK*.
  3. Select *Local Policies > Security Options* and double-click *Network Security: LAN Manager authentication level*.
  4. Select *Send NTLMv2 response only. Refuse LM & NTLM* from the drop-down list.
  5. Click *Apply*.
- Fudo PAM verifies input language settings when negotiation connection and does not support dynamic language change on the login screen.

RemoteApp

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

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

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

2.2.8 SSH

Supported connection modes:

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

Supported features:

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

- X11 - within SSH protocol (video export, session termination, pause, session join, playback, raw data),
- Shell (video export, session termination, pause, session join, playback, raw data),
- Terminal (video export, session termination, pause, session join, playback, raw data).

Supported encryption algorithms: - Server: RSA, DSA - Listener: RSA, DSA

Supported hashing algorithms: - MD5 - SHA256

Notes:

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

2.2.9 Telnet 3270

Supported connection modes:

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

Supported client applications:

- IBM Personal Communications,
- c3270.

Notes:

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

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

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

2.2.10 Telnet 5250

Supported connection modes:

- *Bastion*,
- *Gateway*,
- *Proxy*,

- *Transparent*.

Supported client applications:

- IBM Personal Communications,
- tn5250.

Notes:

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

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

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

2.2.11 Telnet

Supported connection modes:

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

Notes:

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

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

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

2.2.12 VNC

Supported connection modes:

- *Bastion*,
- *Gateway*,

- *Proxy*,
- *Transparent*.

Supported client applications:

- TightVNC,
- RealVNC.

Supported OCR languages:

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

Notes:

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

Connection specifics - VNC server requires authentication

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

Connection specifics - server does not require authentication

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

2.2.13 X11

X11 protocol is supported within the SSH protocol.

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

Supported servers:

- Xorg,

- Xming,
- XQuartz.

Supported fonts:

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

2.2.14 TCP

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

Supported connection modes:

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

Notes:

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

2.2.15 Secret Checkout

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

Note: The protocol is virtual in a sense that there is no TCP/IP session related to it, only meta information is stored (for example checkout time, checkin time, who accessed the secret). As there is no TCP/IP, no data that can be played are saved. This makes checkout sessions lightweight compared to sessions recorded with data, such as RDP.

In case of a breach, having secret checkouts recorded as sessions, allows one to pinpoint who had access to the leaked secret.

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

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

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

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

Notes:

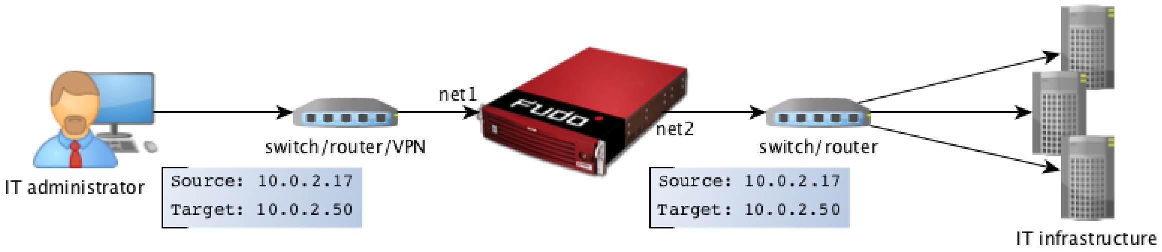
- *Session joining* feature is not supported.
- Playback is not supported.

2.3 Deployment scenarios

Note: It is advised to deploy the 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 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.



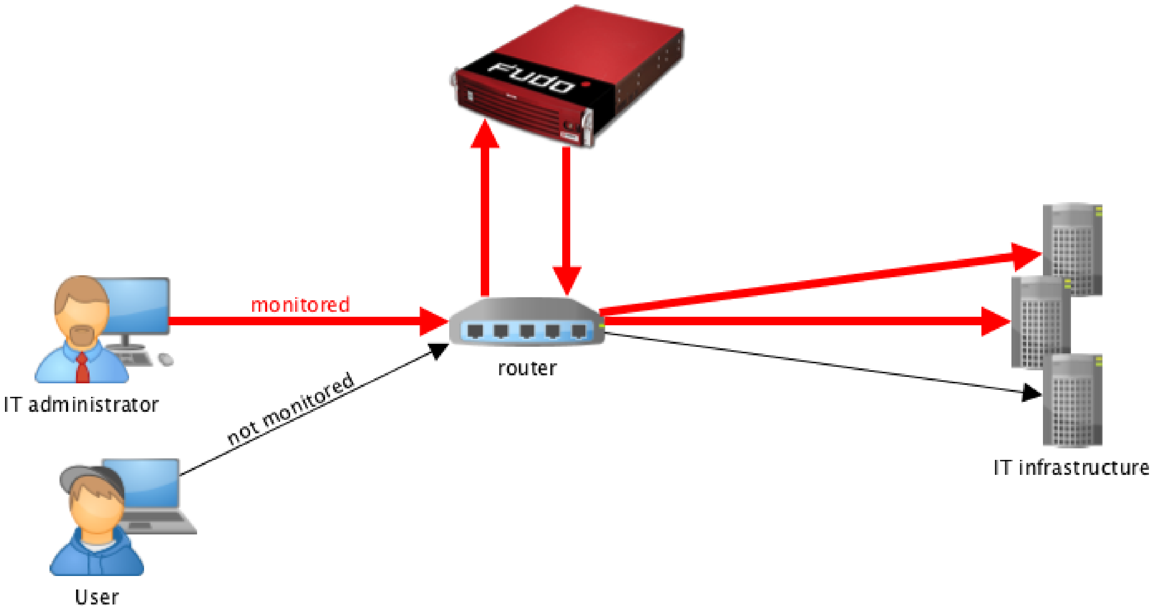
Mediating packages transfer, Fudo PAM preserves source IP address when forwarding requests to destination servers.

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 Fudo PAM and the rest of the traffic is forwarded directly to the destination server.



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

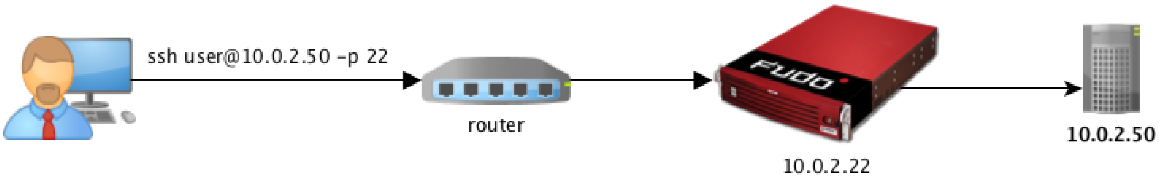
Related topics:

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

2.4 Connection modes

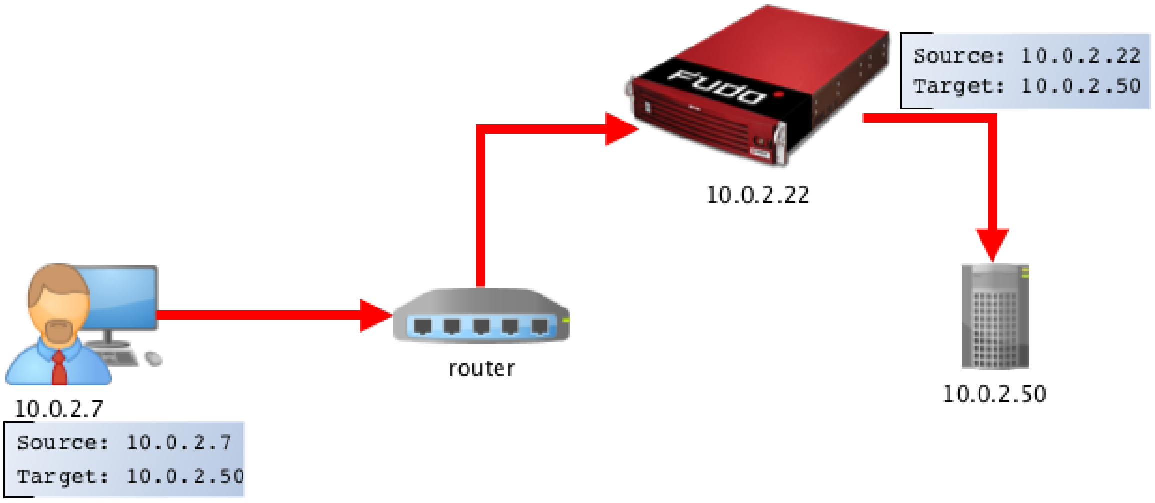
Transparent

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



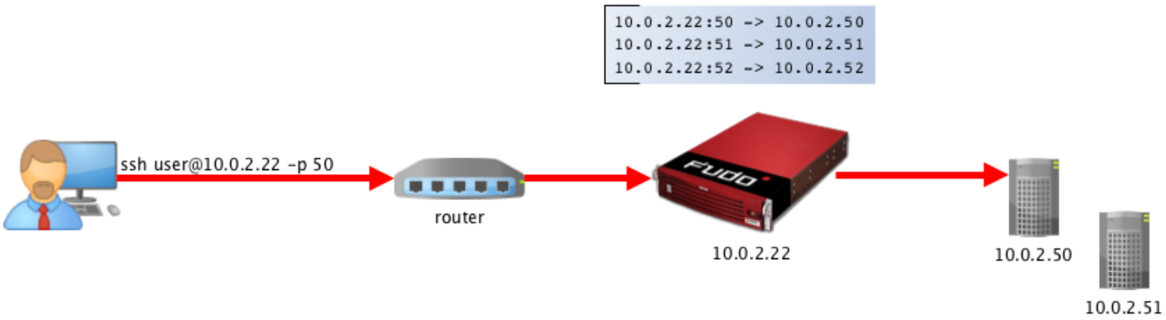
Gateway

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



Proxy

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

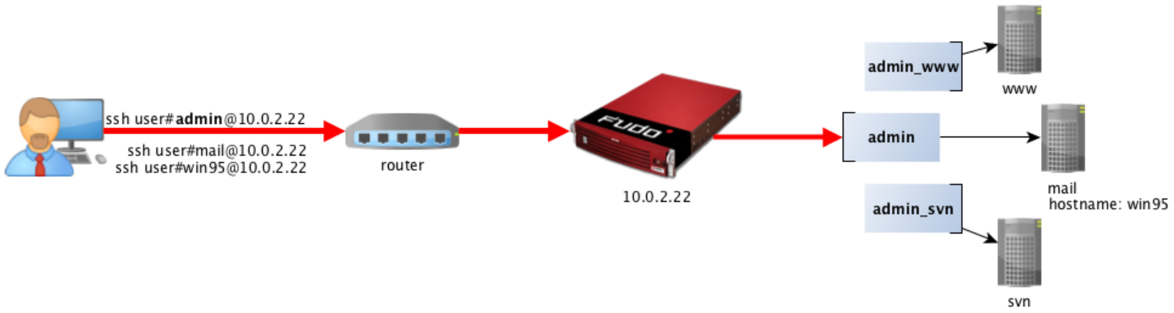


Such approach enables concealing actual IP addressing and allows configuring servers to only accept requests sent from Fudo PAM.

Bastion

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

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



Note: The string specifying the target object must unambiguously identify an account or a server.

Target object string is matched in the following sequence:

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

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

- “domain\user”#bsd01@10.0.60.138
- ‘domain\user’#bsd01@10.0.60.138
- domain\user#bsd01@10.0.60.138

Related topics:

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

2.5 User authentication methods and modes

User authentication methods

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

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

Note:

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

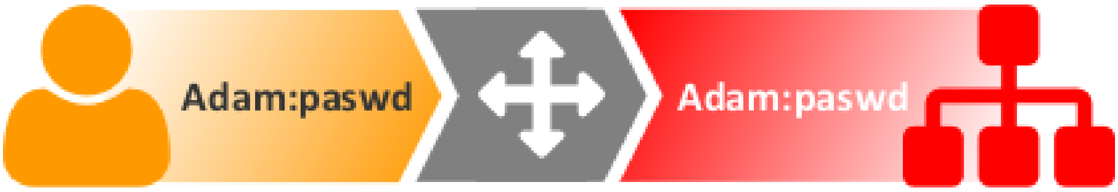
Authentication modes

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

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

Authentication with original login and password

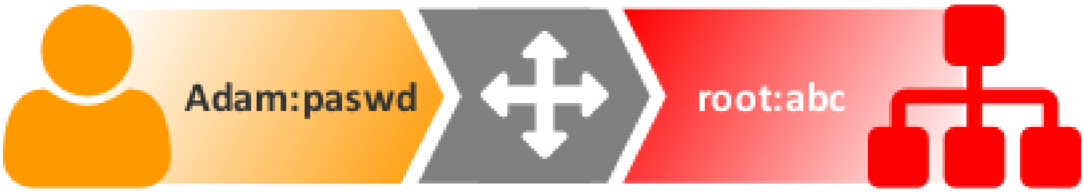
In this authentication mode, Fudo uses login and password provided by the user upon logon to authenticate the user on the target system.



Authentication with login and password substitution

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

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



Note:

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

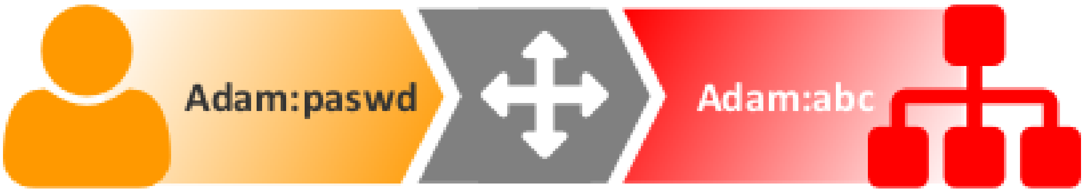
Note: In case of Oracle database, the user password and the privileged account password must be both either shorter than 16 characters or 16-32 characters long.

Two-fold authentication

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

Authentication with password substitution

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



Note:

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

Authentication by target server

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

Administrator approved access

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

Related topics:

- *Creating a safe*
- *Approving pending user requests*
- *Declining pending requests*
- *System overview*
- *External authentication servers configuration*
- *Security measures*

2.6 Security measures

2.6.1 Data encryption

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

Virtual machine distribution

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.

Database

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

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

2.6.2 Backups

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

2.6.3 Permissions

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

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

2.6.4 Sandboxing

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

2.6.5 Reliability

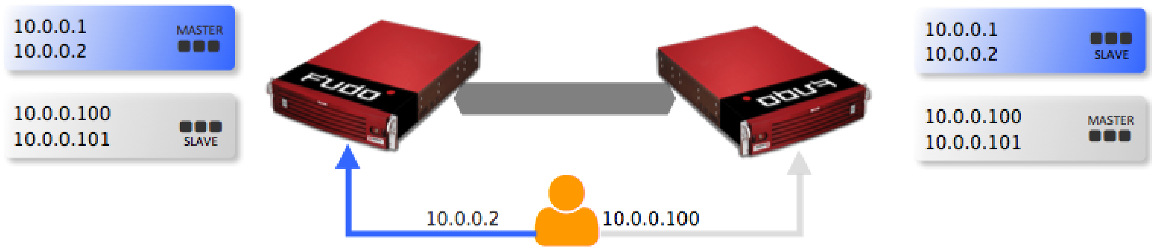
System hardware configuration is optimized to deliver high performance and high availability.

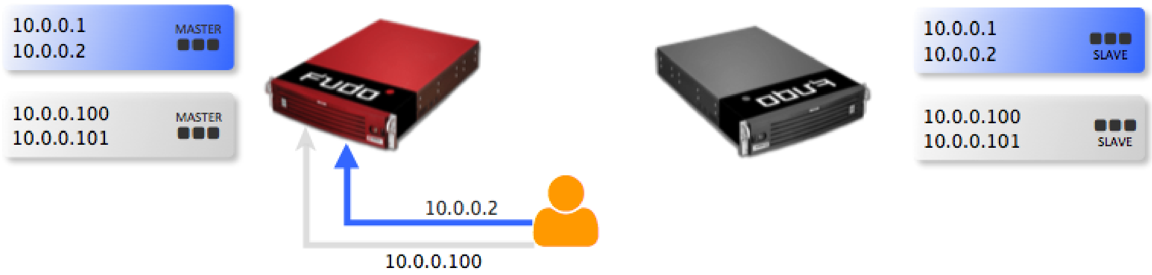
2.6.6 Cluster configuration

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

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

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





Related topics:

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

2.7 Data model

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

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

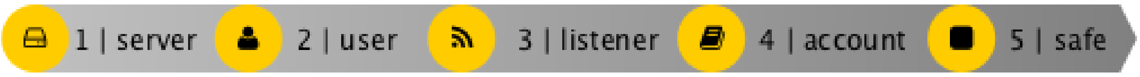
Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

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

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

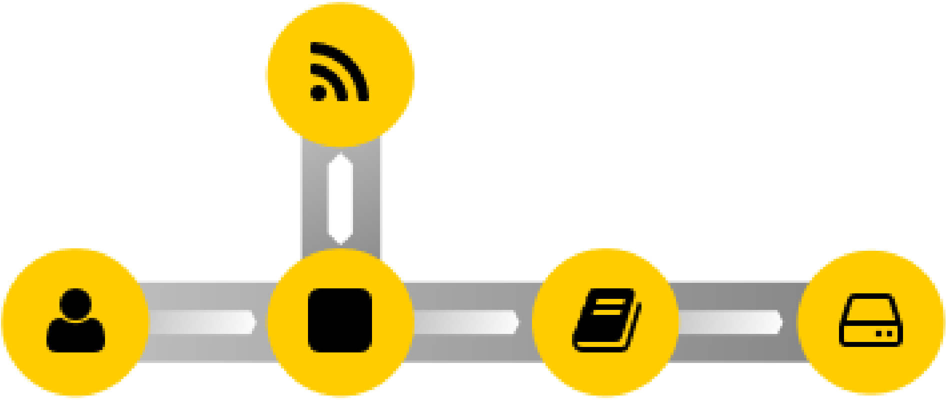
Listener determines server connection mode (proxy, gateway, transparent, bastion) as well as its specifics.

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



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

Objects relations chart



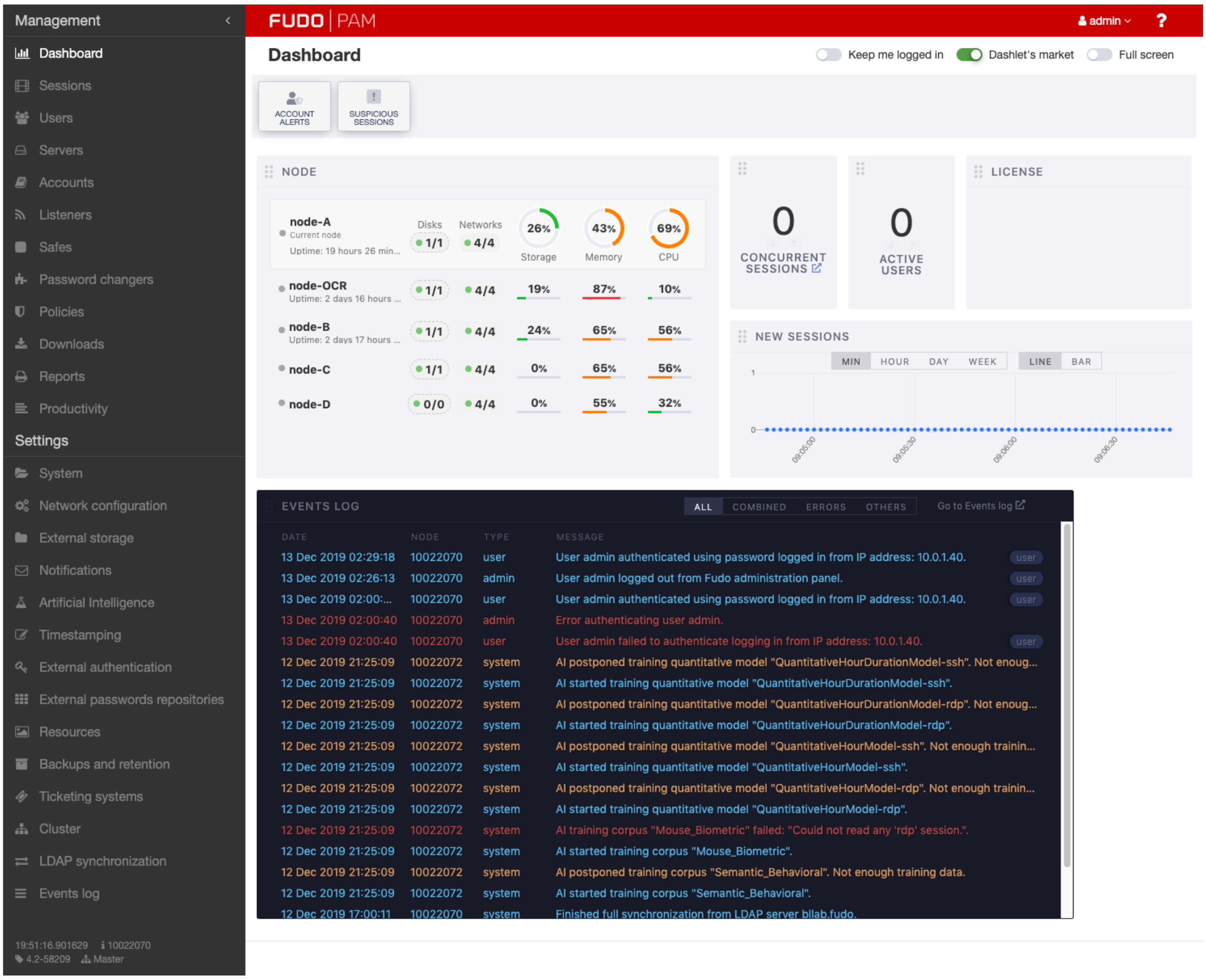
Safe is the central data model object. It regulates access to monitores servers by specifying privileged accounts on monitored servers along with the listeners which determine the actual connection parameters (e.g. IP address, port number) depending on the given protocol. This kind of data model allows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

Related topics:

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

2.8 Dashboard

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



	Disks	Networks	Storage	Memory	CPU
node-A Current node Uptime: 19 hours 26 min...	1/1	4/4	26%	43%	69%
node-OCR Uptime: 2 days 16 hours ...	1/1	4/4	19%	87%	10%
node-B Uptime: 2 days 17 hours ...	1/1	4/4	24%	65%	56%
node-C	1/1	4/4	0%	65%	56%
node-D	0/0	4/4	0%	55%	32%

DATE	NODE	TYPE	MESSAGE	
13 Dec 2019 02:29:18	10022070	user	User admin authenticated using password logged in from IP address: 10.0.1.40.	user
13 Dec 2019 02:26:13	10022070	admin	User admin logged out from Fudo administration panel.	user
13 Dec 2019 02:00:...	10022070	user	User admin authenticated using password logged in from IP address: 10.0.1.40.	user
13 Dec 2019 02:00:40	10022070	admin	Error authenticating user admin.	
13 Dec 2019 02:00:40	10022070	user	User admin failed to authenticate logging in from IP address: 10.0.1.40.	user
12 Dec 2019 21:25:09	10022072	system	AI postponed training quantitative model "QuantitativeHourDurationModel-ssh". Not enoug...	
12 Dec 2019 21:25:09	10022072	system	AI started training quantitative model "QuantitativeHourDurationModel-ssh".	
12 Dec 2019 21:25:09	10022072	system	AI postponed training quantitative model "QuantitativeHourDurationModel-rdp". Not enoug...	
12 Dec 2019 21:25:09	10022072	system	AI started training quantitative model "QuantitativeHourDurationModel-rdp".	
12 Dec 2019 21:25:09	10022072	system	AI postponed training quantitative model "QuantitativeHourModel-ssh". Not enough trainin...	
12 Dec 2019 21:25:09	10022072	system	AI started training quantitative model "QuantitativeHourModel-ssh".	
12 Dec 2019 21:25:09	10022072	system	AI postponed training quantitative model "QuantitativeHourModel-rdp". Not enough trainin...	
12 Dec 2019 21:25:09	10022072	system	AI started training quantitative model "QuantitativeHourModel-rdp".	
12 Dec 2019 21:25:09	10022072	system	AI training corpus "Mouse_Biometric" failed: "Could not read any 'rdp' session.".	
12 Dec 2019 21:25:09	10022072	system	AI started training corpus "Mouse_Biometric".	
12 Dec 2019 21:25:09	10022072	system	AI postponed training corpus "Semantic_Behavioral". Not enough training data.	
12 Dec 2019 21:25:09	10022072	system	AI started training corpus "Semantic_Behavioral".	
12 Dec 2019 17:00:11	10022070	system	Finished full synchronization from LDAP server bllab.fudo.	

Note:

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

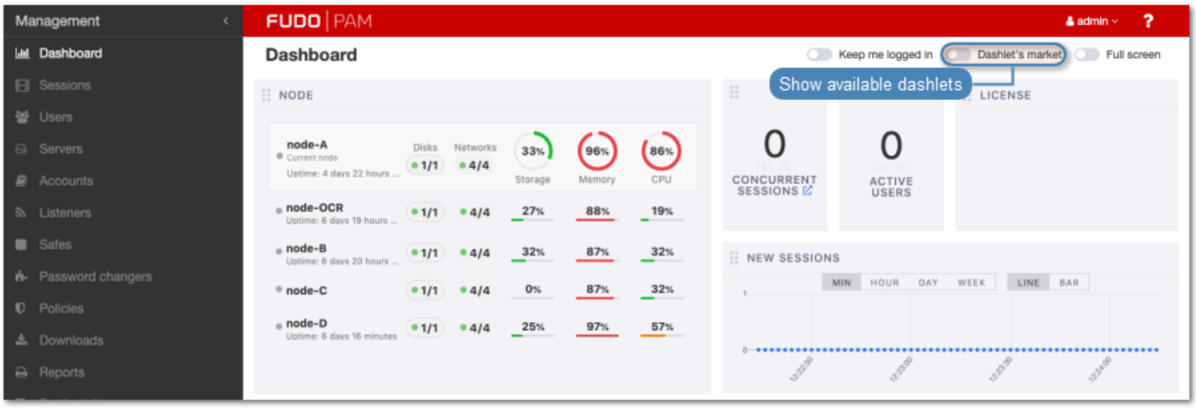
2.8.1 Widgets

New sessions	Chart depicting the number of newly established connections in a given time interval.
Concurrent sessions	The current number of user sessions.
Suspicious sessions	High-threat level sessions. The dashlet allows the following timeline configurations for the sessions: last 12 hours, last day, last week, and last month.
Account alerts	Number of accounts at risk of a security breach.
Active users	Nubmer of currently connected users.
License	Information on the active license.
Node	Status information on the current Fudo PAM instance as well as other nodes.
System logs	Recent system events.

Note: Available widgets depend on the *user role*.

2.8.2 Adding and customizing dashlets

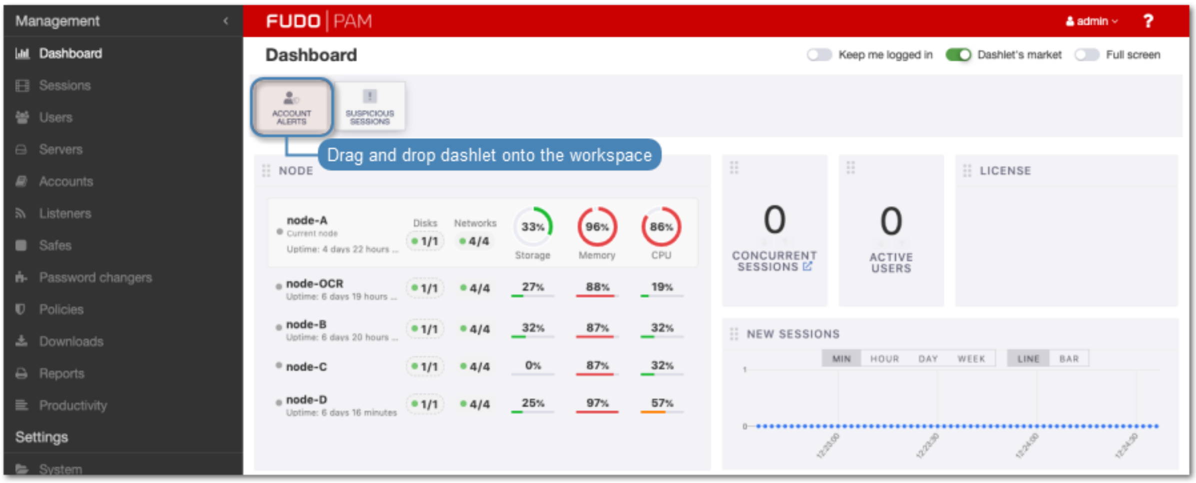
1. Click the *Dashlets market* switcher to display available dashlets.



Show available dashlets

	Disks	Networks	Storage	Memory	CPU
node-A Current node Uptime: 4 days 22 hours ...	1/1	4/4	33%	96%	86%
node-OCR Uptime: 6 days 19 hours ...	1/1	4/4	27%	88%	19%
node-B Uptime: 6 days 20 hours ...	1/1	4/4	32%	87%	32%
node-C	1/1	4/4	0%	87%	32%
node-D Uptime: 6 days 16 minutes	1/1	4/4	25%	97%	57%

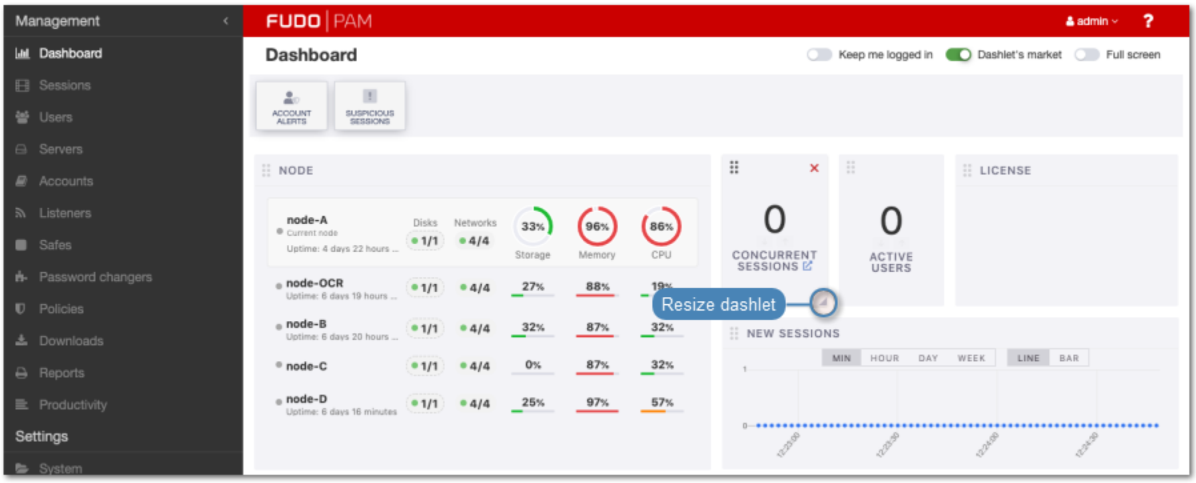
2. Drag and drop a dashlet onto the workspace.



Drag and drop dashlet onto the workspace

	Disks	Networks	Storage	Memory	CPU
node-A Current node Uptime: 4 days 22 hours ...	1/1	4/4	33%	96%	86%
node-OCR Uptime: 6 days 19 hours ...	1/1	4/4	27%	88%	19%
node-B Uptime: 6 days 20 hours ...	1/1	4/4	32%	87%	32%
node-C	1/1	4/4	0%	87%	32%
node-D Uptime: 6 days 16 minutes	1/1	4/4	25%	97%	57%

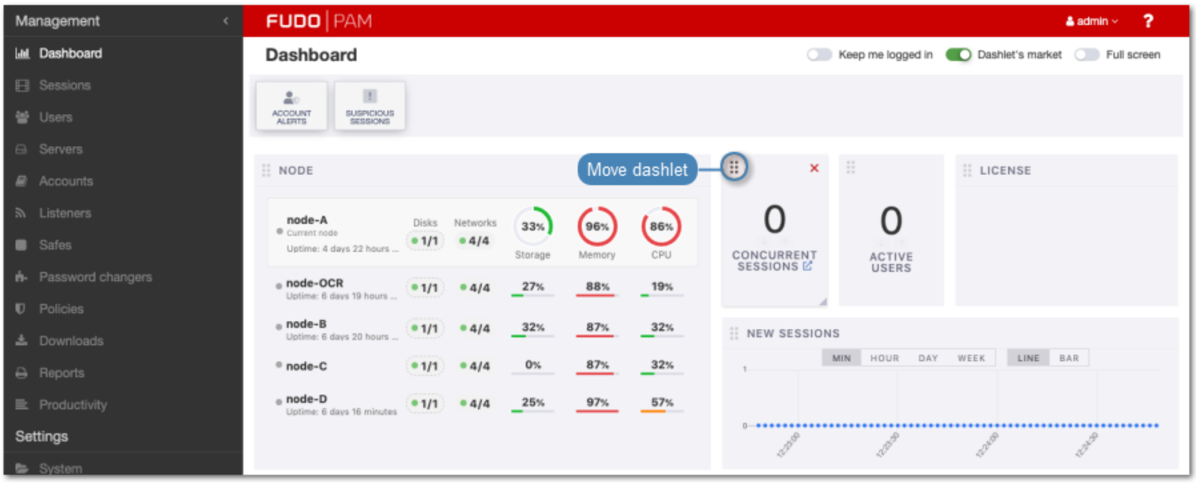
3. Click and drag bottom-right corner of the dashlet to resize it.



Resize dashlet

	Disks	Networks	Storage	Memory	CPU
node-A Current node Uptime: 4 days 22 hours ...	1/1	4/4	33%	96%	86%
node-OCR Uptime: 6 days 19 hours ...	1/1	4/4	27%	88%	19%
node-B Uptime: 6 days 20 hours ...	1/1	4/4	32%	87%	32%
node-C	1/1	4/4	0%	87%	32%
node-D Uptime: 6 days 16 minutes	1/1	4/4	25%	97%	57%

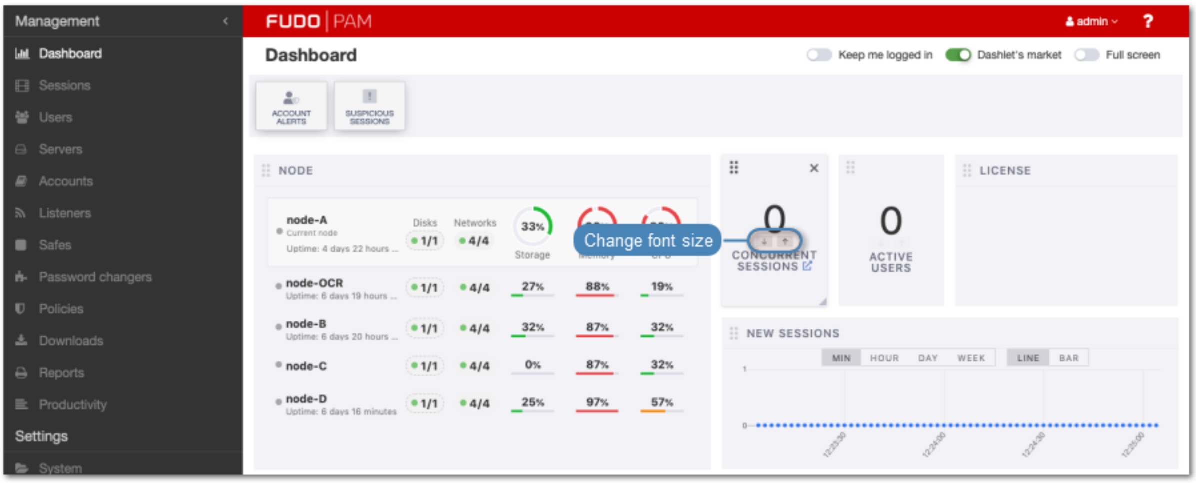
4. Click and drag the top-left corner to relocate the dashlet.



Move dashlet

	Disks	Networks	Storage	Memory	CPU
node-A Current node Uptime: 4 days 22 hours ...	1/1	4/4	33%	96%	86%
node-OCR Uptime: 6 days 19 hours ...	1/1	4/4	27%	88%	19%
node-B Uptime: 6 days 20 hours ...	1/1	4/4	32%	87%	32%
node-C	1/1	4/4	0%	87%	32%
node-D Uptime: 6 days 16 minutes	1/1	4/4	25%	97%	57%

5. Click arrows to change font-size.

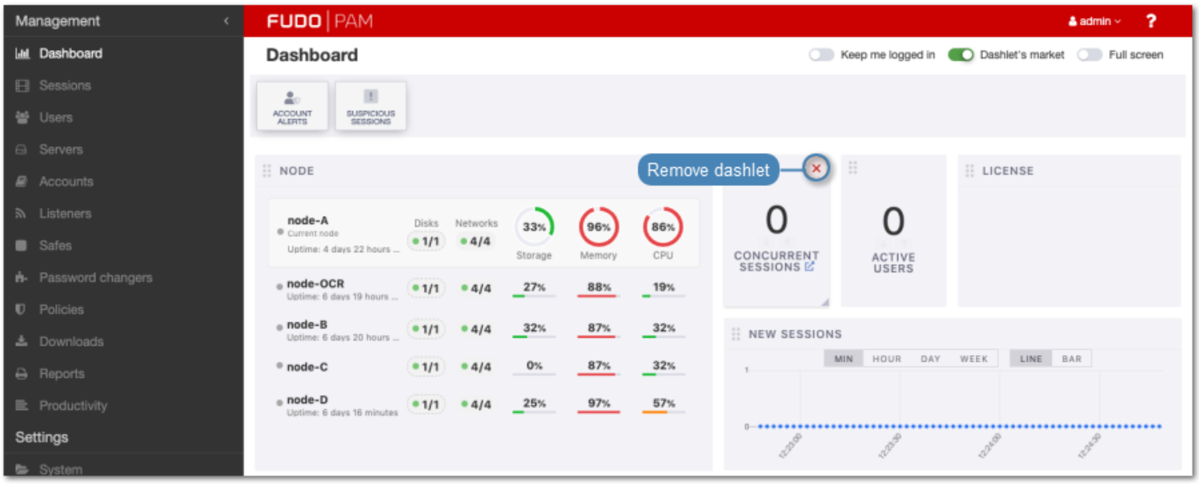


Change font size

	Disks	Networks	Storage	Memory	CPU
node-A Current node Uptime: 4 days 22 hours ...	1/1	4/4	33%		
node-OCR Uptime: 6 days 19 hours ...	1/1	4/4	27%	88%	19%
node-B Uptime: 6 days 20 hours ...	1/1	4/4	32%	87%	32%
node-C	1/1	4/4	0%	87%	32%
node-D Uptime: 6 days 16 minutes	1/1	4/4	25%	97%	57%

2.8.3 Deleting dashlets

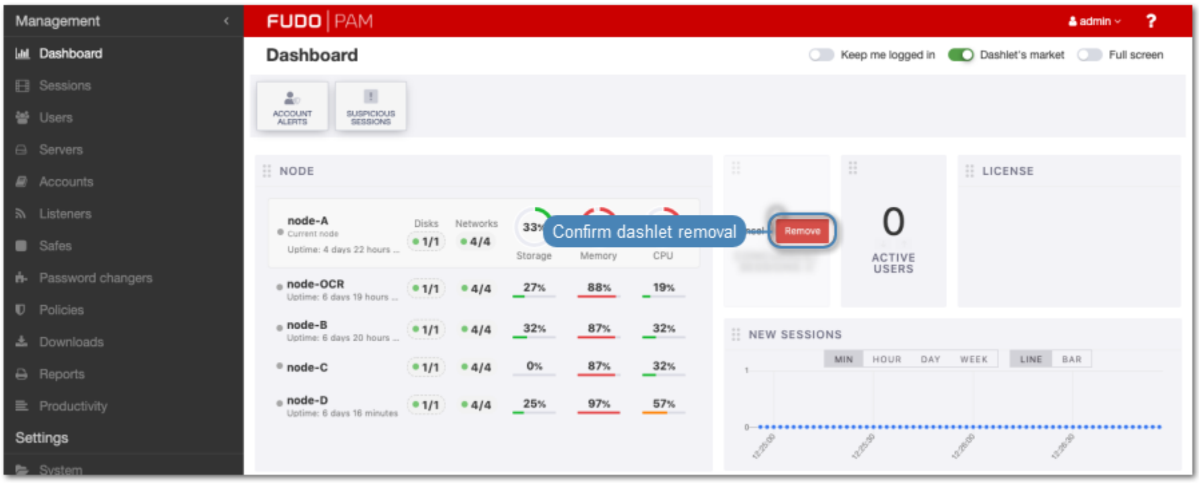
1. Click ✖ icon in the top-right corner.



Remove dashlet

	Disks	Networks	Storage	Memory	CPU
node-A Current node Uptime: 4 days 22 hours ...	1/1	4/4	33%	96%	86%
node-OCR Uptime: 6 days 19 hours ...	1/1	4/4	27%	88%	19%
node-B Uptime: 6 days 20 hours ...	1/1	4/4	32%	87%	32%
node-C	1/1	4/4	0%	87%	32%
node-D Uptime: 6 days 16 minutes	1/1	4/4	25%	97%	57%

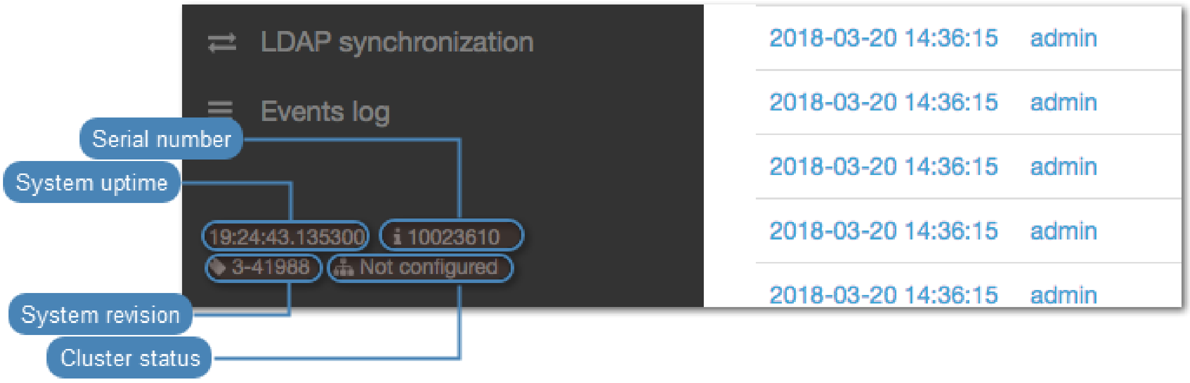
2. Click *Remove* to remove selected dashlet.



	Disks	Networks	Storage	Memory	CPU
node-A Current node Uptime: 4 days 22 hours ...	1/1	4/4	33%		
node-OCR Uptime: 6 days 19 hours ...	1/1	4/4	27%	88%	19%
node-B Uptime: 6 days 20 hours ...	1/1	4/4	32%	87%	32%
node-C	1/1	4/4	0%	87%	32%
node-D Uptime: 6 days 16 minutes	1/1	4/4	25%	97%	57%

Note: Removed dashlets appear in the dashlets market area.

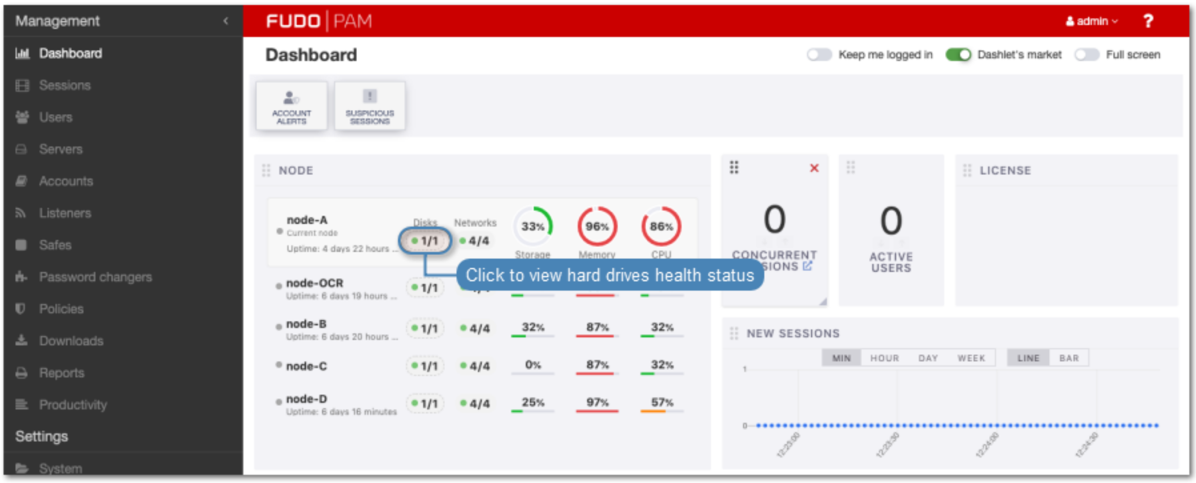
2.8.4 System information



2018-03-20 14:36:15	admin
2018-03-20 14:36:15	admin
2018-03-20 14:36:15	admin
2018-03-20 14:36:15	admin
2018-03-20 14:36:15	admin

2.8.5 Hard drives status information

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



	Disks	Networks	Storage	Memory	CPU
node-A Current node Uptime: 4 days 22 hours ...	1/1	4/4	33%	96%	86%
node-OCR Uptime: 6 days 19 hours ...	1/1				
node-B Uptime: 6 days 20 hours ...	1/1	4/4	32%	87%	32%
node-C	1/1	4/4	0%	87%	32%
node-D Uptime: 6 days 16 minutes	1/1	4/4	25%	97%	57%

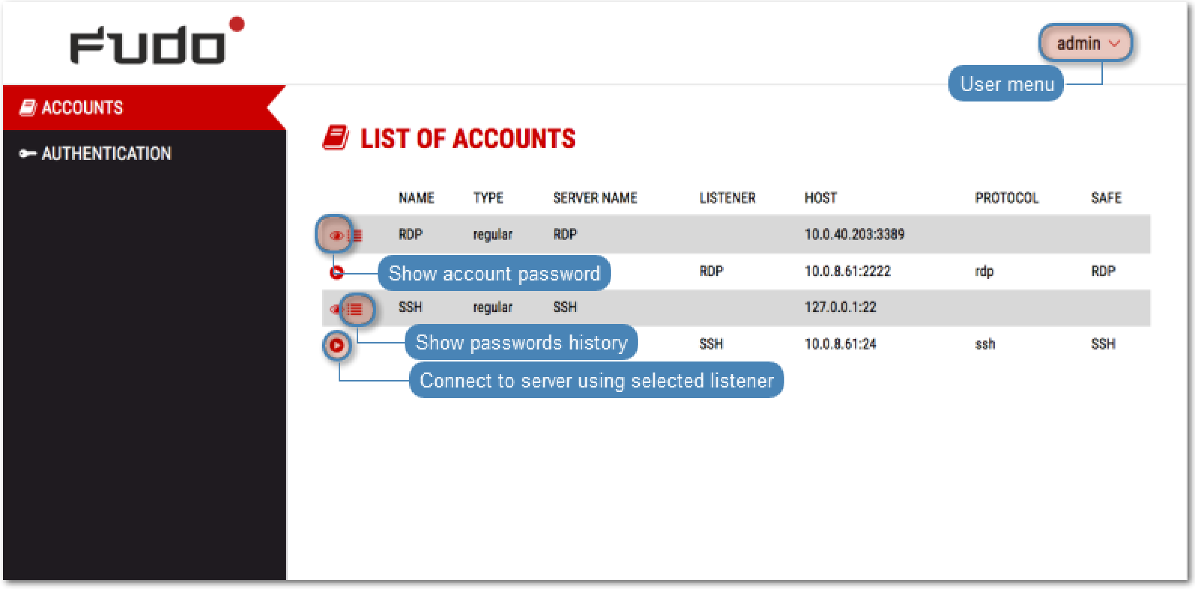
🟢	Hard drive operates properly.
🔵	Data on the hard drive is being synchronized.
🟠	Data read/write errors - the hard drive does not operate properly and it is likely to fail - contact the technical support to discuss hard drive replacement.
🔴	Hard drive failure - the hard drive must be replaced - contact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

Related topics:

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

2.9 User portal

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



LIST OF ACCOUNTS

NAME	TYPE	SERVER NAME	LISTENER	HOST	PROTOCOL	SAFE
RDP	regular	RDP		10.0.40.203:3389		
			RDP	10.0.8.61:2222	rdp	RDP
SSH	regular	SSH		127.0.0.1:22		
			SSH	10.0.8.61:24	ssh	SSH

Related topics:

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

CHAPTER 3

System deployment

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

3.1 Requirements

Administration panel

System is managed in administration panel available through web browser. Recommended browsers are Google Chrome, Mozilla Firefox and Microsoft Edge (Chromium based).

Network requirements

Correct operation requires:

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

Hardware requirements

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

Virtual appliance requirements

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

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

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

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

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

Supported virutalization environments:

- VMware Tools
- VirtualBox

VNC software client requirements

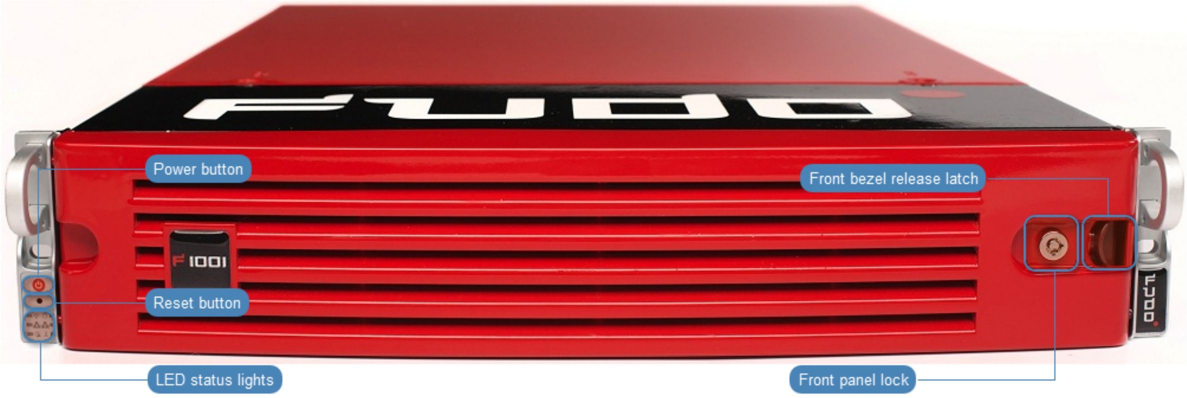
VNC connections require 24-bit (true color) mode.

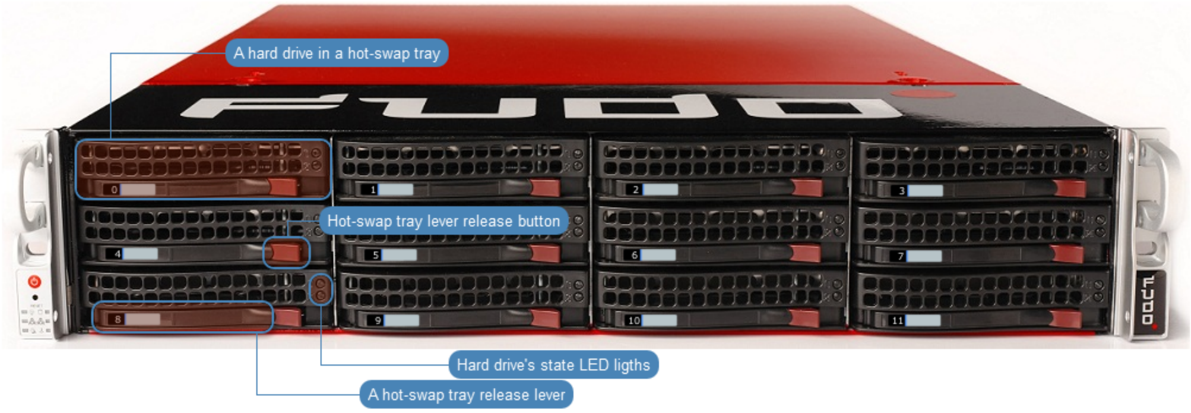
3.2 Hardware overview

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

Fudo PAM F1002

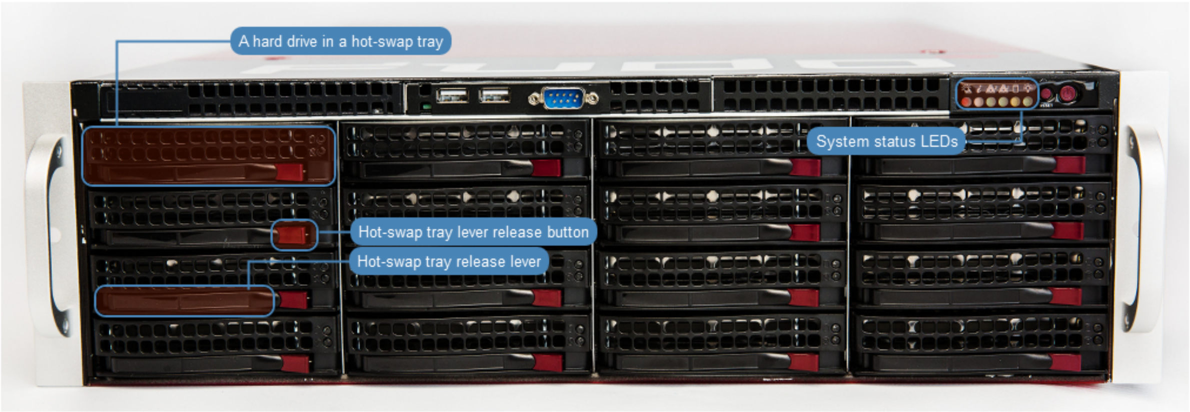
- Chassis: 19" 2U
- Dimensions: 89 mm (height), 437 mm (width), 647 mm (depth)
- PSU: 2x 920 W
- System memory: 32 GB
- Internal storage: 12x 2 TB, 2x 480 GB SSD
- Optional additional network interfaces: Intel I350AM4 4x RJ45 1GbE, Chelsio T520-CR 10G, HP NC364T PCI EXPRESS QUAD PORT GIGABIT or 2X1GB RJ45




A hard drive in a hot-swap tray
Hot-swap tray lever release button
Hard drive's state LED ligths
A hot-swap tray release lever

Fudo PAM F3002

- Chassis: 19" 3U
- Dimensions: 132 mm (height), 437 mm (width), 647 mm (depth)
- PSU: 2x 1000 W
- System memory: 64 GB
- Internal storage: 16x 6 TB HDD, 2x 480 GB SSD
- Optional external storage controller: 2x Qlogic HBA FC QLE2560 8Gb
- Optional additional network interfaces: 2x Intel I350AM4 4x RJ45 1GbE


A hard drive in a hot-swap tray
System status LEDs
Hot-swap tray lever release button
Hot-swap tray release lever

Fudo PAM F5000

- Chassis: 19" 4U
- Dimensions: 178 mm (height), 437 mm (width), 699 mm (depth)
- PSU: 2x 1280 W
- System memory: 128 GB
- Internal storage: 36x 8 TB, 2x 480 GB SSD
- Optional external storage controller: 2x Qlogic HBA FC QLE2560 8Gb
- Optional additional network interfaces: 2x Intel I350AM4 4x RJ45 1GbE

Related topics:

- *Initial boot up*

- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*

3.3 System initiation

Appliance

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

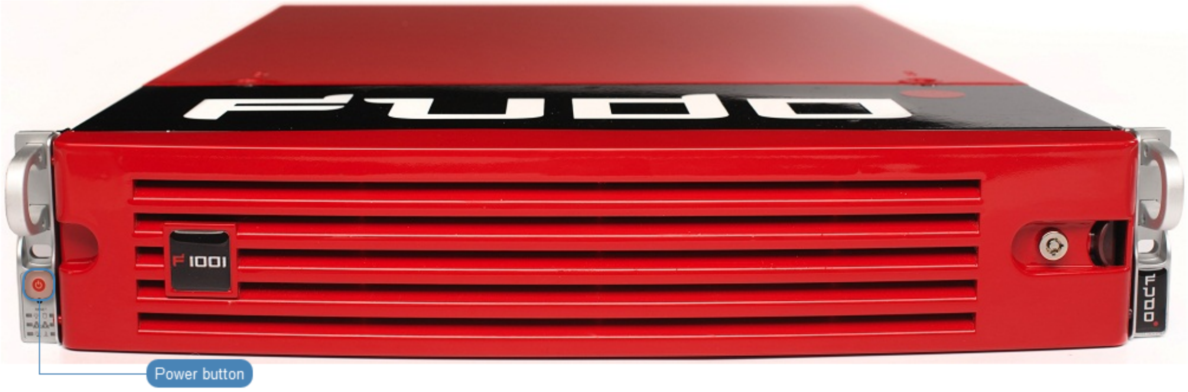
1. Install device in 19" rack cabinet.
2. Connect both power supply units to 230V/110V power outlets.

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 Fudo PAM.

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

5. Press the power button on the front panel.



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

Warning:

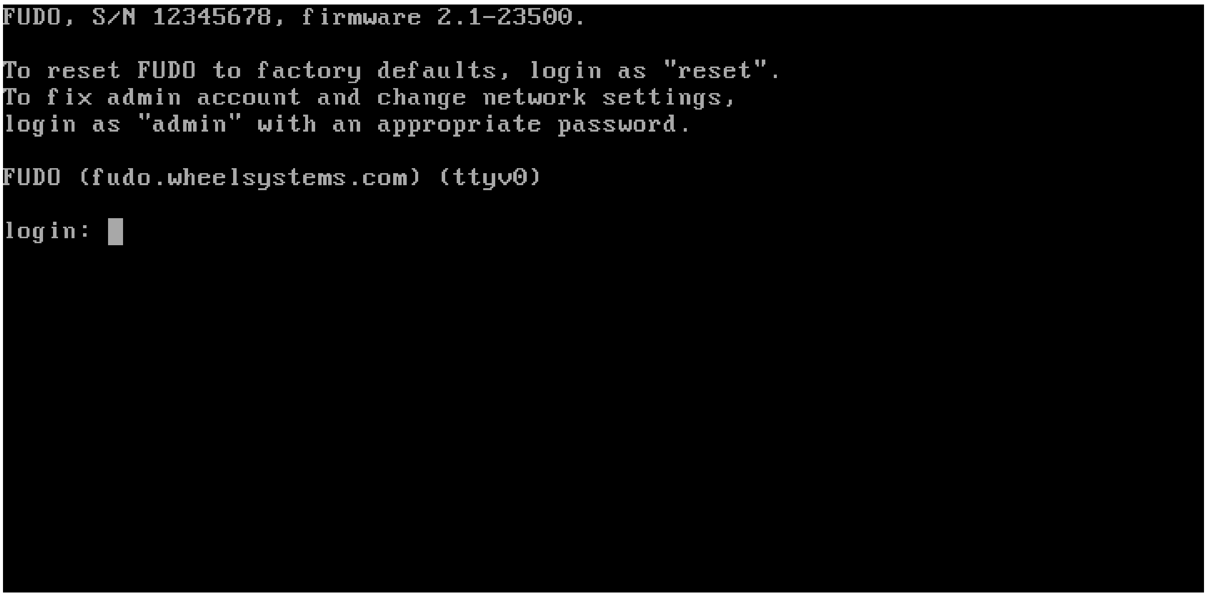
- One of the USB flash drives containing encryption key must be disconnected and placed in a secure location, accessible only to authorized personnel.
- If the USB flash drives with encryption keys are lost, device will not be able to boot up and stored sessions will not be accessible. Manufacturer does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

Note:

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

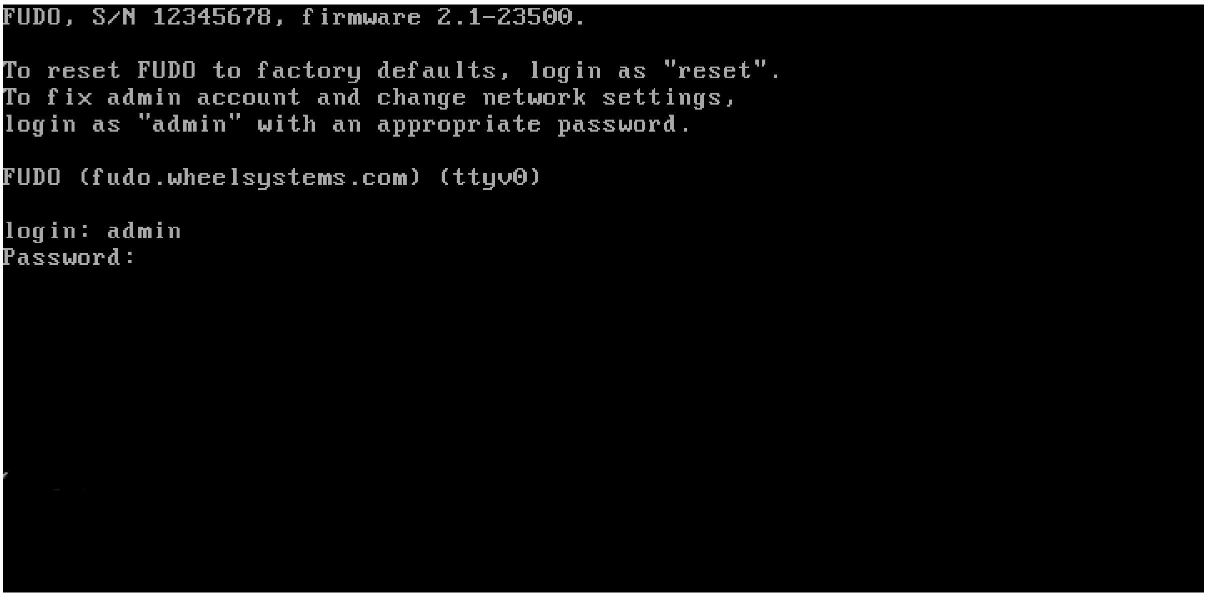
Setting IP address using system console

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



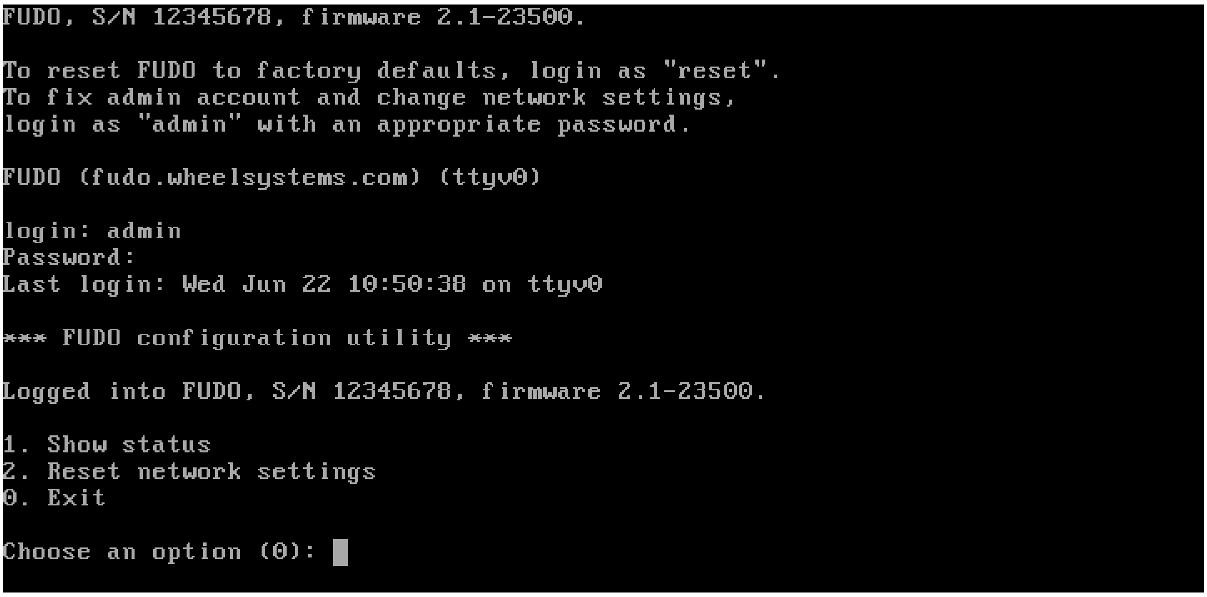
```
FUDO, S/N 12345678, firmware 2.1-23500.

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*.



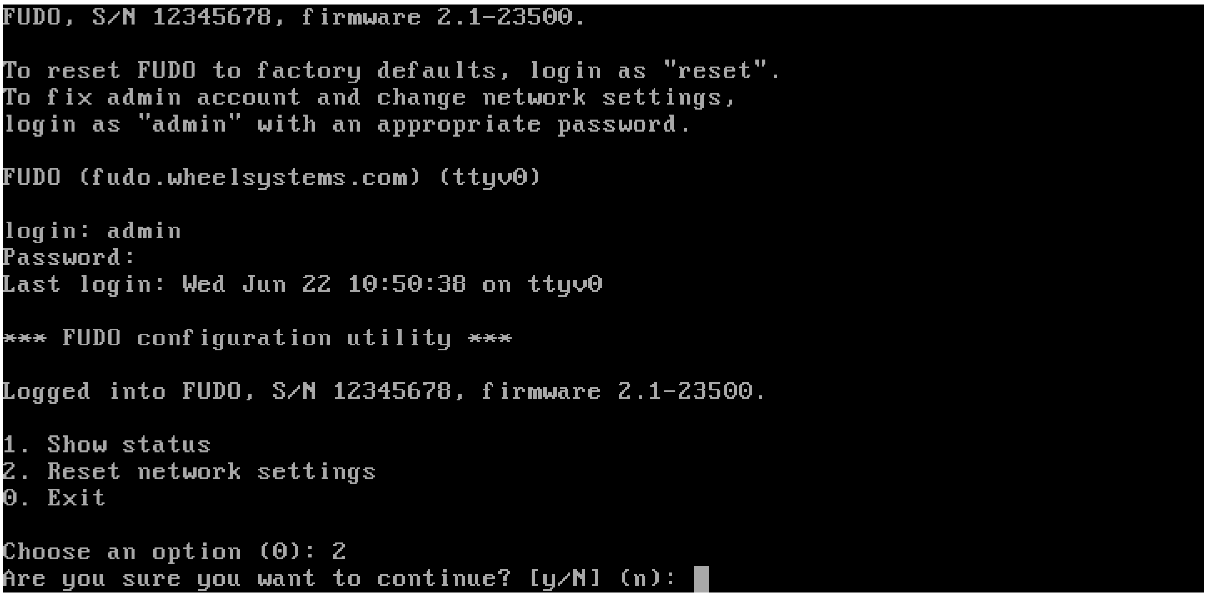
```
FUDO, S/N 12345678, firmware 2.1-23500.

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.



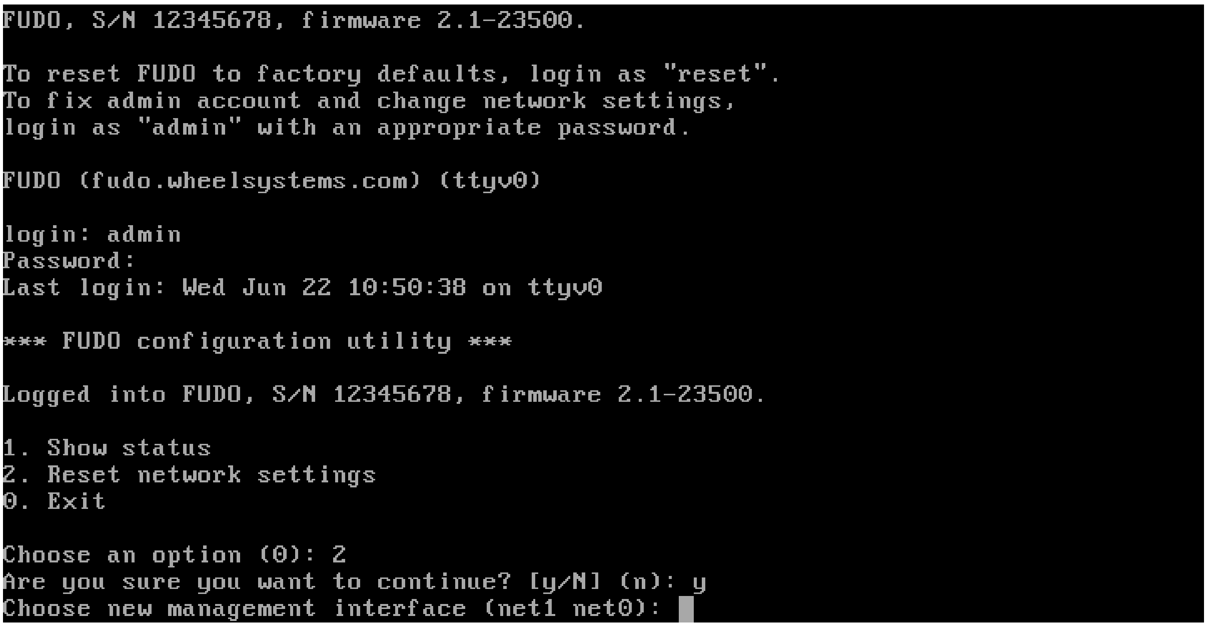
```
FUDO, S/N 12345678, firmware 2.1-23500.

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.



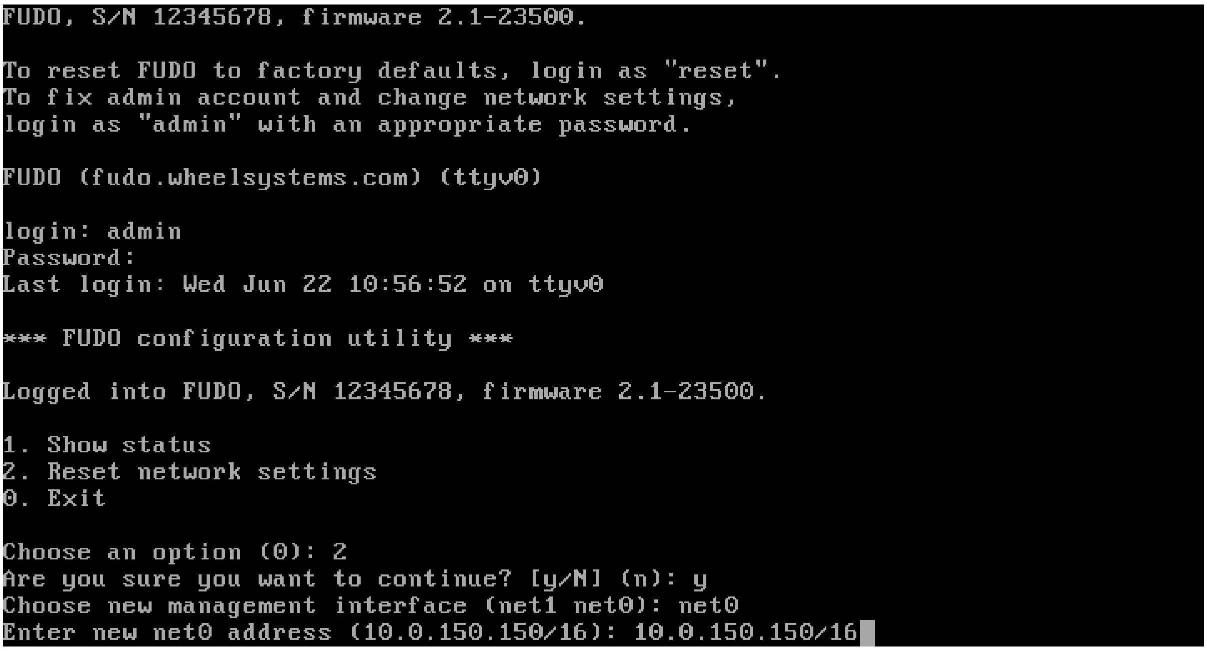
```
FUDO, S/N 12345678, firmware 2.1-23500.

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 (Fudo PAM web interface is accessible through the management interface).



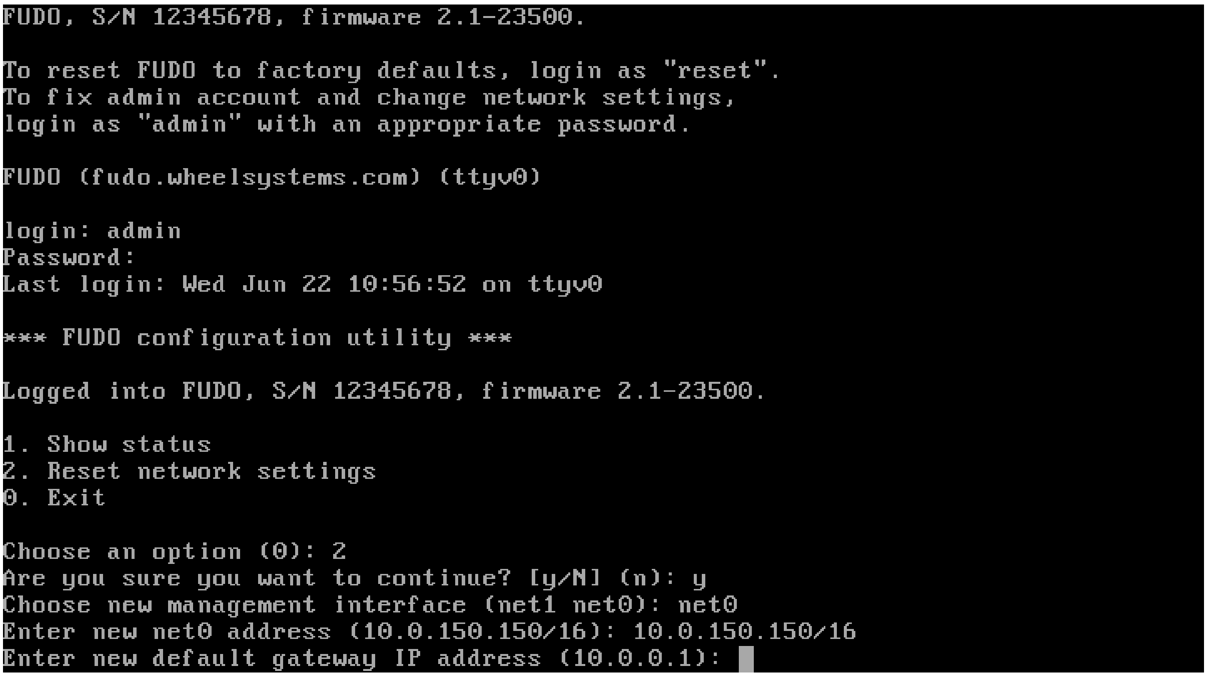
```
FUDO, S/N 12345678, firmware 2.1-23500.

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:

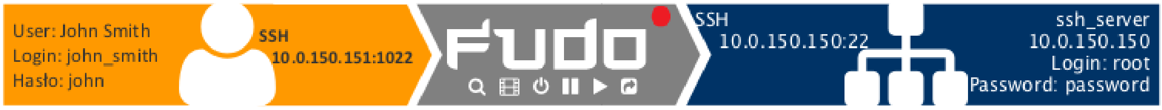
- *Requirements*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*
- *System overview*
- *Security measures*

CHAPTER 4

Quick start

4.1 SSH

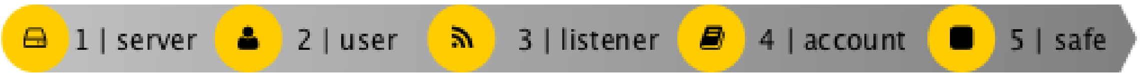
This chapter contains an example of a basic Fudo PAM configuration, to monitor SSH access to a remote server. In this scenario, the user connects to the remote server over the *SSH* protocol and logs in to the Fudo PAM using an individual login and password combination (`john_smith`/`john`). When establishing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



4.1.1 Prerequisites

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

4.1.2 Configuration



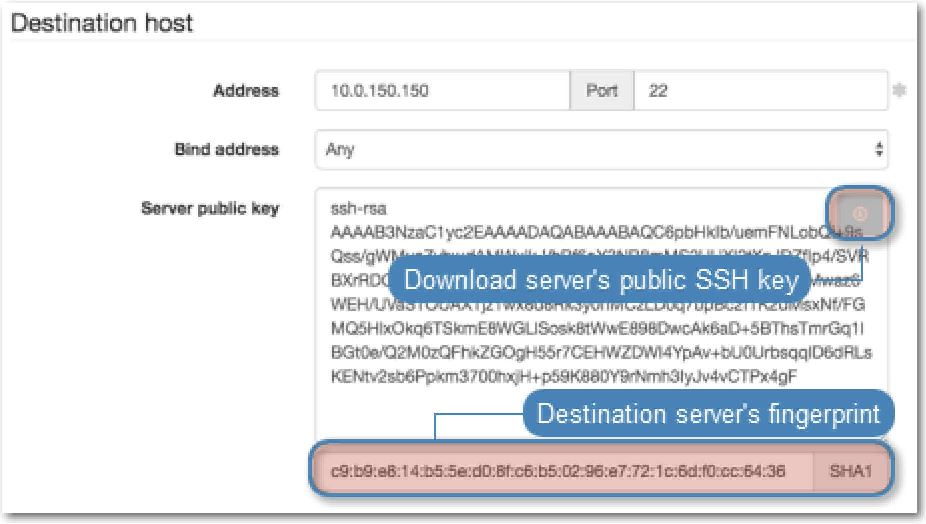
Adding a server

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

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

Parameter	Value
General	
Name	`ssh_server`
Description	✗
Blocked	✗
Protocol	`SSH`
Legacy ciphers	✗
Bind address	`Any`
Permissions	
Granted users	✗
Server addresses	
IP address	`10.0.150.150`
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
AAAAB3NzaC1yc2EAAAADAQABAAABAQC6pbHklb/uemFNLobQ+9s
Qss/gW                                          p4/SVR
BXrRDC                                          Wwaz6
WEH/U                                           sxNf/FG
MQ5HIxOkq6TSkmE8WGLISosk8tWwE898DwcAk6aD+5BThsTmrGq1I
BGt0e/Q2M0zQFhkZGOgH55r7CEHWZDWI4YpAv+bU0UrbsqqID6dRLs
KENtv2sb6Ppkm3700hxjH+p59K880Y9rNmh3lyJv4vCTPx4gF
```

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

Download server's public SSH key
Destination server's fingerprint

5. Click *Save*.

Adding a user

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

1. Select *Management > Users*.

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

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

4. Click *Save*.

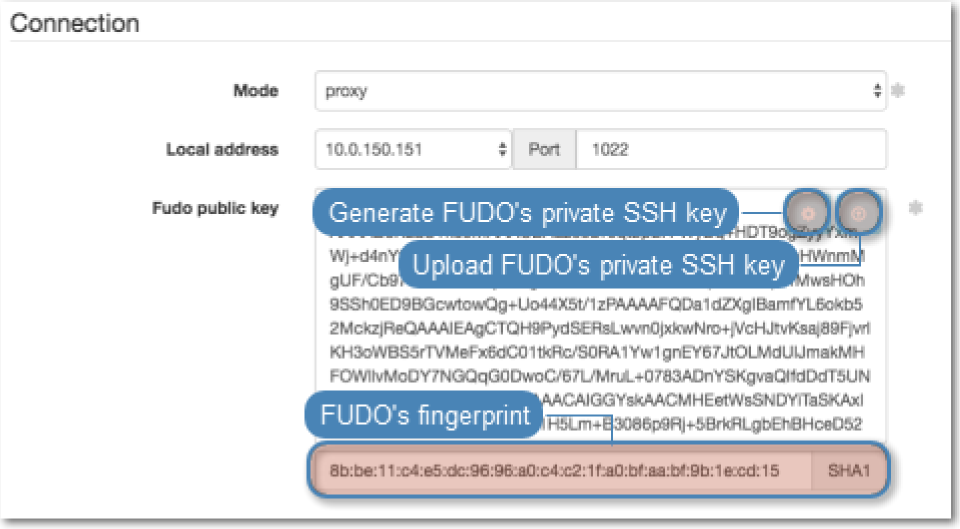
Adding a listener

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

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

Parameter	Value
General	
Name	`ssh_listener`
Blocked	❌
Protocol	`SSH`
Legacy ciphers	❌
Case insensitivity	❌
Permissions	
Granted users	❌
Connection	
Mode	`proxy`
Local address	`10.0.150.151`
Port	`1022`
External address	❌
External port	❌

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



Connection

Mode: proxy

Local address: 10.0.150.151 Port 1022

Fudo public key:

```
9SSh0ED9BGcwtowQg+Uo44X5t/1zPAAAAFQDa1dZXglBamfYL6okb5
2MckzjReQAAAIEAgCTQH9PydSERsLwvn0jxkwNro+jVcHJtvKsaj89Fjvrl
KH3oWBS5rTVMeFx6dC01tkRc/S0RA1Yw1gnEY67JtOLMdUlJmakMH
FOWIlvMoDY7NGQqG0DwoC/67L/MruL+0783ADnYSKgvaQlfdDdT5UN
```

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

Generate FUDO's private SSH key
Upload FUDO's private SSH key
FUDO's fingerprint

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

5. Click *Save*.

Adding an account

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

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

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

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

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

5. Click *Save*.

Defining a safe

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

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

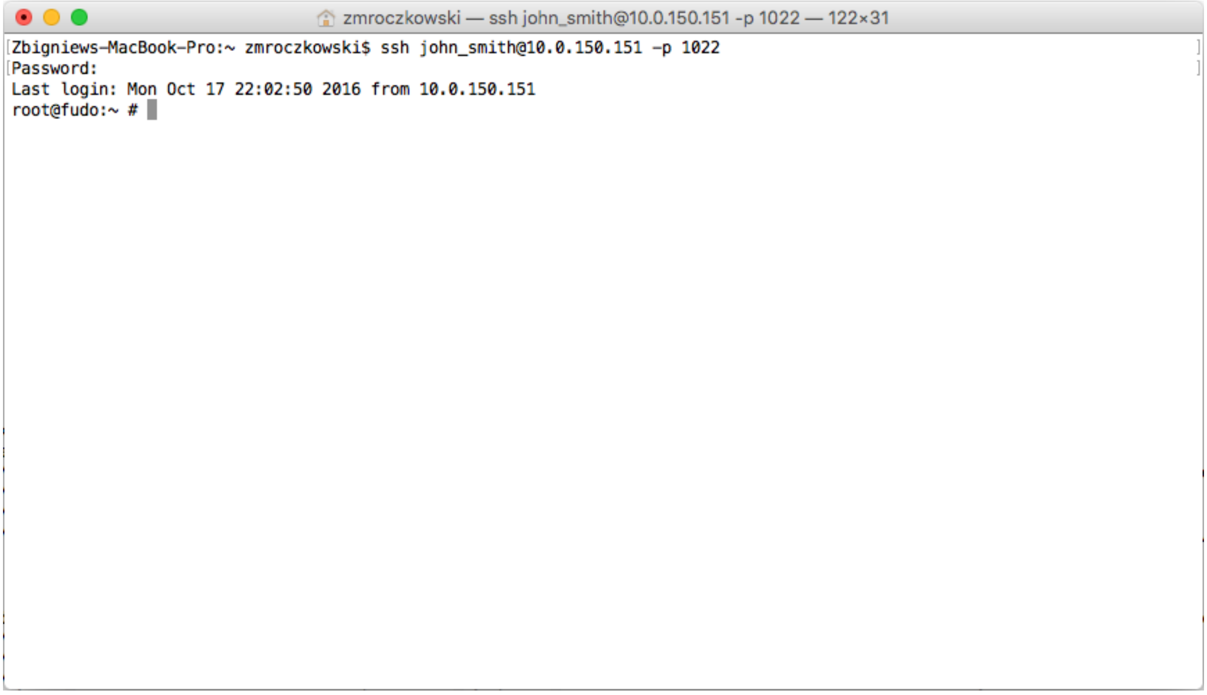
Parameter	Value
General	
Name	`ssh_safe`
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✓
VNC	✗

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

4.1.3 Establishing connection

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

Example:



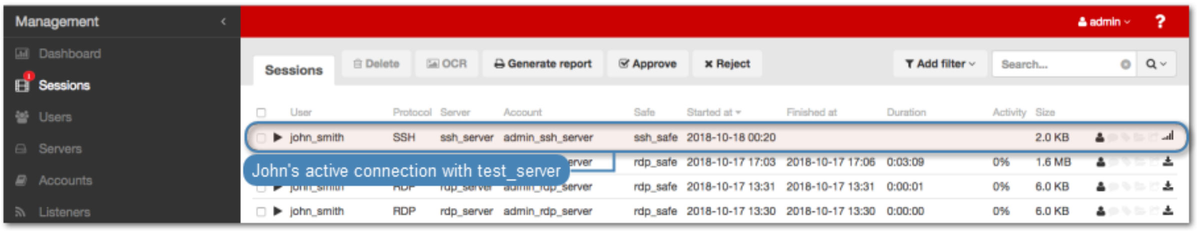
```
Zbigniews-MacBook-Pro:~ zmroczkowski$ ssh john_smith@10.0.150.151 -p 1022
Password:
Last login: Mon Oct 17 22:02:50 2016 from 10.0.150.151
root@fudo:~ #
```

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 Fudo PAM starts recording user's activities.

4.1.4 Viewing user session

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



User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
john_smith	SSH	ssh_server	admin_ssh_server	ssh_safe	2018-10-18 00:20				2.0 KB
			erver	rdp_safe	2018-10-17 17:03	2018-10-17 17:06	0:03:09	0%	1.6 MB
john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 13:31	2018-10-17 13:31	0:00:01	0%	6.0 KB
john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 13:30	2018-10-17 13:30	0:00:00	0%	6.0 KB

John's active connection with test_server

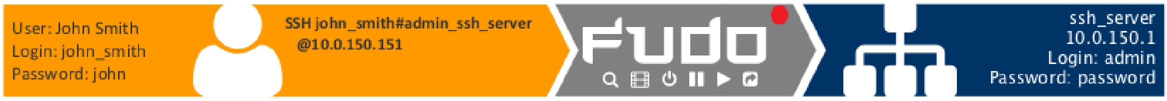
Related topics:

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

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

4.2 SSH in bastion mode

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



4.2.1 Prerequisites

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

4.2.2 Configuration

1 | server
2 | user
3 | listener
4 | account
5 | safe

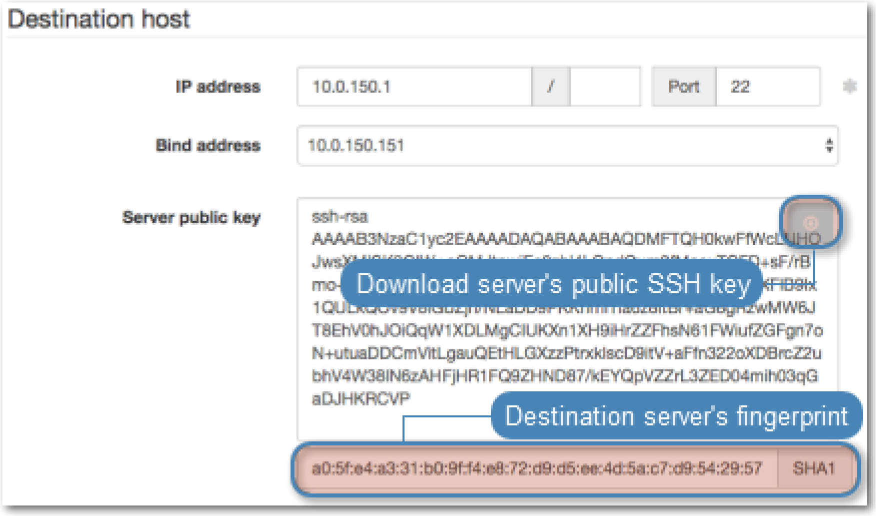
Adding a server

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

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

Parameter	Value
General	
Name	`ssh_server`
Description	❌
Blocked	❌
Protocol	`SSH`
Legacy ciphers	❌
Bind address	`Any`
Permissions	
Granted users	❌
Server addresses	
IP address	`10.0.150.1`
Port	`22`

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



Destination host

IP address: 10.0.150.1 / Port 22

Bind address: 10.0.150.151

Server public key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDMFTQH0kwFfWc[illegible]HO
JwsX[illegible]+sF/rB
mo-[illegible]KFIB9lx
1QU[illegible]zwMW6J
T8EhV0hJOiQqW1XDLMgClUKXn1XH9iHrZZFhsN61FWiufZGFgn7o
N+utuaDDCmVitLgauQEtHLGXzzPtrxklscD9itV+aFfn322oXDBrcZ2u
bhV4W38IN6zAHFjHR1FQ9ZHND87/kEYQpVZZrL3ZED04mih03qG
aDJHKRCVP
```

a0:5f:e4:a3:31:b0:9f:f4:e8:72:d9:d5:ee:4d:5a:c7:d9:54:29:57 SHA1

Download server's public SSH key
Destination server's fingerprint

5. Click *Save*.

Adding a user

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

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

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

4. Click *Save*.

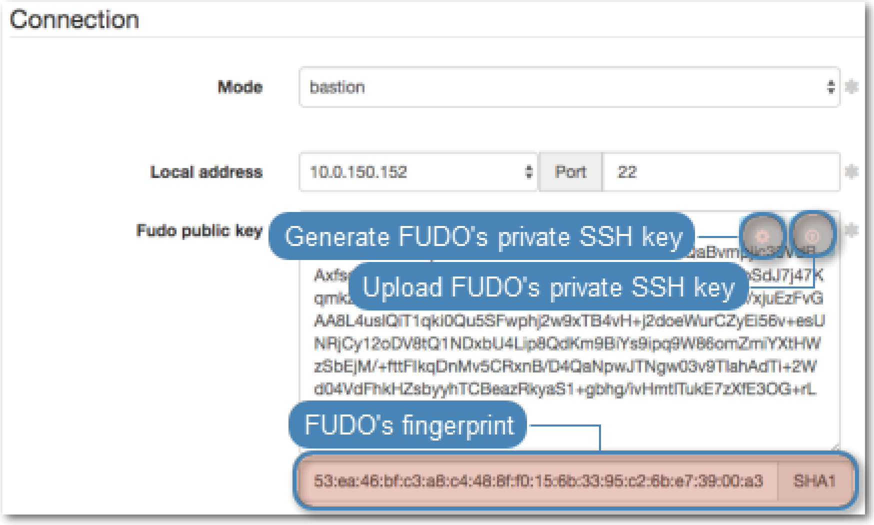
Adding a listener

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

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

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

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



Connection

Mode: bastion

Local address: 10.0.150.152 Port: 22

Fudo public key:

AA8L4usIQiT1qki0Qu5SFwphj2w9xTB4vH+j2doeWurCZyEi56v+esU
NRjCy12oDV8tQ1NDxbU4Lip8QdKm9BiYs9ipq9W86omZmiYXtHW
zSbEjM/+fttFlkqDnMv5CRxnB/D4QaNpwJTNgw03v9TlahAdTi+2W
d04VdFhkHZsbyyhTCBeazRkyaS1+gbhg/ivHmtlTukE7zXfE3OG+rL

53:ea:46:bf:c3:a8:c4:48:8f:f0:15:6b:33:95:c2:6b:e7:39:00:a3 SHA1

Generate FUDO's private SSH key
Upload FUDO's private SSH key
FUDO's fingerprint

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

5. Click *Save*.

Adding an account

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

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

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

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

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

5. Click *Save*.

Defining a safe

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

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

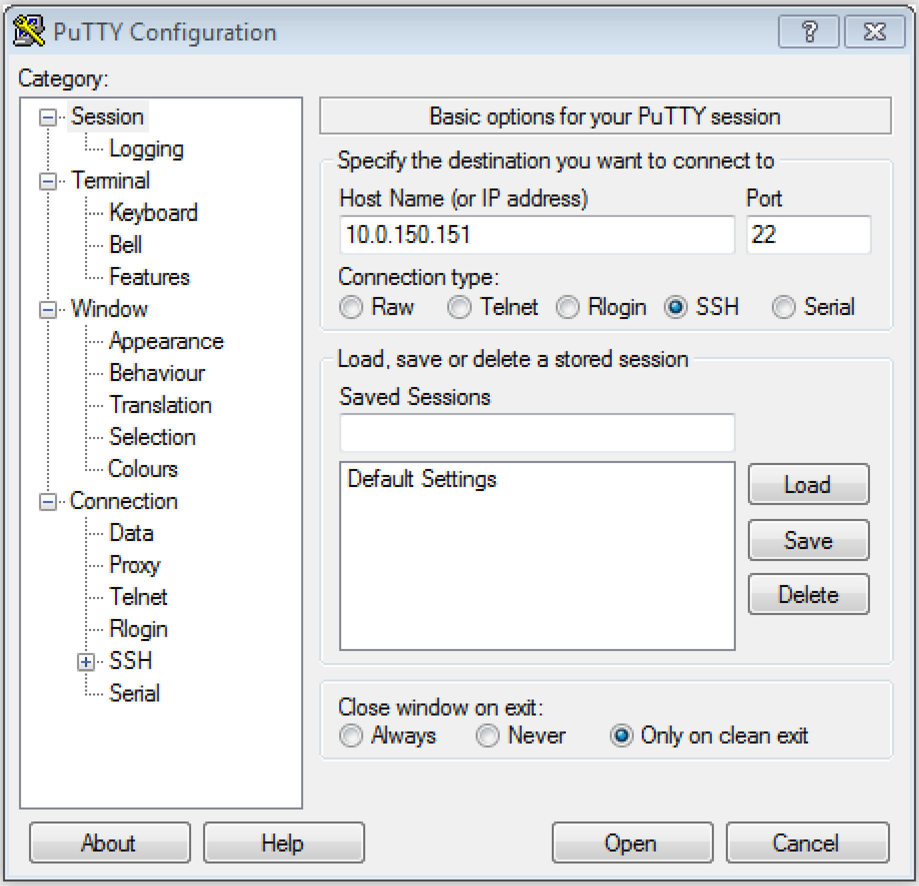
Parameter	Value
General	
Name	`ssh_safe`
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✓
VNC	✗

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

4.2.3 Establishing connection

PuTTY - SSH client for Microsoft Windows

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



Host Name (or IP address): 10.0.150.151

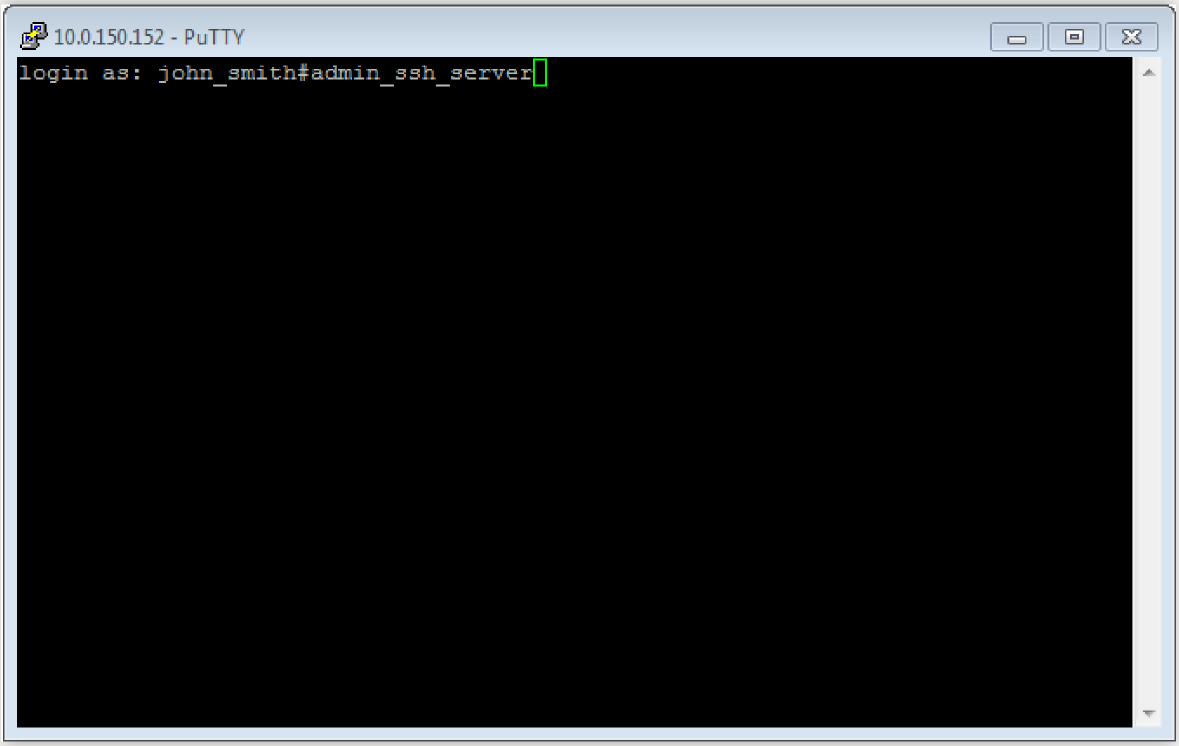
Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

4. Click *Open*.

5. Enter user name along with the account name on the target host.



```
login as: john_smith#admin_ssh_server
```

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

6. Enter password.

Command line interface

Launch terminal and run ssh command:

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

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

- “domain\user”#bsd01@10.0.60.138
- ‘domain\user’#bsd01@10.0.60.138
- domain\user#bsd01@10.0.60.138

4.2.4 Viewing user session

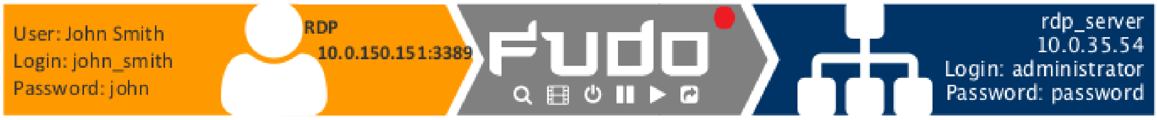
1. Open a web browser and go to the `10.0.150.150` web address.
2. Enter the login and password to login to the Fudo PAM administration panel.
3. Select *Management > Sessions*.
4. Find *John Smith's* session and click the playback icon.

Related topics:

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

4.3 RDP

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



4.3.1 Prerequisites

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

4.3.2 Configuration

1 | server
2 | user
3 | listener
4 | account
5 | safe

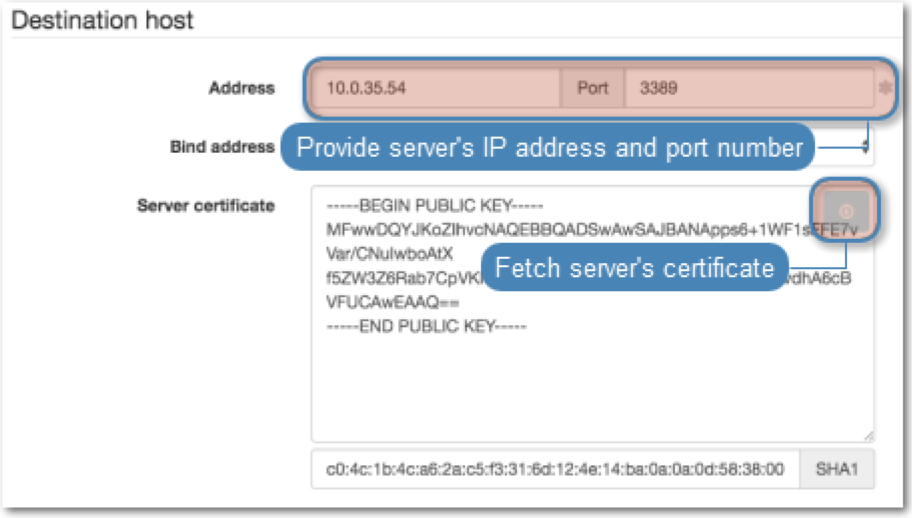
Adding a server

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

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

Parameter	Value
Name	`rdp_server`
Description	✗
Blocked	✗
Protocol	`RDP`
Security	`Standard RDP Security`
Bind address	`10.0.150.151`
Permissions	
Granted users	✗
Server addresses	
IP address	`10.0.35.54`
Port	`3389`

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



Destination host

Address: 10.0.35.54 Port 3389

Bind address

Server certificate:

```
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANApps6+1WF1sFFE7v
Var/CNulwboAtX
f5ZW3Z6Rab7CpVK                                    dhA6cB
VFUCAwEAAQ==
-----END PUBLIC KEY-----
```

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

Provide server's IP address and port number

Fetch server's certificate

5. Click *Save*.

Adding a user

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

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

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

4. Click *Save*.

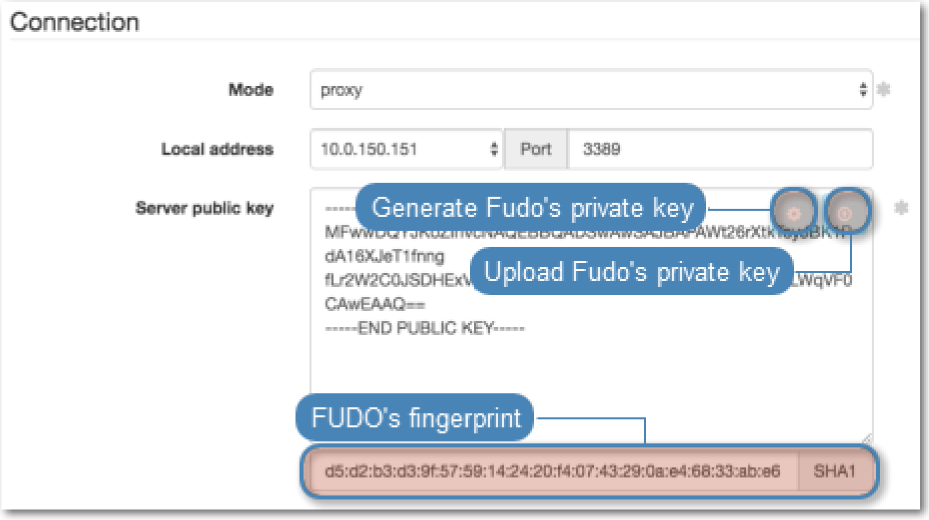
Adding a listener

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

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

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

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



Connection

Mode: proxy

Local address: 10.0.150.151 Port 3389

Server public key:

```
-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPAWt26rXtk
dA16XJeT1fnng
fLr2W2C0JSDHExV                                WqVF0
CAwEAAQ==
-----END PUBLIC KEY-----
```

d5:d2:b3:d3:9f:57:59:14:24:20:f4:07:43:29:0a:e4:68:33: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
General	
Name	`admin_rdp_server`
Blocked	✗
Type	`regular`
Session recording	`all`
OCR sessions	✓
OCR Language	`English`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`rdp_server`
Credentials	
Domain	✗
Login	`administrator`
Replace secret with	`with password`
Password	`password`
Repeat password	`password`
Password change policy	`Static, without restrictions`

4. Click *Save*.

Defining a safe

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

1. Select *Management > Safes*.

2. Click *+ Add*.

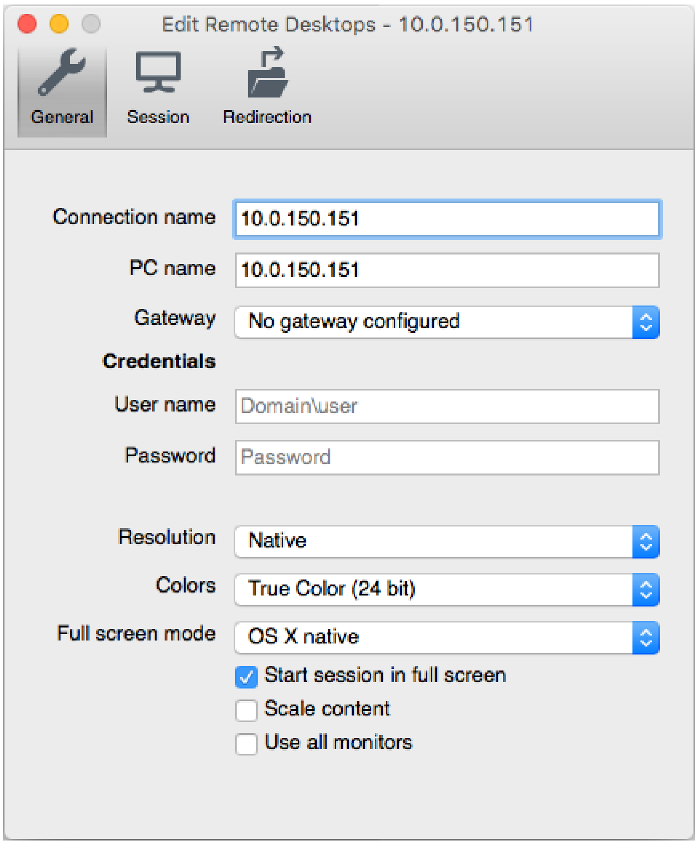
3. Provide essential configuration parameters:

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

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

4.3.3 Establishing an RDP connection with a remote host

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



Connection name: 10.0.150.151

PC name: 10.0.150.151

Gateway: No gateway configured

Credentials

User name: Domain\user

Password: Password

Resolution: Native

Colors: True Color (24 bit)

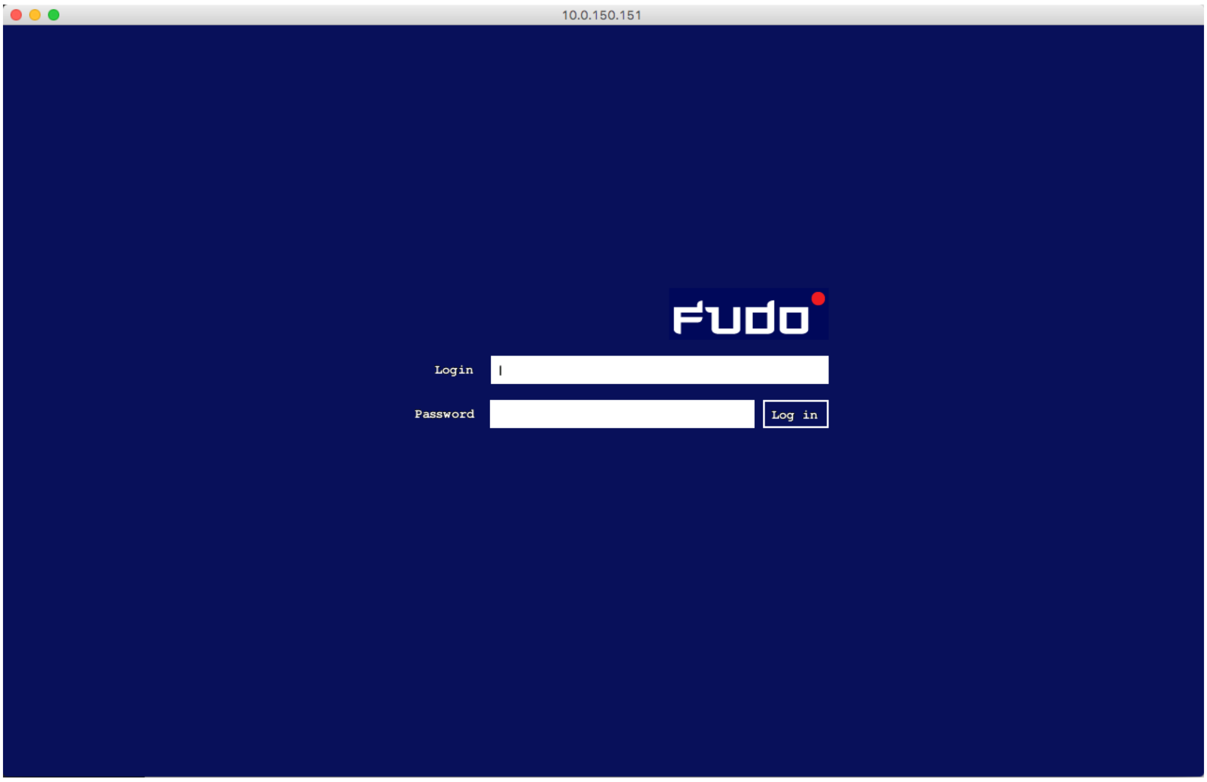
Full screen mode: OS X native

☑ Start session in full screen

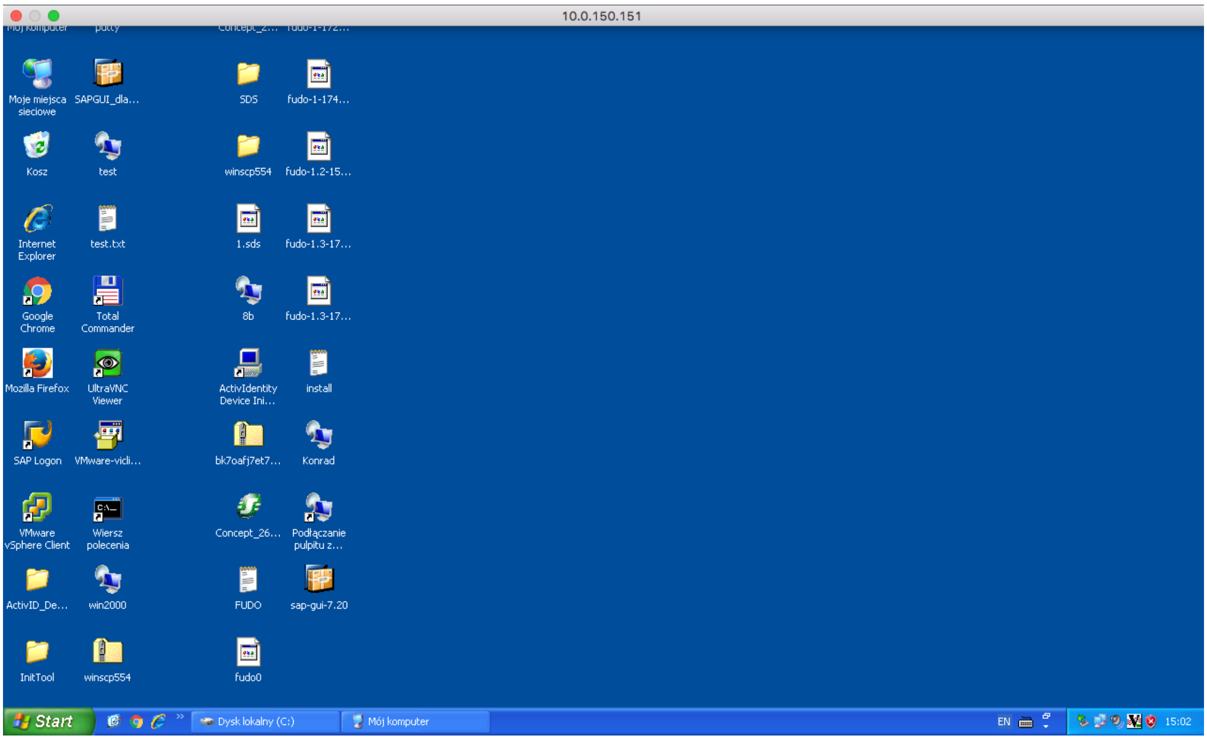
□ Scale content

□ Use all monitors

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

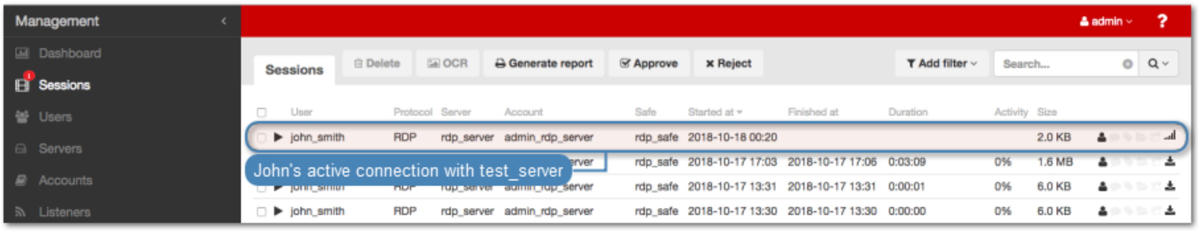


Note: Fudo PAM enables using custom login, no access and session termination screens for RDP and VNC connections. For more information on user defined images for graphical remote sessions, refer to the *Resources* topic.



4.3.4 Viewing user session

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



User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-18 00:20				2.0 KB
			erver	rdp_safe	2018-10-17 17:03	2018-10-17 17:06	0:03:09	0%	1.6 MB
john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 13:31	2018-10-17 13:31	0:00:01	0%	6.0 KB
john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 13:30	2018-10-17 13:30	0:00:00	0%	6.0 KB

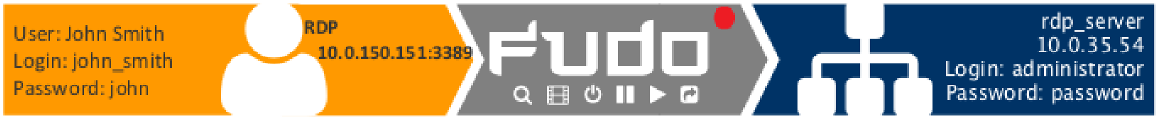
John's active connection with test_server

Related topics:

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

4.4 RDP in bastion mode

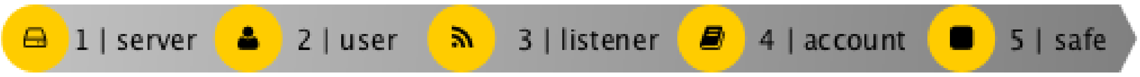
This chapter contains an example of a basic Fudo PAM configuration, to monitor RDP access to a remote server. In this scenario, the user connects to the remote server in bastion mode by specifying the privileged account in the username string. Bastion mode enables facilitating privileged accounts monitoring while preserving default protocols port numbers.



4.4.1 Prerequisites

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

4.4.2 Configuration



Adding a server

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

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

Parameter	Value
Name	`rdp_server`
Description	✗
Blocked	✗
Protocol	`RDP`
Security	`Standard RDP Security`
Bind address	`10.0.150.151`
Permissions	
Granted users	✗
Server addresses	
IP address	`10.0.234.6`
Port	`3389`

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

Adding a user

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

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

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

4. Click *Save*.

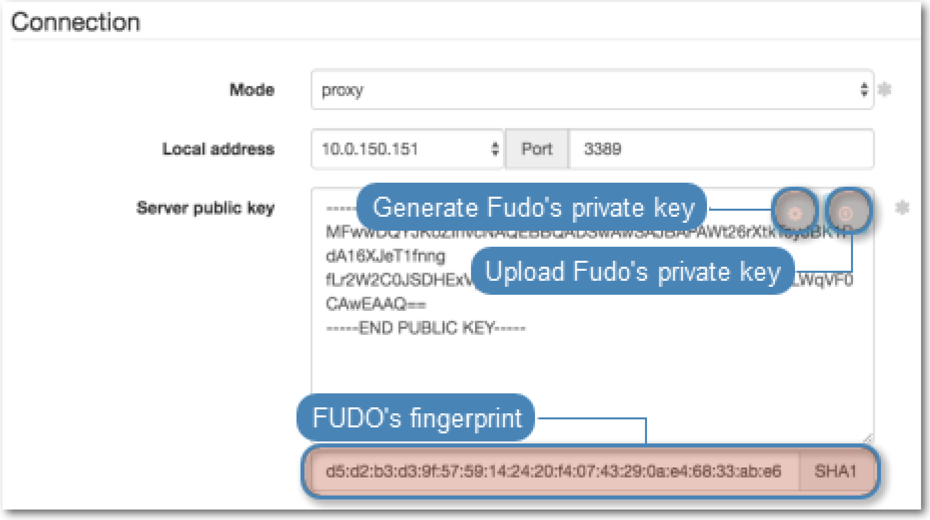
Adding a listener

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

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

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

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



Connection

Mode: proxy

Local address: 10.0.150.151 Port 3389

Server public key:

```
-----
MFwwDQ...AWt26rXtk...
dA16XJeT1fnng
fLr2W2C0JSDHExV...LWqVF0
CAwEAAQ==
-----END PUBLIC KEY-----
```

d5:d2:b3:d3:9f:57:59:14:24:20:f4:07:43:29:0a:e4:68:33: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
General	
Name	`admin_rdp_server`
Blocked	✗
Type	`regular`
Session recording	`all`
OCR sessions	✓
OCR Language	`English`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`rdp_server`
Credentials	
Domain	✗
Login	`administrator`
Replace secret with	`with password`
Password	`password`
Repeat password	`password`
Password change policy	`Static, without restrictions`

4. Click *Save*.

Defining a safe

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

1. Select *Management > Safes*.

2. Click *+ Add*.

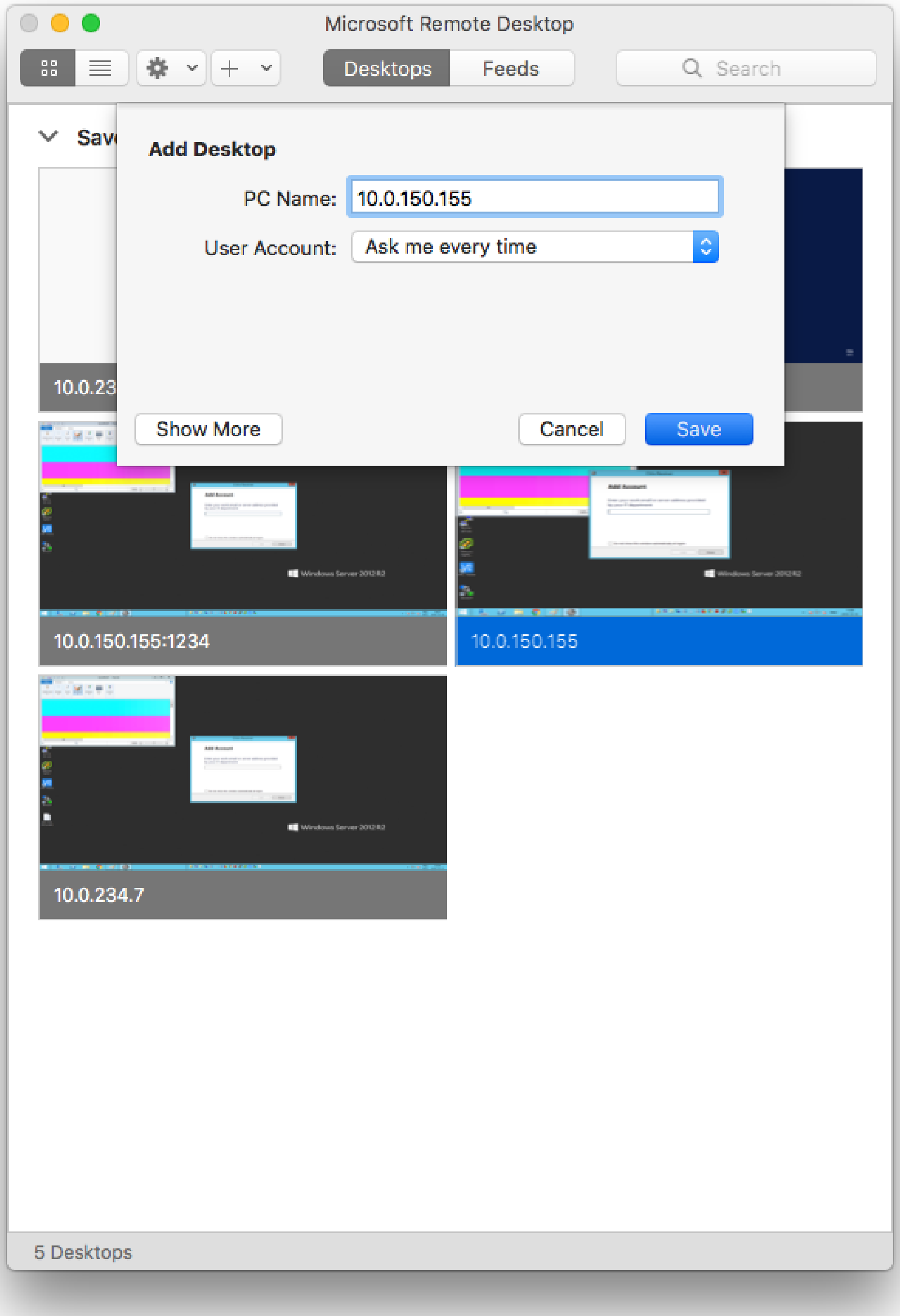
3. Provide essential configuration parameters:

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

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

4.4.3 Establishing an RDP connection with a remote host

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

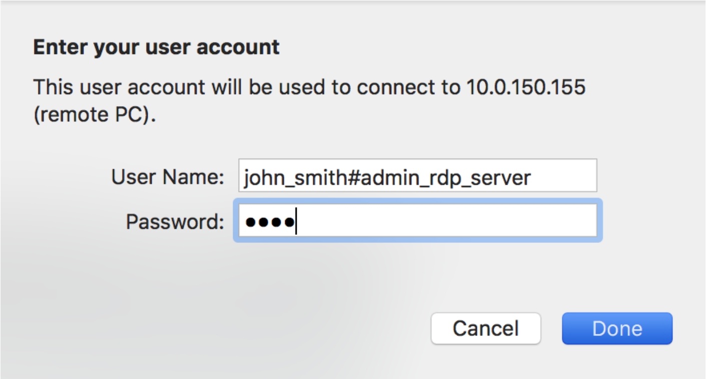


Add Desktop

PC Name: 10.0.150.155

User Account: Ask me every time

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



Enter your user account

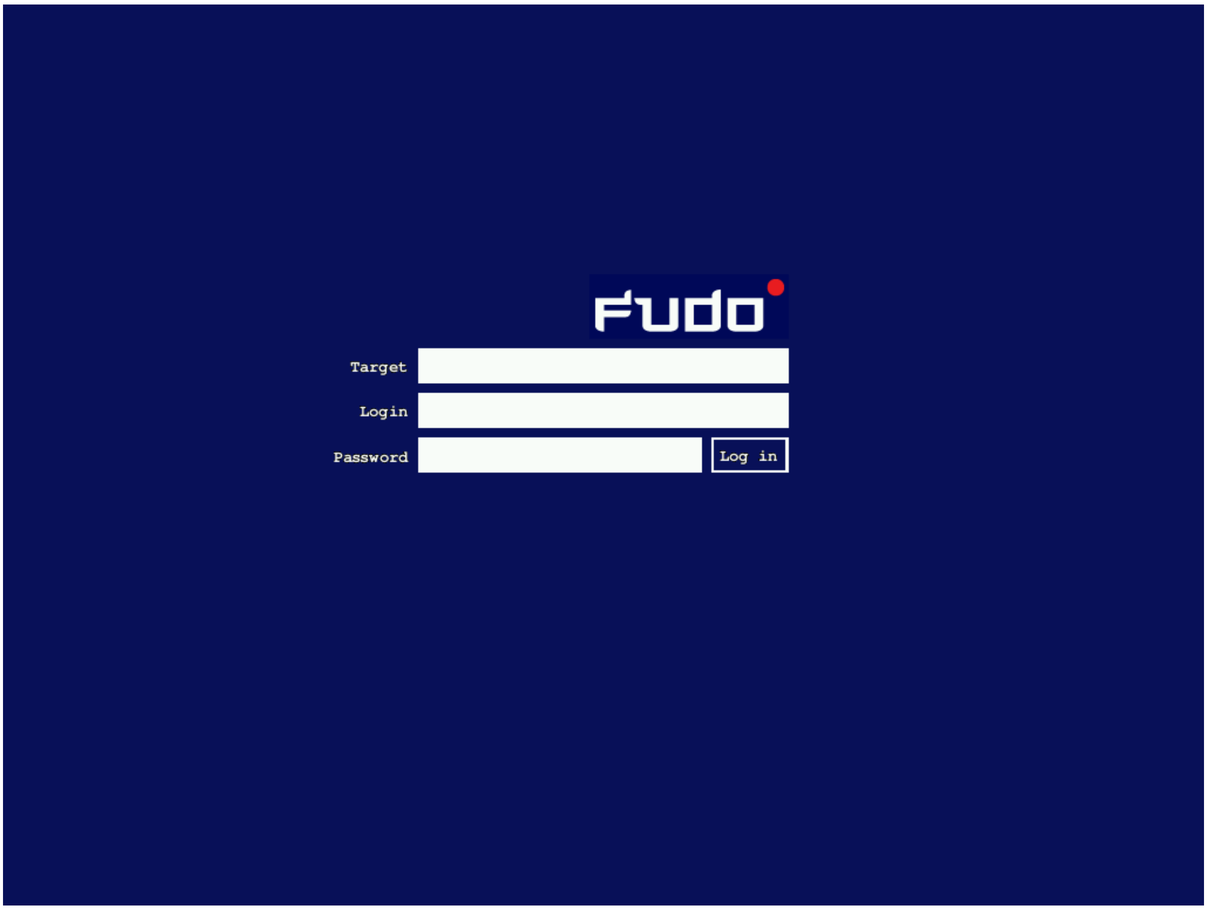
This user account will be used to connect to 10.0.150.155 (remote PC).

User Name: john_smith#admin_rdp_server

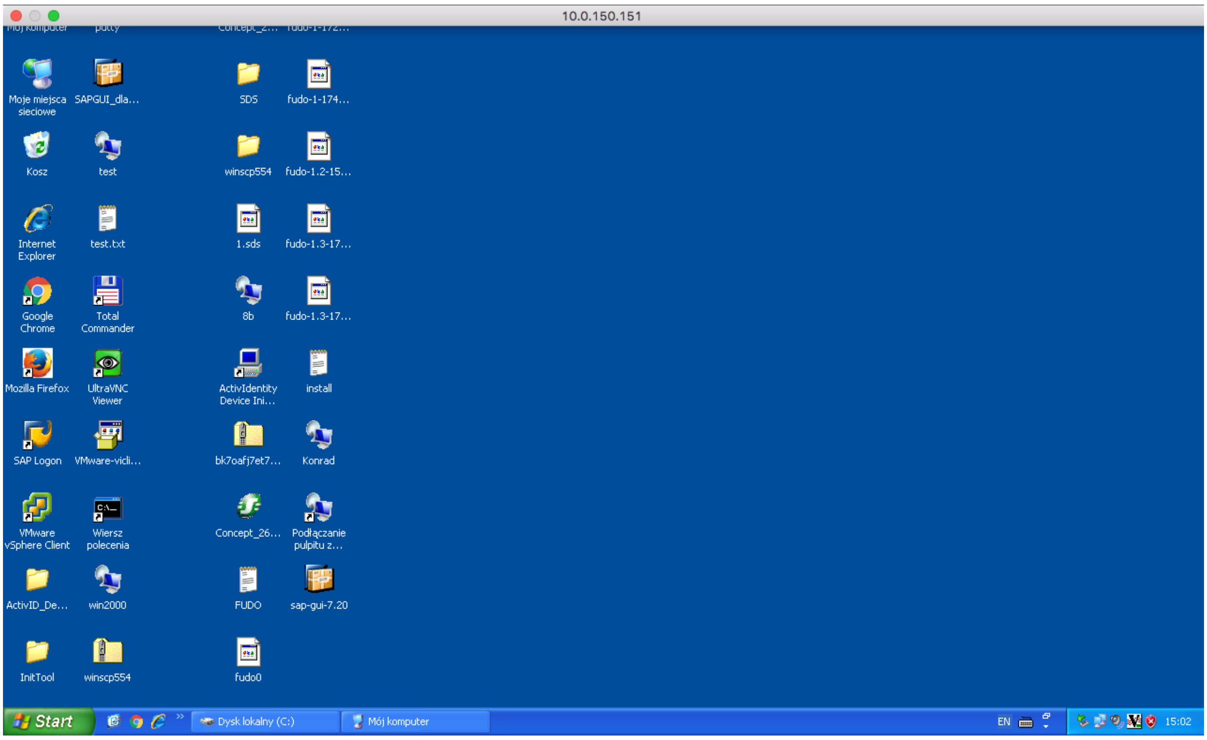
Password: ••••

Note:

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

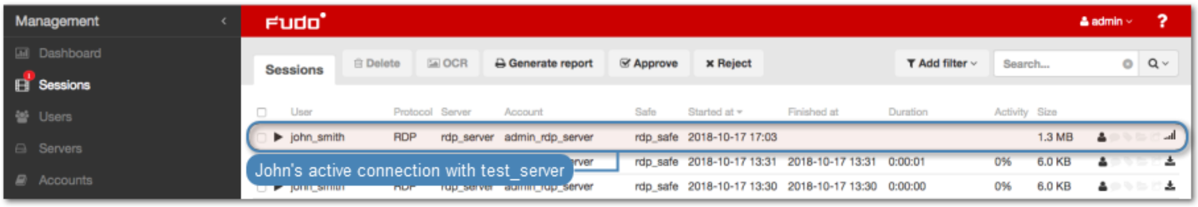


- In case the specified account is not found, Fudo PAM will try to match the name with a server object. If a matching server is not found, system tries to match the string to a host's DNS name.
- Fudo PAM enables using a custom logo on the login screen for RDP and VNC connections. For more information refer to the *Resources* topic.



4.4.4 Viewing user session

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



User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
▶ john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 17:03				1.3 MB
			rver	rdp_safe	2018-10-17 13:31	2018-10-17 13:31	0:00:01	0%	6.0 KB
▶ john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 13:30	2018-10-17 13:30	0:00:00	0%	6.0 KB

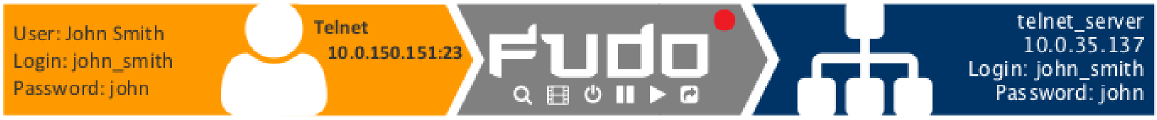
Related topics:

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

4.5 Telnet

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

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



4.5.1 Prerequisites

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

4.5.2 Configuration

1 | server
2 | user
3 | listener
4 | account
5 | safe

Adding a server

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

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

Parameter	Value
General	
Name	`telnet_server`
Description	✗
Blocked	✗
Protocol	`Telnet`
Bind address	`Any`
Use TLS	✗
Permissions	
Granted users	✗
Server addresses	
Address	`10.0.35.137`
Port	`23`

4. Click *Save*.

Adding a user

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

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

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

4. Click *Save*.

Adding a listener

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

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

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

4. Click *Save*.

Adding an account

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

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

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

4. Click *Save*.

Defining a safe

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

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

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

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

4.5.3 Establishing a telnet connection with the remote host

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

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

3. Provide user authentication information defined on Fudo PAM:

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

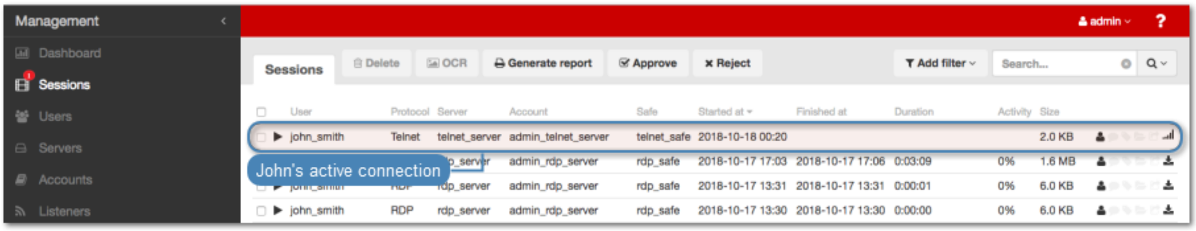
4. Provide user authentication information defined on the target host:

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

Note: Telnet connections do not support user credentials substitution.

4.5.4 Viewing user's session

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



☐	User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
☐	▶ john_smith	Telnet	telnet_server	admin_telnet_server	telnet_safe	2018-10-18 00:20				2.0 KB
☐	[illegible]	[illegible]	p_server	admin_rdp_server	rdp_safe	2018-10-17 17:03	2018-10-17 17:06	0:03:09	0%	1.6 MB
☐	▶ john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 13:31	2018-10-17 13:31	0:00:01	0%	6.0 KB
☐	▶ john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 13:30	2018-10-17 13:30	0:00:00	0%	6.0 KB

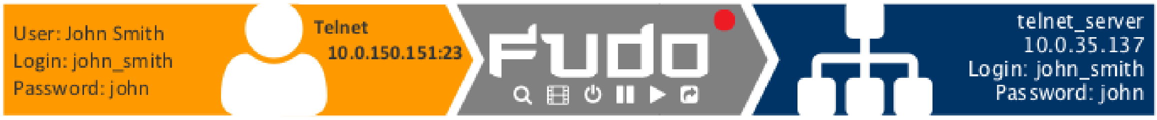
Related topics:

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

4.6 Telnet 5250

This chapter contains an example of a basic Fudo PAM configuration, to monitor Telnet 5250 connections to a remote server. In this scenario, the user connects to the remote server using Telnet client and logs in using individual login and password. Fudo PAM authenticates the user against the information stored in the local database, establishes connection with the remote server and starts recording.

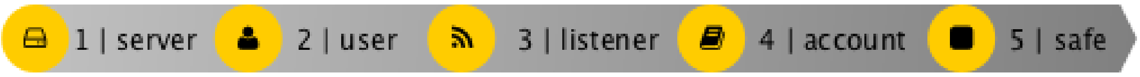
Note: Telnet connections do not support login credentials forwarding and login credentials substitution. When connecting to target host over telnet protocol, users are asked to provide their login credentials twice. First time to authenticate against Fudo PAM and then again, to connect to the target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



4.6.1 Prerequisites

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

4.6.2 Configuration



Adding a server

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

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

Parameter	Value
General	
Name	`telnet_server`
Description	✗
Blocked	✗
Protocol	`Telnet 5250`
Bind address	`Any`
Use TLS	✗
Permissions	
Granted users	✗
Server addresses	
IP Address	`10.0.35.137`
Port	`23`

4. Click *Save*.

Adding a user

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

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

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

4. Click *Save*.

Adding a listener

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

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

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

4. Click *Save*.

Adding an account

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

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

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

4. Click *Save*.

Defining a safe

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

1. Select *Management > Safes*.

2. Click *+ Add*.

3. Provide essential configuration parameters:

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

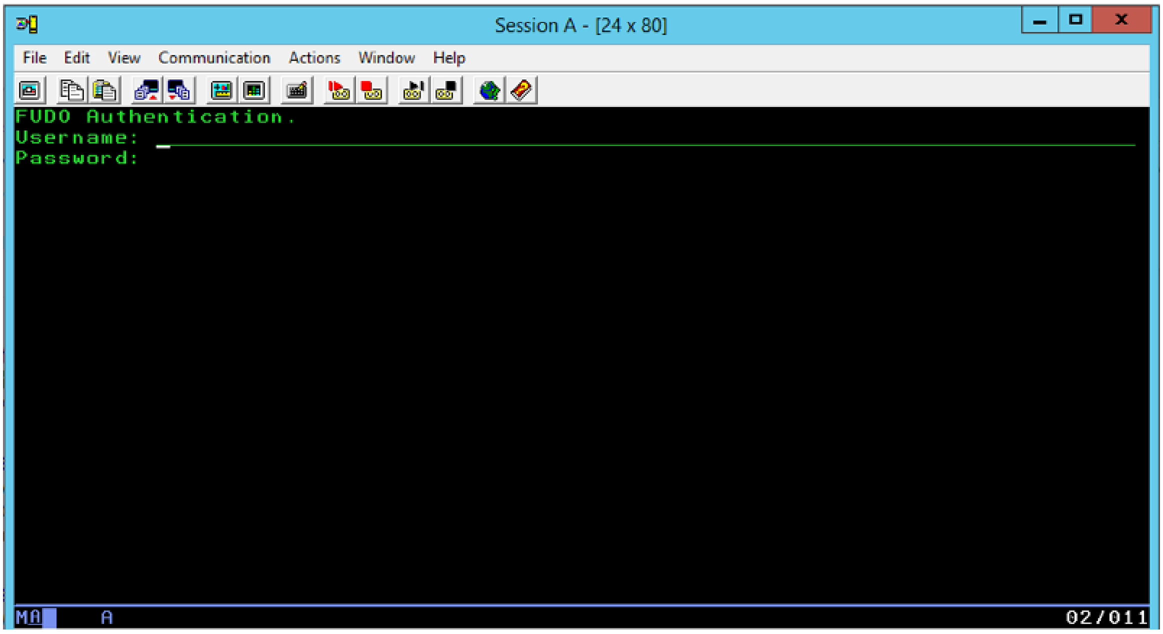
4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_telnet_server` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `telnet_listener` object and click +.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

4.6.3 Establishing a telnet connection with the remote host

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

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

3. Provide user authentication information defined on Fudo PAM:

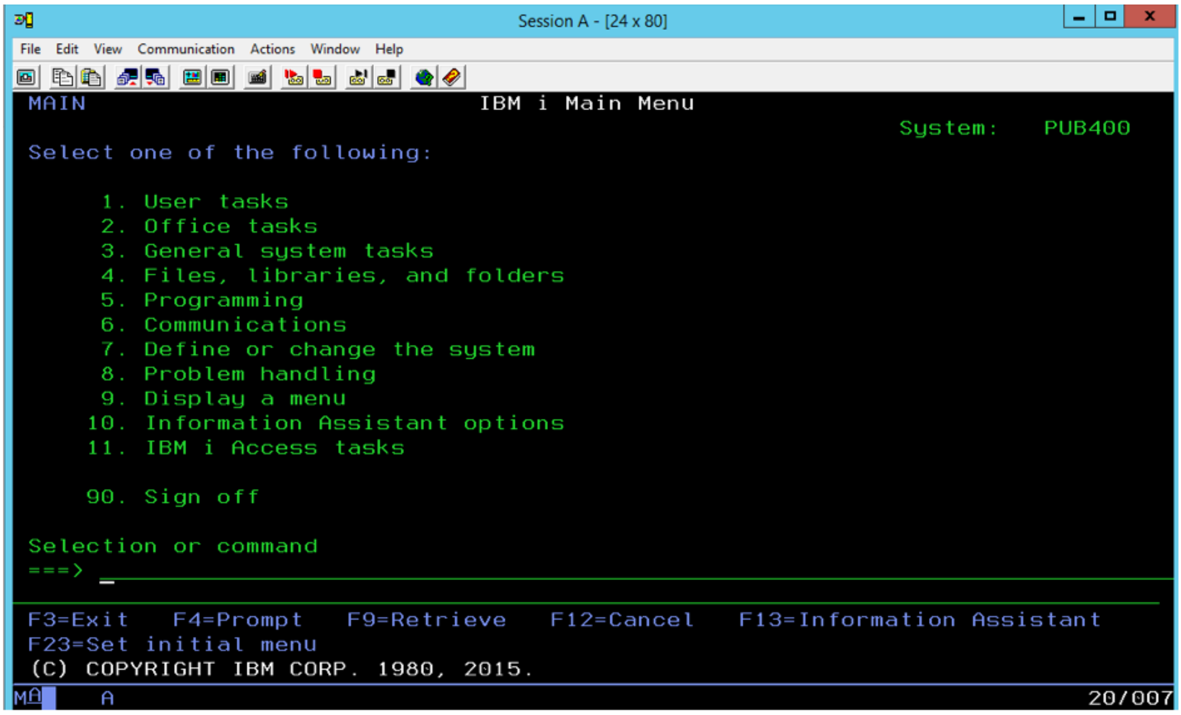


```
FUDO Authentication.
Username: _
Password:
MA      A                                                              02/011
```

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

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

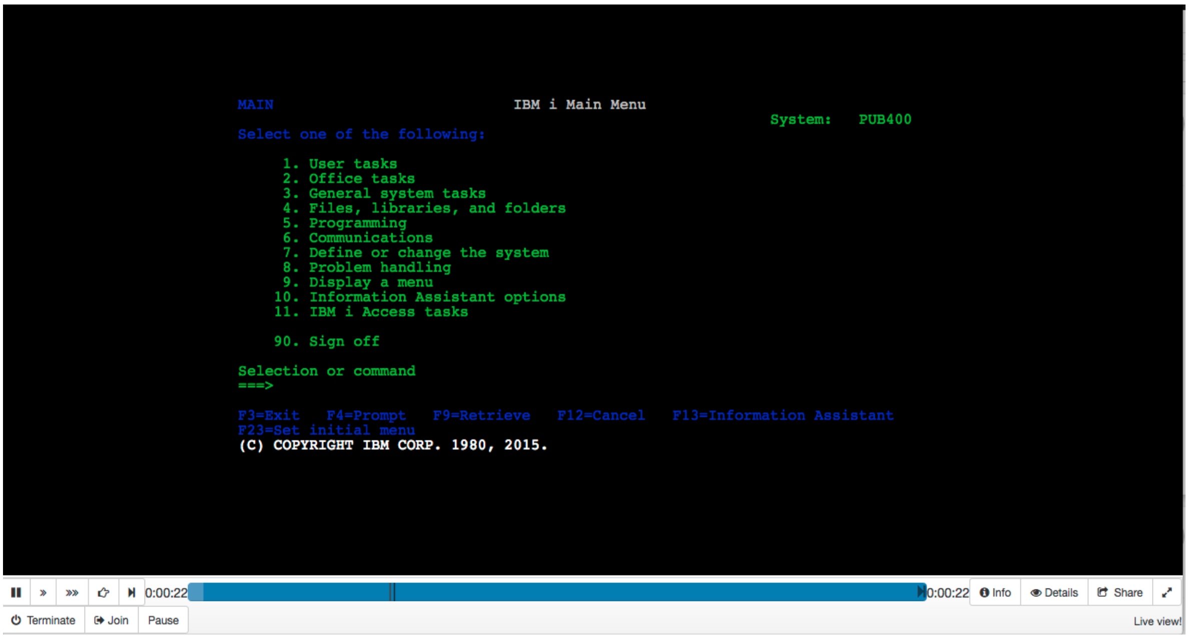
Note: Telnet connections do not support user credentials substitution.



```
MAIN                           IBM i Main Menu
                                                             System:   PUB400
Select one of the following:

     1. User tasks
     2. Office tasks
     3. General system tasks
     4. Files, libraries, and folders
     5. Programming
     6. Communications
     7. Define or change the system
     8. Problem handling
     9. Display a menu
    10. Information Assistant options
    11. IBM i Access tasks

    90. Sign off

Selection or command
===> _

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2015.
MA    A                                                                20/007
```

4.6.4 Viewing user's session

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



```
MAIN                           IBM i Main Menu
                                                             System:   PUB400
Select one of the following:

     1. User tasks
     2. Office tasks
     3. General system tasks
     4. Files, libraries, and folders
     5. Programming
     6. Communications
     7. Define or change the system
     8. Problem handling
     9. Display a menu
    10. Information Assistant options
    11. IBM i Access tasks

    90. Sign off

Selection or command
===>

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

Related topics:

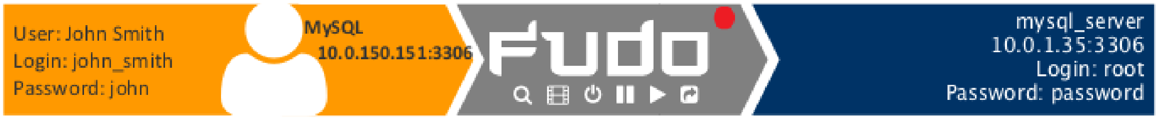
- *Quick start - SSH connection configuration*

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

4.7 MySQL

This chapter contains an example of a basic 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, Fudo PAM substitutes the login and the password with the previously defined values: `root`/`password` (authorization modes are described in the *User authorization modes* section).



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

4.7.1 Prerequisites

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

4.7.2 Configuration

1 | server
2 | user
3 | listener
4 | account
5 | safe

Adding a server

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

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

Parameter	Value
General	
Name	`mysql_server`
Description	❌
Blocked	❌
Protocol	`MySQL`
Bind address	`Any`
Permissions	
Granted users	❌
Server addresses	
IP address	`10.0.1.35`
Port	`3306`

4. Click *Save*.

Adding a user

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

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

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

4. Click *Save*.

Adding a listener

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

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

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

4. Click *Save*.

Adding an account

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

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

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

4. Click *Save*.

Defining a safe

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

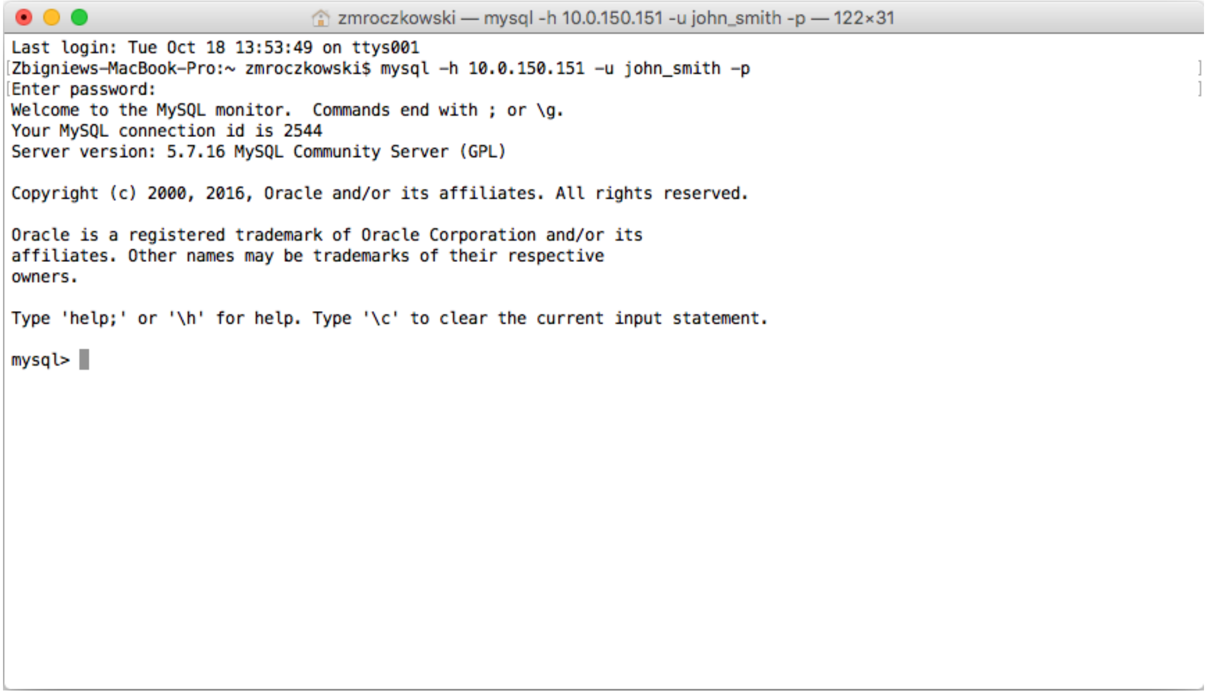
1. Select *Management > Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

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

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

4.7.3 Establishing connection with a MySQL database

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



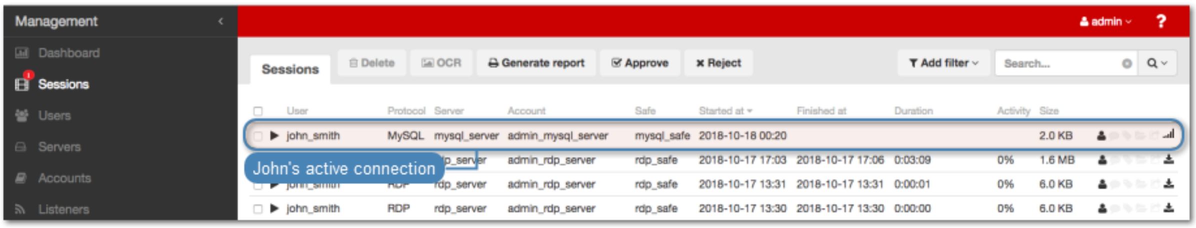
zmroczkowski — mysql -h 10.0.150.151 -u john_smith -p — 122×31

```
Last login: Tue Oct 18 13:53:49 on ttys001
Zbigniews-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> 
```

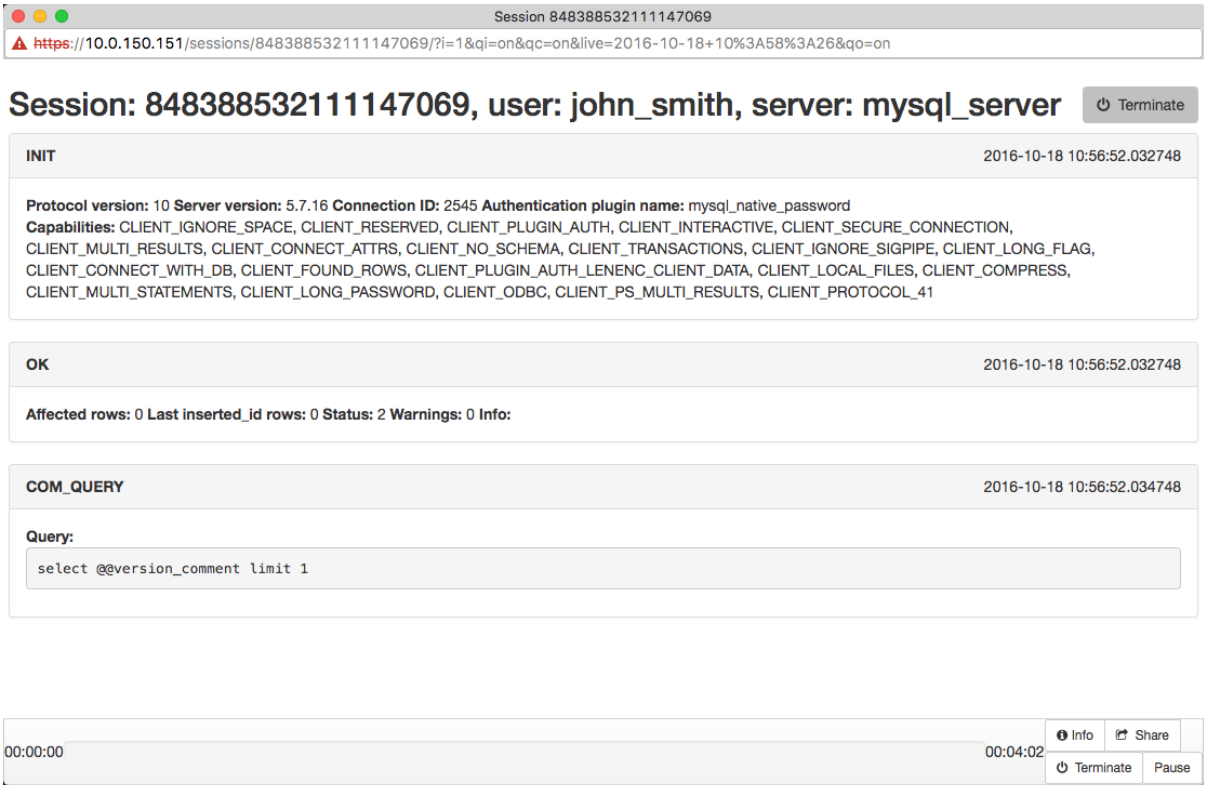
4. Continue browsing the database contents using SQL queries.

4.7.4 Viewing user session

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



User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
john_smith	MySQL	mysql_server	admin_mysql_server	mysql_safe	2018-10-18 00:20				2.0 KB
[illegible]	[illegible]	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 17:03	2018-10-17 17:06	0:03:09	0%	1.6 MB
john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 13:31	2018-10-17 13:31	0:00:01	0%	6.0 KB
john_smith	RDP	rdp_server	admin_rdp_server	rdp_safe	2018-10-17 13:30	2018-10-17 13:30	0:00:00	0%	6.0 KB



Session 848388532111147069

https://10.0.150.151/sessions/848388532111147069/?i=1&qi=on&qc=on&live=2016-10-18+10%3A58%3A26&qo=on

Session: 848388532111147069, user: john_smith, server: mysql_server

INIT 2016-10-18 10:56:52.032748

Protocol version: 10 **Server version:** 5.7.16 **Connection ID:** 2545 **Authentication plugin name:** mysql_native_password
Capabilities: CLIENT_IGNORE_SPACE, CLIENT_RESERVED, CLIENT_PLUGIN_AUTH, CLIENT_INTERACTIVE, CLIENT_SECURE_CONNECTION, CLIENT_MULTI_RESULTS, CLIENT_CONNECT_ATTRS, CLIENT_NO_SCHEMA, CLIENT_TRANSACTIONS, CLIENT_IGNORE_SIGPIPE, CLIENT_LONG_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

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

Query:

```
select @@version_comment limit 1
```

00:00:00 00:04:02

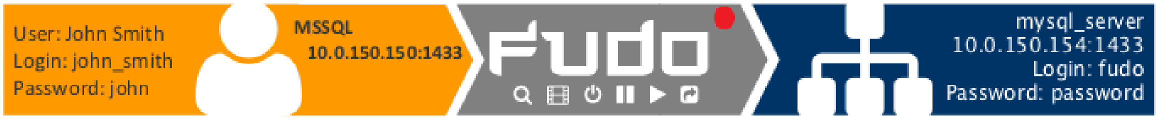
Related topics:

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

4.8 MS SQL

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

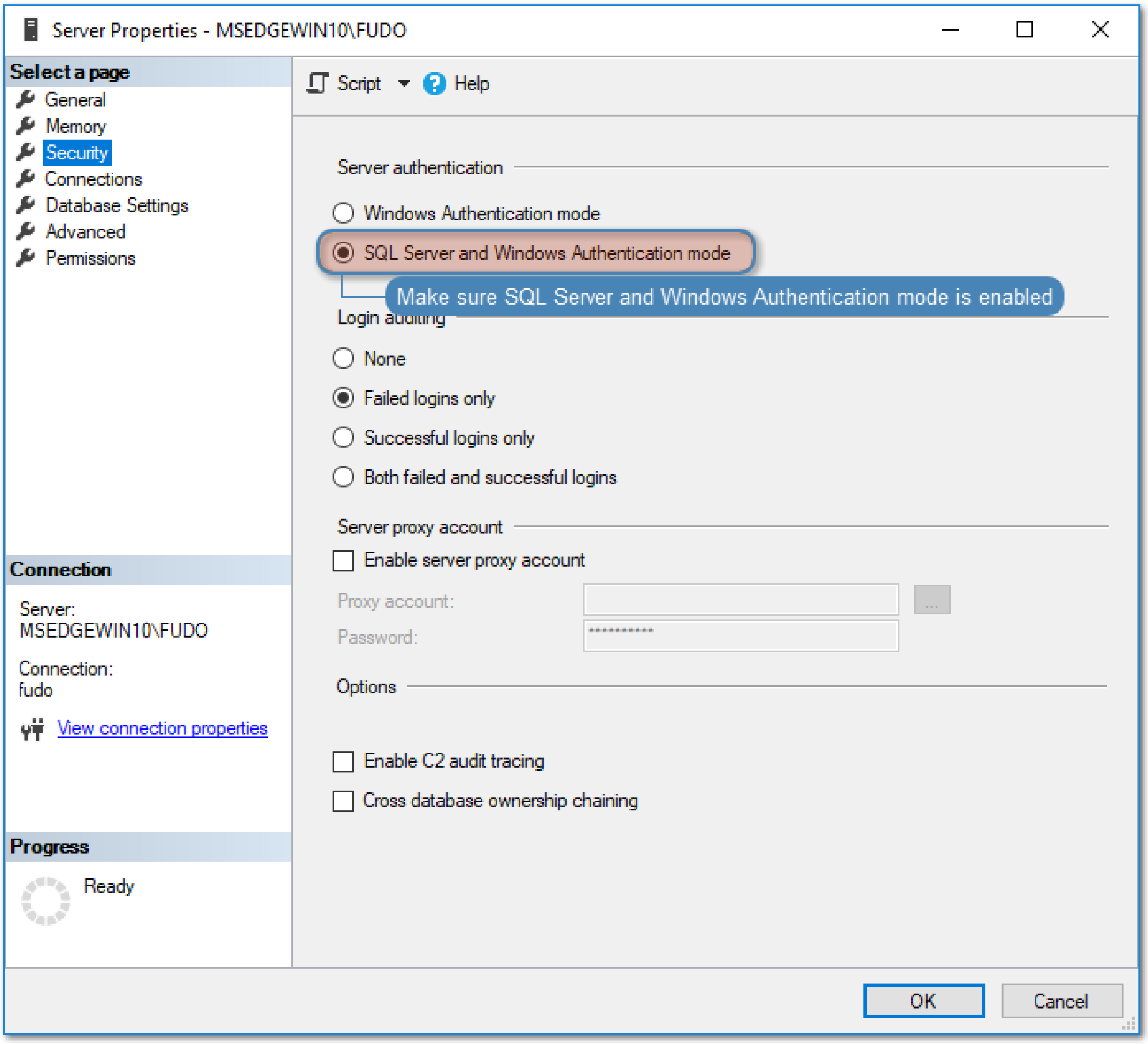
In this scenario, the user connects to a MS SQL database using individual login and password using *SQL Server Management Studio*. When establishing the connection with the remote server, Fudo PAM substitutes the login and the password with the previously defined values: fudo/password (authorization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



4.8.1 Prerequisites

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

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



Server Properties - MSEDGEWIN10\FUDO

Select a page: General, Memory, Security, Connections, Database Settings, Advanced, Permissions

Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Make sure SQL Server and Windows Authentication mode is enabled

Login auditing

○ None

● Failed logins only

○ Successful logins only

○ Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: ***********

Options

□ Enable C2 audit tracing

□ Cross database ownership chaining

Connection

Server: MSEDGEWIN10\FUDO

Connection: fudo

Progress

Ready

4.8.2 Configuration

1 | server
2 | user
3 | listener
4 | account
5 | safe

Adding a server

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

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

Parameter	Value
General	
Name	`mssql_server`
Description	✗
Blocked	✗
Protocol	`MS SQL (TDS)`
Bind address	`Any`
Permissions	
Granted users	✗
Server addresses	
IP address	`10.0.150.154`
Port	`1433`

4. Click *Save*.

Adding a user

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

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

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

4. Click *Save*.

Adding a listener

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

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

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

4. Click *Save*.

Adding an account

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

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

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

4. Click *Save*.

Defining a safe

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

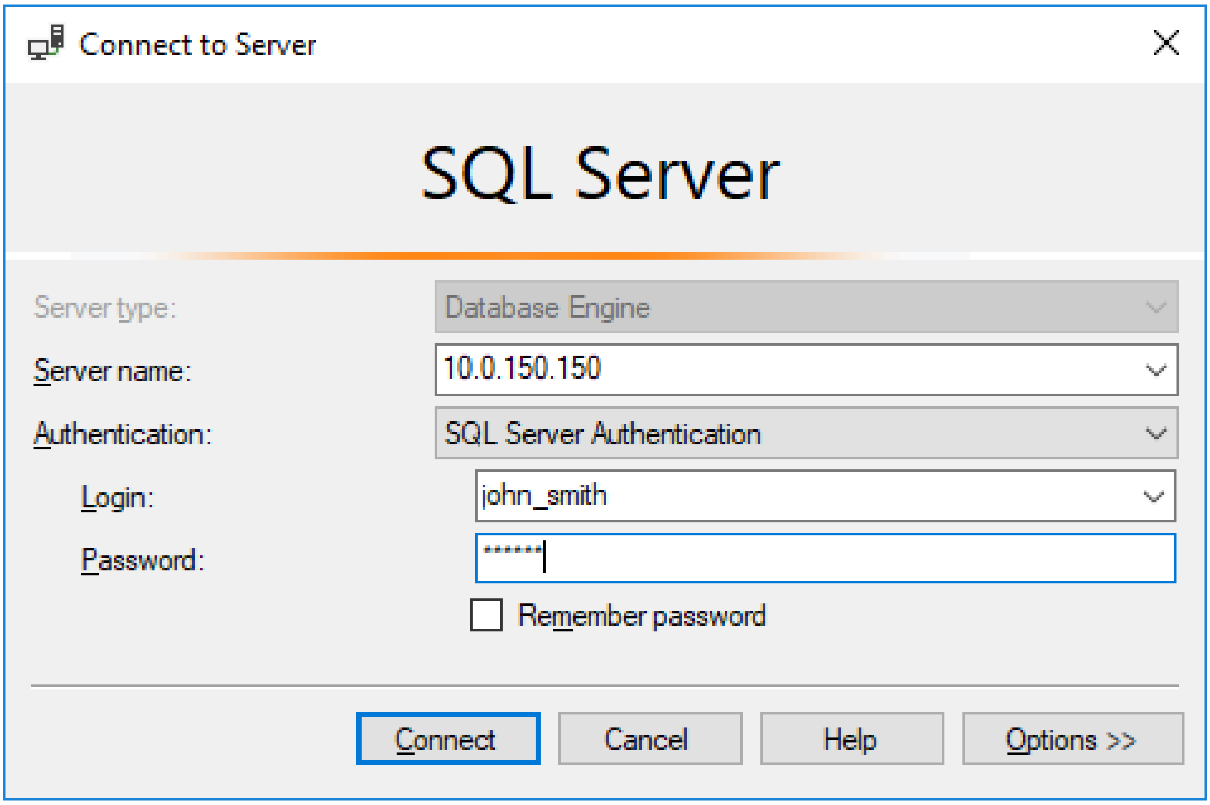
1. Select *Management > Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

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

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

4.8.3 Establishing connection with a MS SQL database

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



Server type: Database Engine

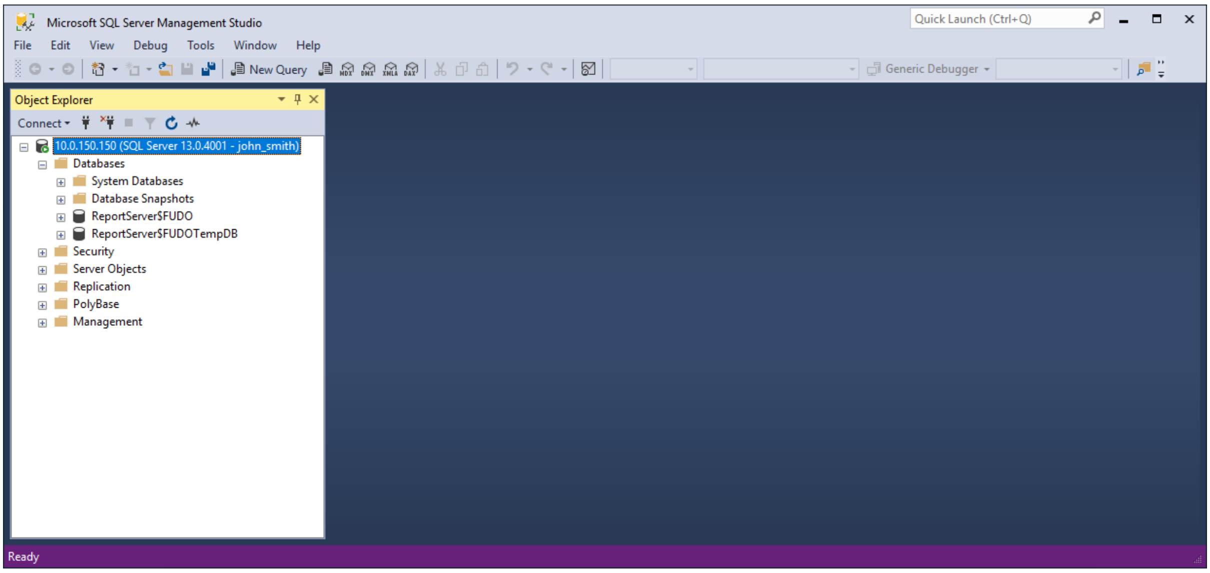
Server name: 10.0.150.150

Authentication: SQL Server Authentication

Login: john_smith

Password: ******

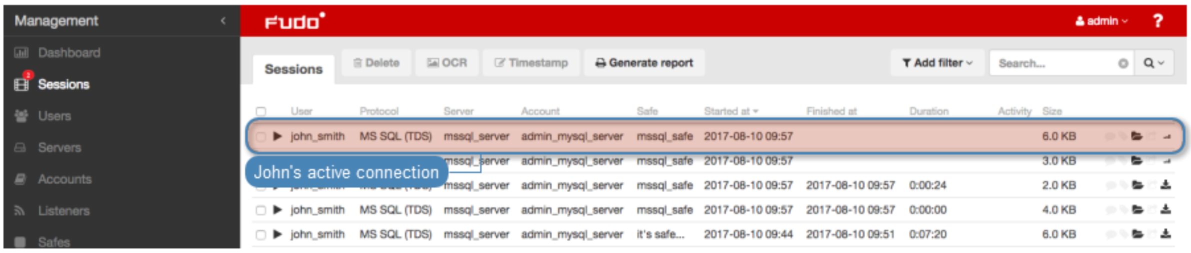
□ Remember password



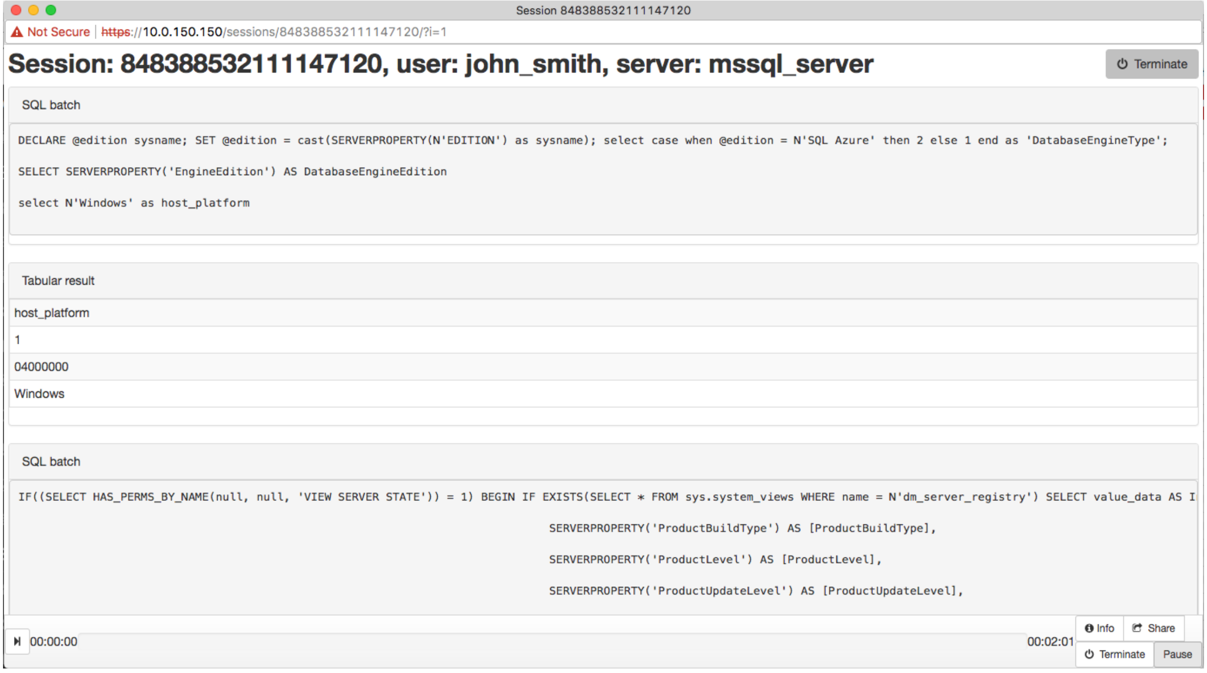
10.0.150.150 (SQL Server 13.0.4001 - john_smith)

4.8.4 Viewing user session

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



User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
john_smith	MS SQL (TDS)	mssql_server	admin_mysql_server	mssql_safe	2017-08-10 09:57				6.0 KB
		mssql_server	admin_mysql_server	mssql_safe	2017-08-10 09:57				3.0 KB
		mssql_server	admin_mysql_server	mssql_safe	2017-08-10 09:57	2017-08-10 09:57	0:00:24		2.0 KB
john_smith	MS SQL (TDS)	mssql_server	admin_mysql_server	mssql_safe	2017-08-10 09:57	2017-08-10 09:57	0:00:00		4.0 KB
john_smith	MS SQL (TDS)	mssql_server	admin_mysql_server	it's safe...	2017-08-10 09:44	2017-08-10 09:51	0:07:20		6.0 KB


Session 848388532111147120
Not Secure | https://10.0.150.150/sessions/848388532111147120/?i=1
Terminate
00:00:00
00:02:01
Info
Share
Terminate
Pause

Session: 848388532111147120, user: john_smith, server: mssql_server

SQL batch

```
DECLARE @edition sysname; SET @edition = cast(SERVERPROPERTY(N'EDITION') as sysname); select case when @edition = N'SQL Azure' then 2 else 1 end as 'DatabaseEngineType';

SELECT SERVERPROPERTY('EngineEdition') AS DatabaseEngineEdition

select N'Windows' as host_platform
```

Tabular result

host_platform
1
04000000
Windows

SQL batch

```
IF((SELECT HAS_PERMS_BY_NAME(null, null, 'VIEW SERVER STATE')) = 1) BEGIN IF EXISTS(SELECT * FROM sys.system_views WHERE name = N'dm_server_registry') SELECT value_data AS I
                                                    SERVERPROPERTY('ProductBuildType') AS [ProductBuildType],
                                                    SERVERPROPERTY('ProductLevel') AS [ProductLevel],
                                                    SERVERPROPERTY('ProductUpdateLevel') AS [ProductUpdateLevel],
```

Related topics:

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

4.9 HTTP

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

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

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

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

4.9.1 Prerequisites

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

4.9.2 Configuration

1 | server
2 | user
3 | listener
4 | account
5 | safe

Adding a server

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

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

Parameter	Value
General	
Name	`twitter`
Description	✗
Blocked	✗
Protocol	`HTTP`
HTTP timeout	`900`
Bind address	`10.0.236.70`
Use TLS	✓
Legacy ciphers	✗
Use root store certificates	✓
CA certificate	Click ⊕ to upload CA certificate.
Permissions	
Granted users	✗
Server addresses	
Address	`twitter.com`
Port	`443`
Server certificate	Click ⊕ to fetch a server's certificate.
HTTP host	✗
Authentication method	`Twitter`

4. Click *Save*.

Adding a user

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

1. Select *Management > Users*.

2. Click *+ Add*.

3. Provide essential user information:

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

4. Click *Save*.

Adding a listener

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

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

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

4. Click *Save*.

Adding an account

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

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

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

4. Click *Save*.

Defining a safe

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

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

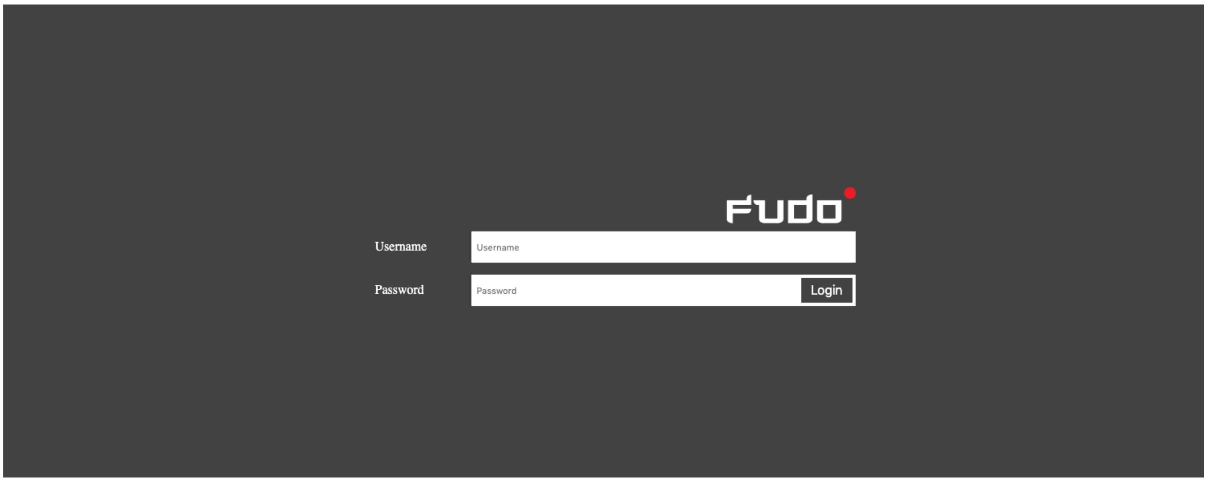
Parameter	Value
General	
Name	`twitter_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Users	`john_smith`
Protocol functionality	
RDP	✗
SSH	✗
VNC	✗

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

4.9.3 Connecting to remote resource

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

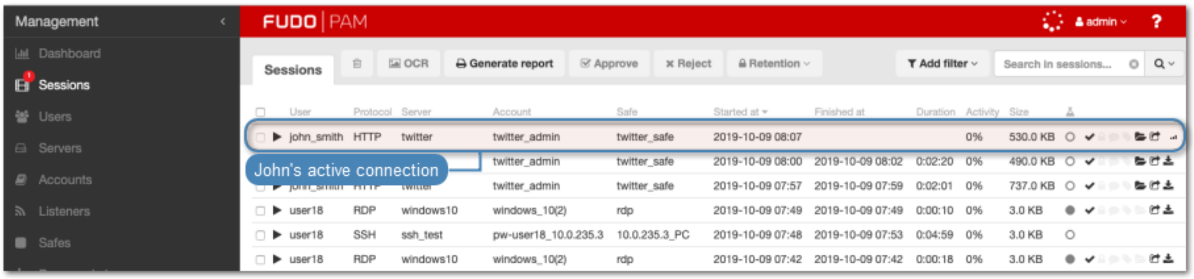
Note: In case you are authenticating using two factors, input your static password along with the dynamic factor (token value) in the password field as a single string of characters.



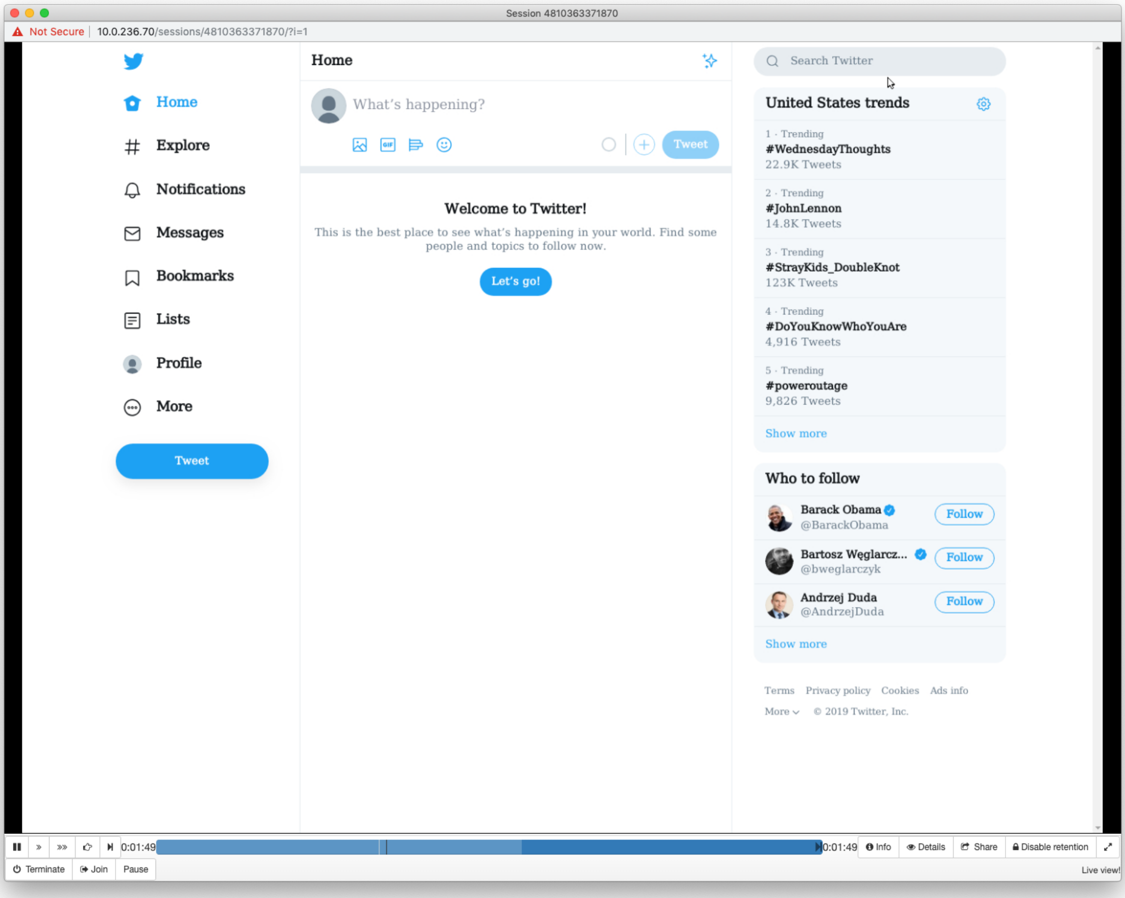
4. Continue browsing the website.

4.9.4 Viewing user session

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



☐	User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
☐	john_smith	HTTP	twitter	twitter_admin	twitter_safe	2019-10-09 08:07			0%	530.0 KB
				twitter_admin	twitter_safe	2019-10-09 08:00	2019-10-09 08:02	0:02:20	0%	490.0 KB
☐	john_smith	HTTP	twitter	twitter_admin	twitter_safe	2019-10-09 07:57	2019-10-09 07:59	0:02:01	0%	737.0 KB
☐	user18	RDP	windows10	windows_10(2)	rdp	2019-10-09 07:49	2019-10-09 07:49	0:00:10	0%	3.0 KB
☐	user18	SSH	ssh_test	pw-user18_10.0.235.3	10.0.235.3_PC	2019-10-09 07:48	2019-10-09 07:53	0:04:59	0%	3.0 KB
☐	user18	RDP	windows10	windows_10(2)	rdp	2019-10-09 07:42	2019-10-09 07:42	0:00:18	0%	3.0 KB



Welcome to Twitter!

This is the best place to see what's happening in your world. Find some people and topics to follow now.

Let's go!

Related topics:

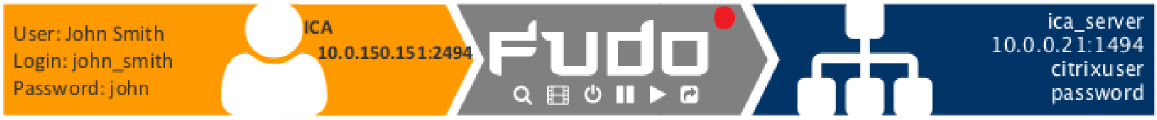
- *Requirements*
- *HTTP protocol*
- *Data model*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - Telnet connection configuration*

4.10 Citrix

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

4.10.1 ICA

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



4.10.1.1 Prerequisites

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

4.10.1.2 Configuration

1 | server
2 | user
3 | listener
4 | account
5 | safe

Adding a server

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

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

Parameter	Value
General	
Name	`ica_server`
Description	✗
Blocked	✗
Protocol	`ICA`
Bind address	`Any`
Use TLS	✗
Permissions	
Granted users	✗
Server addresses	
IP address	`10.0.0.21`
Port	`1494`

4. Click *Save*.

Adding a listener

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

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

Parameter	Value
General	
Name	`ica_listener`
Blocked	✗
Protocol	`ICA`
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.151`
Port	`2494`
Use TLS	✗

4. Click *Save*.

Adding an account

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

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

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

4. Click *Save*.

Adding a user

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

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

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

4. Click *Save*.

Defining a safe

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

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

Parameter	Value
General	
Name	`ica_safe`
Blocked	❌
Notifications	❌
Login reason	❌
Require approval	❌
Policies	❌
Note access	`No access`
Protocol functionality	
RDP	❌
SSH	❌
VNC	❌
Accounts	
`admin_ica_server`	`ica_listener`

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

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

4.10.1.3 Creating `.ica` file with connection parameters

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

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

1. Create configuration file containing the following:

```
[ApplicationServers]
ica_connection_example=

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

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

4.10.1.4 Connecting to remote resource

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

4.10.1.5 Viewing user session

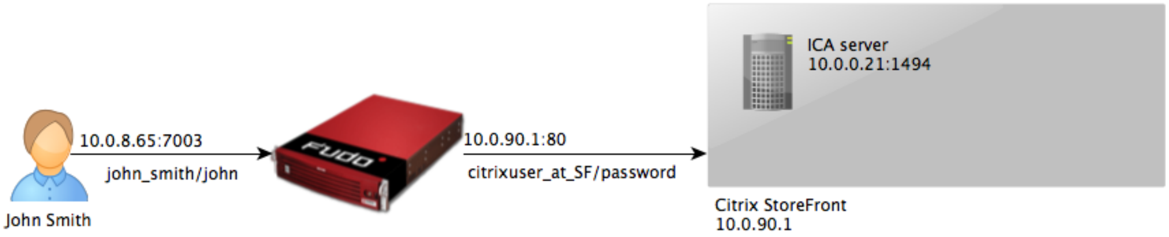
1. Open a web browser and go to the Fudo PAM administration page.
2. Enter user login and password to log in to Fudo PAM administration panel.
3. Select *Management > Sessions*.
4. Find *John Smith's* session and click the playback icon.

Related topics:

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

4.10.2 ICA via Citrix StoreFront

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



4.10.2.1 Prerequisites

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

4.10.2.2 Configuration

1 | server
2 | user
3 | listener
4 | account
5 | safe

Adding an ICA server

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

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

Parameter	Value
General	
Name	`ica_server`
Description	✗
Blocked	✗
Protocol	`ICA`
Bind IP	`Any`
Use TLS	✗
Permissions	
Granted users	✗
Server addresses	
Address	`10.0.0.21`
Port	`1494`

4. Click *Save*.

Adding an ICA listener

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

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

Parameter	Value
General	
Name	`ica_listener`
Blocked	✗
Protocol	`ICA`
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.151`
Port	`2494`
Use TLS	✗

4. Click *Save*.

Adding an account for the ICA server

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

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

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

4. Click *Save*.

Adding a Citrix StoreFront server

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

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

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

4. Click *Save*.

Adding a Citrix StoreFront listener

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

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

Parameter	Value
General	
Name	`citrix_storefront_listener`
Blocked	✗
Protocol	`Citrix StoreFront (HTTP)`
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.8.65`
Port	`7003`
External address	✗
External port	✗
Use TLS	✗

4. Click *Save*.

Adding an account for the Citrix StoreFront server

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

1. Select *Management > Accounts*.

2. Click *+ Add*.

3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`citrixuser_at_SF`
Blocked	✗
Type	`regular`
Session recording	`all`
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`citrix_storefront`
Credentials	
Domain	`tech.whl`
Login	`citrixuser`
Replace secret with	`password`
Password	`password`
Repeat password	`password`
Password change policy	`Static, without restrictions`

Adding a user

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

1. Select *Management > Users*.

2. Click *+ Add*.

3. Provide essential user information:

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

4. Click *Save*.

Defining a safe

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

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

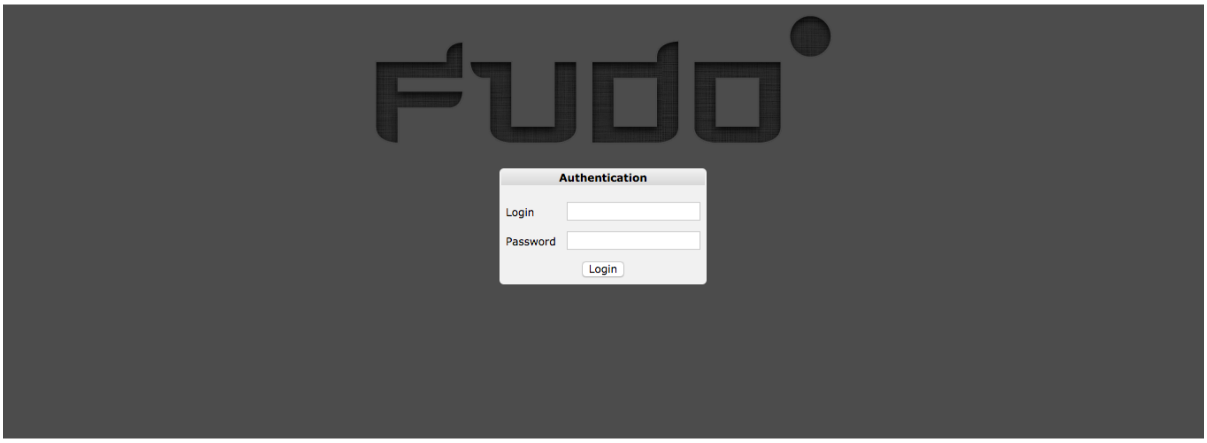
Parameter	Value
General	
Name	`ica_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✗
VNC	✗
Accounts	
`citrixuser_at_SF`	`citrix_storefront_listener`
`ICA_forward`	`ica_listener`

4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `citrixuser_at_SF` object and click +.
11. Find the `ICA_forward` object and click +.
12. Click *OK*.
13. Click ✎ in the *Listeners* column, in the `citrixuser_at_SF` account row.
14. Find the `citrix_storefront_listener` object and click +.
15. Click *OK*.
16. Click ✎ in the *Listeners* column, in the `ICA_forward` account row.
17. Find the `ica_listener` object and click +.
18. Click *OK*.
19. Click *Save*.

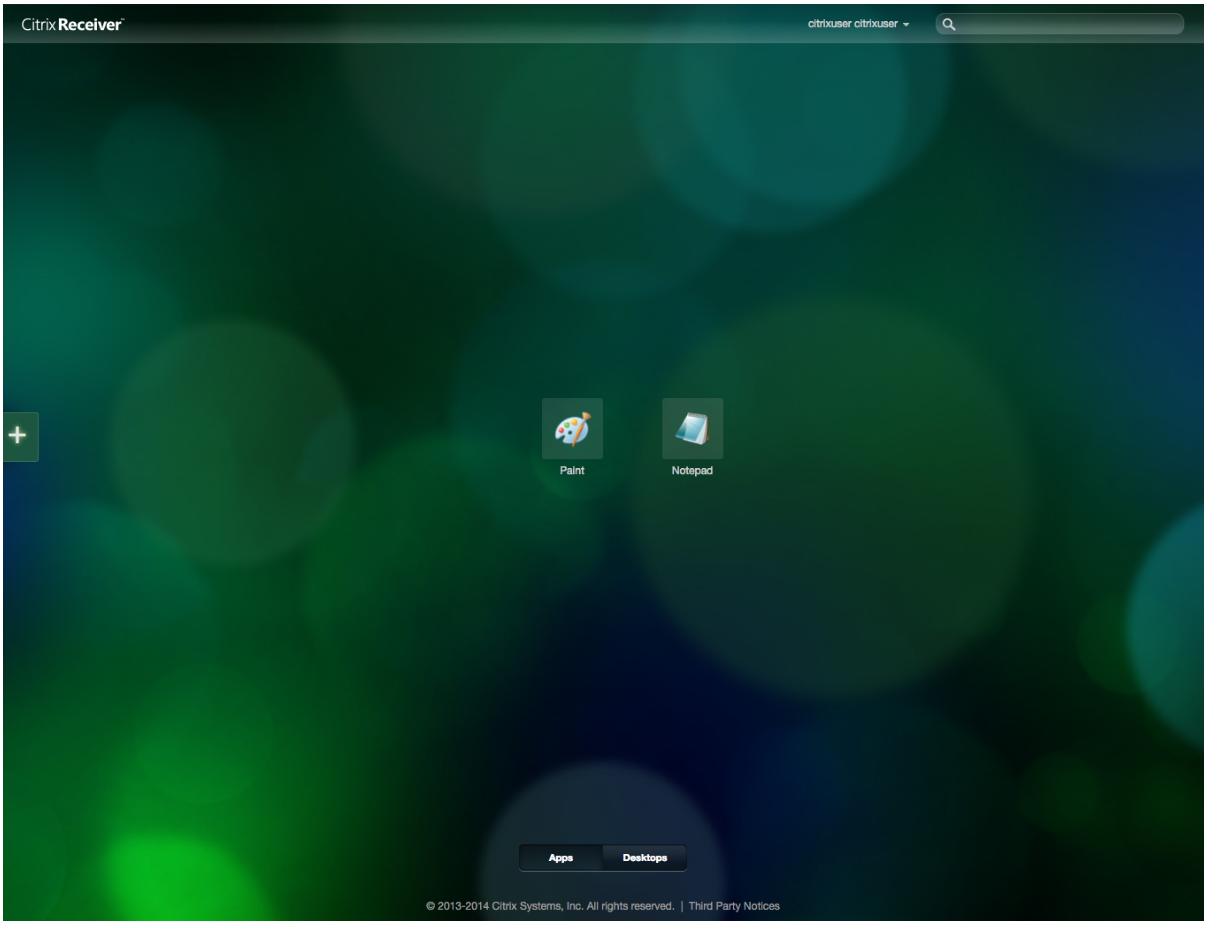
4.10.2.3 Connecting to remote resource

1. Navigate your web browser to the `10.0.8.65:7003` web address.

2. Enter user login and password to log in into the Citrix StoreFront interface.



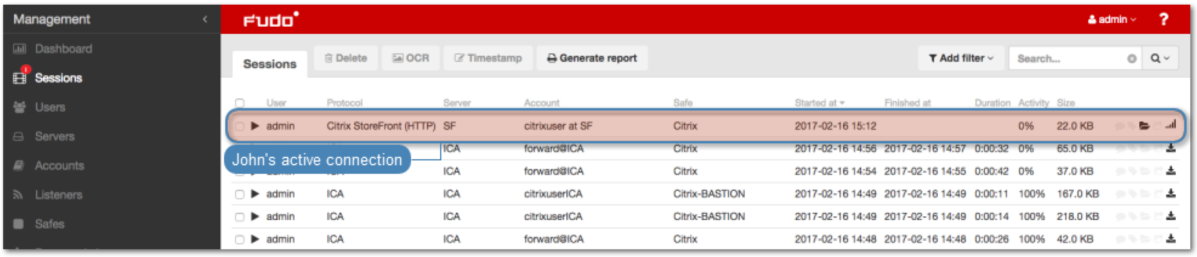
3. Click desired element to establish ICA connection with selected resource.



Citrix Receiver
citrixuser citrixuser
Paint
Notepad
Apps
Desktops
© 2013-2014 Citrix Systems, Inc. All rights reserved. | Third Party Notices

4.10.2.4 Viewing user session

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



User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
admin	Citrix StoreFront (HTTP)	SF	citrixuser at SF	Citrix	2017-02-16 15:12			0%	22.0 KB
		ICA	forward@ICA	Citrix	2017-02-16 14:56	2017-02-16 14:57	0:00:32	0%	65.0 KB
		ICA	forward@ICA	Citrix	2017-02-16 14:54	2017-02-16 14:55	0:00:42	0%	37.0 KB
admin	ICA	ICA	citrixuserICA	Citrix-BASTION	2017-02-16 14:49	2017-02-16 14:49	0:00:11	100%	167.0 KB
admin	ICA	ICA	citrixuserICA	Citrix-BASTION	2017-02-16 14:49	2017-02-16 14:49	0:00:14	100%	218.0 KB
admin	ICA	ICA	forward@ICA	Citrix	2017-02-16 14:48	2017-02-16 14:48	0:00:26	100%	42.0 KB

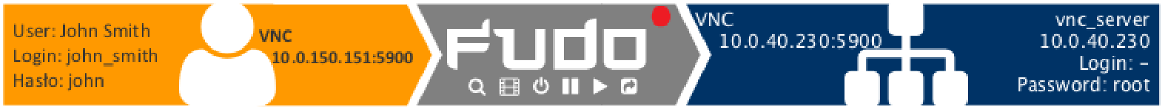
Related topics:

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

4.11 VNC

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

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



4.11.1 Prerequisites

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

4.11.2 Configuration

1 | server
2 | user
3 | listener
4 | account
5 | safe

Adding a server

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

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

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

4. Click *Save*.

Adding a user

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

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

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

4. Click *Save*.

Adding a listener

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

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

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

4. Click *Save*.

Adding an account

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

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

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

4. Click *Save*.

Defining a safe

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

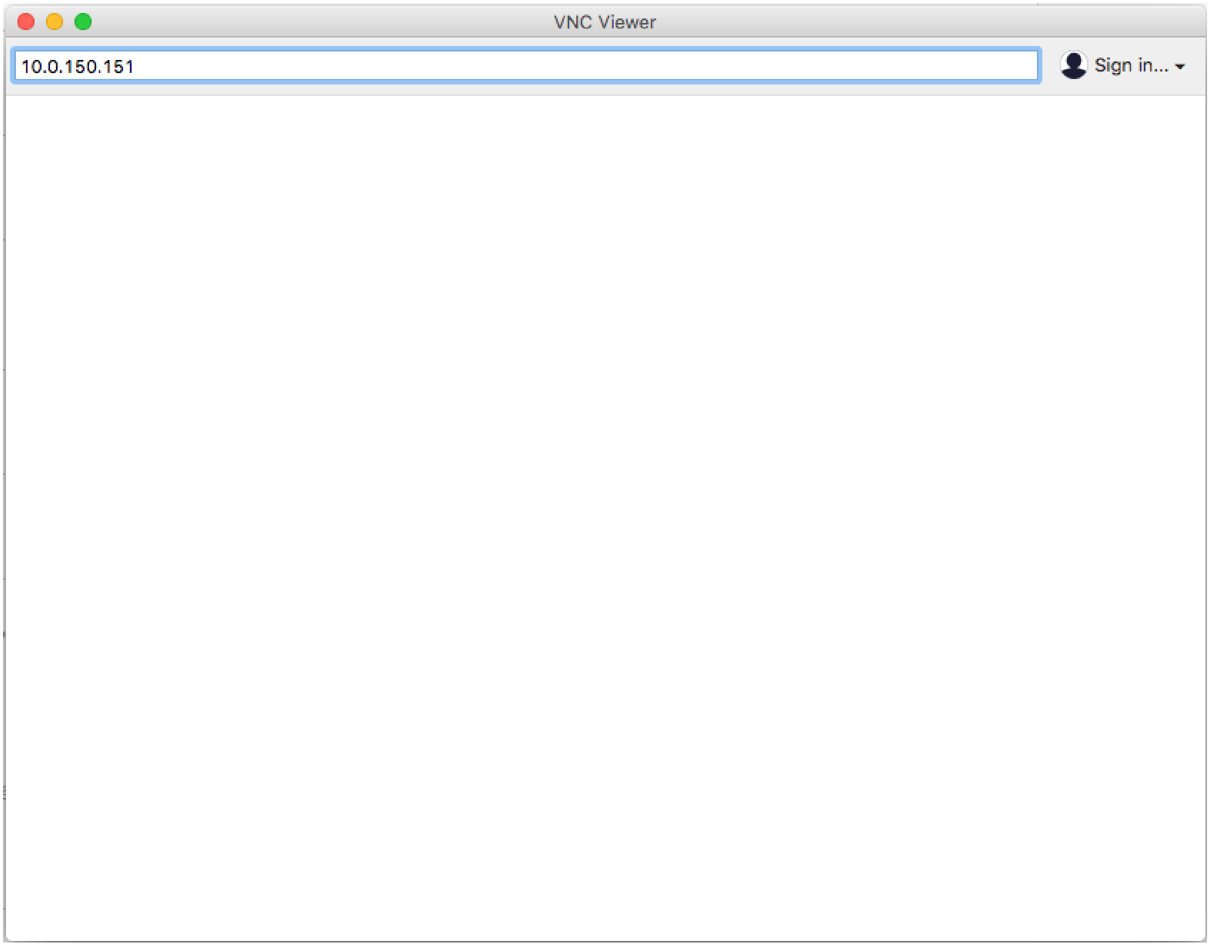
1. Select *Management > Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

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

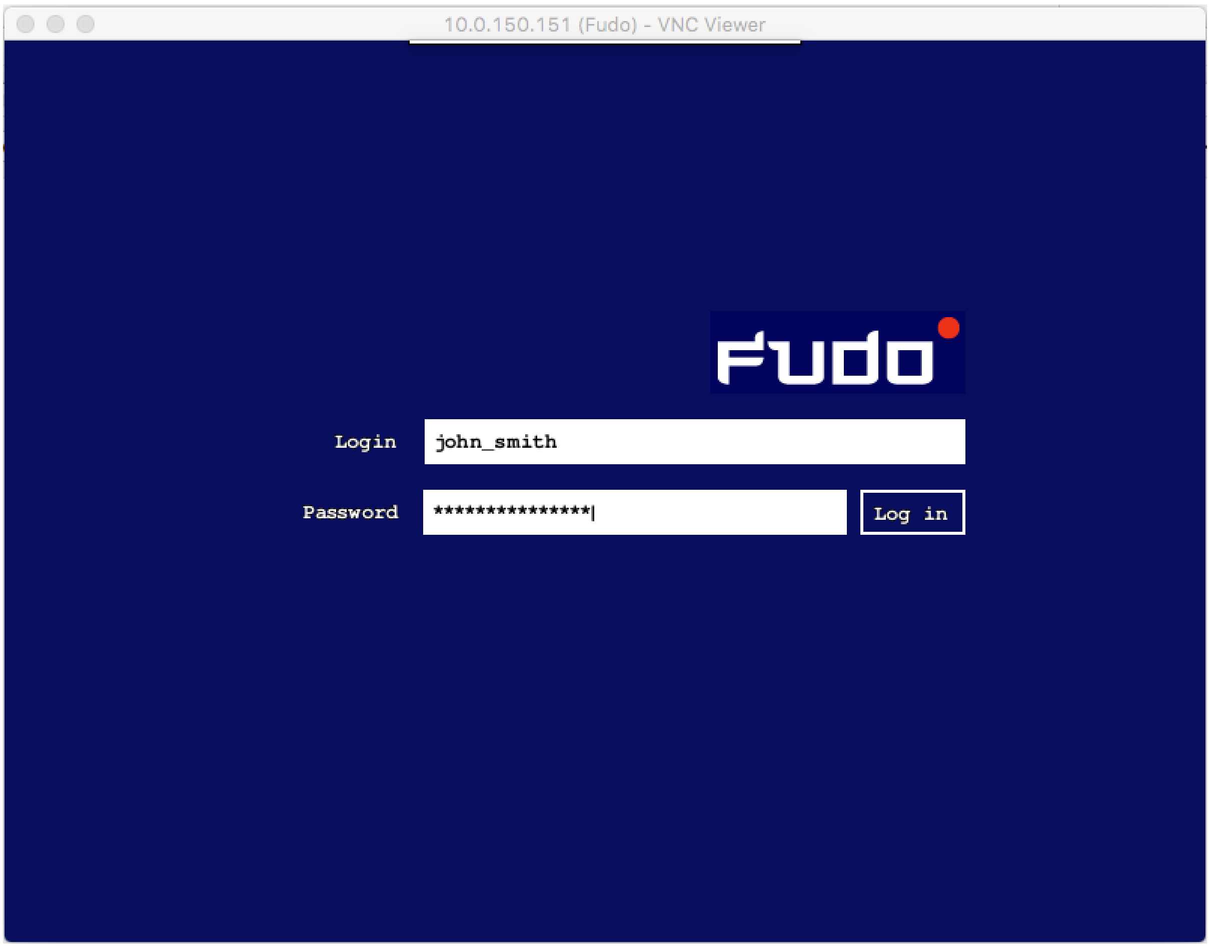
4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click ⊞.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_vnc_server` object and click ⊞.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `vnc_listener` object and click ⊞.
14. Click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

4.11.3 Establishing connection

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

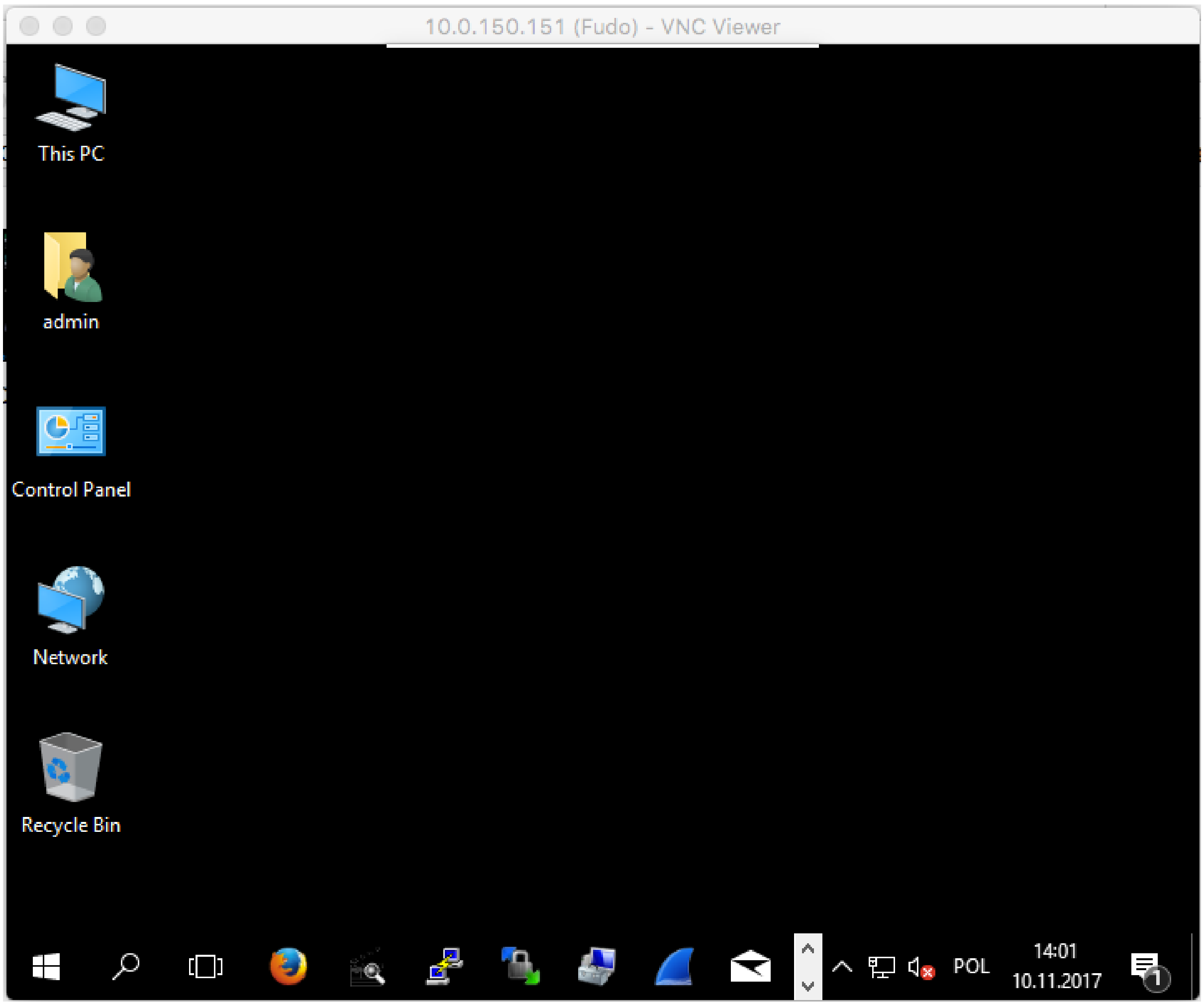


2. Enter username and password and press the enter key.



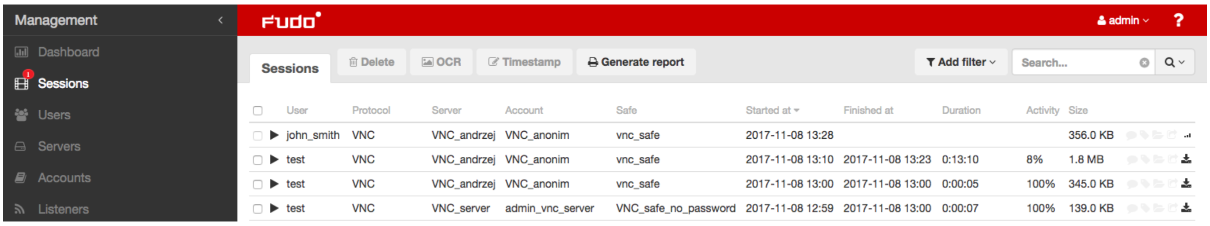
Login john_smith

Password ****************



4.11.4 Viewing user session

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



	User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
□ ▶	john_smith	VNC	VNC_andrzej	VNC_anonim	vnc_safe	2017-11-08 13:28				356.0 KB
□ ▶	test	VNC	VNC_andrzej	VNC_anonim	vnc_safe	2017-11-08 13:10	2017-11-08 13:23	0:13:10	8%	1.8 MB
□ ▶	test	VNC	VNC_andrzej	VNC_anonim	vnc_safe	2017-11-08 13:00	2017-11-08 13:00	0:00:05	100%	345.0 KB
□ ▶	test	VNC	VNC_server	admin_vnc_server	VNC_safe_no_password	2017-11-08 12:59	2017-11-08 13:00	0:00:07	100%	139.0 KB

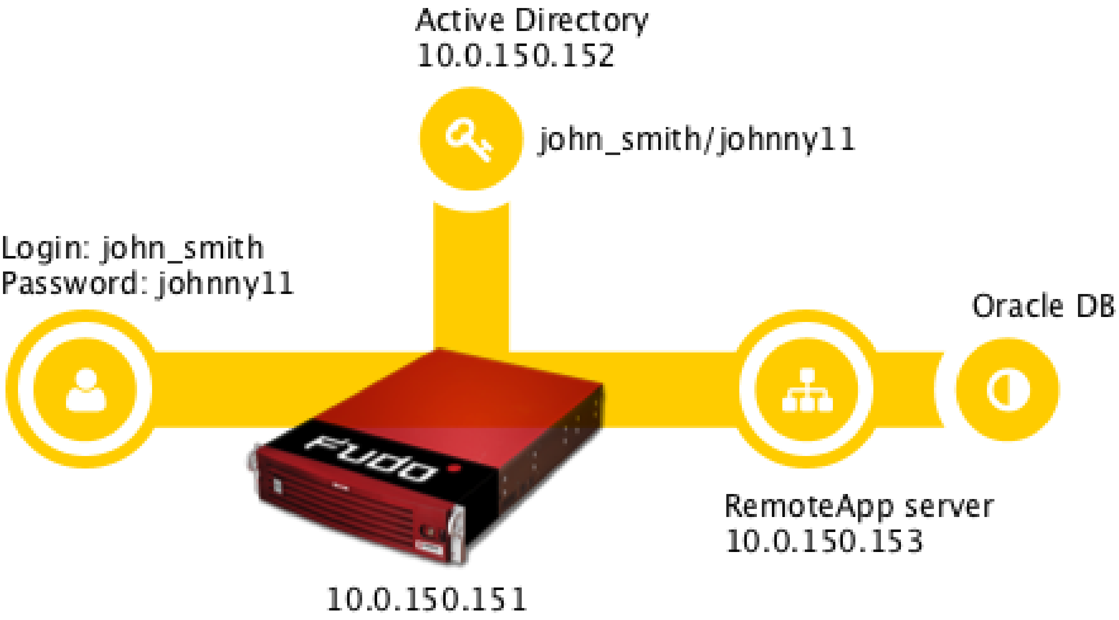
Related topics:

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

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

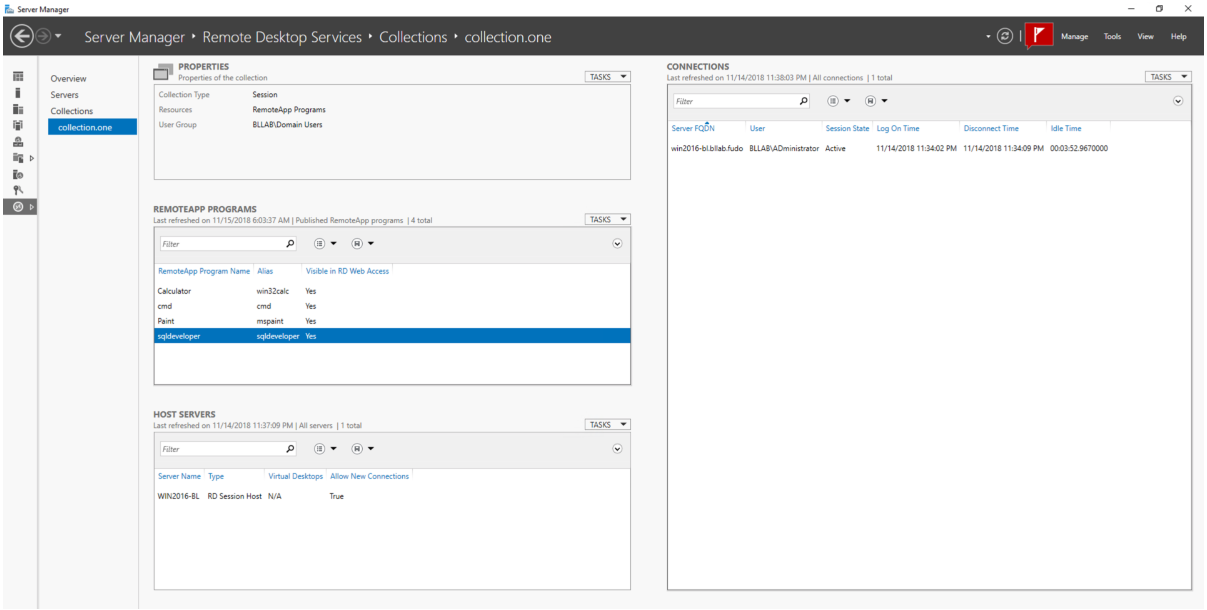
4.12 Oracle over RemoteApp

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



4.12.1 Prerequisites

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



PROPERTIES
Properties of the collection

Collection Type	Session
Resources	RemoteApp Programs
User Group	BLLAB\Domain Users

REMOTEAPP PROGRAMS
Last refreshed on 11/15/2018 6:03:37 AM | Published RemoteApp programs | 4 total

RemoteApp Program Name	Alias	Visible in RD Web Access
Calculator	win32calc	Yes
cmd	cmd	Yes
Paint	mspaint	Yes
sqldeveloper	sqldeveloper	Yes

HOST SERVERS
Last refreshed on 11/14/2018 11:37:09 PM | All servers | 1 total

Server Name	Type	Virtual Desktops	Allow New Connections
WIN2016-BL	RD Session Host	N/A	True

CONNECTIONS
Last refreshed on 11/14/2018 11:38:03 PM | All connections | 1 total

Server FQDN	User	Session State	Log On Time	Disconnect Time	Idle Time
win2016-bl.bllab.fudo	BLLAB\ADministrator	Active	11/14/2018 11:34:02 PM	11/14/2018 11:34:09 PM	00:03:52.9670000

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

4.12.2 Configuration

1 | server
2 | user
3 | listener
4 | account
5 | safe

Adding a server

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

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

Parameter	Value
General	
Name	`RemoteApp server`
Description	❌
Blocked	❌
Protocol	`RDP`
Security	`Enhanced RDP Security (TLS) + NLA`
Bind address	`Any`
Permissions	
Granted users	❌
Server addresses	
IP address	`10.0.150.153`
Port	`3389`

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

5. Click *Save*.

Adding a user

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

1. Select *Management > Users*.

2. Click *+ Add*.

3. Provide essential user information:

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

4. Click *Save*.

Adding a listener

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

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

Parameter	Value
General	
Name	`RemoteApp-listener`
Blocked	✗
Protocol	`RDP`
Security	`Enhanced RDP Security (TLS) + NLA`
Announcement	✗
Permissions	
Granted users	✗
Connection	
Mode	`proxy`
Local address	`10.0.150.151`
Port	`10025`
External address	✗
External port	✗

4. Generate or upload proxy server's private key.
5. Click *Save*.

Adding an account

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

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

Parameter	Value
General	
Name	`RemoteApp-account`
Blocked	✗
Type	`forward`
Session recording	`all`
OCR sessions	✓
OCR Language	`English`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`RemoteApp_server`
Credentials	
Replace secret with	✗
Forward domain	✓
Authenticate against server	✗

4. Click *Save*.

Defining a safe

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

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

Parameter	Value
General	
Name	`RemoteApp-safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Protocol functionality	
RDP	✓
SSH	✗
VNC	✗

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

4.12.3 Changing registry entries on the RDS domain controller

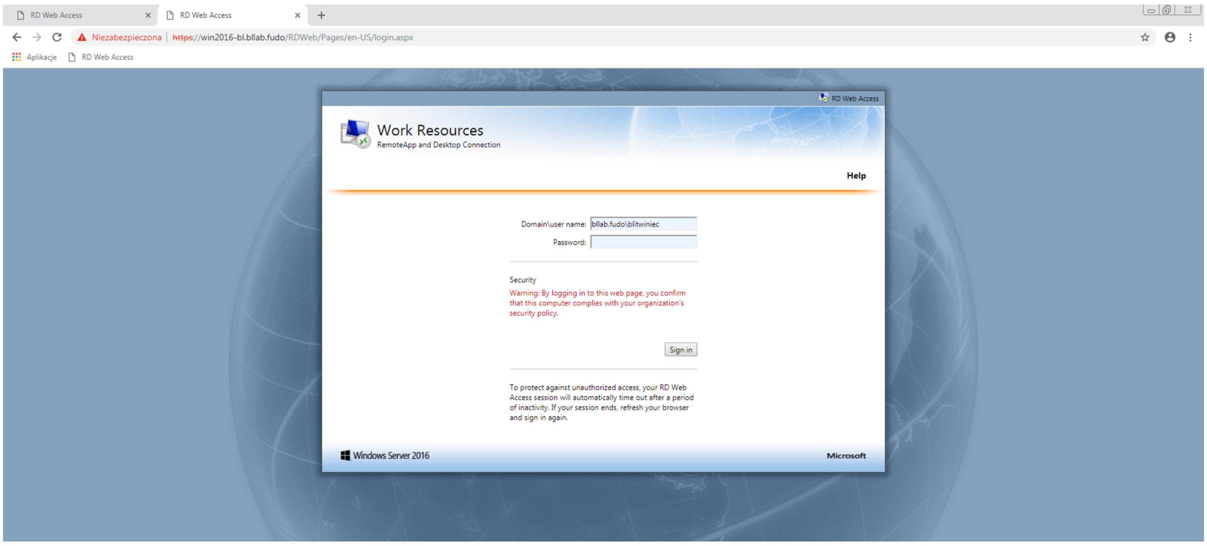
1. Log in, with administrator privileges, onto the server running the RDS service.
2. Start the system registry editor.
3. Browse registry to find the key

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\TerminalServer\
CentralPublishedResources\PublishedFarms\collectionone\Applications\sqldeveloper
```

4. In the *RDPFileContent* parameter, find the *full address:s:* and change its value to the IP address and port number of the previously configured listener, i.e. `full address:s:192.168.3.100:10025`

4.12.4 Establishing connection

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



Domain\user name: bllab.fudo\blitwiniec

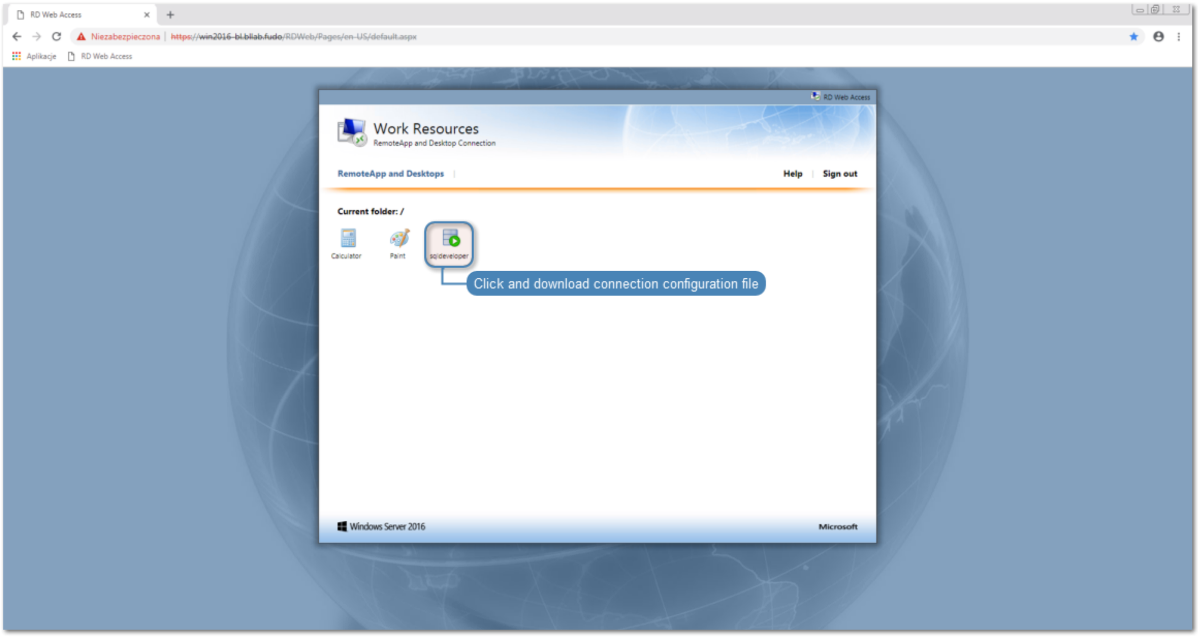
Password:

Security

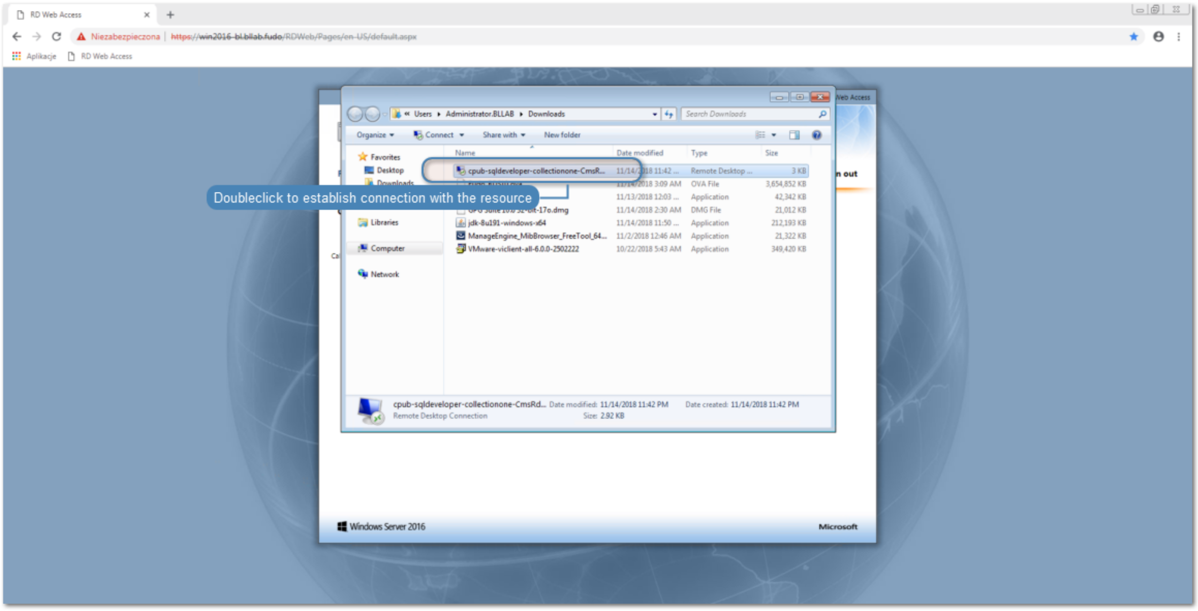
Warning: By logging in to this web page, you confirm that this computer complies with your organization's security policy.

To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

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



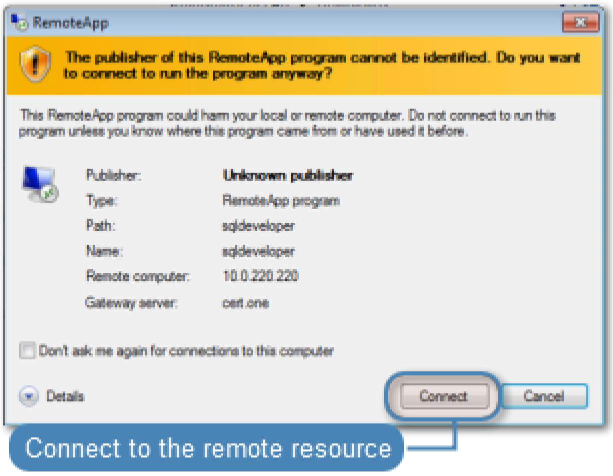
3. Double-click the configuration file.



Doubleclick to establish connection with the resource

RD Web Access
Niezabezpieczona | https://win2016-bl.bllab.fudo/RDWeb/Pages/en-US/default.aspx
Aplikacje
RD Web Access
Users ▸ Administrator.BLLAB ▸ Downloads
Search Downloads
Organize ▾
Connect ▾
Share with ▾
New folder
Favorites
Desktop
Downloads
Libraries
Computer
Network
Name
Date modified
Type
Size
cpub-sqldeveloper-collectionone-CmsR... 11/14/2018 11:42 ... Remote Desktop ... 3 KB
11/14/2018 3:09 AM OVA File 3,654,852 KB
11/13/2018 12:03 ... Application 42,342 KB
GPG Suite 2018 32-bit-17o.dmg 11/14/2018 2:30 AM DMG File 21,012 KB
jdk-8u191-windows-x64 11/14/2018 11:50 ... Application 212,193 KB
ManageEngine_MibBrowser_FreeTool_64... 11/2/2018 12:46 AM Application 21,322 KB
VMware-viclient-all-6.0.0-2502222 10/22/2018 5:43 AM Application 349,420 KB
cpub-sqldeveloper-collectionone-CmsRd... Date modified: 11/14/2018 11:42 PM Date created: 11/14/2018 11:42 PM
Remote Desktop Connection Size: 2.92 KB
Windows Server 2016
Microsoft

4. Click Connect, to establish connection.



RemoteApp

The publisher of this RemoteApp program cannot be identified. Do you want to connect to run the program anyway?

This RemoteApp program could harm your local or remote computer. Do not connect to run this program unless you know where this program came from or have used it before.

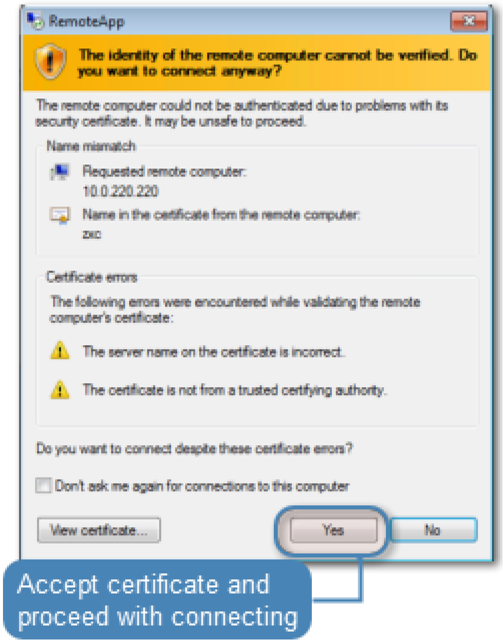
Publisher: **Unknown publisher**
Type: RemoteApp program
Path: sqldeveloper
Name: sqldeveloper
Remote computer: 10.0.220.220
Gateway server: cert.one

□ Don't ask me again for connections to this computer

Connect to the remote resource

5. Provide login credentials.

6. Accept the certificate and proceed with establishing the connection.



The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Requested remote computer:
10.0.220.220

Name in the certificate from the remote computer:
zxo

The following errors were encountered while validating the remote computer's certificate:

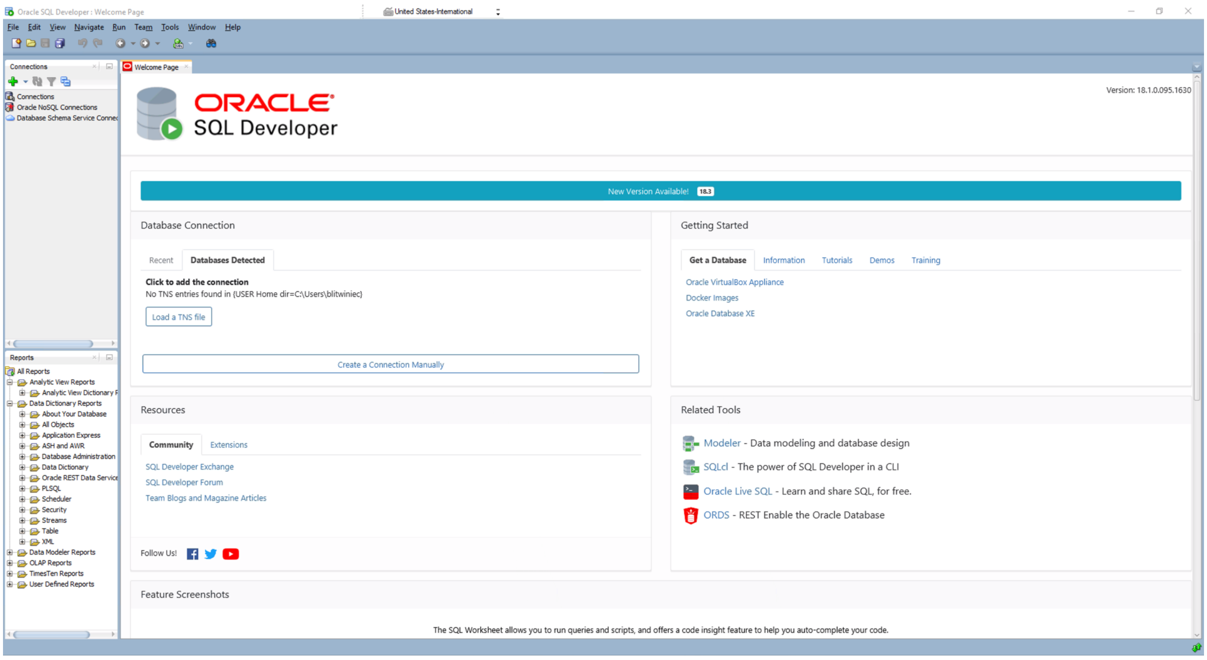
The server name on the certificate is incorrect.

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

Accept certificate and proceed with connecting



Version: 18.1.0.095.1630

Click to add the connection
No TNS entries found in {USER Home dir=C:\Users\blitwiniec}

Modeler - Data modeling and database design

SQLcl - The power of SQL Developer in a CLI

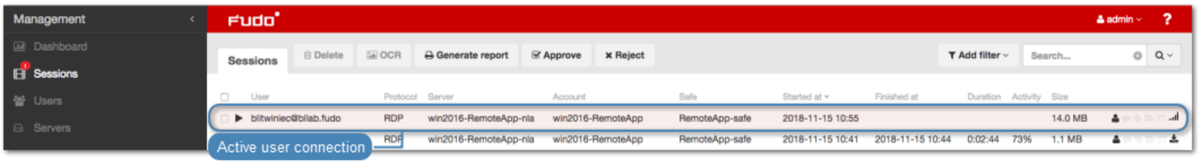
Oracle Live SQL - Learn and share SQL, for free.

ORDS - REST Enable the Oracle Database

The SQL Worksheet allows you to run queries and scripts, and offers a code insight feature to help you auto-complete your code.

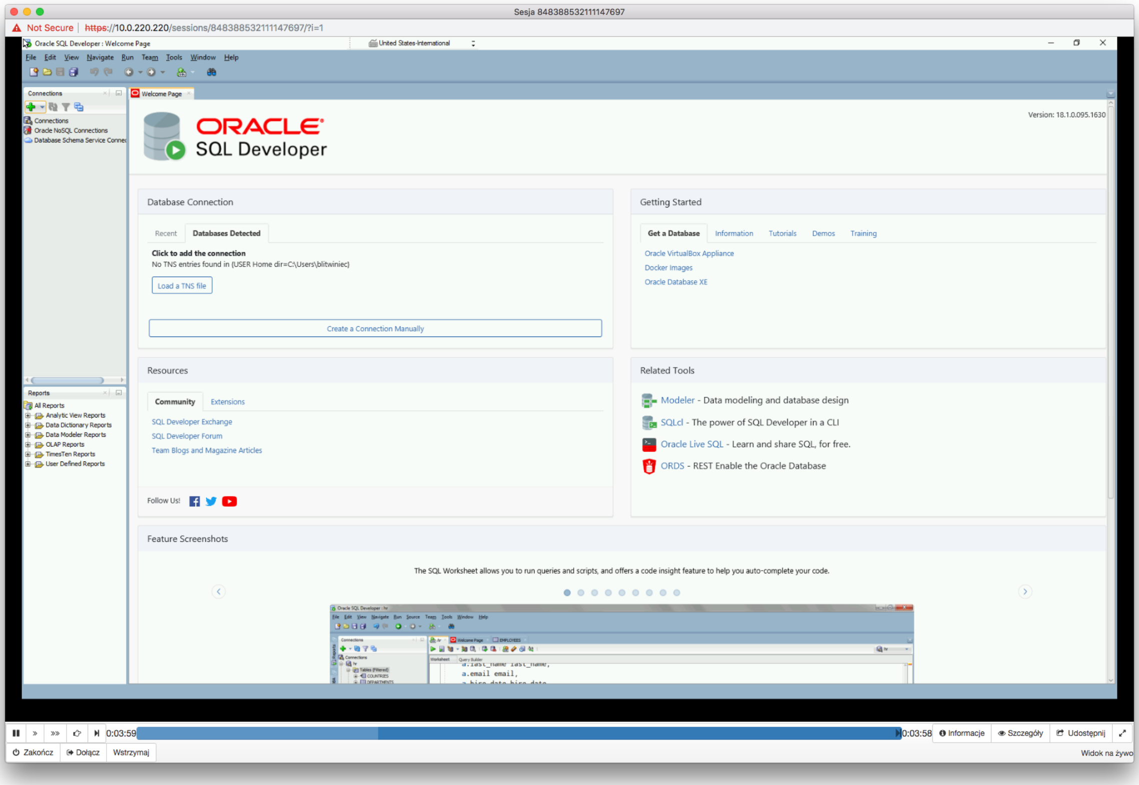
4.12.5 Viewing user session

1. Open a web browser and navigate to Fudo's administration panel.
2. Enter login credentials.
3. Select *Management* > *Sessions*.
4. Find *John Smith's* session and click the playback icon.



User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
blitwiniec@bllab.fudo	RDP	win2016-RemoteApp-nla	win2016-RemoteApp	RemoteApp-safe	2018-11-15 10:55				14.0 MB
	RDP	win2016-RemoteApp-nla	win2016-RemoteApp	RemoteApp-safe	2018-11-15 10:41	2018-11-15 10:44	0:02:44	73%	1.1 MB

Active user connection


Sesja 848388532111147697
Not Secure https://10.0.220.220/sessions/848388532111147697/?i=1
Oracle SQL Developer : Welcome Page
File Edit View Navigate Run Team Tools Window Help
Connections
Welcome Page
ORACLE SQL Developer
Version: 18.1.0.095.1630
Database Connection
Recent
Databases Detected
Click to add the connection
No TNS entries found in (USER Home dir=C:\Users\blitwiniec)
Load a TNS file
Create a Connection Manually
Getting Started
Get a Database
Information
Tutorials
Demos
Training
Oracle VirtualBox Appliance
Docker Images
Oracle Database XE
Resources
Community
Extensions
SQL Developer Exchange
SQL Developer Forum
Team Blogs and Magazine Articles
Follow Us!
Related Tools
Modeler - Data modeling and database design
SQLcl - The power of SQL Developer in a CLI
Oracle Live SQL - Learn and share SQL, for free.
ORDS - REST Enable the Oracle Database
Feature Screenshots
The SQL Worksheet allows you to run queries and scripts, and offers a code insight feature to help you auto-complete your code.
Reports
All Reports
Analytic View Reports
Data Dictionary Reports
Data Modeler Reports
OLAP Reports
TimesTen Reports
User Defined Reports
0:03:59
0:03:58
Informacje
Szczegóły
Udostępnij
Zakończ
Dołącz
Wstrzymaj
Widok na żywo

Related topics:

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

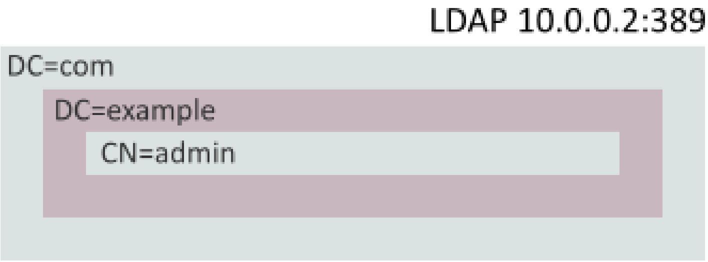
4.13 User authentication against external LDAP server

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

4.13.1 Prerequisites

The following description assumes that the `admin` user's authentication data is stored on LDAP server accessible through 10.0.0.2 IP address and default LDAP service port number - 389.

User definition is stored under `cn=admin,dc=example,dc=com`.

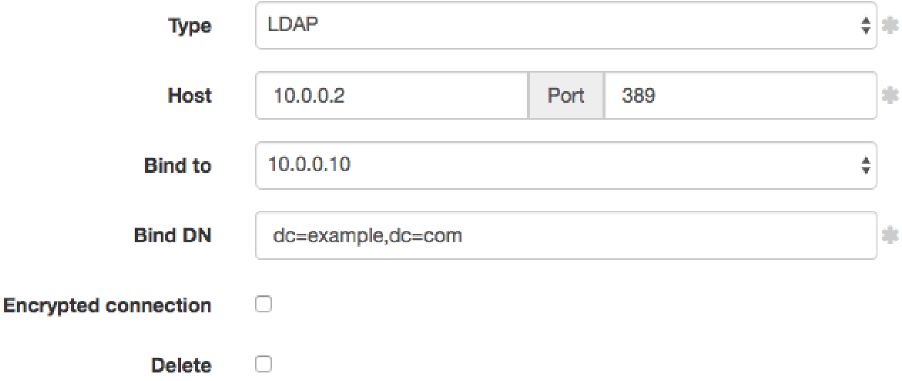


4.13.2 Configuration

Adding external authentication source

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

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



Type: LDAP

Host: 10.0.0.2 Port: 389

Bind to: 10.0.0.10

Bind DN: dc=example,dc=com

Encrypted connection: □

Delete: □

4. Click *Save*.

Adding user authentication method

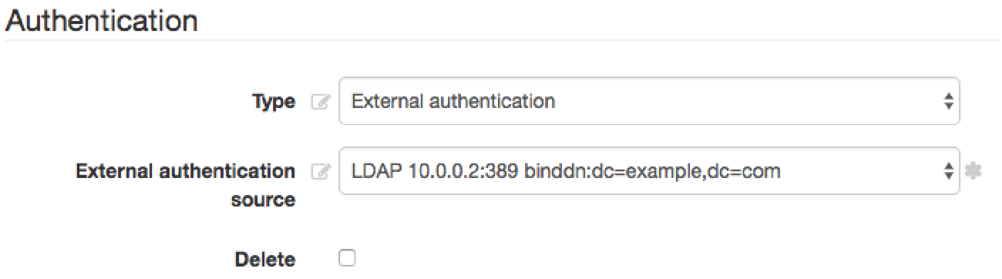
1. Select *Management > Users*.
2. Find and click the `admin` user definition.

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

Note: Leave the *LDAP base* field empty if you specified where users are stored in the LDAP server configuration (`cn=##username##,dc=example,dc=com`).

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

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



Authentication

Type: External authentication

External authentication source: LDAP 10.0.0.2:389 binddn:dc=example,dc=com

Delete □

6. Click *Save*.

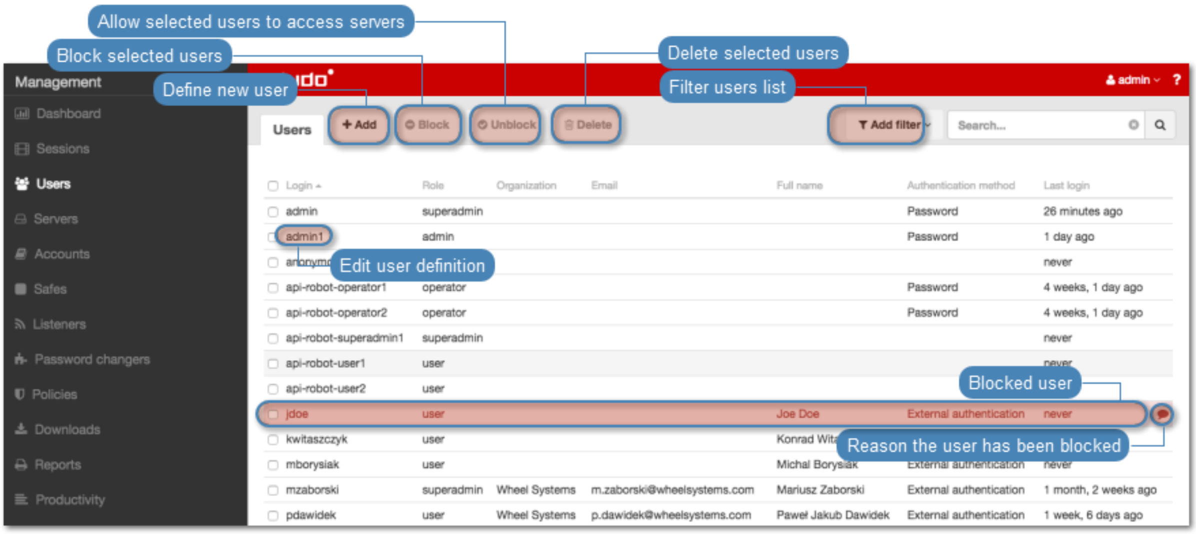
Related topics:

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

CHAPTER 5

Users

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



☐ Login	Role	Organization	Email	Full name	Authentication method	Last login
☐ admin	superadmin				Password	26 minutes ago
☐ admin1	admin				Password	1 day ago
☐ anonymo						never
☐ api-robot-operator1	operator				Password	4 weeks, 1 day ago
☐ api-robot-operator2	operator				Password	4 weeks, 1 day ago
☐ api-robot-superadmin1	superadmin					never
☐ api-robot-user1	user					never
☐ api-robot-user2	user					
☐ jdoe	user			Joe Doe	External authentication	never
☐ kwitaszczyk	user			Konrad Wit		
☐ mborysiak	user			Michal Borysiak	External authentication	never
☐ mzaborski	superadmin	Wheel Systems	m.zaborski@wheelsystems.com	Mariusz Zaborski	External authentication	1 month, 2 weeks ago
☐ pdawidek	user	Wheel Systems	p.dawidek@wheelsystems.com	Paweł Jakub Dawidek	External authentication	1 week, 6 days ago

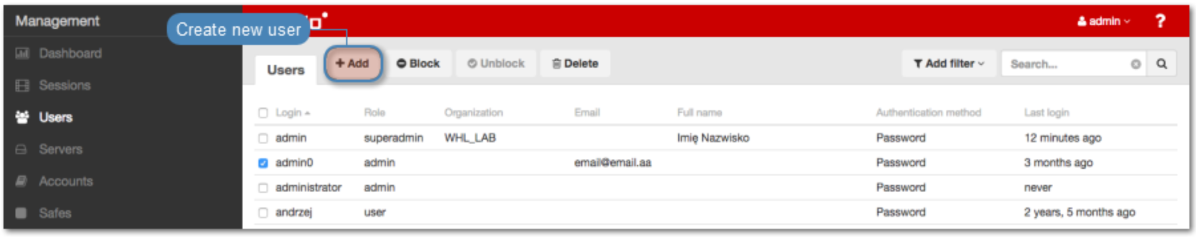
Note: Fudo PAM allows importing users definitions from directory services such as Active Directory or LDAP. For more information on users synchronization service, refer to the *Users synchronization* topic.

5.1 Creating a user

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

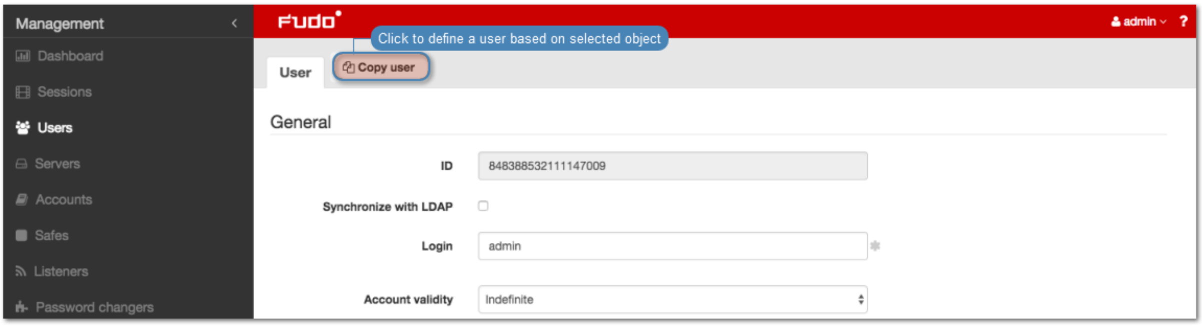
> **Warning:** Creating a User object for MySQL connections, please note that the MySQL server `caching_sha2_password` plugin isn't supported by Fudo PAM. Supportable MySQL plugins by Fudo PAM are `mysql_native_password` and `mysql_old_password`. Server plugin should be set to `mysql_native_password` in `/etc/mysql/mysql.conf.d/mysqld.cnf` and a User object is created with `mysql_native_password` plugin.

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



□ Login	Role	Organization	Email	Full name	Authentication method	Last login
□ admin	superadmin	WHL_LAB		Imię Nazwisko	Password	12 minutes ago
☑ admin0	admin		email@email.aa		Password	3 months ago
□ administrator	admin				Password	never
□ andrzej	user				Password	2 years, 5 months ago

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



ID: 848388532111147009

Synchronize with LDAP: □

Login: admin

Account validity: Indefinite

---

3. Enter user login.

Note:

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

---

4. Enter Fudo domain.

Note:

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

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

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

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

Role	Access rights
superadmin	• Full access rights to objects management. • Full access rights to system configuration options. • Available dashboard widgets: concurrent sessions, suspicious sessions, account alerts, active users, cluster status, concurrent sessions chart, license, system events log.

8. Select user's preferred language in Fudo PAM administration panel.

9. Grant access to safes.

Note:

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

10. Enter user's full name.

11. Enter user's email address.

12. Enter user's organizational unit.

13. Enter user's phone number.

14. Provide user's *Active Directory* domain.

Note: If there are two users with the same login, one of which has the domain configured the same as the *default domain*, and the other does not have the domain defined, Fudo PAM will report authentication problem as it cannot determine which user is trying to connect.

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

Note:

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

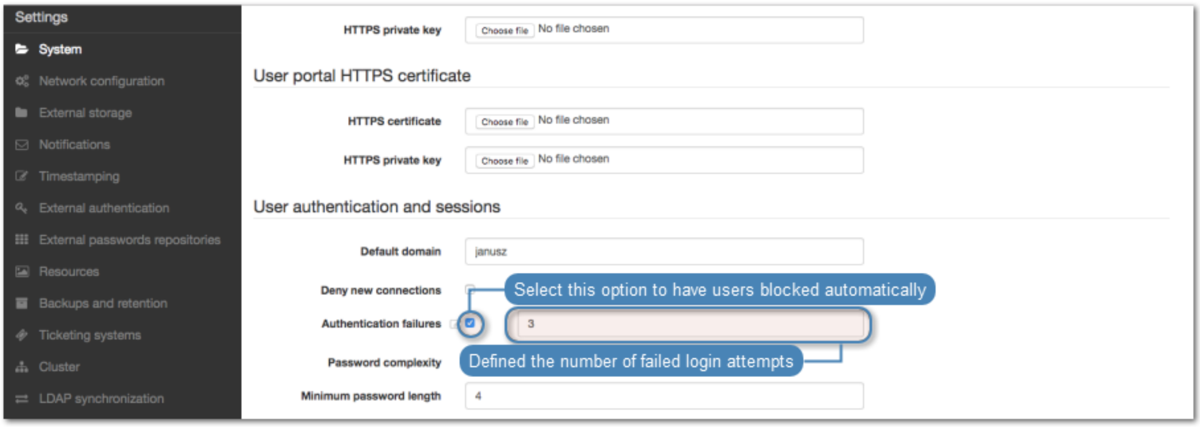
16. In the *Permissions* section, select users allowed to manage this user object and in case of operators/administrators, assign management privileges to selected data model objects.

Note: Granting a user access to certain session requires assigning management priviliges to:

server, account, user and safe objects that were used in the given connection.

17. In the *Authentication* section, select the *Authentication failures* option to block the user automatically after exceeding the number of failed login attempts.

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



HTTPS private key: No file chosen

User portal HTTPS certificate

HTTPS certificate: No file chosen

HTTPS private key: No file chosen

User authentication and sessions

Default domain: janusz

Deny new connections: □

Authentication failures: ☑ 3

Password complexity

Minimum password length: 4

Select this option to have users blocked automatically

Defined the number of failed login attempts

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

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

19. Select authentication type.

External authentication

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

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

Password

- Select `Password` from the *Type* drop-down list.
- Type password in the *Password* field.
- Repeat password in the *Repeat password* field.
- Select *Required password change on next login* to have the user change the password on next login attempt.

Note: If you select the *Required password change on next login* option, the user will not be able to access servers using native protocols clients. The user will have to change the password using the *User portal*.

SSH key

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

One-time password

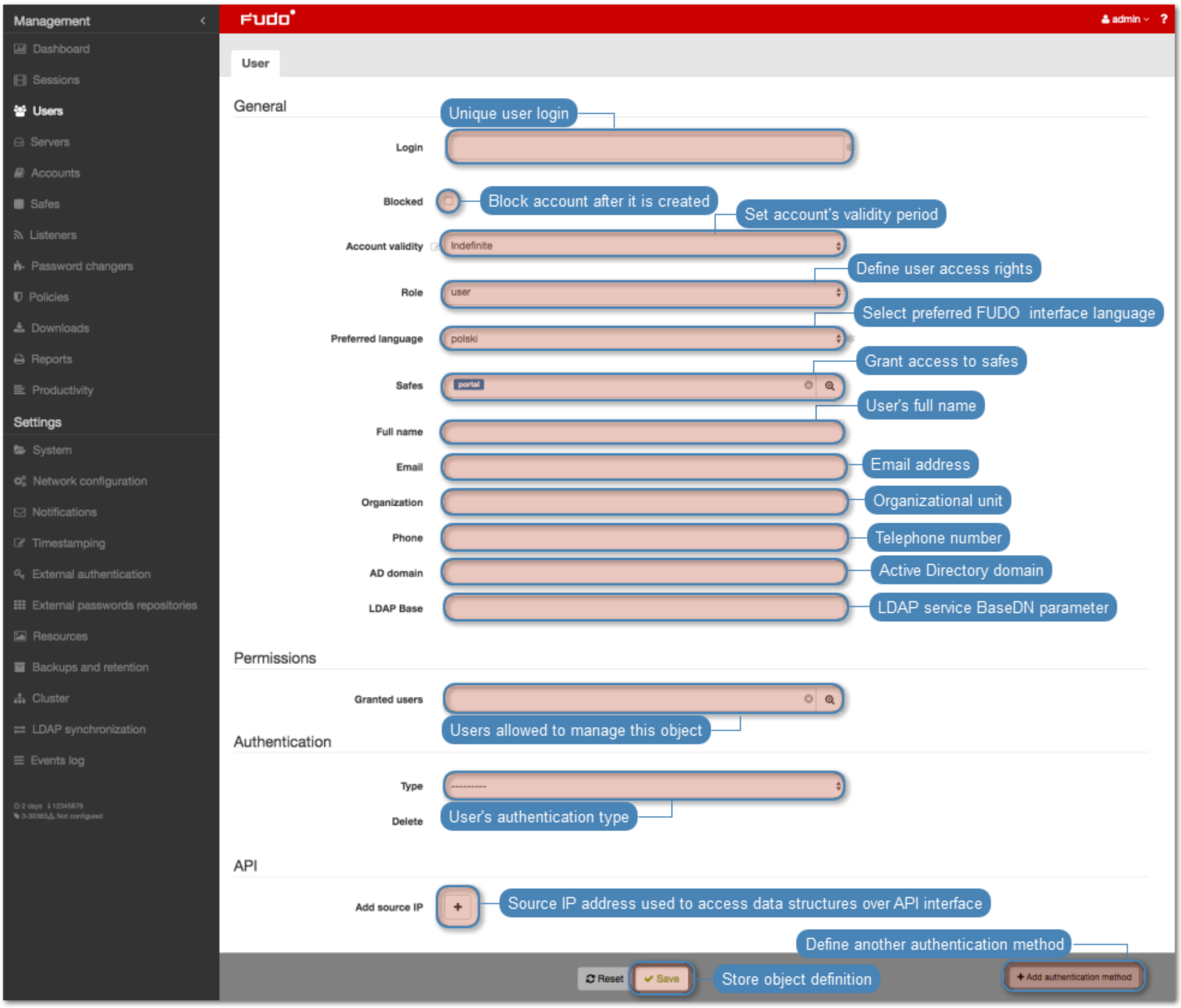
Warning: One-time passwords are used for implementing *AAPM* use case scenarios.

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

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

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

21. In the *API section*, click + and define IP address used by the *Access Gateway* and the *AAPM* to communicate with Fudo PAM.
22. Click *Save*.



Account validity: Indefinite

Role: user

Preferred language: polski

Safes: portal

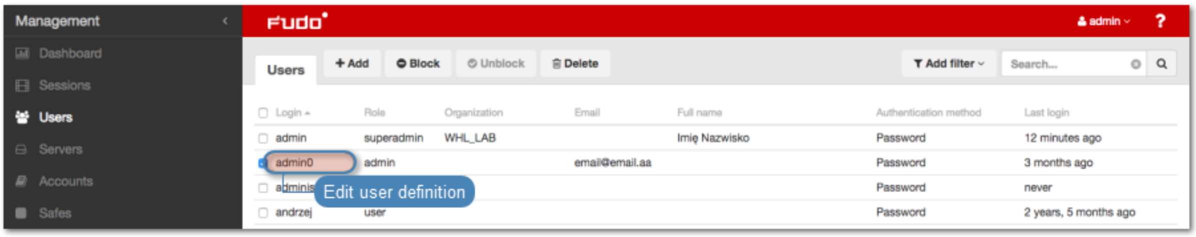
Type: ---------

Related topics:

- *Authentication failures counter*
- *Users synchronization*
- *Data model*
- *Default domain*
- *System initiation*
- *Servers*
- *Accounts*
- *Approving pending user requests*
- *Declining pending requests*

5.2 Editing a user

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



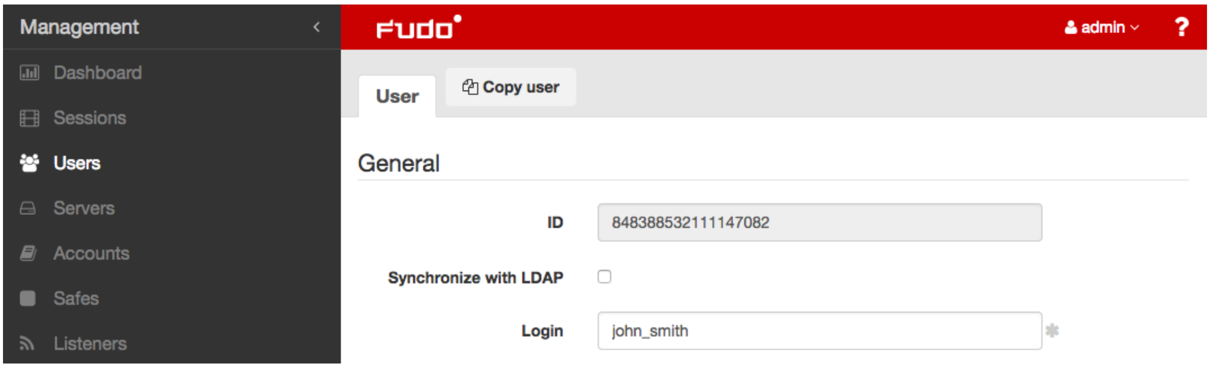
☐ Login	Role	Organization	Email	Full name	Authentication method	Last login
☐ admin	superadmin	WHL_LAB		Imię Nazwisko	Password	12 minutes ago
☑ admin0	admin		email@email.aa		Password	3 months ago
☐ adminis					Password	never
☐ andrzej	user				Password	2 years, 5 months ago

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

3. Modify configuration values as needed.

Note:

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



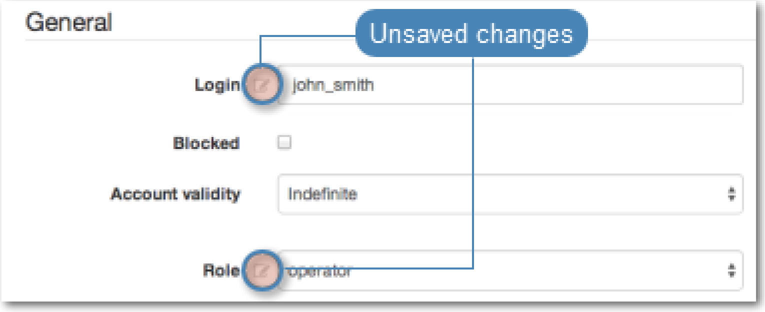
General

ID: 848388532111147082

Synchronize with LDAP: ☐

Login: john_smith

- Unsaved changes are marked with an icon.



General

Login: john_smith

Blocked: ☐

Account validity: Indefinite

Role: operator

4. Click *Save*.

Related topics:

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

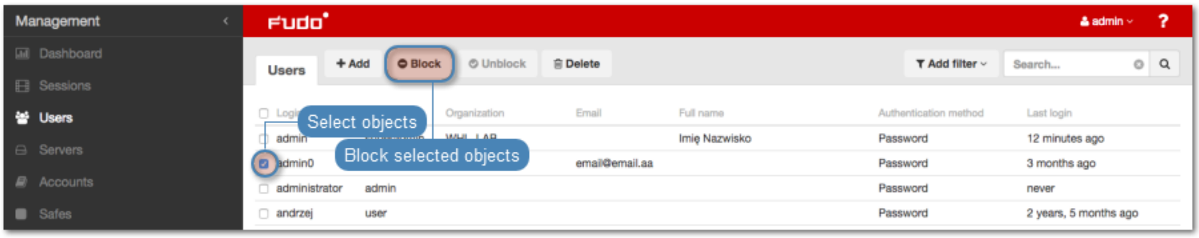
5.3 Blocking a user

Warning: Blocking a user will terminate its current connections.

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

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

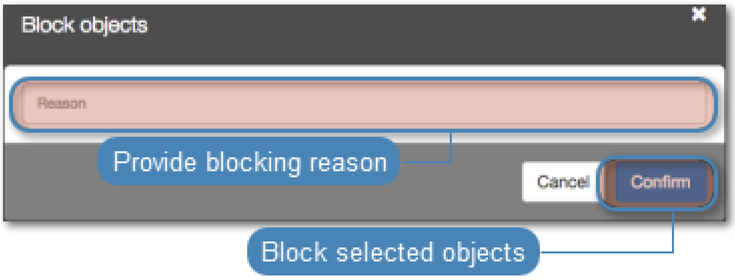
3. Click *Block*.



☐ Logi		Organization	Email	Full name	Authentication method	Last login
☐ admin	[illegible]	[illegible]		Imię Nazwisko	Password	12 minutes ago
☑ admin0			email@email.aa		Password	3 months ago
☐ administrator	admin				Password	never
☐ andrzej	user				Password	2 years, 5 months ago

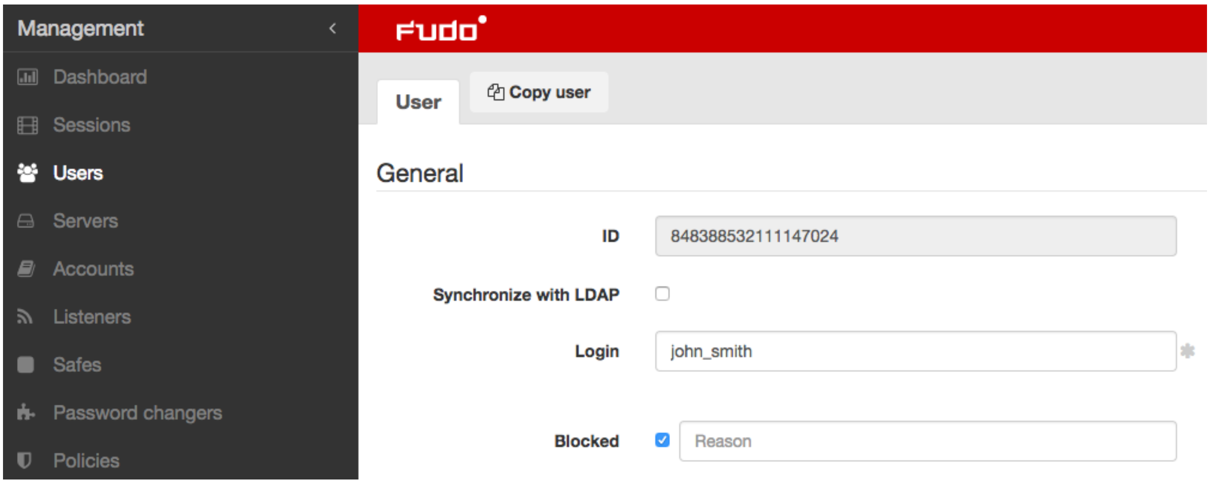
4. Optionally, provide blocking reason and click *Confirm*.

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



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

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



General

ID	848388532111147024
Synchronize with LDAP	□
Login	john_smith
Blocked	☑ Reason

- Click *Save*.

Related topics:

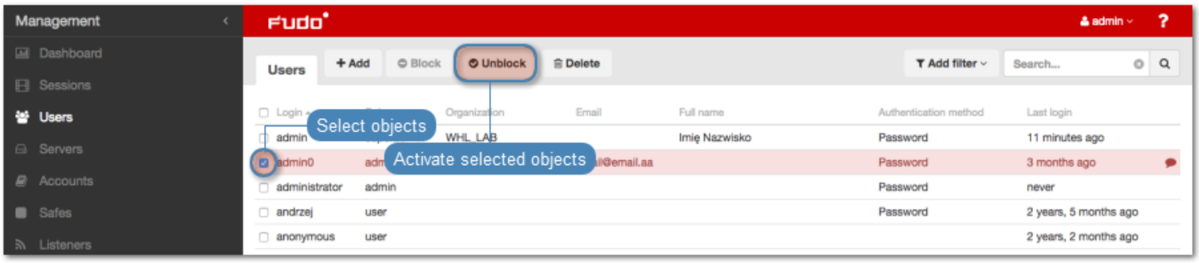
- *Users synchronization*
- *Data model*
- *System initiation*
- *Servers*
- *Accounts*

5.4 Unblocking a user

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

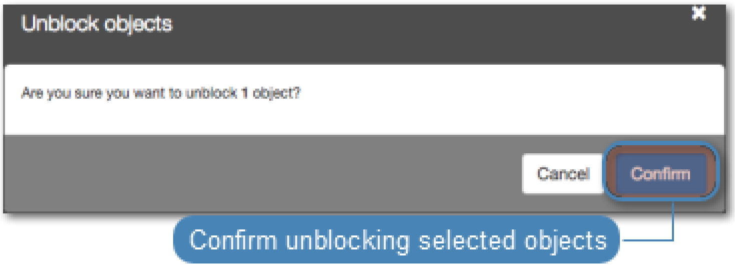
Note: Define filters to limit the number of objects displayed on the list.

3. Click *Unblock*.



	Login		Organization	Email	Full name	Authentication method	Last login
□	admin		WHL_LAB		Imię Nazwisko	Password	11 minutes ago
☑	admin0	adm		l@email.aa		Password	3 months ago
□	administrator	admin				Password	never
□	andrzej	user				Password	2 years, 5 months ago
□	anonymous	user					2 years, 2 months ago

4. Click *Confirm* to unblock selected objects.


Unblock objects

Are you sure you want to unblock 1 object?

Confirm unblocking selected objects

Related topics:

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

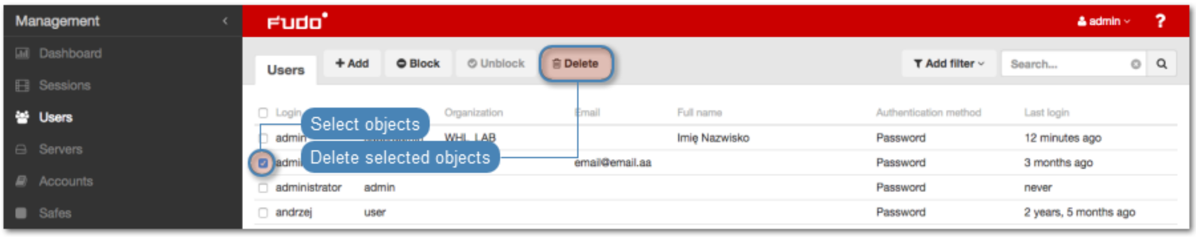
5.5 Deleting a user

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

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

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

3. Click *Delete*.

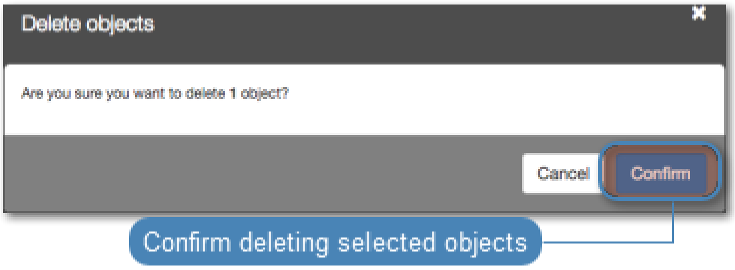


☐ Login		Organization	Email	Full name	Authentication method	Last login
☐ admin		WHL LAB		Imię Nazwisko	Password	12 minutes ago
☑ admi			email@email.aa		Password	3 months ago
☐ administrator	admin				Password	never
☐ andrzej	user				Password	2 years, 5 months ago

Select objects

Delete selected objects

4. Confirm deleting selected objects.


Delete objects

Are you sure you want to delete 1 object?

Confirm deleting selected objects

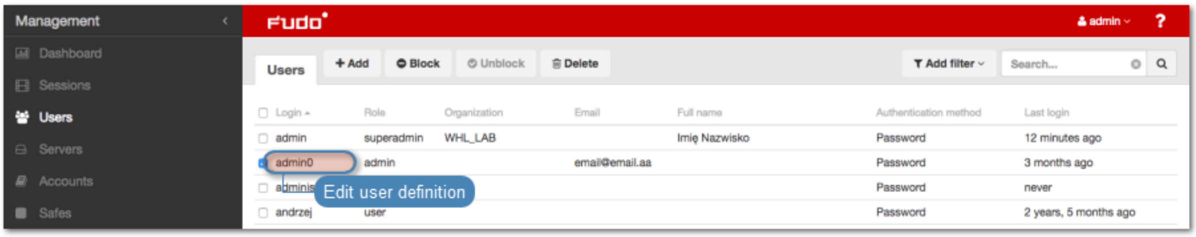
Related topics:

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

5.6 Time access policy

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

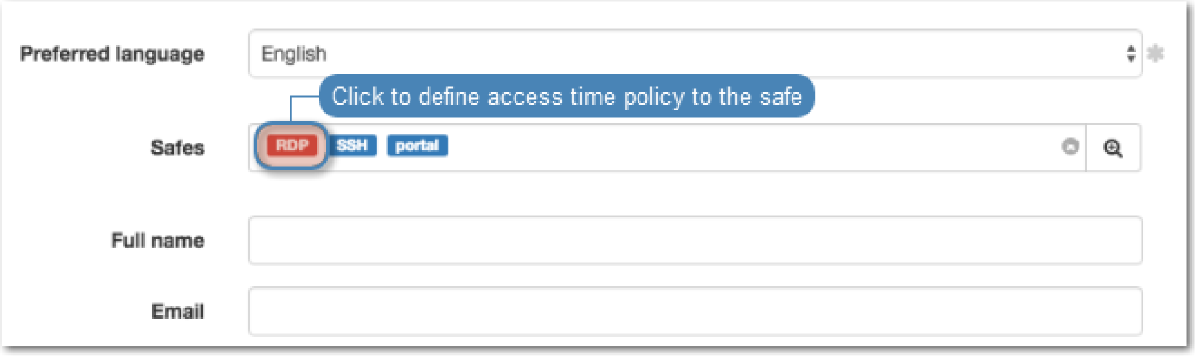
1. Select *Management* > *Users*.
2. Find and click desired user to access its configuration parameters.



Login	Role	Organization	Email	Full name	Authentication method	Last login
admin	superadmin	WHL_LAB		Imię Nazwisko	Password	12 minutes ago
admin0	admin		email@email.aa		Password	3 months ago
adminis					Password	never
andrzej	user				Password	2 years, 5 months ago

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

3. Click desired safe object.



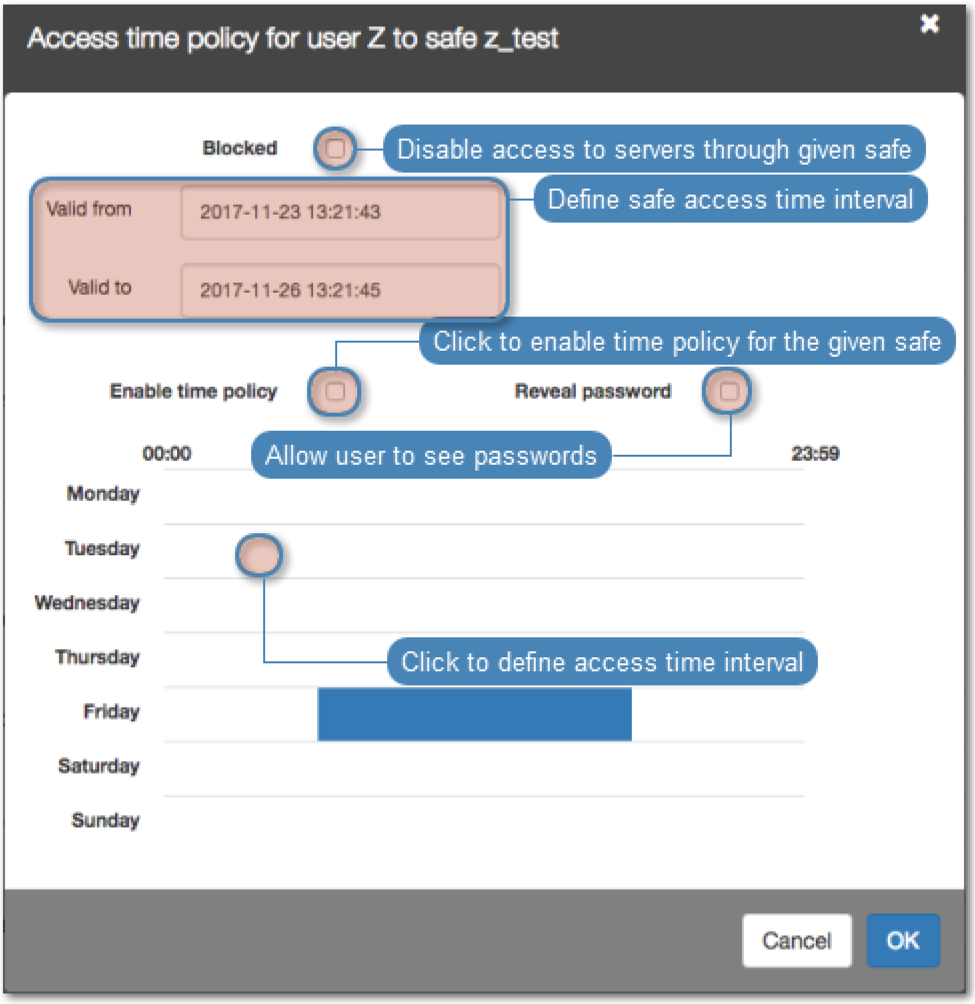
Preferred language	English
Safes	RDP SSH portal
Full name	
Email	

4. Select the *Blocked* option if you want to disable the user's access to the given safe. The user will be blocked until the administrator un-checks the *Blocked* option here or clicks *Enable access* button within the safe configuration.
5. Fill out the *Valid from* and *Valid to* fields with date and time interval when user will be allowed to access servers through the given safe. When defined date and time comes, access to the given safe is granted to the user automatically. Important note: the *Blocked* option from the previous step should be un-checked.
6. Select the *Enable time policy* option.

7. Select the *Reveal password* option to allow user to see the passwords to accounts that are grouped in selected safe.

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

8. Click the weekly calendar to define time interval.



Access time policy for user Z to safe z_test

Blocked □

Valid from 2017-11-23 13:21:43

Valid to 2017-11-26 13:21:45

Enable time policy □

Reveal password □

Disable access to servers through given safe
Define safe access time interval
Click to enable time policy for the given safe
Allow user to see passwords
Click to define access time interval
00:00
23:59
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Cancel
OK

9. Click *OK*.

10. Click *Save*.

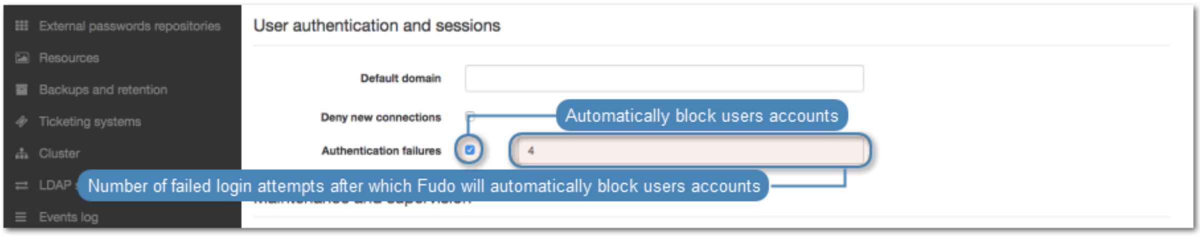
Related topics:

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

5.7 Authentication failures counter

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

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



User authentication and sessions

Default domain

Deny new connections □

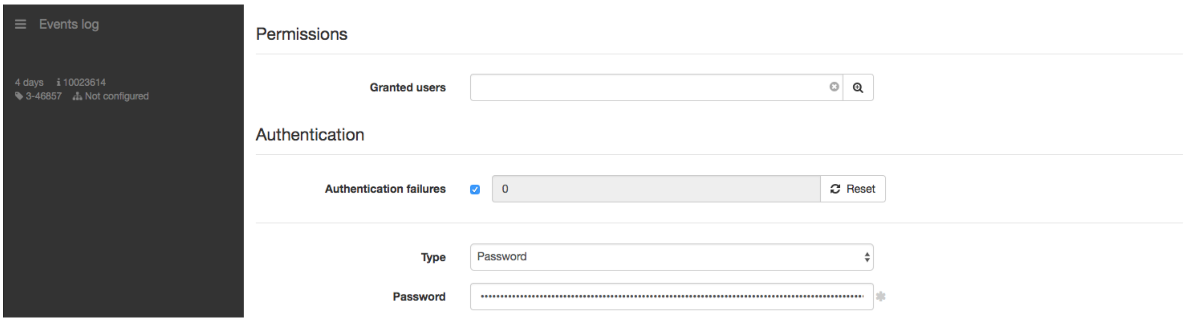
Authentication failures ☑ 4

Automatically block users accounts

Number of failed login attempts after which Fudo will automatically block users accounts

4. Click *Save*.
5. Select *Management > Users*.
6. Find and click a user that you want to block automatically after a number of failed login attempts.
7. In the *Authentication* section, select *Authentication failures*.
8. Click *Save*.

Note: Click Reset button to reset the counter.



Permissions

Granted users

Authentication

Authentication failures ☑ 0

Type: Password

Password: ••

Related topics:

- *User authentication methods and modes*

5.8 Roles

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

Role	Access rights
superadmin	• Full access rights to objects management. • Full access rights to system configuration options. • Available dashboard widgets: concurrent sessions, suspicious sessions, account alerts, active users, cluster status, concurrent sessions chart, license, system events log.

Related topics:

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

5.9 Users synchronization

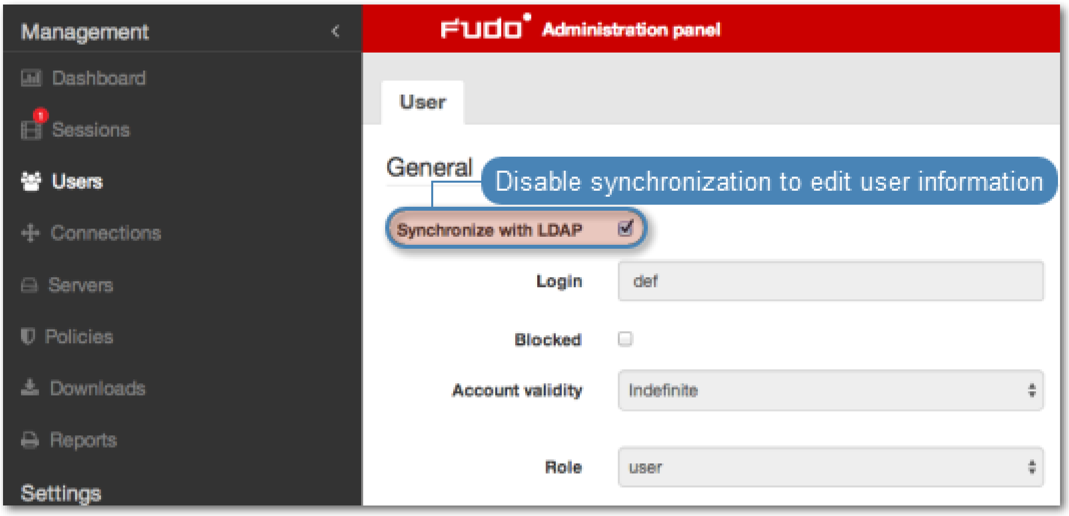
User is one of the fundamental *data model* entity. Only defined users are allowed to connect to monitored servers. Fudo PAM features automatic users synchronization service which enables importing users information from *Active Directory* servers or other servers compatible with the *LDAP* protocol.

Warning: It is required that LDAP server supports a `memberOf` parameter - an attribute that specifies the distinguished names of the groups to which this object belongs.

New users definitions and changes in existing objects are imported from the directory service periodically every 5 minutes. Deleting a user object from an *AD* or an *LDAP* server requires performing the full synchronization to reflect those changes on Fudo PAM. The full synchronization process is triggered automatically once a day at 00:00, or can be triggered manually.

Note:

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



Synchronize with LDAP ☑

Login: def

Blocked □

Account validity: Indefinite

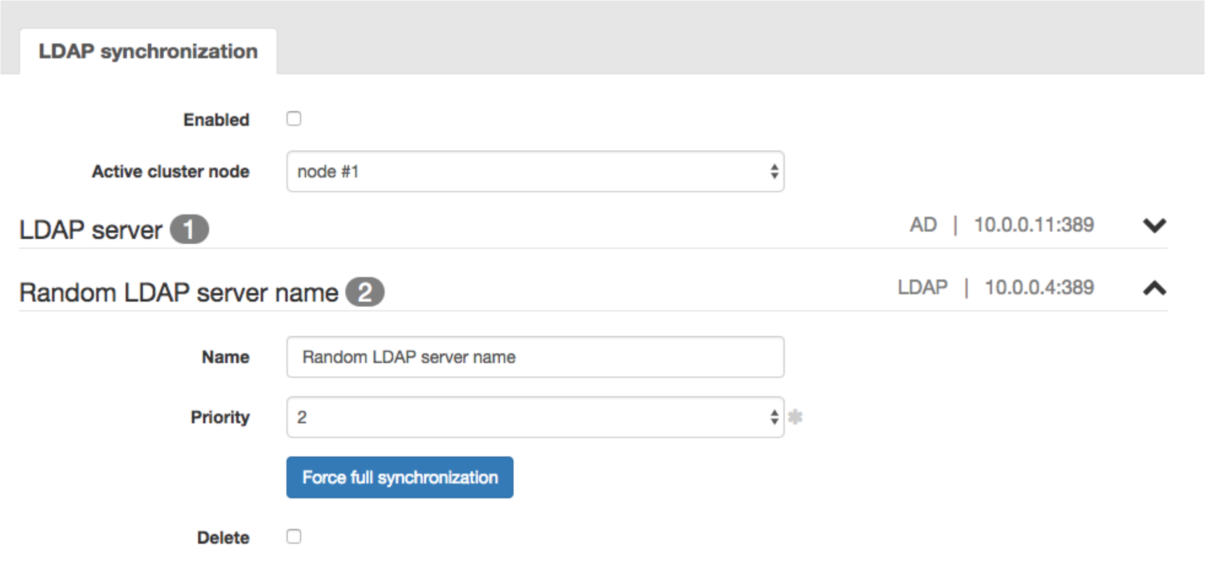
Role: user

Configuring users synchronization service

To enable users synchronization feature, proceed as follows.

1. Select *Settings > LDAP synchronization*.
2. Select *Enabled*.
3. In case of *cluster configuration*, from the *Active cluster node* drop-down list, select which node will be performing objects synchronization with LDAP service.
4. Click *+ Add LDAP domain*.
5. Provide domain's name.
6. Define priority, determining the order in which domains are queried.

Note: Lower number translates to higher priority.



Enabled □

Active cluster node: node #1

LDAP server 1 — AD | 10.0.0.11:389

Random LDAP server name 2 — LDAP | 10.0.0.4:389

Name: Random LDAP server name

Priority: 2

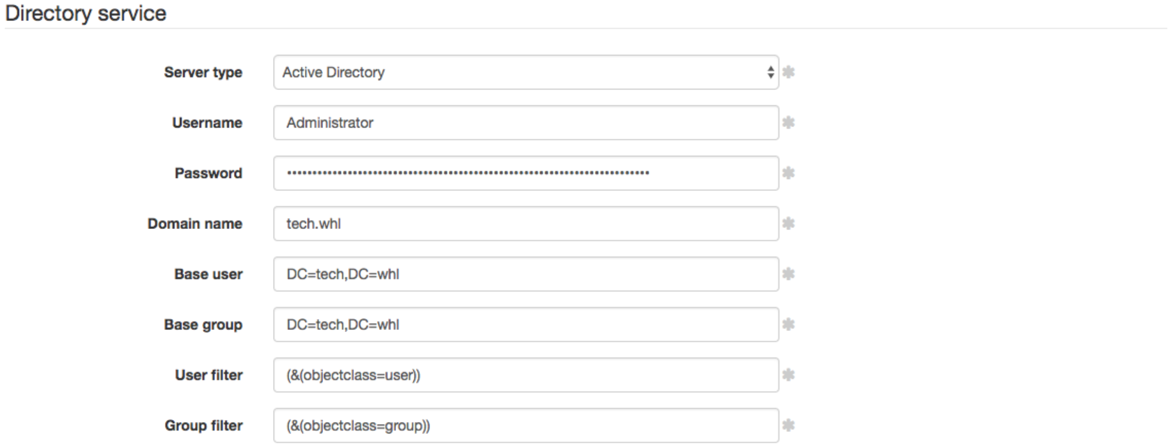
Delete □

7. In the *Directory service* section, select data source type from the *Server type* drop-down list.

8. Provide the user authentication information to access user data on given server.
9. Enter domain name, to which imported users are assigned to.
10. Provide base DN parameter for users' objects (eg. `DC=devel,DC=whl`).
11. Provide base DN for parameter groups' objects (eg. `DC=tech,DC=whl`).

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

12. Define filter (or leave the default value) for user records, which are subject to synchronization.
13. Define filter (or leave the default value) for user groups, which are subject to synchronization.



Directory service

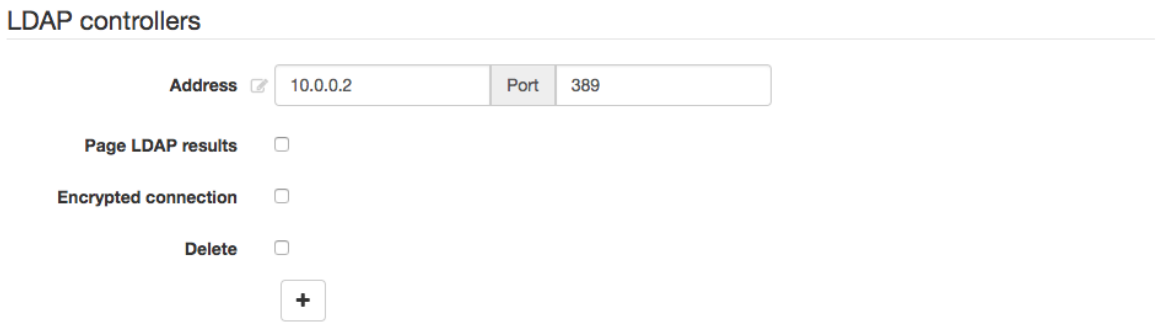
Server type	Active Directory
Username	Administrator
Password	••
Domain name	tech.whl
Base user	DC=tech,DC=whl
Base group	DC=tech,DC=whl
User filter	(&(objectclass=user))
Group filter	(&(objectclass=group))

14. Select *Block automatically* to automatically block local users' accounts blocked in the directory.
15. Click + in the *LDAP controllers* section to define directory service server.
16. Provide IP address and port number.

Note: In case of TLS-encrypted connection, define LDAP server's address using its full domain name (e.g. `tech.ldap.com`) instead of an IP address, to ensure the certificate is verified properly. Make sure that the given server name is included in certificate's *Common Name* field.

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

Note: Click + to add more directory servers.



LDAP controllers

Address: 10.0.0.2 Port: 389

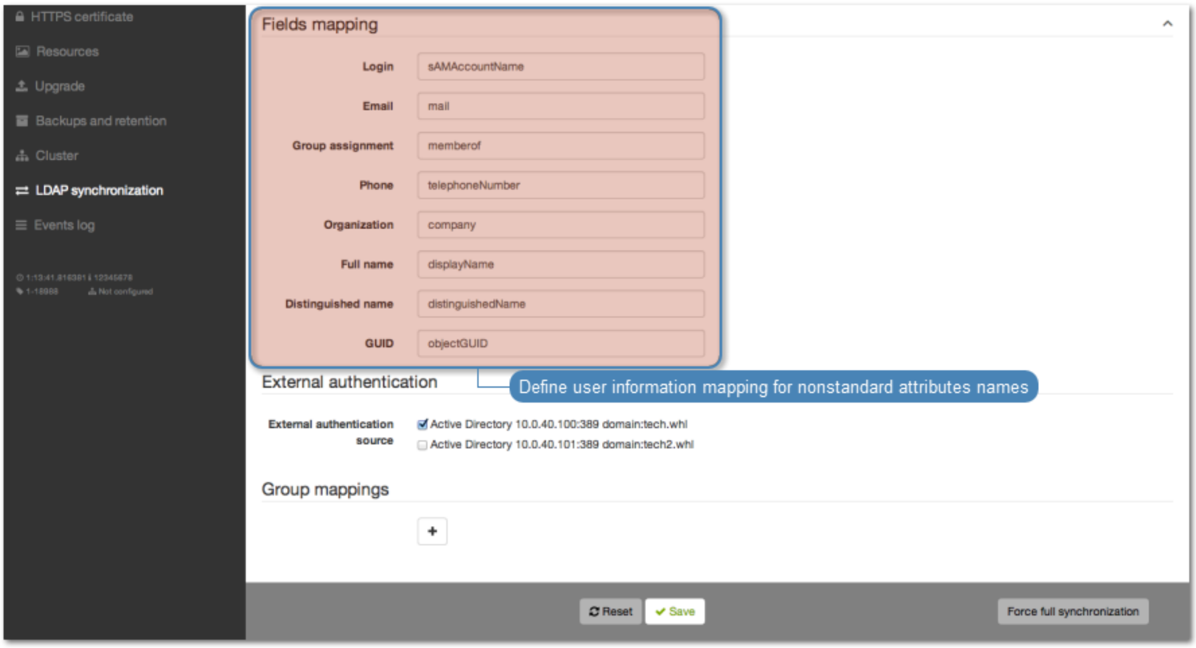
Page LDAP results □

Encrypted connection □

Delete □

19. 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*.



Fields mapping

Login: sAMAccountName

Email: mail

Group assignment: memberof

Phone: telephoneNumber

Organization: company

Full name: displayName

Distinguished name: distinguishedName

GUID: objectGUID

Define user information mapping for nonstandard attributes names

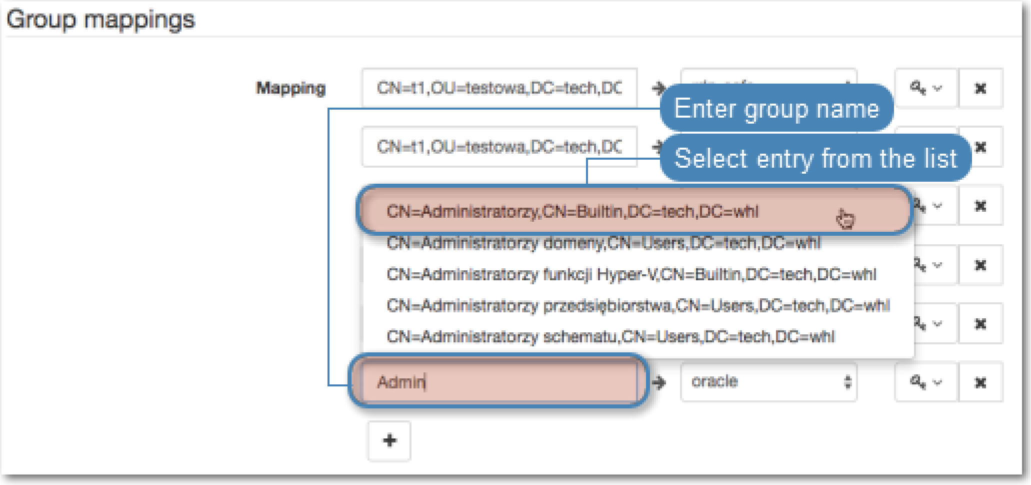
External authentication

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

20. Click **+** in the *Groups mapping* section to define user groups to safes assignment.

21. Type in user group and select desired entry.



Group mappings

Mapping CN=t1,OU=testowa,DC=tech,DC →

Enter group name

CN=t1,OU=testowa,DC=tech,DC →

Select entry from the list

CN=Administratorzy,CN=Builtin,DC=tech,DC=whl
CN=Administratorzy domeny,CN=Users,DC=tech,DC=whl
CN=Administratorzy funkcji Hyper-V,CN=Builtin,DC=tech,DC=whl
CN=Administratorzy przedsiębiorstwa,CN=Users,DC=tech,DC=whl
CN=Administratorzy schematu,CN=Users,DC=tech,DC=whl

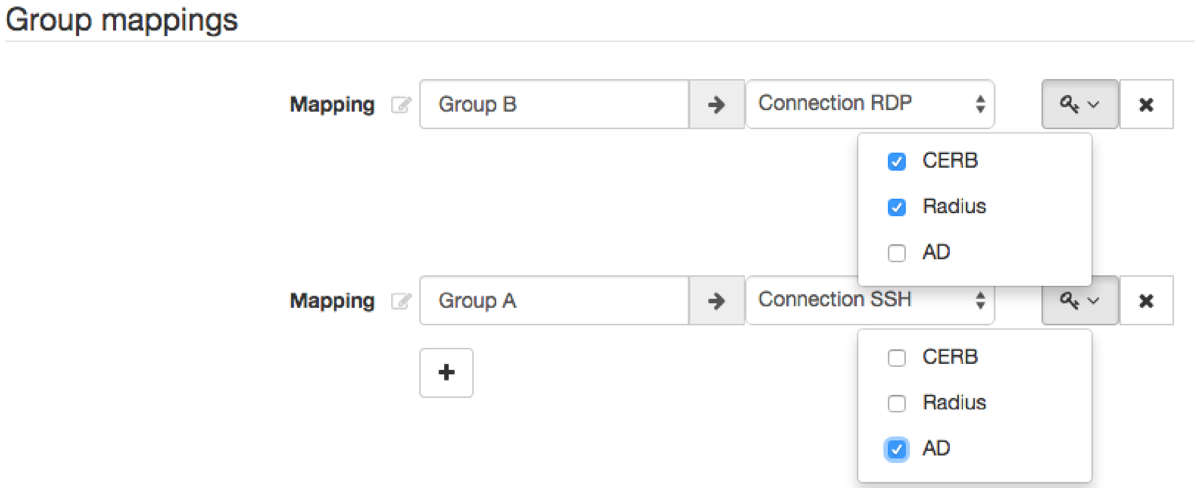
Admin → oracle

22. Assign safes to user groups.
23. 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, 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

Mapping Group B → Connection RDP

☑ CERB
☑ Radius
☐ AD

Mapping Group A → Connection SSH

☐ CERB
☐ Radius
☑ AD

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

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

24. 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.
- Use *diagnostics tools* to troubleshoot problems with LDAP configuration.
- Fudo PAM supports nested LDAP groups.

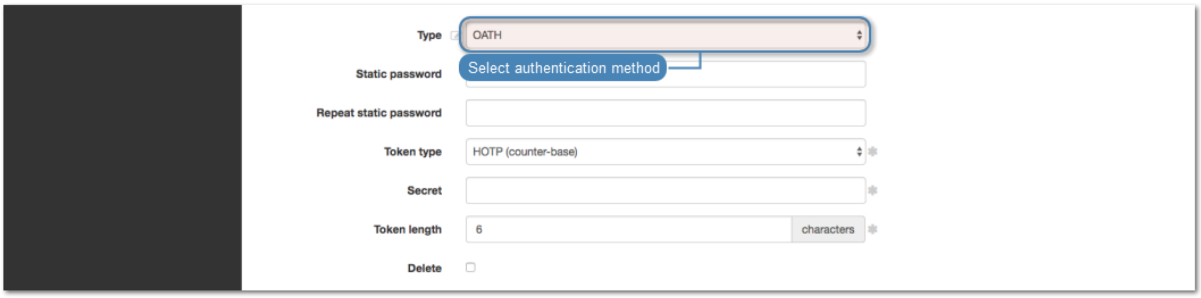
Related topics:

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

5.10 Two-factor OATH authentication with Google Authenticator

Google Authenticator allows for adding a dynamic component to a static password for increased account security.

1. Select *Management > Users*.
2. Find and click the user for whom you want to add the OATH authentication method.
3. Click *+ Add authentication method*.
4. From the *Type* drop-down list, select `OATH`.



Type: OATH

Select authentication method

Static password:

Repeat static password:

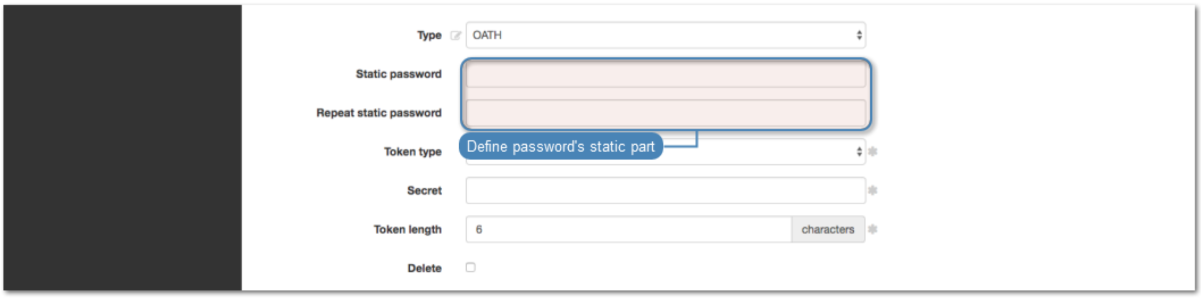
Token type: HOTP (counter-base)

Secret:

Token length: 6 characters

Delete: □

5. Enter password's static part.



Type: OATH

Static password:

Repeat static password:

Define password's static part

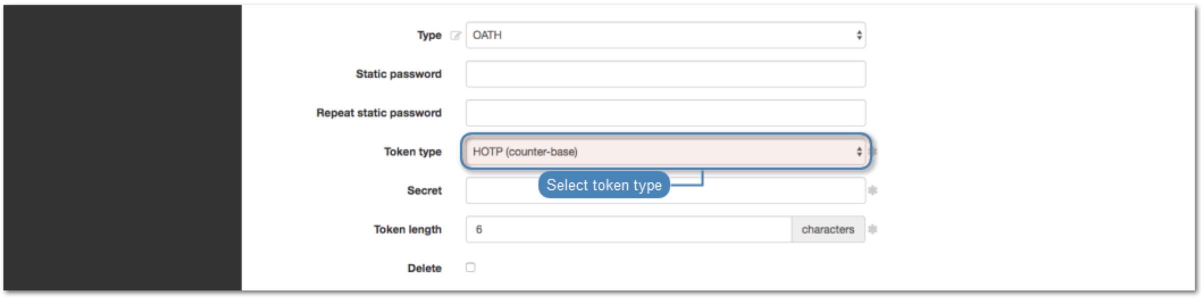
Token type:

Secret:

Token length: 6 characters

Delete: □

6. From the *Token type* drop-down list, select `HOTP (counter-based)`.



Type: OATH

Static password:

Repeat static password:

Token type: HOTP (counter-base)

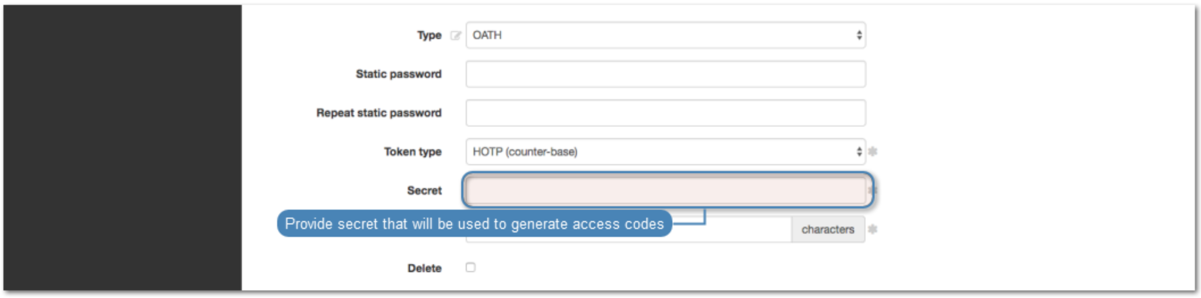
Select token type

Secret:

Token length: 6 characters

Delete: □

7. Enter a secret that will be used by *Google Authenticator* or click ⚙ to generate it automatically.



Type: OATH

Static password:

Repeat static password:

Token type: HOTP (counter-base)

Secret:

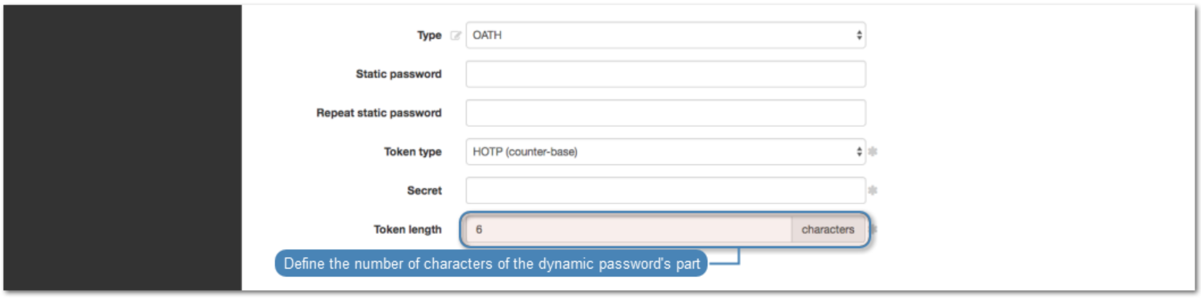
Provide secret that will be used to generate access codes

characters

Delete: □

Note: The secret must be a `Base32` encoded value.

8. In the *Length* field, enter `6`.



Type: OATH

Static password:

Repeat static password:

Token type: HOTP (counter-base)

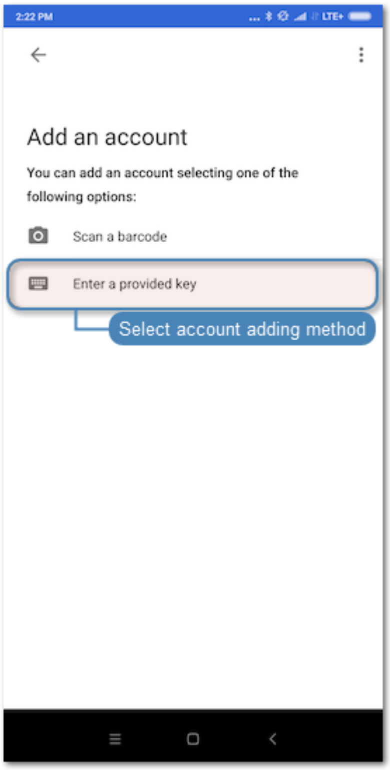
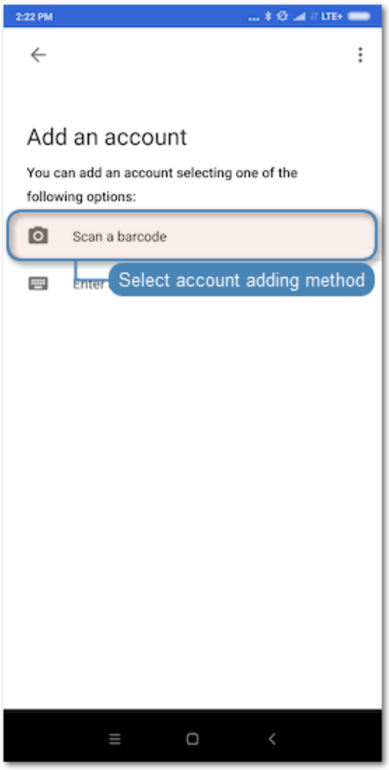
Secret:

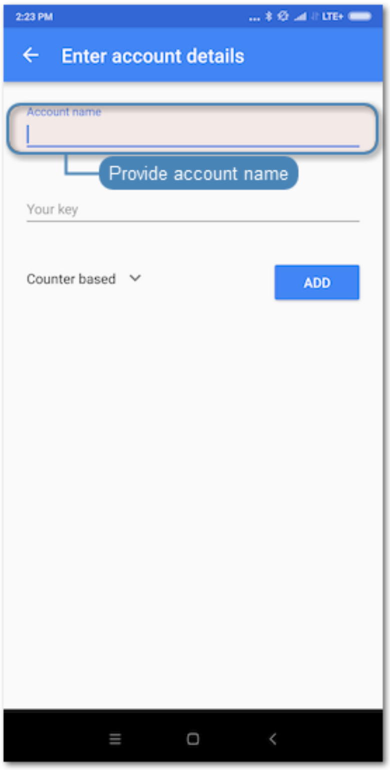
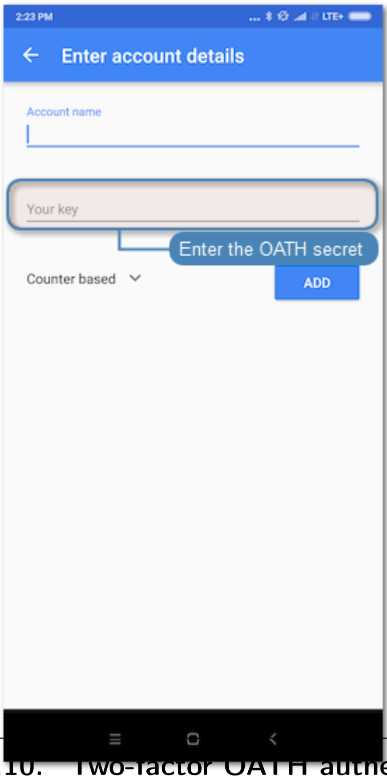
Token length: 6 characters

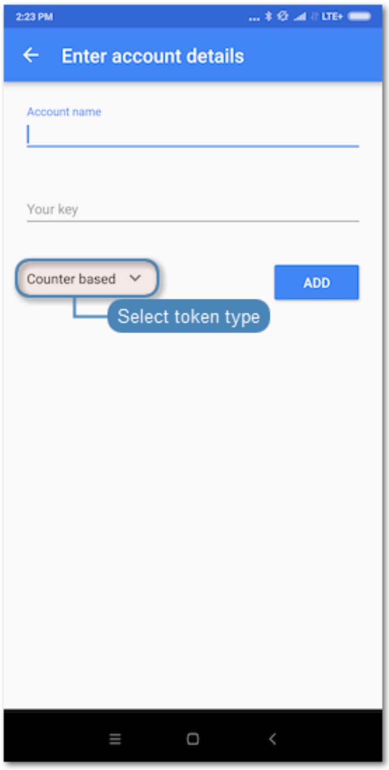
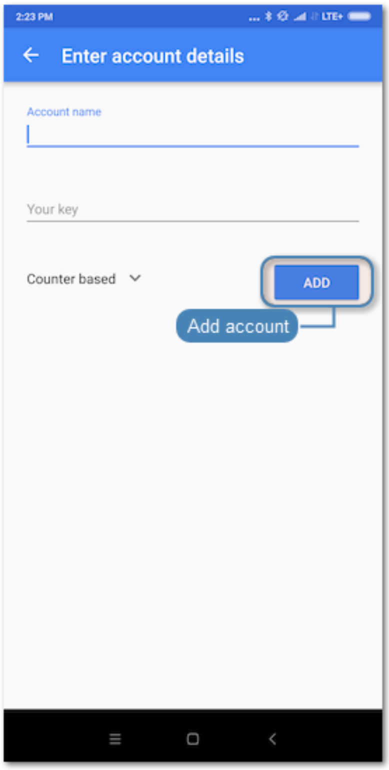
Define the number of characters of the dynamic password's part

9. Click *Save*.

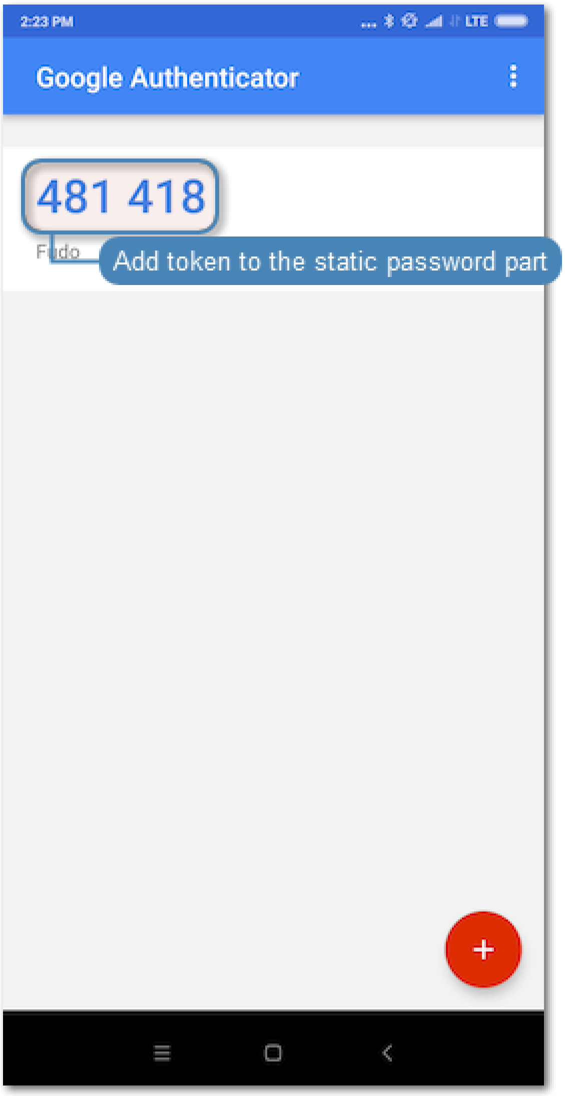
10. Launch *Google Authenticator*.

Manual entry	QR Code
• Select *Enter a provided key*.  2:22 PM Add an account You can add an account selecting one of the following options: Scan a barcode Enter a provided key Select account adding method	• Click ▦ on user configuration form, next to the *Secret* field in the *Authentication* section. • Select *Scan a barcode* in *Google Authenticator* and scan the code.  2:22 PM Add an account You can add an account selecting one of the following options: Scan a barcode Enter Select account adding method

Manual entry	QR Code
- Enter account name.  2:23 PM LTE+ Enter account details Account name Provide account name Your key Counter based ADD - Enter the secret defined in OATH authentication method. **Note:** Click 👁 on the user configuration form in the *Authentication* section to reveal the secret.  2:23 PM LTE+ Enter account details Account name Your key Enter the OATH secret Counter based ADD	

Manual entry	QR Code
- Select *Counter based*.  2:23 PM Enter account details Account name Your key Counter based ADD Select token type - Select ADD.  2:23 PM Enter account details Account name Your key Counter based ADD Add account	

11. When logging in, the password string consists of a static password defined in the authentication method and dynamic part generated by the *Google Authenticator*, e.g. `password481418`.



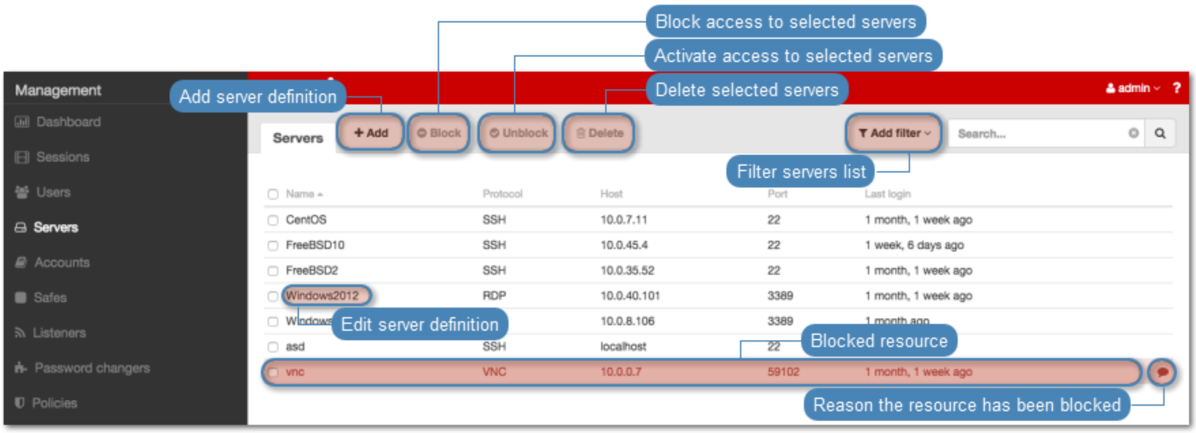
Related topics:

- *User authentication methods and modes*

CHAPTER 6

Servers

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



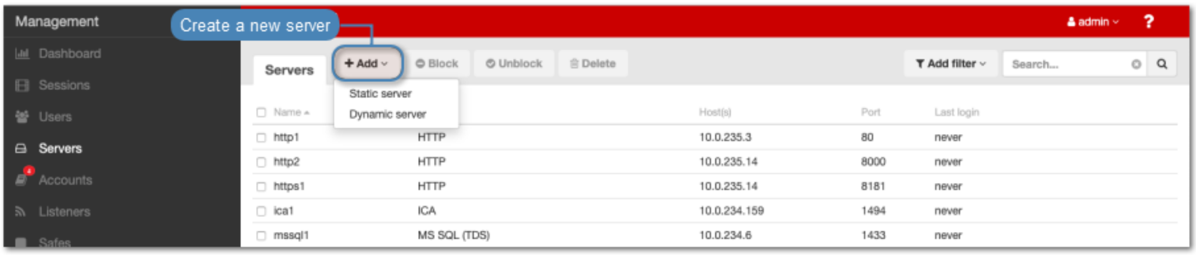
□ Name	Protocol	Host	Port	Last login
□ CentOS	SSH	10.0.7.11	22	1 month, 1 week ago
□ FreeBSD10	SSH	10.0.45.4	22	1 week, 6 days ago
□ FreeBSD2	SSH	10.0.35.52	22	1 month, 1 week ago
□ Windows2012	RDP	10.0.40.101	3389	1 month, 1 week ago
□ Windows		10.0.8.106	3389	1 month ago
□ asd	SSH	localhost	22	
□ vnc	VNC	10.0.0.7	59102	1 month, 1 week ago

6.1 Creating a server

6.1.1 Static server

6.1.1.1 Creating a Citrix server

1. Select *Management* > *Servers*.
2. Click + *Add* and select *Static server*.



Name		Host(s)	Port	Last login
http1	HTTP	10.0.235.3	80	never
http2	HTTP	10.0.235.14	8000	never
https1	HTTP	10.0.235.14	8181	never
ica1	ICA	10.0.234.159	1494	never
mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.

4. Enter optional description, which will help identifying this server object.

5. Select *Blocked* option to disable access to server after it's created.

5. Select `Citrix StoreFront (HTTP)` from the *Protocol* drop-down list.

6. Enter value of the *HTTP timeout* parameter, determining the time period of inactivity (expressed in seconds), after which the user will have to authenticate again.

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

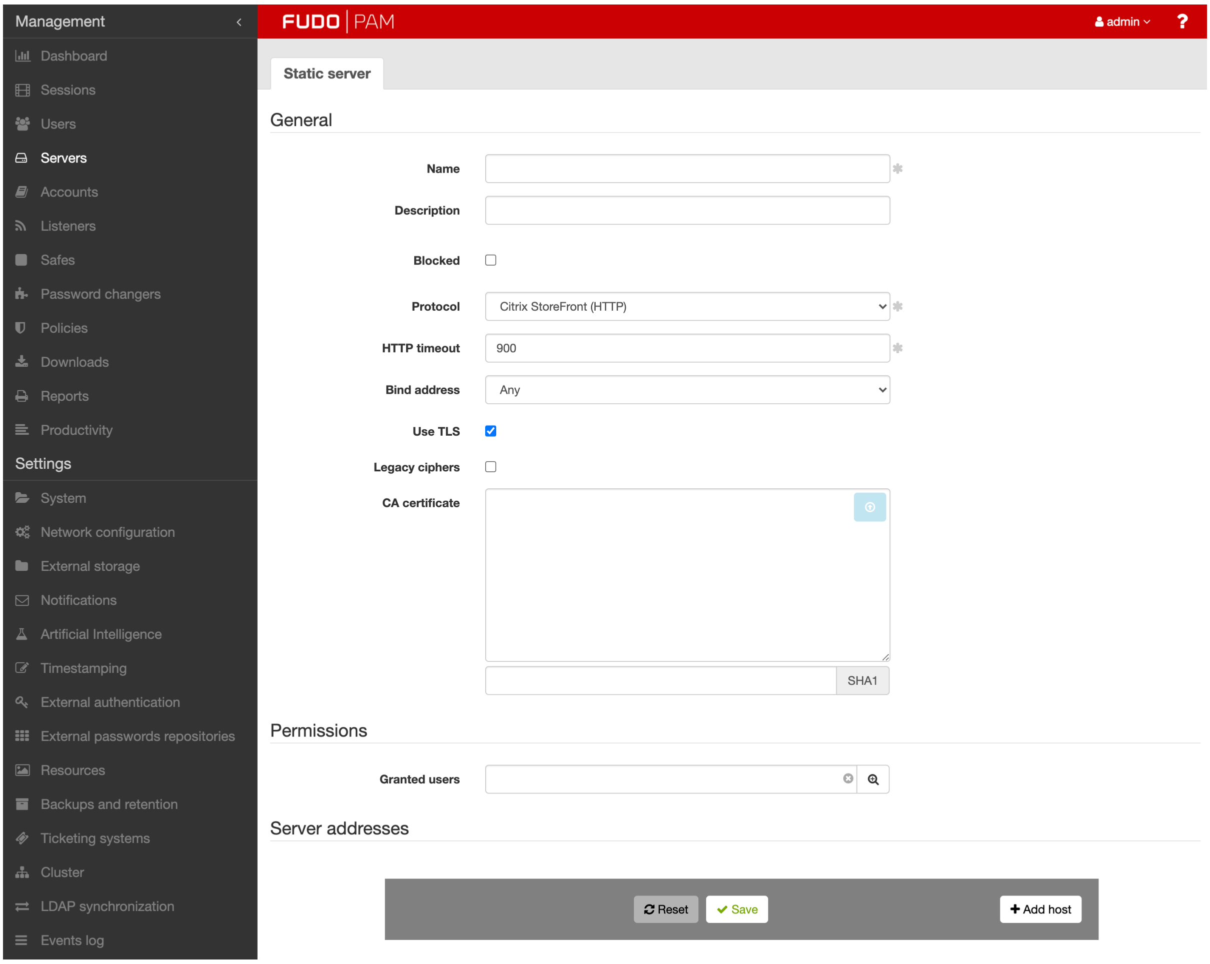
Note:

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

8. Select the *Use TLS* option to connect to monitored server over TLS.

- Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
- In the *CA certificate* field, click ⬆ to upload a certificate.

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



General

Name: *

Description:

Blocked: ☐

Protocol: Citrix StoreFront (HTTP) *

HTTP timeout: 900 *

Bind address: Any

Use TLS: ☑

Legacy ciphers: ☐

CA certificate:

SHA1

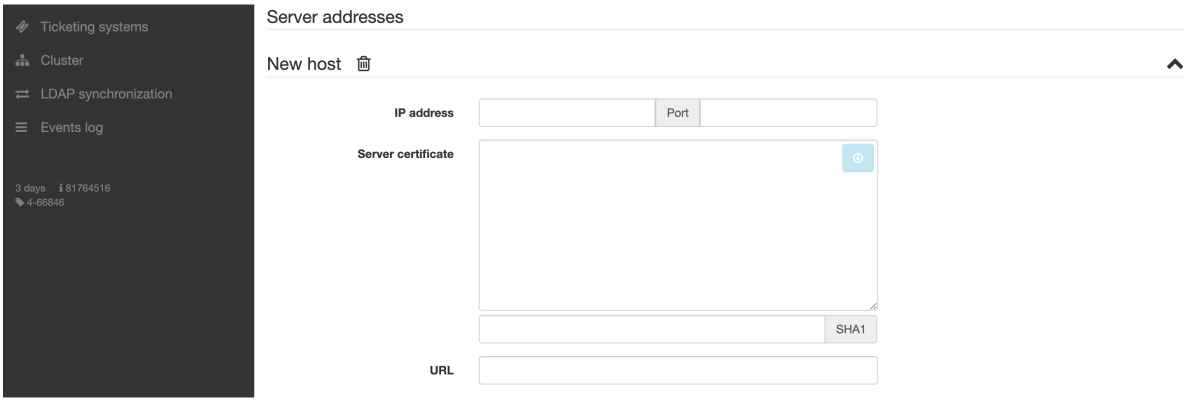
Permissions

Granted users:

Server addresses

10. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.
- If *Use TLS* option above was chosen, additionally click ⬇ to download server key or paste the certificate into the text area.
- In the *URL* field, enter Citrix StoreFront base URL.



Server addresses

New host

IP address: Port

Server certificate:

SHA1

URL:

11. Click *Save*.

Related topics:

- *Data model*

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

6.1.1.2 Creating an HTTP server

Note:

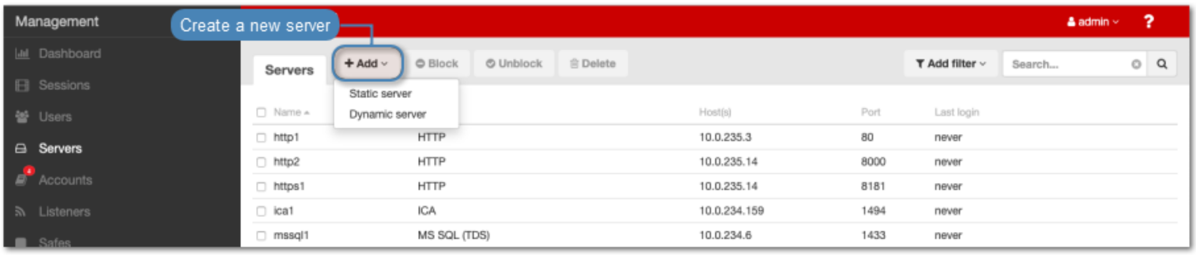
- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.

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

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

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

1. Select *Management* > *Servers*.
2. Click *+ Add* and select *Static server*.



Name		Host(s)	Port	Last login
http1	HTTP	10.0.235.3	80	never
http2	HTTP	10.0.235.14	8000	never
https1	HTTP	10.0.235.14	8181	never
ica1	ICA	10.0.234.159	1494	never
mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.
5. Select *Blocked* option to disable access to server after it's created.
6. Select `HTTP` from the *Protocol* drop-down list.
7. Enter value of the *HTTP timeout* parameter, determining the time period of inactivity (expressed in seconds), after which the user will have to authenticate again.

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

Note:

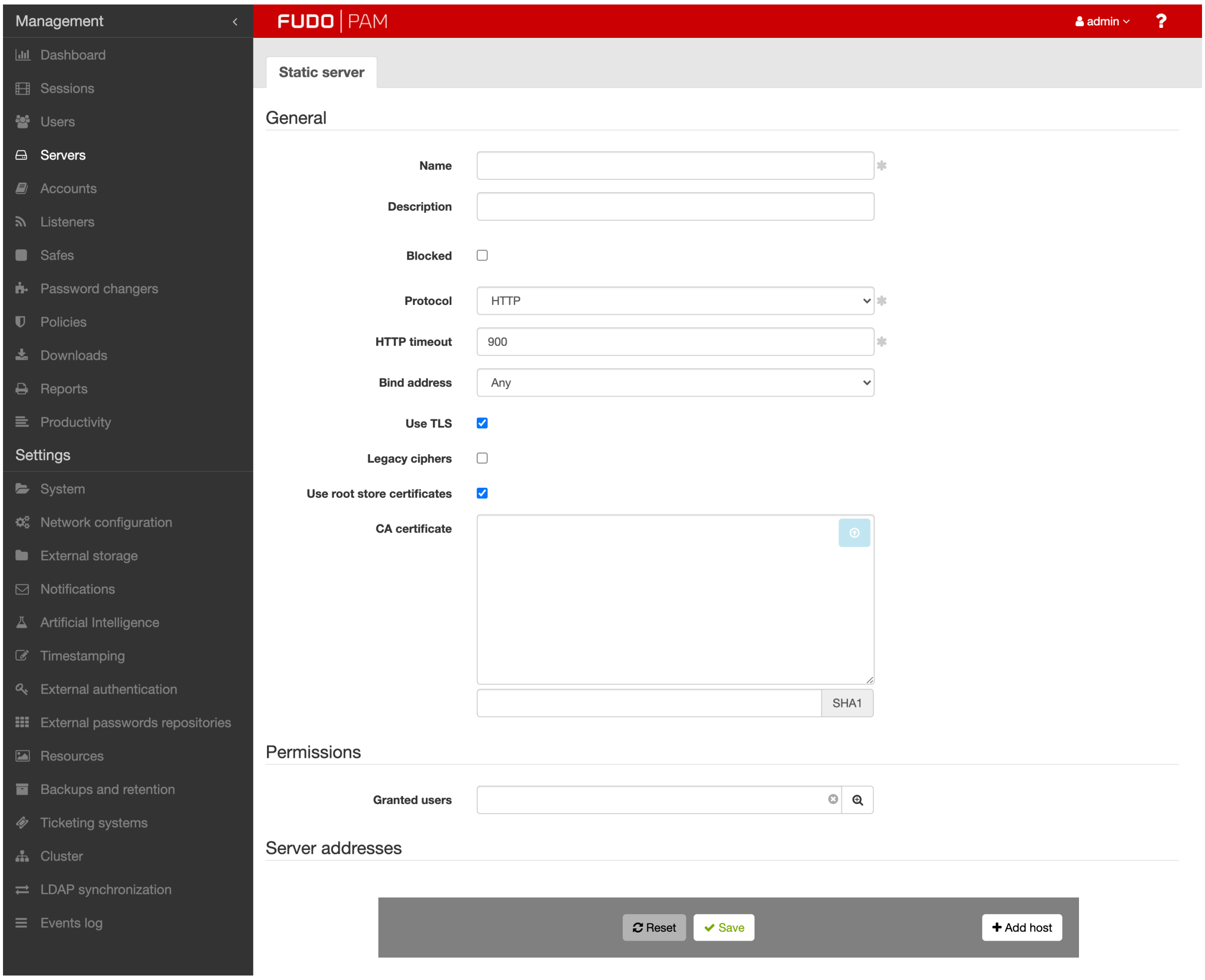
- The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make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

---

9. Select the *Use TLS* option to connect to monitored server over TLS.

- Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
- Select *Use root store certificates* option.
- In the *CA certificate* field, click ⬆ to upload a certificate.

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



General

Name: *

Description:

Blocked: ☐

Protocol: HTTP *

HTTP timeout: 900 *

Bind address: Any

Use TLS: ☑

Legacy ciphers: ☐

Use root store certificates: ☑

CA certificate: SHA1

Permissions

Granted users:

Server addresses

11. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.
- If *Use TLS* option above was chosen, additionally click ⊙ to download server key or paste the certificate into the text area.
- In the *HTTP host* field, provide the HTTP host header value.

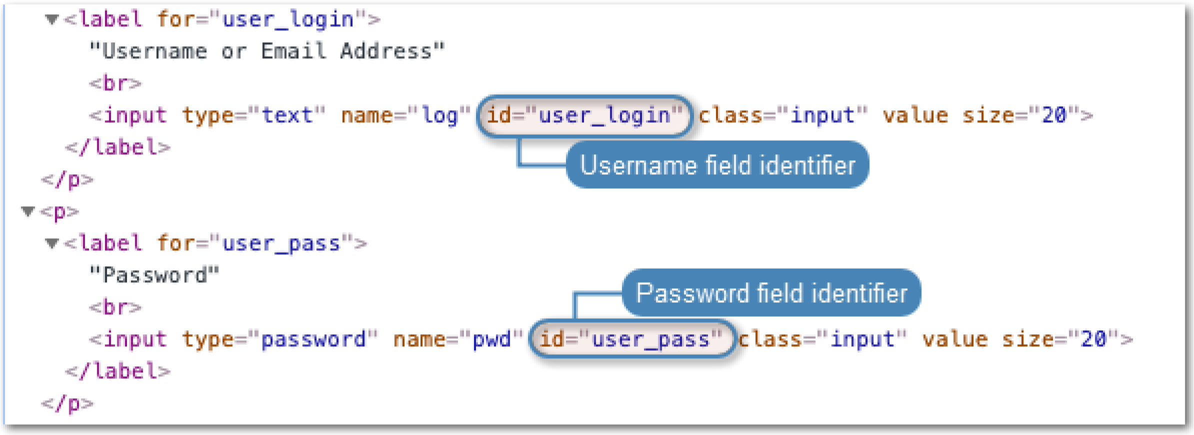
Note:

The HTTP host header determines the requested content in case there are many web sites hosted on the specified server.

- From the *Authentication method* drop-down list, select one of the pre-defined online services or select `Other` to provide custom login page details.

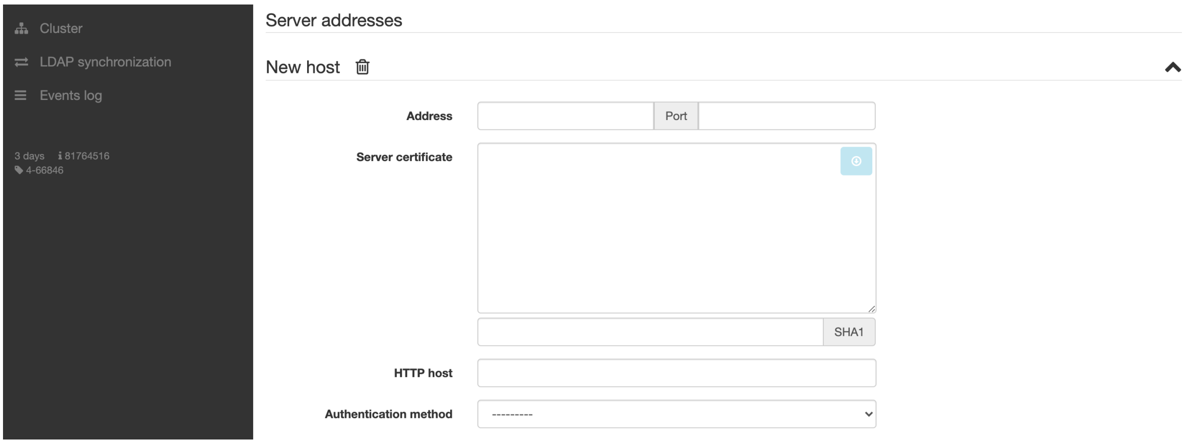
Note: Authentication method enables seamless login credentials substitution when establishing a monitored HTTP connection.

In case of custom login credentials, the login and the password fields are identified using CSS selectors.



```
  ▼<label for="user_login">
      "Username or Email Address"
      <br>
      <input type="text" name="log" id="user_login" class="input" value size="20">
    </label>
  </p>
▼<p>
  ▼<label for="user_pass">
      "Password"
      <br>
      <input type="password" name="pwd" id="user_pass" class="input" value size="20">
    </label>
  </p>
```

For more information on CSS selectors refer to https://www.w3.org/TR/selectors-3/



Server addresses

New host

Address

Port

Server certificate

SHA1

HTTP host

Authentication method ---------

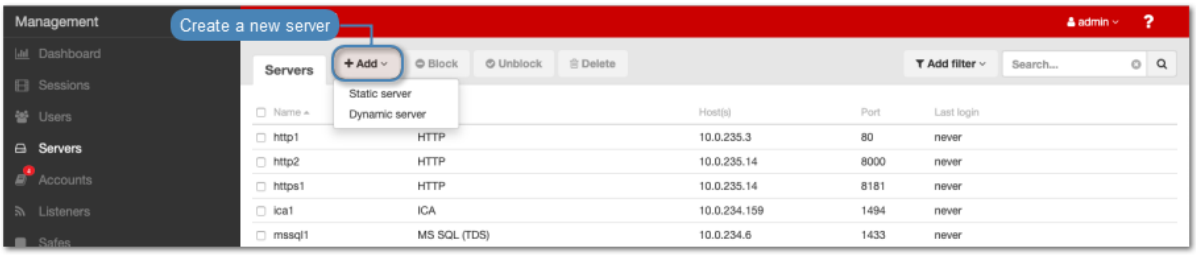
12. Click *Save*.

Related topics:

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

6.1.1.3 Creating an ICA server

1. Select *Management* > *Servers*.
2. Click + *Add* and select *Static server*.



Name ▴		Host(s)	Port	Last login
http1	HTTP	10.0.235.3	80	never
http2	HTTP	10.0.235.14	8000	never
https1	HTTP	10.0.235.14	8181	never
ica1	ICA	10.0.234.159	1494	never
mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.
5. Select *Blocked* option to disable access to server after it's created.
6. Select `ICA` from the *Protocol* drop-down list.
7. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

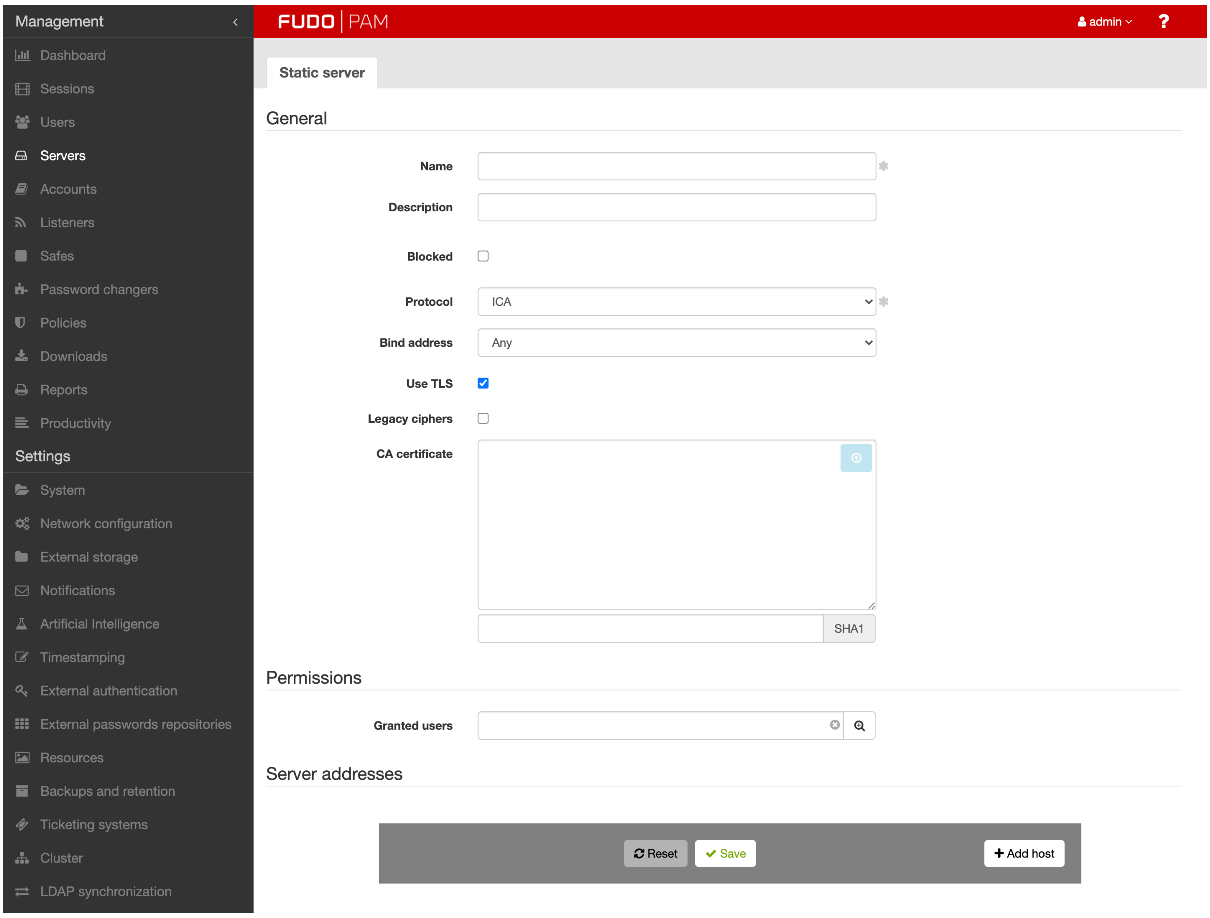
Note:

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

8. Select the *Use TLS* options to connect to monitored server over TLS.

- Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
- In the *CA certificate* field, click ⊙ to upload a certificate.

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



General

Name

Description

Blocked ☐

Protocol: ICA

Bind address: Any

Use TLS ☑

Legacy ciphers ☐

CA certificate

SHA1

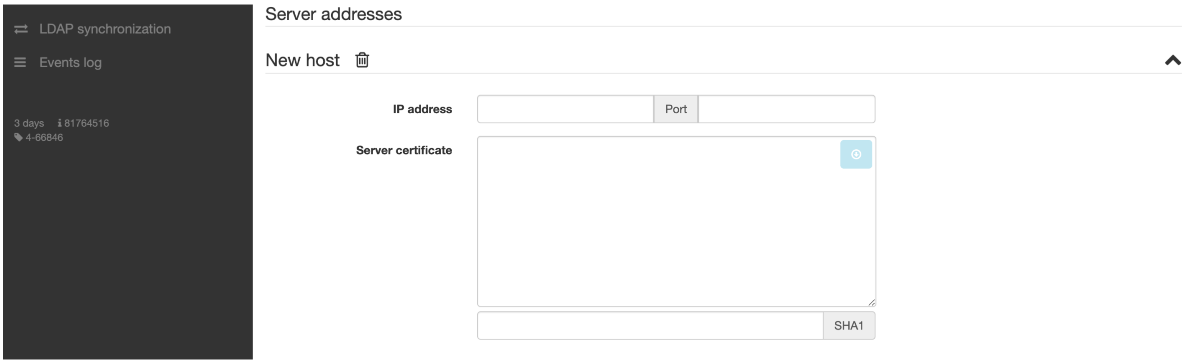
Permissions

Granted users

Server addresses

10. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.
- If *Use TLS* option above was chosen, additionally click ⬇ to download server key or paste the certificate into the text area.



Server addresses

New host

IP address

Port

Server certificate

SHA1

11. Click *Save*.

Related topics:

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

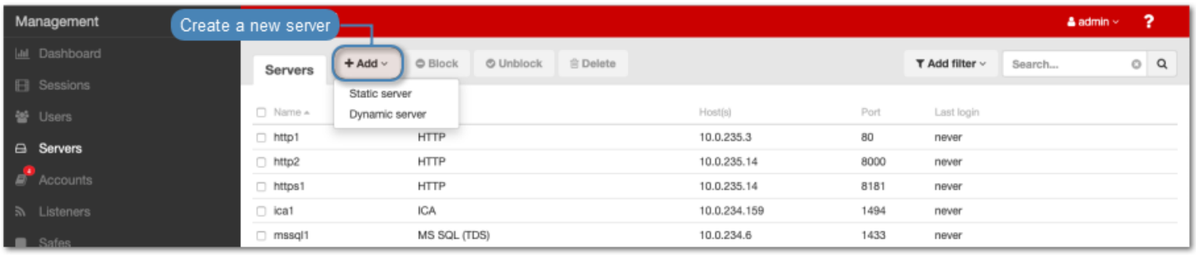
- *ICA*

6.1.1.4 Creating a Modbus server

Note:

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

1. Select *Management > Servers*.
2. Click *+ Add* and select *Static server*.



Name		Host(s)	Port	Last login
http1	HTTP	10.0.235.3	80	never
http2	HTTP	10.0.235.14	8000	never
https1	HTTP	10.0.235.14	8181	never
ica1	ICA	10.0.234.159	1494	never
mssql1	MS SQL (TDS)	10.0.234.6	1433	never

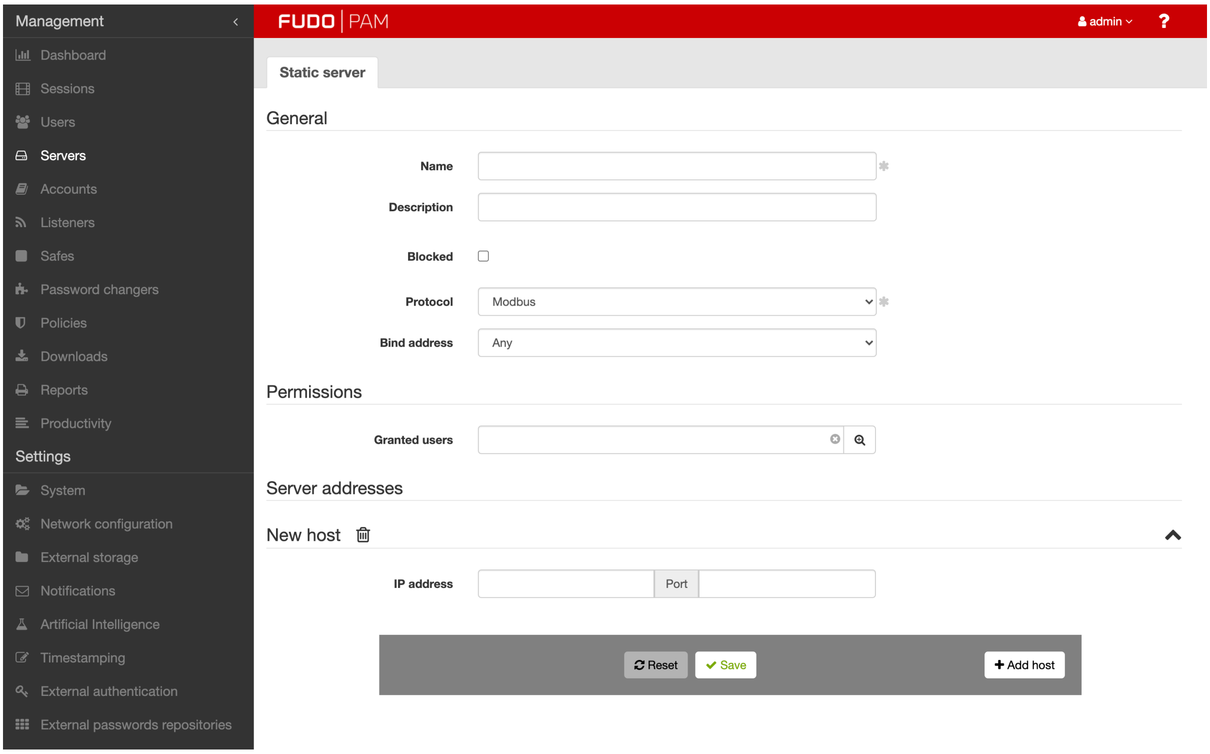
3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.
5. Select *Blocked* option to disable access to server after it's created.
6. Select `Modbus` from the *Protocol* drop-down list.
7. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

Note:

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

8. In the *Permissions* section, add users allowed to manage this object.
9. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.



General

Name

Description

Blocked □

Protocol: Modbus

Bind address: Any

Permissions

Granted users

Server addresses

New host

IP address | Port

10. Click *Save*.

Related topics:

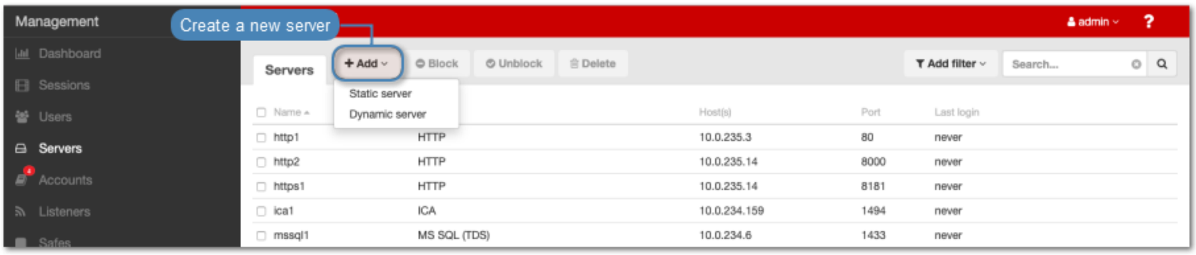
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

6.1.1.5 Creating a MS SQL server

Note:

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

1. Select *Management > Servers*.
2. Click *+ Add* and select *Static server*.



□ Name		Host(s)	Port	Last login
□ http1	HTTP	10.0.235.3	80	never
□ http2	HTTP	10.0.235.14	8000	never
□ https1	HTTP	10.0.235.14	8181	never
□ ica1	ICA	10.0.234.159	1494	never
□ mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.
5. Select *Blocked* option to disable access to server after it's created.
6. Select `MS SQL (TDS)` from the *Protocol* drop-down list.
7. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

Note:

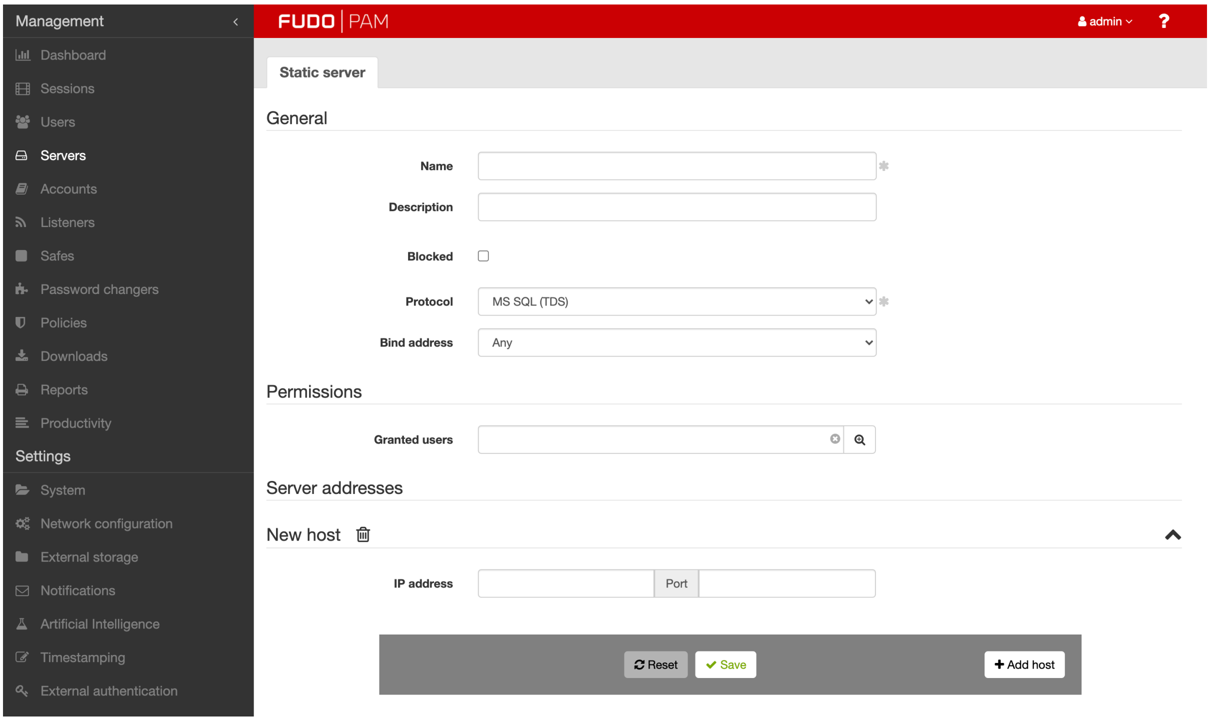
- The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make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

---

8. In the *Permissions* section, add users allowed to manage this object.
9. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.

10. Click *Save*.



General

Name	
Description	
Blocked	□
Protocol	MS SQL (TDS)
Bind address	Any

Permissions

Granted users	

Server addresses

New host

IP address	Port

Related topics:

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

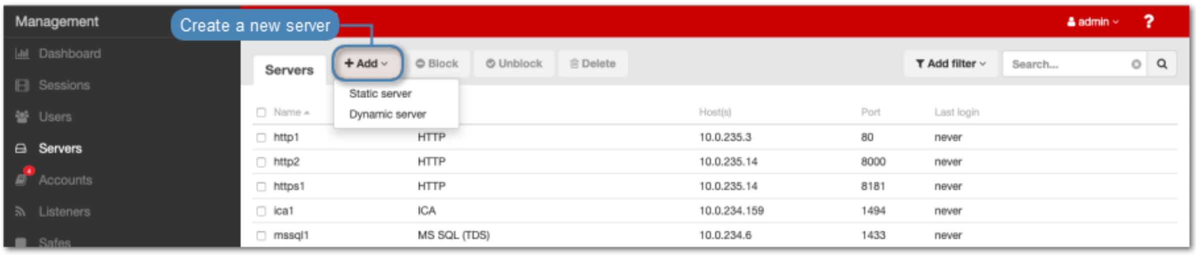
6.1.1.6 Creating a MySQL server

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

Note:

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

1. Select *Management* > *Servers*.
2. Click + *Add* and select *Static server*.



Name		Host(s)	Port	Last login
http1	HTTP	10.0.235.3	80	never
http2	HTTP	10.0.235.14	8000	never
https1	HTTP	10.0.235.14	8181	never
ica1	ICA	10.0.234.159	1494	never
mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.
5. Select *Blocked* option to disable access to server after it's created.
6. Select `MySQL` from the *Protocol* drop-down list.
7. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

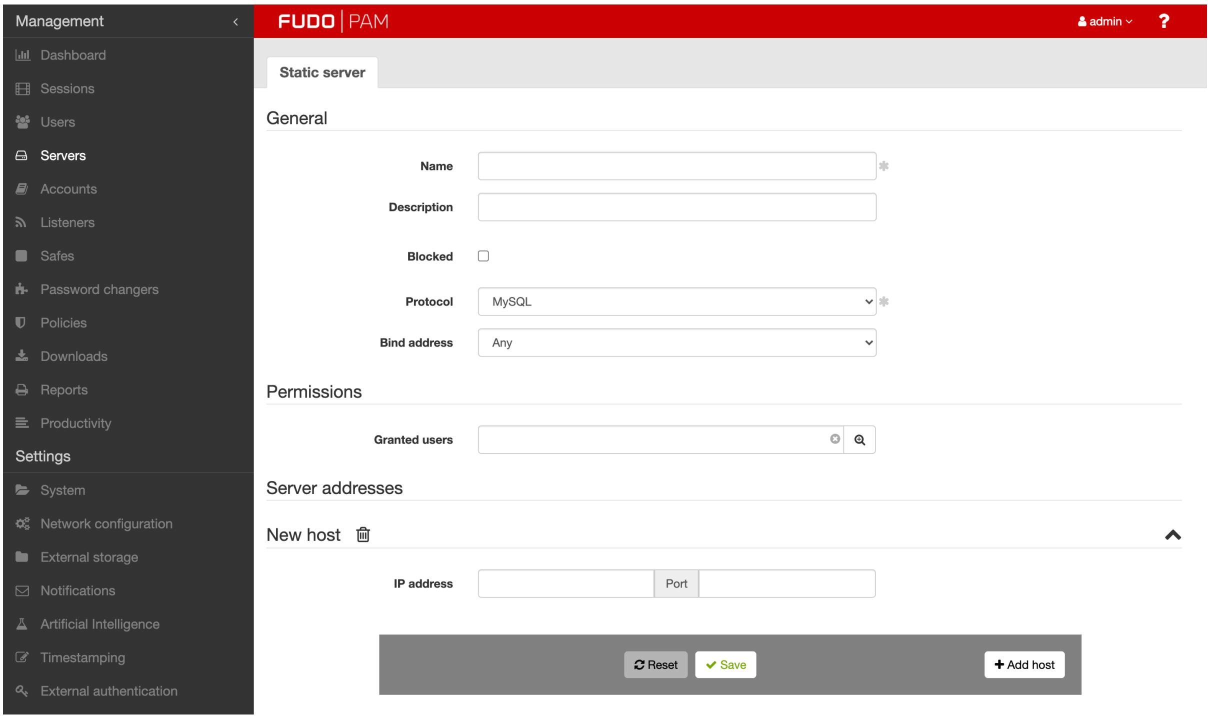
Note:

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

8. In the *Permissions* section, add users allowed to manage this object.
9. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.

10. Click *Save*.



General

Name	
Description	
Blocked	□
Protocol	MySQL
Bind address	Any

Permissions

Granted users	

Server addresses

New host

IP address		Port	

Related topics:

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

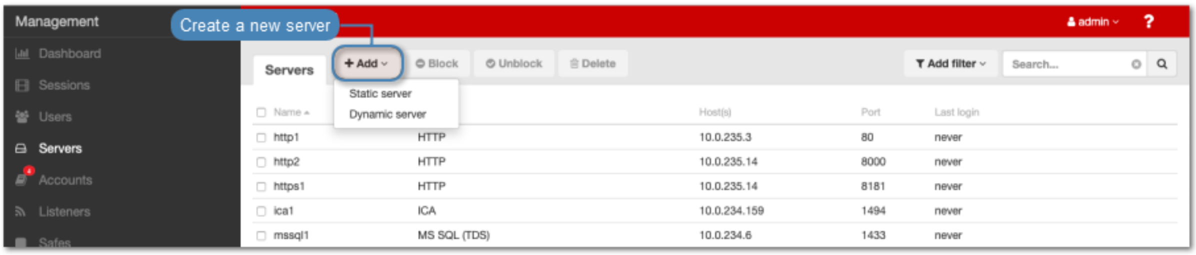
6.1.1.7 Creating an RDP server

Note:

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

---

1. Select *Management* > *Servers*.
2. Click + *Add* and select *Static server*.



Name		Host(s)	Port	Last login
http1	HTTP	10.0.235.3	80	never
http2	HTTP	10.0.235.14	8000	never
https1	HTTP	10.0.235.14	8181	never
ica1	ICA	10.0.234.159	1494	never
mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. In the *General* section, enter server's unique name.
4. Enter optional description, which will help identifying this server object.
4. Select *Blocked* option to disable access to server after it's created.
5. Select `RDP` from the *Protocol* drop-down list.
6. From the `Security` drop-down list, select RDP connection security mode.

Note: Security mode must match the security mode setting in the *RDP listener configuration*.

In case *Enhanced RDP Security (TLS)* or *Enhanced RDP Security (TLS) + NLA* option is chosen, select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing RDP connections.

---

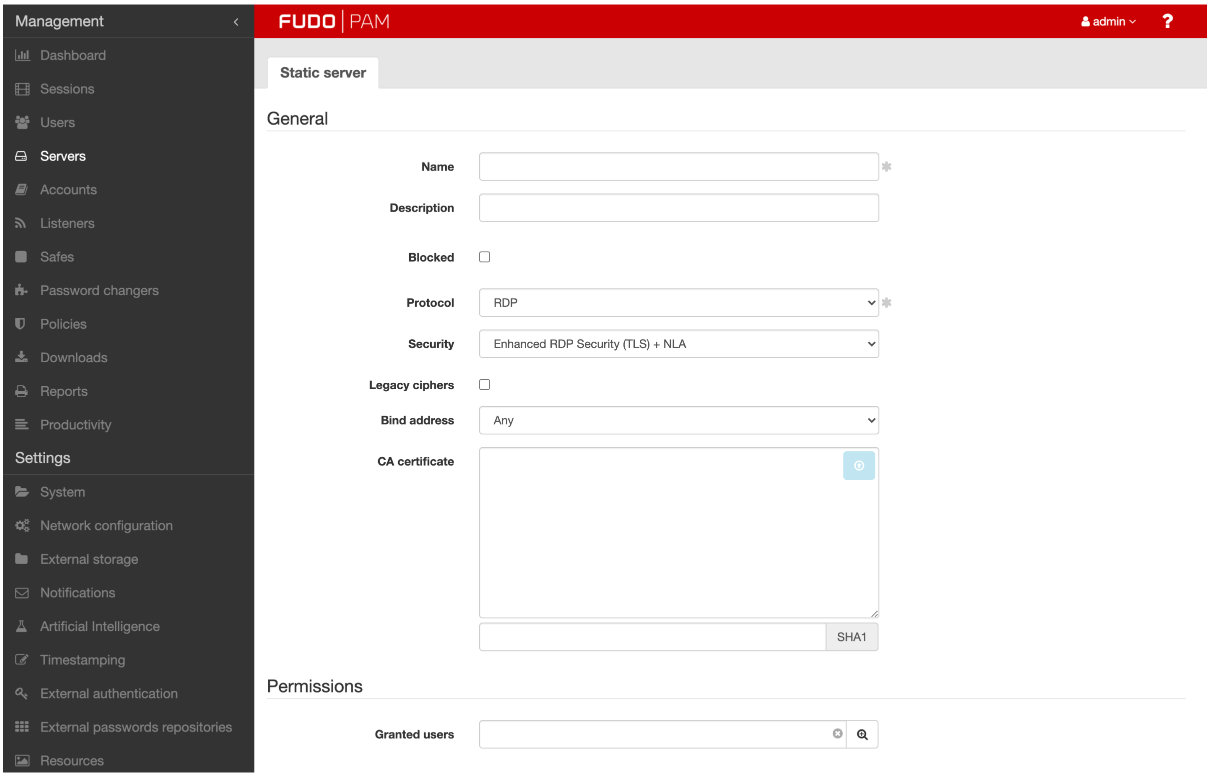
7. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

Note:

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

---

8. Click ⬆ to upload CA certificate.
9. In the *Permissions* section, add users allowed to manage this object.



General

Name	
Description	
Blocked	□
Protocol	RDP
Security	Enhanced RDP Security (TLS) + NLA
Legacy ciphers	□
Bind address	Any
CA certificate	SHA1

Permissions

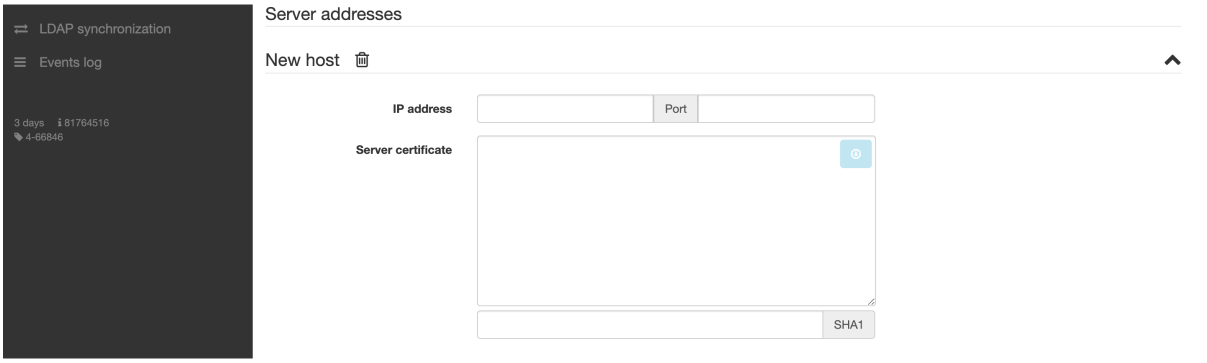
Granted users	

10. In the *Remote applications* section, click +Add application to add a Remote Application, which will be accessible in the *User Portal*.

- Enter application's *Name*, provide *Path* to the executable file and *Arguments* within two %% symbols, e.g., `%%variable%%`.
- Choose *Object type* and *Object property* for each of your Argument. You can encrypt each of the given argument by selecting *Encrypt* option.

12. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.
- Click ⊙ to download server key or paste the certificate into the text area.



Server addresses

New host

IP address	Port
Server certificate	SHA1

13. Click *Save*.

14. Select *Management > Accounts*.

- Pick an Account with RDP server chosen
- Scroll down to *Remote applications* section and Add remote application

- Select your predefined RemoteApp and fill the variables definition with your values.

Related topics:

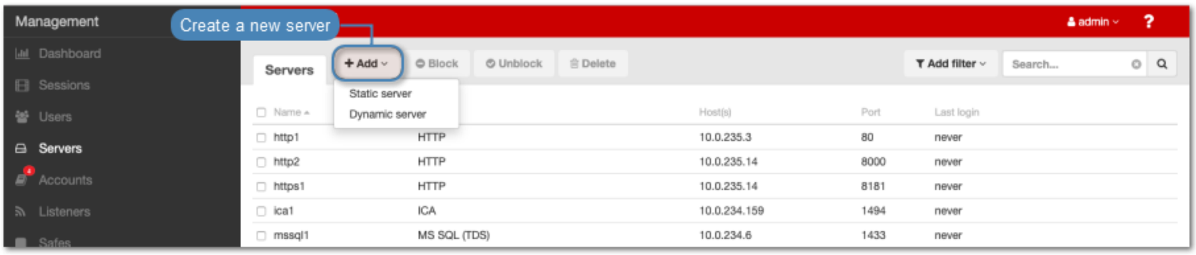
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

6.1.1.8 Creating an SSH server

Note:

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

1. Select *Management* > *Servers*.
2. Click + *Add* and select *Static server*.



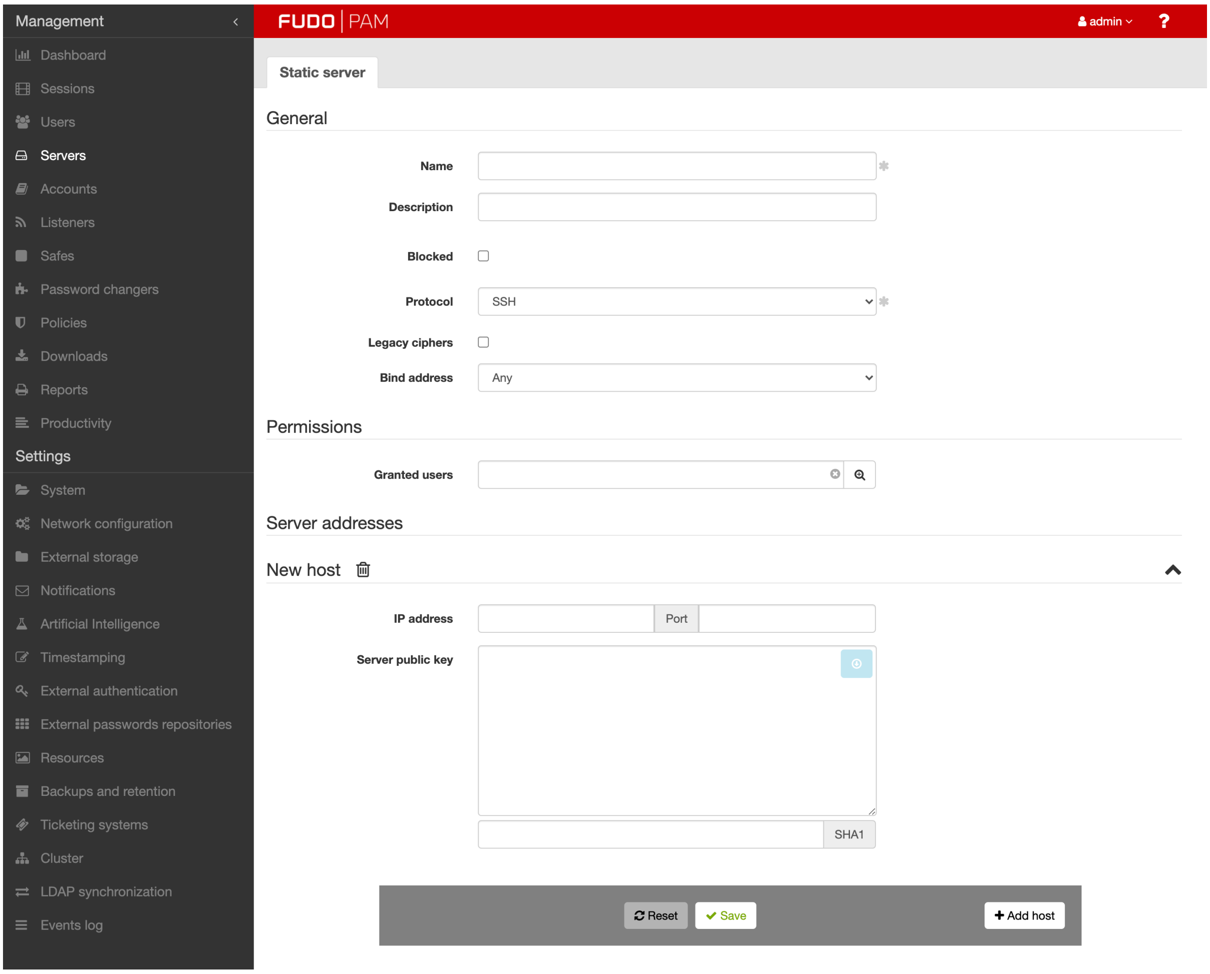
Name		Host(s)	Port	Last login
http1	HTTP	10.0.235.3	80	never
http2	HTTP	10.0.235.14	8000	never
https1	HTTP	10.0.235.14	8181	never
ica1	ICA	10.0.234.159	1494	never
mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.
5. Select *Blocked* option to disable access to server after it's created.
6. Select `SSH` from the *Protocol* drop-down list.
7. Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing SSH connections.
8. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

Note:

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

9. In the *Permissions* section, add users allowed to manage this object.
10. Click an *Add host* button in order to add address(es) into the *Server adresses* section.
    - Enter server's IP address and port number.
    - Click the fetch key icon to download server's public key or paste the certificate into the text area.



Static server

General

Name

Description

Blocked ☐

Protocol: SSH

Legacy ciphers ☐

Bind address: Any

Permissions

Granted users

Server addresses

New host

IP address | Port

Server public key

SHA1

Reset | Save | Add host

11. Click *Save*.

Related topics:

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

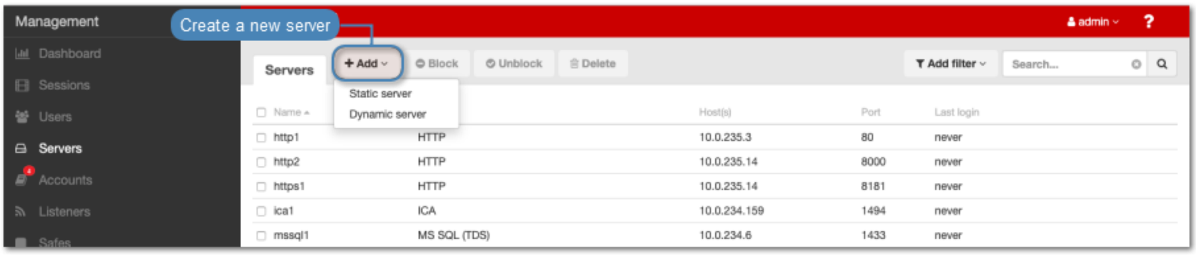
- *Safes*
- *Accounts*

6.1.1.9 Creating a Telnet server

Note:

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

1. Select *Management* > *Servers*.
2. Click + *Add* and select *Static server*.



□ Name		Host(s)	Port	Last login
□ http1	HTTP	10.0.235.3	80	never
□ http2	HTTP	10.0.235.14	8000	never
□ https1	HTTP	10.0.235.14	8181	never
□ ica1	ICA	10.0.234.159	1494	never
□ mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.
5. Select *Blocked* option to disable access to server after it's created.
6. Select `Telnet` from the *Protocol* drop-down list.
7. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

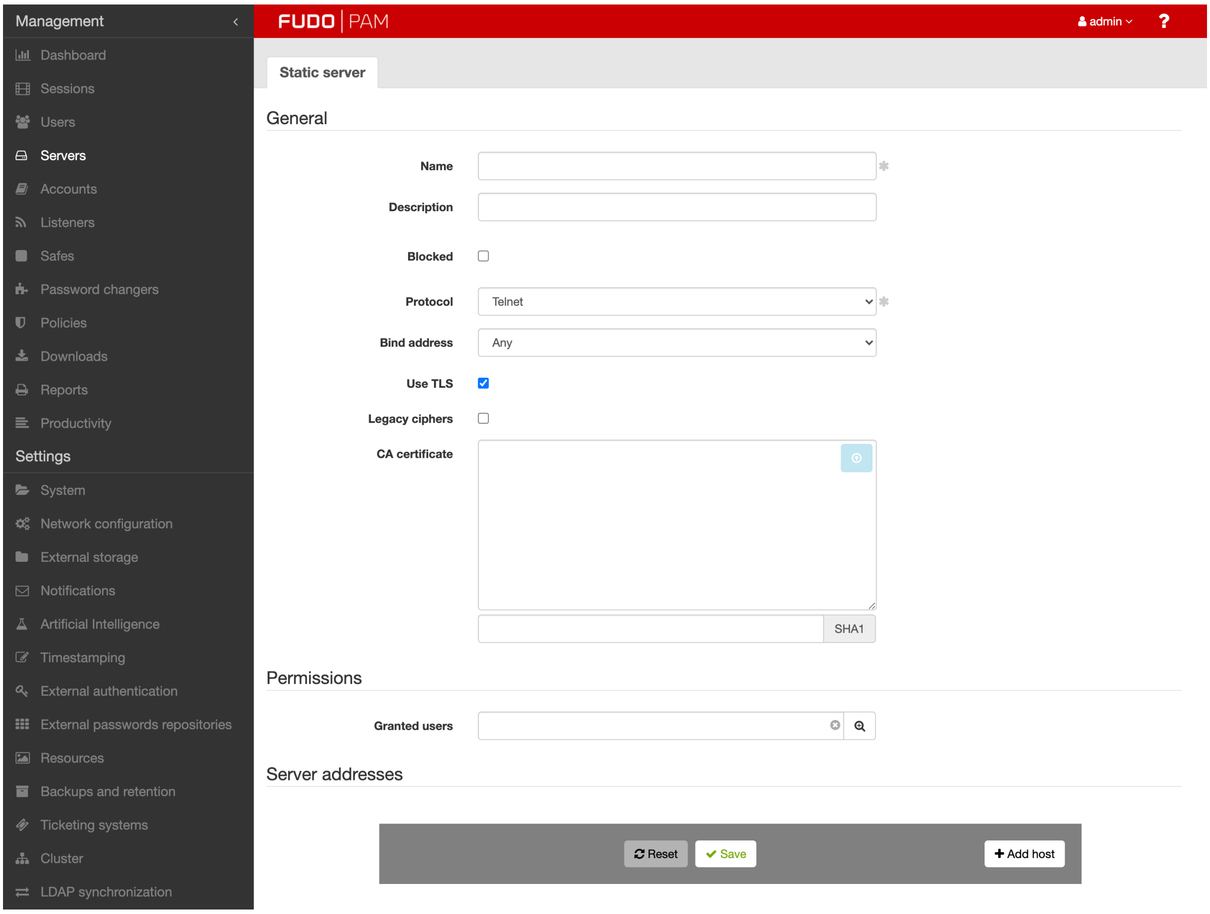
Note:

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

8. Select the *Use TLS* option to connect to monitored server over TLS.

- Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
- In the *CA certificate* field, click ⬆ to upload a certificate.

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



General

Name
Description
Blocked □
Protocol: Telnet
Bind address: Any
Use TLS ☑
Legacy ciphers □
CA certificate
SHA1

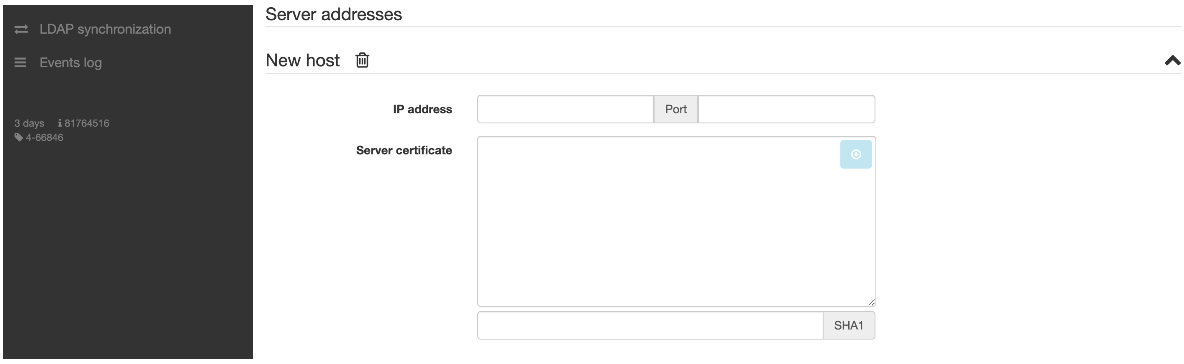
Permissions

Granted users

Server addresses

10. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.
- If *Use TLS* option above was chosen, additionally click ⊙ to download server key or paste the certificate into the text area.



Server addresses

New host

IP address
Port
Server certificate
SHA1

11. Click *Save*.

Related topics:

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

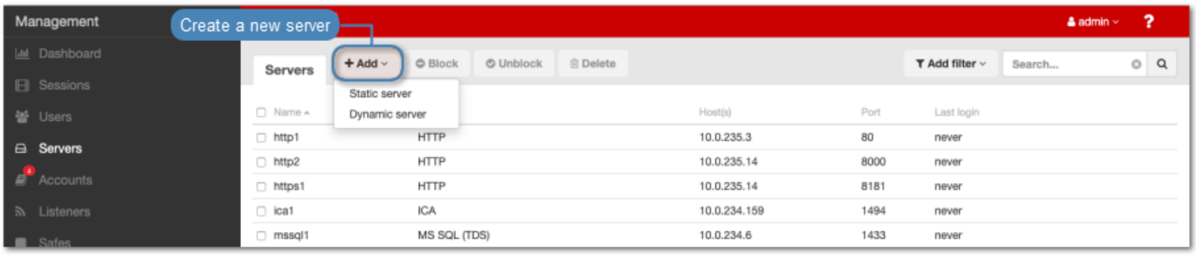
- *Listeners*
- *Safes*
- *Accounts*

6.1.1.10 Creating a Telnet 3270 server

Note:

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

1. Select *Management* > *Servers*.
2. Click + *Add* and select *Static server*.



Name		Host(s)	Port	Last login
http1	HTTP	10.0.235.3	80	never
http2	HTTP	10.0.235.14	8000	never
https1	HTTP	10.0.235.14	8181	never
ica1	ICA	10.0.234.159	1494	never
mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.
5. Select *Blocked* option to disable access to server after it's created.
6. Select `Telnet 3270` from the *Protocol* drop-down list.
7. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

Note:

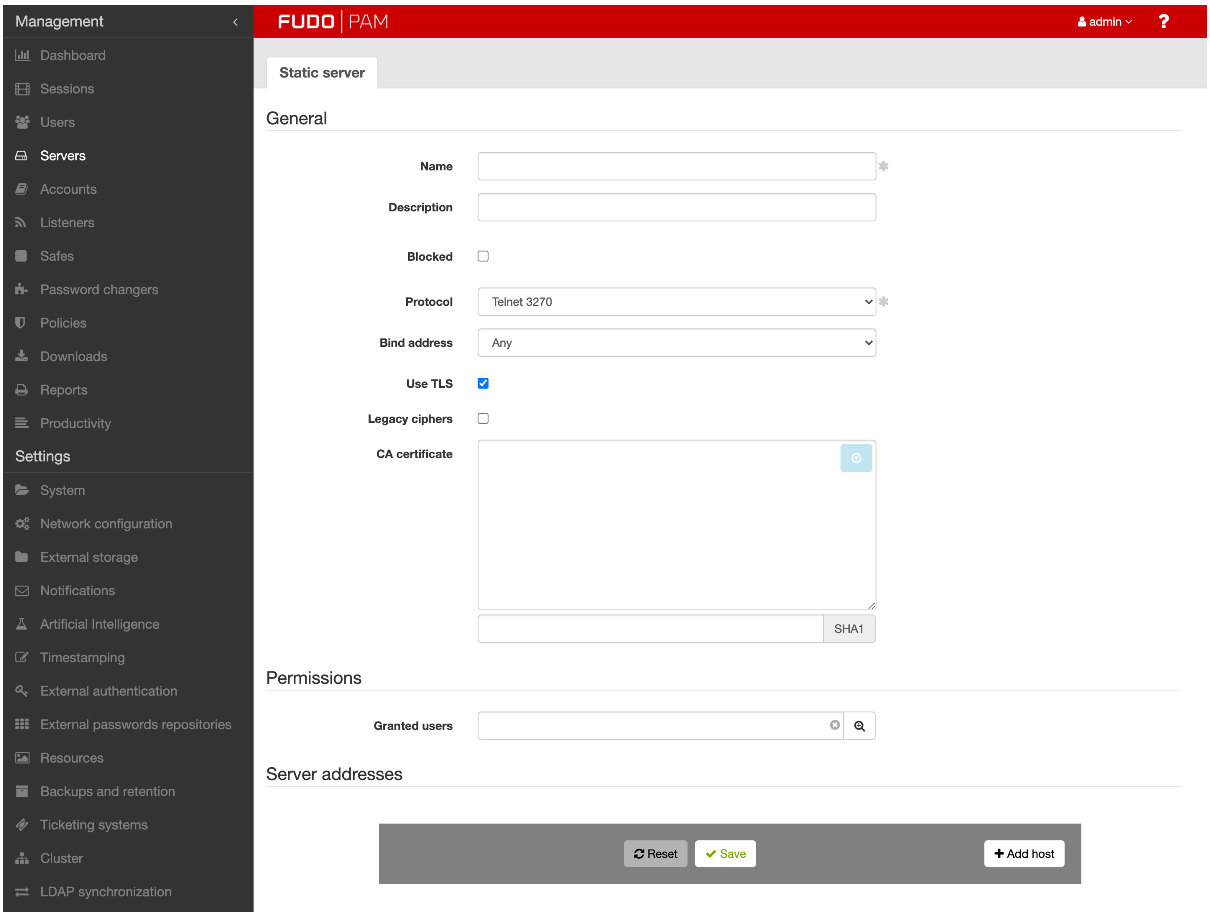
- The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make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

8. Select the *Use TLS* option to connect to monitored server over TLS.

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

- In the *CA certificate* field, click ⬆ to upload a certificate.

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



General

Name

Description

Blocked □

Protocol: Telnet 3270

Bind address: Any

Use TLS ☑

Legacy ciphers □

CA certificate

SHA1

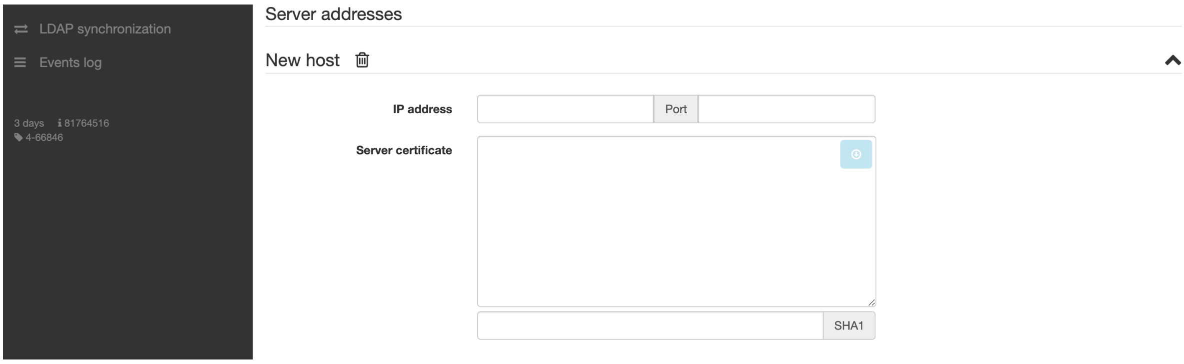
Permissions

Granted users

Server addresses

10. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.
- If *Use TLS* option above was chosen, additionally click ⬇ to download server key or paste the certificate into the text area.



Server addresses

New host

IP address

Port

Server certificate

SHA1

11. Click *Save*.

Related topics:

- *Data model*
- *System initiation*

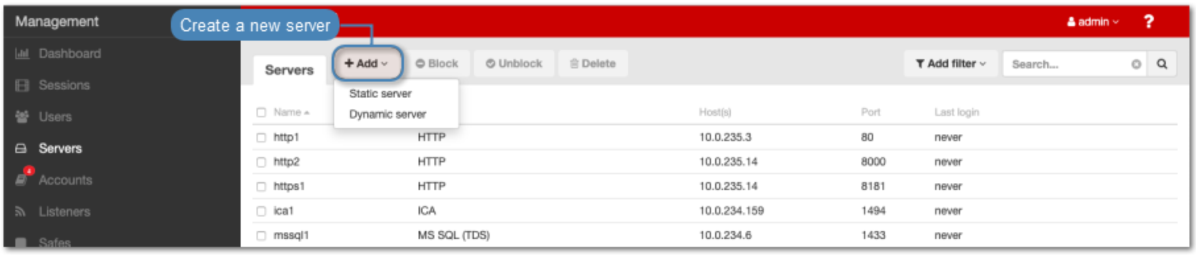
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

6.1.1.11 Creating a Telnet 5250 server

Note:

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

1. Select *Management > Servers*.
2. Click *+ Add* and select *Static server*.



Name		Host(s)	Port	Last login
□ http1	HTTP	10.0.235.3	80	never
□ http2	HTTP	10.0.235.14	8000	never
□ https1	HTTP	10.0.235.14	8181	never
□ ica1	ICA	10.0.234.159	1494	never
□ mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.
5. Select *Blocked* option to disable access to server after it's created.
6. Select `Telnet 5250` from the *Protocol* drop-down list.
7. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

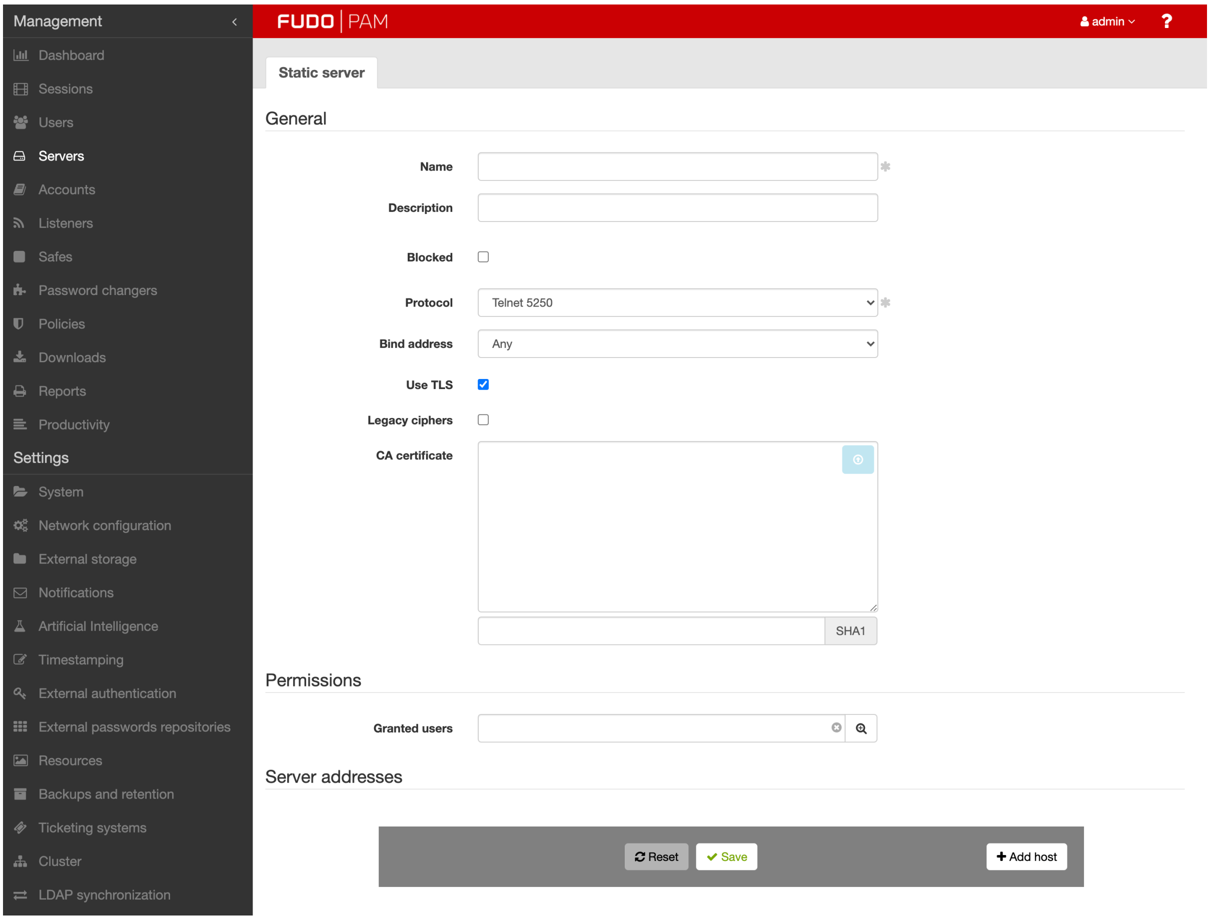
Note:

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

8. Select the *Use TLS* option to connect to monitored server over TLS.

- Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
- In the *CA certificate* field, click ⬆ to upload a certificate.

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



General

Name	
Description	
Blocked	□
Protocol	Telnet 5250
Bind address	Any
Use TLS	☑
Legacy ciphers	□
CA certificate	SHA1

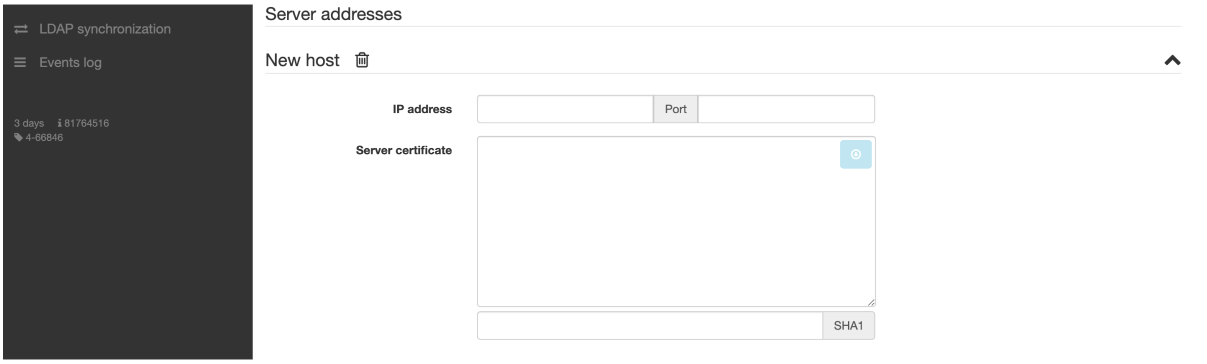
Permissions

Granted users	

Server addresses

10. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.
- If *Use TLS* option above was chosen, additionally click ⬇ to download server key or paste the certificate into the text area.



Server addresses

New host

IP address	Port
Server certificate	SHA1

11. Click *Save*.

Related topics:

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

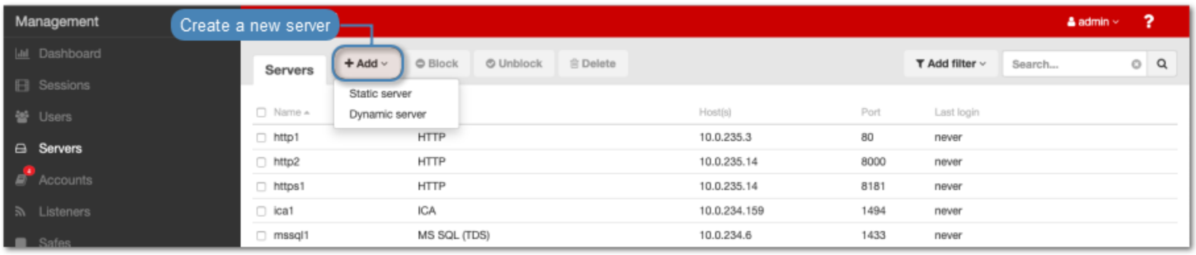
6.1.1.12 Creating a VNC server

Note:

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

---

1. Select *Management > Servers.*
2. Click *+ Add* and select *Static server.*



Name		Host(s)	Port	Last login
http1	HTTP	10.0.235.3	80	never
http2	HTTP	10.0.235.14	8000	never
https1	HTTP	10.0.235.14	8181	never
ica1	ICA	10.0.234.159	1494	never
mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.
5. Select *Blocked* option to disable access to server after it's created.
6. Select `VNC` from the *Protocol* drop-down list.
7. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

Note:

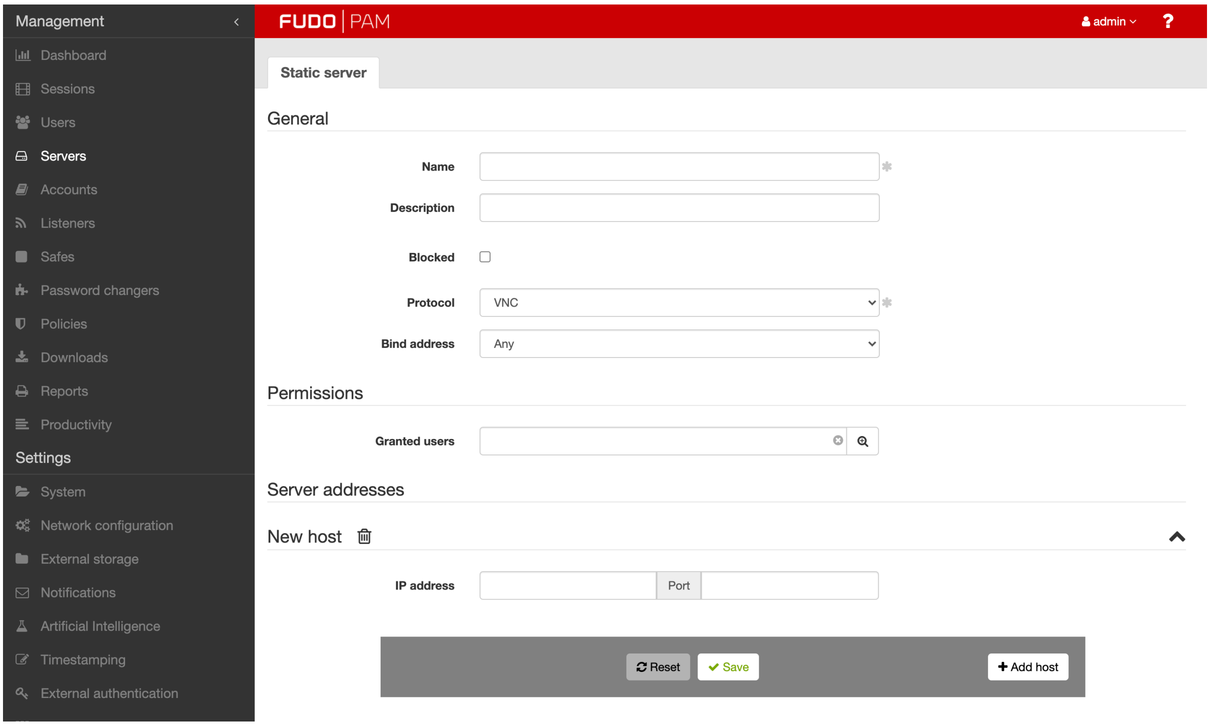
- The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make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

---

8. In the *Permissions* section, add users allowed to manage this object.
9. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.

10. Click *Save*.



General

Name: *

Description:

Blocked: □

Protocol: VNC *

Bind address: Any

Permissions

Granted users:

Server addresses

New host

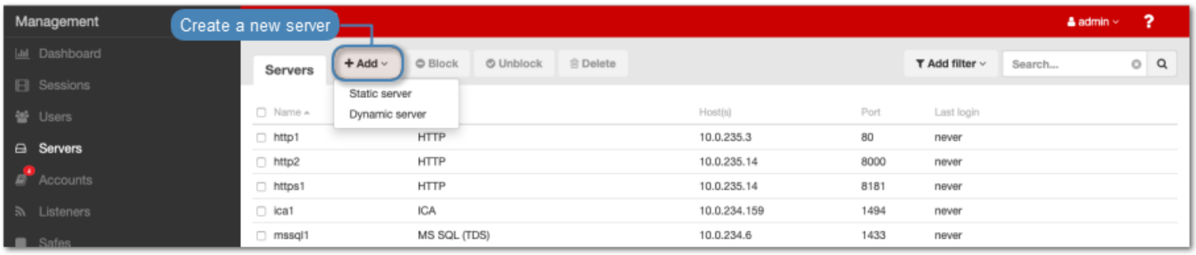
IP address: Port

Related topics:

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

6.1.1.13 Creating a TCP server

1. Select *Management > Servers*.
2. Click *+ Add* and select *Static server*.



Name ▲		Host(s)	Port	Last login
□ http1	HTTP	10.0.235.3	80	never
□ http2	HTTP	10.0.235.14	8000	never
□ https1	HTTP	10.0.235.14	8181	never
□ ica1	ICA	10.0.234.159	1494	never
□ mssql1	MS SQL (TDS)	10.0.234.6	1433	never

3. Enter server's unique name.
4. Enter optional description, which will help identifying this server object.

5. Select *Blocked* option to disable access to server after it's created.
6. Select `TCP` from the *Protocol* drop-down list.
7. From the *Bind address* drop-down list, select Fudo PAM IP address used for communicating with this server.

Note:

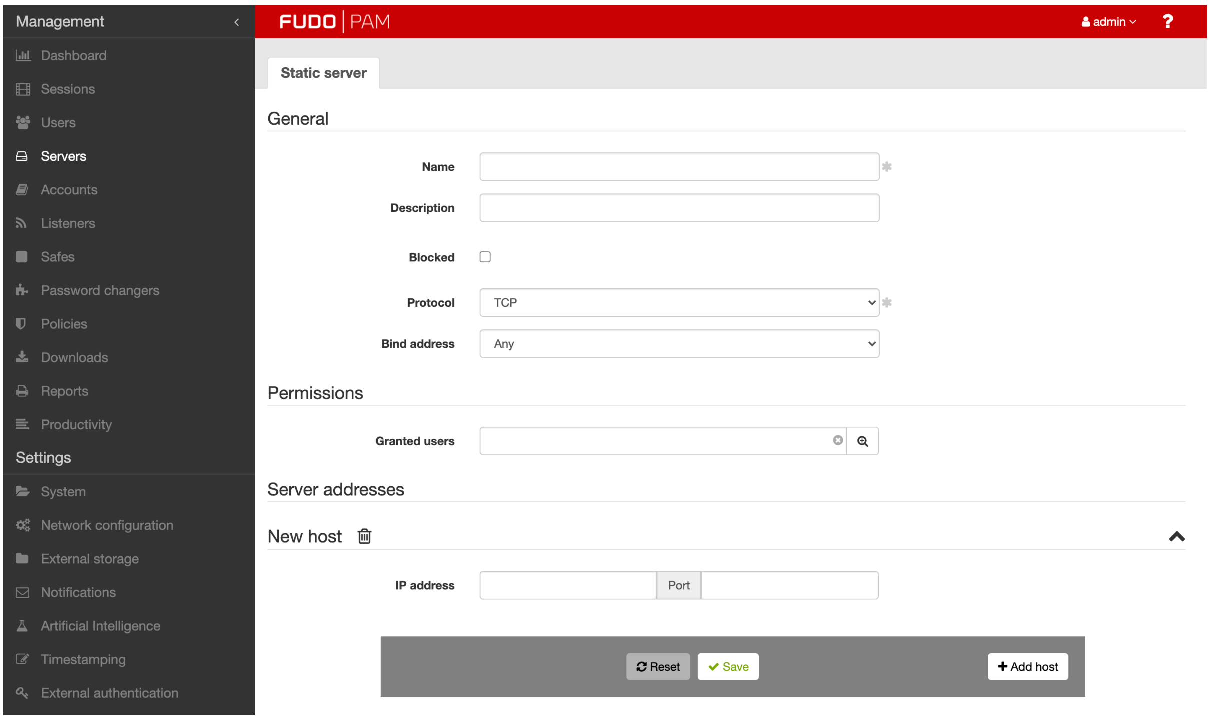
- The *Bind address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make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

---

8. In the *Permissions* section, add users allowed to manage this object.
9. Click an *Add host* button in order to add address(es) into the *Server adresses* section.

- Enter server's IP address and port number.

10. Click *Save*.



General

Name:

Description:

Blocked: □

Protocol: TCP

Bind address: Any

Permissions

Granted users:

Server addresses

New host

IP address: Port

Related topics:

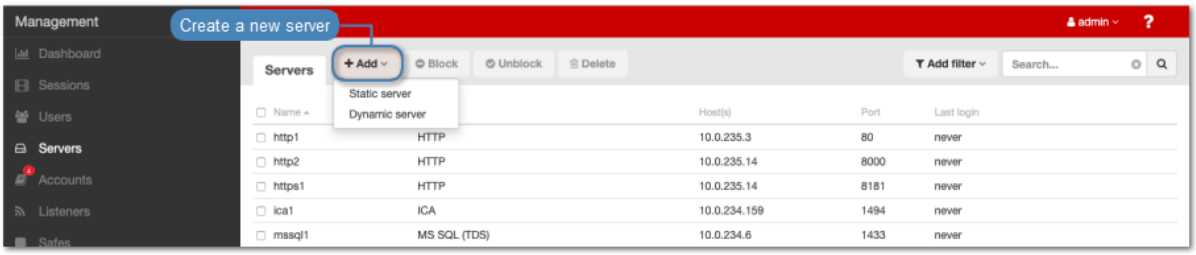
- *TCP*
- *Data model*
- *Creating a TCP listener*

6.1.2 Dynamic server

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

6.1.2.1 Creating a dynamic servers group

1. Select *Management* > *Servers*.
2. Click + *Add* and select *Dynamic server*.



□ Name ▴		Host(s)	Port	Last login
□ http1	HTTP	10.0.235.3	80	never
□ http2	HTTP	10.0.235.14	8000	never
□ https1	HTTP	10.0.235.14	8181	never
□ ica1	ICA	10.0.234.159	1494	never
□ mssql1	MS SQL (TDS)	10.0.234.6	1433	never

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

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

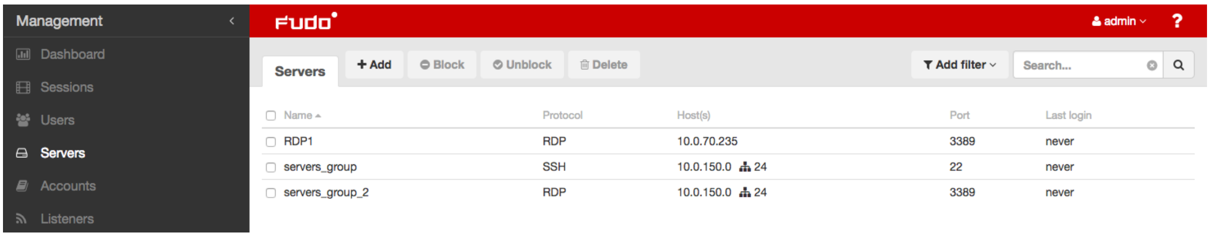
---

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

6.1.2.2 Adding a single host to a servers group

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

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



□	Name	Protocol	Host(s)	Port	Last login
□	RDP1	RDP	10.0.70.235	3389	never
□	servers_group	SSH	10.0.150.0 24	22	never
□	servers_group_2	RDP	10.0.150.0 24	3389	never

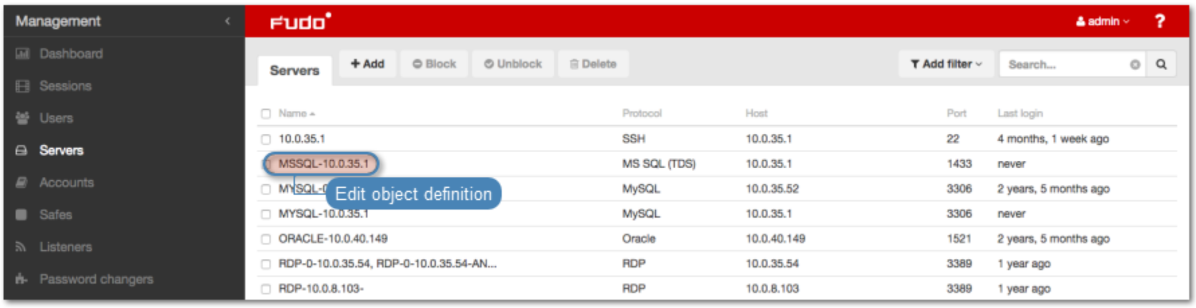
3. Click *+ Add host*.
4. Provide server's IP address.
5. Click the icon to download server's certificate.
6. Click *Save*.

Related topics:

- *Data model*
- *Static server*

6.2 Editing a server

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

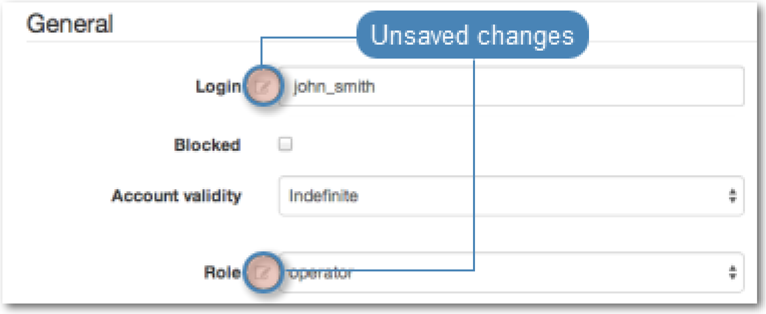


□	Name	Protocol	Host	Port	Last login
□	10.0.35.1	SSH	10.0.35.1	22	4 months, 1 week ago
□	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	never
□	MYSQL-	MySQL	10.0.35.52	3306	2 years, 5 months ago
□	MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	never
□	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 years, 5 months ago
□	RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN...	RDP	10.0.35.54	3389	1 year ago
□	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 year ago

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

3. Modify configuration parameters as needed.

Note: Unsaved changes are marked with the ✎ icon.



Login john_smith

Blocked □

Account validity Indefinite

Role operator

4. Click *Save*.

Related topics:

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

6.3 Blocking a server

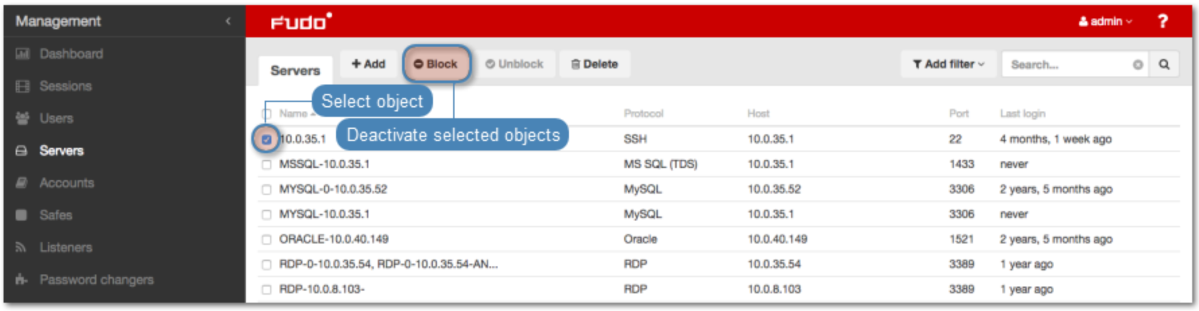
Fudo PAM allows blocking access to given server for all users.

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

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

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

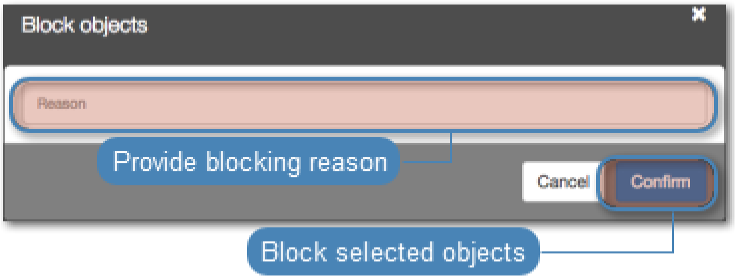
3. Click *Block*.



	Name	Protocol	Host	Port	Last login
☑	10.0.35.1	SSH	10.0.35.1	22	4 months, 1 week ago
□	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	never
□	MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 years, 5 months ago
□	MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	never
□	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 years, 5 months ago
□	RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN...	RDP	10.0.35.54	3389	1 year ago
□	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 year ago

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

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



Related topics:

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

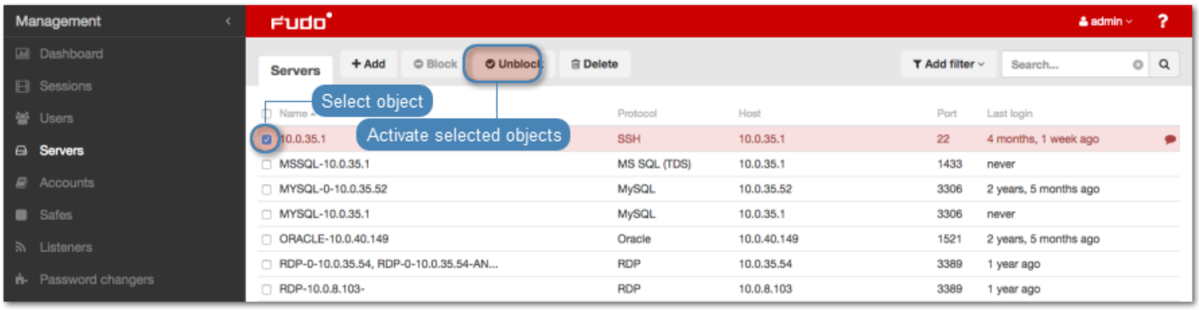
6.4 Unblocking a server

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

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

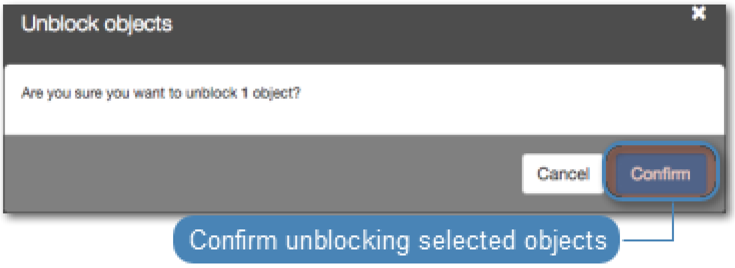
Note: Define filters to limit the number of objects displayed on the list.

3. Click *Unblock*.



	Name	Protocol	Host	Port	Last login	
☑	10.0.35.1	SSH	10.0.35.1	22	4 months, 1 week ago	💬
□	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	never	
□	MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 years, 5 months ago	
□	MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	never	
□	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 years, 5 months ago	
□	RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN...	RDP	10.0.35.54	3389	1 year ago	
□	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 year ago	

4. Click *Confirm* to unblock selected objects.



Are you sure you want to unblock 1 object?

Confirm unblocking selected objects

Related topics:

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

6.5 Deleting a server

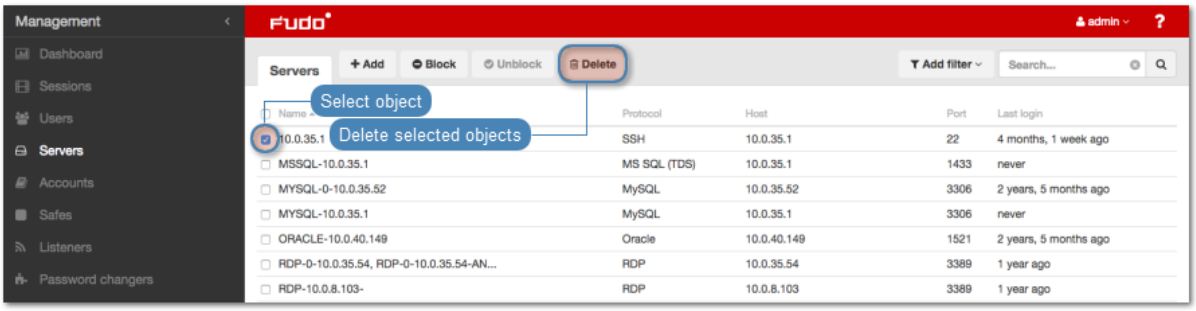
Warning: Deleting a server definition will terminate current connections with the given server.

6.5.1 Deleting a static server definition

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

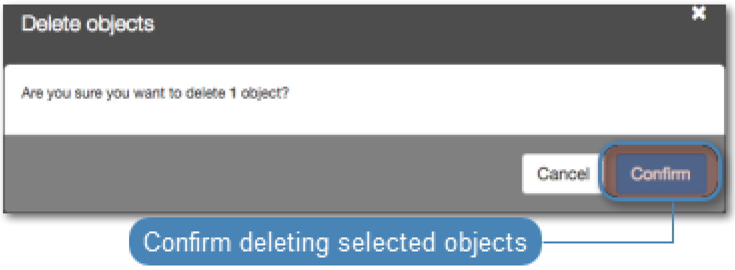
Note: Define filters to limit the number of objects displayed on the list.

3. Click *Delete*.



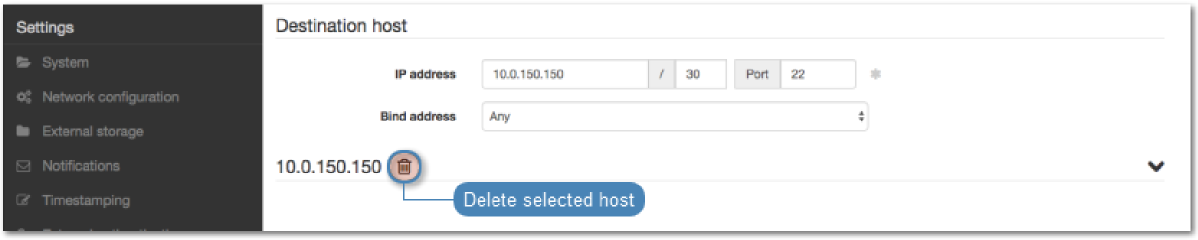
	Name	Protocol	Host	Port	Last login
☑	10.0.35.1	SSH	10.0.35.1	22	4 months, 1 week ago
□	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	never
□	MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 years, 5 months ago
□	MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	never
□	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 years, 5 months ago
□	RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN...	RDP	10.0.35.54	3389	1 year ago
□	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 year ago

4. Confirm deletion of selected objects.


Delete objects
Are you sure you want to delete 1 object?
Cancel
Confirm
Confirm deleting selected objects

6.5.2 Deleting a dynamically added host

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



4. Click *Save*.

Related topics:

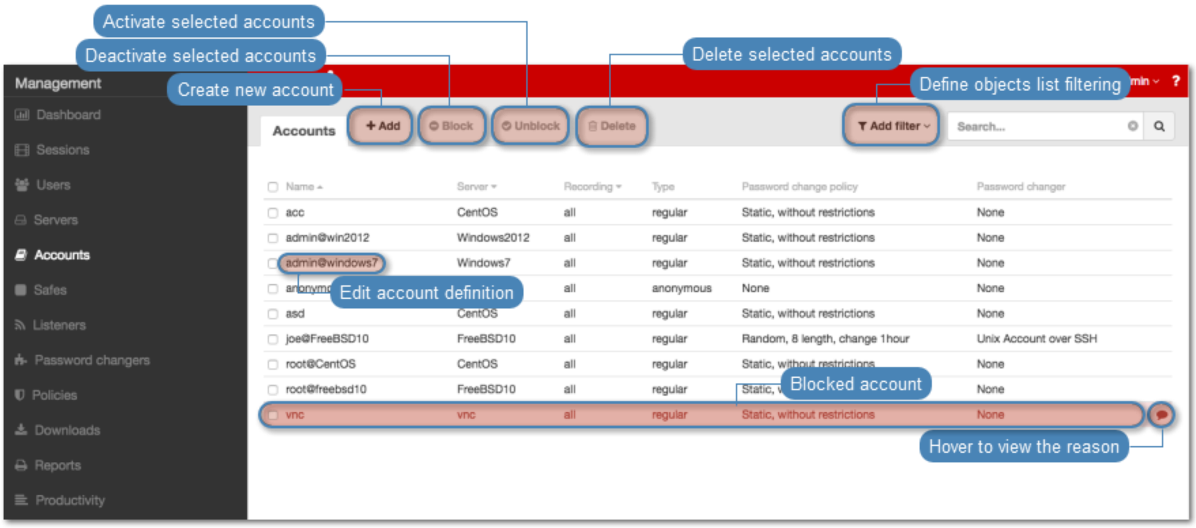
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

CHAPTER 7

Accounts

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

Note: In case of Telnet connections, user has to go through authentication process twice. First time to authenticate against Fudo PAM and then to connect to the target host.



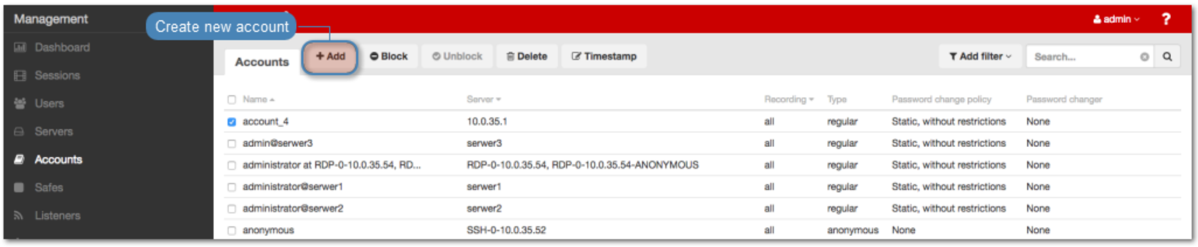
☐ Name	Server	Recording	Type	Password change policy	Password changer
☐ acc	CentOS	all	regular	Static, without restrictions	None
☐ admin@win2012	Windows2012	all	regular	Static, without restrictions	None
☐ admin@windows7	Windows7	all	regular	Static, without restrictions	None
☐ anonymo		all	anonymous	None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

7.1 Creating an account

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

7.1.1 Creating an *anonymous* account

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



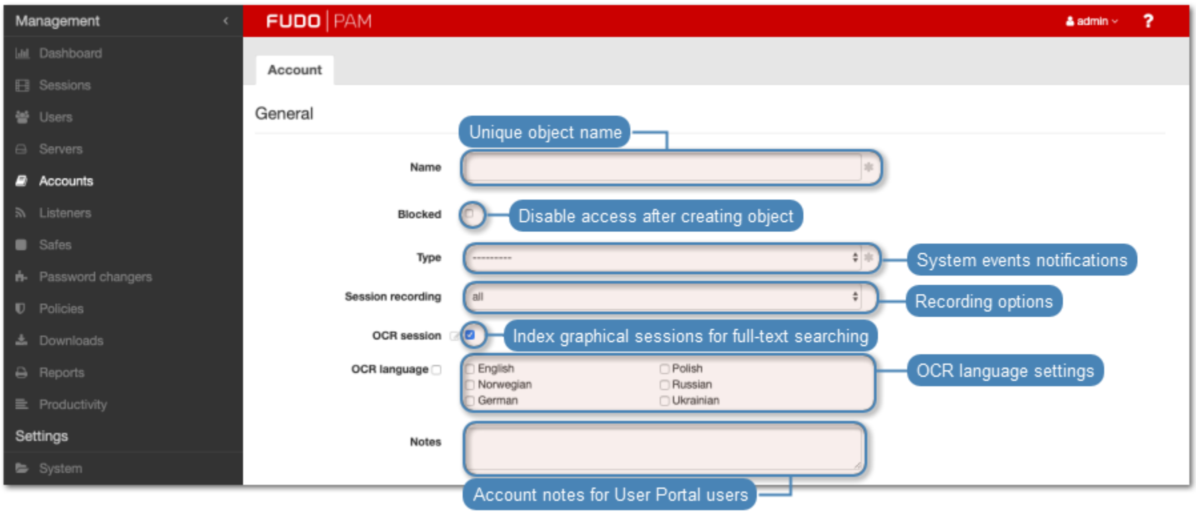
	Name	Server	Recording	Type	Password change policy	Password changer
☑	account_4	10.0.35.1	all	regular	Static, without restrictions	None
□	admin@serwer3	serwer3	all	regular	Static, without restrictions	None
□	administrator at RDP-0-10.0.35.54, RD...	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None
□	administrator@serwer1	serwer1	all	regular	Static, without restrictions	None
□	administrator@serwer2	serwer2	all	regular	Static, without restrictions	None
□	anonymous	SSH-0-10.0.35.52	all	anonymous	None	None

3. Define object's name.
4. Select *Blocked* option to disable account after it's created.
5. Select `anonymous` from the *Type* drop-down list.
6. Select desired session recording option.
   - `all` - Fudo PAM saves session metadata (basic session information), records raw network traffic (RAW file) and stores session data in internal file format (FBS). The latter enables session playback using the built-in session player, as well as exporting sessions to a selection of video file formats.
   - `raw` - Fudo PAM saves session metadata (basic session information) and records raw network traffic (RAW file). The raw data can be downloaded but it cannot be played back in graphical form using the built-in session player (session player only depicts the networks packet exchange between the client and the target host).
   - `none` - Fudo PAM saves only session metadata (basic session information).
7. Select the *OCR sessions* option to fully index RDP and VNC sessions contents.

Note: Indexing sessions enables full-text content searching.

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

8. Select language used for processing recorded sessions.
9. In the *Notes* field, enter a message to *User Portal* users.



General

Name: Unique object name

Blocked □: Disable access after creating object

Type: --------- : System events notifications

Session recording: all : Recording options

OCR session ☑: Index graphical sessions for full-text searching

OCR language □: □ English □ Norwegian □ German □ Polish □ Russian □ Ukrainian : OCR language settings

Notes: Account notes for User Portal users

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

    - Select *Override global retention settings* option to set different retention values for connections established using this account.
    - Change the global parameter value or uncheck the *Delete session data* option to exclude sessions from retention mechanism.
    - In the *Move session data to external storage after*, define the number of days after which the session data will moved to external storage device.

11. In the *Delete session data after* field, define the number of days after which the session data will be deleted.
12. In the *Permissions* section, add users allowed to manage this object.
13. In the *Server* section, assign account to a specific server by selecting it from the *Server* drop-down list.
14. Select *SSH Agent forwarding* option to authenticate the user against the target host using client's SSH key.

Note: This option is availble only after selecting an SSH server. Use -A option for connecting to SSH server.

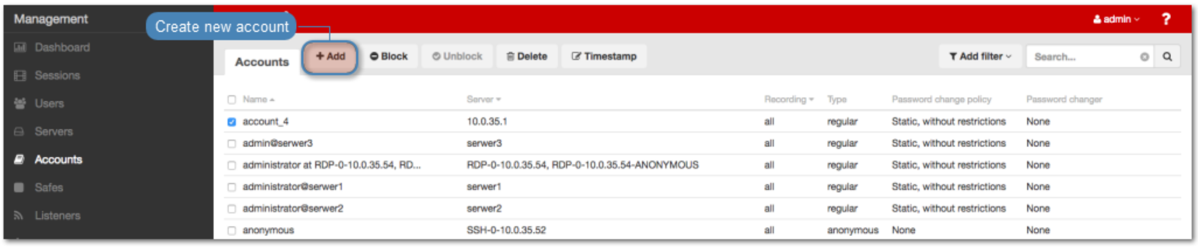
15. Click *Save*.

Related topics:

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

7.1.2 Creating a *forward* account

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



	Name	Server	Recording	Type	Password change policy	Password changer
☑	account_4	10.0.35.1	all	regular	Static, without restrictions	None
□	admin@serwer3	serwer3	all	regular	Static, without restrictions	None
□	administrator at RDP-0-10.0.35.54, RD...	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None
□	administrator@serwer1	serwer1	all	regular	Static, without restrictions	None
□	administrator@serwer2	serwer2	all	regular	Static, without restrictions	None
□	anonymous	SSH-0-10.0.35.52	all	anonymous	None	None

3. Define object's name.
4. Select *Blocked* option to disable account after it's created.
5. Select `forward` from the *Type* drop-down list.
6. Select desired session recording option.

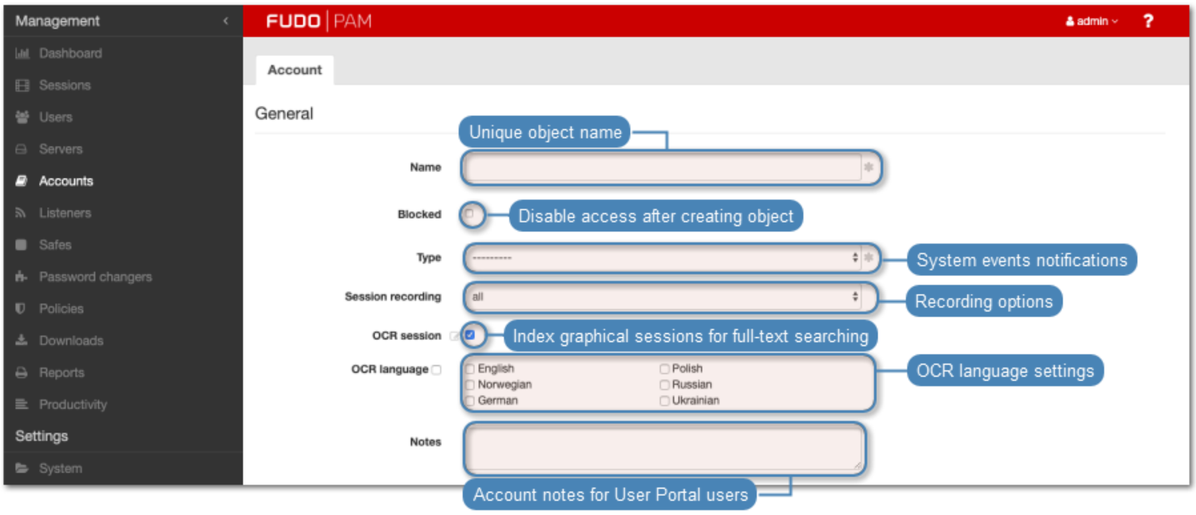
   - `all` - Fudo PAM saves session metadata (basic session information), records raw network traffic (RAW file) and stores session data in internal file format (FBS). The latter enables session playback using the built-in session player, as well as exporting sessions to a selection of video file formats.
   - `raw` - Fudo PAM saves session metadata (basic session information) and records raw network traffic (RAW file). The raw data can be downloaded but it cannot be played back in graphical form using the built-in session player (session player only depicts the networks packet exchange between the client and the target host).
   - `none` - Fudo PAM saves only session metadata (basic session information).

7. Select the *OCR sessions* option to fully index RDP and VNC sessions contents.

Note: Indexing sessions enables full-text content searching.

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

8. Select language used for processing recorded sessions.
9. In the *Notes* field, enter a message to *User Portal* users.



General

Unique object name

Name

Blocked ○ Disable access after creating object

Type --------- System events notifications

Session recording all Recording options

OCR session ☑ Index graphical sessions for full-text searching

OCR language □ English □ Norwegian □ German □ Polish □ Russian □ Ukrainian OCR language settings

Notes

Account notes for User Portal users

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

    - Select *Override global retention settings* option to set different retention values for connections established using this account.
    - Change the global parameter value or uncheck the *Delete session data* option to exclude sessions from retention mechanism.
    - In the *Move session data to external storage after*, define the number of days after which the session data will moved to external storage device.

11. In the *Permissions* section, add users allowed to manage this object.
12. In the *Server* section, assign the account to a server by selecting it from the *Server* drop-down list.
13. From the *Replace secret with* drop down list in the *Credentials*, select desired option.

`other account`

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

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

`key`

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

`password`

- Provide account password.
- Repeat account password.

Note: *Two-fold authentication*

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

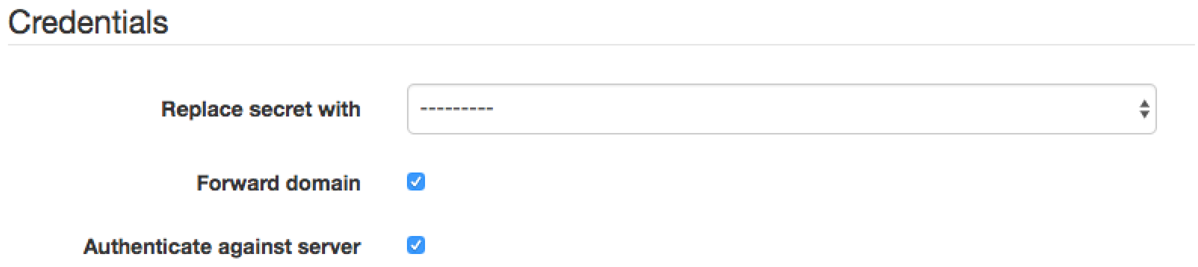
To enable two-fold authentication, select `password` from the *Replace secret with* drop-down list and leave the password and login fields empty.

`password from external repository`

- Select external repository.

Note: *Authentication by the server*

With the *Authentication against server* option enabled, Fudo PAM does not verify the correctness of user credentials. Login information is forwarded to the target host, which verifies whether the user is allowed to access it. Verification status is returned to Fudo, which establishes monitored connection. To enable this authentication scenario, select the *Authenticate against server* option in the *Credentials* section (available only for SSH servers and RDP hosts with the *Enhanced RDP Security (TLS) + NLA* security option selected).



Credentials

Replace secret with: ---------

Forward domain: ☑

Authenticate against server: ☑

Also note that 2FA/MFA authentication won't work here. If you create a user with OATH+AD authentication the OATH part is bypassed and only the password is used and sent to the server – Fudo won't ask for the OATH token in this situation. The same goes for Duo, SMS an any other 2FA user authentication scheme that can be configured in Fudo. This restriction is specific only to forward account types.

14. Select *Forward domain* option to have the domain name included in the string identifying the user.
15. Select *SSH Agent forwarding* option to authenticate the user against the target host using client's SSH key.

Note: This option is availble only after selecting an SSH server. Use -A option for connecting to SSH server.

16. Click *Save*.

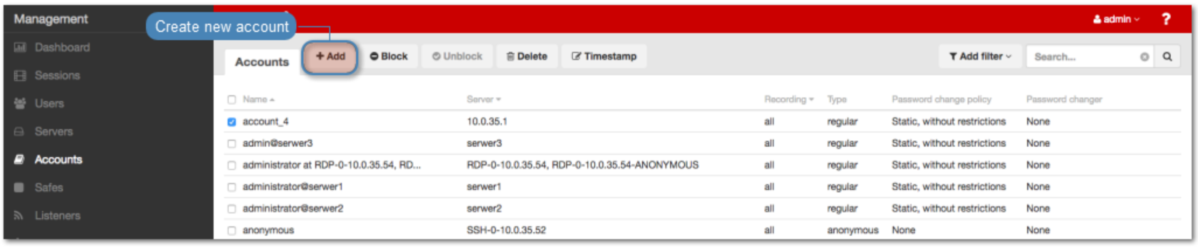
Related topics:

- *Data model*
- *Deleting an account*

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

7.1.3 Creating a *regular* account

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



	Name	Server	Recording	Type	Password change policy	Password changer
☑	account_4	10.0.35.1	all	regular	Static, without restrictions	None
□	admin@serwer3	serwer3	all	regular	Static, without restrictions	None
□	administrator at RDP-0-10.0.35.54, RD...	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None
□	administrator@serwer1	serwer1	all	regular	Static, without restrictions	None
□	administrator@serwer2	serwer2	all	regular	Static, without restrictions	None
□	anonymous	SSH-0-10.0.35.52	all	anonymous	None	None

3. Define object's name.
4. Select *Blocked* option to disable account after it's created.
5. Select `regular` from the *Type* drop-down list.
6. Select desired session recording option.

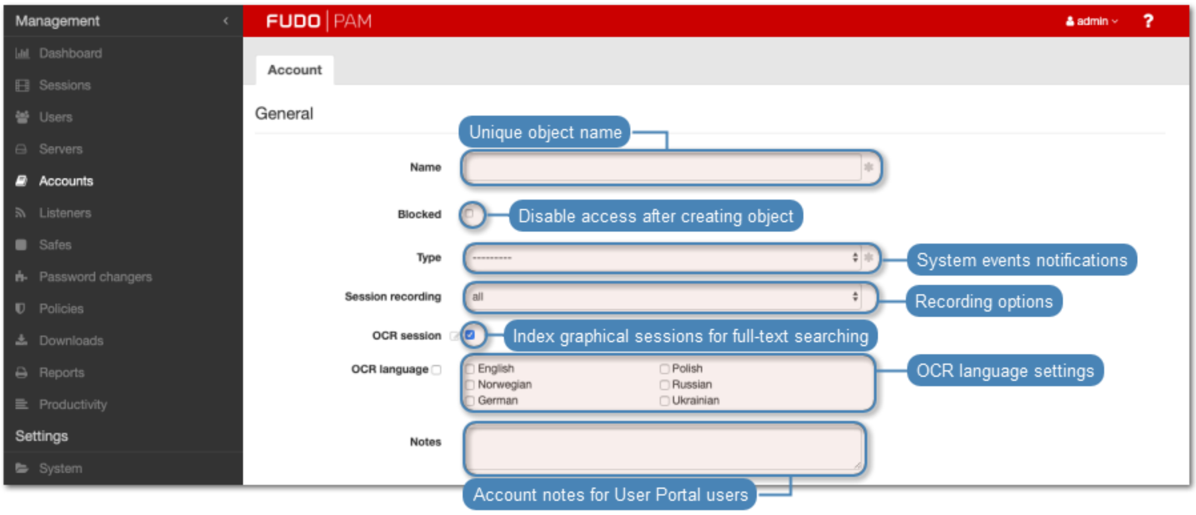
    - `all` - Fudo PAM saves session metadata (basic session information), records raw network traffic (RAW file) and stores session data in internal file format (FBS). The latter enables session playback using the built-in session player, as well as exporting sessions to a selection of video file formats.
    - `raw` - Fudo PAM saves session metadata (basic session information) and records raw network traffic (RAW file). The raw data can be downloaded but it cannot be played back in graphical form using the built-in session player (session player only depicts the networks packet exchange between the client and the target host).
    - `none` - Fudo PAM saves only session metadata (basic session information).

7. Select the *OCR sessions* option to fully index RDP and VNC sessions contents.

Note: Indexing sessions enables full-text content searching.

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

8. Select language used for processing recorded sessions.
9. In the *Notes* field, enter a message to *User Portal* users.



Type: ---------

Session recording: all

OCR session: ☑

OCR language: □ English □ Norwegian □ German □ Polish □ Russian □ Ukrainian

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

    - Select *Override global retention settings* option to set different retention values for connections established using this account.
    - Change the global parameter value or uncheck the *Delete session data* option to exclude sessions from retention mechanism.
    - In the *Move session data to external storage after*, define the number of days after which the session data will moved to external storage device.

11. In the *Permissions* section, add users allowed to manage this object.
12. In the *Server* section, assign account to a specific server by selecting it from the *Server* drop-down list.
13. In the *Credentials* section, enter privileged account domain.
14. Type in login to the privileged account.
15. From the *Replace secret with* drop down list, select desired option.

    `secret from a different account`

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

    `key`

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

    `password`

    - Provide account password.
    - Repeat account password.

Note: *Two-fold authentication*

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

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

`password from external repository`

- Select external repository.

16. Select the defined password changing policy from the *Password change policy* drop-down list.
17. In the *Password checkout time limit*, define the time after which the password is returned automatically.

Note: Defining the password checkout time limit automatically enables the Secret Checkout feature.

18. Select *Change password after last checkin* option to change the password automatically after it has been returned by the last user.

Note: This options is available only for Secret Checkout feature and it's enabled after specifying the *Password checkout time limit.*

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

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

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

20. Select *SSH Agent forwarding* option to authenticate user against the target host using client's SSH key.

Note: This option is availble only after selecting an SSH server. Use -A option for connecting to SSH server.

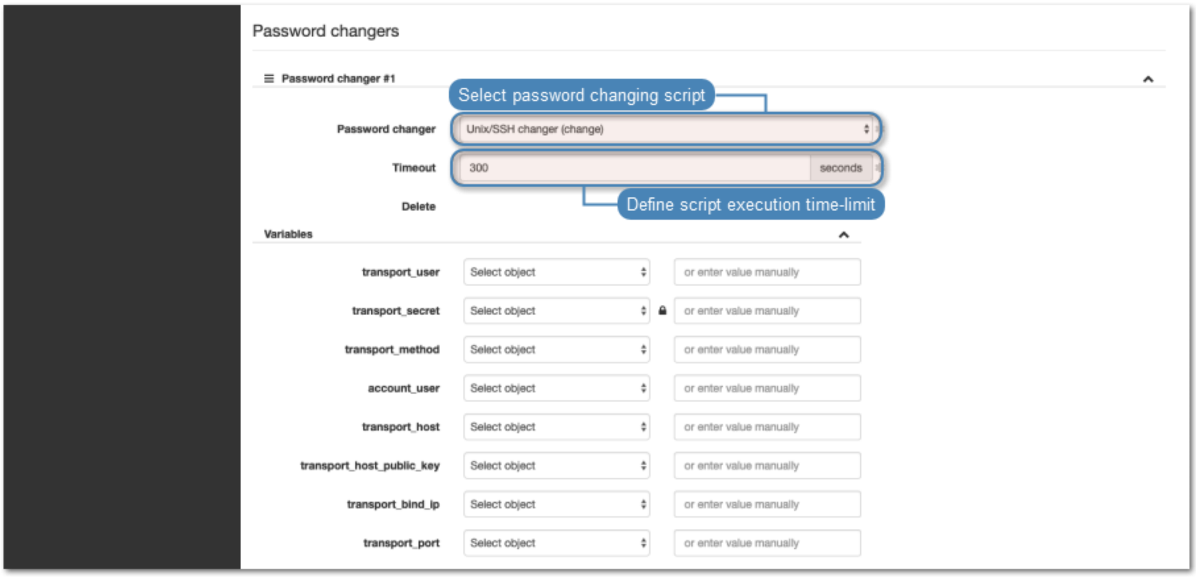
21. Check the *Password recovery* option to set a password verifier, to automatically trigger a password changer if it verifies that the password for an Account was changed and a new password is not stored in Fudo PAM.

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

22. Click *+ Add password modifier*, to have the password to the account changed automatically according to the *password policy*.

Note: Option to add a password changer is available after choosing an option to replace secret with a password.

23. In the *Password changer* section, from the *Password changer* drop-down list select password changer specific for given account.
24. In the *Timeout* field, define the script's execution time limit.



Password changers

Password changer #1

Select password changing script

Password changer: Unix/SSH changer (change)

Timeout: 300 seconds

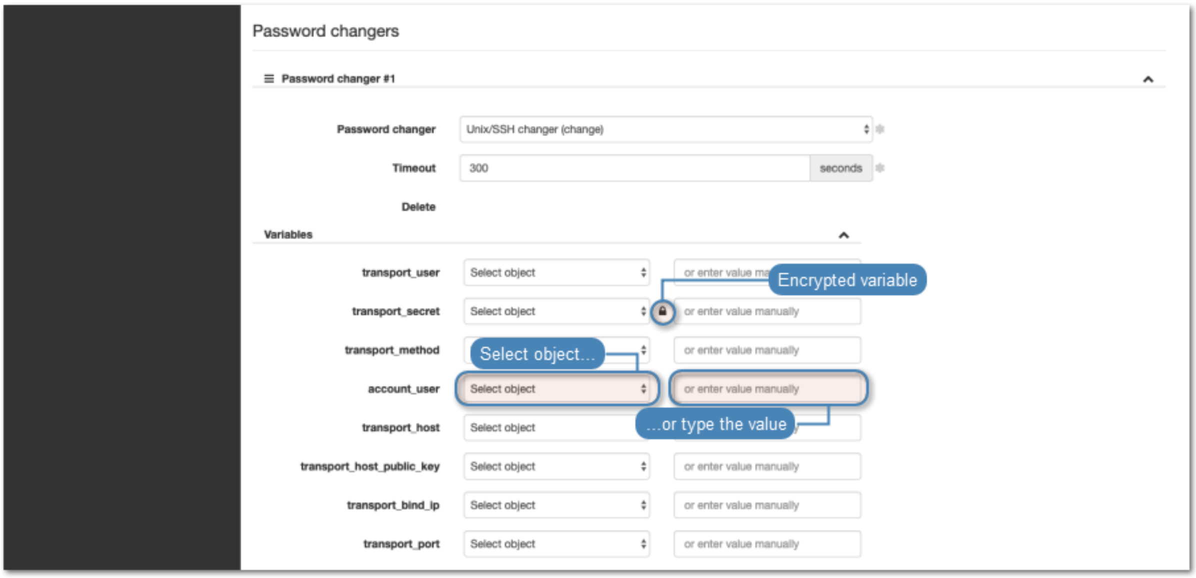
Define script execution time-limit

Delete

Variables

transport_user	Select object	or enter value manually
transport_secret	Select object	or enter value manually
transport_method	Select object	or enter value manually
account_user	Select object	or enter value manually
transport_host	Select object	or enter value manually
transport_host_public_key	Select object	or enter value manually
transport_bind_ip	Select object	or enter value manually
transport_port	Select object	or enter value manually

25. In the *Variables* section, assign attributes to variables.



Password changers

Password changer #1

Password changer: Unix/SSH changer (change)

Timeout: 300 seconds

Delete

Variables

Encrypted variable

Select object...

...or type the value

transport_user	Select object	or enter value manually
transport_secret	Select object	or enter value manually
transport_method	Select object	or enter value manually
account_user	Select object	or enter value manually
transport_host	Select object	or enter value manually
transport_host_public_key	Select object	or enter value manually
transport_bind_ip	Select object	or enter value manually
transport_port	Select object	or enter value manually

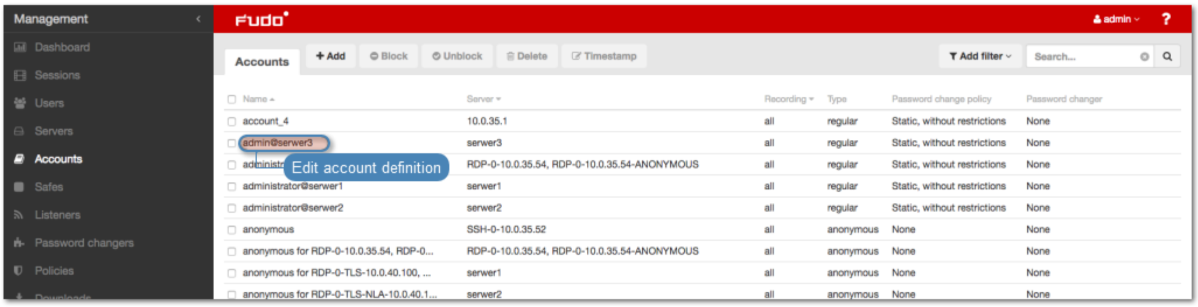
26. Click *Save*.

Related topics:

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

7.2 Editing an account

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

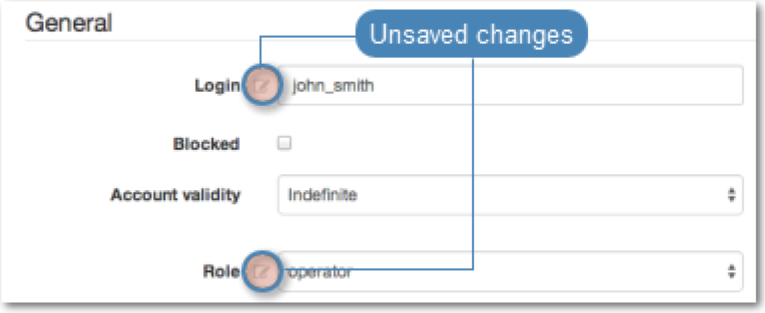


☐ Name	Server	Recording	Type	Password change policy	Password changer
☐ account_4	10.0.35.1	all	regular	Static, without restrictions	None
☐ admin@serwer3	serwer3	all	regular	Static, without restrictions	None
☐ administr	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None
☐ administrator@serwer1	serwer1	all	regular	Static, without restrictions	None
☐ administrator@serwer2	serwer2	all	regular	Static, without restrictions	None
☐ anonymous	SSH-0-10.0.35.52	all	anonymous	None	None
☐ anonymous for RDP-0-10.0.35.54, RDP-0...	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	anonymous	None	None
☐ anonymous for RDP-0-TLS-10.0.40.100, ...	serwer1	all	anonymous	None	None
☐ anonymous for RDP-0-TLS-NLA-10.0.40.1...	serwer2	all	anonymous	None	None

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

3. Modify configuration parameters as needed.

Note: Unsaved changes are marked with the 📝 icon.



General

Login john_smith

Blocked ☐

Account validity Indefinite

Role operator

4. Click *Save*.

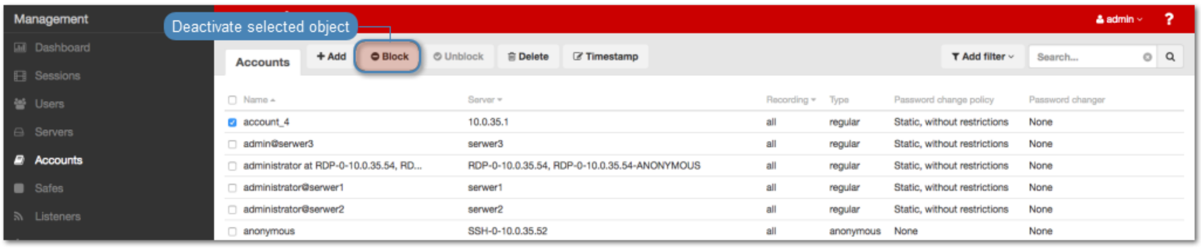
Related topics:

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

7.3 Blocking an account

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

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

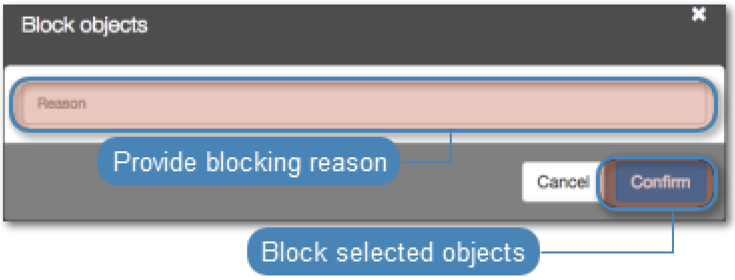


Deactivate selected object

	Name	Server	Recording	Type	Password change policy	Password changer
☑	account_4	10.0.35.1	all	regular	Static, without restrictions	None
□	admin@serwer3	serwer3	all	regular	Static, without restrictions	None
□	administrator at RDP-0-10.0.35.54, RD...	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None
□	administrator@serwer1	serwer1	all	regular	Static, without restrictions	None
□	administrator@serwer2	serwer2	all	regular	Static, without restrictions	None
□	anonymous	SSH-0-10.0.35.52	all	anonymous	None	None

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

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



Provide blocking reason

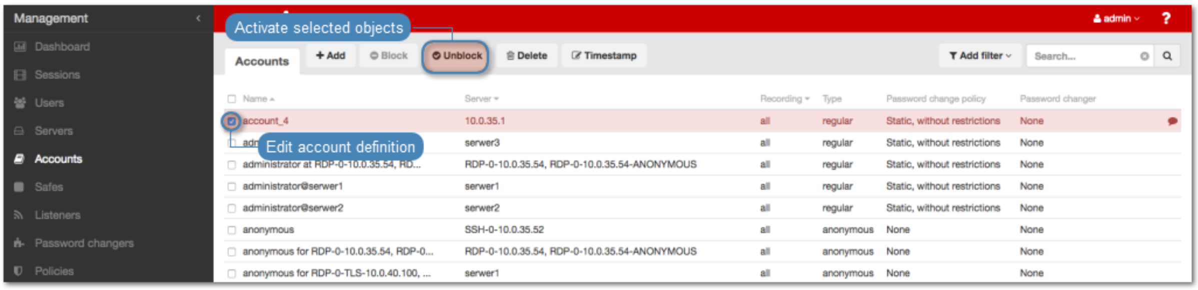
Block selected objects

Related topics:

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

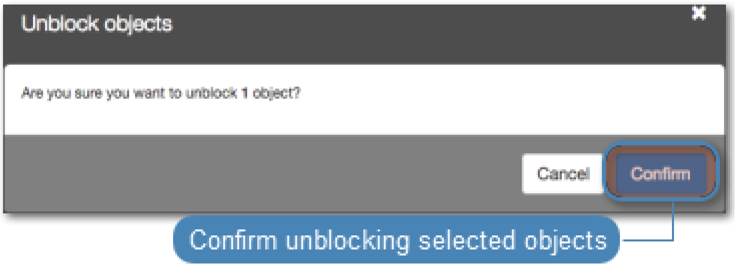
7.4 Unblocking an account

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



Name	Server	Recording	Type	Password change policy	Password changer
☑ account_4	10.0.35.1	all	regular	Static, without restrictions	None
□ adm	serwer3	all	regular	Static, without restrictions	None
□ administrator at RDP-0-10.0.35.54, RD...	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None
□ administrator@serwer1	serwer1	all	regular	Static, without restrictions	None
□ administrator@serwer2	serwer2	all	regular	Static, without restrictions	None
□ anonymous	SSH-0-10.0.35.52	all	anonymous	None	None
□ anonymous for RDP-0-10.0.35.54, RDP-0...	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	anonymous	None	None
□ anonymous for RDP-0-TLS-10.0.40.100, ...	serwer1	all	anonymous	None	None

4. Confirm unblocking selected objects.


Unblock objects

Are you sure you want to unblock 1 object?

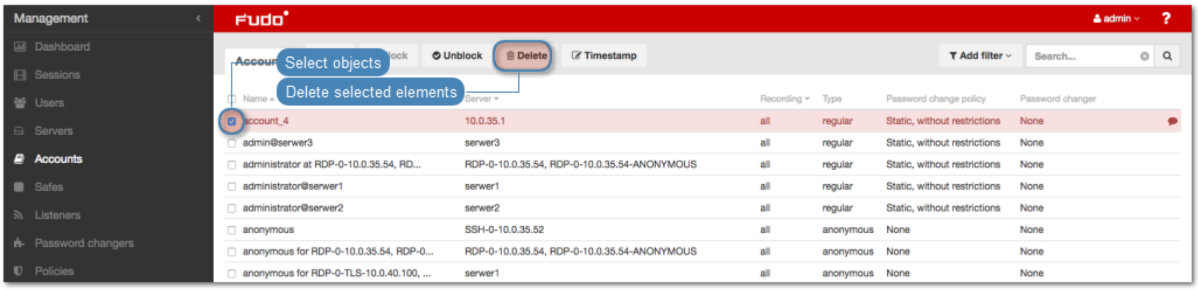
Related topics:

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

7.5 Deleting an account

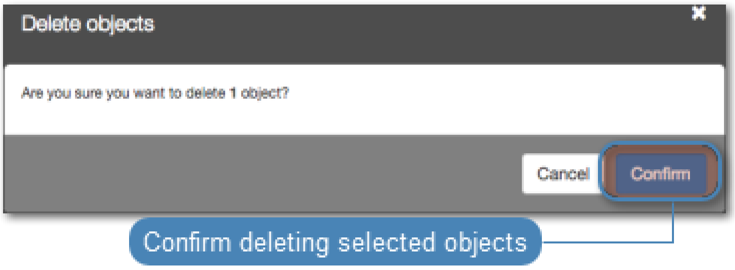
Warning: Deleting an accout definition will terminate all current connections to servers which use selected account for accessing those servers.

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



Name	Server	Recording	Type	Password change policy	Password changer
☑ account_4	10.0.35.1	all	regular	Static, without restrictions	None
□ admin@serwer3	serwer3	all	regular	Static, without restrictions	None
□ administrator at RDP-0-10.0.35.54, RD...	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None
□ administrator@serwer1	serwer1	all	regular	Static, without restrictions	None
□ administrator@serwer2	serwer2	all	regular	Static, without restrictions	None
□ anonymous	SSH-0-10.0.35.52	all	anonymous	None	None
□ anonymous for RDP-0-10.0.35.54, RDP-0...	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	anonymous	None	None
□ anonymous for RDP-0-TLS-10.0.40.100, ...	serwer1	all	anonymous	None	None

4. Confirm deletion of selected objects.



Are you sure you want to delete 1 object?

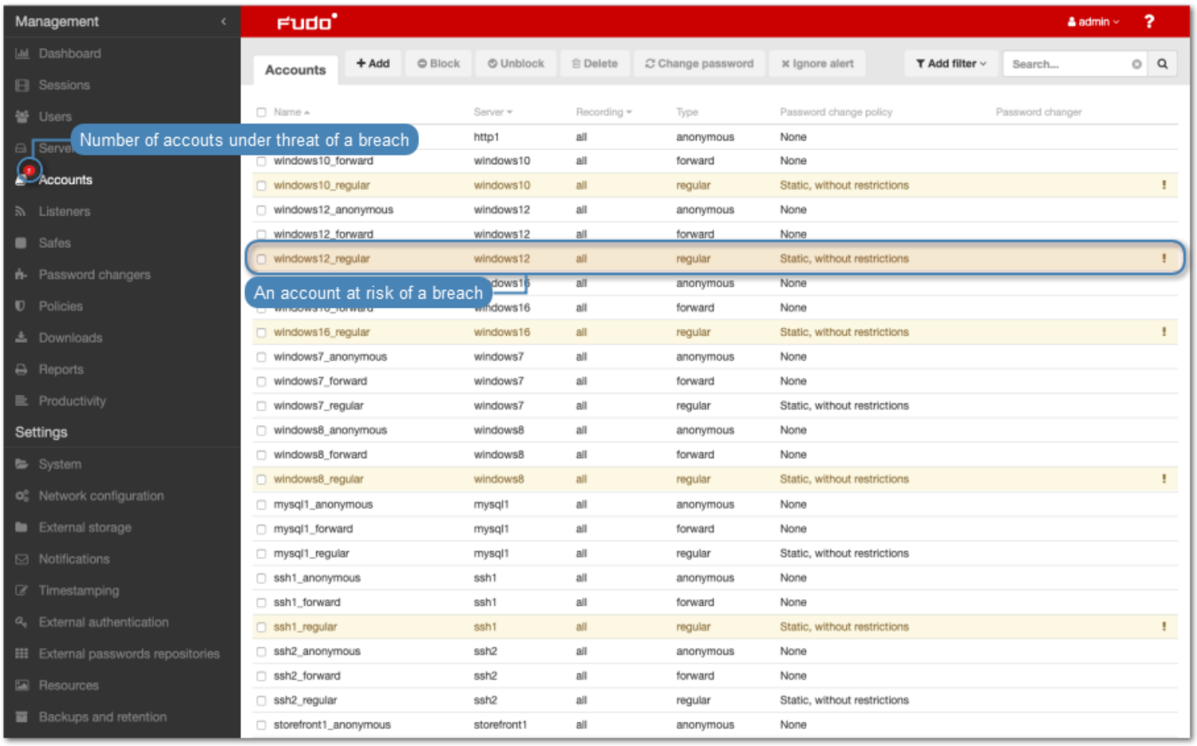
Confirm deleting selected objects

Related topics:

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

7.6 Managing security alerts

Fudo PAM tracks user's action in *User portal* and registers every password viewing. Blocking a user who has seen the current password is a potential security breach. Fudo PAM identifies such events and communicates them to system's administrators.



Number of accouts under threat of a breach

An account at risk of a breach

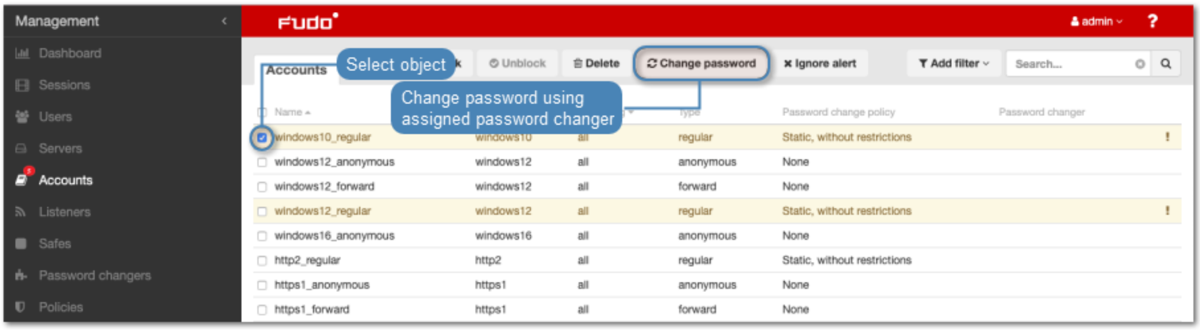
Name	Server	Recording	Type	Password change policy	Password changer
[illegible]	http1	all	anonymous	None	
windows10_forward	windows10	all	forward	None	
windows10_regular	windows10	all	regular	Static, without restrictions	!
windows12_anonymous	windows12	all	anonymous	None	
windows12_forward	windows12	all	forward	None	
windows12_regular	windows12	all	regular	Static, without restrictions	!
[illegible]	dows16	all	anonymous	None	
[illegible]	ndows16	all	forward	None	
windows16_regular	windows16	all	regular	Static, without restrictions	!
windows7_anonymous	windows7	all	anonymous	None	
windows7_forward	windows7	all	forward	None	
windows7_regular	windows7	all	regular	Static, without restrictions	
windows8_anonymous	windows8	all	anonymous	None	
windows8_forward	windows8	all	forward	None	
windows8_regular	windows8	all	regular	Static, without restrictions	!
mysql1_anonymous	mysql1	all	anonymous	None	
mysql1_forward	mysql1	all	forward	None	
mysql1_regular	mysql1	all	regular	Static, without restrictions	
ssh1_anonymous	ssh1	all	anonymous	None	
ssh1_forward	ssh1	all	forward	None	
ssh1_regular	ssh1	all	regular	Static, without restrictions	!
ssh2_anonymous	ssh2	all	anonymous	None	
ssh2_forward	ssh2	all	forward	None	
ssh2_regular	ssh2	all	regular	Static, without restrictions	
storefront1_anonymous	storefront1	all	anonymous	None	

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

7.6.1 Triggering password change

Triggering password change on the accounts list

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



Select object

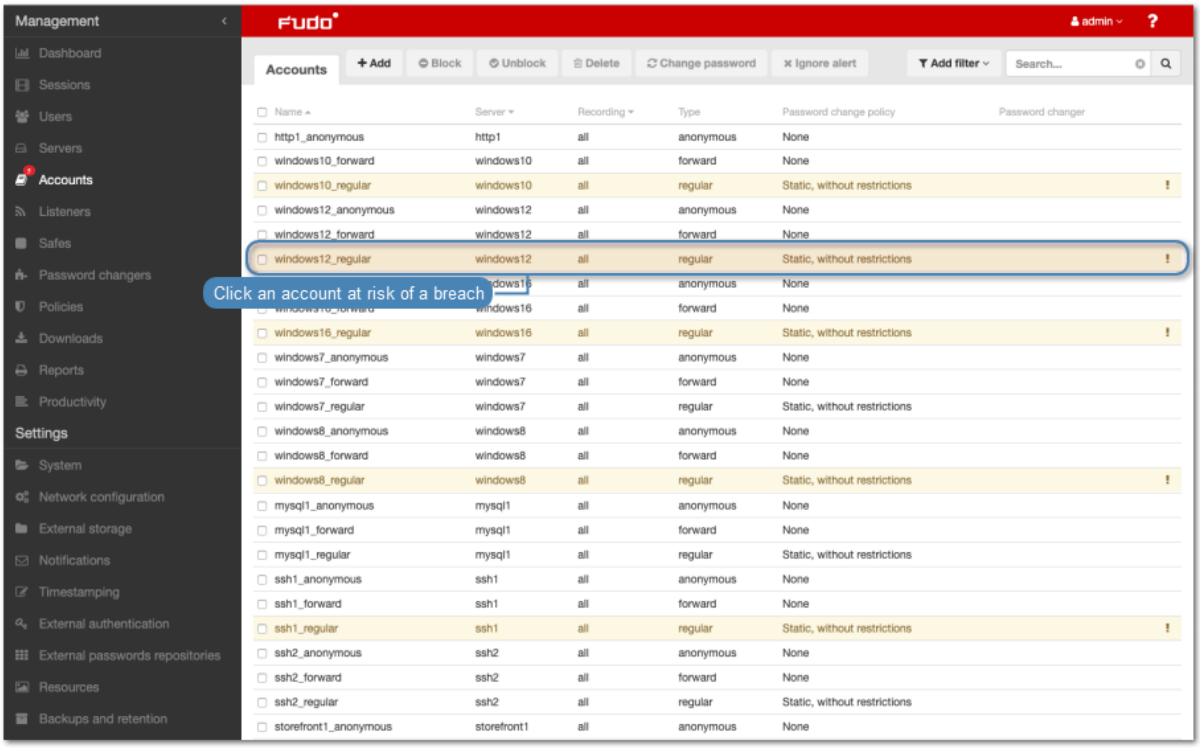
Change password using assigned password changer

	Name			Type	Password change policy	Password changer	
☑	windows10_regular	windows10	all	regular	Static, without restrictions		!
□	windows12_anonymous	windows12	all	anonymous	None		
□	windows12_forward	windows12	all	forward	None		
□	windows12_regular	windows12	all	regular	Static, without restrictions		!
□	windows16_anonymous	windows16	all	anonymous	None		
□	http2_regular	http2	all	regular	Static, without restrictions		
□	https1_anonymous	https1	all	anonymous	None		
□	https1_forward	https1	all	forward	None		

4. Confirm changing password to selected accounts.

Triggering password change from account form

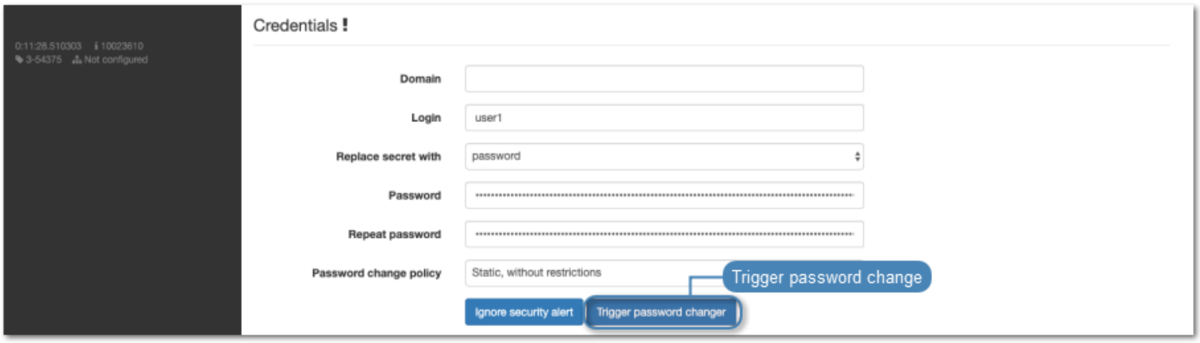
1. Select *Management* > *Accounts*.
2. Find and click desired account.



Click an account at risk of a breach

□	Name	Server	Recording	Type	Password change policy	Password changer	
□	http1_anonymous	http1	all	anonymous	None		
□	windows10_forward	windows10	all	forward	None		
□	windows10_regular	windows10	all	regular	Static, without restrictions		!
□	windows12_anonymous	windows12	all	anonymous	None		
□	windows12_forward	windows12	all	forward	None		
□	windows12_regular	windows12	all	regular	Static, without restrictions		!
	[illegible]	dows16	all	anonymous	None		
	[illegible]	ndows16	all	forward	None		
□	windows16_regular	windows16	all	regular	Static, without restrictions		!
□	windows7_anonymous	windows7	all	anonymous	None		
□	windows7_forward	windows7	all	forward	None		
□	windows7_regular	windows7	all	regular	Static, without restrictions		
□	windows8_anonymous	windows8	all	anonymous	None		
□	windows8_forward	windows8	all	forward	None		
□	windows8_regular	windows8	all	regular	Static, without restrictions		!
□	mysql1_anonymous	mysql1	all	anonymous	None		
□	mysql1_forward	mysql1	all	forward	None		
□	mysql1_regular	mysql1	all	regular	Static, without restrictions		
□	ssh1_anonymous	ssh1	all	anonymous	None		
□	ssh1_forward	ssh1	all	forward	None		
□	ssh1_regular	ssh1	all	regular	Static, without restrictions		!
□	ssh2_anonymous	ssh2	all	anonymous	None		
□	ssh2_forward	ssh2	all	forward	None		
□	ssh2_regular	ssh2	all	regular	Static, without restrictions		
□	storefront1_anonymous	storefront1	all	anonymous	None		

3. In the *Credentials* section, click *Trigger password changer*.

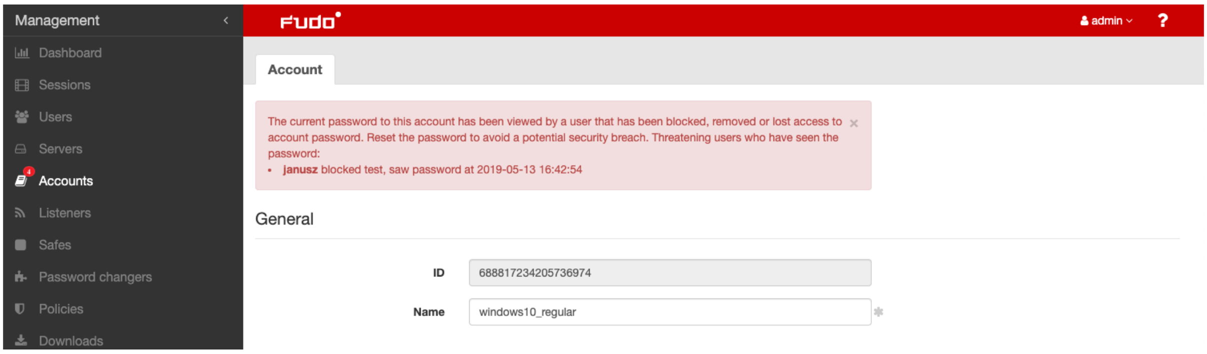


0:11:28.510303 10023610
3-54375 Not configured

Credentials !

Domain	
Login	user1
Replace secret with	password
Password	••
Repeat password	••
Password change policy	Static, without restrictions

Note: Account edit form contains a list of blocked users who have seen current password.



The current password to this account has been viewed by a user that has been blocked, removed or lost access to account password. Reset the password to avoid a potential security breach. Threatening users who have seen the password:

- **janusz** blocked test, saw password at 2019-05-13 16:42:54

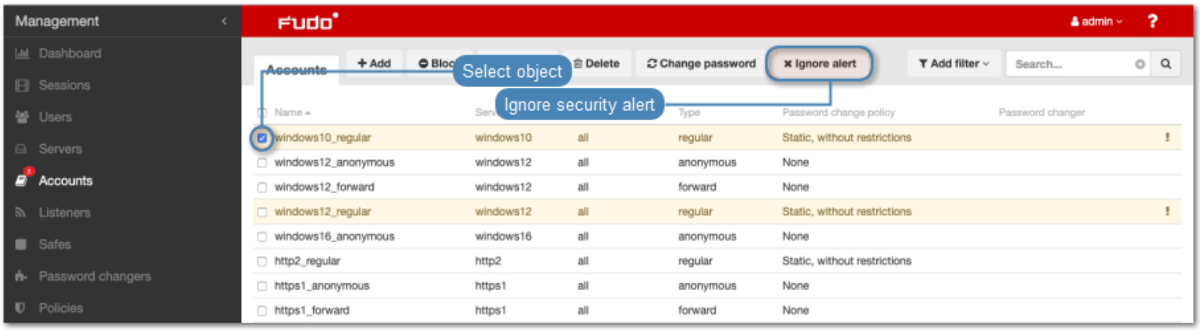
General

ID	688817234205736974
Name	windows10_regular

7.6.2 Ignoring security alert

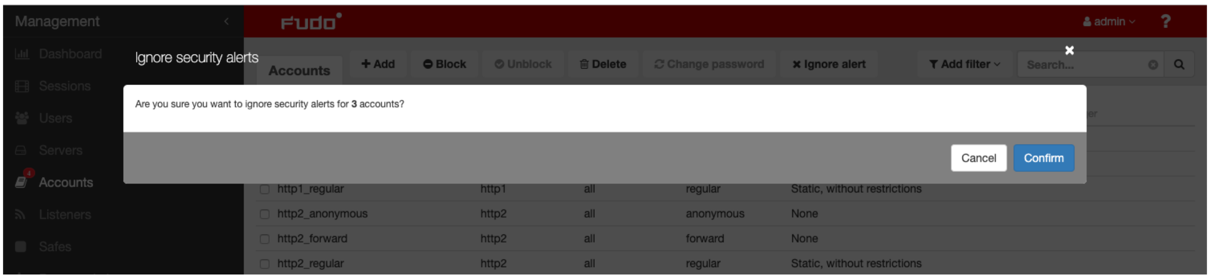
Ignoring security alert on the accounts list

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



	Name	Serv		Type	Password change policy	Password changer	
☑	windows10_regular	windows10	all	regular	Static, without restrictions		!
□	windows12_anonymous	windows12	all	anonymous	None		
□	windows12_forward	windows12	all	forward	None		
□	windows12_regular	windows12	all	regular	Static, without restrictions		!
□	windows16_anonymous	windows16	all	anonymous	None		
□	http2_regular	http2	all	regular	Static, without restrictions		
□	https1_anonymous	https1	all	anonymous	None		
□	https1_forward	https1	all	forward	None		

4. Confirm ignoring security alerts for selected accounts.



Ignore security alerts

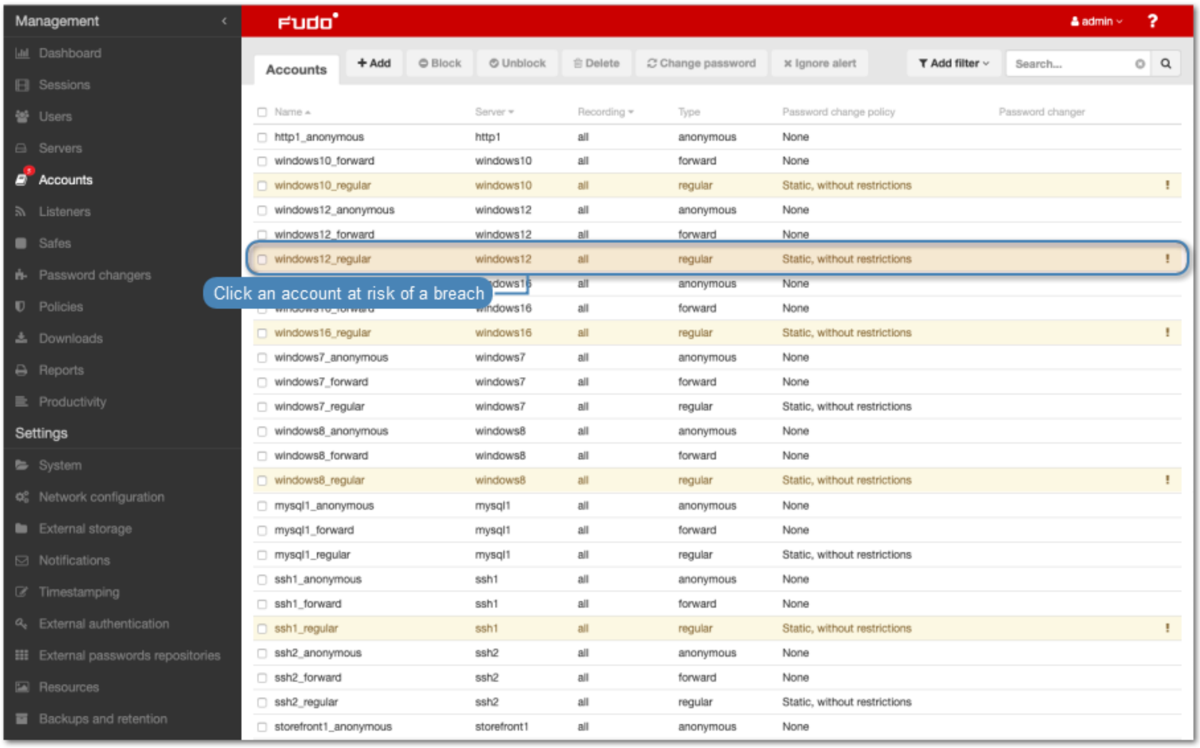
Are you sure you want to ignore security alerts for **3** accounts?

Cancel | Confirm

http1_regular	http1	all	regular	Static, without restrictions
http2_anonymous	http2	all	anonymous	None
http2_forward	http2	all	forward	None
http2_regular	http2	all	regular	Static, without restrictions

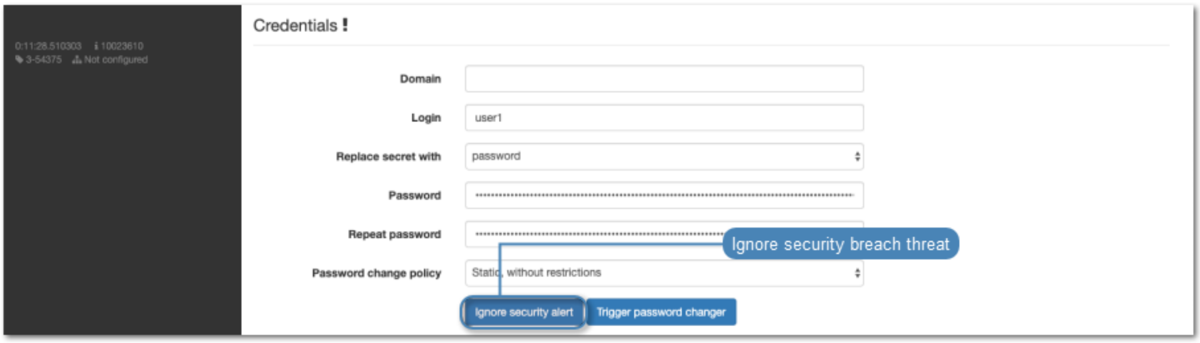
Ignoring security alert from the account form

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



Name	Server	Recording	Type	Password change policy	Password changer	
http1_anonymous	http1	all	anonymous	None		
windows10_forward	windows10	all	forward	None		
windows10_regular	windows10	all	regular	Static, without restrictions		!
windows12_anonymous	windows12	all	anonymous	None		
windows12_forward	windows12	all	forward	None		
windows12_regular	windows12	all	regular	Static, without restrictions		!
[illegible]	windows16	all	anonymous	None		
windows16_forward	windows16	all	forward	None		
windows16_regular	windows16	all	regular	Static, without restrictions		!
windows7_anonymous	windows7	all	anonymous	None		
windows7_forward	windows7	all	forward	None		
windows7_regular	windows7	all	regular	Static, without restrictions		
windows8_anonymous	windows8	all	anonymous	None		
windows8_forward	windows8	all	forward	None		
windows8_regular	windows8	all	regular	Static, without restrictions		!
mysql1_anonymous	mysql1	all	anonymous	None		
mysql1_forward	mysql1	all	forward	None		
mysql1_regular	mysql1	all	regular	Static, without restrictions		
ssh1_anonymous	ssh1	all	anonymous	None		
ssh1_forward	ssh1	all	forward	None		
ssh1_regular	ssh1	all	regular	Static, without restrictions		!
ssh2_anonymous	ssh2	all	anonymous	None		
ssh2_forward	ssh2	all	forward	None		
ssh2_regular	ssh2	all	regular	Static, without restrictions		
storefront1_anonymous	storefront1	all	anonymous	None		

3. In the *Credentials* section, click *Ignore security alert*.

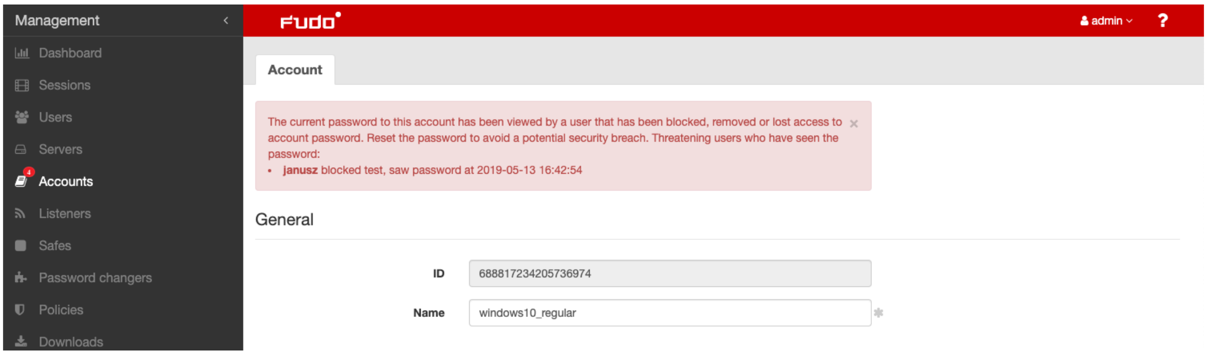


Credentials !

Domain	
Login	user1
Replace secret with	password
Password	••
Repeat password	••
Password change policy	Static, without restrictions

Ignore security alert | Trigger password changer

Note: Account edit form contains a list of blocked users who have seen current password.



The current password to this account has been viewed by a user that has been blocked, removed or lost access to account password. Reset the password to avoid a potential security breach. Threatening users who have seen the password:

- **janusz** blocked test, saw password at 2019-05-13 16:42:54

ID: 688817234205736974

Name: windows10_regular

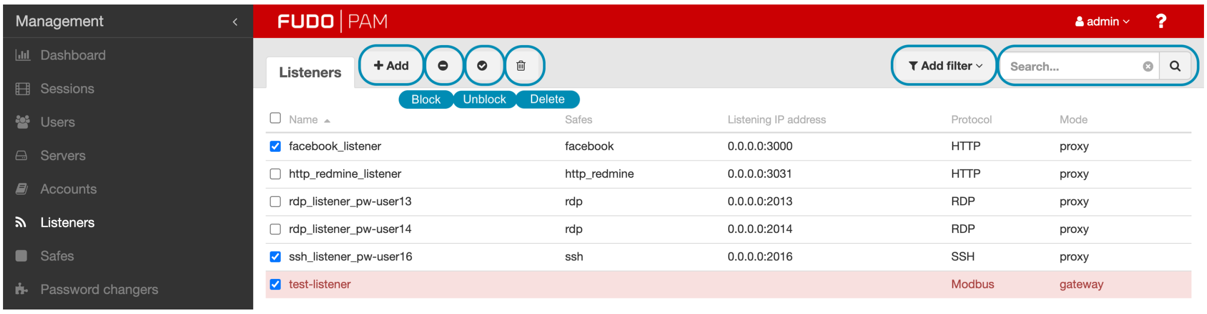
Related topics:

- *Password changers*
- *User portal*

CHAPTER 8

Listeners

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



☐	Name	Safes	Listening IP address	Protocol	Mode
☑	facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
☐	http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
☐	rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
☐	rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
☑	ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy
☑	test-listener			Modbus	gateway

Note:

- A listener cannot link to an account that is assigned to a server with a different protocol then the one defined in the listener.
- A *proxy* type listener can link to only one server.
- A *bastion* type listener cannot link to an anonymous account.
- A listener cannot link to the same anonymous account through two different safes.
- A listener cannot link to an *anonymous* and a *regular* or *forward* account to the same server with the same protocol as the listener's protocol.
- A listener cannot link to two *regular* or *forward* type accounts to the same server with the same protocol as the listener's protocol, to which a single user has access.
- For a given linked RDP listener and RDP server, both have to use either *Standard RDP Security* or *TLS* or *NLA*.

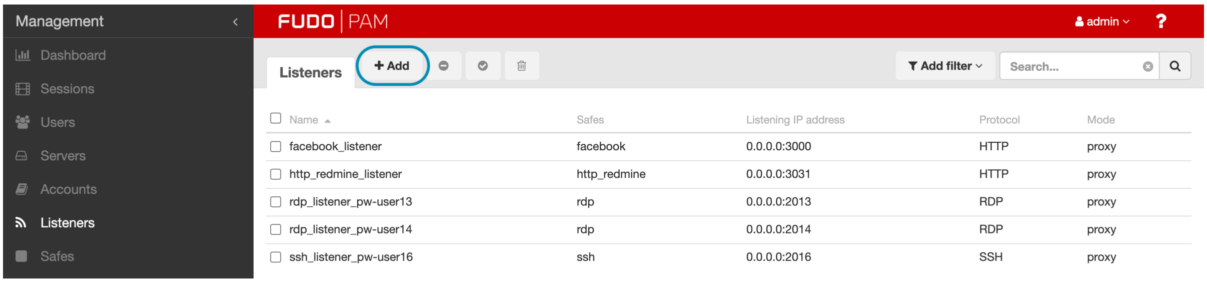
8.1 Creating a listener

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

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

8.1.1 Creating a Citrix listener

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



Name	Safes	Listening IP address	Protocol	Mode
□ facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
□ http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
□ rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
□ rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
□ ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `Citrix StoreFront (HTTP)` from the *Protocol* drop-down list.
6. In the *Permissions* section, add users allowed to manage this object.
7. In the *Connection* section, select desired connection mode:

   gateway

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

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

   proxy

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

- In the *External address* field, enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Note: The external address is listed in *user portal* and it enables establishing connections from external networks.

transparent

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

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

8. Select *Use TLS* option to enable encryption.
9. Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
10. In the *TLS certificate* field, click ⚙ to generate TLS certificate, or click ⊙ to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.
11. Click *Save*.

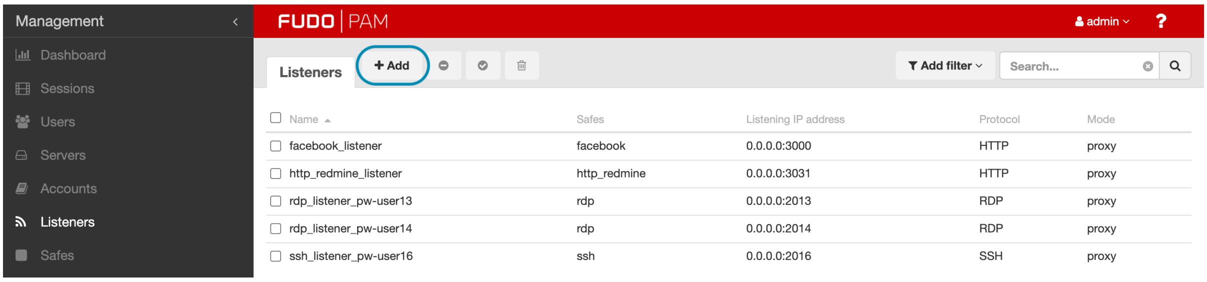
Related topics:

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

8.1.2 Creating a HTTP listener

Portal users connecting to an HTTP listener don't have to provide credentials in an HTTP login page but are presented to an already authenticated session based on the fact they're already authenticated on a portal.

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



Name	Safes	Listening IP address	Protocol	Mode
facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `HTTP` from the *Protocol* drop-down list.
6. Select `Render sessions` to enable graphical session rendering.

Note:

- Graphical HTTP rendering requires a substantial amount of processing power. It is recommended to limit the number of rendered HTTP sessions to minimum to ensure high system's responsiveness.
- In case of rendered HTTP sessions, raw protocol data is not recorded.

7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Connection* section, select desired connection mode.

   bastion

   Note:

   - Bastion mode is supported for rendered mode only.
   - User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
   - For details on bastion connection mode, refer to *Connection modes* topic.

   - Select `bastion` from the *Mode* drop-down list.
   - Select the the IP address from the *Local address* drop-down list and enter port number.
   - In the *External address* field, enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Note: The external address is listed in *user portal* and it enables establishing connections from external networks.

gateway

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

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

proxy

Note:

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

- In the *External address* field, enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

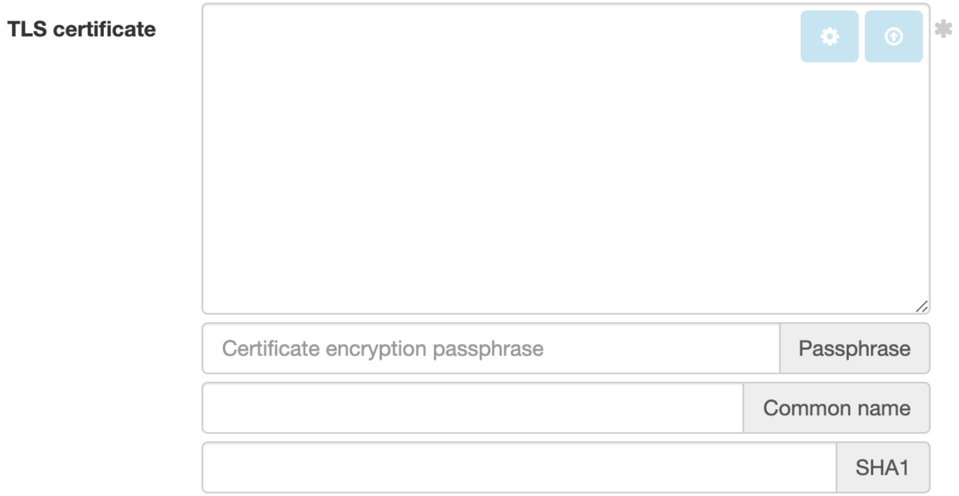
Note: The external address is listed in *user portal* and it enables establishing connections from external networks.

transparent

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

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

9. Select the *Use TLS* option to enable encryption.
10. Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
11. In the *TLS certificate* field, click ⚙ to generate TLS certificate, or click ⇧ to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.



TLS certificate

Certificate encryption passphrase | Passphrase

Common name

SHA1

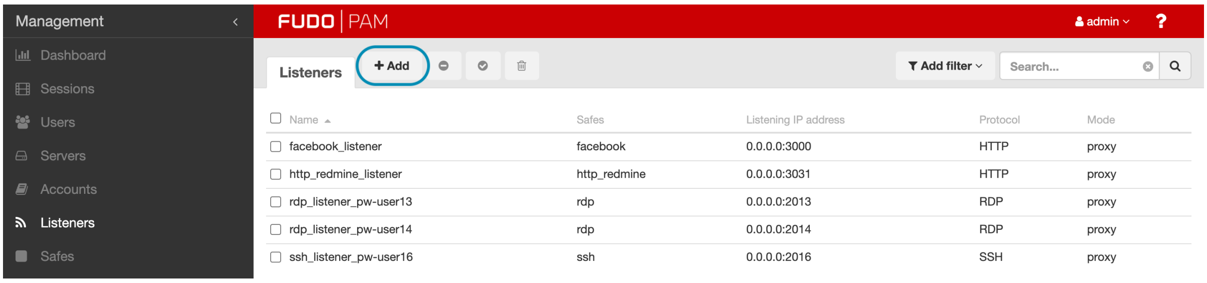
12. Click *Save*.

Related topics:

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

8.1.3 Creating an ICA listener

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



Name	Safes	Listening IP address	Protocol	Mode
□ facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
□ http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
□ rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
□ rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
□ ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `ICA` from the *Protocol* drop-down list.
6. In the *Permissions* section, add users allowed to manage this object.
7. In the *Connection* section, select desired connection mode.

bastion

Note:

- User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
- For details on bastion connection mode, refer to *Connection modes* topic.

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

gateway

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

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

proxy

Note:

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

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

> **Note:**
>
> - The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
> - Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
> - In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

transparent

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

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

8. Select *Use TLS* option to enable encryption.
9. Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
10. In the *TLS certificate* field, click ⚙ to generate TLS certificate, or click ⊙ to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.

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

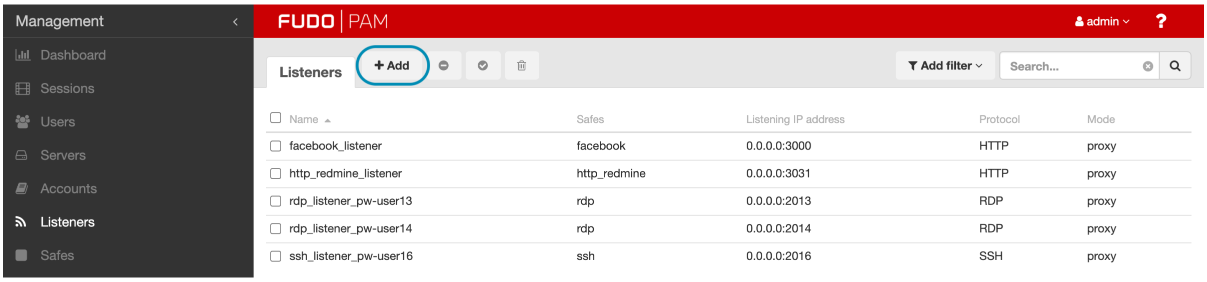
11. Click *Save*.

Related topics:

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

8.1.4 Creating a Modbus listener

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



Name	Safes	Listening IP address	Protocol	Mode
□ facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
□ http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
□ rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
□ rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
□ ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `Modbus` from the *Protocol* drop-down list.
6. In the *Permissions* section, add users allowed to manage this object.
7. In the *Connection* section, select desired connection mode.

   gateway

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

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

   proxy

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

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

   > **Note:**
   >
   > - The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
   > - Selecting the `Any` option will result in Fudo listening on all configured IP addresses.

- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

transparent

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

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

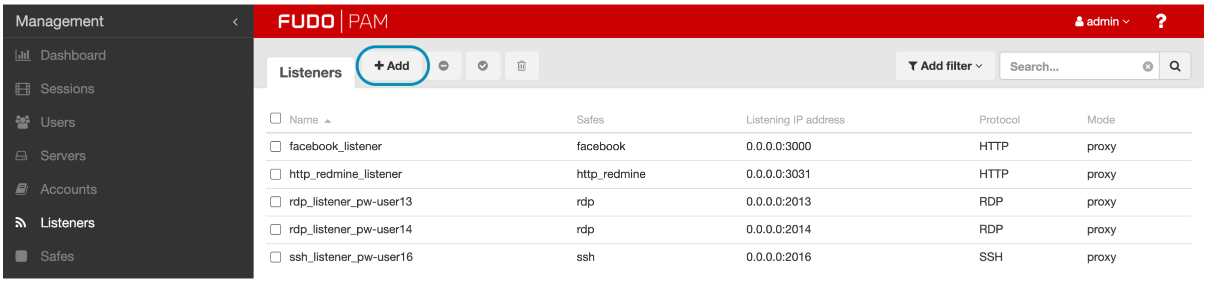
8. Click *Save*.

Related topics:

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

8.1.5 Creating a MySQL listener

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



Name	Safes	Listening IP address	Protocol	Mode
facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `MySQL` from the *Protocol* drop-down list.
6. In the *Permissions* section, add users allowed to manage this object.
7. In the *Connection* section, select desired connection mode.

   gateway

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

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

proxy

Note:

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

transparent

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

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

8. Click *Save*.

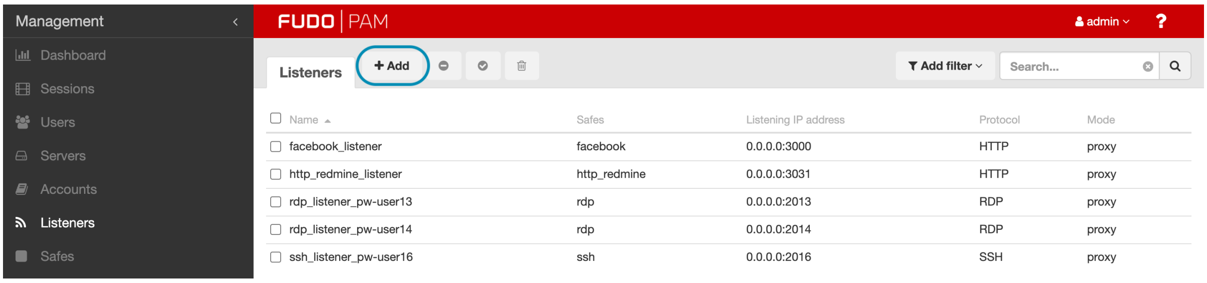
Related topics:

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

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

8.1.6 Creating an RDP listener

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



□ Name	Safes	Listening IP address	Protocol	Mode
□ facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
□ http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
□ rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
□ rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
□ ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `RDP` from the *Protocol* drop-down list.
6. From the `Security` drop-down list, select RDP connection security mode.

Note: Security mode must match the security mode setting in the *RDP server configuration*.

In case *Enhanced RDP Security (TLS)* or *Enhanced RDP Security (TLS) + NLA* option is chosen, select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing RDP connections.

7. In the *Announcement* field, type in the announcement that will be presented to the user on the login screen.
8. In the *Permissions* section, add users allowed to manage this object.
9. In the *Connection* section, select desired connection mode.

   bastion

   Note:

   - User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
   - For details on bastion connection mode, refer to *Connection modes* topic.

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

   Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

- In the *External address* field, enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Note: The external address is listed in *user portal* and it enables establishing connections from external networks.

---

gateway

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

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

proxy

Note:

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.

- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

- In the *External address* field, enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Note: The external address is listed in *user portal* and it enables establishing connections from external networks.

---

transparent

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

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

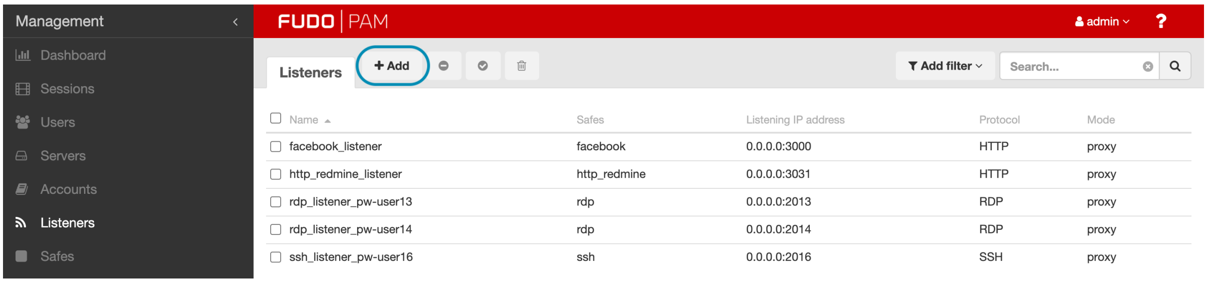
10. In the *TLS certificate* field, click ⚙ to generate TLS certificate, or click ⬆ to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.
11. Click *Save*.

Related topics:

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

8.1.7 Creating an SSH listener

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



Name	Safes	Listening IP address	Protocol	Mode
facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select the *Case insensitivity* option to disable case sensitivity in the username string when connecting over this listener.
6. Select `SSH` from the *Protocol* drop-down list.
7. Select *ProxyJump* option to allow an intermediary system to connect to the target server.
8. Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing SSH connections.
9. In the *Announcement* field, type in the announcement that will be presented to the user on the login screen.
10. In the *Permissions* section, add users allowed to manage this object.
11. In the *Connection* section, select desired connection mode.

    bastion

    Note:

    - User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
    - For details on bastion connection mode, refer to *Connection modes* topic.

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

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

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

    Note:

    - The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
    - Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
    - In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

- In the *External address* field, enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Note: The external address is listed in *user portal* and it enables establishing connections from external networks.

gateway

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

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

proxy

Note:

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

- In the *External address* field, enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Note: The external address is listed in *user portal* and it enables establishing connections from external networks.

transparent

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

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

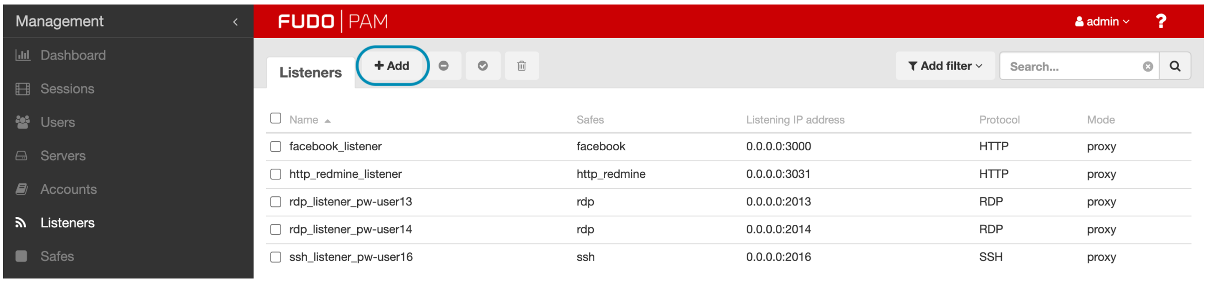
12. In the *Fudo public key* field, click ⬆ to upload (optionally provide encryption passphrase) or ⚙ to generate TLS certificate.
13. Click *Save*.

Related topics:

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

8.1.8 Creating a MS SQL listener

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



Name	Safes	Listening IP address	Protocol	Mode
facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `MS SQL (TDS)` from the *Protocol* drop-down list.
6. In the *Permissions* section, add users allowed to manage this object.
7. In the *Connection* section, select desired connection mode.

bastion

Note:

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

- For details on bastion connection mode, refer to *Connection modes* topic.

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

gateway

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

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

proxy

Note:

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

---

transparent

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

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

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

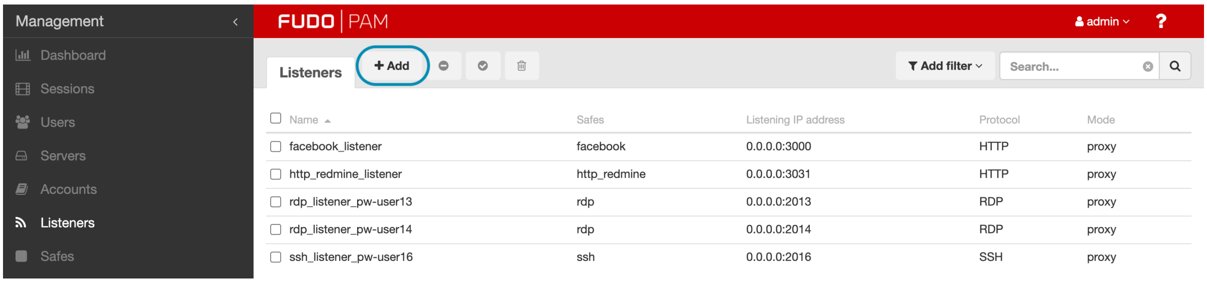
8. Click *Save*.

Related topics:

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

8.1.9 Creating a Telnet listener

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



Name	Safes	Listening IP address	Protocol	Mode
facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `Telnet` from the *Protocol* drop-down list.
6. In the *Permissions* section, add users allowed to manage this object.
7. In the *Connection* section, select desired connection mode.

   bastion

   Note:

   - User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
   - For details on bastion connection mode, refer to *Connection modes* topic.

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

   gateway

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

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

proxy

Note:

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

transparent

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

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

8. Select the *Use TLS* option to enable encryption.
9. Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
10. In the *TLS certificate* field, click ⚙ to generate TLS certificate, or click ⊙ to upload server certificate file with private key pasted at the end of the file. The rest of the required

fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.

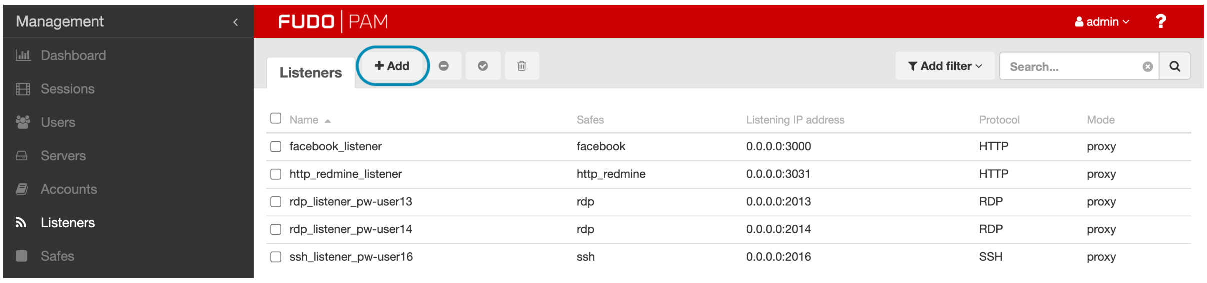
11. Click *Save*.

Related topics:

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

8.1.10 Creating a Telnet 3270 listener

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



Name	Safes	Listening IP address	Protocol	Mode
facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `Telnet 3270` from the *Protocol* drop-down list.
6. In the *Permissions* section, add users allowed to manage this object.
7. In the *Connection* section, select desired connection mode.

   bastion

   Note:

   - User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
   - For details on bastion connection mode, refer to *Connection modes* topic.

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

   gateway

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

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

proxy

Note:

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

---

transparent

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

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

8. Select the *Use TLS* option to enable encryption.
9. Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
10. In the *TLS certificate* field, click ⚙ to generate TLS certificate, or click ⊙ to upload server certificate file with private key pasted at the end of the file. The rest of the required

fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.

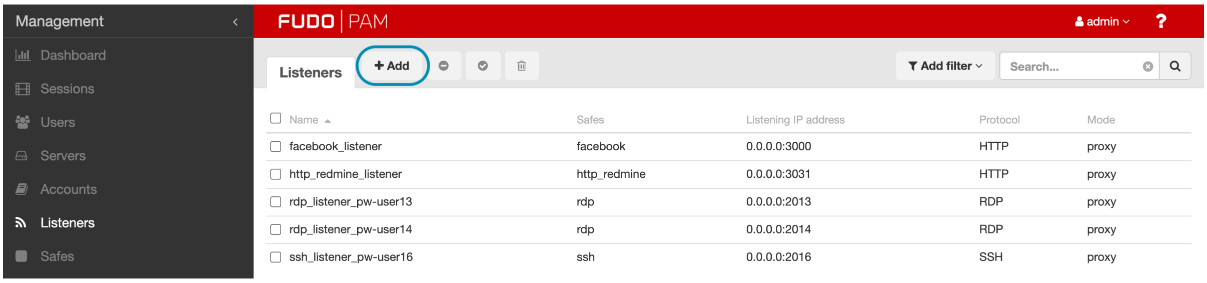
11. Click *Save*.

Related topics:

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

8.1.11 Creating a Telnet 5250 listener

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



□ Name	Safes	Listening IP address	Protocol	Mode
□ facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
□ http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
□ rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
□ rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
□ ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `Telnet 5250` from the *Protocol* drop-down list.
6. In the *Permissions* section, add users allowed to manage this object.
7. In the *Connection* section, select desired connection mode.

   bastion

   Note:

   - User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
   - For details on bastion connection mode, refer to *Connection modes* topic.

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

   gateway

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

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

proxy

Note:

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

transparent

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

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

8. Select the *Use TLS* option to enable encryption.
9. Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
10. In the *TLS certificate* field, click **|icon-generate-key|** to generate TLS certificate, or click **|icon-upload-key|** to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the

server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.

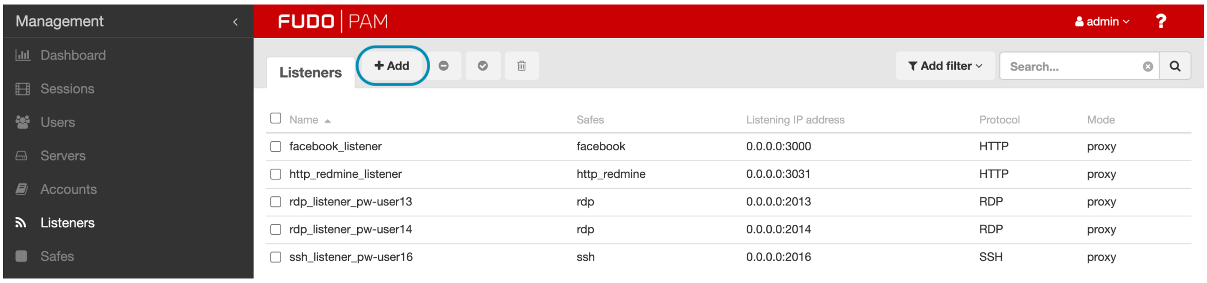
11. Click *Save*.

Related topics:

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

8.1.12 Creating a VNC listener

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



Name	Safes	Listening IP address	Protocol	Mode
facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `VNC` from the *Protocol* drop-down list.
6. In the *Announcement* field, type in the announcement that will be presented to the user on the login screen.
7. In the *Permissions* section, add users allowed to manage this object.
8. In the *Connection* section, select desired connection mode.

   bastion

   Note:

   - User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
   - For details on bastion connection mode, refer to *Connection modes* topic.

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

Note:

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

- In the *External address* field, enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Note: The external address is listed in *user portal* and it enables establishing connections from external networks.

gateway

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

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

proxy

Note:

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.

- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

- In the *External address* field, enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Note: The external address is listed in *user portal* and it enables establishing connections from external networks.

---

transparent

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

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

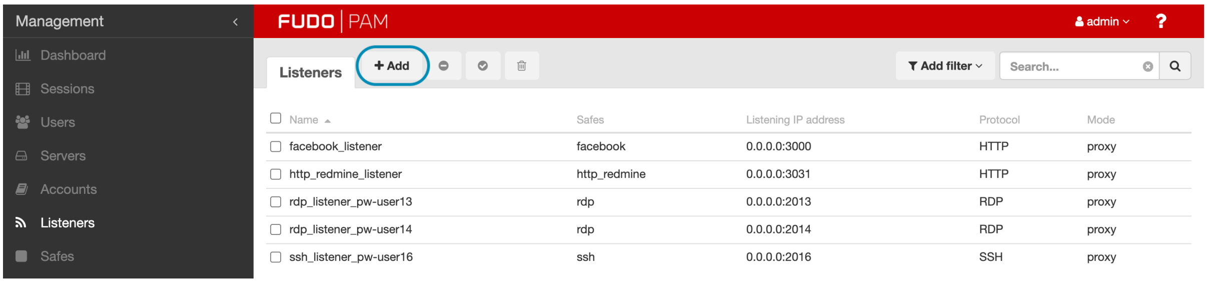
9. Click *Save*.

Related topics:

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

8.1.13 Creating a TCP listener

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



☐ Name	Safes	Listening IP address	Protocol	Mode
☐ facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
☐ http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
☐ rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
☐ rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
☐ ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy

3. Enter listener's unique name.
4. Select *Blocked* option to disable access to servers through this listener after it's created.
5. Select `TCP` from the *Protocol* drop-down list.

6. In the *Permissions* section, add users allowed to manage this object.
7. In the *Connection* section, select desired connection mode.

gateway

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

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

proxy

Note:

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

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

Note:

- The *Local address* drop-down list elements are IP address defined in the *Network configuration* menu (*Network interfaces configuration*) or labeled IP addresses (*Labeled IP addresses*).
- Selecting the `Any` option will result in Fudo listening on all configured IP addresses.
- In case of cluster configuration, select a labeled IP address from the *Local address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

- In the *External address* field, enter an IP address (or FQDN name) along with the port number, under which Fudo can be accessed from outside the local network.

Note: The external address is listed in *user portal* and it enables establishing connections from external networks.

transparent

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

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

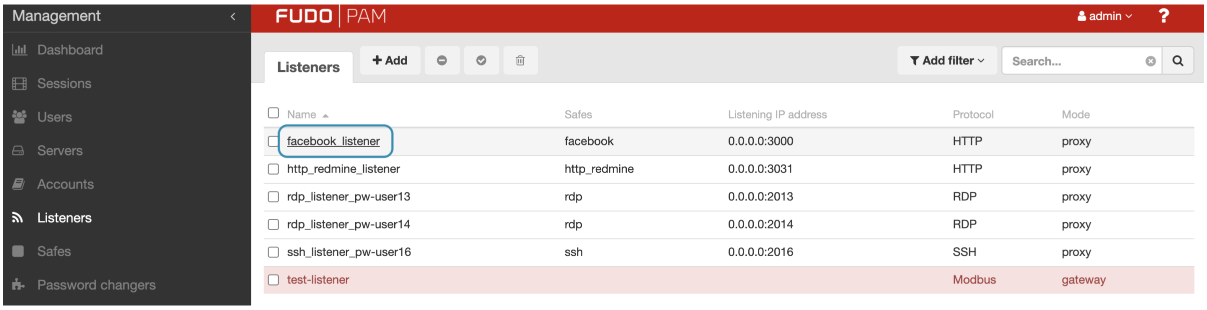
8. Click *Save*.

Related topics:

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

8.2 Editing a listener

1. Select *Management* > *Listeners*.
2. Find and click on a name of the desired listener to access its configuration parameters.



☐ Name	Safes	Listening IP address	Protocol	Mode
☐ facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
☐ http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
☐ rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
☐ rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
☐ ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy
☐ test-listener			Modbus	gateway

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

3. Modify configuration values as needed.
4. Click *Save*.

Related topics:

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

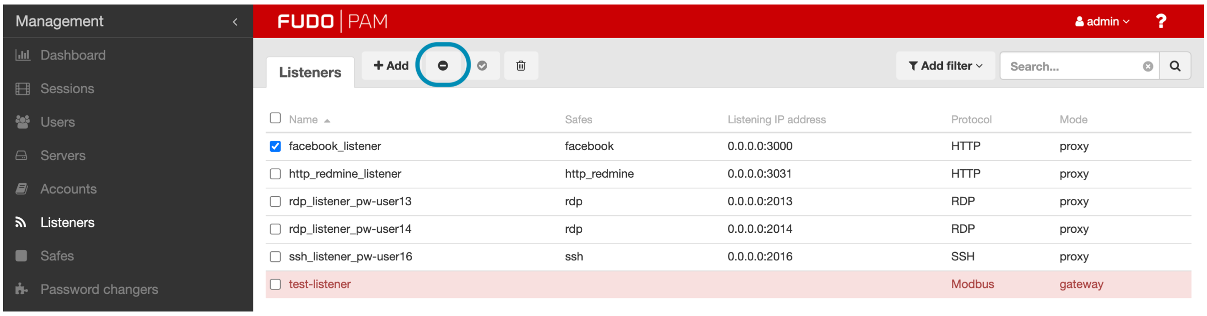
8.3 Blocking a listener

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

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

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

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



	Name	Safes	Listening IP address	Protocol	Mode
☑	facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
☐	http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
☐	rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
☐	rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
☐	ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy
☐	test-listener			Modbus	gateway

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

Related topics:

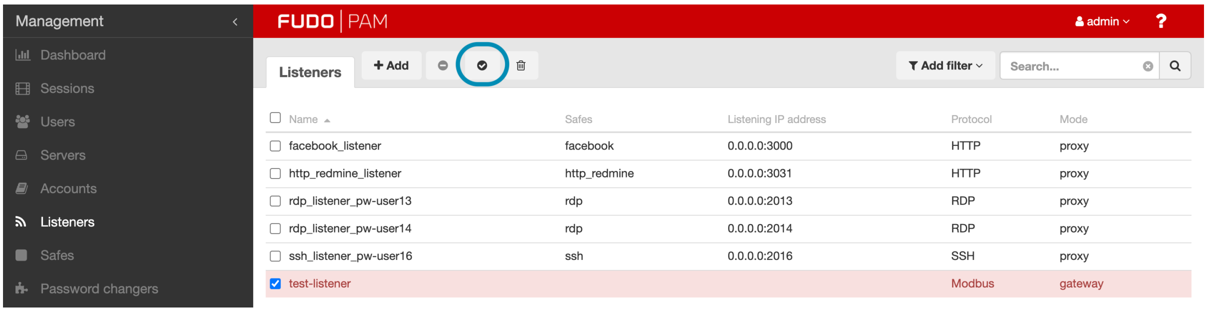
- *Data model*
- *System initiation*
- *Servers*

8.4 Unblocking a listener

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

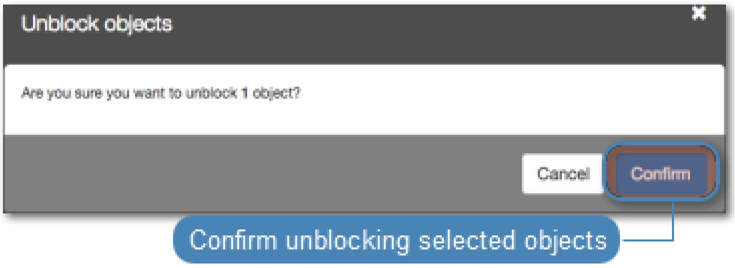
Note: Define filters to limit the number of objects displayed on the list.

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



	Name	Safes	Listening IP address	Protocol	Mode
☐	facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
☐	http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
☐	rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
☐	rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
☐	ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy
☑	test-listener			Modbus	gateway

4. Click *Confirm* to unblock selected objects.



Are you sure you want to unblock 1 object?

Confirm unblocking selected objects

Related topics:

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

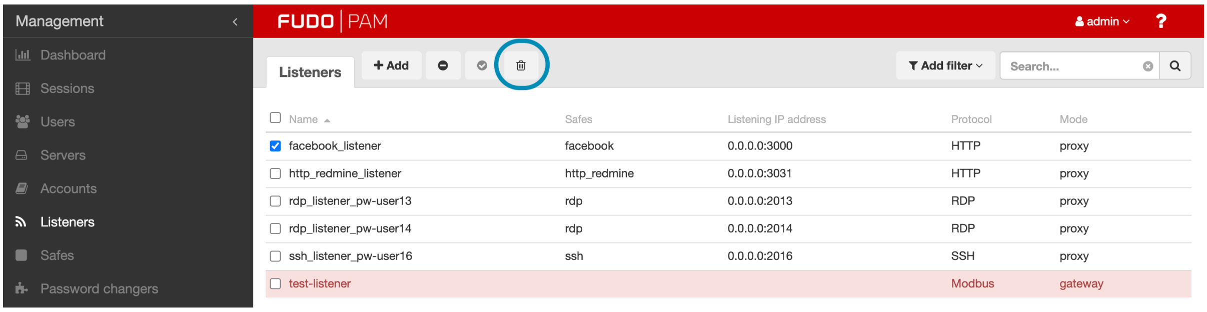
8.5 Deleting a listener

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

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

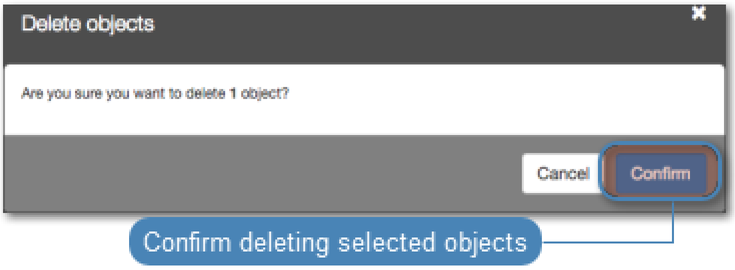
Note: Define filters to limit the number of objects displayed on the list.

3. Click *Delete*.



□ Name	Safes	Listening IP address	Protocol	Mode
☑ facebook_listener	facebook	0.0.0.0:3000	HTTP	proxy
□ http_redmine_listener	http_redmine	0.0.0.0:3031	HTTP	proxy
□ rdp_listener_pw-user13	rdp	0.0.0.0:2013	RDP	proxy
□ rdp_listener_pw-user14	rdp	0.0.0.0:2014	RDP	proxy
□ ssh_listener_pw-user16	ssh	0.0.0.0:2016	SSH	proxy
□ test-listener			Modbus	gateway

4. Confirm deleting selected objects.



Are you sure you want to delete 1 object?

Confirm deleting selected objects

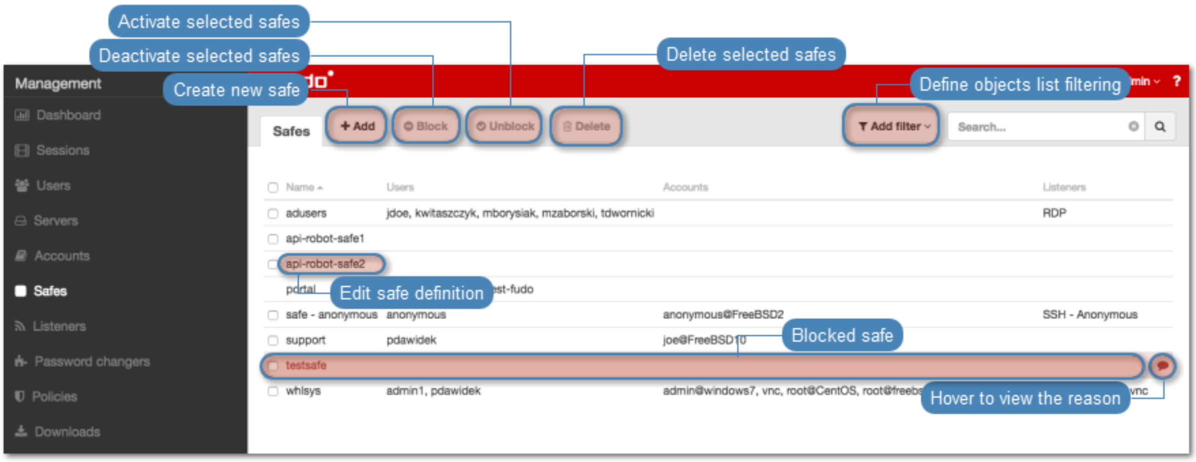
Related topics:

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

CHAPTER 9

Safes

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



Activate selected safes

Deactivate selected safes

Create new safe

Delete selected safes

Define objects list filtering

Edit safe definition

Blocked safe

Hover to view the reason

Name	Users	Accounts	Listeners
adusers	jdoe, kwitaszczyk, mborysiak, mzaborski, tdwornicki		RDP
api-robot-safe1			
api-robot-safe2			
portal	st-fudo		
safe - anonymous	anonymous	anonymous@FreeBSD2	SSH - Anonymous
support	pdawidek	joe@FreeBSD10	
testsafe			
whisys	admin1, pdawidek	admin@windows7, vnc, root@CentOS, root@freebs	vnc

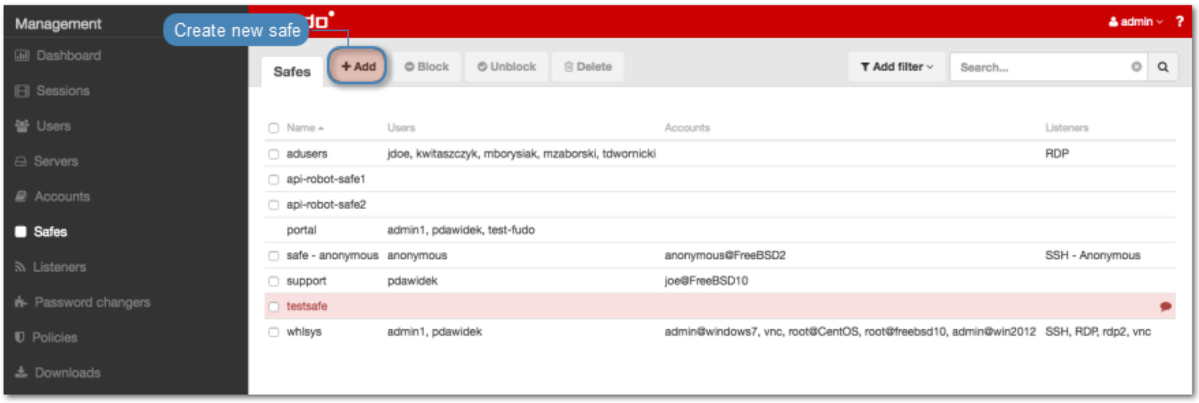
Note:

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

9.1 Creating a safe

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

1. Select *Management* > *Safes*.



Name	Users	Accounts	Listeners
□ adusers	jdoe, kwitaszczyk, mborysiak, mzaborski, tdwornicki		RDP
□ api-robot-safe1			
□ api-robot-safe2			
portal	admin1, pdawidek, test-fudo		
□ safe - anonymous	anonymous	anonymous@FreeBSD2	SSH - Anonymous
□ support	pdawidek	joe@FreeBSD10	
□ testsafe			
□ whisys	admin1, pdawidek	admin@windows7, vnc, root@CentOS, root@freebsd10, admin@win2012	SSH, RDP, rdp2, vnc

2. Click + *Add*.

3. Enter object's name.

4. Select *Blocked* option to disable access to object after it's created.

5. Select system events, about which you want to be notified.

Note:

- Notification settings are applied only to the currently logged in Fudo PAM administrator/operator (user with a *superadmin*, *admin* or *operator* role). Each system administrator/operator must log in to Fudo PAM web interface and adjust their settings individually to receive notifications regarding a particular safe.

6. Select *Login reason* option, to display prompt upon logging in, asking user to enter login reason.

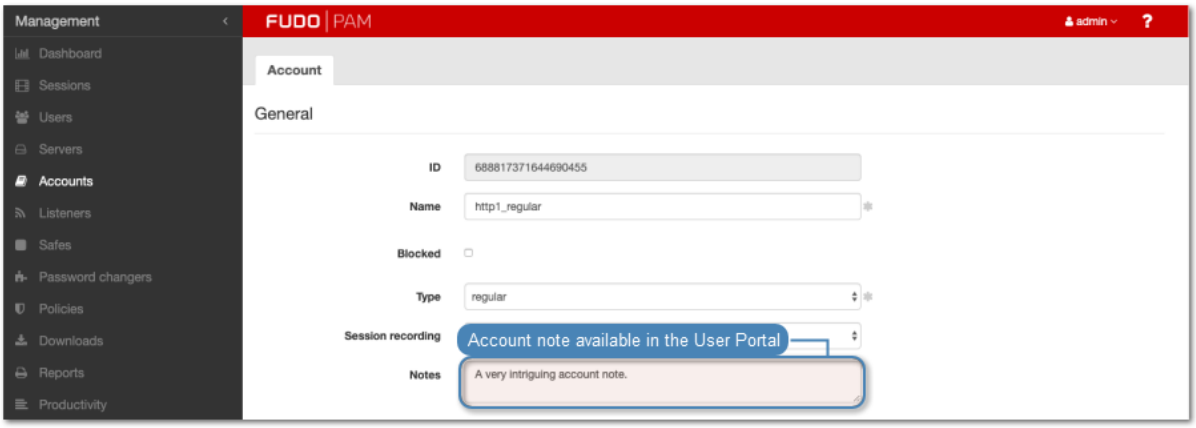
Note: Login reason is not supported in *HTTP* connections.

7. Select *Require approval* option to have the administrator approve each connection to servers accessed through configured safe. Provide how many minutes the administrator has to approve or reject a request.

8. Assign *security policies* in the *Policies* field.

9. From the *Note access* drop-down list, select user access rights to account related notes.

Note: Notes can be accessed either from the account edit form

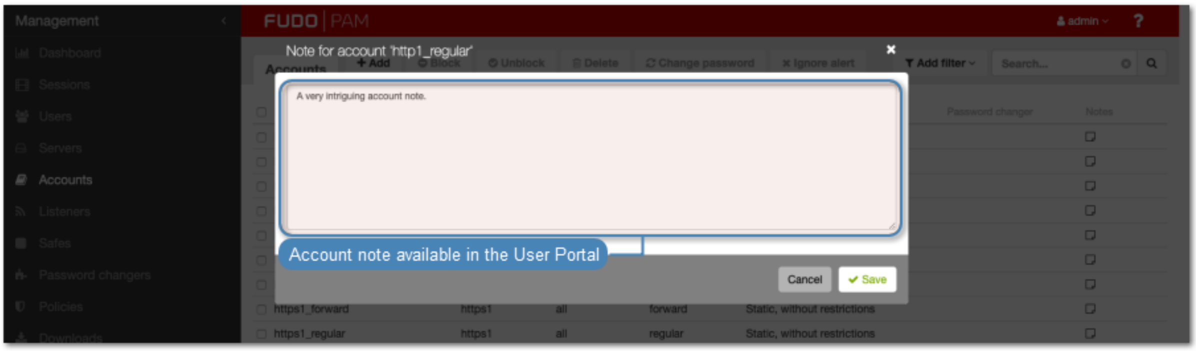


General

ID	6888173716446904455
Name	http1_regular
Blocked	□
Type	regular
Session recording	
Notes	A very intriguing account note.

Account note available in the User Portal

accounts list



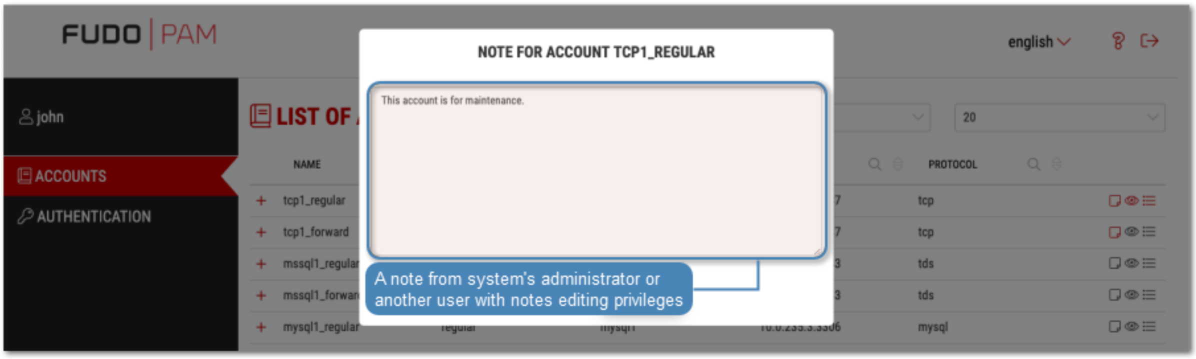
Note for account 'http1_regular'

A very intriguing account note.

Account note available in the User Portal

https1_forward	https1	all	forward	Static, without restrictions
https1_regular	https1	all	regular	Static, without restrictions

or in the *User Portal*.

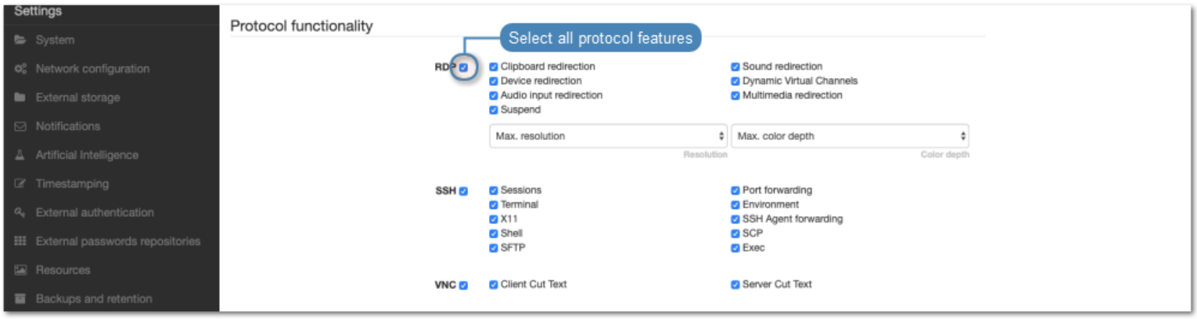


NOTE FOR ACCOUNT TCP1_REGULAR

This account is for maintenance.

A note from system's administrator or another user with notes editing privileges

10. Select *Session time limit* option and input a minutes value.
11. Select *Session inactivity limit* option and input a minutes value.
12. For RDP and SSH-based safes, select *WEB Client* option to allow connecting to the session in browser.
13. In the *Protocol functionality* section, select allowed protocols' features.



Protocol functionality

RDP ☑
☑ Clipboard redirection ☑ Sound redirection
☑ Device redirection ☑ Dynamic Virtual Channels
☑ Audio input redirection ☑ Multimedia redirection
☑ Suspend
Max. resolution
Max. color depth

SSH ☑
☑ Sessions ☑ Port forwarding
☑ Terminal ☑ Environment
☑ X11 ☑ SSH Agent forwarding
☑ Shell ☑ SCP
☑ SFTP ☑ Exec

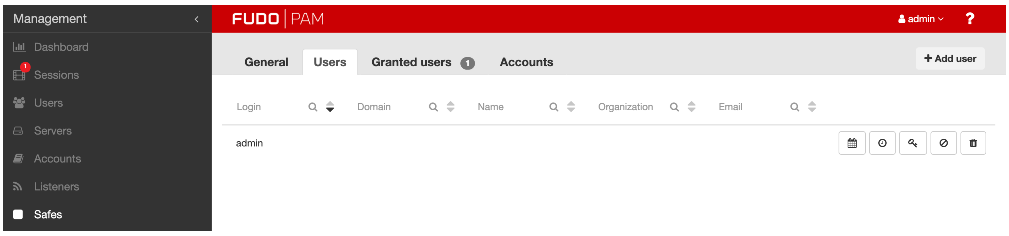
VNC ☑
☑ Client Cut Text ☑ Server Cut Text

Note: With the *Suspend* option enabled for the RDP sessions, its content will not be available for viewing when the user minimizes its client application.

With the *Client Cut Text* option enabled for the VNC sessions, a user is allowed to paste text into the VNC server computer.

With the *Server Cut Text* option enabled for the VNC sessions, a user is allowed to copy and paste text from the VNC server computer into the user's computer.

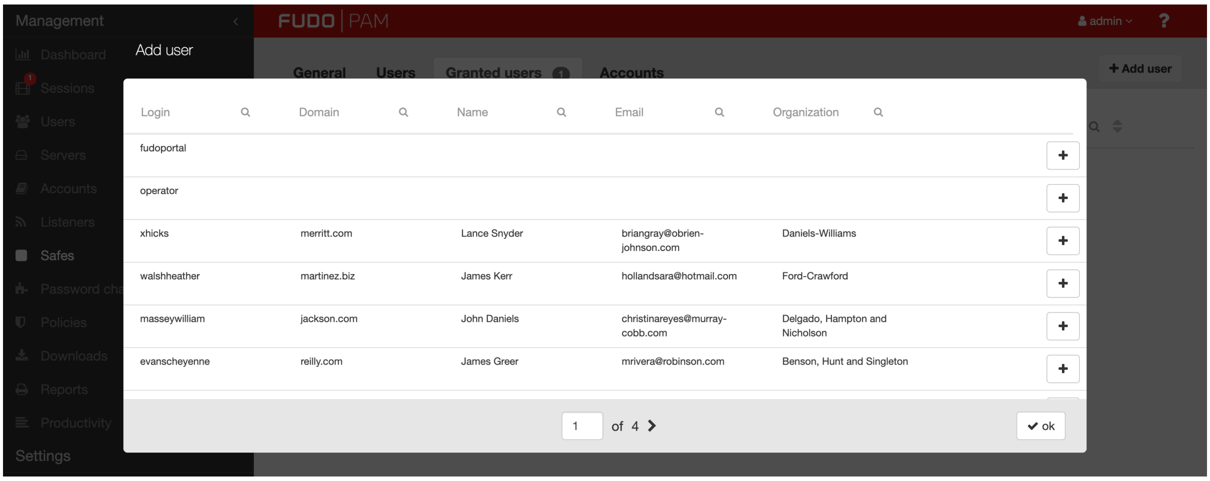
14. Select **Users** tab to assign users allowed to access accounts assigned to this safe.
15. Click *+ Add user*.
16. Click + to add users.
17. Click *ok* to close the modal window.
18. Define safe access options.



admin

- Click 📅 to define the timeframe when given user can access this object.
- Click ⊙ to define daily access policy.
- Click 🔑 to allow user to use Secret Checkout feature and view passwords in the User Portal.
- Click ⊘ to disable access for selected user.
- Click an icon to delete selected user from the safe.

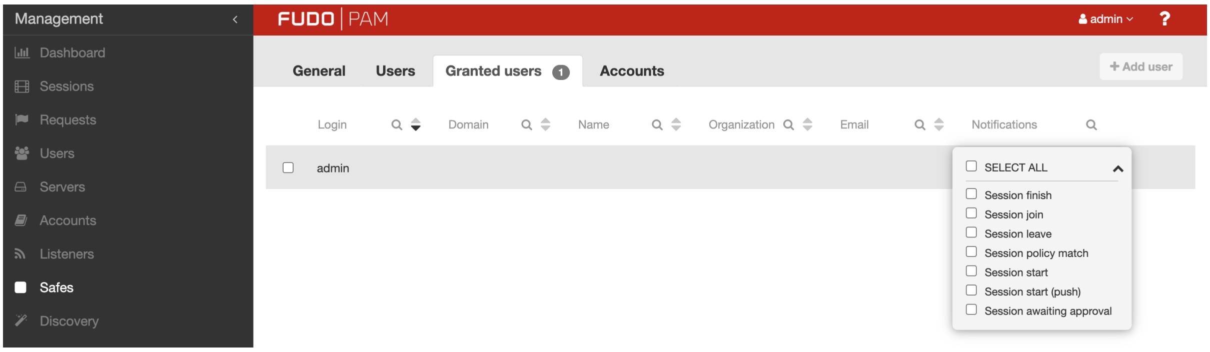
19. Select **Granted users** tab to assign users allowed to manage this object.
20. Click *+ Add user*.
21. Click + to add users.



Login	Domain	Name	Email	Organization	
fudoportal					+
operator					+
xhicks	merritt.com	Lance Snyder	briangray@obrien-johnson.com	Daniels-Williams	+
walshheather	martinez.biz	James Kerr	hollandsara@hotmail.com	Ford-Crawford	+
masseywilliam	jackson.com	John Daniels	christinareyes@murray-cobb.com	Delgado, Hampton and Nicholson	+
evanscheyenne	reilly.com	James Greer	mrivera@robinson.com	Benson, Hunt and Singleton	+

1 of 4 ✓ ok

22. Select notifications that will be enabled for the particular granted user:

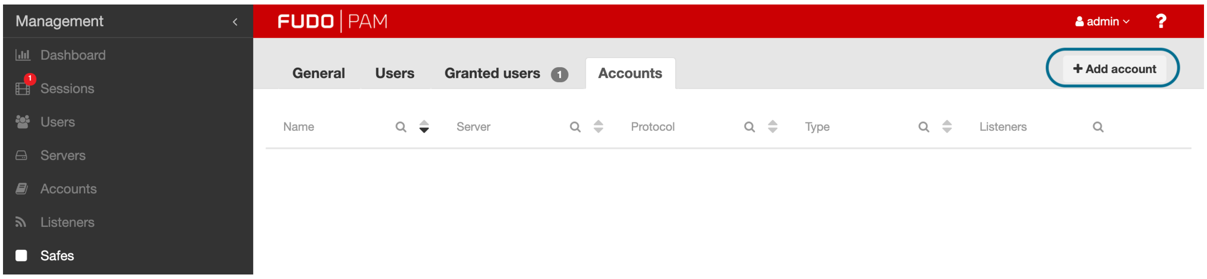


	Login	Domain	Name	Organization	Email	Notifications
□	admin					

23. Click *ok* to close the modal window.

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

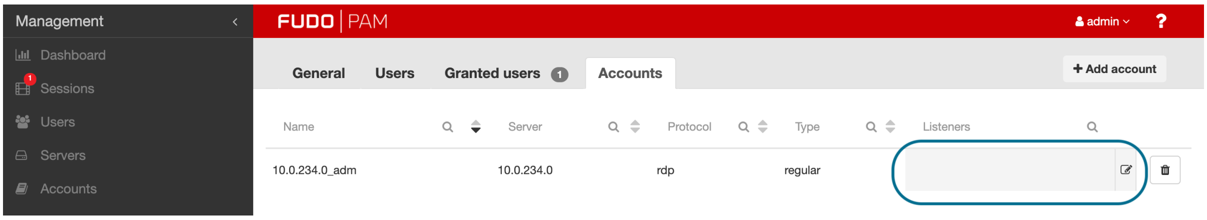
25. Click *+ Add account.*



26. Click + to add accounts.

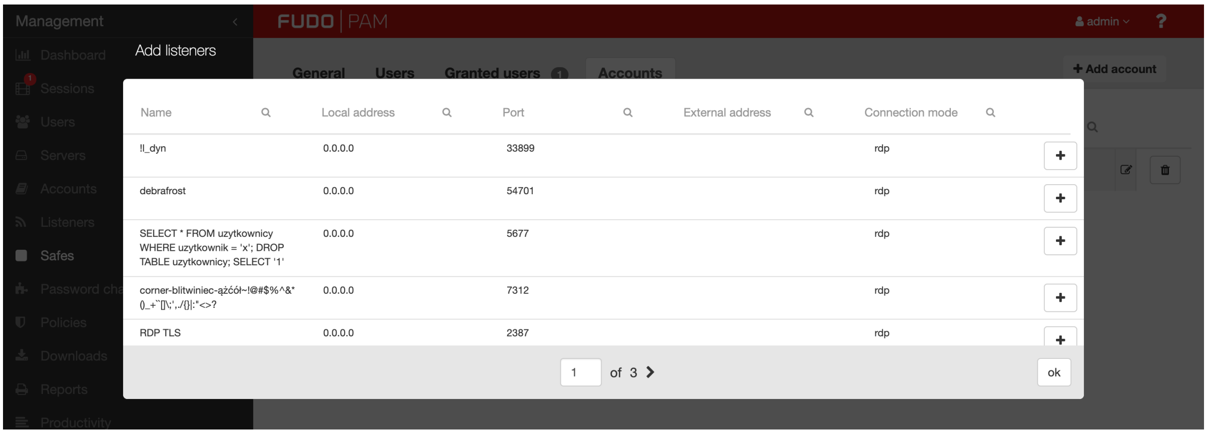
27. Click *ok* to close the modal window.

28. Click ✎ to assign listeners to accounts.



Name	Server	Protocol	Type	Listeners
10.0.234.0_adm	10.0.234.0	rdp	regular	

29. Click + to add listeners.



Add listeners

Name	Local address	Port	External address	Connection mode	
!l_dyn	0.0.0.0	33899		rdp	+
debrafrost	0.0.0.0	54701		rdp	+
SELECT * FROM uzytkownicy WHERE uzytkownik = 'x'; DROP TABLE uzytkownicy; SELECT '1'	0.0.0.0	5677		rdp	+
corner-blitwiniec-ążćół~!@#$%^&*()_+`[]\;',./{}|:"<>?	0.0.0.0	7312		rdp	+
RDP TLS	0.0.0.0	2387		rdp	+

1 of 3 ok

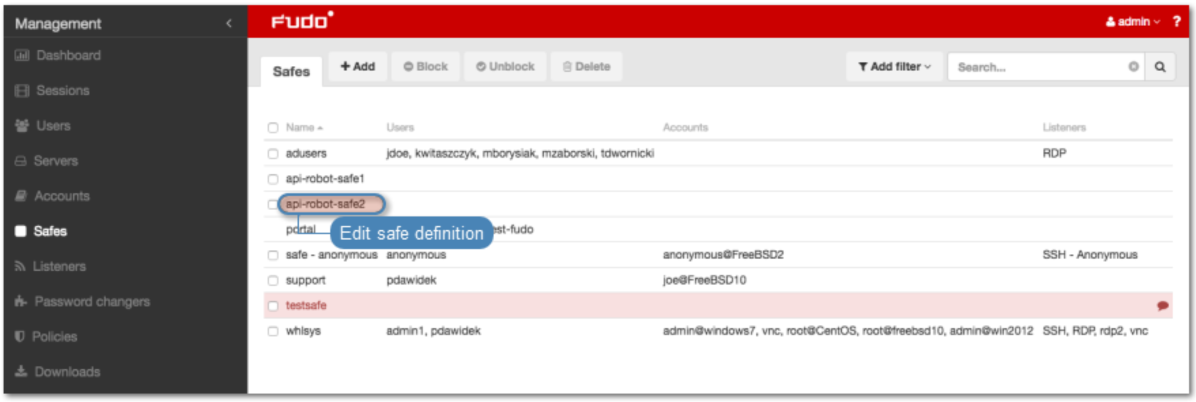
30. Click *ok* to close the modal window.
31. Click *Save*.

Related topics:

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

9.2 Editing a safe

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

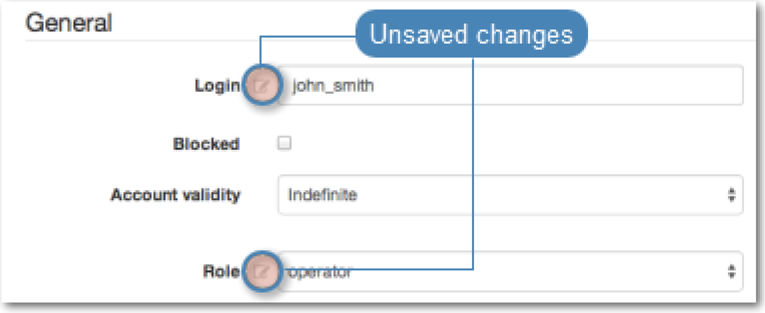


□ Name	Users	Accounts	Listeners
□ adusers	jdoe, kwitaszczyk, mborysiak, mzaborski, tdwornicki		RDP
□ api-robot-safe1			
□ api-robot-safe2			
portal	...est-fudo		
□ safe - anonymous	anonymous	anonymous@FreeBSD2	SSH - Anonymous
□ support	pdawidek	joe@FreeBSD10	
□ testsafe			
□ whisys	admin1, pdawidek	admin@windows7, vnc, root@CentOS, root@freebsd10, admin@win2012	SSH, RDP, rdp2, vnc

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

3. Modify configuration parameters as needed.

Note: Unsaved changes are marked with the ✎ icon.



General

Login	john_smith
Blocked	☐
Account validity	Indefinite
Role	operator

4. Click *Save*.

Related topics:

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

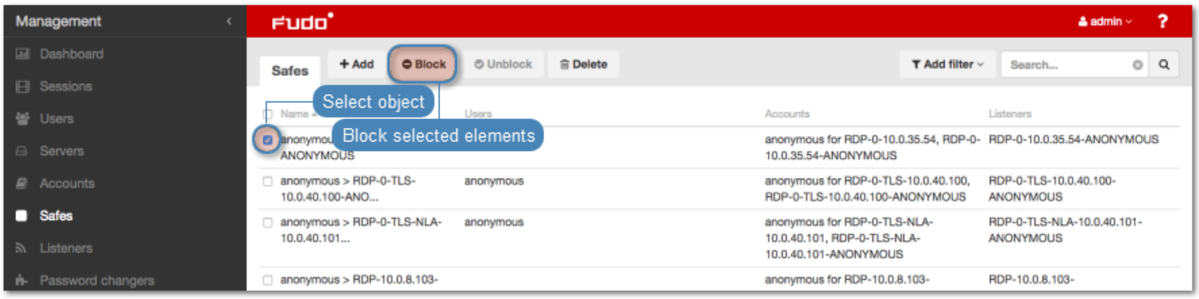
9.3 Blocking a safe

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

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

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

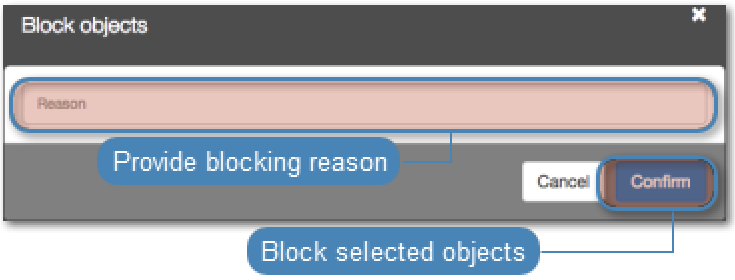
3. Click *Block*.



	Name	Users	Accounts	Listeners
☑	anonymou… ANONYMOUS		anonymous for RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	RDP-0-10.0.35.54-ANONYMOUS
☐	anonymous > RDP-0-TLS-10.0.40.100-ANO...	anonymous	anonymous for RDP-0-TLS-10.0.40.100, RDP-0-TLS-10.0.40.100-ANONYMOUS	RDP-0-TLS-10.0.40.100-ANONYMOUS
☐	anonymous > RDP-0-TLS-NLA-10.0.40.101...	anonymous	anonymous for RDP-0-TLS-NLA-10.0.40.101, RDP-0-TLS-NLA-10.0.40.101-ANONYMOUS	RDP-0-TLS-NLA-10.0.40.101-ANONYMOUS
☐	anonymous > RDP-10.0.8.103-		anonymous for RDP-10.0.8.103-	RDP-10.0.8.103-

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

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



Related topics:

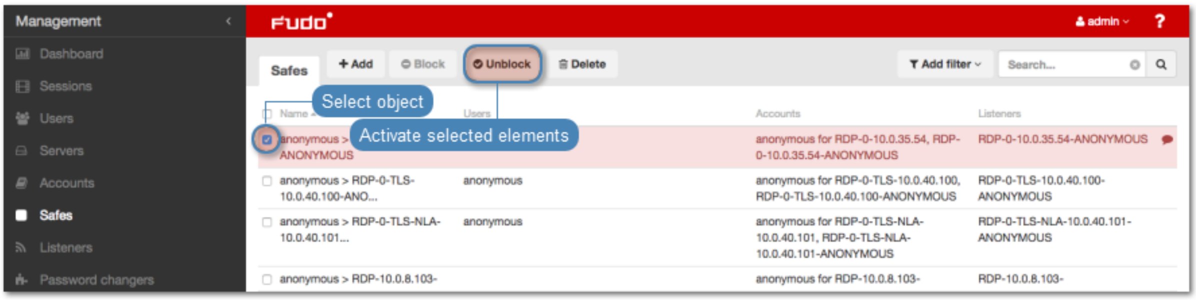
- *Unblocking a safe*
- *Data model*
- *Creating a safe*
- *Blocking a safe*

9.4 Unblocking a safe

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

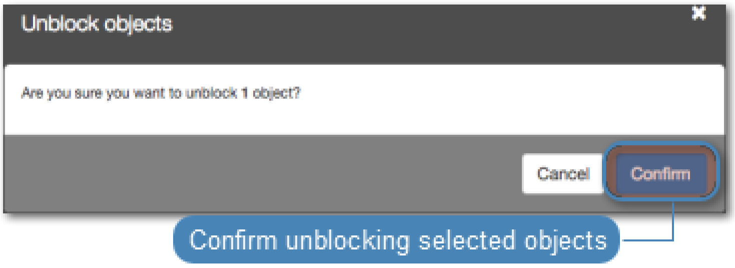
Note: Define filters to limit the number of objects displayed on the list.

3. Click *Unblock*.



Name	Users	Accounts	Listeners
☑ anonymous > ANONYMOUS		anonymous for RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	RDP-0-10.0.35.54-ANONYMOUS
□ anonymous > RDP-0-TLS-10.0.40.100-ANO...	anonymous	anonymous for RDP-0-TLS-10.0.40.100, RDP-0-TLS-10.0.40.100-ANONYMOUS	RDP-0-TLS-10.0.40.100-ANONYMOUS
□ anonymous > RDP-0-TLS-NLA-10.0.40.101...	anonymous	anonymous for RDP-0-TLS-NLA-10.0.40.101, RDP-0-TLS-NLA-10.0.40.101-ANONYMOUS	RDP-0-TLS-NLA-10.0.40.101-ANONYMOUS
□ anonymous > RDP-10.0.8.103-		anonymous for RDP-10.0.8.103-	RDP-10.0.8.103-

4. Click *Confirm* to unblock selected objects.



Are you sure you want to unblock 1 object?

Related topics:

- *Blocking a safe*
- *Data model*

- *Creating a safe*
- *Deleting a safe*

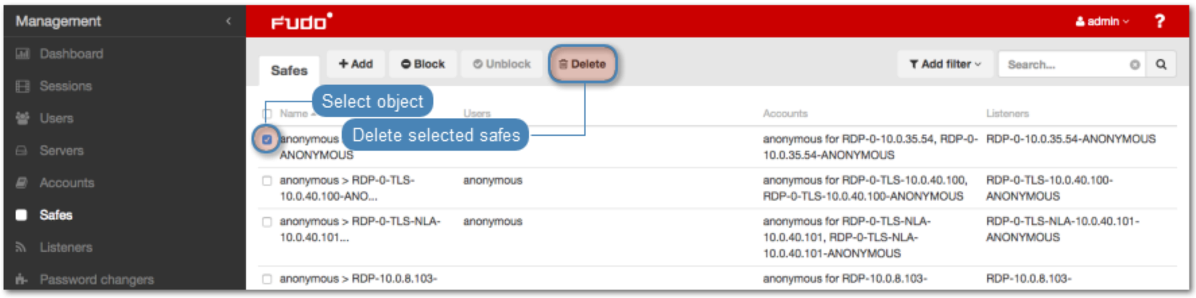
9.5 Deleting a safe

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

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

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

3. Click *Delete*.

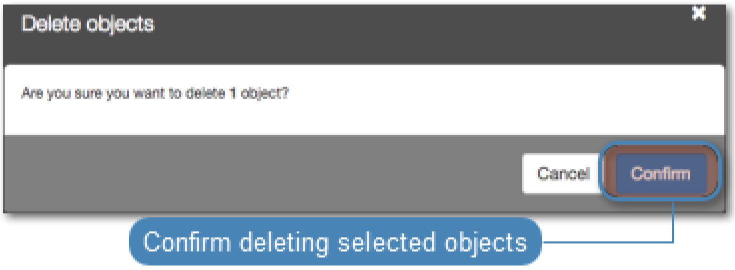


Select object

Delete selected safes

☐ Name	Users	Accounts	Listeners
☑ anonymous ANONYMOUS		anonymous for RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	RDP-0-10.0.35.54-ANONYMOUS
☐ anonymous > RDP-0-TLS-10.0.40.100-ANO...	anonymous	anonymous for RDP-0-TLS-10.0.40.100, RDP-0-TLS-10.0.40.100-ANONYMOUS	RDP-0-TLS-10.0.40.100-ANONYMOUS
☐ anonymous > RDP-0-TLS-NLA-10.0.40.101...	anonymous	anonymous for RDP-0-TLS-NLA-10.0.40.101, RDP-0-TLS-NLA-10.0.40.101-ANONYMOUS	RDP-0-TLS-NLA-10.0.40.101-ANONYMOUS
☐ anonymous > RDP-10.0.8.103-		anonymous for RDP-10.0.8.103-	RDP-10.0.8.103-

4. Confirm deletion of selected objects.



Are you sure you want to delete 1 object?

Confirm deleting selected objects

Related topics:

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

CHAPTER 10

Password changers

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

Password changers run on a separate transport layer: SSH, LDAP, Telnet or WinRM, and you can either use one of the built-in ones or *create your own script*. You can also *write custom plugins* and *upload* them to your Fudo PAM.

The built-in password changers cover the following scenarios:

- Unix over SSH
- MySQL over SSH
- Cisco over SSH and Telnet
- Cisco Enable Password over SSH and Telnet
- WinRM
- LDAP

10.1 Password changer policy

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

10.1.1 Defining a password changer policy

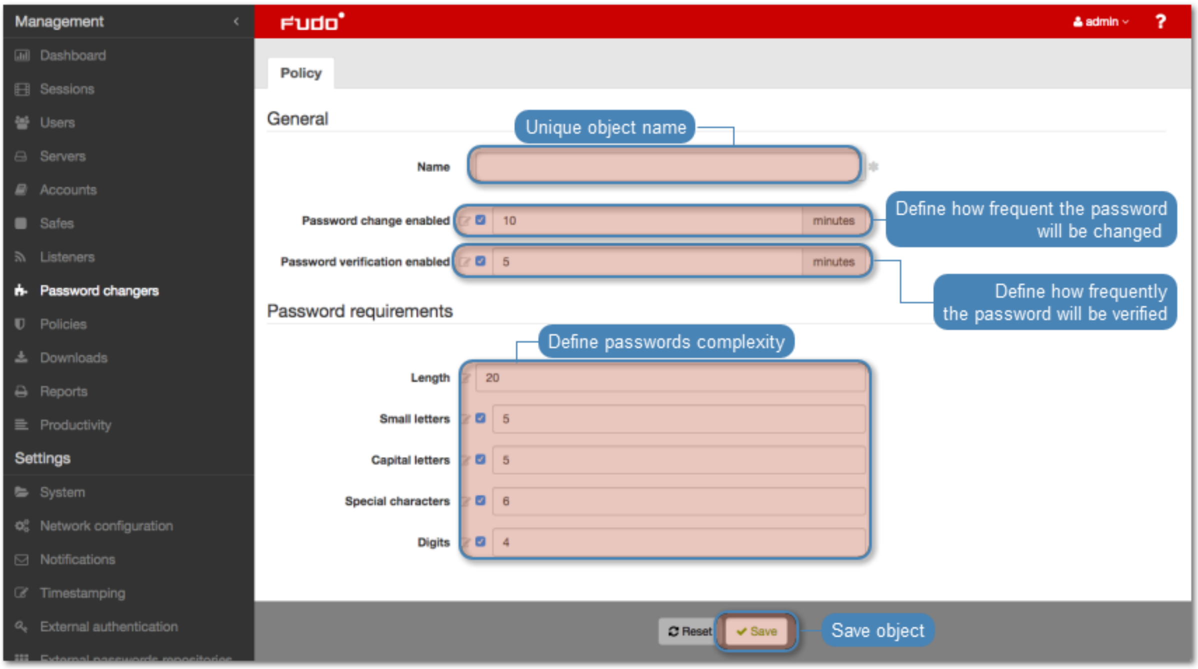
1. Select *Management > Password changers.*
2. Click *+ Add.*
3. Enter object name.

4. Select the *Password change enabled* option and specify the time interval between each password change.
5. Select the *Password verification enabled* option and specify the time interval between each password verification.
6. Define password complexity.

Parameter	Description
Length	Provide the number of characters comprising the password.
Small letters	Select to include lowercase characters, define their minimal number.
Capital letters	Select to include uppercase characters, define their minimal number.
Special characters	Select to include special characters, define their minimal number.
Digits	Select to include digits, define their minimal number.

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

7. Click *Save*.



General

Name

Password change enabled ☑ 10 minutes

Password verification enabled ☑ 5 minutes

Password requirements

Length 20

Small letters ☑ 5

Capital letters ☑ 5

Special characters ☑ 6

Digits ☑ 4

Unique object name

Define how frequent the password will be changed

Define how frequently the password will be verified

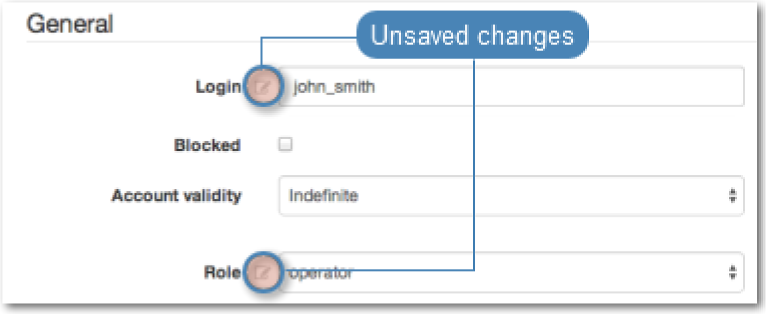
Define passwords complexity

Save object

10.1.2 Editing a password changer policy

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

Note: Unsaved changes are marked with an icon.



4. Click *Save*.

10.1.3 Deleting a password changer policy

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

Related topics:

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

10.2 Custom password changers

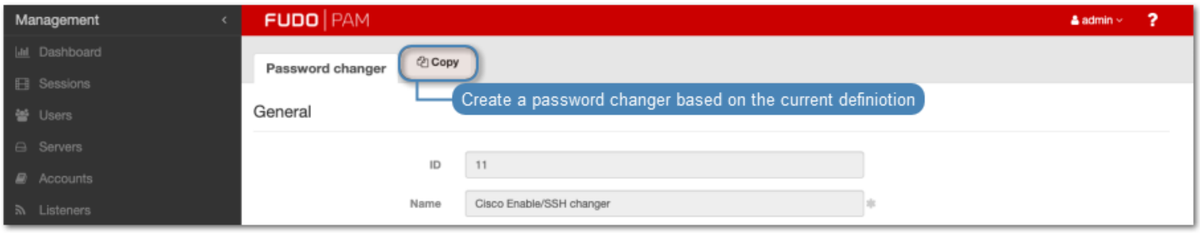
Custom password changers enable defining a set of commands executed on a remote host in case the built-in password changers cannot handle a specific use case scenario.

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

10.2.1 Defining a custom password changer

1. Select *Management > Password changers*.
2. Select *Custom changers* tab.
3. Click *+ Add*.

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

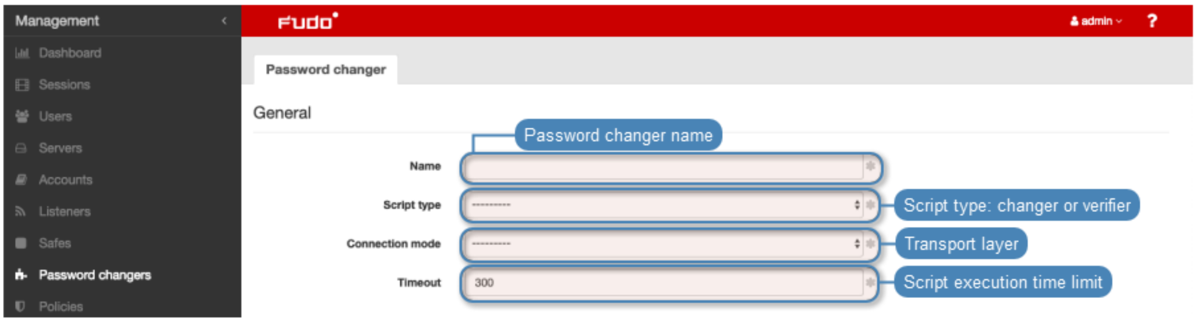


Create a password changer based on the current definiotion

ID 11

Name Cisco Enable/SSH changer

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



Password changer name

Name

Script type ---------

Script type: changer or verifier

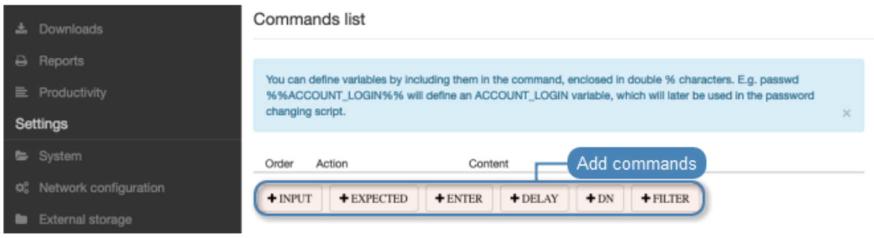
Connection mode ---------

Transport layer

Timeout 300

Script execution time limit

8. In the *Commands list* section, click + to add a command.



You can define variables by including them in the command, enclosed in double % characters. E.g. passwd %%ACCOUNT_LOGIN%% will define an ACCOUNT_LOGIN variable, which will later be used in the password changing script.

Add commands

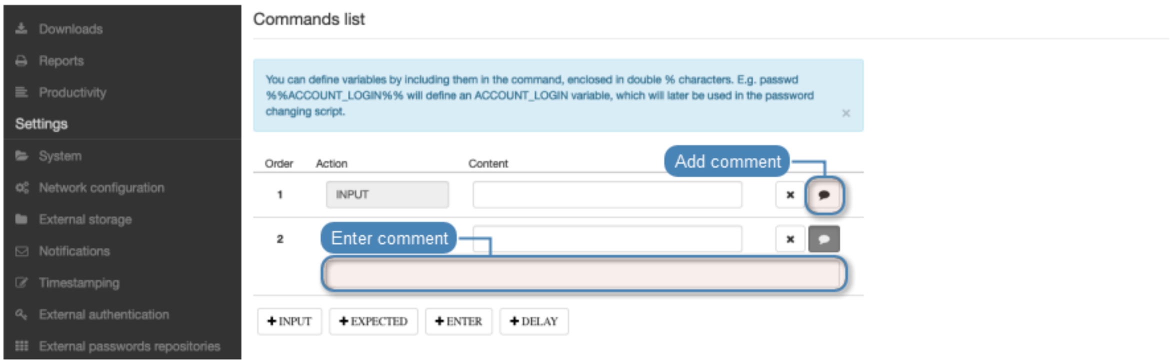
Note: Available commands depend on selected transport layer. For more information on connection modes, refer to the *Connection modes* topic.

- `INPUT` - command executed on target host.
- `EXPECTED` - output that is expected after executing a command.
- `ENTER`
- `DELAY` - delay between commands' execution.
- `DN` - directory service DN (Distinguished Name) parameter.
- `FILTER` - directory service user filter.

9. Enter the command or define action's parameters.

Note: You can use pre-defined transport layer or user defined variables in commands. To use or define a variable, enclose it in %% characters (e.g. `%%transport_host%%`, `%%custom_variable%%`).

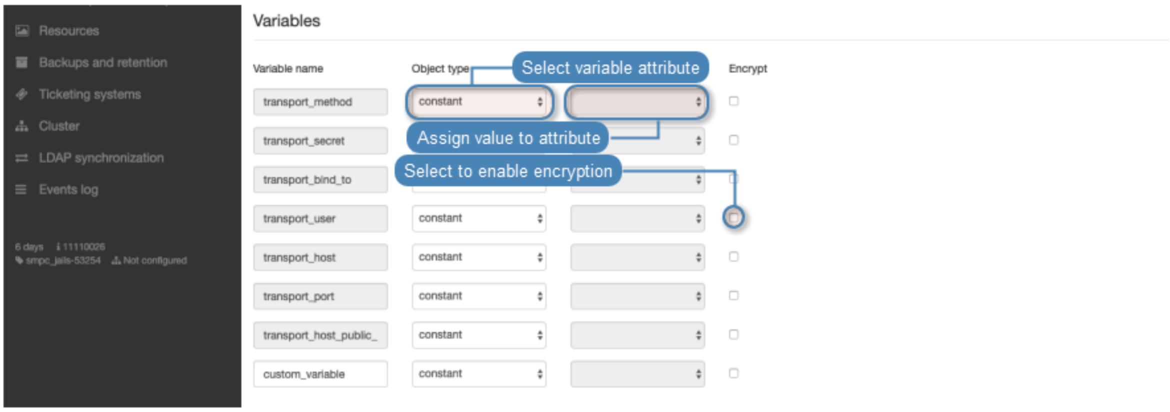
10. Click 💬 to add optional comment.



You can define variables by including them in the command, enclosed in double % characters. E.g. passwd %%ACCOUNT_LOGIN%% will define an ACCOUNT_LOGIN variable, which will later be used in the password changing script.

11. Repeat steps 8-10 to add more commands.

12. In the *Variables* section, define variables' attributes.



Note: Variables can be initiated with values referenced from other objects or they can be assigned a constant value.

13. Click *Save*.

14. *Define password change policy* and *assign the password changer to account*.

Note: Example

In this password changer example, the password change is triggered with the `passwd` command executed with sudo privileges on a host running FreeBSD operating system.

Commands list

	Action	Content	Comment
1	EXPECTED	`Password`	Expected terminal output with a 'Password' word in it.
2	INPUT	`%%transport_secret%%`	A value of the `transport_secret` variable is a secret for authorizing a priveleged account to change the password.
3	EXPECTED	`\[newtd_pc@john-laptop.*\]`	Expected terminal output within given regular expression.
4	INPUT	`sudo passwd %%account_login%%`	Change password for account where `account_login` reflects a login of the user, whose password is being changed.
5	EXPECTED	`Password`	Expected terminal output with 'Password' word in it.
6	INPUT	`%%transport_secret%%`	A value of the `transport_secret` variable is a secret for authorizing a priveleged account to change the password.
7	EXPECTED	`Changing local password`	Expected terminal output with 'Changing local password' phrase in it.
8	EXPECTED	`New Password`	Expected terminal output with 'New Password' phrase in it.
9	INPUT	`%%account_new_secret%%`	A value of the `account_new_secret` variable would be a new password.
10	EXPECTED	`Retype New Password`	Expected terminal output with 'Retype New Password' phrase in it.
11	INPUT	`%%account_new_secret%%`	A value of the `account_new_secret` variable would be a new password.
12	INPUT	`echo $?`	
13	EXPECTED	`0`	

Variables

Variable name	Object type	Object property	Encrypt
transport_method	constant		✗
transport_bind_to	server_property	bind_ip	✗
transport_user	account	login	✗
transport_host	server_address_property	host	✗
transport_port	server_property	port	✗
transport_secret	account	secret	✓
transport_host_public_key	constant		✗
account_login	account	login	✗

10.2.2 Editing a custom password changer

> **Warning:** Modifying a password changer, be aware that new variables will have to be initiated in every account instance that uses the modified password changer. You will be provided with the list of that accounts.

1. Select *Management > Password changers*.
2. Select *Custom changers* tab.
3. Click the name of desired password changer.
4. Edit selected commands.
5. Click *X* to remove selected command.
6. Click *Save*.

10.2.3 Deleting a custom password changer

1. Select *Management > Password changers*.
2. Select *Custom changers* tab.
3. Select desired elements and click *Delete*.
4. Confirm deleting selected objects.

Related topics:

- *Password changers - active cluster node*
- *Connection modes*
- *Accounts*
- *Password changer policy*
- *Setting up password changing on a Unix system*

10.3 Connection modes

Connection modes specifies transport layer used in the password change process. The transport layer determines the list of available commands and default variables.

10.3.1 SSH

SSH connection mode uses SSH protocol to establish connection with remote host.

Commands

Command	Description
INPUT	Command executed on target host.
EXPECTED	Expected result.
ENTER	
DELAY	Delay between commands' execution.

Variables

Variable	Description
transport_bind_ip	Fudo IP address used to establish connection with the remote host.
transport_host	An IP address of the remote host that the password changer/verifier connects to.
transport_host_public_key	Public key of the remote host.
transport_login	An account on the target system authorized to change passwords.
transport_method	Transport layer authentication method: `password` or `sshkey`.
transport_password_prompt	Regular expression describing the password prompt. **Note:** In case this parameter is defined as *constant* but the user does not explicitly define the value after the password changer is assigned to the account, the default string will be used to determine the password prompt.
transport_port	A port number that the password changer/verifier connects to.
transport_secret	Secret used to authorize the account to execute password change.
account_login	Login of the user whose password is being changed.
account_new_secret	System default variable initiated with the value automatically generated by Fudo.

10.3.2 LDAP

LDAP transport layer runs an LDAP query to change the password property of an object defined in the directory service.

Commands

Command	Description
DN	Directory service DN (Distinguished Name) parameter.
FILTER	Directory service user filter.

Note: Password changers based on the LDAP transport layer can have only one command defined.

Variables

Variable	Description
transport_base	Base distinguished name.
transport_bind_ip	Fudo IP address used to establish connection with the remote host.
transport_ca_certificate	CA certificate of the target system.
transport_domain	Domain used to login to the target system.
transport_encoding	Text encoding used by the target system.
transport_host	An IP address of the remote host that the password changer/verifier connects to.
transport_login	An account on the target system authorized to change passwords.
transport_port	A port number that the password changer/verifier connects to.
transport_secret	Secret used to authorize the account to execute password change.
transport_server_certificate	Certificate of the target server.
account_domain	Domain of the user whose password is being changed.
account_new_secret	System default variable initiated with the value automatically generated by Fudo.

10.3.3 Telnet

Telnet connection mode uses Telnet protocol to establish connection with remote host and continue to communicate with the server in order to change the password.

Commands

Command	Description
INPUT	Command executed on target host.
EXPECTED	Expected result.
ENTER	
DELAY	Delay between commands' execution.

Variables

Variable	Description
transport_bind_ip	Fudo IP address used to establish connection with the remote host.
transport_host	An IP address of the remote host that the password changer/verifier connects to.
transport_login	An account on the target system authorized to change passwords.
transport_port	A port number that the password changer/verifier connects to.
transport_secret	Secret used to authorize the account to execute password change.
account_login	Login of the user whose password is being changed.
account_new_secret	System default variable initiated with the value automatically generated by Fudo.

10.3.4 WinRM

WinRM transport layer uses Windows Remote Management protocol to interface with remote operating system and facilitate password change. WinRM is compatible with Certificate Revocation List (CRL) so that the used digital certificates are always up to date and valid.

Note: The default settings of WinRM Password Changer and Verifier allow changing and verifying passwords of *local* users only. If the *domain* users should be included too, add them to the "Allow log on locally" group so that the executing script takes *domain* users' passwords while running, too.

Commands

Command	Description
INPUT	Command executed on target host.
EXPECTED	Expected result.
ENTER	
DELAY	Delay between commands' execution.

Variables

Variable	Description
transport_bind_ip	Fudo IP address used to establish connection with the remote host.
transport_ca_certificate	CA certificate of the target system.
transport_encoding	Text encoding used by the target system.
transport_host	An IP address of the remote host that the password changer/verifier connects to.
transport_login	An account on the target system used to change passwords.
transport_port	A port number that the password changer/verifier connects to.
transport_secret	Secret used to access the account to execute password change.
account_login	Login of the user whose password is being changed.
account_new_secret	System default variable initiated with the value automatically generated by Fudo.

Related topics:

- *Custom password changers*
- *Password changer policy*
- *Setting up password changing on a Unix system*

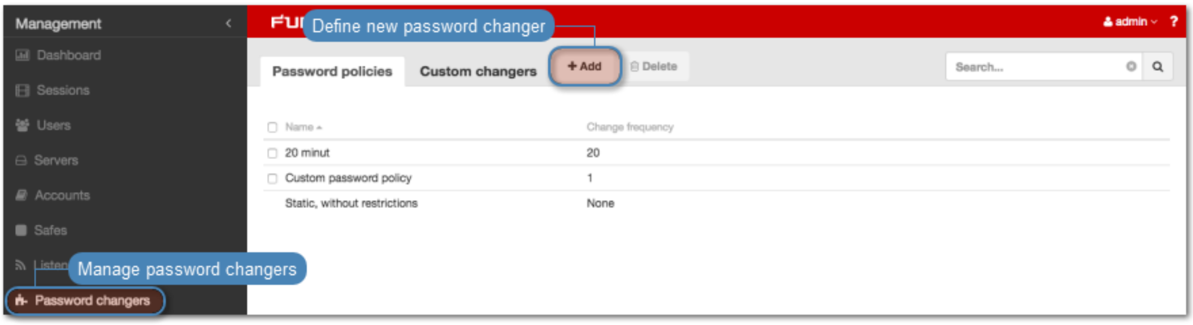
10.4 Setting up password changing on a Unix system

This topic contains an example of setting up password changing on a Unix system.

Adding a password change policy

1. Select *Management > Password changers*.

2. Click *+ Add* to create a new password changing policy.



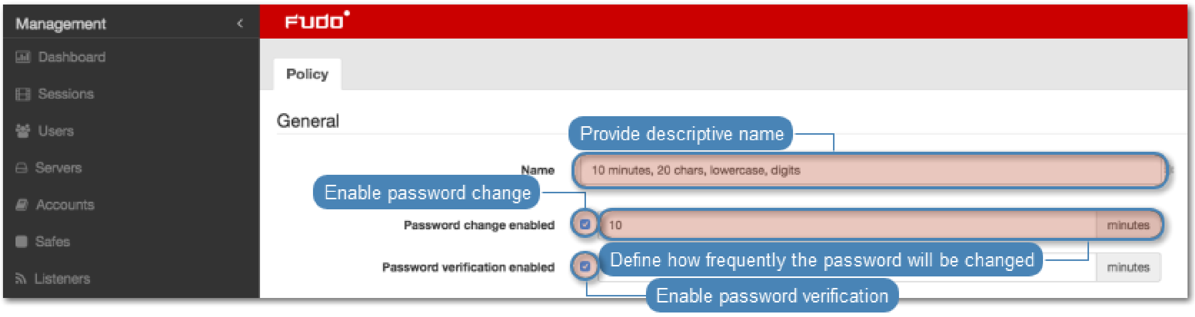
Name	Change frequency
20 minut	20
Custom password policy	1
Static, without restrictions	None

3. Provide password change policy name.

Note: Provide a descriptive name so that anyone administrating 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.



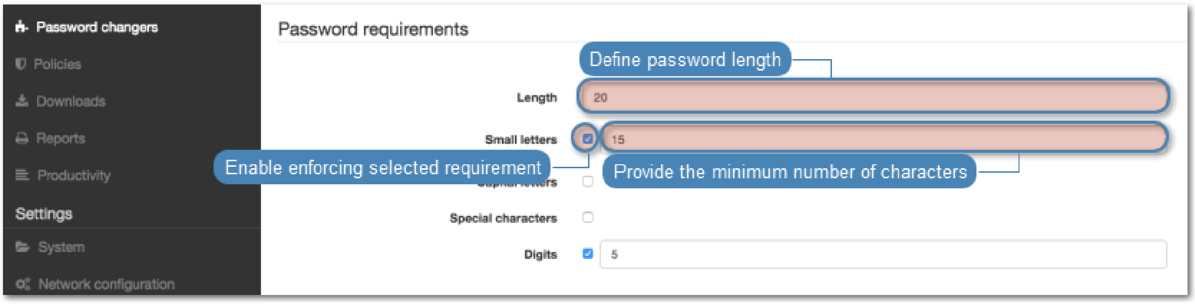
Name: 10 minutes, 20 chars, lowercase, digits

Password change enabled ☑ 10 minutes

Password verification enabled ☑ minutes

6. Provide the number of characters comprising the password.

7. Select desired password complexity options and provide the minimal number of characters for each.



Length: 20

Small letters ☑ 15

Capital letters □

Special characters □

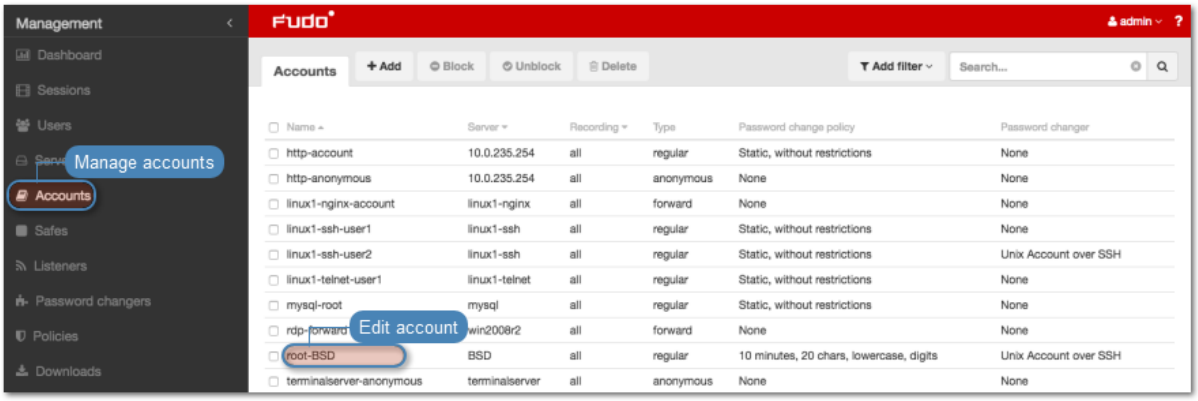
Digits ☑ 5

8. Click *Save* to store password changer policy.

Assigning a password changer and a verifier to the privileged account

1. Select *Management > Accounts*.

2. Find and click desired account object.



Manage accounts

Edit account

Name	Server	Recording	Type	Password change policy	Password changer
http-account	10.0.235.254	all	regular	Static, without restrictions	None
http-anonymous	10.0.235.254	all	anonymous	None	None
linux1-nginx-account	linux1-nginx	all	forward	None	None
linux1-ssh-user1	linux1-ssh	all	regular	Static, without restrictions	None
linux1-ssh-user2	linux1-ssh	all	regular	Static, without restrictions	Unix Account over SSH
linux1-telnet-user1	linux1-telnet	all	regular	Static, without restrictions	None
mysql-root	mysql	all	regular	Static, without restrictions	None
rdp-forward	win2008r2	all	forward	None	None
root-BSD	BSD	all	regular	10 minutes, 20 chars, lowercase, digits	Unix Account over SSH
terminalserver-anonymous	terminalserver	all	anonymous	None	None

3. Click + *Add password changer*.

4. From the *Password verifier* drop-down list, select `Unix/SSH changer`.

5. Define the script execution time limit.

6. Review and modify default values.

Variable	Value
transport_bind_ip	`cont_int: Any`
transport_host	`cont_int: 10.0.0.12`
transport_host_public_key	`cont_int: ssh-rsa AAA[...]`
transport_login	*Enter manually:* `root`
transport_method	*Enter manually:* `password`
transport_password_prompt	`constant`
transport_port	`cont_int: 22`
transport_secret	`cont_int_mr_jenkins: *****`
account_login	`cont_int_mr_jenkins: mr_jenkins`

Note:

- Variables starting with `transport_` are the transport layer variables determining connection parameters with the target host.
- Password changer variables can be assigned values manually or initiated with properties of other objects.

7. Click + *Add password verifier*.

8. From the *Password verifier* drop-down list, select `Unix/SSH changer`.

9. Define the script execution time limit.

10. Review and modify default values.

Variable	Value
transport_bind_ip	`cont_int: Any`
transport_host	`cont_int: 10.0.0.12`
transport_host_public_key	`cont_int: ssh-rsa AAA[...]`
transport_login	`cont_int_mr_jenkins: mr_jenkins`
transport_method	`cont_int_mr_jenkins: password`
transport_password_prompt	`constant`
transport_port	`cont_int: 22`
transport_secret	`cont_int_mr_jenkins: *****`

11. Click *Save*.

Related topics:

- *Connection modes*
- *Custom password changers*

10.5 Plug-ins

Plug-ins enable convenient development and deployment of complex password changers.

10.5.1 Developing plug-ins

Plug-ins enable convenient development and deployment of advanced, custom password changers.

10.5.1.1 Development environment

Creating plug-ins requires development environment based on FreeBSD operating system with Python 3.6 installed. The system version depends on the Fudo PAM revision (10.4 in case of Fudo 3.11).

Development environment folder structure:

```
  /
  |-- bin
  |-- dev
  |-- etc
  |-- lib
  |-- libexec
* |-- plugin
  |-- sbin
* |-- tmp
  `-- usr
          |-- bin
          |-- lib
*         |-- local
          `-- sbin
```

Plugin archive is unpacked in the `/plugin` folder. Python's interpreter is located in the `/usr/local` folder. The `/tmp` folder can be used for storing temporary files. Its size cannot exceed 10 MB and its contents is deleted each time the password changer script is run.

Related topics:

- *Plugin structure*
- *Preparing plug-ins for deployment*
- *Custom password changers*
- *Password changer policy*
- *Setting up password changing on a Unix system*

10.5.1.2 Plugin structure

Plugin is a `zip` archive comprising following files:

- *manifest.json*
- *change script*
- *verify script*
- *password change/verification code*

Warning: The size of compressed archive cannot exceed 10 MB. Uncompressed, total files' size cannot exceed 100 MB.

manifest.json

The manifest declares plugin's essential meta data and variables used by password modifier and verifier.

Parameter	Description
`name`	Unique name allowing to identify the plugin.
`plugin_version`	Plugin's revision. **Note:** We suggest using the *MAJOR.MINOR.PATCH* semantic versioning described at https://semver.org/.
`type`	In case of both - password changer and verifier, this should be set to `password_changer`.
`engine_version`	Fudo PAM provides plugins execution environment in a specific revision. Plugin requires declaration of the compatible engine version.
`timeout`	Maximum script execution time (expressed in seconds). In case the modification/verification script does not finish successfully, the process responsible for its execution will be terminated and the password change/verification attempt will be considered unsuccessful.

The manifest also declares a list of variables used by the modifier and the verifier in the `change` and the `verify` sections respectively. The variables can either refer to existing data model objects or be defined manually. A variable is defined by the following structure:

Parameter	Type	Required	Description
`name`	string	✓	Variable name.
`description`	string	✗	Variable description.
`required`	boolean	✓	Specifies whether the variable is required or not.
`object_type`	string	✗	Type of the object that the variable refers to.
`object_property`	string	✗	Referenced object's property that will be used to initiate variable's value.
`encrypt`	boolean	?	Specifies whether the value should be encrypted or not. Required if `object_type` and `object_property` have not been defined.

Available objects and their properties

Object/property	Description
server	*Server* object defined in the local database.
name	Object's name.
bind_ip	IP address used by Fudo PAM to communicate with the server.
ca_certificate	CA certificate.
port	Port number the target host uses to listen for connection requests.
protocol	Target host communication protocol: citrixsf, http, ica, modbus, mysql, oracle, rdp, ssh, system, tcp, tds, telnet, tn3270, tn5250, vnc.
secproto	Security protocol used by an RDP server: nla, tls, std.
ssl_to_server	1 if the server uses SSL/TLS, 0 if the server does not use SSL/TLS.
ssl_v2	1 if the SSL version 2.0 is allowed by the target host; 0 if the target host does not allow SSL 2.0 communication.
ssl_v3	1 if the SSL version 3.0 is allowed by the target host; 0 if the target host does not allow SSL 3.0 communication.
subnet	Dynamic server network subnet specifier, e.g. 192.168.0.0/24
server_address	Server IP address. In case of dynamic servers, a single object can have many IP addresses assigned.
host	Server address.
certificate	Certificate for specific IP address.
public_key	Public SSH key for specific IP address.

Object/property	Description
account	*Account* object defined in the local database.
name	Object's name.
description	Object's description.
login	Privileged account login.
method	Authentication method - can be either password or ssh key
secret	Secret used in authentication process.

Example:

```
{
  "name": "Redmine",
  "plugin_version": "1.0.3",
  "type": "password changer",
  "engine_version": "1.0.0",
  "timeout": "300",
  "change":
  {
        "variables":
        [
          {
                "name": "transport_login",
                "description": "User name used to login to account.",
                "required": true,
                "object_type": "account",
                "object_property": "login"
          },
          {
                "name": "transport_secret",
                "description": "A secret to be used when logging in.",
                "required": true,
                "object_type": "account",
                "object_property": "secret"
          },
          {
                "name": "transport_host",
                "description": "Host name or IP address. IPv4 and IPv6 are both␣
↪supported.",
                "required": true,
                "object_type": "server_address",
                "object_property": "host"
          },
          {
                "name": "account_login",
                "description": "User name for which to change password.",
                "required": true,
```

(continues on next page)

(continued from previous page)

```
                "object_type": "account",
                "object_property": "login"
          }
        ]
  },
  "verify":
  {
        "variables":
        [
          {
                "name": "transport_login",
                "description": "User name used to login to account. This user's password will be verified.",
                "required": true,
                "object_type": "account",
                "object_property": "login"
          },
          {
                "name": "transport_secret",
                "description": "A secret that will be verified.",
                "required": true,
                "object_type": "account",
                "object_property": "secret"
          },
          {
                "name": "transport_host",
                "description": "Host name or IP address. IPv4 and IPv6 are both supported.",
                "required": true,
                "object_type": "server_address",
                "object_property": "host"
          }
        ]
  }
}
```

change script

Script used to execute the actual password changing code.

Example:

```
#!/bin/sh
CURR_DIR="$(realpath $(dirname "${0}"))"

echo "Script located in '${CURR_DIR}' directory."

export PYTHONPATH="${CURR_DIR}/site-packages"
python3 "${CURR_DIR}/redmine_changer.py" change
```

verify script

Script used to execute the actual password verifying code.

Example:

```
#!/bin/sh
CURR_DIR="$(realpath $(dirname "${0}"))"

echo "Script located in '${CURR_DIR}' directory."

export PYTHONPATH="${CURR_DIR}/site-packages"
python3 "${CURR_DIR}/redmine_changer.py" verify
```

Password changing code

Note: All variables declared in the `manifest.json` file are available through environment variables. Apart from those, there is a special `account_new_secret` variable available only in the password changing script. This value is initiated automatically by Fudo PAM.

Exemplary application:

```
import os

print('New secret: {}'.format(os.environ['account_new_secret']))
```

Example of Python code used to change passwords to Redmine using REST API:

```
import os
import sys

import requests


MODE_CHANGE = 1
MODE_VERIFY = 2


def eprint(*args, **kwargs):
        print(*args, file=sys.stderr, **kwargs)


class RedmineChangerError(Exception):
        pass


def redmine_get_user_id(server_uri, admin_login, admin_password, user_login):
        req = requests.get(
                server_uri + '/users.json',
                params={'name': user_login},
                auth=(admin_login, admin_password),
                verify=False,
        )
        if req.status_code != 200:
                raise RedmineChangerError(
                        'HTTP status code {} from {}.'.format(req.status_code,␣
↪server_uri)
```

(continues on next page)

(continued from previous page)

```
                )

        user_list = [x for x in req.json()['users'] if x['login'] == user_login]
        if len(user_list) > 1:
                raise RedmineChangerError(
                        'Ambigious answer from {}: Multiple users with "{}" login'.
↪format(
                                server_uri, user_login
                        )
                )
        if len(user_list) < 1:
                raise RedmineChangerError(
                        'Response from {} doesn\'t contain user with login "{}"'.
↪format(
                                server_uri, user_login
                        )
                )

        try:
                user_id = user_list[0]['id']
        except KeyError:
                raise RedmineChangerError(
                        'Response from {} doesn\'t contain "id".'.format(server_uri)
                )
        return user_id


def redmine_set_user_password(
        server_uri, admin_login, admin_password, user_id, user_password
):
        uri = '{}/users/{}.json'.format(server_uri, user_id)
        req = requests.put(
                uri,
                json={'user': {'password': user_password}},
                auth=(admin_login, admin_password),
                verify=False,
        )
        if req.status_code != 200:
                raise RedmineChangerError(
                        'HTTP status code {} from {}.'.format(req.status_code,␣
↪server_uri)
                )


# https://redmine.hostonly.vm/users/current.json
def redmine_get_current_user_login(server_uri, admin_login, admin_password):
        req = requests.get(
                server_uri + '/users/current.json',
                auth=(admin_login, admin_password),
                verify=False,
        )
        if req.status_code != 200:
                raise RedmineChangerError(
                        'HTTP status code {} from {}.'.format(req.status_code,␣
↪server_uri)
                )
```

(continues on next page)

(continued from previous page)

```
        try:
                login = req.json()['user']['login']
        except KeyError:
                raise RedmineChangerError('Unable to get "user.login".')

        return login


def change(
        transport_login,
        transport_secret,
        transport_uri,
        account_login,
        account_new_secret,
):
        try:
                user_id = redmine_get_user_id(
                        transport_uri, transport_login, transport_secret, account_
↪login
                )
        except RedmineChangerError as err:
                print('Error getting user id: {}'.format(err), file=sys.stderr)
                return 1

        print('User "{}" has id {}.'.format(account_login, user_id))

        try:
                redmine_set_user_password(
                        transport_uri,
                        transport_login,
                        transport_secret,
                        user_id,
                        account_new_secret,
                )
        except RedmineChangerError as err:
                print('Error setting user password: {}'.format(err), file=sys.stderr)
                return 1

        print('Successfully changed password for user "{}".'.format(account_login))
        return 0


def verify(transport_login, transport_secret, transport_uri):
        try:
                login = redmine_get_current_user_login(
                        transport_uri, transport_login, transport_secret
                )
        except RedmineChangerError as err:
                print(
                        'Error getting current user login: {}'.format(err), file=sys.
↪stderr
                )
                return 1

        if login != transport_login:
```

(continues on next page)

(continued from previous page)

```
                print(
                        'Server {} returned wrong login "{}" - expected "{}".'.
↪format(
                                transport_uri, login, transport_login
                        ),
                        file=sys.stderr,
                )
                return 1

        print('Successfully logged in as "{}".'.format(transport_login))
        return 0


# TODO: There are some improvements that we can implement in future versions of
# plugin to test update procedure:
# - respect TLS: at the moment we assume TLS is on and connect using HTTPS,
# - verify server certificate,
# - optionally, get port of the server.
def main():
        if len(sys.argv) != 2:
                print('Provide "change" or "verify" as plugin mode', file=sys.stderr)
                sys.exit(1)

        if sys.argv[1] == 'change':
                mode = MODE_CHANGE
        elif sys.argv[1] == 'verify':
                mode = MODE_VERIFY
        else:
                print('Incorrect plugin mode: "{}".'.format(sys.argv[1]))
                sys.exit(1)

        transport_login = os.environ['transport_login']
        transport_secret = os.environ['transport_secret']
        transport_uri = 'https://' + os.environ['transport_host']
        if mode == MODE_CHANGE:
                account_login = os.environ['account_login']
                account_new_secret = os.environ['account_new_secret']

        result = 1
        if mode == MODE_CHANGE:
                result = change(
                        transport_login,
                        transport_secret,
                        transport_uri,
                        account_login,
                        account_new_secret,
                )
        else:
                result = verify(transport_login, transport_secret, transport_uri)

        sys.exit(result)


if __name__ == '__main__':
        main()
```

Note: Successfully executed code should exit with status 0. Any other value will be interpreted as a failure.

Related topics:

- *Development environment*
- *Preparing plug-ins for deployment*
- *Custom password changers*
- *Password changer policy*
- *Setting up password changing on a Unix system*

10.5.1.3 Preparing plug-ins for deployment

Preparing a plug-in for deployment requires copying contents of the workspace catalog and installing `requests` in the `site-packages` folder.

```
mkdir /tmp/workdir-redmine
cp -a core/usr.local.share/plugins/ex02-redmine/* /tmp/workdir-redmine
cd /tmp/workdir-redmine
pip3 install -t site-packages requests
zip /tmp/ex02-redmine.zip -9r *
```

Related topics:

- *Development environment*
- *Plugin structure*
- *Custom password changers*
- *Password changer policy*
- *Setting up password changing on a Unix system*

Related topics:

- *Custom password changers*
- *Password changer policy*
- *Setting up password changing on a Unix system*

10.5.2 Uploading plug-ins

1. Select *Management > Password changers*.
2. Select *Custom changers* tab.
3. Click *Upload*.
4. Browse the filesystem and find the plugin file.
5. *Define password change policy* and *assign the password changer to account*.

Related topics:

- *Custom password changers*
- *Data model*
- *Accounts*
- *Password changer policy*
- *Setting up password changing on a Unix system*

Related topics:

- *Custom password changers*
- *Data model*
- *Accounts*
- *Password changer policy*
- *Setting up password changing on a Unix system*

CHAPTER 11

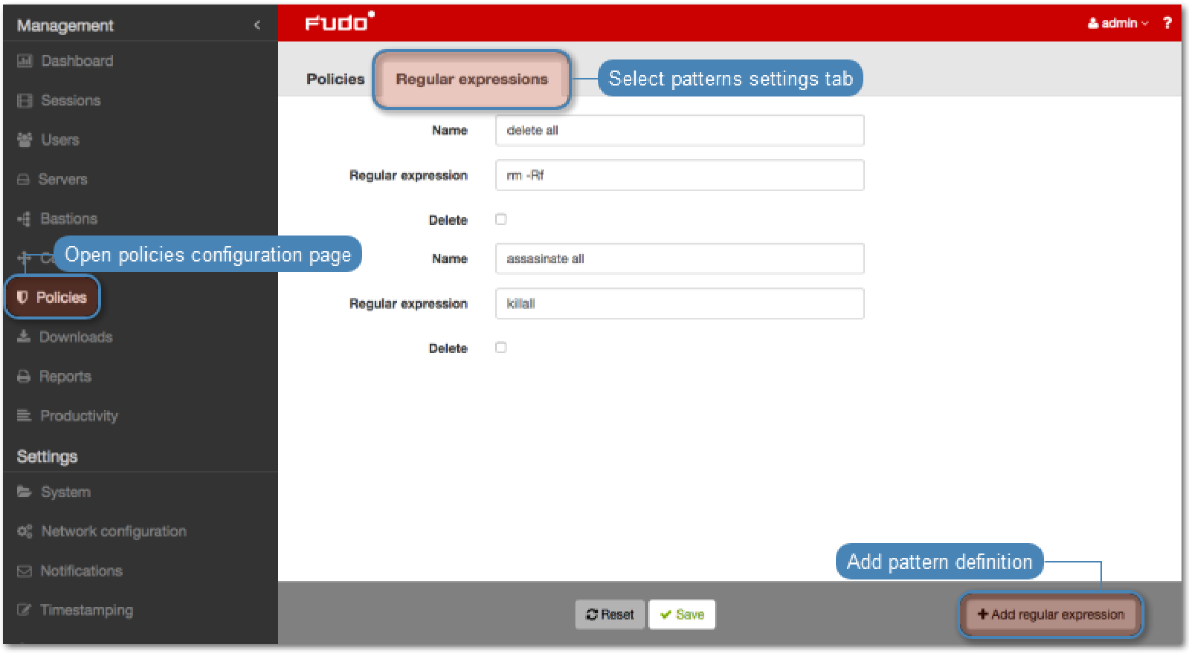
Policies

Policies are patterns definitions facilitating proactive session monitoring. In case a defined pattern is detected, Fudo PAM can automatically pause or terminate given connection, block the user and send notification to Fudo PAM administrator.

Defining patterns

Note: Fudo PAM supports POSIX extended regular expression.

1. Select *Management* > *Policies*.
2. Select *Regular expressions* tab.
3. Click + *Add regular expression*.



Name: delete all

Regular expression: rm -Rf

Delete □

Name: assasinate all

Regular expression: killall

Delete □

Select patterns settings tab

Open policies configuration page

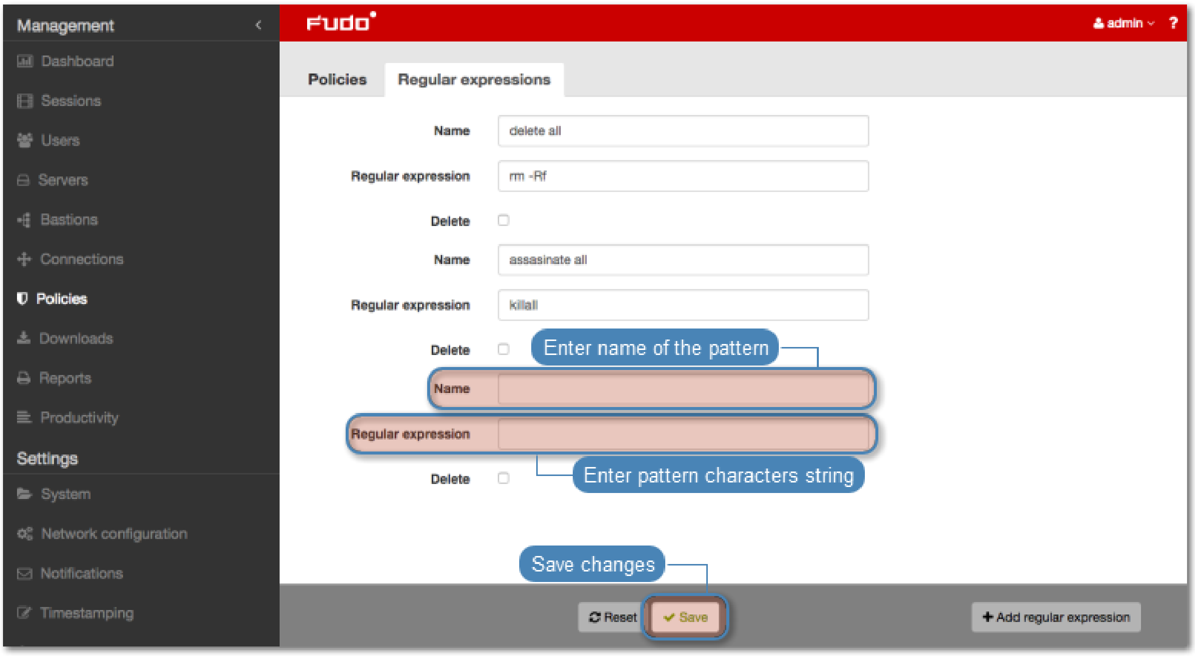
Add pattern definition

4. Enter pattern name.
5. Define the pattern itself.

Note:

- Patterns can be defined as regular expressions.
- 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.



Name: delete all

Regular expression: rm -Rf

Delete □

Name: assasinate all

Regular expression: killall

Delete □

Enter name of the pattern

Name

Regular expression

Delete □

Enter pattern characters string

Save changes

Note: Regular expressions examples

Command `rm`

`(^|[^a-zA-Z])rm[[:space:]]`

Command `rm -rf` (*also* `-fr`; `-Rf`; `-fR`)

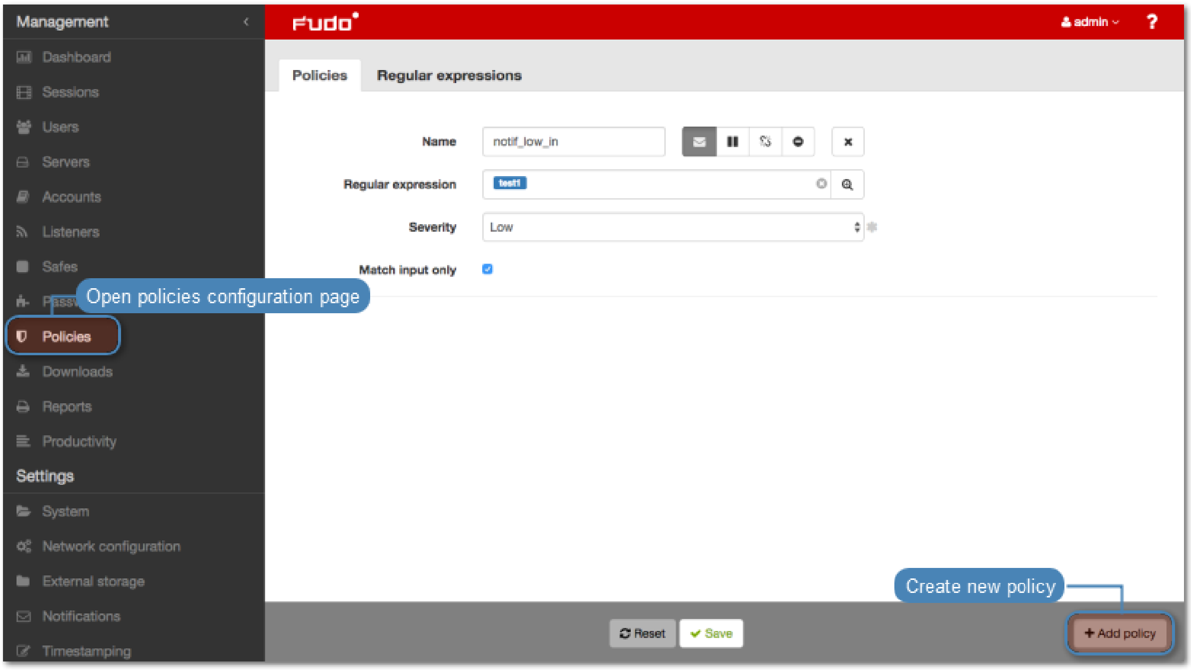
`(^|[^a-zA-Z])rm[[:space:]]+-([rR]f|f[rR])`

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*.



Name: notif_low_in

Regular expression: test1

Severity: Low

Match input only: ☑

Open policies configuration page

Create new policy

3. Enter policy name.
4. Select actions.

✉	Send email notification to system administrator.
⏸	Pause connection.
⛓	Terminate connection.
⛔	Block user.

Note:

- Sending email notifications requires configuring and enabling *notification service* as well as *Session policy match* notification enabled in *safe configuration*.
- Note that blocking the user automatically terminates the connection.

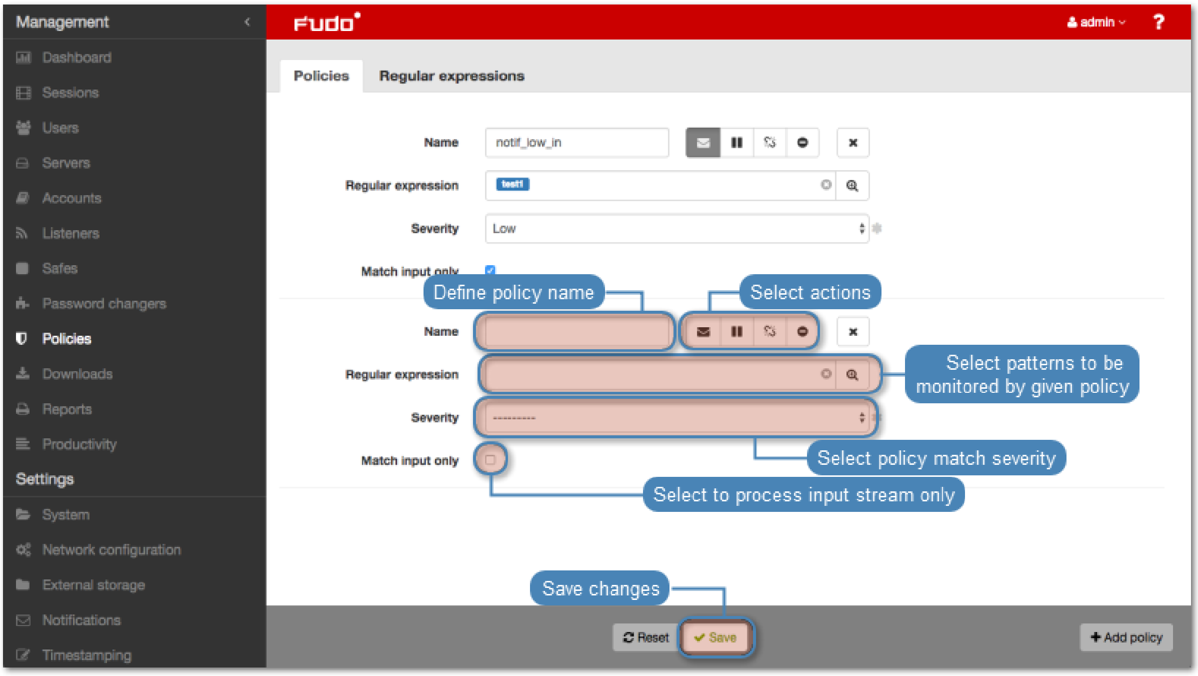
5. Select monitored patterns.
6. Select policy severity.

Note: Severity parameter value is included in the email notification message.

7. Select the *Match input only* option to process input stream only.

Note: In RDP, VNC and MySQL protocols only input data is processed.

8. Click *Save*.



Name: notif_low_in

Regular expression: test1

Severity: Low

Match input only: ☑

Name:

Regular expression:

Severity: ---------

Match input only: □

Define policy name

Select actions

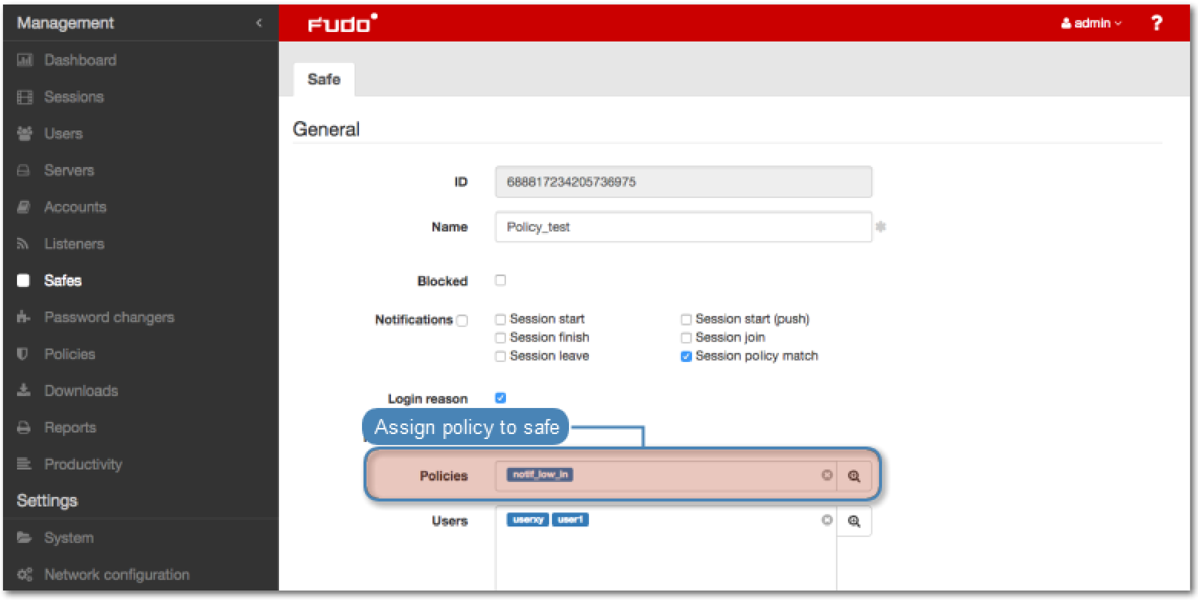
Select patterns to be monitored by given policy

Select policy match severity

Select to process input stream only

Save changes

Note: After defining a policy, you can assign it to a *safe* that is used to establish connections to servers.



General

ID: 688817234205736975

Name: Policy_test

Blocked: □

Notifications □: □ Session start, □ Session finish, □ Session leave, □ Session start (push), □ Session join, ☑ Session policy match

Login reason: ☑

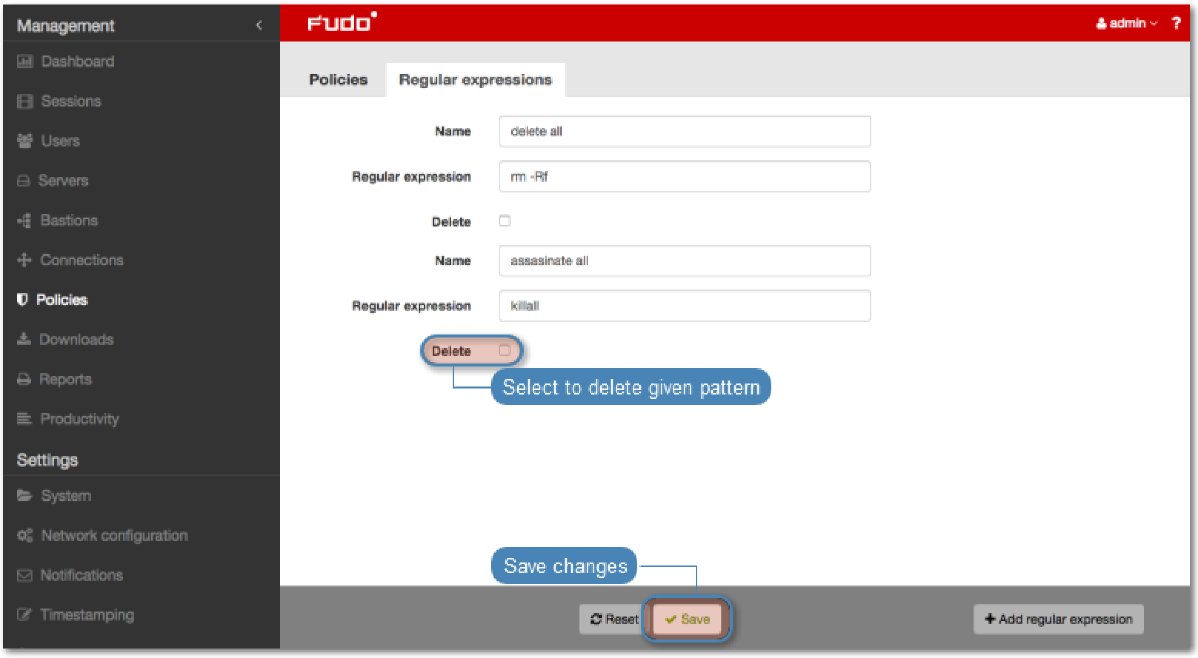
Assign policy to safe

Policies: notif_low_in

Users: userxy user1

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*.



Name: delete all
Regular expression: rm -Rf
Delete ☐
Name: assasinate all
Regular expression: killall
Delete ☐

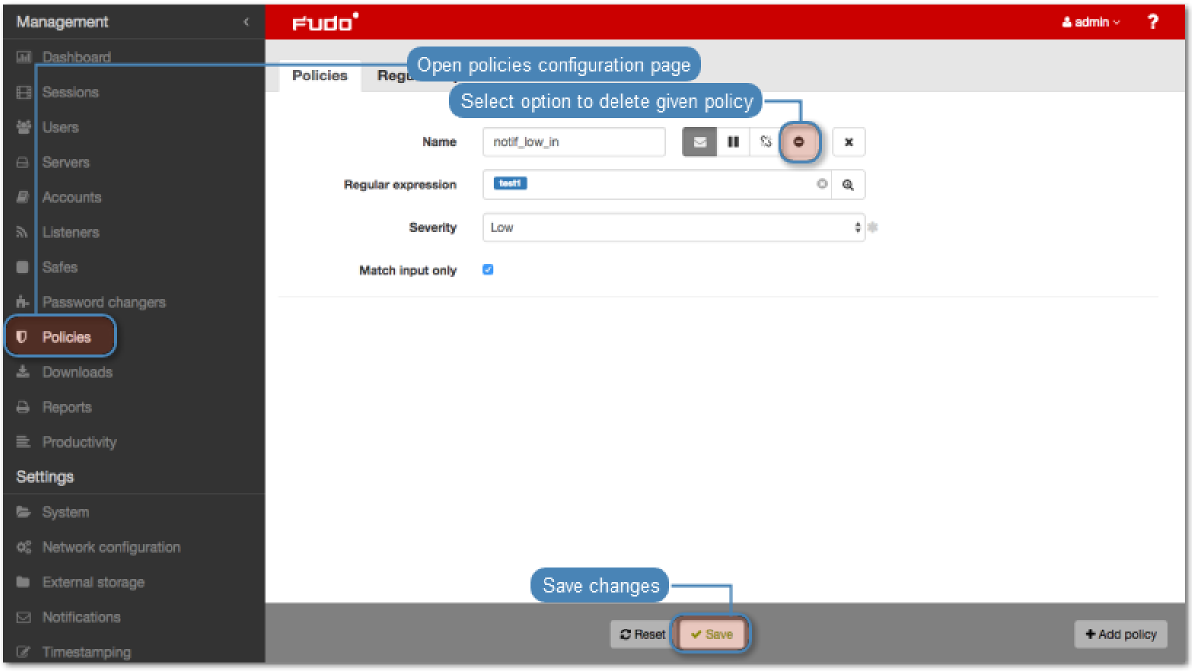
Select to delete given pattern

Save changes

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*.



Open policies configuration page

Select option to delete given policy

Name: notif_low_in
Regular expression: test1
Severity: Low
Match input only ☑

Save changes

Related topics:

- *Safes*
- *Terminating connection*
- *Notifications*

- *Security*

CHAPTER 12

Sessions

Fudo PAM stores all recorded servers access sessions, allowing to playback, review, delete and export to the supported video formats.

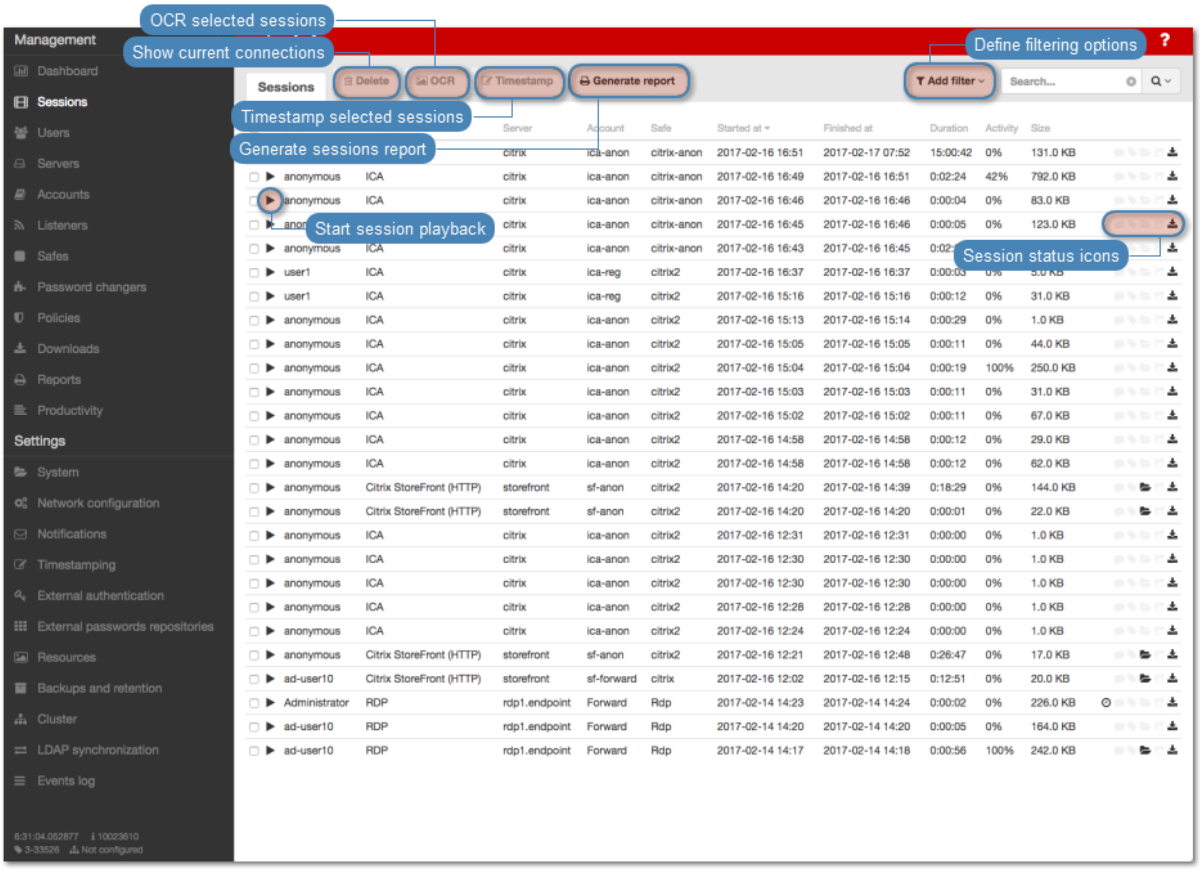
Sessions management page allows filtering stored user sessions, accessing current users connections and downloading stored sessions. It also provides status information on each session and enables access to session sharing options.

Note: Contents of the session list depend on the logged in user's access rights. Being able to access a given session requires having management privileges to: server, account, user and safe objects that were used in the given connection.

Icon	Description
▶	Start session playback (*applicable to sessions with the entire traffic recording option selected in connection properties*).
🕘	Icon indicating that session has been timestamped.
💬	Purpose why the user has connected to the server.
🏷	Session has been commented.
📂	Session has been processed for full-text search purposes.
⇄	Session replication status.
↗	Access session sharing management options.
⬇	Download session material in selected file format (*applicable to sessions with either complete or raw traffic recording option selected in connection properties*).
📶	User activity monitor (*applicable to live sessions*).
👤	Username of the user for whom approved pending session.
✔	Approve pending request.
✖	Decline pending request.
?	Pending request awaiting authorization.
+	Element aggregating connections established within the same session.
🔒	Session excluded from the retention mechanism.
⚗	Behavioral analysis status. *This is an evaluation version of the AI component.* ○ - session under analysis, initial result - no threat. ○ - session under analysis, initial result - medium threat level. ○ - session under analysis, initial result - high threat level. ○ - session awaiting analysis or being initially processed. ○ - session not analyzed due to missing a trained model. 🟢 - session processed - no risk. 🟡 - session processed - medium threat level. 🔴 - session processed - high threat level. ● - session processed - no result.

To open sessions management page, select *Management* > *Sessions*.

Note: Fudo PAM stores compressed session material which may result in differences between the displayed and the actual session size.



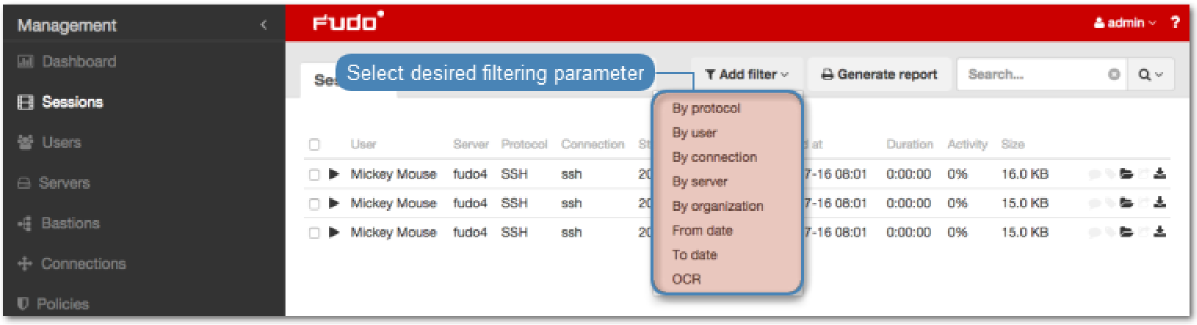
		Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
		citrix	ica-anon	citrix-anon	2017-02-16 16:51	2017-02-17 07:52	15:00:42	0%	131.0 KB
anonymous	ICA	citrix	ica-anon	citrix-anon	2017-02-16 16:49	2017-02-16 16:51	0:02:24	42%	792.0 KB
anonymous	ICA	citrix	ica-anon	citrix-anon	2017-02-16 16:46	2017-02-16 16:46	0:00:04	0%	83.0 KB
anon		citrix	ica-anon	citrix-anon	2017-02-16 16:45	2017-02-16 16:46	0:00:05	0%	123.0 KB
anonymous	ICA	citrix	ica-anon	citrix-anon	2017-02-16 16:43	2017-02-16 16:45	0:02		
user1	ICA	citrix	ica-reg	citrix2	2017-02-16 16:37	2017-02-16 16:37	0:00:03	0%	5.0 KB
user1	ICA	citrix	ica-reg	citrix2	2017-02-16 15:16	2017-02-16 15:16	0:00:12	0%	31.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:13	2017-02-16 15:14	0:00:29	0%	1.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:05	2017-02-16 15:05	0:00:11	0%	44.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:04	2017-02-16 15:04	0:00:19	100%	250.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:03	2017-02-16 15:03	0:00:11	0%	31.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:02	2017-02-16 15:02	0:00:11	0%	67.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 14:58	2017-02-16 14:58	0:00:12	0%	29.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 14:58	2017-02-16 14:58	0:00:12	0%	62.0 KB
anonymous	Citrix StoreFront (HTTP)	storefront	sf-anon	citrix2	2017-02-16 14:20	2017-02-16 14:39	0:18:29	0%	144.0 KB
anonymous	Citrix StoreFront (HTTP)	storefront	sf-anon	citrix2	2017-02-16 14:20	2017-02-16 14:20	0:00:01	0%	22.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:31	2017-02-16 12:31	0:00:00	0%	1.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:30	2017-02-16 12:30	0:00:00	0%	1.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:30	2017-02-16 12:30	0:00:00	0%	1.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:28	2017-02-16 12:28	0:00:00	0%	1.0 KB
anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:24	2017-02-16 12:24	0:00:00	0%	1.0 KB
anonymous	Citrix StoreFront (HTTP)	storefront	sf-anon	citrix2	2017-02-16 12:21	2017-02-16 12:48	0:26:47	0%	17.0 KB
ad-user10	Citrix StoreFront (HTTP)	storefront	sf-forward	citrix	2017-02-16 12:02	2017-02-16 12:15	0:12:51	0%	20.0 KB
Administrator	RDP	rdp1.endpoint	Forward	Rdp	2017-02-14 14:23	2017-02-14 14:24	0:00:02	0%	226.0 KB
ad-user10	RDP	rdp1.endpoint	Forward	Rdp	2017-02-14 14:20	2017-02-14 14:20	0:00:05	0%	164.0 KB
ad-user10	RDP	rdp1.endpoint	Forward	Rdp	2017-02-14 14:17	2017-02-14 14:18	0:00:56	100%	242.0 KB

12.1 Filtering sessions

Sessions filtering allows to find desired sessions easily by limiting the number of displayed sessions on the sessions management page.

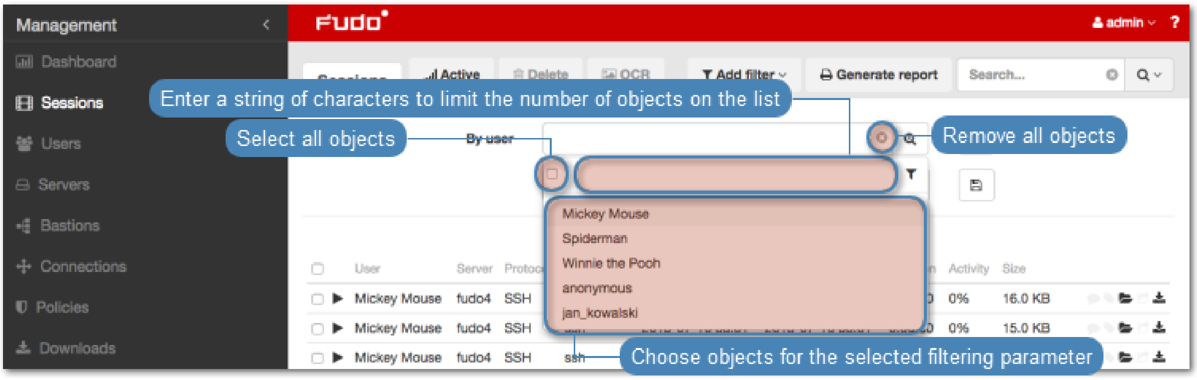
12.1.1 Defining filters

1. Click *Add Filters* and select desired data type from the drop-down list.



User	Server	Protocol	Connection	St	at	Duration	Activity	Size
Mickey Mouse	fudo4	SSH	ssh	20	7-16 08:01	0:00:00	0%	16.0 KB
Mickey Mouse	fudo4	SSH	ssh	20	7-16 08:01	0:00:00	0%	15.0 KB
Mickey Mouse	fudo4	SSH	ssh	20	7-16 08:01	0:00:00	0%	15.0 KB

2. Select desired values for the given filtering type parameter.



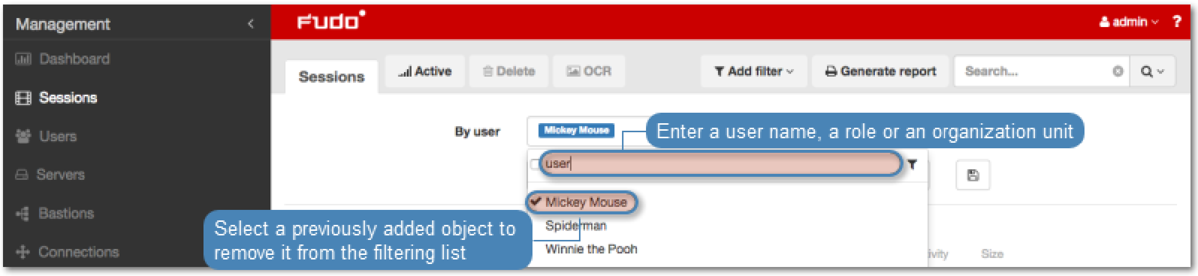
Enter a string of characters to limit the number of objects on the list

Select all objects

Remove all objects

Choose objects for the selected filtering 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.

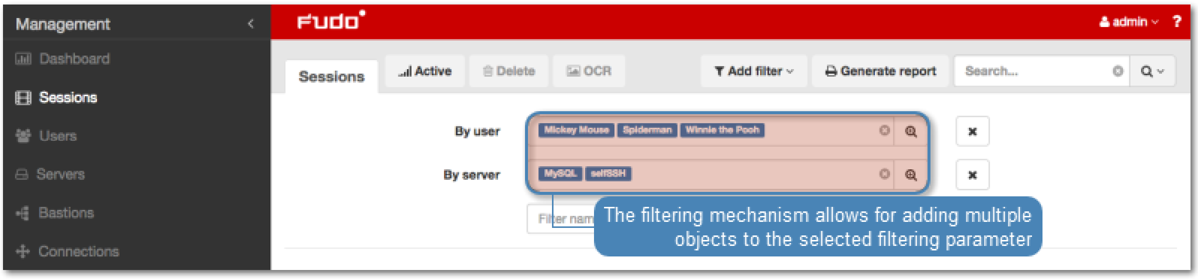


Enter a user name, a role or an organization unit

Select a previously added object to remove it from the filtering list

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.

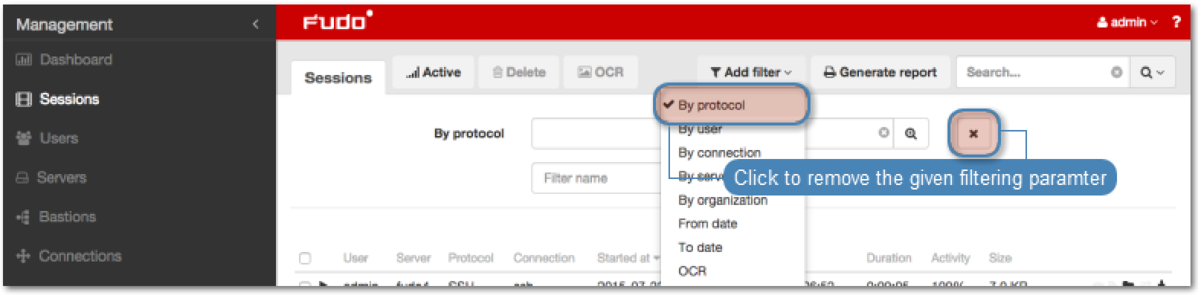


The filtering mechanism allows for adding multiple objects to the selected filtering parameter

3. Repeat steps 2 and 3 to define additional filters.

Note: Only sessions which match all defined filtering parameters will be displayed.

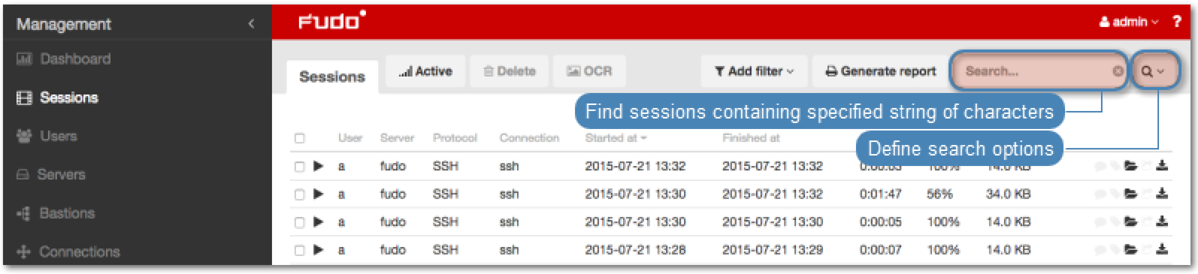
4. Click *Add Filter* and select previously added filtering parameter to disable given filter.



Click to remove the given filtering paramter

12.1.2 Full text search

Fudo PAM enables searching stored data to limit the number of elements on the sessions list only to those containing the specified phrase.



Find sessions containing specified string of characters

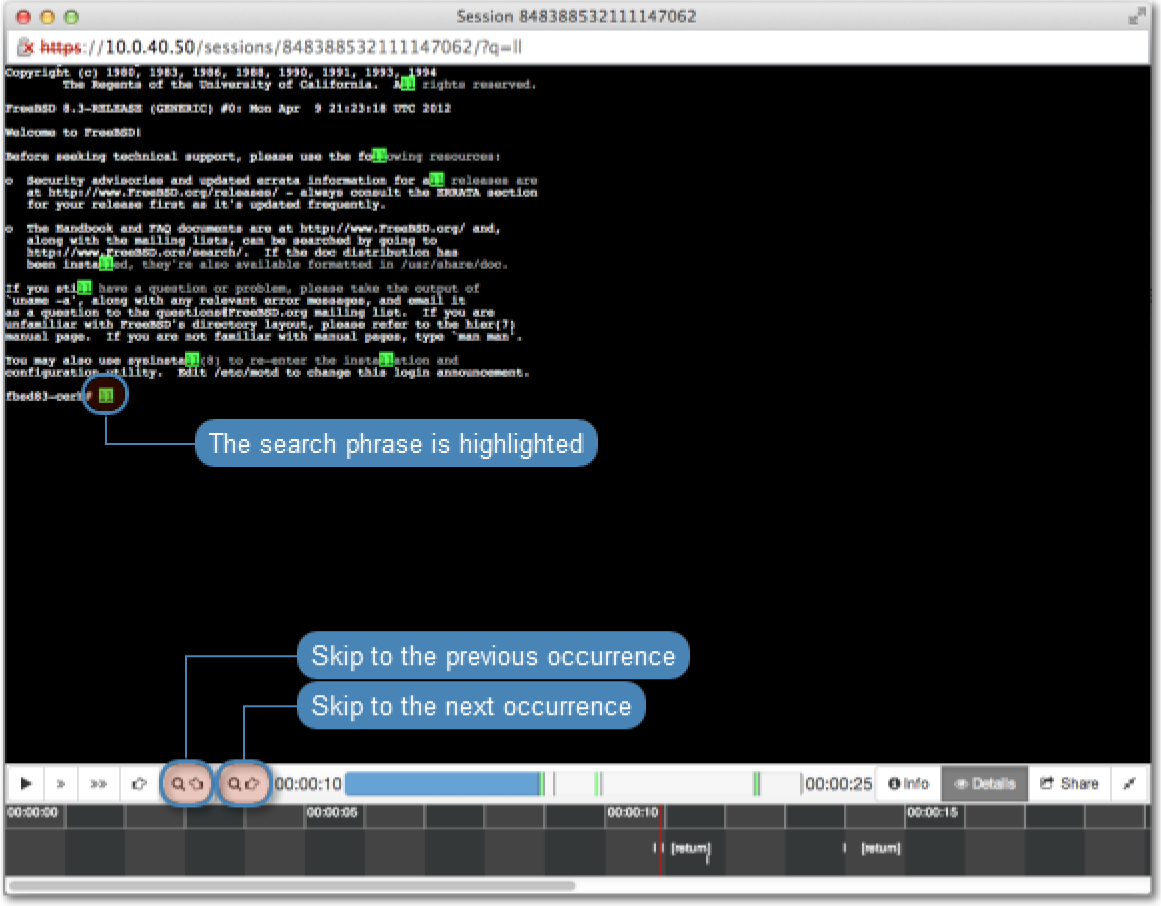
Define search options

User	Server	Protocol	Connection	Started at	Finished at			
a	fudo	SSH	ssh	2015-07-21 13:32	2015-07-21 13:32	[illegible]	100%	14.0 KB
a	fudo	SSH	ssh	2015-07-21 13:30	2015-07-21 13:32	0:01:47	56%	34.0 KB
a	fudo	SSH	ssh	2015-07-21 13:30	2015-07-21 13:30	0:00:05	100%	14.0 KB
a	fudo	SSH	ssh	2015-07-21 13:28	2015-07-21 13:29	0:00:07	100%	14.0 KB

Note:

- Use quotation marks to search for sessions containing all phrases, e.g. “fudo pam”.
- 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.



Session 848388532111147062
https://10.0.40.50/sessions/848388532111147062/?q=ll

```
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.  All rights reserved.

FreeBSD 8.3-RELEASE (GENERIC) #0: Mon Apr  9 21:23:18 UTC 2012

Welcome to FreeBSD!

Before seeking technical support, please use the following resources:

o  Security advisories and updated errata information for all releases are
   at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
   for your release first as it's updated frequently.

o  The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
   along with the mailing lists, can be searched by going to
   http://www.FreeBSD.org/search/.  If the doc distribution has
   been installed, they're also available formatted in /usr/share/doc.

If you still have a question or problem, please take the output of
`uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list.  If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page.  If you are not familiar with manual pages, type `man man'.

You may also use sysinstall(8) to re-enter the installation and
configuration utility.  Edit /etc/motd to change this login announcement.

fbsd83-cert# ll
```

The search phrase is highlighted

Skip to the previous occurrence

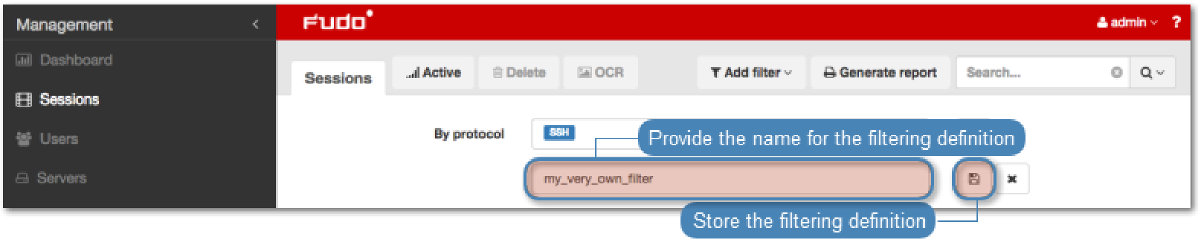
Skip to the next occurrence

12.1.3 Managing user defined filter definitions

Current filtering settings can be stored as a user defined filtering preset for the convinience of the system's operator.

Storing a user defined filter definition

1. Define filtering options as described in the *Filtering sessions* section.
2. Provide the name for the filter definition.
3. Click the save icon to store the filter definition.



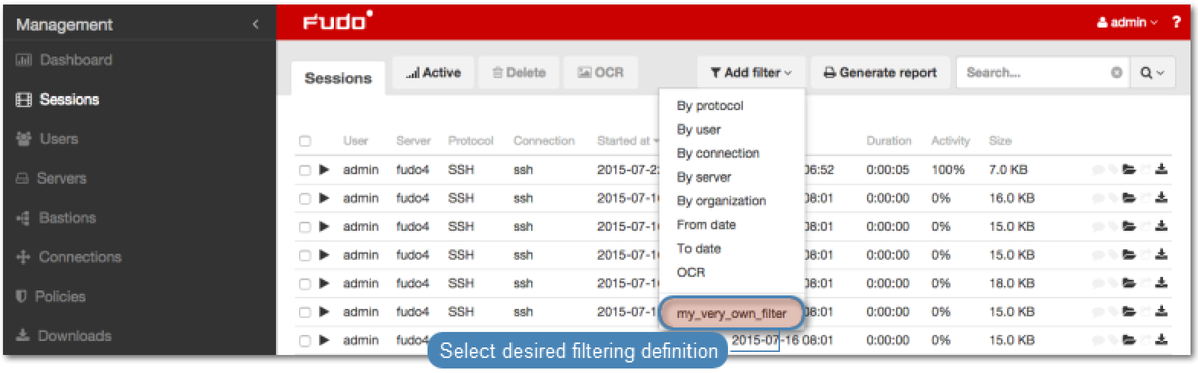
my_very_own_filter

Provide the name for the filtering definition

Store the filtering definition

Editing a user defined filter definition

1. Click *Add filter* and select the desired filter definition.

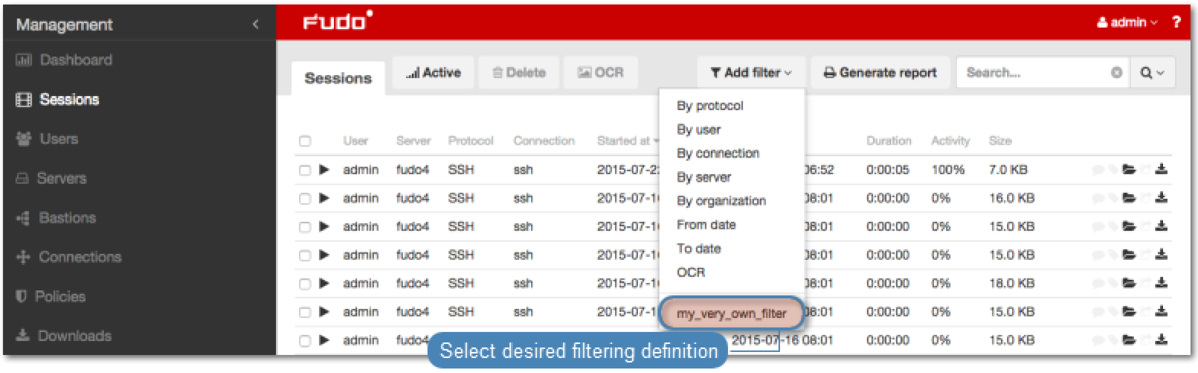


Select desired filtering definition

2. Change the filtering parameters as desired.
3. Click the save icon to store changes in the filter definition.

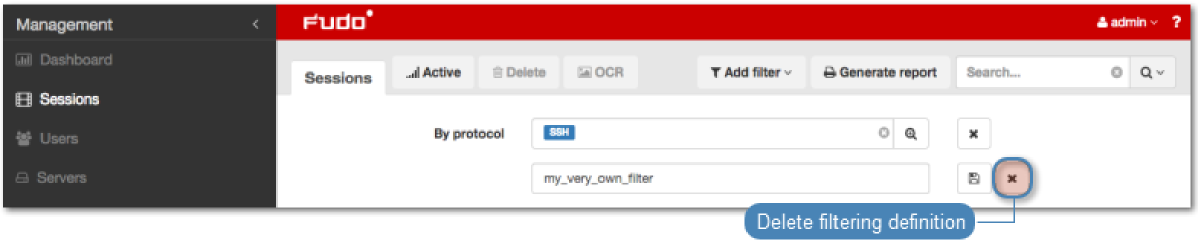
Deleting a user defined filter definition

1. Click *Add filter* and select the desired filter definition.



Select desired filtering definition

2. Click the delete icon to remove the filtering definition.



Delete filtering definition

3. Confirm deleting the selected filtering definition.

Related topics:

- *System overview*
- *Reports*

12.2 Viewing sessions

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.

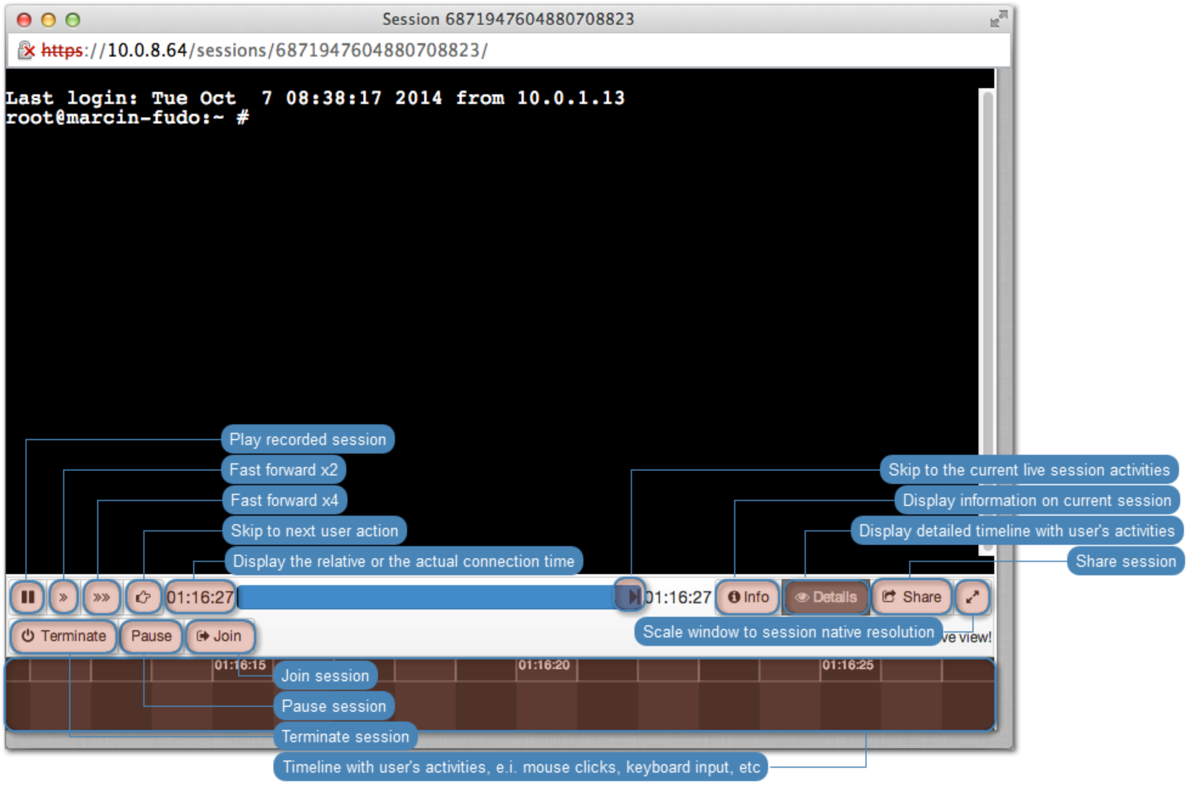
Note: Filter sessions to display only active connections:

- Click *Add filter* and select *Active*.
- Select *Yes* from the drop-down list.

Session player options

Note: Some options are available for live sessions only.

SSH, RDP, VNC, X11, Telnet

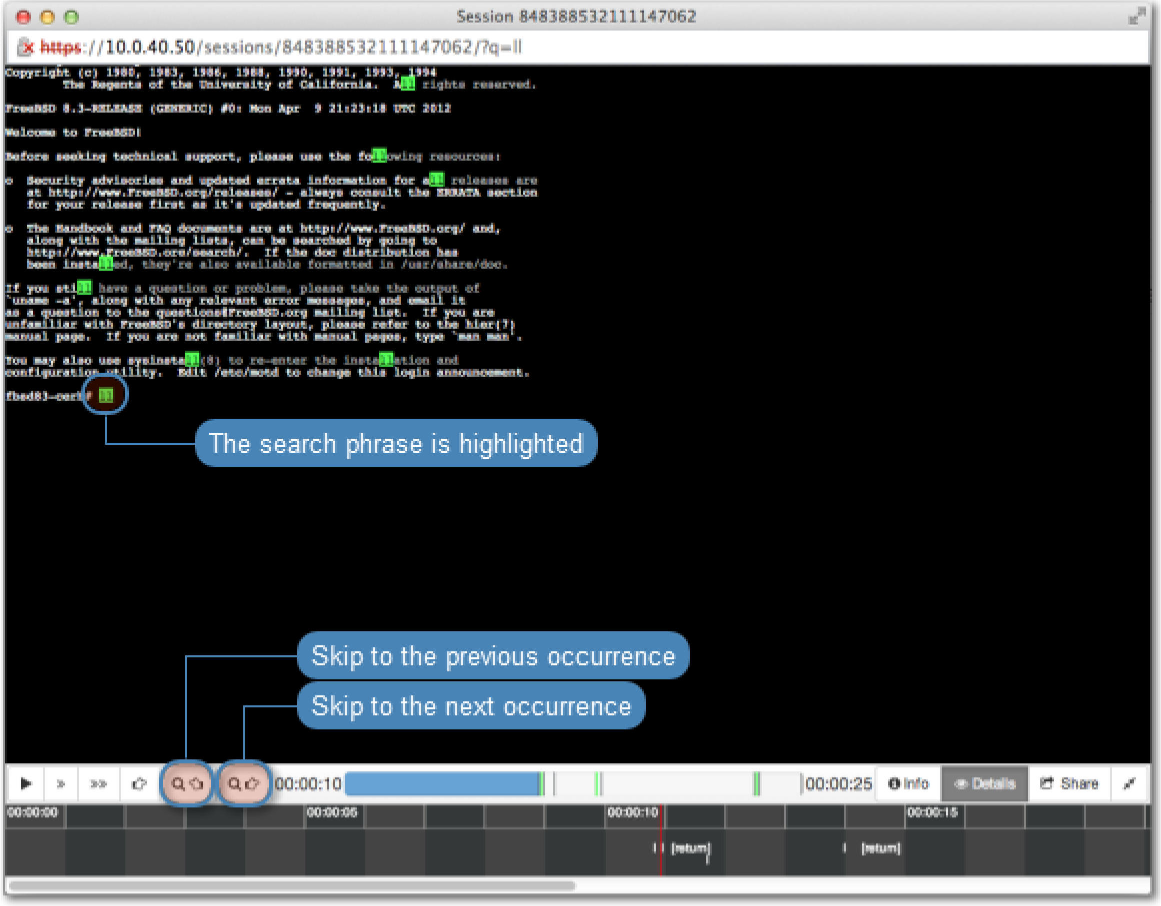


```
Last login: Tue Oct  7 08:38:17 2014 from 10.0.1.13
root@marcin-fudo:~ #
```

Session 6871947604880708823
https://10.0.8.64/sessions/6871947604880708823/
Play recorded session
Fast forward x2
Fast forward x4
Skip to next user action
Display the relative or the actual connection time
Skip to the current live session activities
Display information on current session
Display detailed timeline with user's activities
Share session
01:16:27
01:16:27
Info
Details
Share
Terminate
Pause
Join
Scale window to session native resolution
ve view!
01:16:15
01:16:20
01:16:25
Join session
Pause session
Terminate session
Timeline with user's activities, e.i. mouse clicks, keyboard input, etc

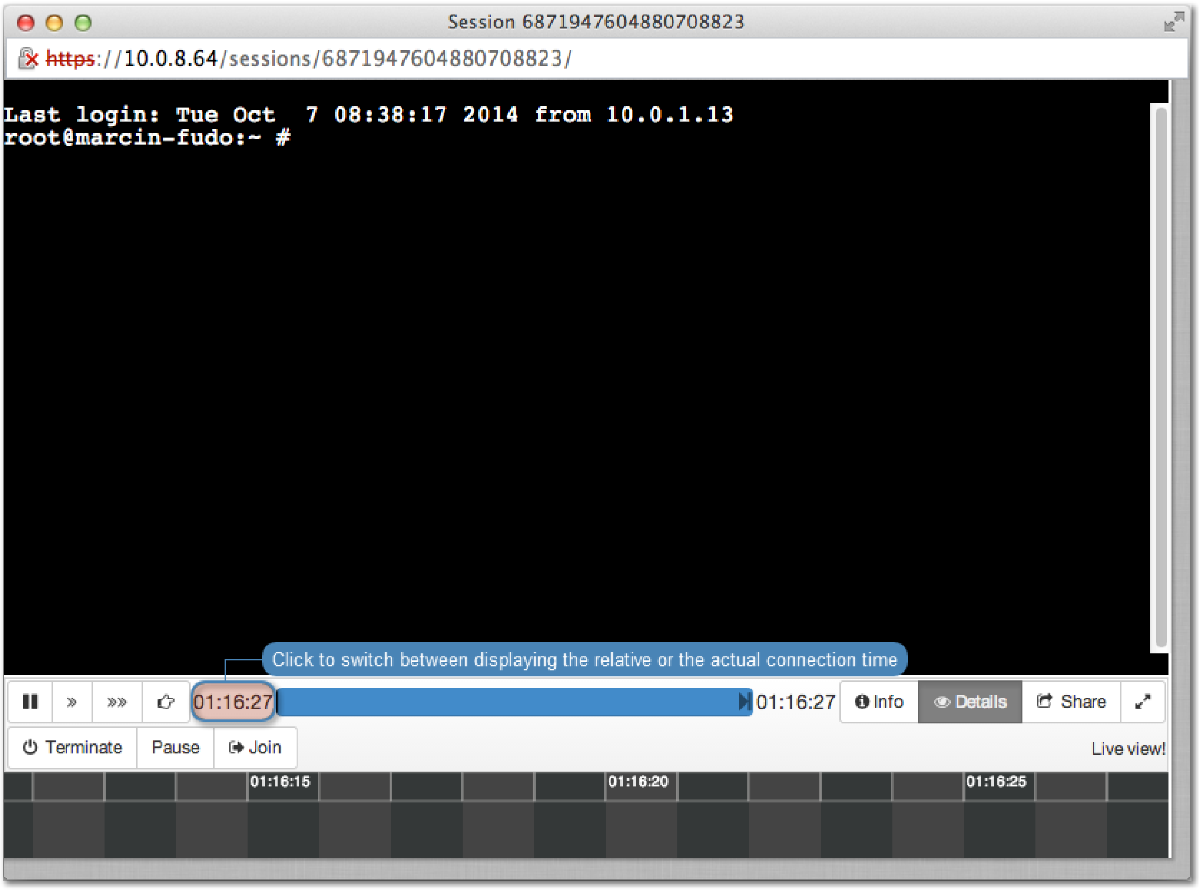
Note: Playing a session containing the specified phrase starts from the moment of its first occurrence.

The player enables skipping between each occurrence of the specified phrase.


Session 848388532111147062
https://10.0.40.50/sessions/848388532111147062/?q=ll
The search phrase is highlighted
Skip to the previous occurrence
Skip to the next occurrence
00:00:10
00:00:25
Info
Details
Share
00:00:00
00:00:05
00:00:10
00:00:15
[return]
[return]

```
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.  All rights reserved.

FreeBSD 8.3-RELEASE (GENERIC) #0: Mon Apr  9 21:23:18 UTC 2012

Welcome to FreeBSD!

Before seeking technical support, please use the following resources:

o  Security advisories and updated errata information for all releases are
   at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
   for your release first as it's updated frequently.

o  The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
   along with the mailing lists, can be searched by going to
   http://www.FreeBSD.org/search/.  If the doc distribution has
   been installed, they're also available formatted in /usr/share/doc.

If you still have a question or problem, please take the output of
`uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list.  If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page.  If you are not familiar with manual pages, type `man man'.

You may also use sysinstall(8) to re-enter the installation and
configuration utility.  Edit /etc/motd to change this login announcement.

fbsd83-cert# ll
```

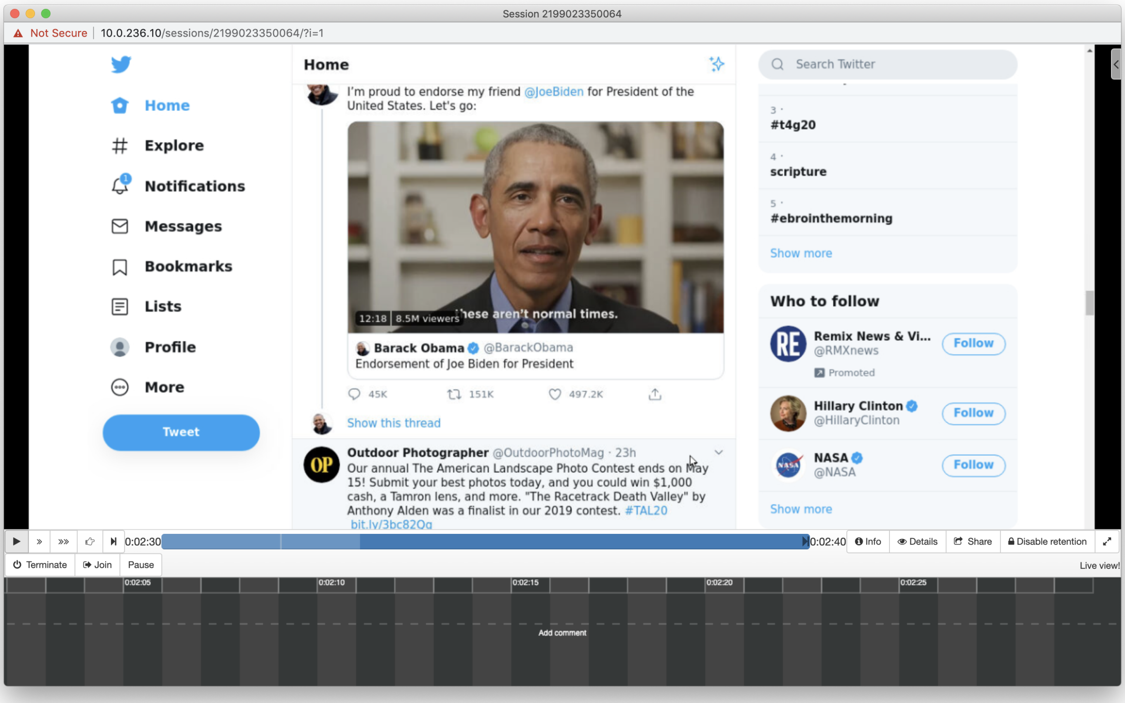
Note: Click the displayed elapsed time to switch between the connections's actual and relative time.



```
Last login: Tue Oct  7 08:38:17 2014 from 10.0.1.13
root@marcin-fudo:~ #
```

Click to switch between displaying the relative or the actual connection time

HTTP - rendered



I'm proud to endorse my friend @JoeBiden for President of the United States. Let's go:

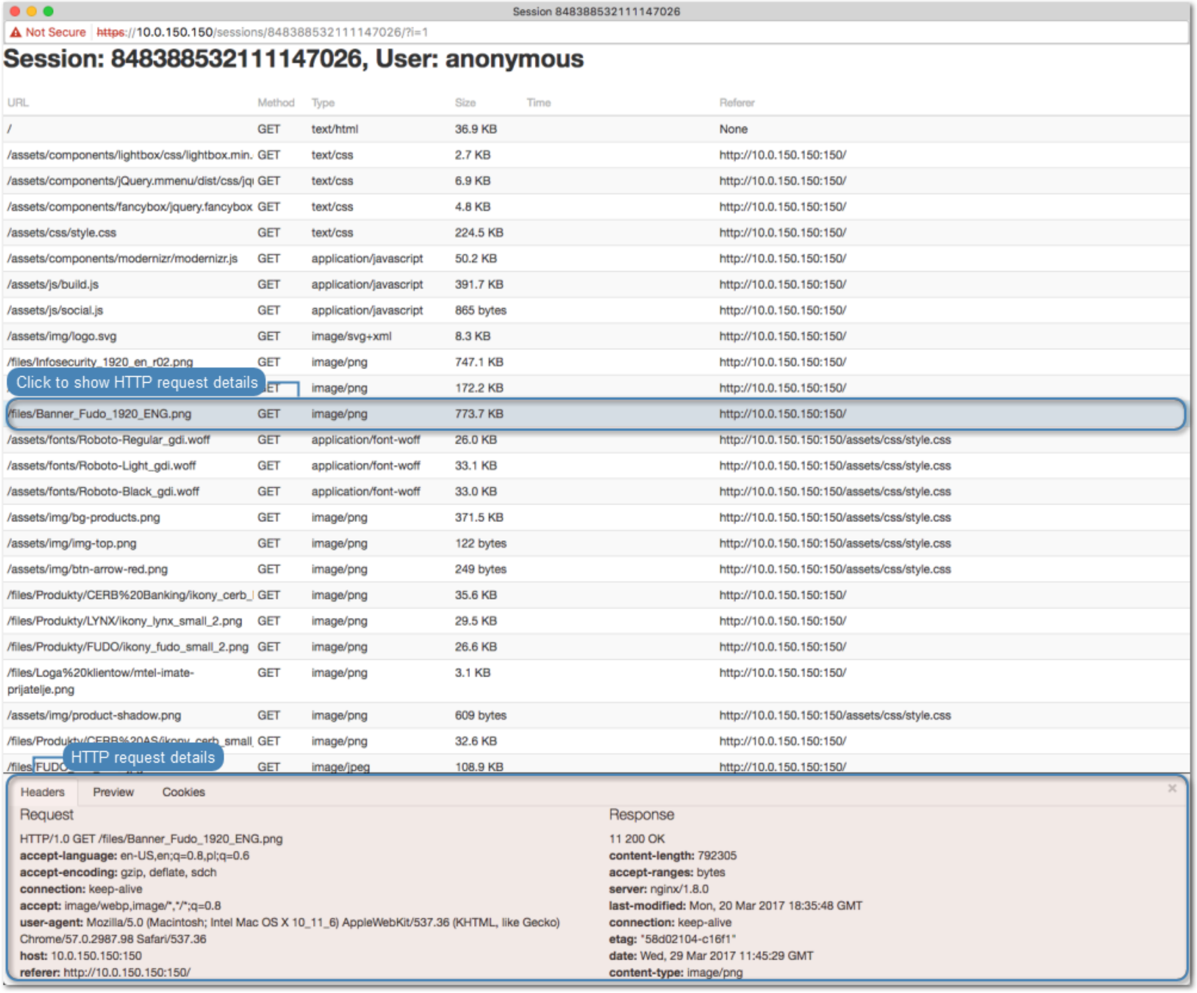
…hese aren't normal times.

Barack Obama @BarackObama
Endorsement of Joe Biden for President

Outdoor Photographer @OutdoorPhotoMag · 23h
Our annual The American Landscape Photo Contest ends on May 15! Submit your best photos today, and you could win $1,000 cash, a Tamron lens, and more. "The Racetrack Death Valley" by Anthony Alden was a finalist in our 2019 contest. #TAL20
bit.ly/3bc82Qq

Note: In case of rendered HTTP sessions, raw protocol data is not recorded.

HTTP - raw



Session 848388532111147026

⚠ Not Secure | ~~https~~://10.0.150.150/sessions/848388532111147026/?i=1

Session: 848388532111147026, User: anonymous

URL	Method	Type	Size	Time	Referer
/	GET	text/html	36.9 KB		None
/assets/components/lightbox/css/lightbox.min.	GET	text/css	2.7 KB		http://10.0.150.150:150/
/assets/components/jQuery.mmenu/dist/css/jq	GET	text/css	6.9 KB		http://10.0.150.150:150/
/assets/components/fancybox/jquery.fancybox	GET	text/css	4.8 KB		http://10.0.150.150:150/
/assets/css/style.css	GET	text/css	224.5 KB		http://10.0.150.150:150/
/assets/components/modernizr/modernizr.js	GET	application/javascript	50.2 KB		http://10.0.150.150:150/
/assets/js/build.js	GET	application/javascript	391.7 KB		http://10.0.150.150:150/
/assets/js/social.js	GET	application/javascript	865 bytes		http://10.0.150.150:150/
/assets/img/logo.svg	GET	image/svg+xml	8.3 KB		http://10.0.150.150:150/
/files/Infosecurity_1920_en_r02.png	GET	image/png	747.1 KB		http://10.0.150.150:150/
[illegible]	GET	image/png	172.2 KB		http://10.0.150.150:150/
/files/Banner_Fudo_1920_ENG.png	GET	image/png	773.7 KB		http://10.0.150.150:150/
/assets/fonts/Roboto-Regular_gdi.woff	GET	application/font-woff	26.0 KB		http://10.0.150.150:150/assets/css/style.css
/assets/fonts/Roboto-Light_gdi.woff	GET	application/font-woff	33.1 KB		http://10.0.150.150:150/assets/css/style.css
/assets/fonts/Roboto-Black_gdi.woff	GET	application/font-woff	33.0 KB		http://10.0.150.150:150/assets/css/style.css
/assets/img/bg-products.png	GET	image/png	371.5 KB		http://10.0.150.150:150/assets/css/style.css
/assets/img/img-top.png	GET	image/png	122 bytes		http://10.0.150.150:150/assets/css/style.css
/assets/img/btn-arrow-red.png	GET	image/png	249 bytes		http://10.0.150.150:150/assets/css/style.css
/files/Produkty/CERB%20Banking/ikony_cerb_	GET	image/png	35.6 KB		http://10.0.150.150:150/
/files/Produkty/LYNX/ikony_lynx_small_2.png	GET	image/png	29.5 KB		http://10.0.150.150:150/
/files/Produkty/FUDO/ikony_fudo_small_2.png	GET	image/png	26.6 KB		http://10.0.150.150:150/
/files/Loga%20klientow/mtel-imate-prijatelje.png	GET	image/png	3.1 KB		http://10.0.150.150:150/
/assets/img/product-shadow.png	GET	image/png	609 bytes		http://10.0.150.150:150/assets/css/style.css
/files/Produkty/CERB%20AS/ikony_cerb_small_	GET	image/png	32.6 KB		http://10.0.150.150:150/
/files/FUDO	GET	image/jpeg	108.9 KB		http://10.0.150.150:150/

Headers | Preview | Cookies

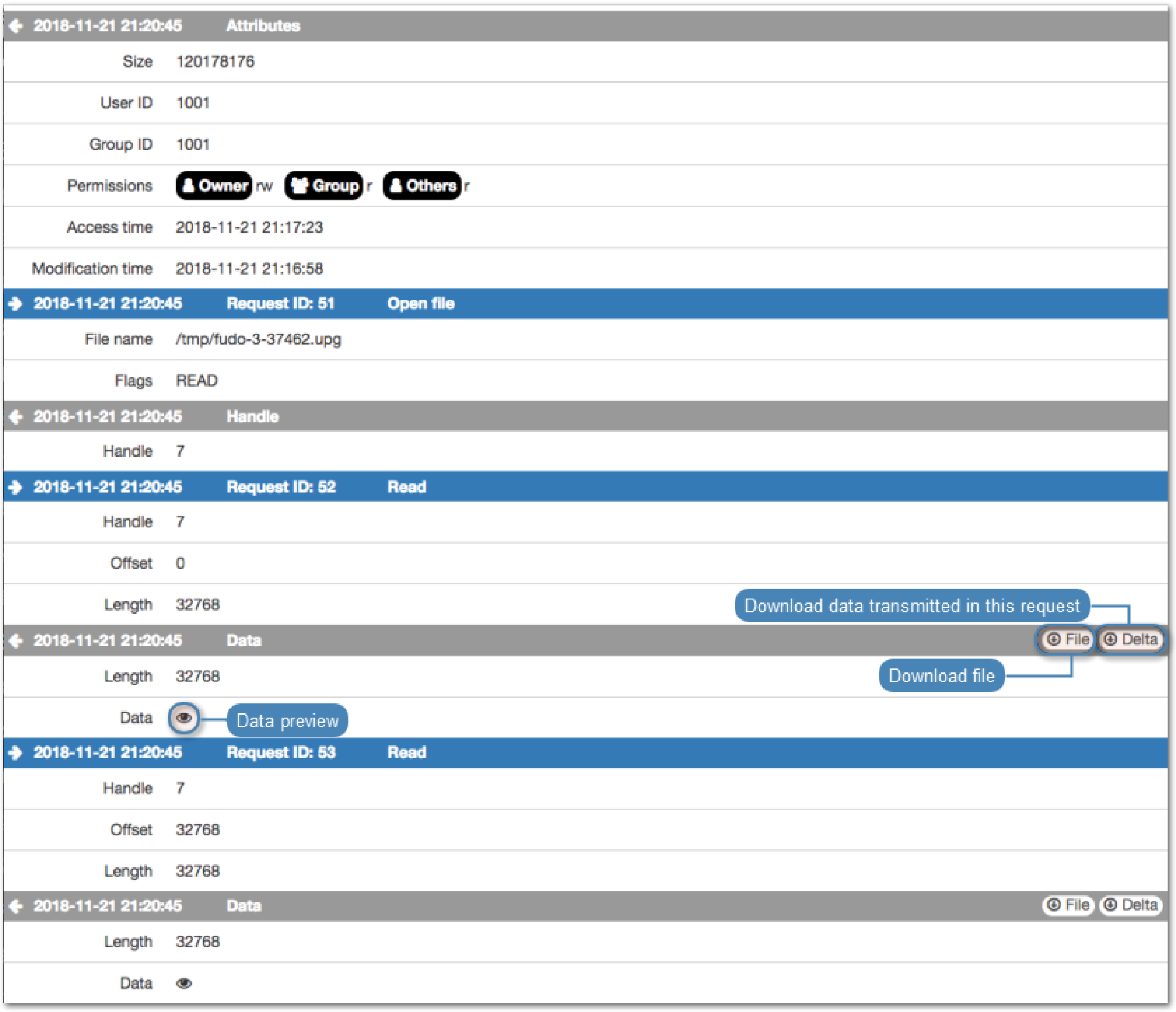
Request

HTTP/1.0 GET /files/Banner_Fudo_1920_ENG.png
accept-language: en-US,en;q=0.8,pl;q=0.6
accept-encoding: gzip, deflate, sdch
connection: keep-alive
accept: image/webp,image/*,*/*;q=0.8
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.98 Safari/537.36
host: 10.0.150.150:150
referer: http://10.0.150.150:150/

Response

11 200 OK
content-length: 792305
accept-ranges: bytes
server: nginx/1.8.0
last-modified: Mon, 20 Mar 2017 18:35:48 GMT
connection: keep-alive
etag: "58d02104-c16f1"
date: Wed, 29 Mar 2017 11:45:29 GMT
content-type: image/png

SFTP



2018-11-21 21:20:45 Attributes

Size 120178176

User ID 1001

Group ID 1001

Permissions Owner rw Group r Others r

Access time 2018-11-21 21:17:23

Modification time 2018-11-21 21:16:58

2018-11-21 21:20:45 Request ID: 51 Open file

File name /tmp/fudo-3-37462.upg

Flags READ

2018-11-21 21:20:45 Handle

Handle 7

2018-11-21 21:20:45 Request ID: 52 Read

Handle 7

Offset 0

Length 32768

2018-11-21 21:20:45 Data

Length 32768

Data

2018-11-21 21:20:45 Request ID: 53 Read

Handle 7

Offset 32768

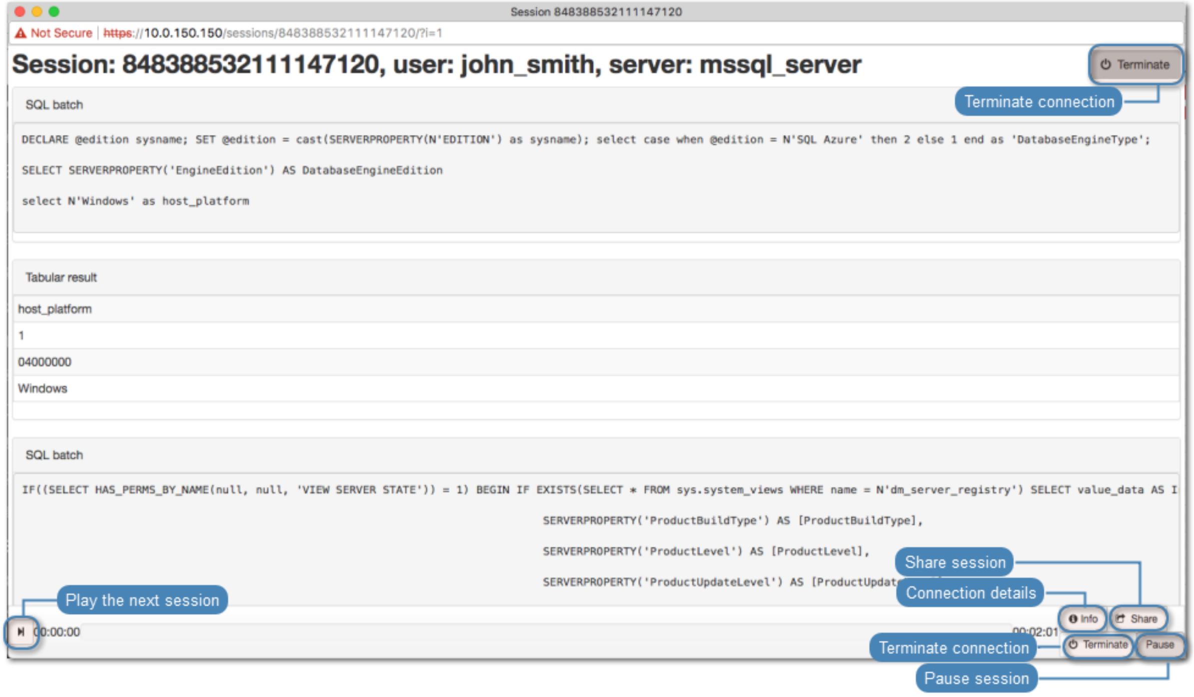
Length 32768

2018-11-21 21:20:45 Data

Length 32768

Data

MySQL, MSSQL, Oracle



Session 848388532111147120

Not Secure | https://10.0.150.150/sessions/848388532111147120/?i=1

Session: 848388532111147120, user: john_smith, server: mssql_server

SQL batch

```
DECLARE @edition sysname; SET @edition = cast(SERVERPROPERTY(N'EDITION') as sysname); select case when @edition = N'SQL Azure' then 2 else 1 end as 'DatabaseEngineType';

SELECT SERVERPROPERTY('EngineEdition') AS DatabaseEngineEdition

select N'Windows' as host_platform
```

Tabular result

host_platform

1

04000000

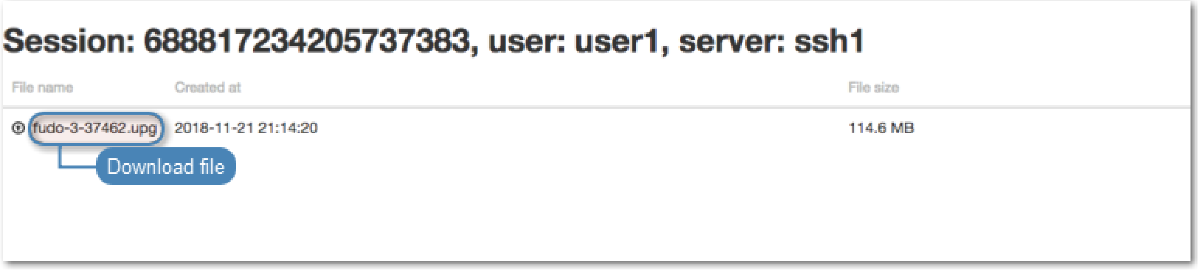
Windows

SQL batch

```
IF((SELECT HAS_PERMS_BY_NAME(null, null, 'VIEW SERVER STATE')) = 1) BEGIN IF EXISTS(SELECT * FROM sys.system_views WHERE name = N'dm_server_registry') SELECT value_data AS I

                                             SERVERPROPERTY('ProductBuildType') AS [ProductBuildType],

                                             SERVERPROPERTY('ProductLevel') AS [ProductLevel],

                                             SERVERPROPERTY('ProductUpdateLevel') AS [ProductUpdat
```

00:00:00 00:02:01

SCP



Session: 6888172342057373383, user: user1, server: ssh1

File name	Created at	File size
fudo-3-37462.upg	2018-11-21 21:14:20	114.6 MB

Related topics:

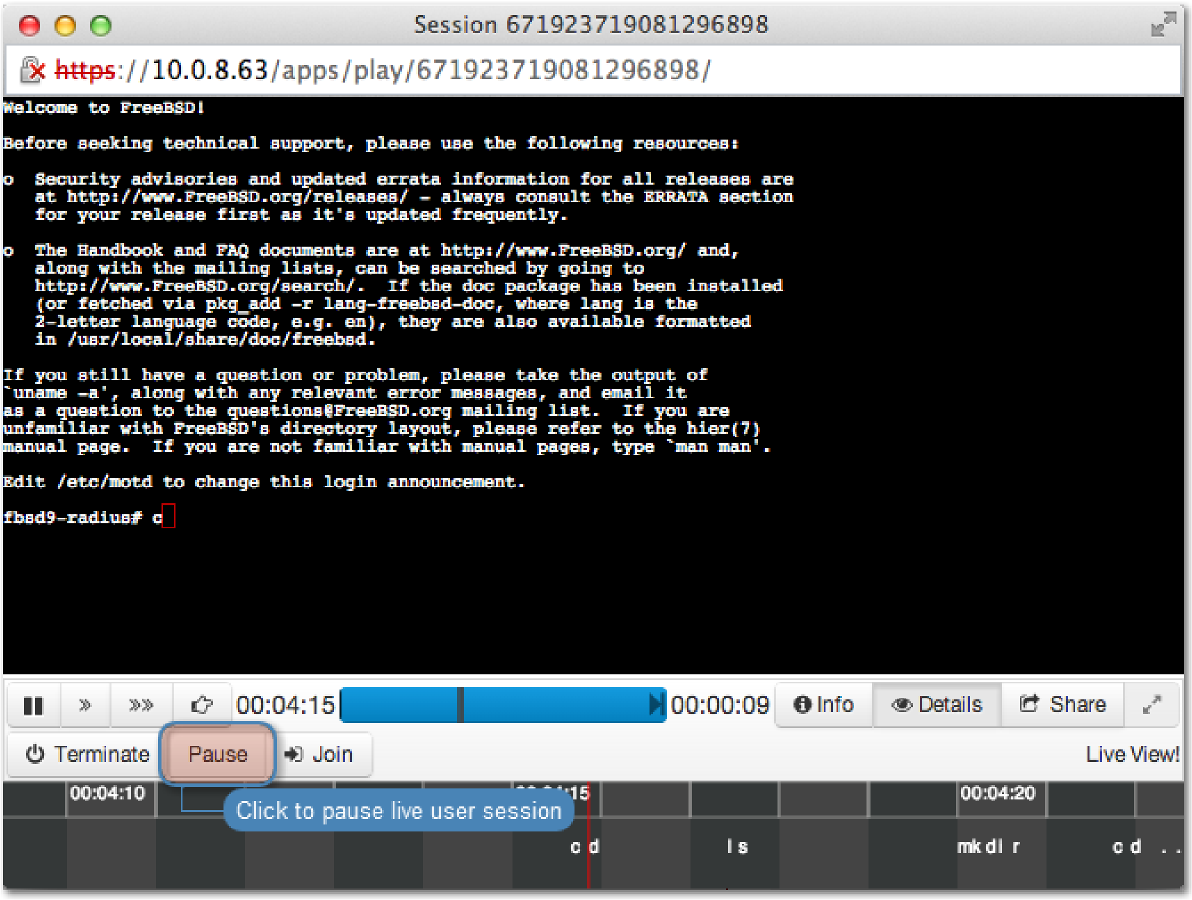
- *Sensitive features*

12.3 Pausing connection

In case a current user action requires analysis, the connection to the server can be paused.

Note: Pausing connection temporarily suspends data transmission. After resuming connection, buffered user's actions are forwarded to the server.

1. Select *Management* > *Sessions*.
2. Click *Add filter* and select *Active*.
3. Select *Yes* from the drop-down list.
4. Find desired session and and click the play icon to start playback.
5. Click *Pause*.



Session 671923719081296898
https://10.0.8.63/apps/play/671923719081296898/
00:04:15
00:00:09
Info
Details
Share
Terminate
Pause
Join
Live View!
00:04:10
00:04:15
00:04:20
Click to pause live user session
c d
l s
mk dl r
c d . .

```
Welcome to FreeBSD!

Before seeking technical support, please use the following resources:

o  Security advisories and updated errata information for all releases are
   at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
   for your release first as it's updated frequently.

o  The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
   along with the mailing lists, can be searched by going to
   http://www.FreeBSD.org/search/.  If the doc package has been installed
   (or fetched via pkg_add -r lang-freebsd-doc, where lang is the
   2-letter language code, e.g. en), they are also available formatted
   in /usr/local/share/doc/freebsd.

If you still have a question or problem, please take the output of
`uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list.  If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page.  If you are not familiar with manual pages, type `man man'.

Edit /etc/motd to change this login announcement.

fbsd9-radius# c
```

Related topics:

- Replaying session
- *Joining session*
- *Filtering session*

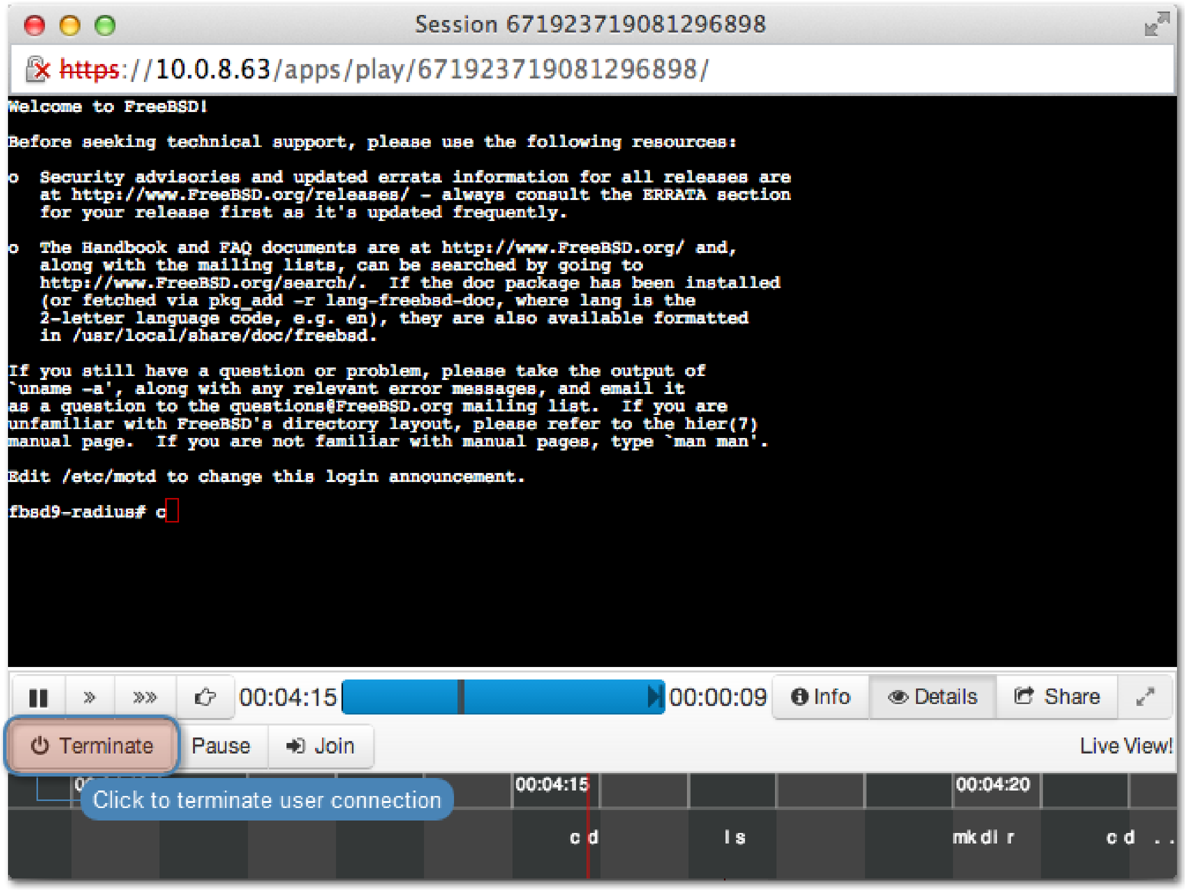
12.4 Terminating connection

In case the administrator notices access rights misuse, Fudo PAM allows to terminate the session and automatically block given user.

Note: Fudo PAM can automatically block user account upon detecting a defined pattern. For more information refer to *Policies*.

1. Select *Management > Sessions*.
2. Click *Add filter* and select *Active*.
3. Select *Yes* from the drop-down list.
4. Find desired session and click the playback icon to start playback.
5. Click *Terminate*.

Note: Terminating connection automatically blocks given user.


Session 671923719081296898
https://10.0.8.63/apps/play/671923719081296898/
00:04:15
00:00:09
Info
Details
Share
Terminate
Pause
Join
Live View!
Click to terminate user connection
00:04:15
00:04:20
c d
l s
mk dl r
c d
. .

```
Welcome to FreeBSD!

Before seeking technical support, please use the following resources:

o  Security advisories and updated errata information for all releases are
   at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
   for your release first as it's updated frequently.

o  The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
   along with the mailing lists, can be searched by going to
   http://www.FreeBSD.org/search/.  If the doc package has been installed
   (or fetched via pkg_add -r lang-freebsd-doc, where lang is the
   2-letter language code, e.g. en), they are also available formatted
   in /usr/local/share/doc/freebsd.

If you still have a question or problem, please take the output of
`uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list.  If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page.  If you are not familiar with manual pages, type `man man'.

Edit /etc/motd to change this login announcement.

fbsd9-radius# c
```

6. Decide whether the user should remain blocked or not.

Related topics:

- *Policies*
- *Security measures*
- *Joining live session*
- *Sharing sessions*
- *Filtering sessions*

12.5 Joining live session

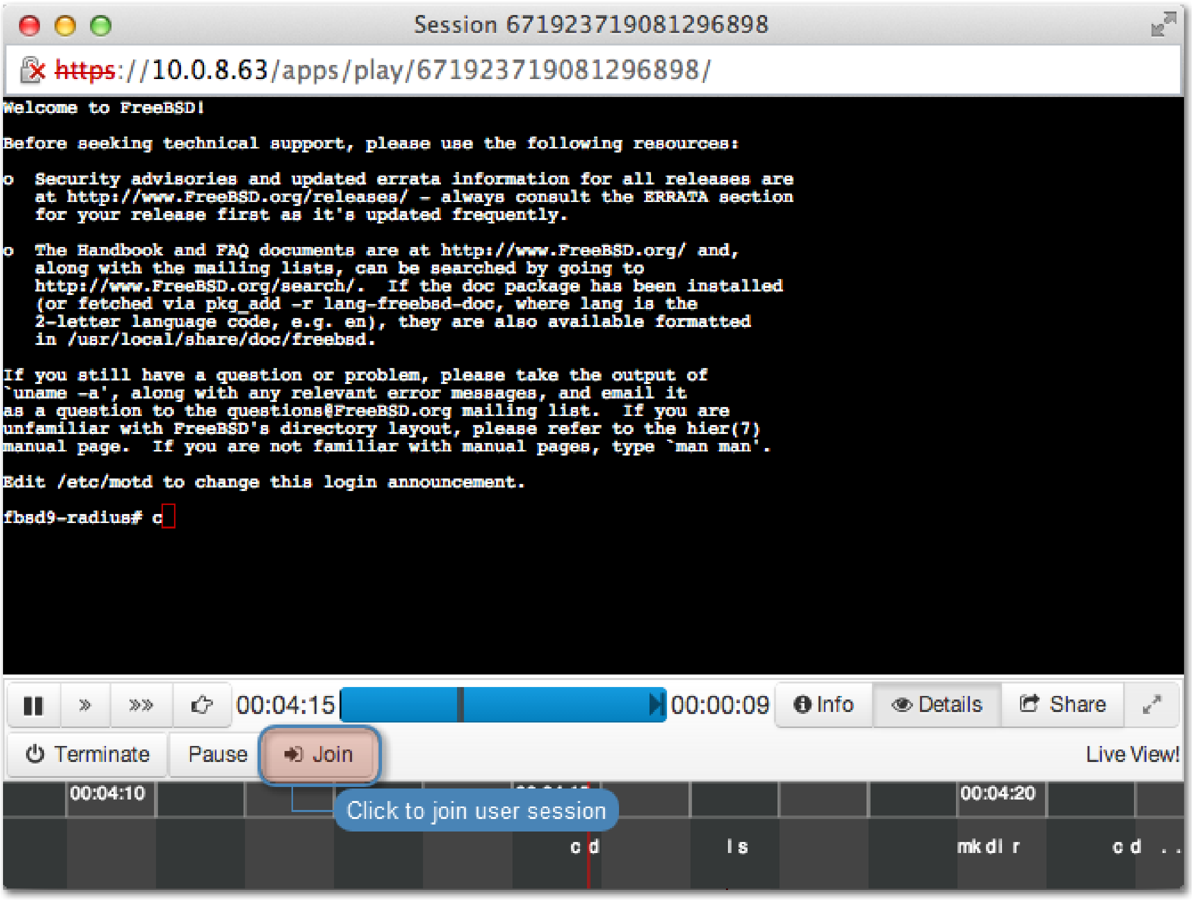
Fudo PAM allows joining an ongoing session to work simultaneously with the remote user.

Note:

- Session joining feature is supported in SSH, RDP, VNC and Telnet (excluding 5250 and 3270) connections.
- In case of cluster configurations, joining session is only possible after logging into the administration panel on the node that handles the given access session.

To join currently established session, proceed as follows.

1. Select *Management* > *Sessions*.
2. Click *Add filter* and select *Active*.
3. Select *Yes* from the drop-down list.
4. Find desired session and and click the play icon to start playback.
5. Click *Join*.


Session 671923719081296898
https://10.0.8.63/apps/play/671923719081296898/
00:04:15
00:00:09
Info
Details
Share
Terminate
Pause
Join
Live View!
00:04:10
00:04:20
Click to join user session
cd
ls
mkdir
cd ..

```
Welcome to FreeBSD!

Before seeking technical support, please use the following resources:

o   Security advisories and updated errata information for all releases are
    at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
    for your release first as it's updated frequently.

o   The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
    along with the mailing lists, can be searched by going to
    http://www.FreeBSD.org/search/.  If the doc package has been installed
    (or fetched via pkg_add -r lang-freebsd-doc, where lang is the
    2-letter language code, e.g. en), they are also available formatted
    in /usr/local/share/doc/freebsd.

If you still have a question or problem, please take the output of
`uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list.  If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page.  If you are not familiar with manual pages, type `man man'.

Edit /etc/motd to change this login announcement.

fbsd9-radius# c
```

Related topics:

- Replaying sessions
- *Sharing sessions*
- *Filtering sessions*
- *Supported protocols*

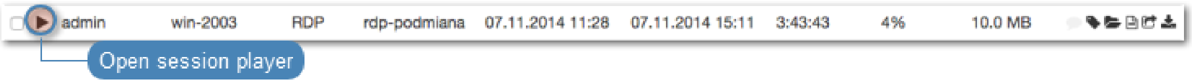
12.6 Sharing sessions

Fudo PAM enables sharing given session with another user.

Sharing a session

To share a session, proceed as follows.

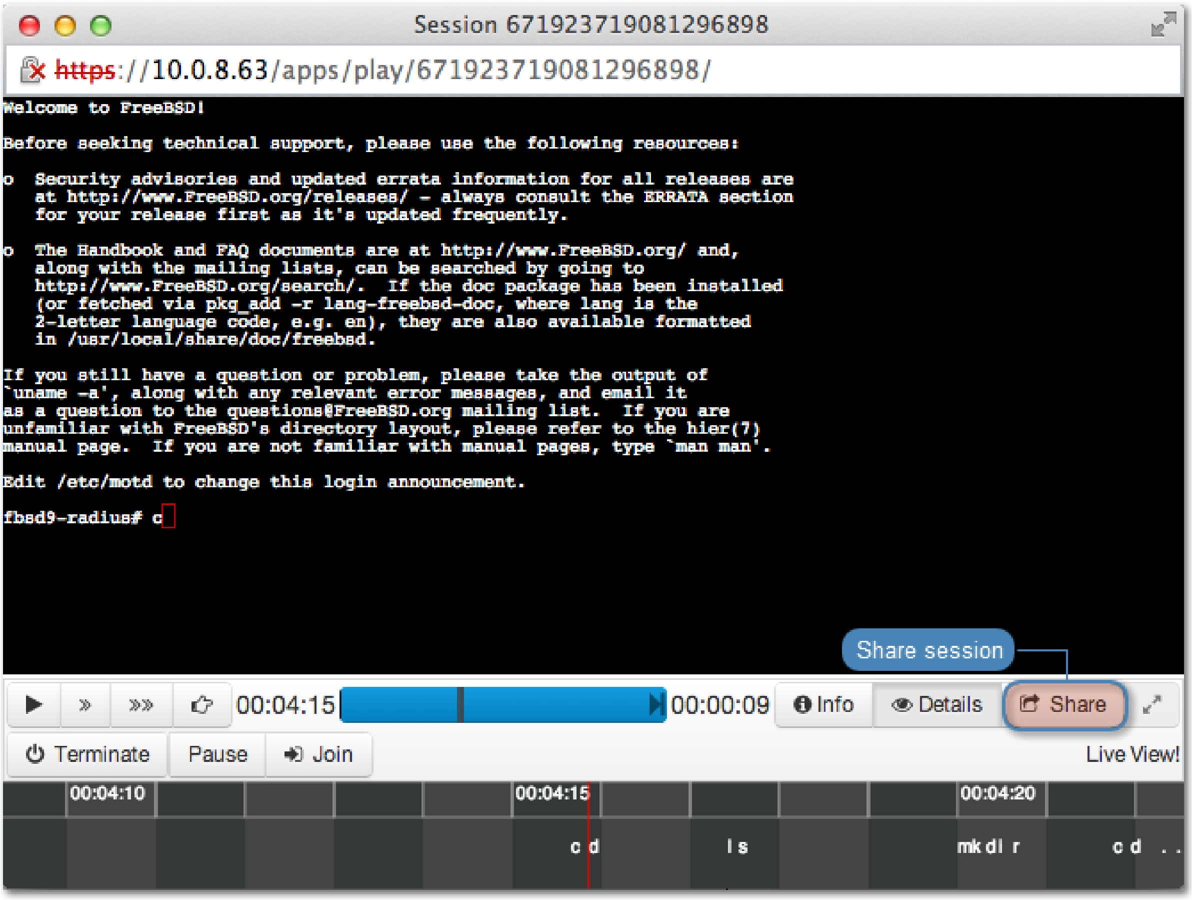
1. Select *Management* > *Sessions*.
2. Find desired session and and click the play icon to start playback.



admin win-2003 RDP rdp-podmiana 07.11.2014 11:28 07.11.2014 15:11 3:43:43 4% 10.0 MB

Open session player

3. Click *Share*.



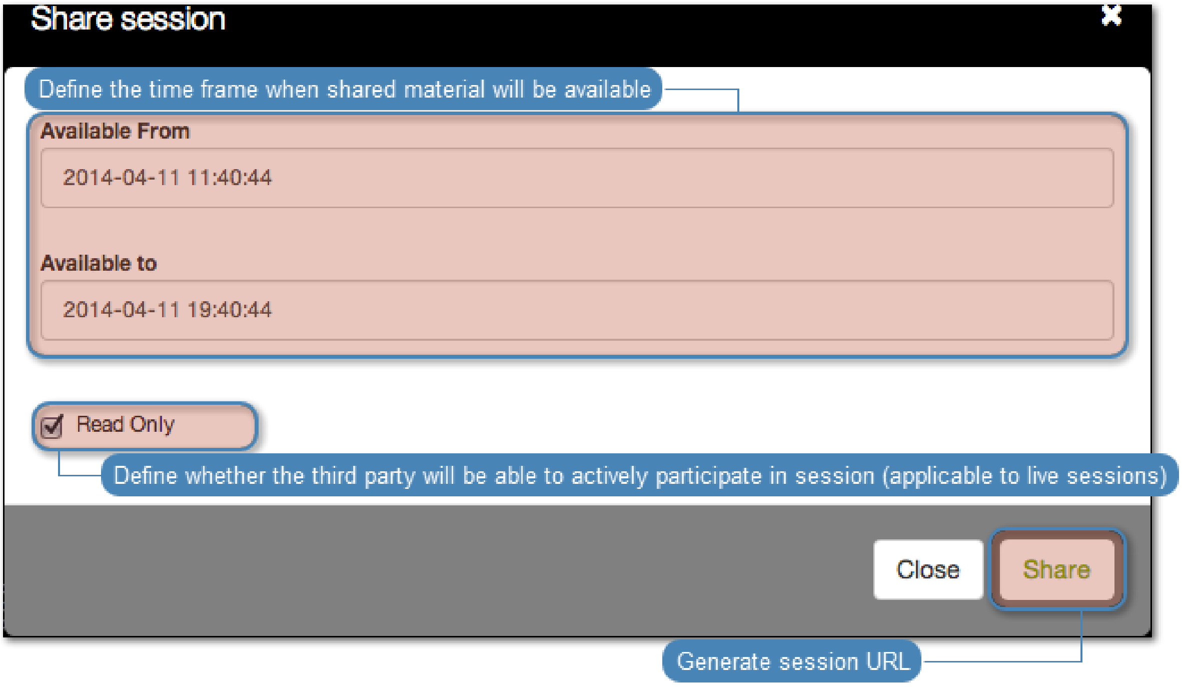
Session 671923719081296898

https://10.0.8.63/apps/play/671923719081296898/

```
Welcome to FreeBSD!

Before seeking technical support, please use the following resources:

o   Security advisories and updated errata information for all releases are
    at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
    for your release first as it's updated frequently.

o   The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
    along with the mailing lists, can be searched by going to
    http://www.FreeBSD.org/search/.  If the doc package has been installed
    (or fetched via pkg_add -r lang-freebsd-doc, where lang is the
    2-letter language code, e.g. en), they are also available formatted
    in /usr/local/share/doc/freebsd.

If you still have a question or problem, please take the output of
`uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list.  If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page.  If you are not familiar with manual pages, type `man man'.

Edit /etc/motd to change this login announcement.

fbsd9-radius# c
```

Share session

4. Provide session availability time frame and click *Confirm* to generate URL.



Share session

Define the time frame when shared material will be available

Available From: 2014-04-11 11:40:44

Available to: 2014-04-11 19:40:44

☑ Read Only

Define whether the third party will be able to actively participate in session (applicable to live sessions)

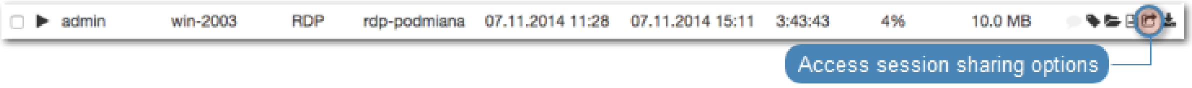
Generate session URL

5. Copy the system generated URL and click *Close*.

Revoking session URL

To revoke a session URL, proceed as follows:

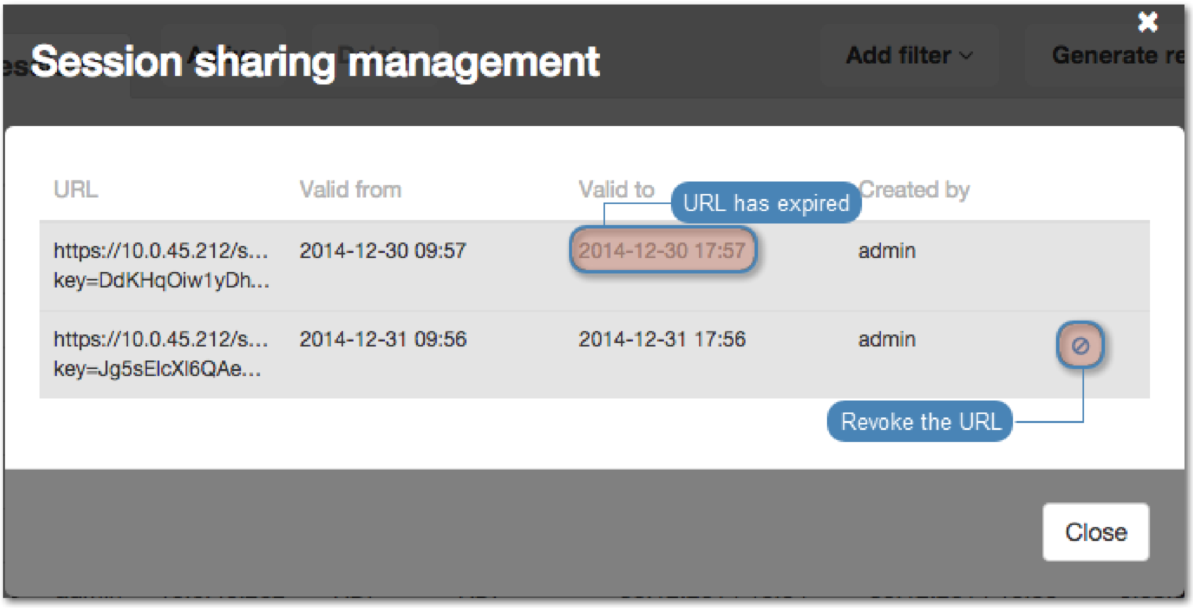
1. Select *Management* > *Sessions*.
2. Find desired session and click the *share* icon to display sessions sharing management options.



□ ▶	admin	win-2003	RDP	rdp-podmiana	07.11.2014 11:28	07.11.2014 15:11	3:43:43	4%	10.0 MB

Access session sharing options

3. Click the *revoke* icon to deactivate given URL.



Session sharing management

URL	Valid from	Valid to	Created by	
https://10.0.45.212/s... key=DdKHqOiw1yDh...	2014-12-30 09:57	2014-12-30 17:57	admin	
https://10.0.45.212/s... key=Jg5sElcXI6QAe...	2014-12-31 09:56	2014-12-31 17:56	admin	⊘

URL has expired

Revoke the URL

Related topics:

- Replaying sessions
- *Joining sessions*
- *Filtering sessions*

12.7 Commenting sessions

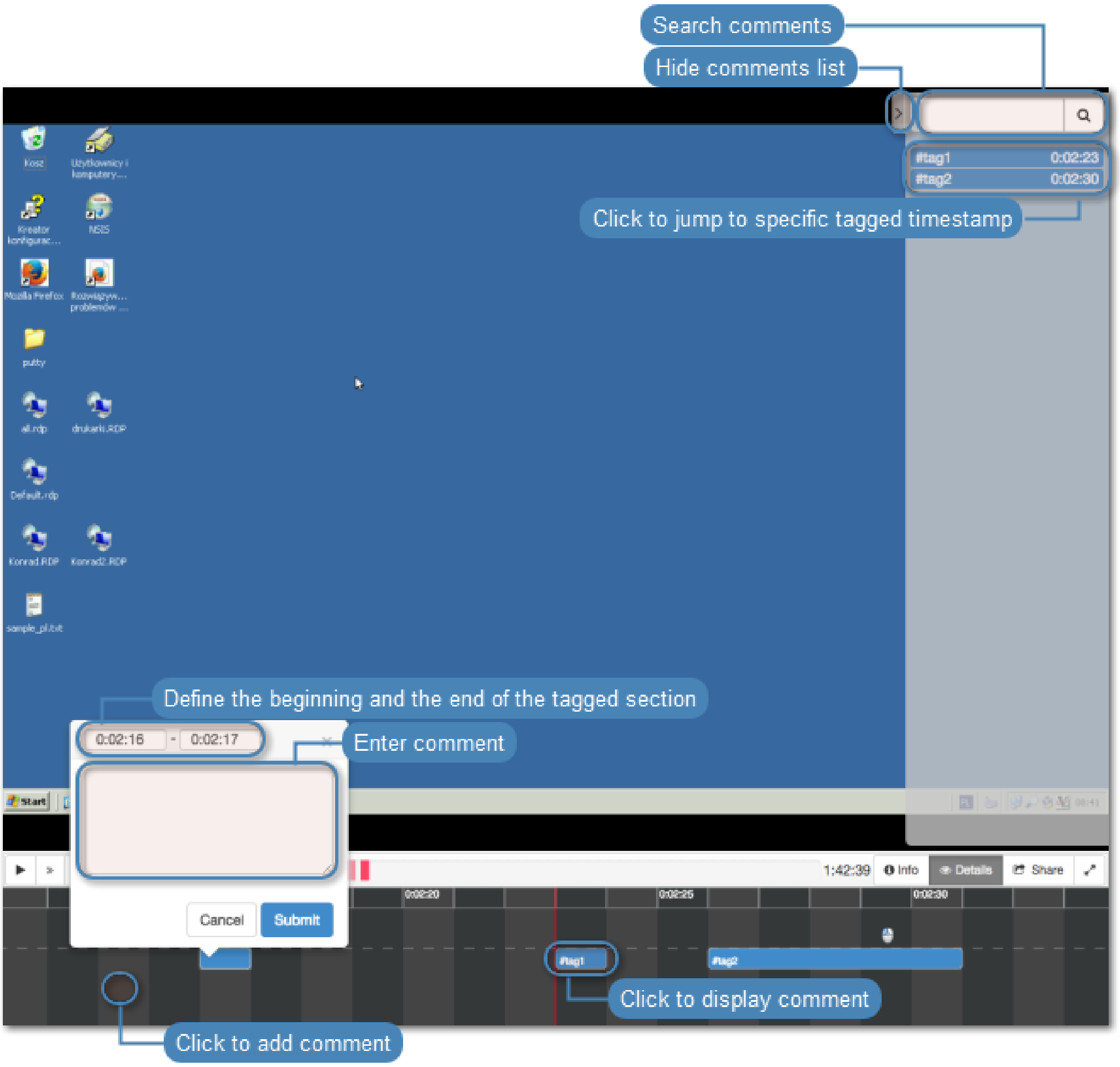
Fudo PAM enables adding comments and tags to recorded sessions.

Adding a comment

1. Select *Management > Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Details*.
4. Click the lower part of the timeline to add a comment.
5. Define time interval which applies to this comment.

Note: Click and drag either side of the tag to change the starting/ending time.

6. Add comment.
7. Click *Submit*.



Editing a comment

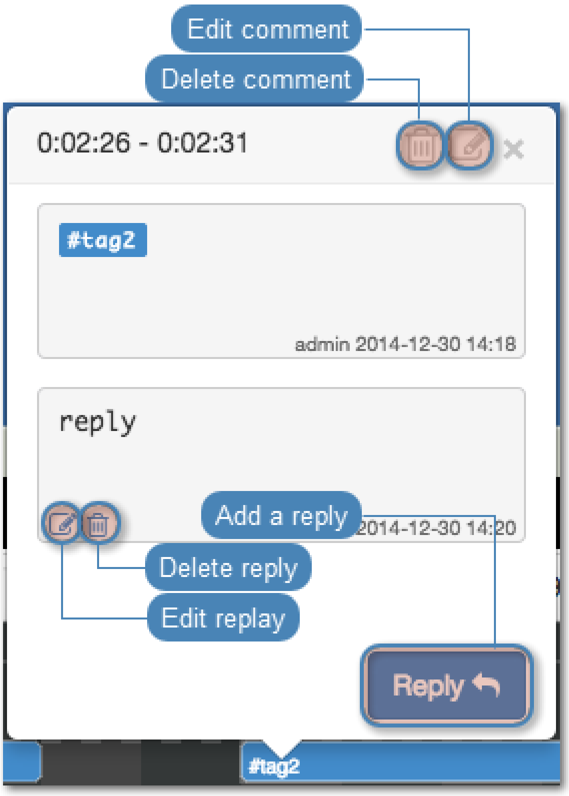
1. Select *Management* > *Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Details*.
4. Find and click desired comment.
5. Click the edit icon.
6. Change the comment and *Submit*.

Deleting a comment

1. Select *Management* > *Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Details*.
4. Find and click desired comment.

5. Click the trashcan icon.

6. Click *Delete* to delete the comment.



Replying to a comment

1. Select *Management* > *Sessions*.
2. Find desired session and click the playback icon to start playback.
3. Click *Details*.
4. Find and click desired comment.
5. Click *Reply*.
6. Enter message and click *Submit*.

Related topics:

- *Sensitive features*

12.8 Sessions' retention lockdown

Data retention feature automatically deletes sessions after a specified time interval. Fudo allows for excluding selected sessions from the retention mechanism.

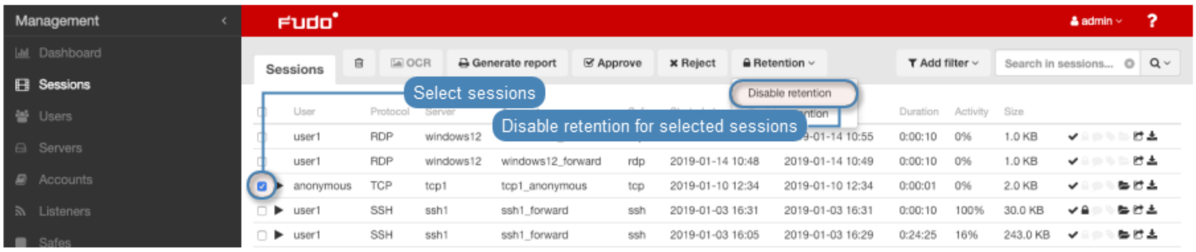
Disabling retention

To disable retention for specified sessions, proceed as follows.

1. Select *Management* > *Sessions*.
2. Find and select desired sessions.

3. Click *Retention*.

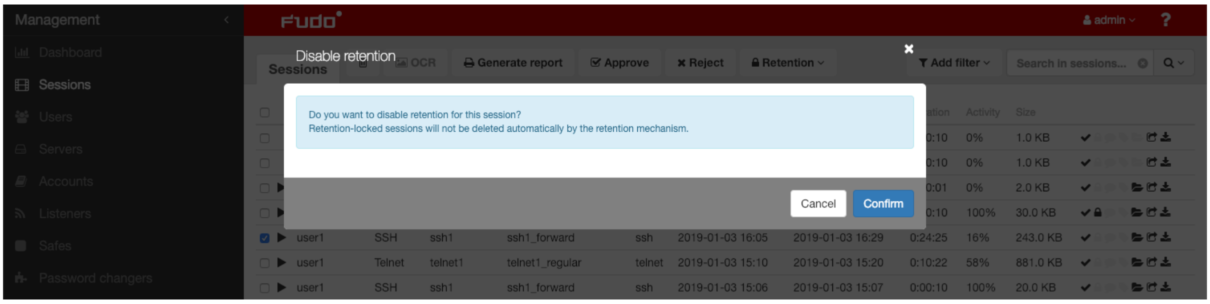
4. Select *Disable retention*.



Select sessions

Disable retention for selected sessions

5. Click *Confirm* to disable retention for selected sessions.



Disable retention

Do you want to disable retention for this session?
Retention-locked sessions will not be deleted automatically by the retention mechanism.

Note: Retention locked sessions are differentiated with the 🔒 status icon.

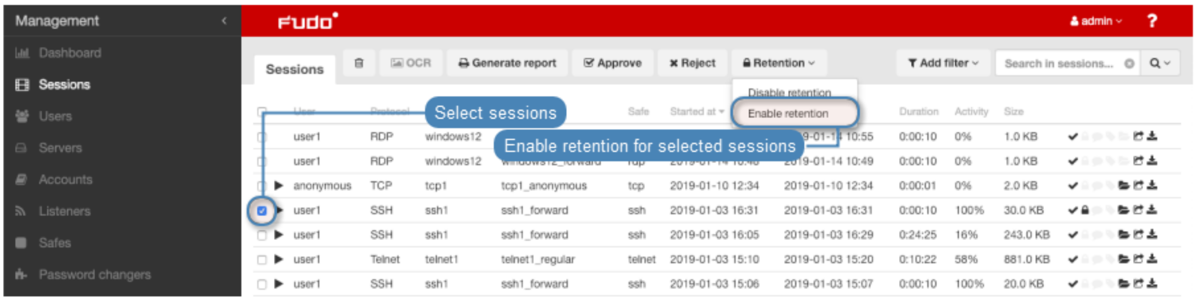
Enabling retention

1. Select *Management* > *Sessions*.

2. Find and select desired sessions.

3. Click *Retention*.

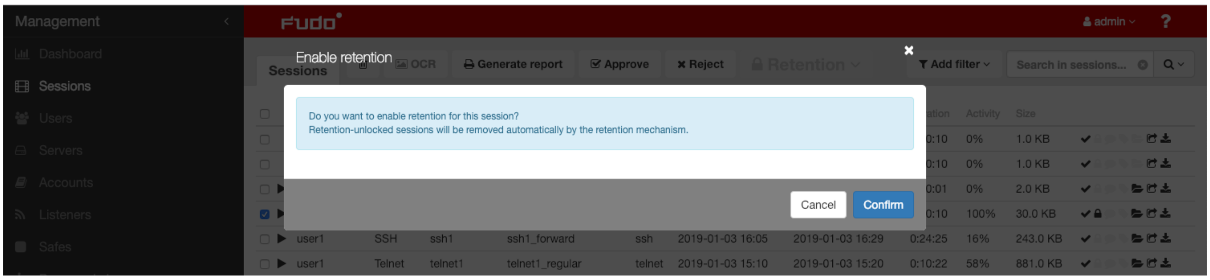
4. Select *Enable retention*.



Select sessions

Enable retention for selected sessions

5. Click *Confirm* to enable retention for selected sessions.



Enable retention

Do you want to enable retention for this session?
Retention-unlocked sessions will be removed automatically by the retention mechanism.

Related topics:

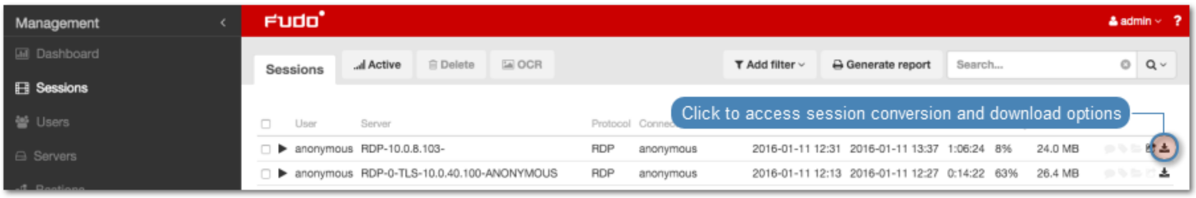
- *Backups and retention*

12.9 Exporting sessions

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.

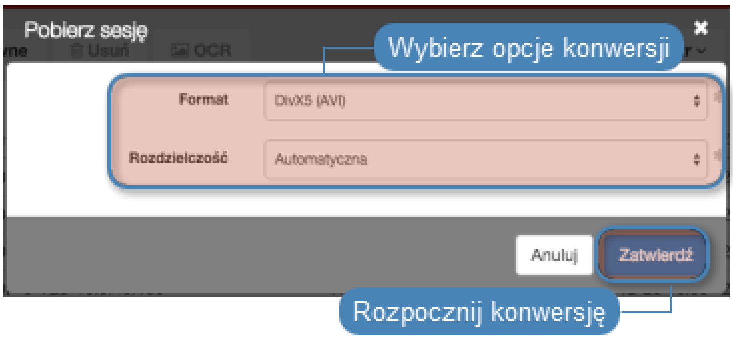


Click to access session conversion and download options

	User	Server	Protocol	Connec					
□ ▶	anonymous	RDP-10.0.8.103-	RDP	anonymous	2016-01-11 12:31	2016-01-11 13:37	1:06:24	8%	24.0 MB
□ ▶	anonymous	RDP-0-TLS-10.0.40.100-ANONYMOUS	RDP	anonymous	2016-01-11 12:13	2016-01-11 12:27	0:14:22	63%	26.4 MB

3. Select the output file format.

Note: The output file format and the resolution determine conversion time and the size of the output file.



Wybierz opcje konwersji

Format: DivX5 (AVI)

Rozdzielczość: Automatyczna

Rozpocznij konwersję

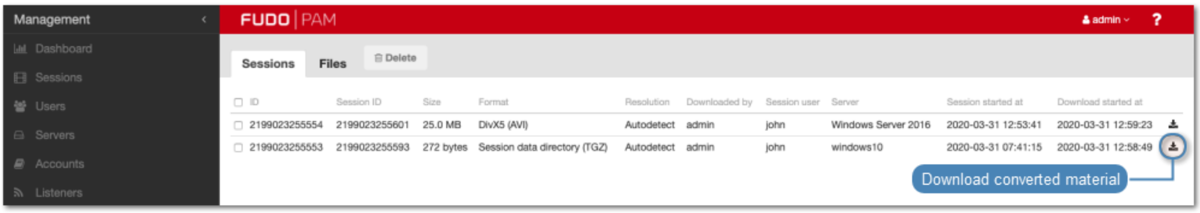
4. Select the video resolution (*not applicable to the text log file format*).

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.



□ ID	Session ID	Size	Format	Resolution	Downloaded by	Session user	Server	Session started at	Download started at	
□ 2199023255554	2199023255601	25.0 MB	DivX5 (AVI)	Autodetect	admin	john	Windows Server 2016	2020-03-31 12:53:41	2020-03-31 12:59:23	⤓
□ 2199023255553	2199023255593	272 bytes	Session data directory (TGZ)	Autodetect	admin	john	windows10	2020-03-31 07:41:15	2020-03-31 12:58:49	⤓

Related topics:

- *Filtering sessions*
- *Sharing sessions*
- Viewing sessions
- *Joining sessions*

12.10 Deleting sessions

To delete a recorded session, proceed as follows.

1. Select *Management > Sessions*.
2. Find and select desired session.
3. Click *Delete*.
4. Select *Remove associated resources* to also delete exported session material.
5. Confirm deleting selected sessions.

Note: Fudo PAM can automatically delete sessions after certain time, specified by the retention parameter. Refer to the *Backups and retention* topic for more on data retention.

Related topics:

- *Filtering sessions*
- *Sharing sessions*
- Replaying sessions
- *Exporting sessions*

12.11 OCR processing sessions

Recorded ICA, RDP, VNC and rendered HTTP sessions can be processed and indexed for full-text search purposes.

Warning: OCR processing is CPU intensive and may have negative impact on system's performance. It is recommended to enable it only for those accounts, which require detailed supervision.

Automated sessions processing

To have ICA, RDP, VNC or rendered HTTP sessions automatically processed, proceed as follows.

1. Select *Management > Accounts*.
2. Find and click desired account.
3. Select the *OCR sessions* option.
4. Select the language of processed data.
5. Click *Save*.

Processing selected sessions

To process selected sessions, proceed as follows.

1. Select *Management > Sessions*.
2. Select desired RDP or VNC sessions and click *OCR*.

Note: Filtering options allows for selecting processed or unprocessed objects.

3. Confirm processing selected sessions.

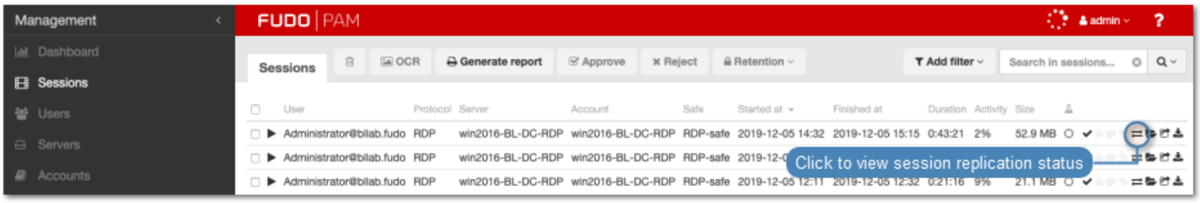
Related topics:

- *Filtering sessions*
- *Accounts*

12.12 Session data replication

Additionally to automated session data replication, Fudo PAM enables on-demand replication to Fudo PAM instances to which the given data is not replicated automatically.

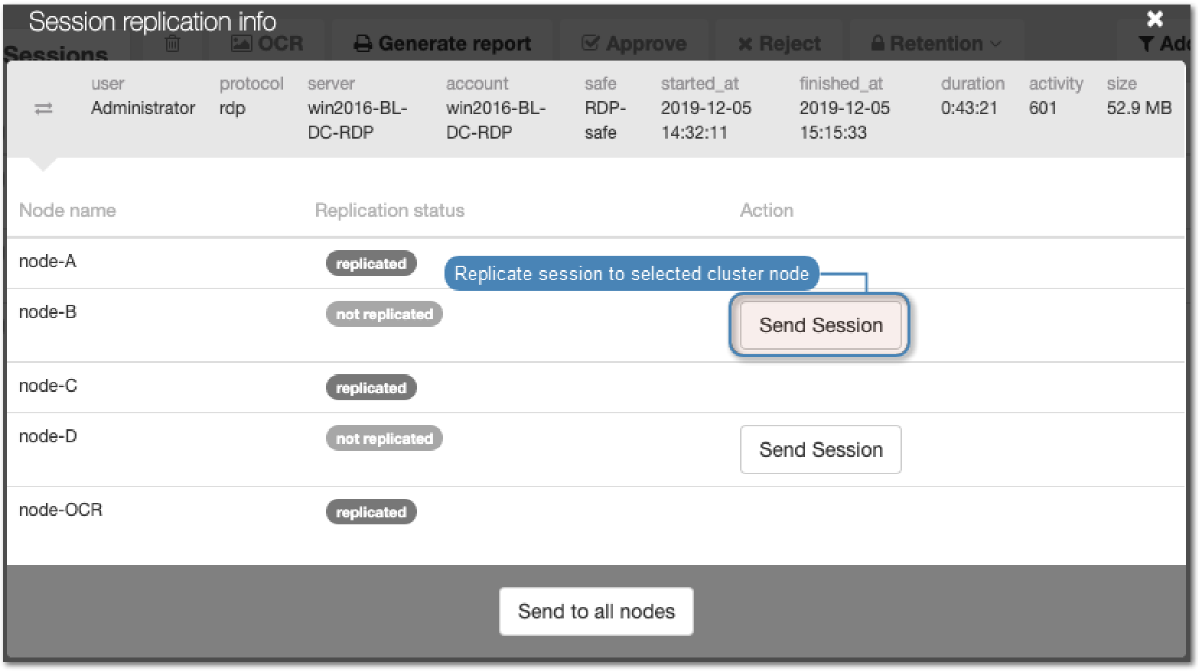
1. Select *Management > Sessions*.
2. Click ⇄ next to a session that you want to replicate.



□	User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
□ ▶	Administrator@bllab.fudo	RDP	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 14:32	2019-12-05 15:15	0:43:21	2%	52.9 MB
□ ▶	Administrator@bllab.fudo	RDP	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-0				
□ ▶	Administrator@bllab.fudo	RDP	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 12:11	2019-12-05 12:32	0:21:16	9%	21.1 MB

Click to view session replication status

3. Click *Send session* next to a specific cluster node to replicate session to selected Fudo PAM instance



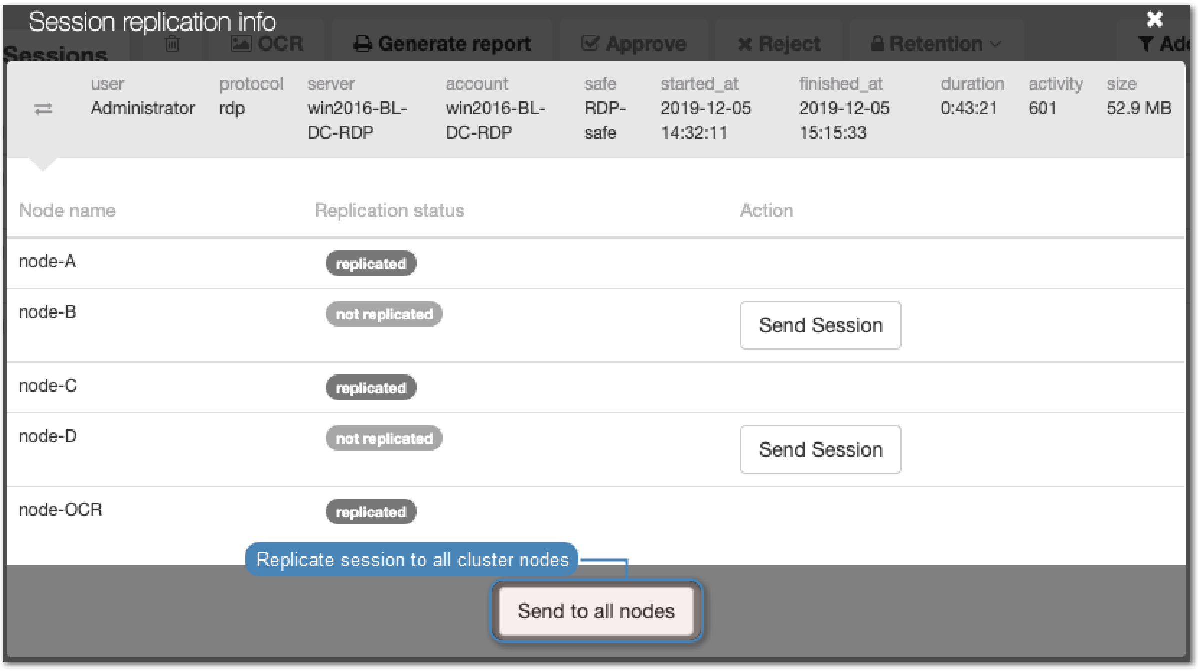
Session replication info

user	protocol	server	account	safe	started_at	finished_at	duration	activity	size
Administrator	rdp	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 14:32:11	2019-12-05 15:15:33	0:43:21	601	52.9 MB

Node name	Replication status	Action
node-A	replicated	
node-B	not replicated	Send Session
node-C	replicated	
node-D	not replicated	Send Session
node-OCR	replicated	

Send to all nodes

or click *Send to all nodes* to replicate session to all cluster nodes.



Session replication info

user	protocol	server	account	safe	started_at	finished_at	duration	activity	size
Administrator	rdp	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 14:32:11	2019-12-05 15:15:33	0:43:21	601	52.9 MB

Node name	Replication status	Action
node-A	replicated	
node-B	not replicated	Send Session
node-C	replicated	
node-D	not replicated	Send Session
node-OCR	replicated	

Send to all nodes

Related topics:

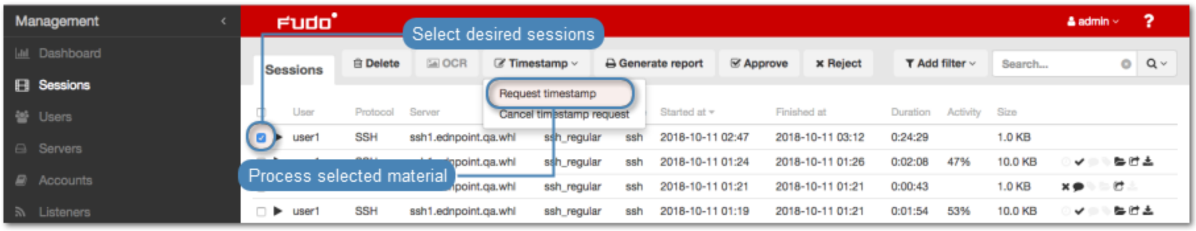
- *Cluster configuration*
- *Sessions*

12.13 Timestamping selected sessions

To timestamp selected sessions, proceed as follows.

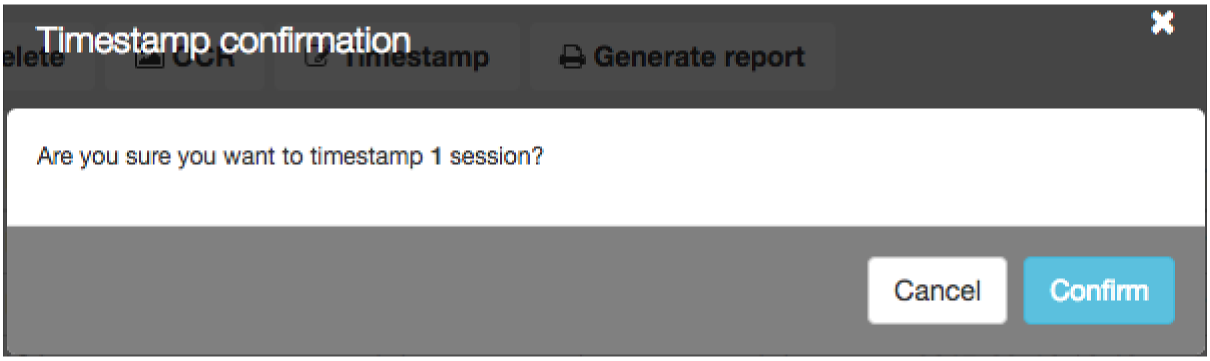
1. Select *Management* > *Sessions*.

2. Select desired sessions, *Timestamp* and select *Request timestamp*.



	User	Protocol	Server			Started at	Finished at	Duration	Activity	Size
☑	user1	SSH	ssh1.ednpoint.qa.whl	ssh_regular	ssh	2018-10-11 02:47	2018-10-11 03:12	0:24:29		1.0 KB
			point.qa.whl	ssh_regular	ssh	2018-10-11 01:24	2018-10-11 01:26	0:02:08	47%	10.0 KB
			point.qa.whl	ssh_regular	ssh	2018-10-11 01:21	2018-10-11 01:21	0:00:43		1.0 KB
□	user1	SSH	ssh1.ednpoint.qa.whl	ssh_regular	ssh	2018-10-11 01:19	2018-10-11 01:21	0:01:54	53%	10.0 KB

3. Click *Confirm*.



Timestamp confirmation

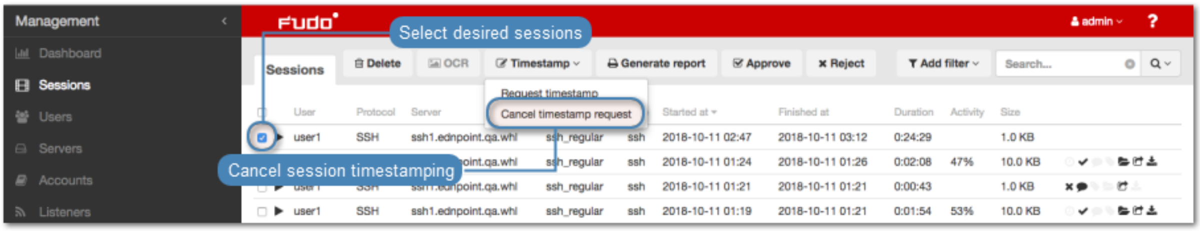
Are you sure you want to timestamp 1 session?

Note: Click the ⏲ to view the timestamp data.

12.14 Cancelling sessions timestamping

To cancel sessions timestamping, proceed as follows.

1. Select *Management > Sessions*.
2. Select desired sessions, *Timestamp* and select *Cancel timestamp request*.



	User	Protocol	Server			Started at	Finished at	Duration	Activity	Size
☑	user1	SSH	ssh1.ednpoint.qa.whl	ssh_regular	ssh	2018-10-11 02:47	2018-10-11 03:12	0:24:29		1.0 KB
			oint.qa.whl	ssh_regular	ssh	2018-10-11 01:24	2018-10-11 01:26	0:02:08	47%	10.0 KB
			point.qa.whl	ssh_regular	ssh	2018-10-11 01:21	2018-10-11 01:21	0:00:43		1.0 KB
□	user1	SSH	ssh1.ednpoint.qa.whl	ssh_regular	ssh	2018-10-11 01:19	2018-10-11 01:21	0:01:54	53%	10.0 KB

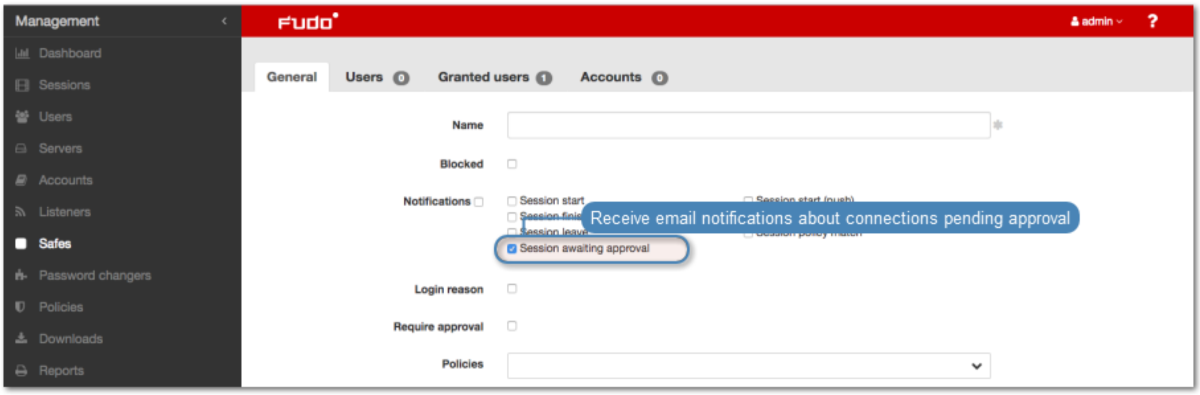
3. Click *Confirm*.

Related topics:

- *Filtering sessions*
- *Accounts*

12.15 Approving pending user requests

Note: To receive email notifications about pending sessions, select *Session awaiting approval* notification in safe configuration.



Name

Blocked □

Notifications □ □ Session start □ Session start (push) □ Session finis... □ Session leave... □ Session policy match ☑ Session awaiting approval

Receive email notifications about connections pending approval

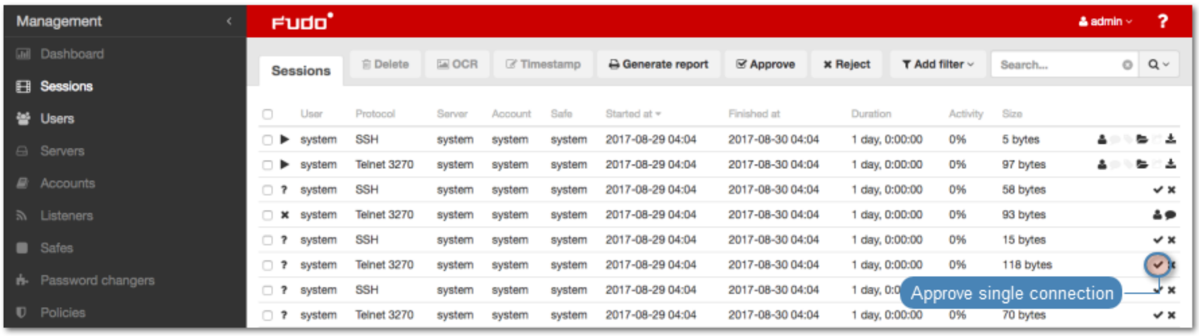
Login reason □

Require approval □

Policies

12.15.1 Fudo management interface

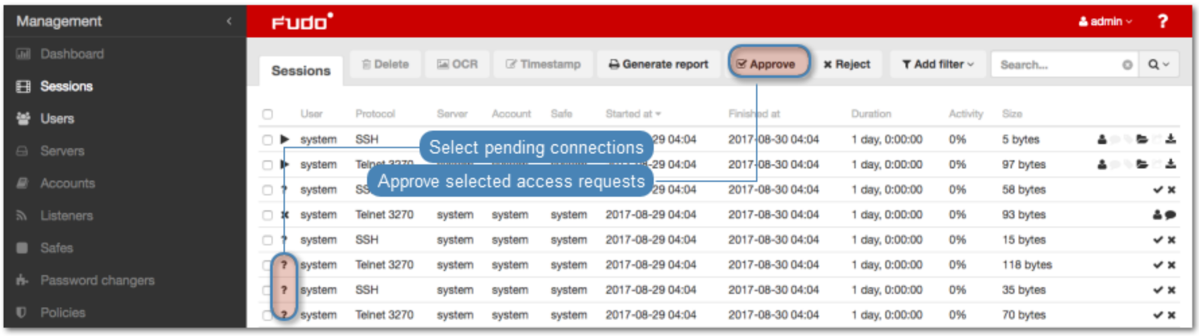
1. Select *Management* > *Sessions*.
2. Click ✔ in a specific row



□		User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size	
□	▶	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	5 bytes	
□	▶	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	97 bytes	
□	?	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	58 bytes	✔ ✖
□	✖	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	93 bytes	
□	?	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	15 bytes	✔ ✖
□	?	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	118 bytes	✔ ✖
□	?	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:0			✔ ✖
□	?	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	70 bytes	✔ ✖

Approve single connection

or select desired pending request and click *Approve*.



□		User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size	
□	▶	system	SSH				29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	5 bytes	
□	▶	system					-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	97 bytes	
□	?	system	SS				29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	58 bytes	✔ ✖
□	✖	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	93 bytes	
□	?	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	15 bytes	✔ ✖
□	?	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	118 bytes	✔ ✖
□	?	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	35 bytes	✔ ✖
□	?	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	70 bytes	✔ ✖

Select pending connections

Approve selected access requests

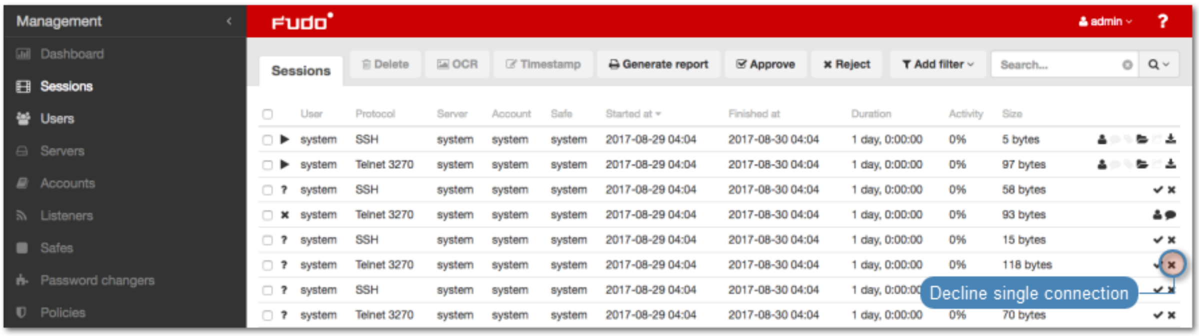
Related topics:

- *User authentication methods and modes*
- *Declining pending requests*
- *Sessions*

12.16 Declining pending requests

12.16.1 Fudo administration interface

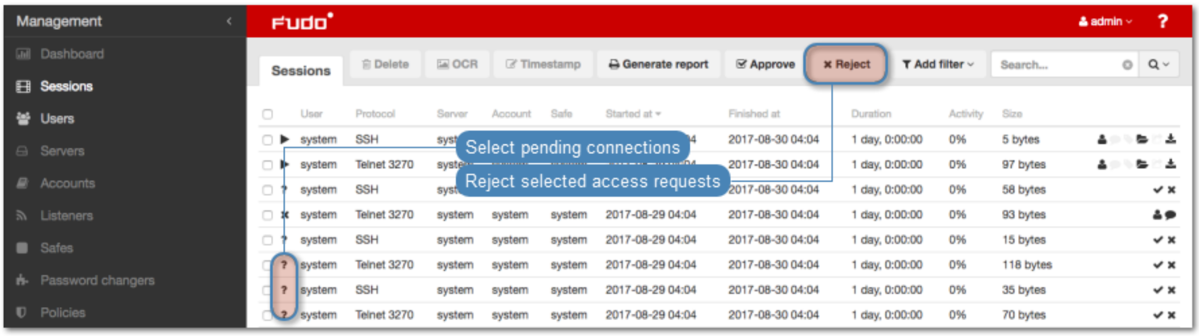
1. Select *Management* > *Sessions*.
2. Click ✖ in a specific row



	User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
▶	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	5 bytes
▶	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	97 bytes
?	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	58 bytes
✖	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	93 bytes
?	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	15 bytes
?	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	118 bytes
?	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:0		
?	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	70 bytes

Decline single connection

or select pending sessions and click *Reject*.



	User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
▶	system	SSH	syst			4	2017-08-30 04:04	1 day, 0:00:00	0%	5 bytes
▶	system	Telnet 3270	syste				2017-08-30 04:04	1 day, 0:00:00	0%	97 bytes
?	system	SSH	syst				2017-08-30 04:04	1 day, 0:00:00	0%	58 bytes
✖	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	93 bytes
?	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	15 bytes
?	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	118 bytes
?	system	SSH	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	35 bytes
?	system	Telnet 3270	system	system	system	2017-08-29 04:04	2017-08-30 04:04	1 day, 0:00:00	0%	70 bytes

Select pending connections

Reject selected access requests

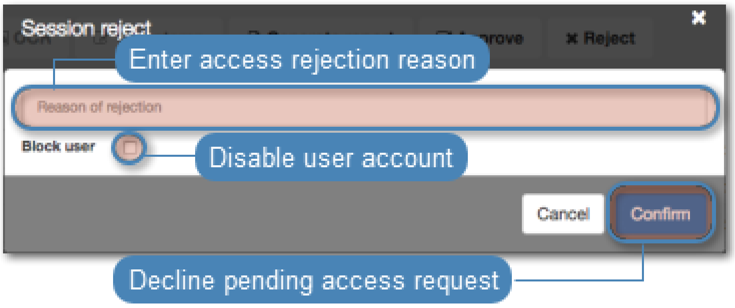
3. Optionally, enter the reason for rejecting given request.

Note: Rejection reason is displayed on the session list after positioning cursor over the 💬 icon.

4. Optionally, select the option to block the user.

Note: User blocking reason will be the same as the entered session rejection reason.

5. Click *Confirm*.



Enter access rejection reason

Disable user account

Decline pending access request

Related topics:

- *User authentication methods and modes*
- *Approving pending user requests*
- *Terminating connection*
- *Blocking a user*
- *Sessions*

12.17 AI sessions processing

Note: *This is an evaluation version of the AI component.*

Fudo PAM is able to detect changes in user behavior and determine if user credentials have been compromised. It can also alert system administrator if there is an unusually high number of connections or a particular session is longer than expected.

12.17.1 Content models

Content models process and analyze RDP and SSH sessions in order to build behavioral user profiles. Based on these, Fudo PAM can detect even the slightest change in user behavior and help prevent a security breach.

RDP content model

The RDP model is based on mouse cursor movements.

The following requirements must be met in order to produce an RDP model:

Minimum:

- 5 hours of sessions recordings per predictor,
- 5 unique predictors (e.g. users).

Optimal:

- 30 hours of sessions recordings,
- 10 unique predictors.

Note: RDP model's quality depends on the consistency of how the user interacts with the monitored system. If the user has used different operating systems and input devices (e.g. different mice, a trackpad or a trackball) the resulting model will not be very effective as it will have a higher tolerance for a variety of behaviors.

SSH content model

The SSH content model is based on the keyboard input (commands).

The following requirements must be met in order to produce an SSH model:

Minimum:

- 65 sessions recorded (25 unique commands minimum),
- 5 unique predictors (e.g. users).

Optimal:

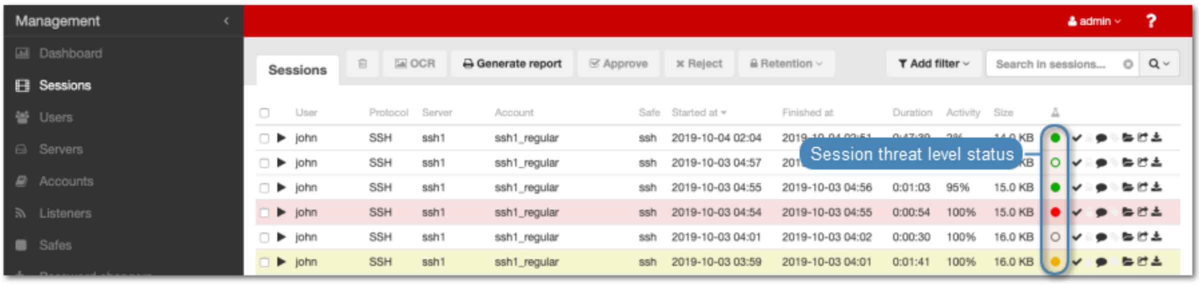
- 300 sessions recorded per predictor,
- 10 unique predictors (e.g. users).

12.17.2 Session scoring

Fudo PAM analyzes sessions in real-time and produces threat level scores (OK, LOW, HIGH) depending on how the user fares against the trained model.

Note: Sessions are processed in chunks containing a specific number of events. Processing is done in real-time as long as there are workers available. When there are no workers available, ongoing sessions' parts are not analyzed.

Models are calibrated individually and session scores are presented on the *session list*.



□		User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size	
□	▶	john	SSH	ssh1	ssh1_regular	ssh	2019-10-04 02:04	2019-10-04 02:51	0:47:30	3%	14.0 KB	🟢
□	▶	john	SSH	ssh1	ssh1_regular	ssh	2019-10-03 04:57	201[illegible]	[illegible]	[illegible]	[illegible]KB	○
□	▶	john	SSH	ssh1	ssh1_regular	ssh	2019-10-03 04:55	2019-10-03 04:56	0:01:03	95%	15.0 KB	🟢
□	▶	john	SSH	ssh1	ssh1_regular	ssh	2019-10-03 04:54	2019-10-03 04:55	0:00:54	100%	15.0 KB	🔴
□	▶	john	SSH	ssh1	ssh1_regular	ssh	2019-10-03 04:01	2019-10-03 04:02	0:00:30	100%	16.0 KB	○
□	▶	john	SSH	ssh1	ssh1_regular	ssh	2019-10-03 03:59	2019-10-03 04:01	0:01:41	100%	16.0 KB	🟡

Icon	Description
○	Session under analysis, initial result - no threat.
○	Session under analysis, initial result - medium threat level.
○	Session under analysis, initial result - high threat level.
○	Session awaiting analysis or being initially processed.
○	Session not analyzed due to missing a trained model.
🟢	Session processed - no risk.
🟡	Session processed - medium threat level.
🔴	Session processed - high threat level.
⚫	Session processed - no result.

Note: When it comes to building user models, data quality is essential. If users shared login credentials, the resulting model will be less likely to detect the variance in user behavior.

12.17.3 Quantitive models

Fudo keeps track of the number of sessions as well as their length. It can alert system administrator if there's an unusually high number of connections or a particular session is suspiciously long.

It does so by learning typical values for each user, account and server and making predictions for every hour and weekday.

Related topics:

- *Artificial Intelligence*
- *Sessions*
- *Frequently asked questions*

CHAPTER 13

Reports

Reporting service generates detailed statistics of users access sessions.

Full reports are generated periodically (daily, weekly, monthly, quarterly, annually) by the system and can be accessed by users with the `superadmin` role assigned to them. 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 pre-defined reports, periodic 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 sessions.

Predefined reports

Account access report	This report contains accounts and corresponding servers and safes which have been accessed in the given time period.
Safe access report	This report contains safes and the corresponding servers accessed in the given time period.
Server access report	This report contains servers accessed in the specified time period in combination with safes and accounts.
Session approvals by user	This report contains approved 4-Eyes sessions.
Session sharing invites by user	This report contains shared sessions.
Session summary	This report provides information on sessions recorded in the given time period.
Sessions by server report	This report provides a list of recorded sessions and the server details for the given time period.
User access report	This report contains users in combination with servers they have accessed in the specified time period along with safes, listeners and accounts that were used to access these servers.
User activity report	This report shows data about user and his actions in administration panel - creating, removing and changing data for objects.
User privilege report	This report contains users and objects that they are allowed to edit.
User report	This report contains users along with their role, status, creation date, recent login and the entity that has created the given user instance.

Subscribing to a periodic report

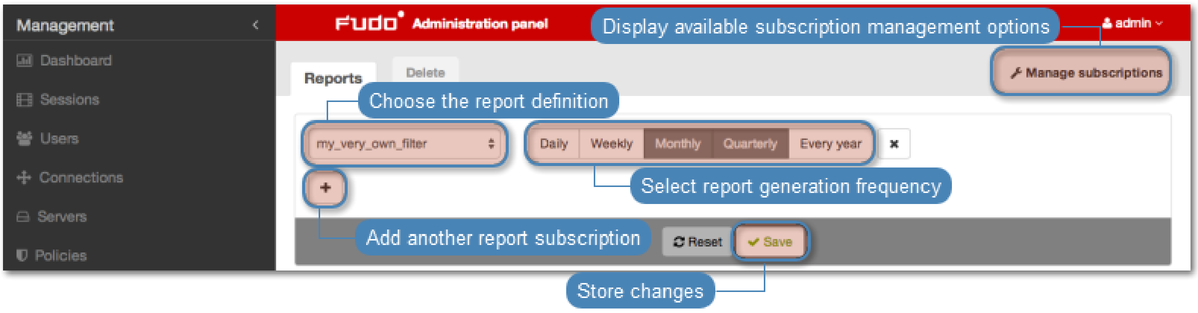
Subscribing cause sending the reports via e-mail, so remember to configure your SMTP server as described on a *Notifications* page. To enable automatic periodic report generation for the logged in user, proceed as follows.

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 pre-defined options and user defined *filtering definitions*.

4. Choose how often the given report should be generated.
5. Click *Save*.



Display available subscription management options

Choose the report definition

Select report generation frequency

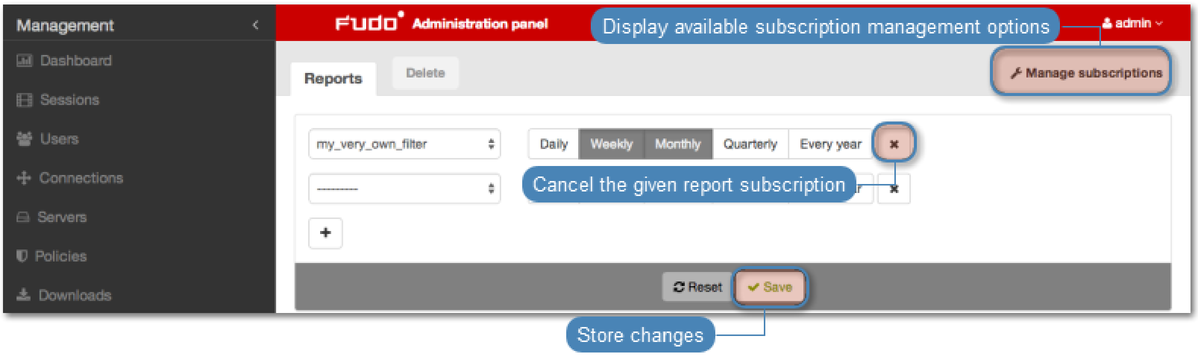
Add another report subscription

Store changes

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*.



Display available subscription management options

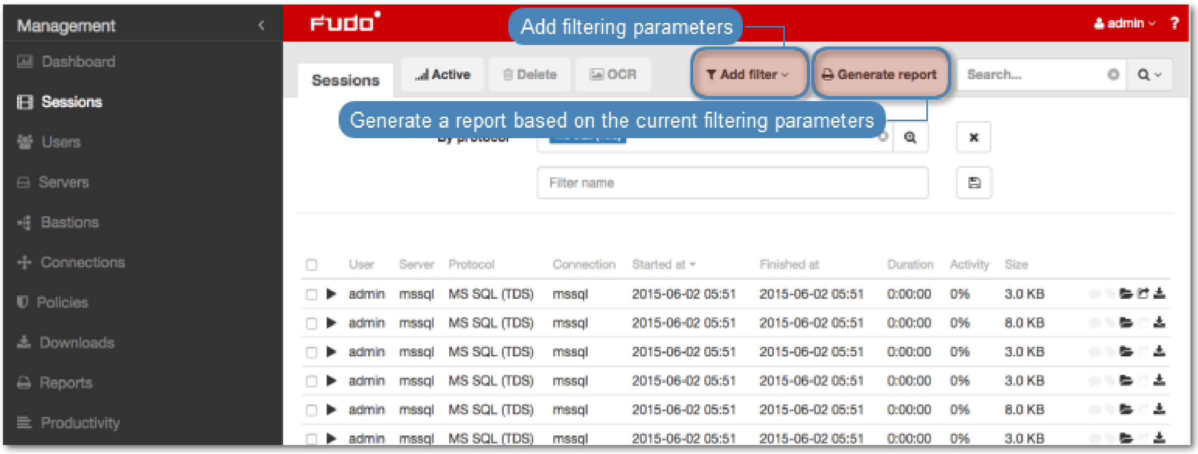
Cancel the given report subscription

Store changes

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.

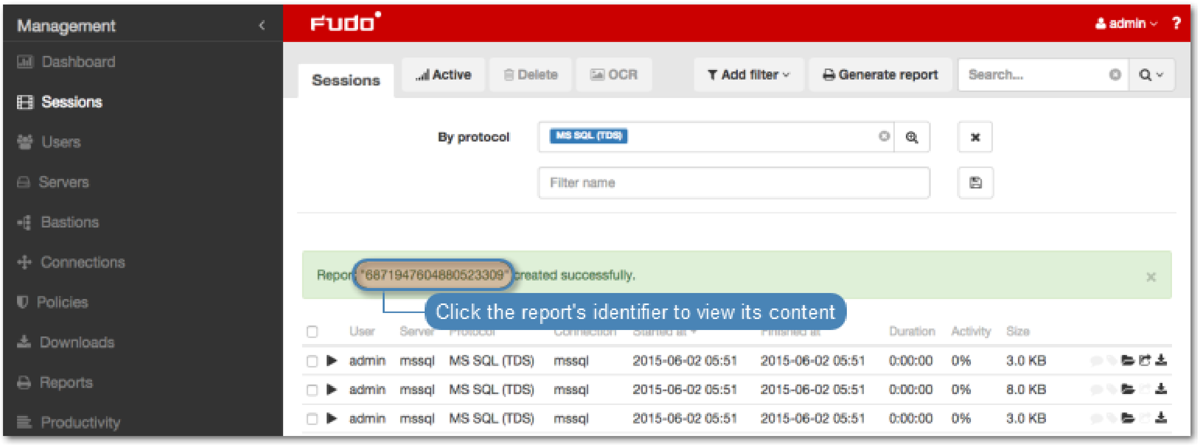


Add filtering parameters

Generate a report based on the current filtering parameters

	User	Server	Protocol	Connection	Started at	Finished at	Duration	Activity	Size
□ ▶	admin	mssql	MS SQL (TDS)	mssql	2015-06-02 05:51	2015-06-02 05:51	0:00:00	0%	3.0 KB
□ ▶	admin	mssql	MS SQL (TDS)	mssql	2015-06-02 05:51	2015-06-02 05:51	0:00:00	0%	8.0 KB
□ ▶	admin	mssql	MS SQL (TDS)	mssql	2015-06-02 05:51	2015-06-02 05:51	0:00:00	0%	3.0 KB
□ ▶	admin	mssql	MS SQL (TDS)	mssql	2015-06-02 05:51	2015-06-02 05:51	0:00:00	0%	3.0 KB
□ ▶	admin	mssql	MS SQL (TDS)	mssql	2015-06-02 05:51	2015-06-02 05:51	0:00:00	0%	8.0 KB
□ ▶	admin	mssql	MS SQL (TDS)	mssql	2015-06-02 05:51	2015-06-02 05:51	0:00:00	0%	3.0 KB

4. Note your report’s identifier or click it to display the report.



Report "6871947604880523309" created successfully.

	User	Server	Protocol	Connection	Started at	Finished at	Duration	Activity	Size
▶	admin	mssql	MS SQL (TDS)	mssql	2015-06-02 05:51	2015-06-02 05:51	0:00:00	0%	3.0 KB
▶	admin	mssql	MS SQL (TDS)	mssql	2015-06-02 05:51	2015-06-02 05:51	0:00:00	0%	8.0 KB
▶	admin	mssql	MS SQL (TDS)	mssql	2015-06-02 05:51	2015-06-02 05:51	0:00:00	0%	3.0 KB

5. Select *Management* > *Reports*.

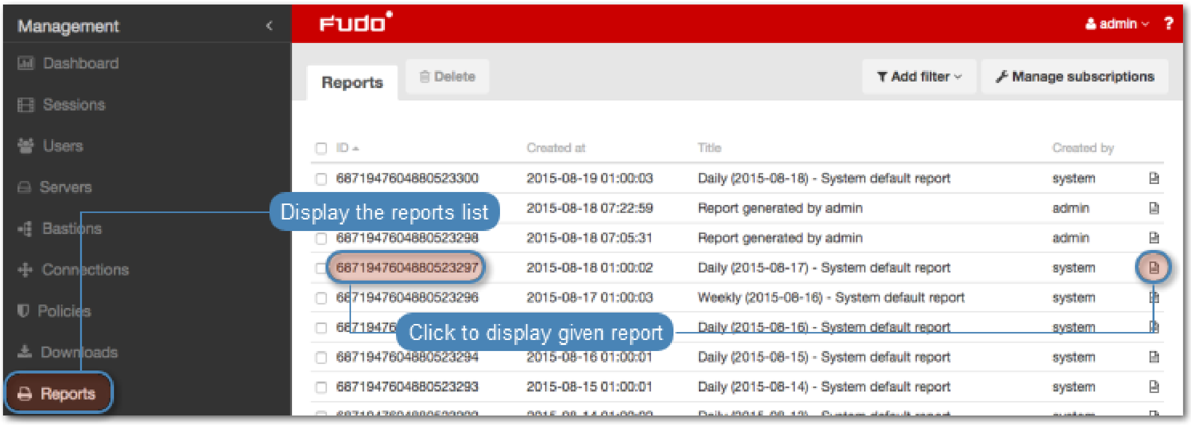
6. Find desired report and click the view icon.

7. Click the corresponding button to save the report in selected format.

Opening and downloading reports

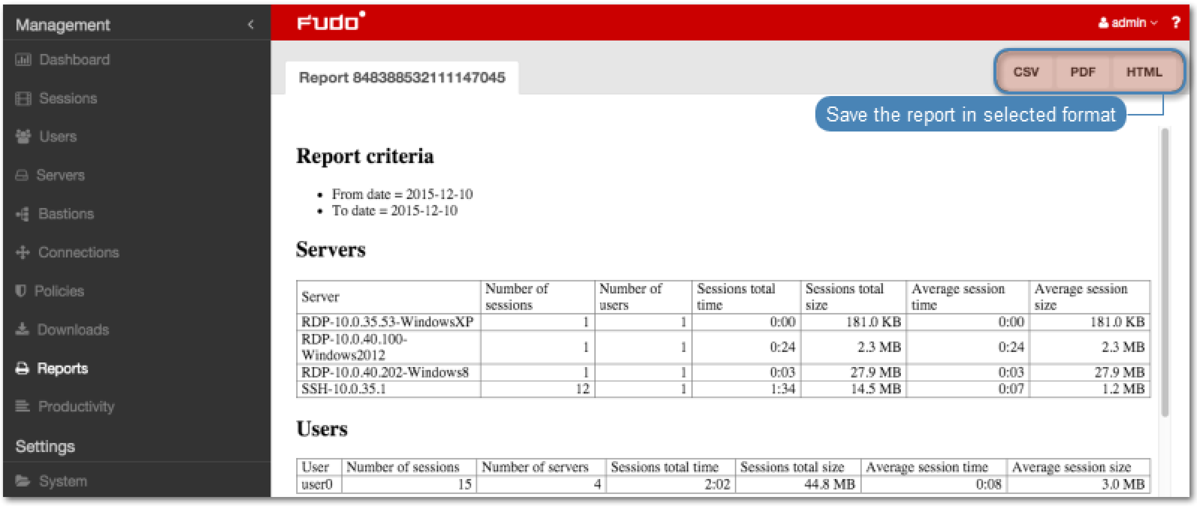
1. Select *Management* > *Reports*.

2. Find desired report and click the view icon.



ID	Created at	Title	Created by
6871947604880523300	2015-08-19 01:00:03	Daily (2015-08-18) - System default report	system
	2015-08-18 07:22:59	Report generated by admin	admin
6871947604880523298	2015-08-18 07:05:31	Report generated by admin	admin
6871947604880523297	2015-08-18 01:00:02	Daily (2015-08-17) - System default report	system
6871947604880523296	2015-08-17 01:00:03	Weekly (2015-08-16) - System default report	system
6871947		Daily (2015-08-16) - System default report	system
6871947604880523294	2015-08-16 01:00:01	Daily (2015-08-15) - System default report	system
6871947604880523293	2015-08-15 01:00:01	Daily (2015-08-14) - System default report	system

3. Click the corresponding button to save the report in selected format.



Report 848388532111147045

Save the report in selected format

Report criteria

- From date = 2015-12-10
- To date = 2015-12-10

Servers

Server	Number of sessions	Number of users	Sessions total time	Sessions total size	Average session time	Average session size
RDP-10.0.35.53-WindowsXP	1	1	0:00	181.0 KB	0:00	181.0 KB
RDP-10.0.40.100-Windows2012	1	1	0:24	2.3 MB	0:24	2.3 MB
RDP-10.0.40.202-Windows8	1	1	0:03	27.9 MB	0:03	27.9 MB
SSH-10.0.35.1	12	1	1:34	14.5 MB	0:07	1.2 MB

Users

User	Number of sessions	Number of servers	Sessions total time	Sessions total size	Average session time	Average session size
user0	15	4	2:02	44.8 MB	0:08	3.0 MB

Deleting reports

1. Select *Management* > *Reports*.
2. Find, select desired reports and click *Delete*.
3. Confirm deleting selected reports.

Related topics:

- *Notifications*
- *Filtering sessions*

CHAPTER 14

Efficiency analyzer

Fudo PAM features a productivity analysis component which tracks users' activities and can provide precise information on activity and idle times.

14.1 Overview

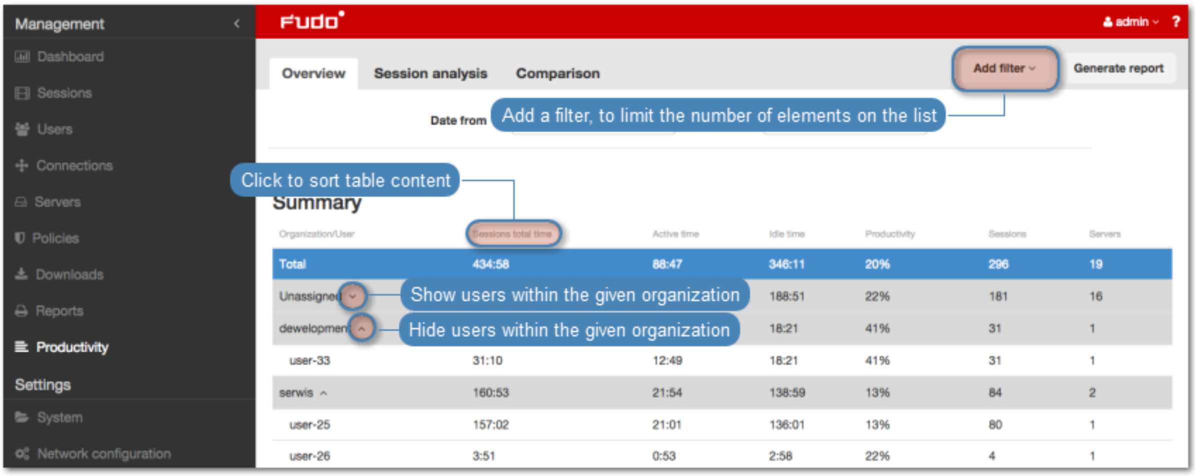
Overview displays data on users' activity in selected time interval.

Note: Activity rating is based on the user's interaction with the monitored system. 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.



Add a filter, to limit the number of elements on the list

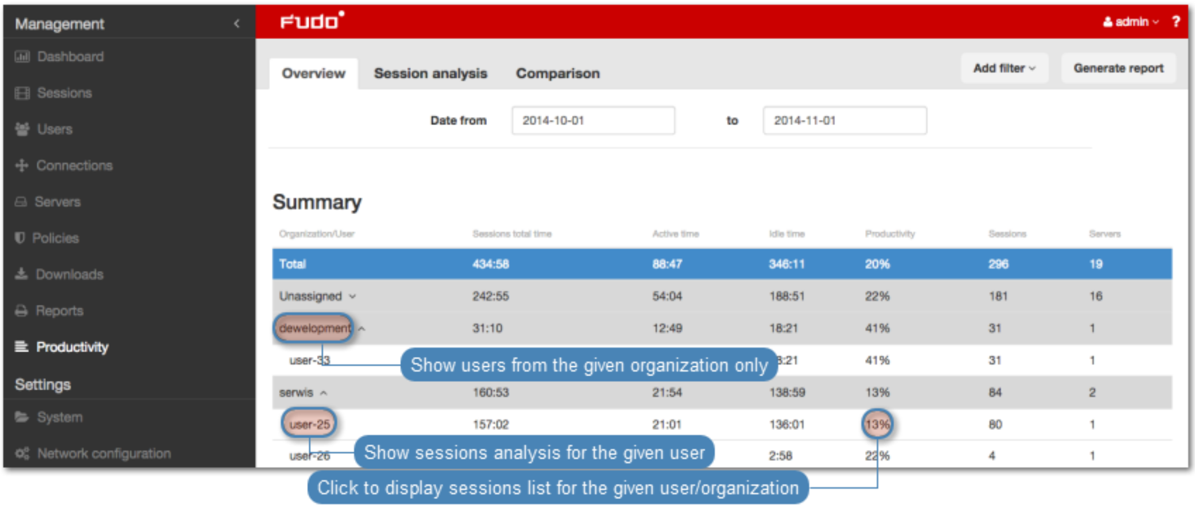
Click to sort table content

Summary

Organization/User	Sessions total time	Active time	Idle time	Productivity	Sessions	Servers
Total	434:58	88:47	346:11	20%	296	19
Unassigne			188:51	22%	181	16
developmen			18:21	41%	31	1
user-33	31:10	12:49	18:21	41%	31	1
serwis	160:53	21:54	138:59	13%	84	2
user-25	157:02	21:01	136:01	13%	80	1
user-26	3:51	0:53	2:58	22%	4	1

Show users within the given organization

Hide users within the given organization



Date from 2014-10-01 to 2014-11-01

Summary

Organization/User	Sessions total time	Active time	Idle time	Productivity	Sessions	Servers
Total	434:58	88:47	346:11	20%	296	19
Unassigned	242:55	54:04	188:51	22%	181	16
dewelopment	31:10	12:49	18:21	41%	31	1
user-33			:21	41%	31	1
serwis	160:53	21:54	138:59	13%	84	2
user-25	157:02	21:01	136:01	13%	80	1
user-26			2:58	22%	4	1

Show users from the given organization only

Show sessions analysis for the given user

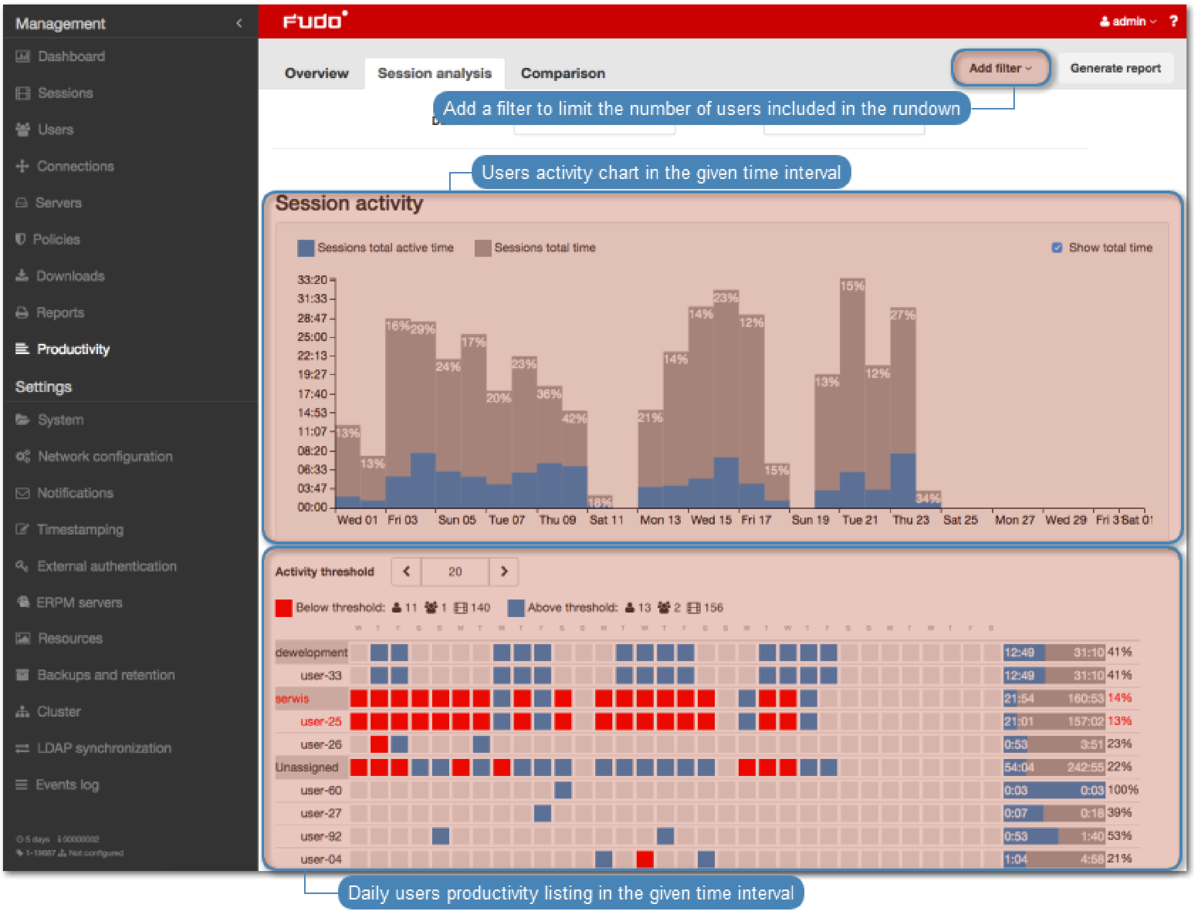
Click to display sessions list for the given user/organization

Related topics:

- *Productivity analysis - Sessions analysis*
- *Productivity analysis - Comparison*
- *Sessions*

14.2 Sessions analysis

Sessions analysis shows in detail users/organizations productivity in the given time period. The activity threshold parameter allows identifying sessions, users and organisations which do not exceed the required user activity rating and helps establishing the threshold value attainable for a given number of users or sessions.



dewelopment	12:49	31:10	41%
user-33	12:49	31:10	41%
serwis	21:54	160:53	14%
user-25	21:01	157:02	13%
user-26	0:53	3:51	23%
Unassigned	54:04	242:55	22%
user-60	0:03	0:03	100%
user-27	0:07	0:18	39%
user-92	0:53	1:40	53%
user-04	1:04	4:58	21%

Add a filter to limit the number of users included in the rundown

Users activity chart in the given time interval

Daily users productivity listing in the given time interval

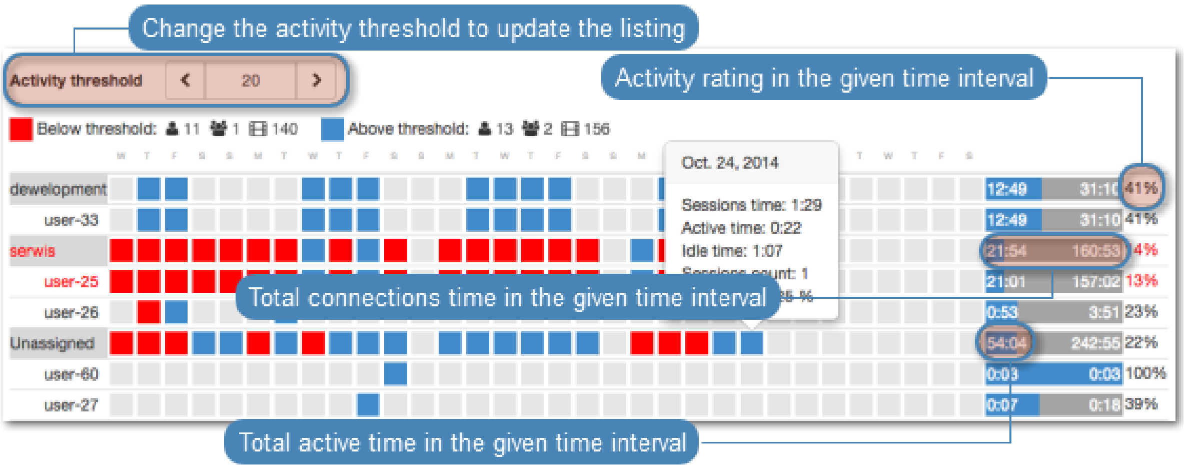
Users activity rating

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.

Change the activity threshold to update the listing

Activity rating in the given time interval



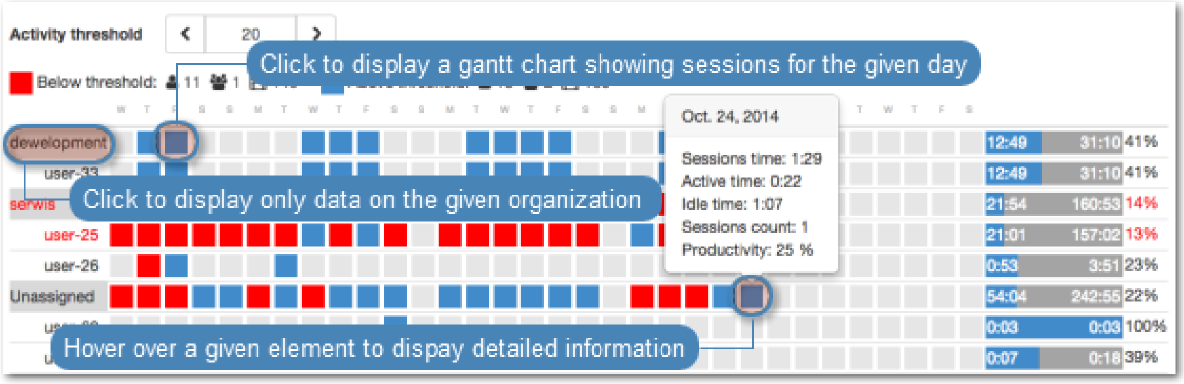
Oct. 24, 2014

Sessions time: 1:29
Active time: 0:22
Idle time: 1:07
Sessions count: 1

dewelopment	12:49	31:10	41%
user-33	12:49	31:10	41%
serwis	21:54	160:53	14%
user-25	21:01	157:02	13%
user-26	0:53	3:51	23%
Unassigned	54:04	242:55	22%
user-60	0:03	0:03	100%
user-27	0:07	0:18	39%

Total connections time in the given time interval

Total active time in the given time interval



Click to display a gantt chart showing sessions for the given day

Oct. 24, 2014

Sessions time: 1:29
Active time: 0:22
Idle time: 1:07
Sessions count: 1
Productivity: 25 %

Click to display only data on the given organization

Hover over a given element to dispay detailed information

Related topics:

- *Productivity analysis - Overview*
- *Productivity analysis - Comparison*

14.3 Activity comparison

Efficiency analyzer module enables comparing users/organizations activity in given time periods.

To compare users/organizations, proceed as follows.

1. Select *Management > Productivity*.
2. Select the *Comparison* tab.
3. Select object types being compared.
4. Select the time interval.
5. Add objects to the comparison and define starting date for each object.
6. Click *Confirm* to compare selected objects.

Related topics:

- *Productivity analysis - Sessions analysis*
- *Productivity analysis - Overview*
- *Sessions*

CHAPTER 15

Administration

This section covers Fudo PAM administration topics.

15.1 System

15.1.1 Date and time

System events registered by Fudo PAM (sessions, system log events, etc.) are timestamped. Fudo PAM can obtain the time information either from an NTP server or the system clock.

Warning:

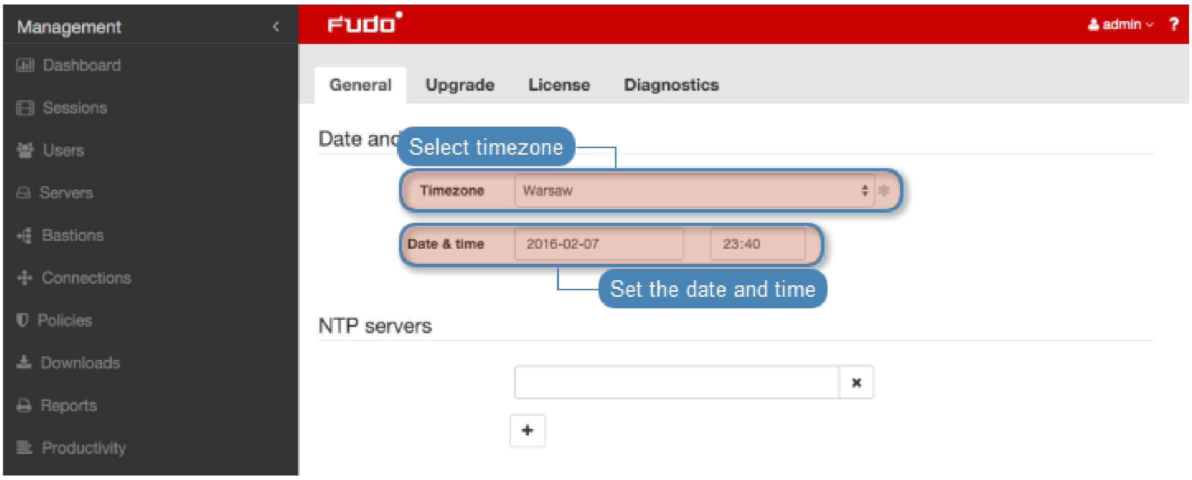
- It is strongly advised for the date and time settings to be obtained from a reliable NTP server. Changing date and time settings manually may result in system malfunction.
- Date and time synchronization with NTP server is required in *cluster configurations*.

Changing date and time settings

Note: Manual time setting is disabled if there are NTP servers configured.

To change the 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.



Select timezone

Timezone: Warsaw

Date & time: 2016-02-07 23:40

Set the date and time

3. Click *Save*.

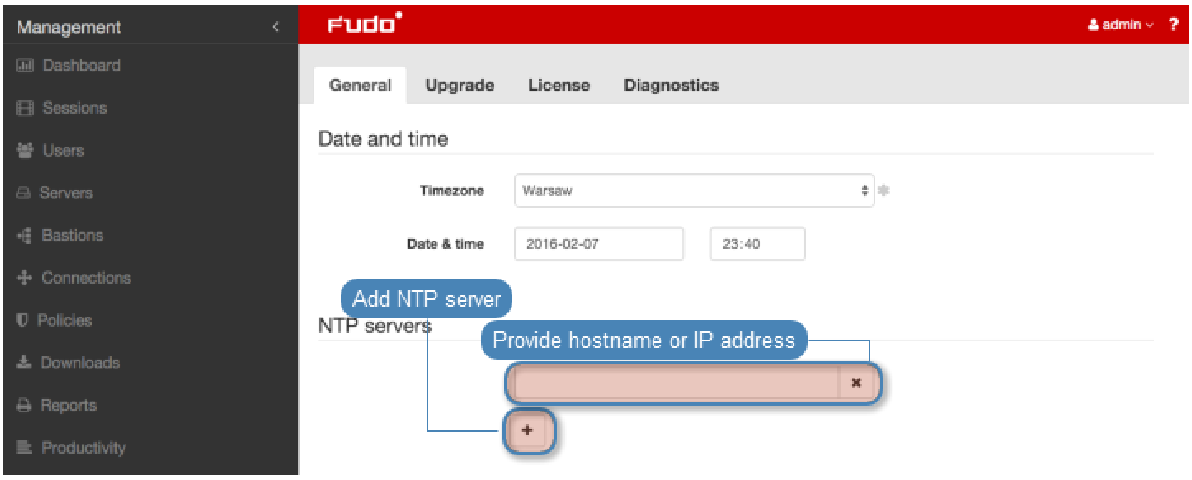
Time servers configuration

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.



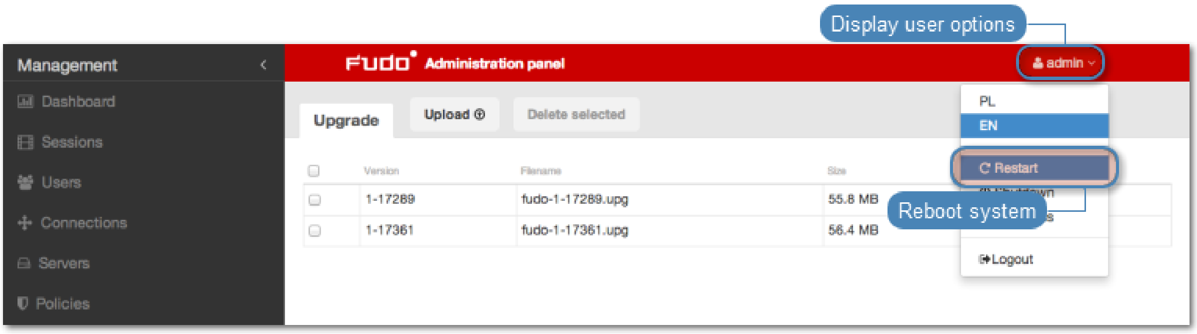
Timezone: Warsaw

Date & time: 2016-02-07 23:40

Add NTP server

Provide hostname or IP address

4. Click *Save*.
5. Select *Restart* from user menu to reboot Fudo PAM and apply new time settings.

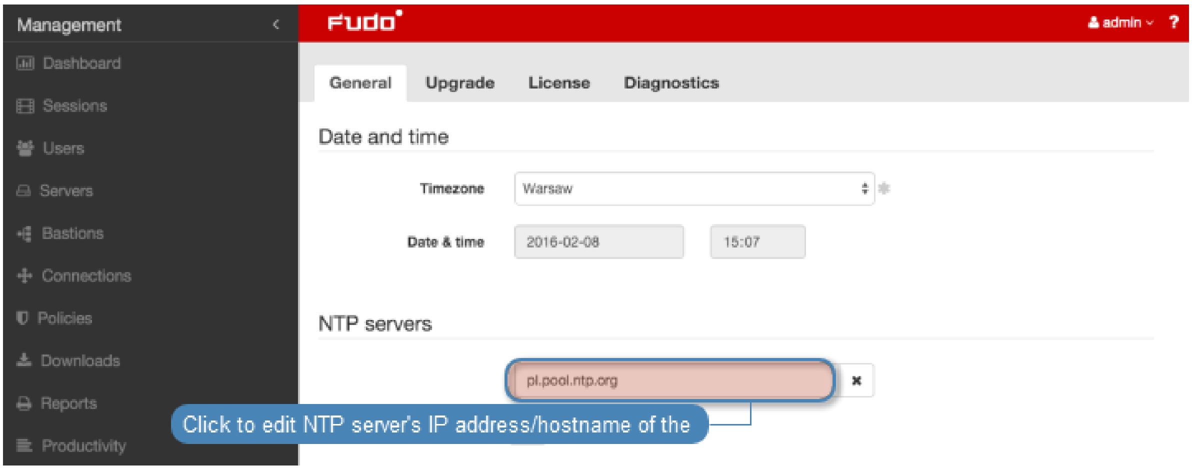


Version	Filename	Size
1-17289	fudo-1-17289.upg	55.8 MB
1-17361	fudo-1-17361.upg	56.4 MB

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.



Date and time

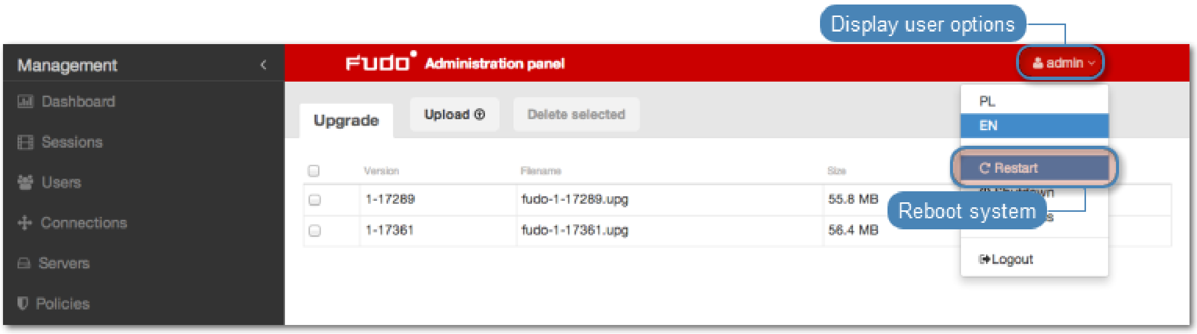
Timezone: Warsaw

Date & time: 2016-02-08 15:07

NTP servers

pl.pool.ntp.org

3. Click *Save*.
4. Select *Restart* from user menu to reboot Fudo PAM and apply new time settings.

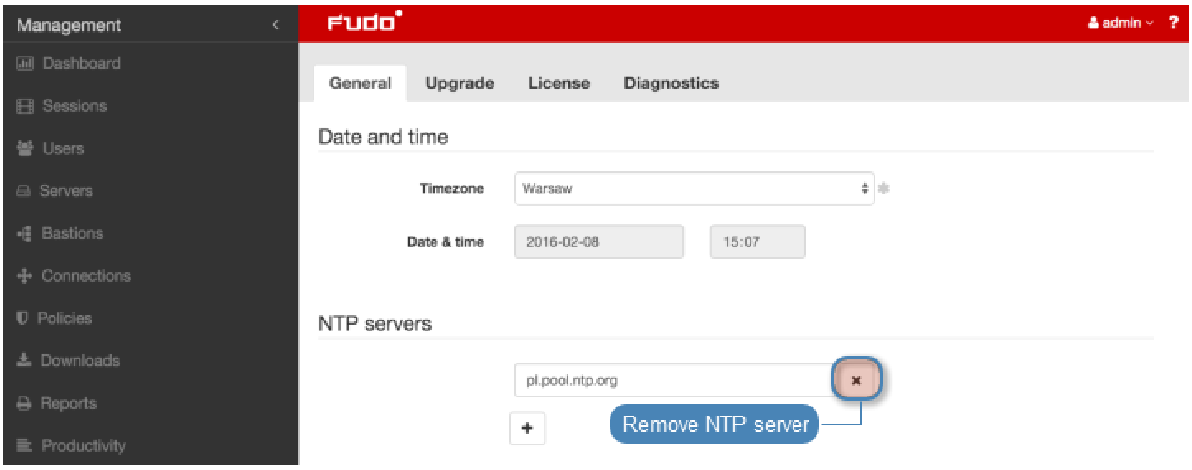


Version	Filename	Size
1-17289	fudo-1-17289.upg	55.8 MB
1-17361	fudo-1-17361.upg	56.4 MB

Deleting an NTP server definition

To remove and NTP server definition, proceed as follows.

1. Select *Settings* > *System*.
2. Find desired NTP server definition in the *NTP servers* section and click the *X* icon.



3. Click *Save*.

Related topics:

- *Timestamping*

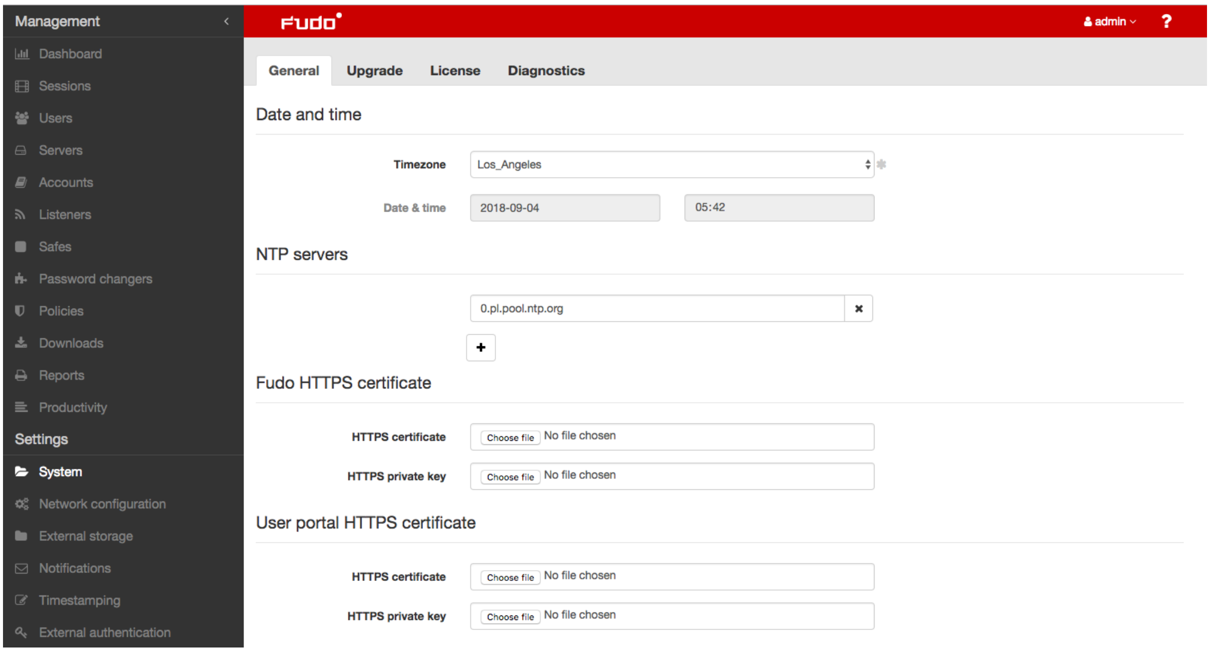
15.1.2 SSL certificates

SSL certificate allows prevent phishing attacks.

Note: Fudo requires using unencrypted keys to the certificate. In this case a user is not obligated to input its password at every restart. Check how to decrypt a password protected RSA private key.

Configuring SSL certificate for Fudo administration panel

1. Select *Settings > System*.
2. In the *Fudo HTTPS certificate* section, click the *Browse* button next to the *HTTPS Certificate* field and point to the location of the SSL certificate file in PEM format.
3. Click the *Browse* button next to the *HTTPS Private Key* field and point to the location of the SSL key definition.



Date and time

Timezone: Los_Angeles

Date & time: 2018-09-04 05:42

NTP servers

0.pl.pool.ntp.org

Fudo HTTPS certificate

HTTPS certificate: Choose file No file chosen

HTTPS private key: Choose file No file chosen

User portal HTTPS certificate

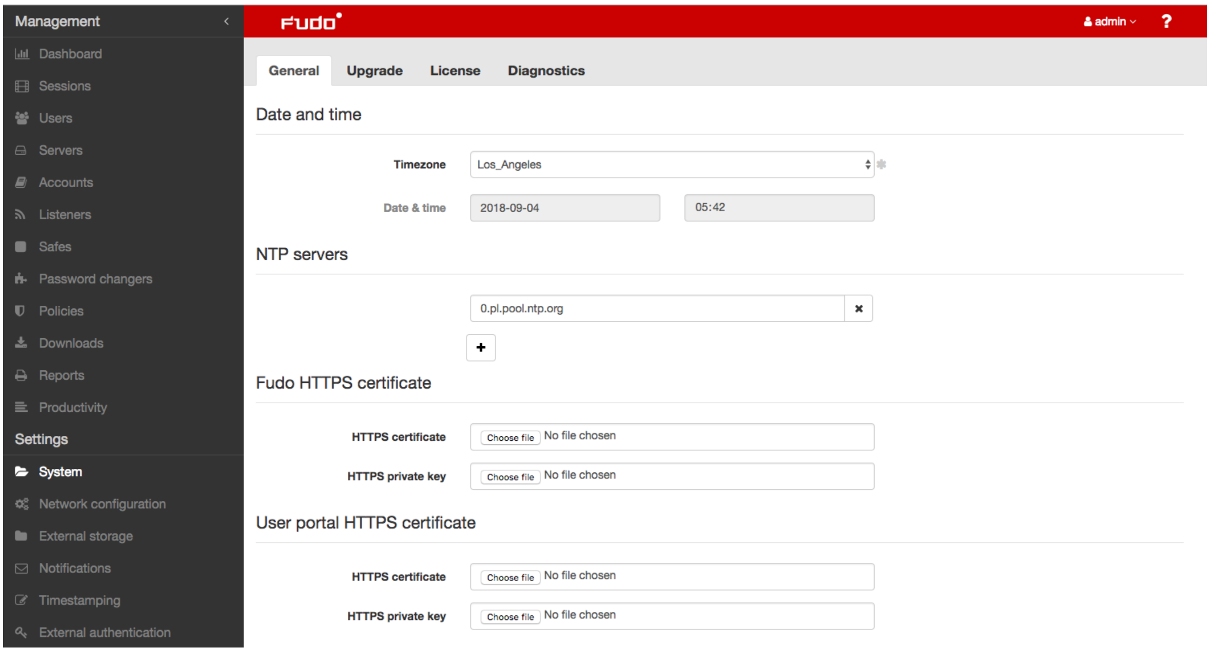
HTTPS certificate: Choose file No file chosen

HTTPS private key: Choose file No file chosen

4. Click *Save*.

Configuring user portal SSL certificate

1. Select *Settings* > *System*.
2. In the *Fudo HTTPS certificate* section, click the *Browse* button next to the *HTTPS Certificate* field in the *HTTPS certificate* section and point to the location of the SSL certificate file in PEM format.
3. Click the *Browse* button next to the *HTTPS Private Key* field and point to the location of the SSL key definition.



Date and time

Timezone: Los_Angeles

Date & time: 2018-09-04 05:42

NTP servers

0.pl.pool.ntp.org

Fudo HTTPS certificate

HTTPS certificate: Choose file No file chosen

HTTPS private key: Choose file No file chosen

User portal HTTPS certificate

HTTPS certificate: Choose file No file chosen

HTTPS private key: Choose file No file chosen

4. Click *Save*.

Related topics:

- *Security measures*

- *Servers*

15.1.3 Deny new connections

Enabling this option results in a denial of all new connections requests.

Blocking new connections

1. Select *Settings* > *System*.
2. Select *Deny new connections* option in the *User authentication and sessions* section.
3. Click *Save* button.

Related topics:

- *Network interfaces configuration*

15.1.4 SSH access

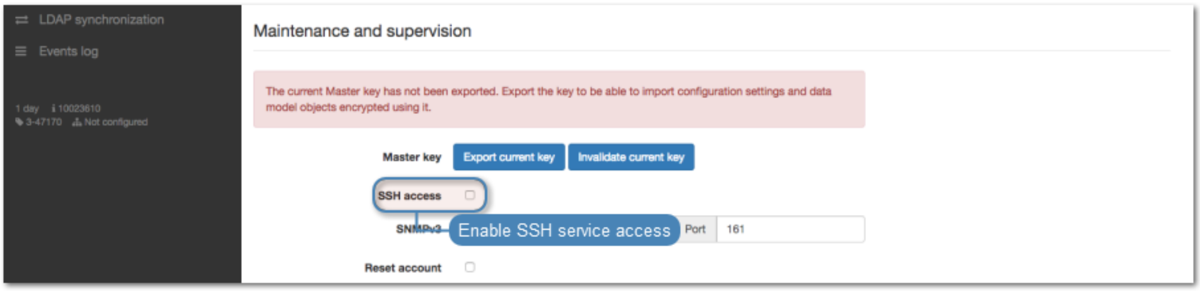
SSH access option enables remote access to Fudo PAM for servicing and maintenance purposes.

Note: The default port number for service access over SSH protocol is 65522.

Enabling SSH access

To enable SSH access, proceed as follows.

1. Select *Settings* > *System*.
2. Select *SSH access* option in the *Maintenance and supervision* section.



The current Master key has not been exported. Export the key to be able to import configuration settings and data model objects encrypted using it.

Master key

SSH access □

SNMPv3 Port 161

Reset account □

3. Click *Save* button.

Related topics:

- *Network interfaces configuration*

15.1.5 Sensitive features

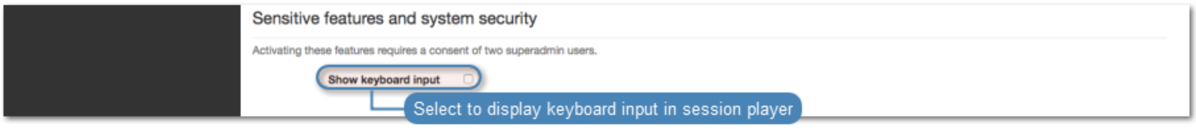
Sensitive features is a set of options enabling which requires a consent from two `superadmin` users.

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*.



Sensitive features and system security

Activating these features requires a consent of two superadmin users.

Show keyboard input □

Select to display keyboard input in session player

4. Notify another system administrator that the keyboard input showing feature has been initiated and requires a confirmation.

Related topics:

- *Viewing sessions*

15.1.6 System update

Note:

- In addition to the current system version, Fudo PAM stores the previous revision, allowing for restoring the system to its previous state. In the event of an unsuccessful system update, Fudo PAM detects the problem during system restart and restarts itself using the previous system revision.
- The system update process does not influence the system configuration or the session data stored on Fudo PAM.
- The storage usage may temporarily increase during system update.

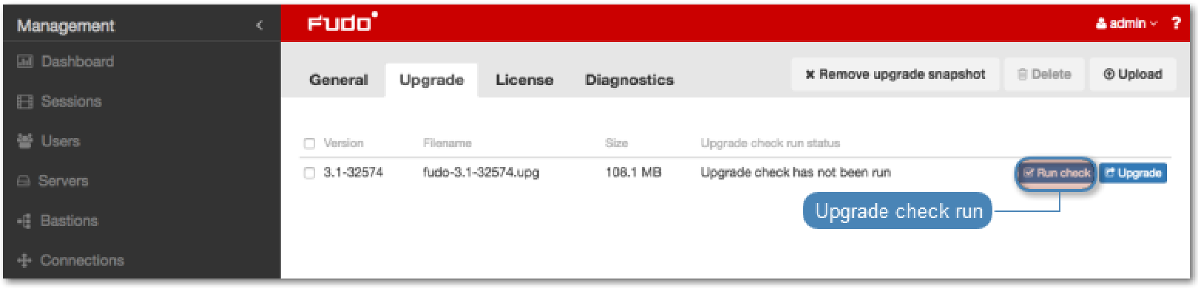
15.1.6.1 Updating system

Warning:

- If the upgrade package requires preparation, it is recommended to wait for the preparation process to finish. This will minimize the system's downtime when performing the actual upgrade.
- Before updating the system it is advised to *run a preliminary check* to ensure that the current system configuration can be successfully upgraded to the new version.
- If the storage usage on the system being updated exceeds 85%, contact Fudo PAM technical support before proceeding with upgrading the system.

- During the system update, all current users' connections will be terminated. Use the *Deny new connections* option in the *Sessions* section of the system settings menu to *limit the number* of active connections before performing system upgrade.
- After running system update, Fudo PAM will restart automatically. Connect the USB flash drive containing the encryption key to the USB port before proceeding or have the passphrase ready in case of virtual machine instance. Note that entering incorrect passphrase will restart the machine in previous revision.
- In case of cluster configuration, upgrade slave node first and after successful upgrade, move onto upgrading the master node.

1. Select *Settings* > *System*.
2. Select the *Upgrade* tab.
3. Click *Upload*.
4. Browse the file system to find and upload the update image file (`.upg`).
5. Optionally, click *Run check* to verify if the current configuration and data model objects are compatible with the new system revision.

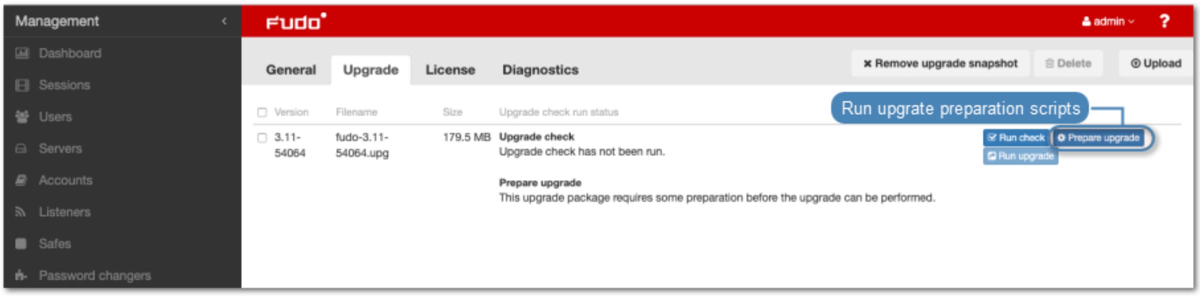


□ Version	Filename	Size	Upgrade check run status
□ 3.1-32574	fudo-3.1-32574.upg	108.1 MB	Upgrade check has not been run

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. If the upgrade requires initial preparation, click *Prepare upgrade*.

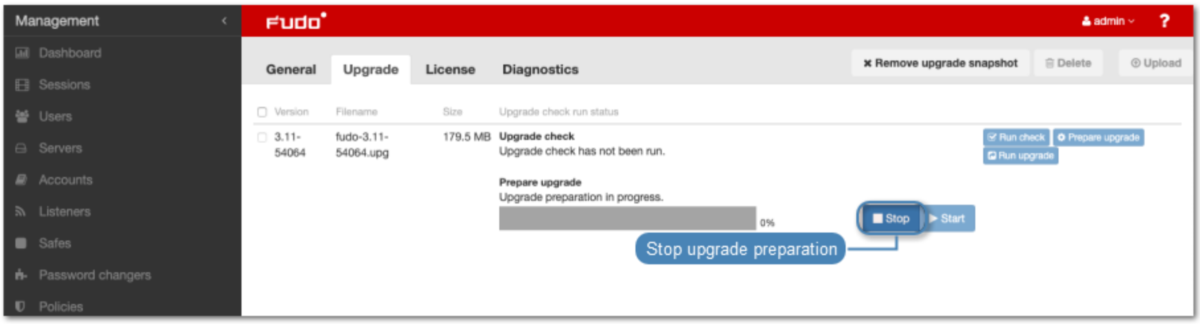


□ Version	Filename	Size	Upgrade check run status
□ 3.11-54064	fudo-3.11-54064.upg	179.5 MB	**Upgrade check** Upgrade check has not been run. **Prepare upgrade** This upgrade package requires some preparation before the upgrade can be performed.

Note:

- Upgrade preparation minimizes the system's downtime when running the actual update.

- Click *Stop* to cancel upgrade preparation. Note that the current preparation stage must complete, thus cancelling might take a while.

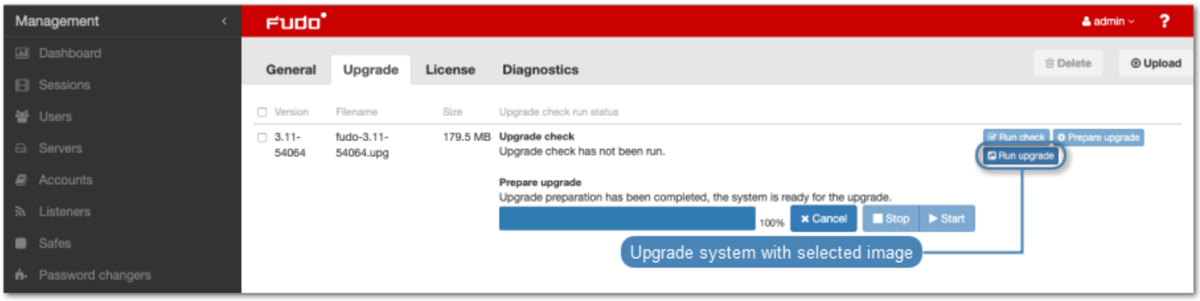


Version	Filename	Size	Upgrade check run status
3.11-54064	fudo-3.11-54064.upg	179.5 MB	**Upgrade check** Upgrade check has not been run. **Prepare upgrade** Upgrade preparation in progress. 0%

- Click *Start* to resume upgrade preparation.

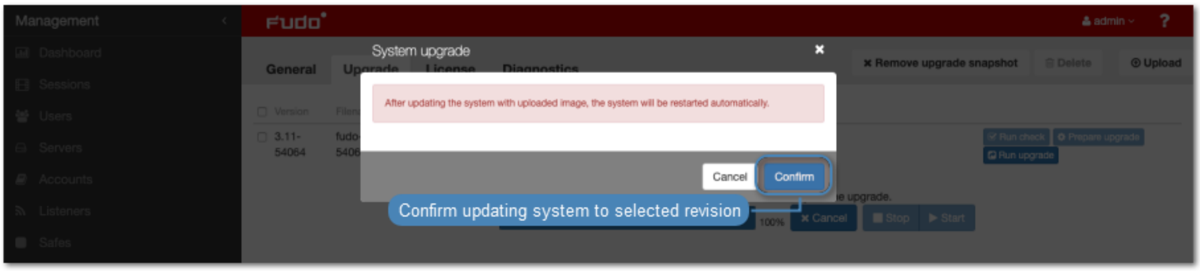
7. Click *Run upgrade*.

Note: In case the upgrade requires preparation, the system upgrade can be performed once the initial preparation stage is completed. Although it is recommended to wait for the preparation process to finish. This will reduce the downtime when running the actual system upgrade.



Version	Filename	Size	Upgrade check run status
3.11-54064	fudo-3.11-54064.upg	179.5 MB	**Upgrade check** Upgrade check has not been run. **Prepare upgrade** Upgrade preparation has been completed, the system is ready for the upgrade. 100%

8. Click *Confirm* to proceed with system update.


System upgrade

After updating the system with uploaded image, the system will be restarted automatically.

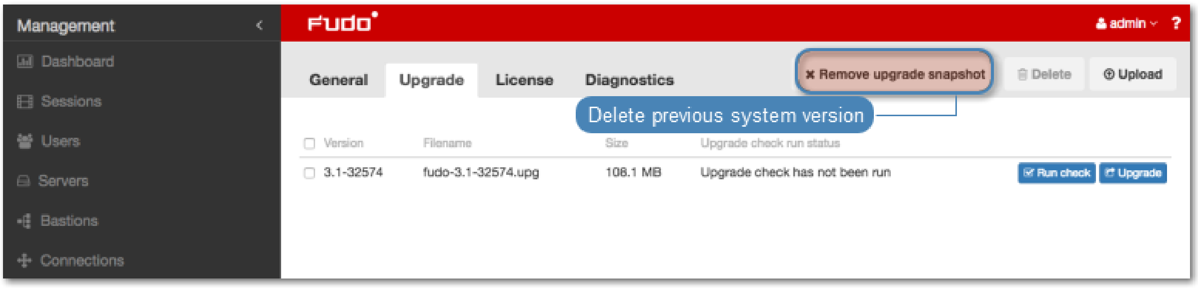
Note: If you *enabled* the *Deny new connections* option before upgrading, make sure to disable it after restarting the system.

15.1.6.2 Deleting upgrade snapshot

Deleting upgrade snapshot will free the storage space occupied by previous system version.

Warning: After deleting the upgrade snapshot it will not be possible to restore the system to previous version.

1. Select *Settings > System*.
2. Select the *Upgrade* tab.
3. Click *Remove upgrade snapshot*.



Delete previous system version

□ Version	Filename	Size	Upgrade check run status
□ 3.1-32574	fudo-3.1-32574.upg	108.1 MB	Upgrade check has not been run

4. Confirm deleting previous system version.

Related topics:

- *System version restore*
- *Restarting system*

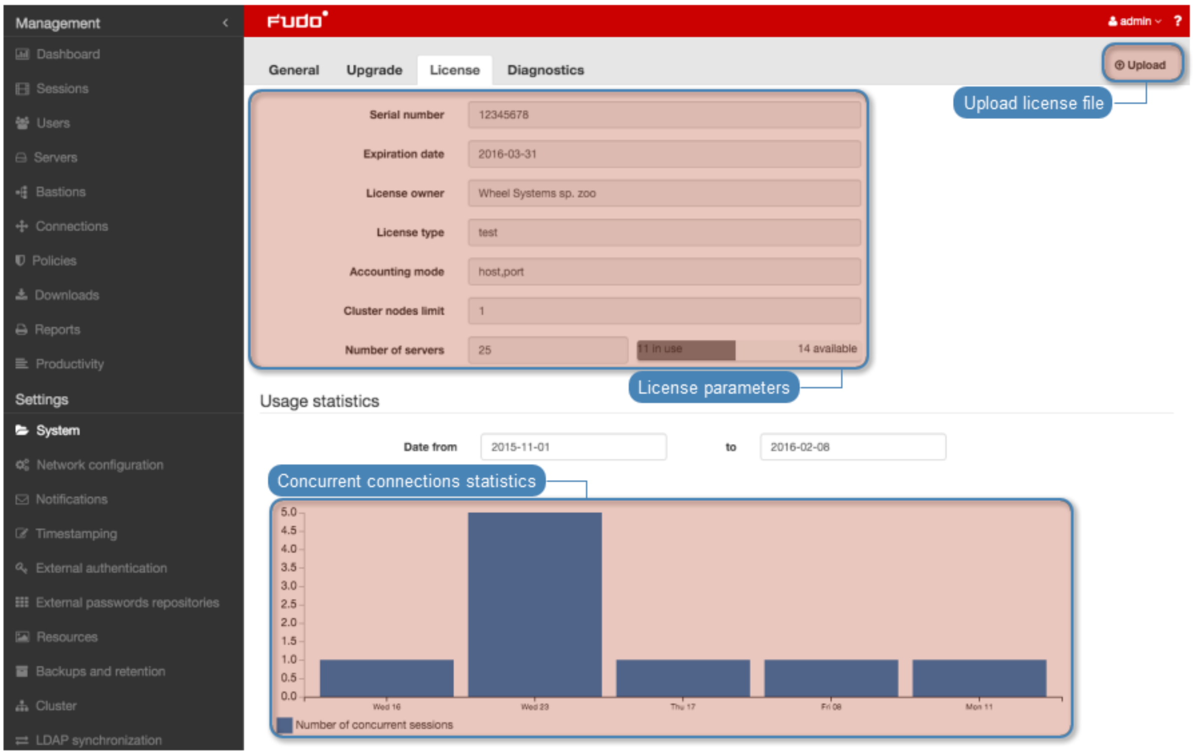
15.1.7 License

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*.



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

Number of servers: 25 (11 in use, 14 available)

Date from: 2015-11-01 to 2016-02-08

4. Browse the file system to find the license file and click *OK* to upload and replace current license definition.

Related topics:

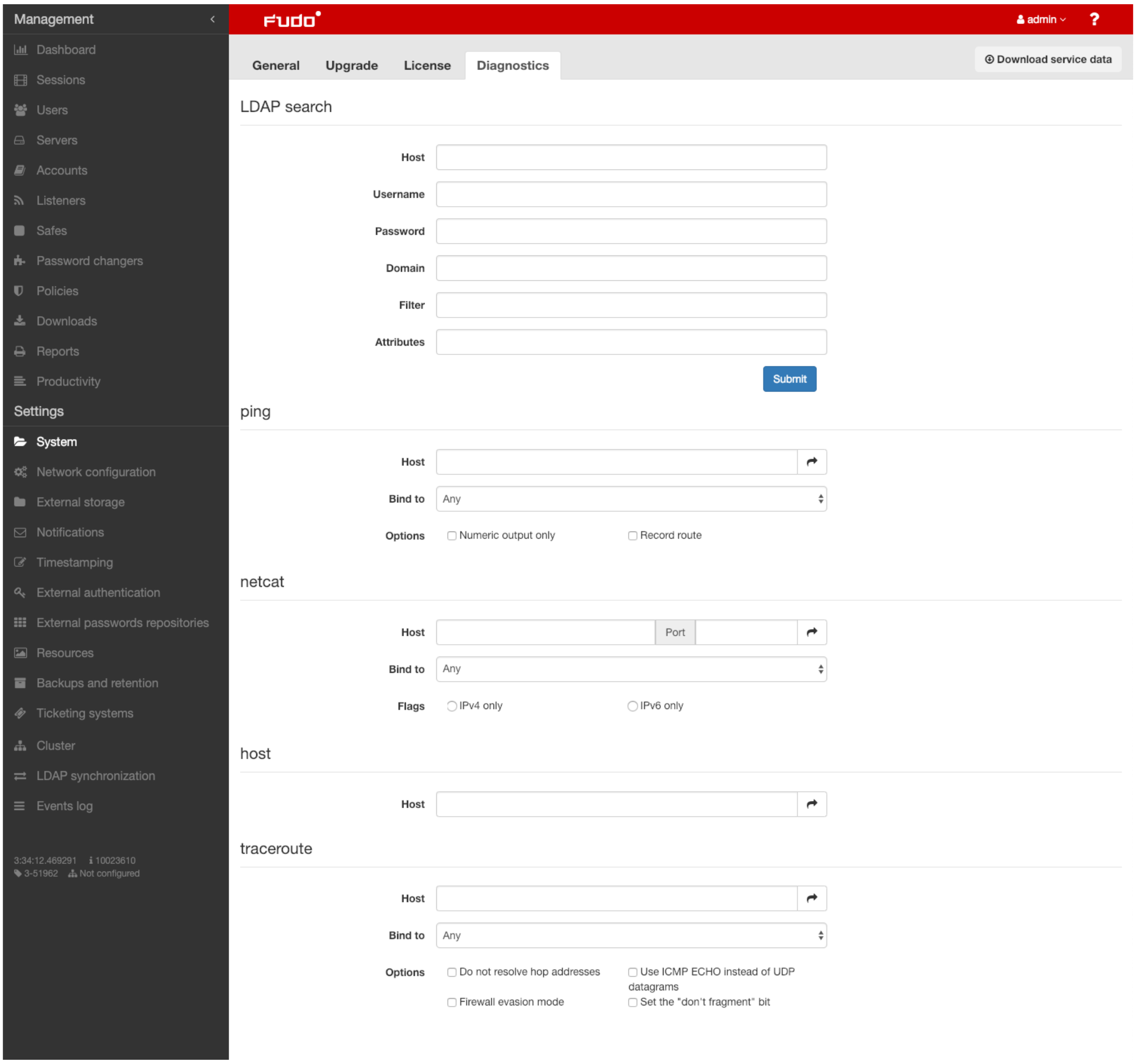
- *System*

15.1.8 Diagnostics

System diagnostics module enables executing basic system command, such as ping, netcat or traceroute.

To run a diagnostic utility, proceed as follows.

1. Select *Settings > System*.
2. Select the Diagnostics tab.
3. Find desired utility, provide necessary parameters and execute the command.



LDAP search

Host

Username

Password

Domain

Filter

Attributes

Submit

ping

Host

Bind to: Any

Options: □ Numeric output only □ Record route

netcat

Host: Port

Bind to: Any

Flags: ○ IPv4 only ○ IPv6 only

host

Host

traceroute

Host

Bind to: Any

Options: □ Do not resolve hop addresses □ Use ICMP ECHO instead of UDP datagrams □ Firewall evasion mode □ Set the "don't fragment" bit

Command/parameter	Description
LDAP search	LDAP search allows querying LDAP server for objects.
Host	LDAP server IP address.
Login	Login of the user allowed to browse the directory.
Password	Password of the user allowed to browse the directory.
Domain	Directory domain to query.
Filter	Objects filtering parameter.
Attributes	LDAP search attributes.
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 Fudo PAM and the specified host.
Do not resolve hop addresses	Subsequent hop IP addresses are not resolved to mnemonic names.
Use ICMP ECHO instead of UDP datagrams	Enforces `traceroute` to use UDP packets instead of ICMP.
Firewall evasion mode	Enforces the same port numbers for UDP and TCP packets. Target port is not incremented with each packet sent.
Set the "don't fragment" bit	Disables packet fragmentation in case the packet exceeds defined MTU (Maximum Transmission Unit) value defined for the network. Exceeding the MTU value results in an error.

Related topics:

- *Troubleshooting*

15.1.9 Configuration encryption

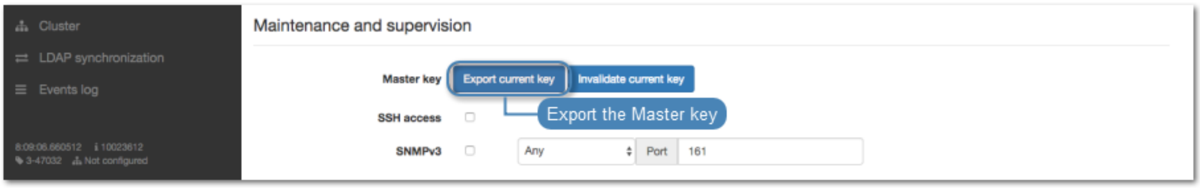
The *Master key* enables encrypting sensitive configuration parameters, system backups and external storage volumes. It also allows for recovering internal storage encryption key in case the pen drives containing encryption key are lost or damaged.

Note:

- The Master key is exported to PEM format and it is encrypted with SMIME using administrator's public key/certificate.
- It is essential to have the *Master key* exported and stored in a safe location.
- In case the *Master key* has been compromised, you can invalidate it, which will result in generating a new one and re-encrypting the data.

Exporting master key

1. Select *Settings* > *System*.
2. In the *Maintenance and supervision* click *Export current key*.



3. Click *Choose file* and browse the file system to find the certificate that will be used to encrypt the *Master key*.

Note:

- Generate the keys and the CSR (Certificate Signing Request) using *openssl*:

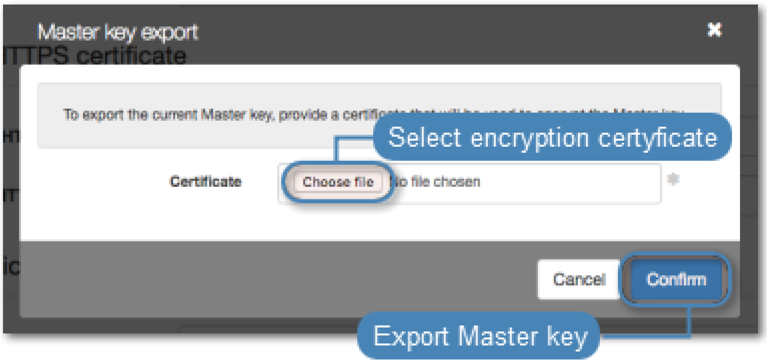
```
openssl req -newkey rsa:4096 -keyout privkey.pem -out req.pem
```

```
openssl req -nodes -newkey rsa:4096 -keyout privkey.pem -out req.pem # Do not
prompt for a password.
```

- Sign the CSR:

```
openssl x509 -req -in req.pem -signkey privkey.pem -out cert.pem
```

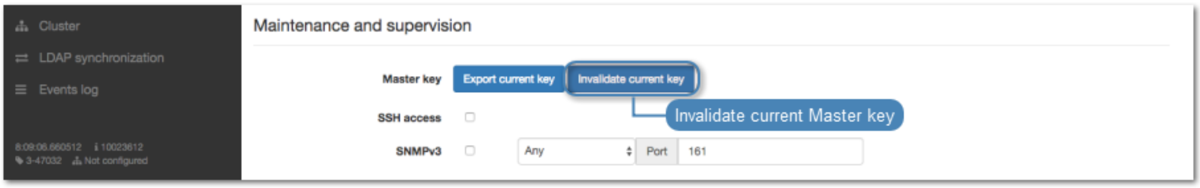
4. Click *Confirm* and save the the *Master key* file.



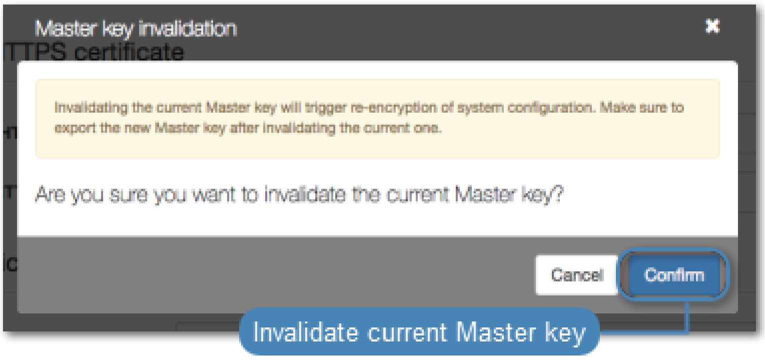
Invalidating current master key

In case the current *Master key* has been compromised, you can invalidate it. Invalidating the current *Master key* generates a new one and triggers data re-encryption.

1. Select *Settings* > *System*.
2. In the *Maintenance and supervision* click *Invalidate current key*.



3. Confirm invalidating the current key.



Master key invalidation

Invalidating the current Master key will trigger re-encryption of system configuration. Make sure to export the new Master key after invalidating the current one.

Are you sure you want to invalidate the current Master key?

4. Make sure to *export the newly generated key*.

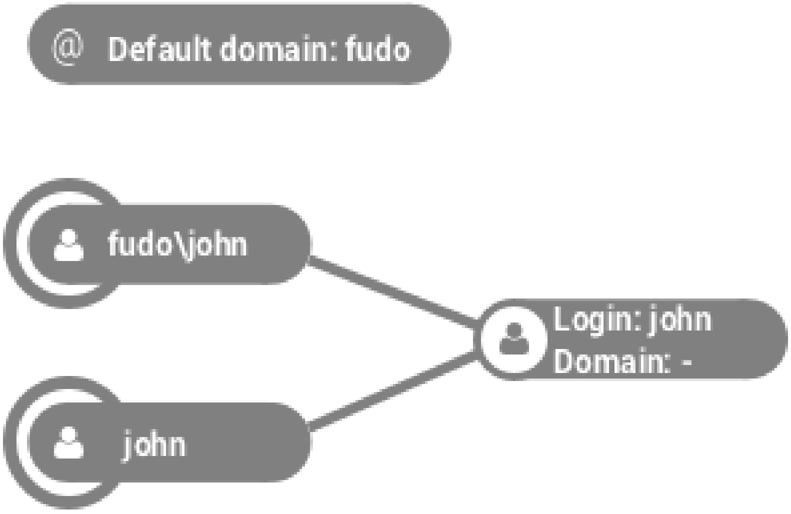
Related topics:

- *Security measures*

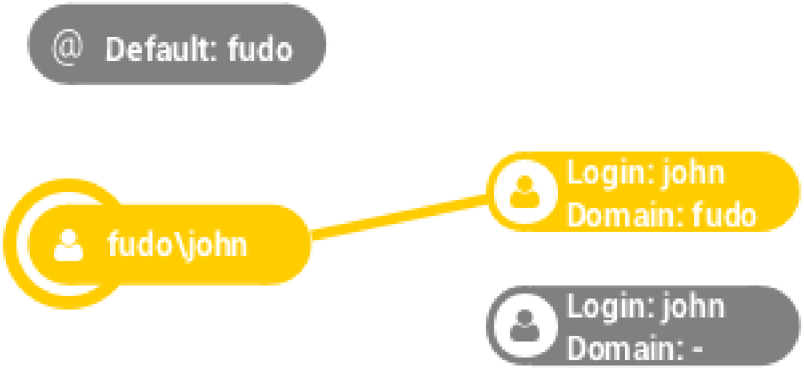
15.1.10 Default domain

Note:

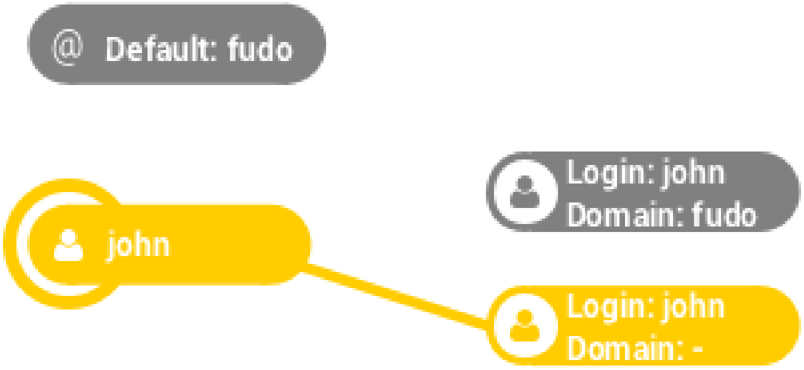
- In case the default domain is specified and the user does not have a domain defined, when logging in, the user can either include the domain (e.g. `john_smith@domain`) or leave it out (e.g. `john_smith`).



- If there are two users with the same login, one of which has the domain configured the same as the default domain, and the other does not have the domain defined, if the user provides the domain, Fudo PAM will match the user that has the domain explicitly specified.



In case the user does not provide the domain, Fudo PAM will match the user that does not have the domain explicitly specified.



Defining default domain

1. Select *Settings > System*.
2. In the *User authentication and sessions* section, provide the default domain.
3. Click *Save*.

Related topics:

- *Creating a user*
- *Users synchronization*

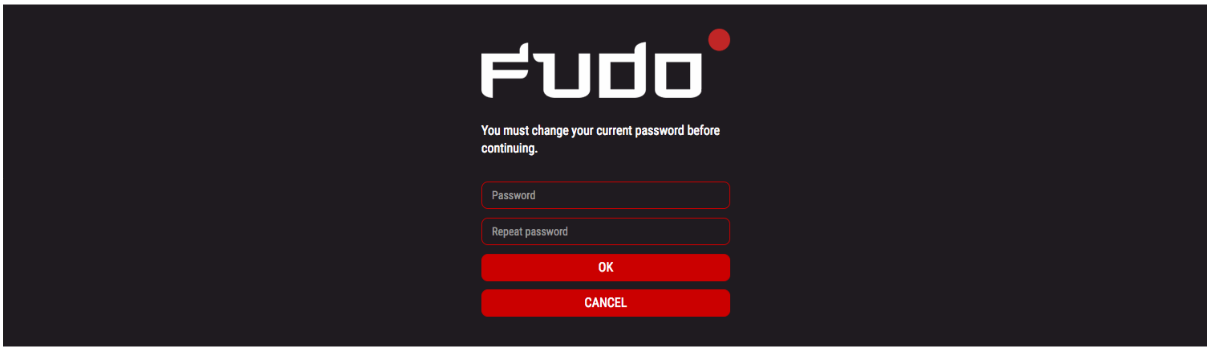
15.1.11 Password complexity

Fudo PAM enables defining static passwords complexity enabling you to enforce passwords that meet your internal regulations.

Defining password complexity

1. Select *Settings > System*.
2. In the *User authentication and sessions* section, select *Password complexity* to enforce defined rules.

Note: Enabling password complexity will trigger password change for users with the *Enforce static password complexity* option enabled whose passwords do not comply with the complexity settings. The password will have to be changed upon logging into the *User Portal*.



You must change your current password before continuing.

Password

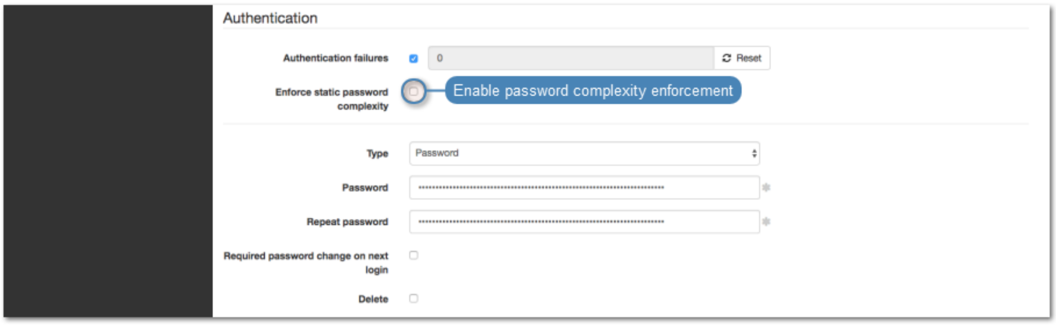
Repeat password

OK

CANCEL

3. Define the minimum number of characters.
4. Select *Small letters* and provide the minimal number of small letters in the password.
5. Select *Capital letters* and provide the minimal number of capital letters in the password.
6. Select *Special characters* and provide the minimal number of special characters in the password.
7. Select *Digits* and provide the minimal number of digits in the password.
8. Select the *Different password than current* option to enforce a password different from the current one.
9. Click *Save*.

Note: To enable static password complexity for a particular user, select the *Enforce static password complexity* option in the *Authentication* section on the user form.



Authentication

Authentication failures ☑ 0 Reset

Enforce static password complexity □ Enable password complexity enforcement

Type Password

Password ••

Repeat password ••

Required password change on next login □

Delete □

Related topics:

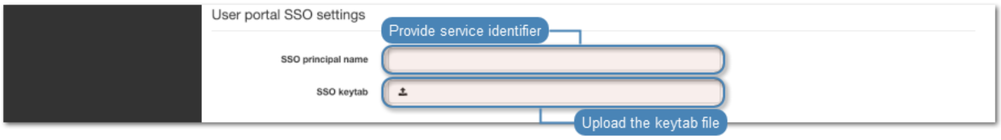
- *Creating a user*
- *Users synchronization*

15.1.12 Single Sign On in User Portal

Single Sign On automatically authenticates the user when logging into the User Portal.

15.1.12.1 Setting up Fudo PAM for SSO

1. Set Fudo PAM hostname to `fudo.sso.dwt`.
    - Select *Settings > Network configuration*.
    - Switch to the *Name & DNS* tab.
    - Enter `fudo.sso.dwt` in the *Hostname* field.
2. Configure DNS server to point to a DNS server in the *sso.dwt* domain.
    - Click *Add new* to define new DNS server.
    - Enter DNS server IP address.
    - Click *Save*.
3. Add user, that has an AD domain account.
    - *Set up LDAP users synchronization* or
    - *add user account manually*, with Active Directory eternal authentication method.
4. Define SSO service parameters in system settings.
    - Select *Settings > System*.
    - In the *User portal SSO settings* section, provide service identifier that will match the user account with the service instance.
    - Upload the keytab file containing user's ID and encryption keys for encrypting and decrypting Kerberos tickets.



    - Click *Save*.

15.1.12.2 Setting up domain controller

1. Add user account, which will be used by the *User Portal* to communicate with the *sso.dwt* domain.

    Note: When adding the account, enable the *Password does not expire* option.

2. On the DNS server add forward and reverse DNS entries for ‘fudo.sso.dwt.
3. Create a Kerberos ticket for Fudo PAM running the following command in the Powershell or CMD console:

‘‘ktpass -princ HTTP/fudo.sso.dwt@SSO.DWT -mapuser ssousername -pass password. -ptype KRB5_NT_PRINCIPAL -out fudo.sso.dwt.keytab‘‘

15.1.12.3 Setting up user workstations

1. Log in using credential of a user that will be connecting to servers through the *User Portal*.
2. Launch Internet Explorer.
3. Open the *Internet options* settings window.
4. Switch to the *Security* tab.
5. Select the *Local intranet* option and click *Sites*.
6. Click *Advanced*.
7. Add the *User Portal* address - `fudo.sso.dwt`.
8. Close settings window.

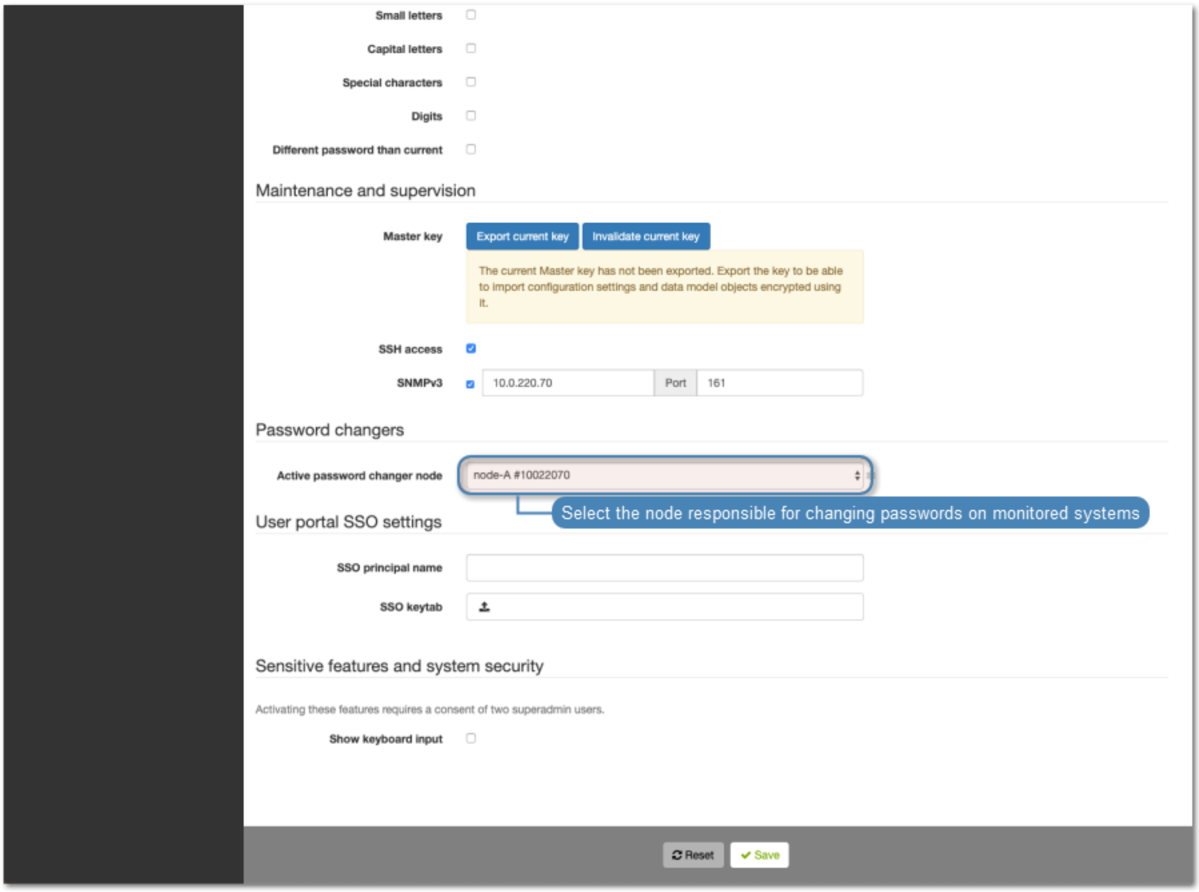
Related topics:

- *Creating a user*
- *Users synchronization*

15.1.13 Password changers - active cluster node

Active cluster node option determines the Fudo PAM instance responsible for changing passwords on monitored systems.

1. Select *Settings > System*.
2. In the *Password changers* section, select the node delegated to password changing.



Small letters □

Capital letters □

Special characters □

Digits □

Different password than current □

Maintenance and supervision

Master key

The current Master key has not been exported. Export the key to be able to import configuration settings and data model objects encrypted using it.

SSH access ☑

SNMPv3 ☑ 10.0.220.70 Port 161

Password changers

Active password changer node: node-A #10022070

Select the node responsible for changing passwords on monitored systems

User portal SSO settings

SSO principal name

SSO keytab

Sensitive features and system security

Activating these features requires a consent of two superadmin users.

Show keyboard input □

3. Click *Save*.

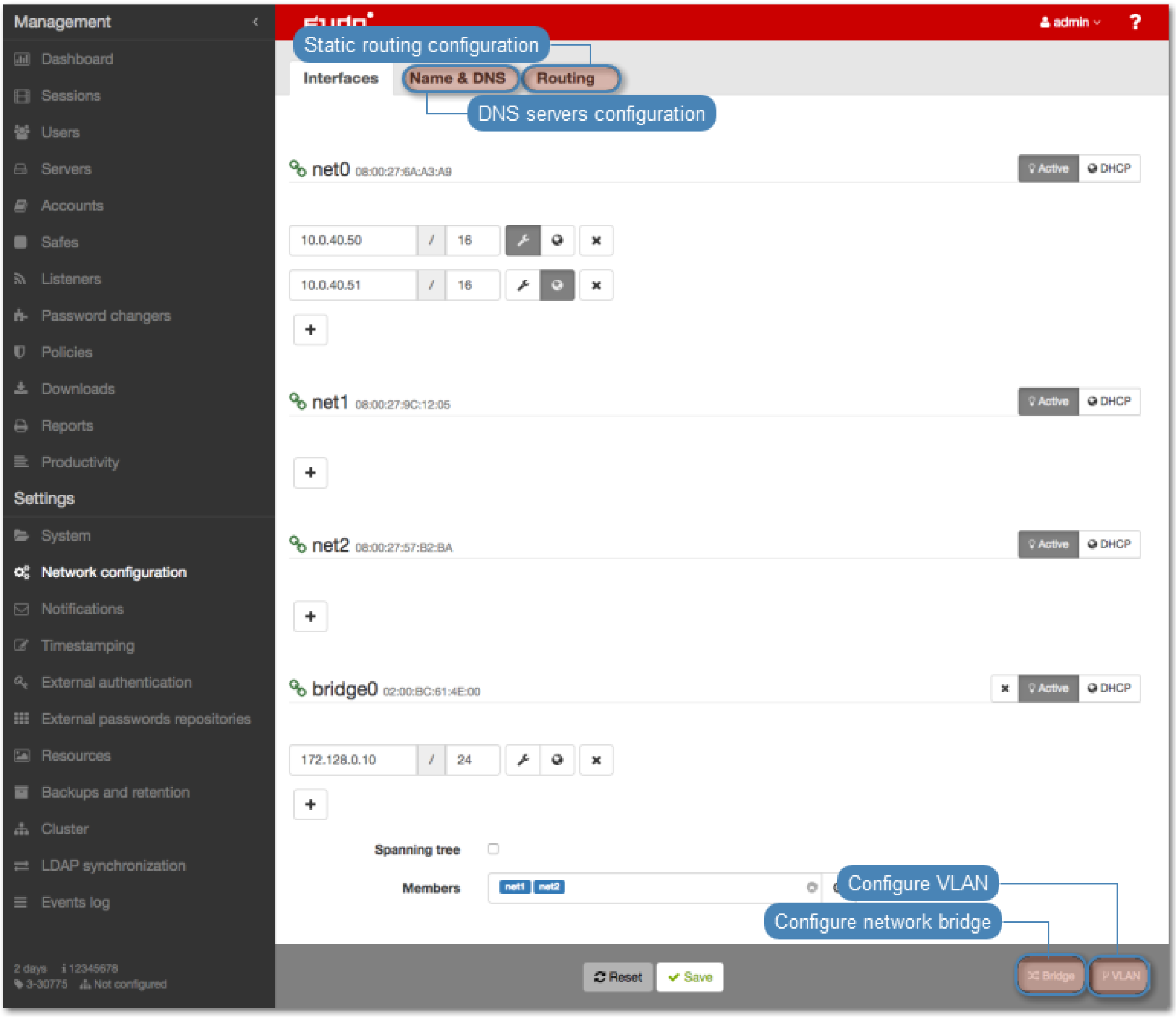
Note: In case the node responsible for changing passwords fails, the task will not be automatically picked up by another Fudo PAM instance. In order to restore automatic password changing, the system administrator will have to change the active password changing node or bring back the failed node.

Related topics:

- *Password changers*
- *Custom password changers*

15.2 Network settings

To change network settings select *Settings > Network configuration*.



net0 08:00:27:6A:A3:A9

10.0.40.50 / 16

10.0.40.51 / 16

net1 08:00:27:9C:12:05

net2 08:00:27:57:B2:BA

bridge0 02:00:BC:61:4E:00

172.128.0.10 / 24

Spanning tree □

Members: net1 net2

15.2.1 Network interfaces configuration

15.2.1.1 Managing physical interfaces

Defining IP address

Defined IP addresses are physical interface's aliases, which are used in server's *configuration procedures* (*Local address* field in proxy configuration).

Note: If the list of the assigned IP addresses is empty and the is no option to define an IP address, check if given interface is a member of a bridge.

To define an IP of a physical network interface, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Click + and provide IP address and subnet mask in CIDR format.

Note: + will be inactive if the *DHCP* option is enabled on the given interface.

3. Choose additional options for the IP address being defined.

🔧 Enable access to administration panel on given IP address. Note that the management IP address is also used for replicating data between cluster nodes as well as *service access over SSH protocol*.

Note: The default port number for service access over SSH protocol is 65522.

🖧 Make the alias a virtual IP address which will be take over by another cluster node in case of the master node's failure.

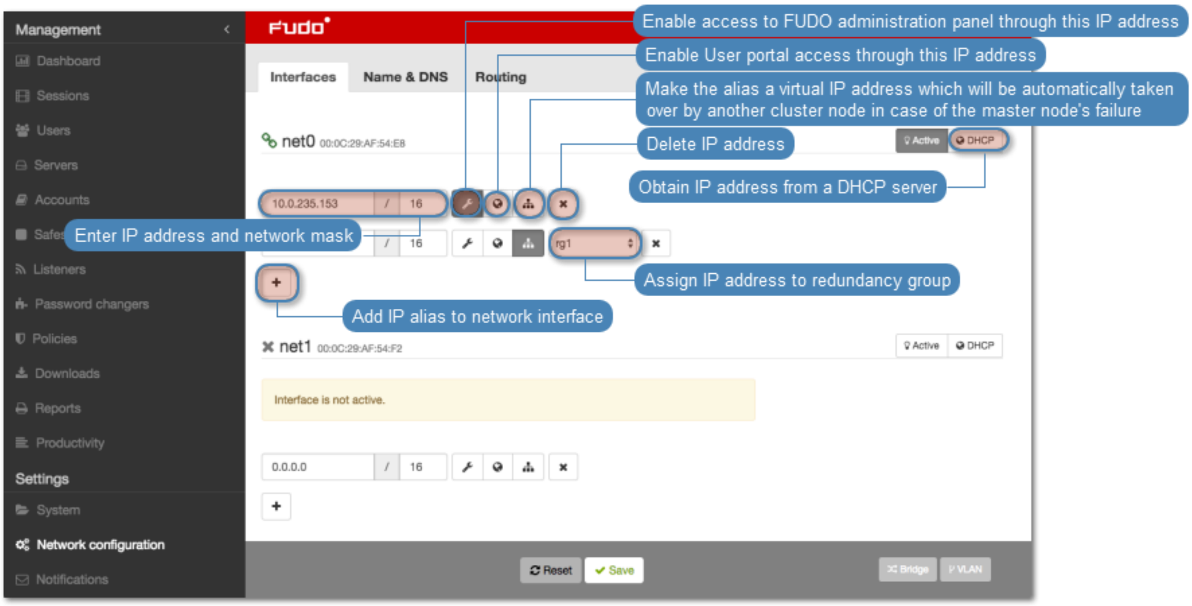
Note: Cluster IP address must be added manually on every cluster node, with the 🖧 option enabled.

🌐 Enable access to *User portal* on given IP address.

4. Select the redundancy group that the IP address will be assigned to (*applicable to virtual IP addresses*).

Note: *Redundancy groups* are defined in the *Cluster* view in the *Redundancy groups* tab. For more information refer to the *Redundancy groups* topic.

5. Click *Save*.



Interface is not active.

Enable access to FUDO administration panel through this IP address

Enable User portal access through this IP address

Make the alias a virtual IP address which will be automatically taken over by another cluster node in case of the master node's failure

Delete IP address

Obtain IP address from a DHCP server

Enter IP address and network mask

Assign IP address to redundancy group

Add IP alias to network interface

Note: Current state of each network interface is represented with an icon.

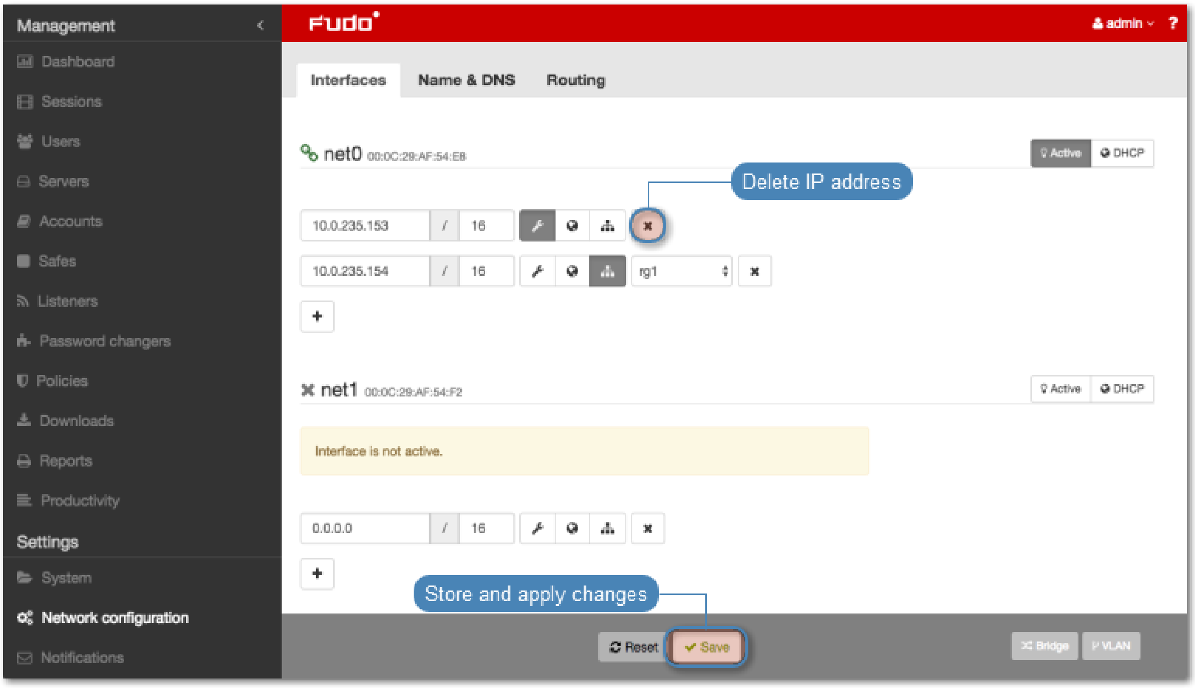
🔗	Interface active and connected.
⛓️‍💥	Interface active but disconnected.
✖	Interface disabled.

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.*



Delete IP address

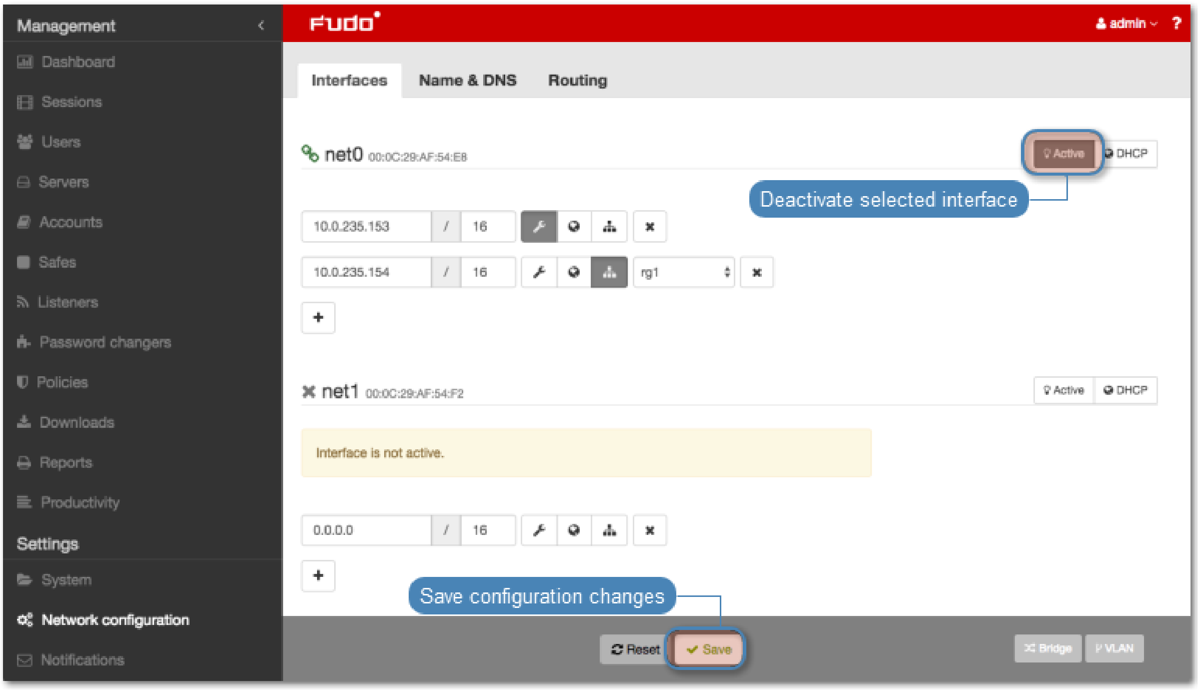
Interface is not active.

Store and apply changes

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.



net0 00:0C:29:AF:54:E8

10.0.235.153 / 16

10.0.235.154 / 16 rg1

net1 00:0C:29:AF:54:F2

Interface is not active.

0.0.0.0 / 16

Deactivate selected interface

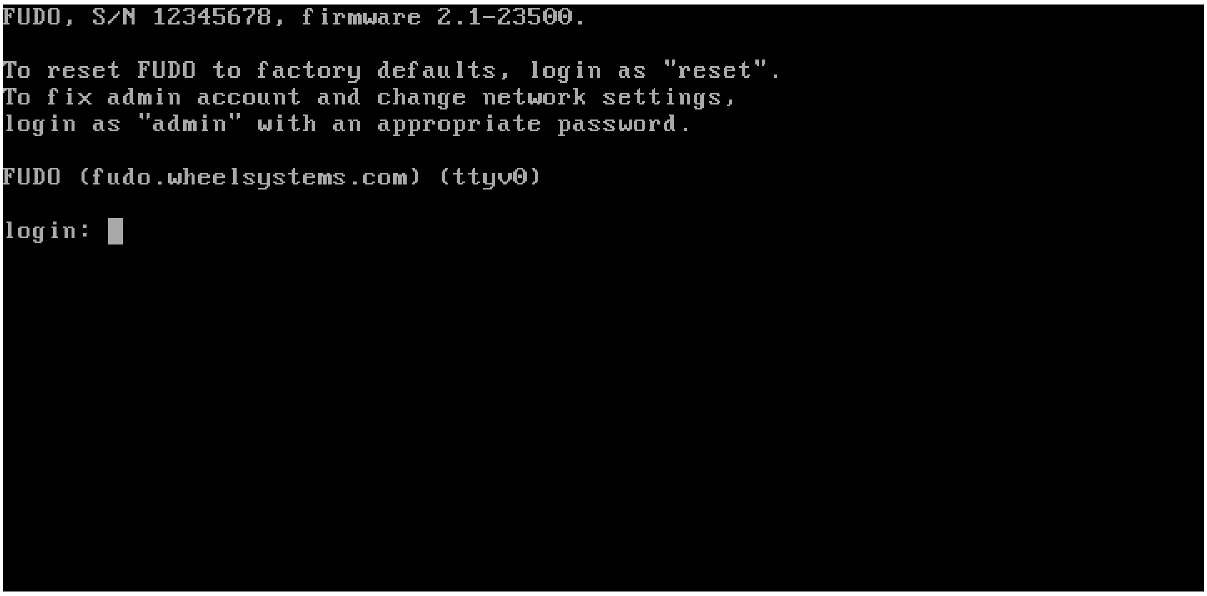
Save configuration changes

3. Click *Save*.

15.2.1.2 Defining IP address using system console

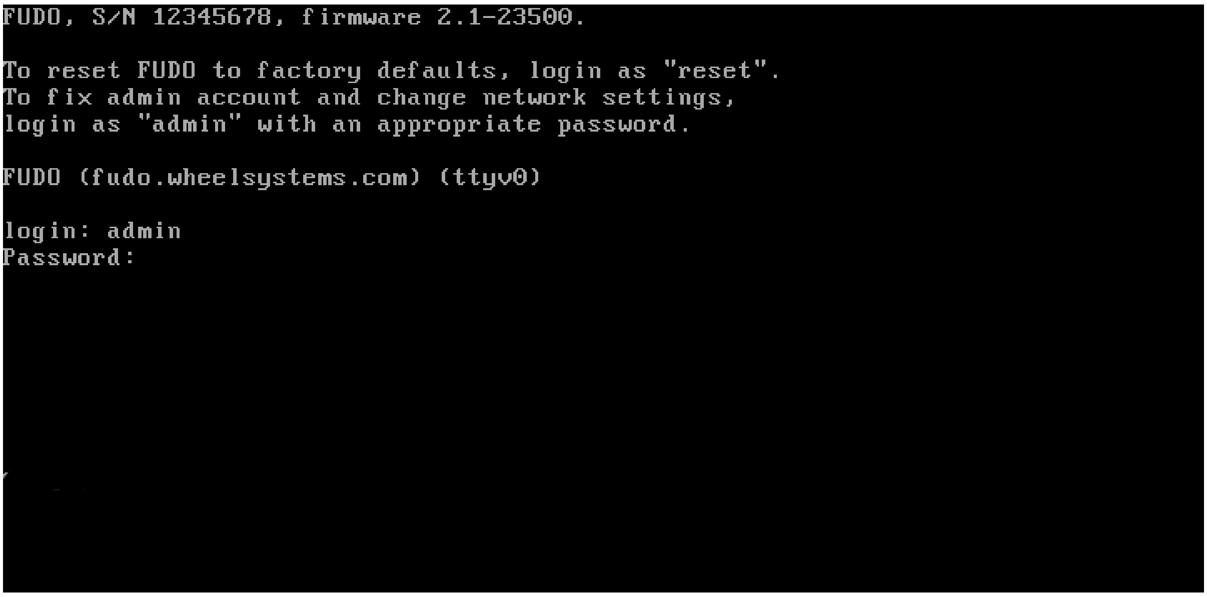
In case the web administration interface cannot be accessed, IP address can be defined using console connection.

1. Connect monitor and keyboard to the device.
2. Enter administrator account login and press *Enter*.



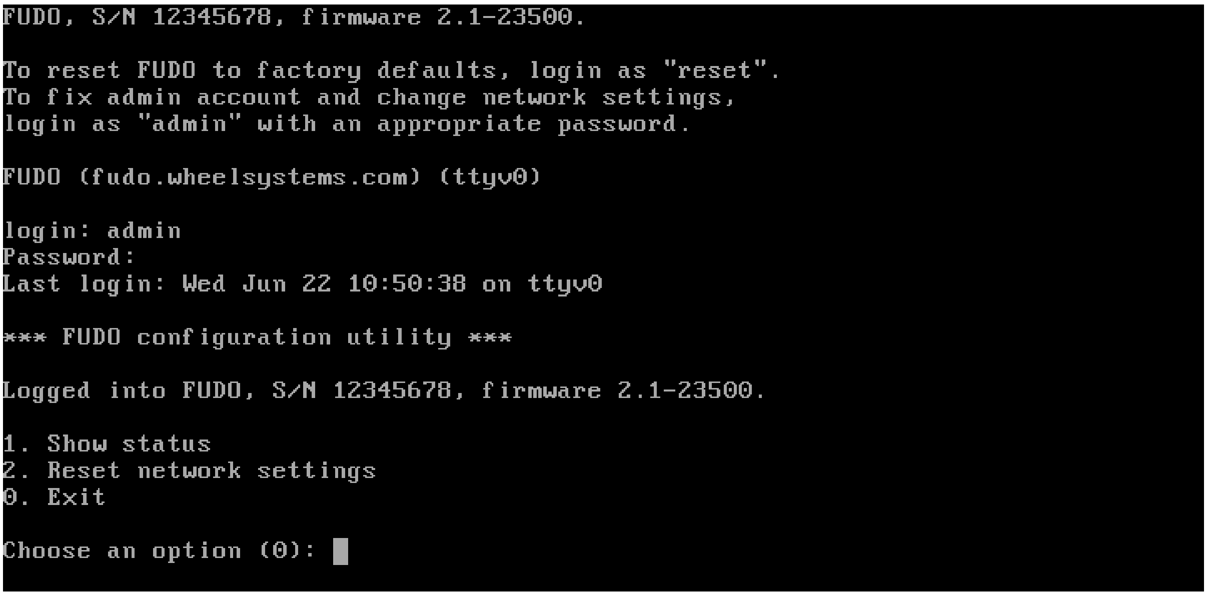
```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login:
```

3. Enter administrator account password and press *Enter*.



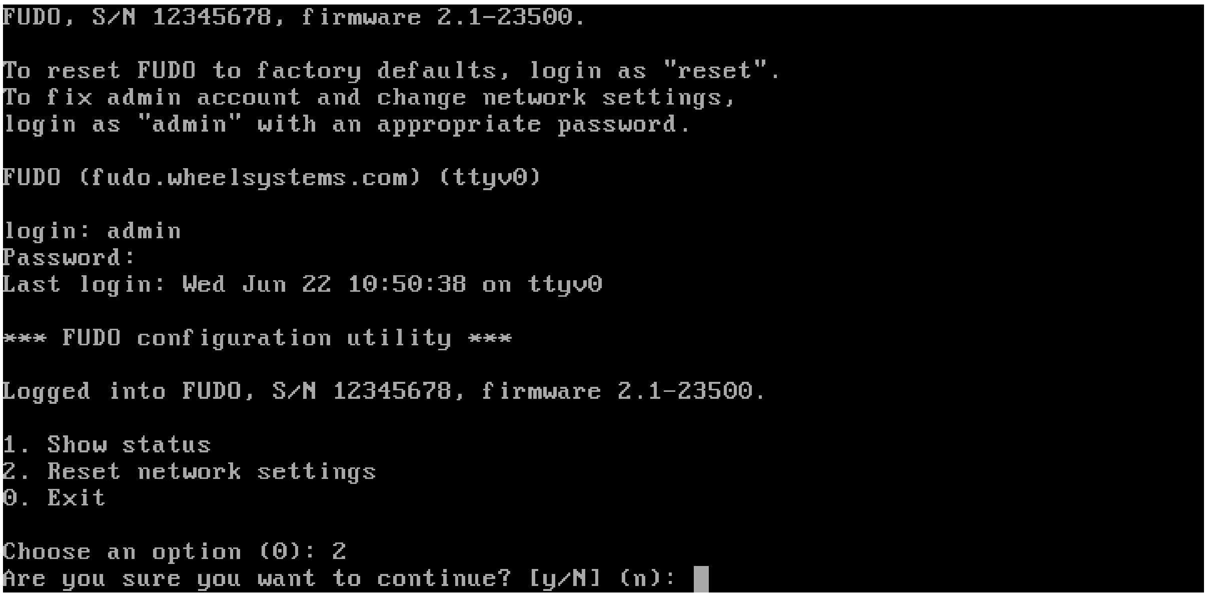
```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
```

4. Enter 2 and press *Enter* to change network configuration.



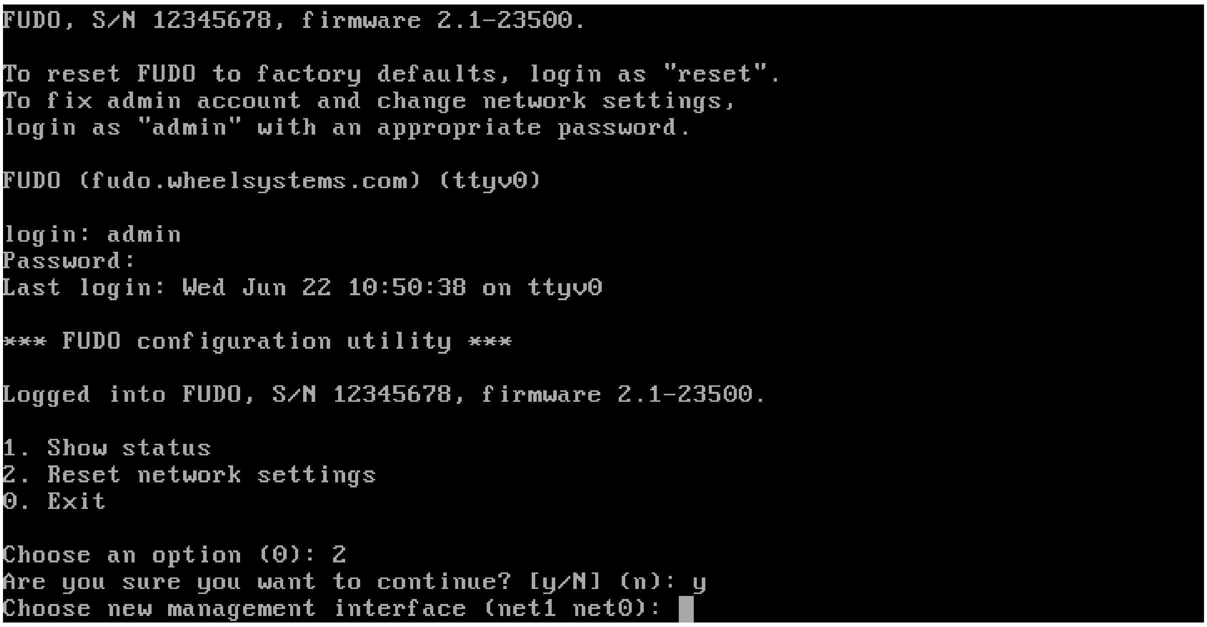
```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:50:38 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0):
```

5. Enter y and press *Enter* to proceed with resetting network configuration.



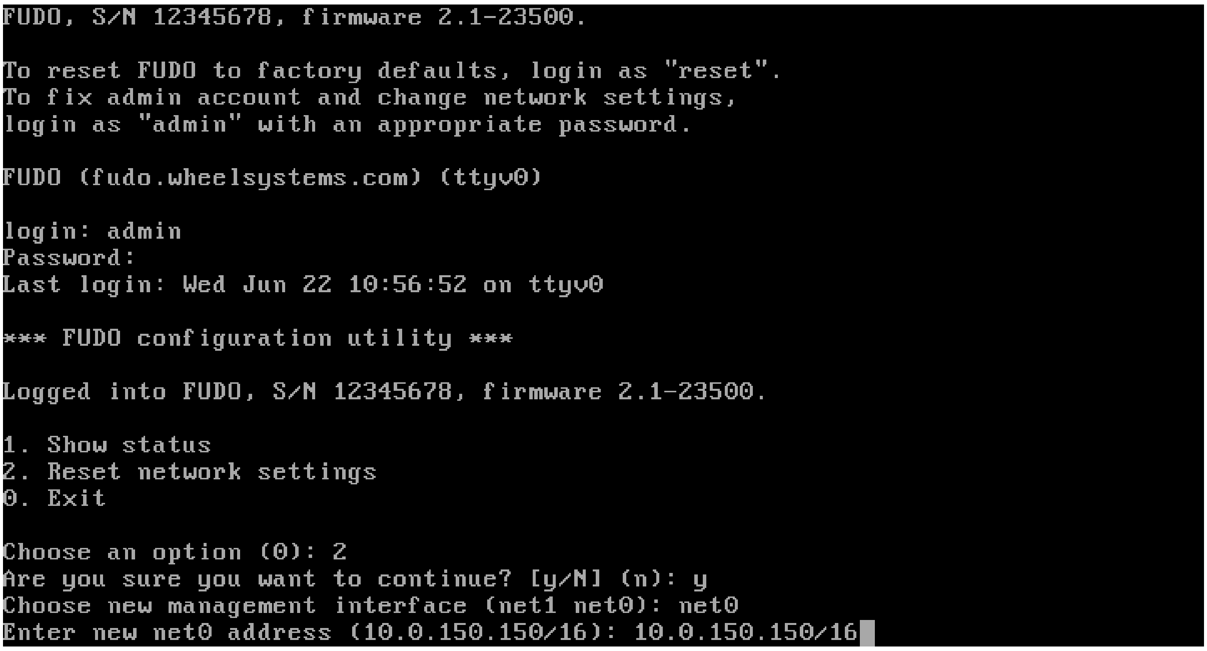
```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:50:38 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n):
```

6. Enter the name of the new management interface (Fudo PAM web interface is accessible through the management interface).



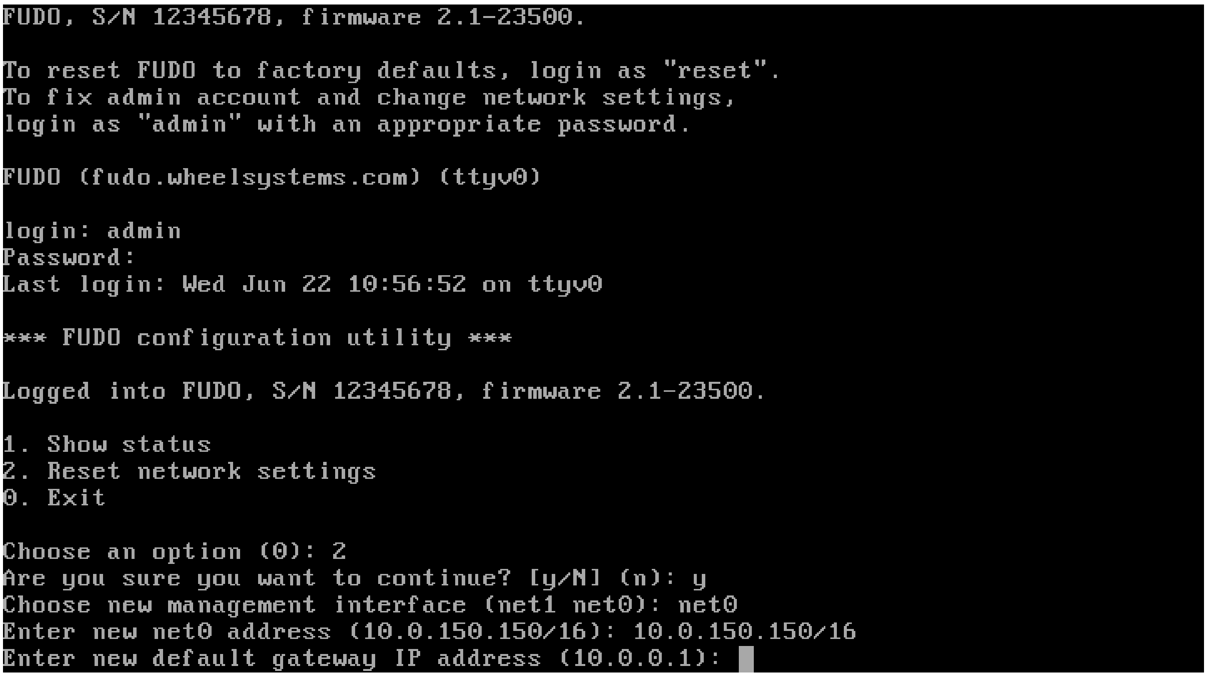
```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:50:38 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0):
```

7. Enter IP address along with the network subnet mask separated with `/` (e.g. `10.0.0.8/24`) and press *Enter*.



```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
```

8. Enter network gate and press *Enter*.



```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
Enter new default gateway IP address (10.0.0.1):
```

15.2.1.3 Setting up a network bridge

Bridge deployment scenario requires setting up a network bridge.

To configure a network bridge, proceed as follows.

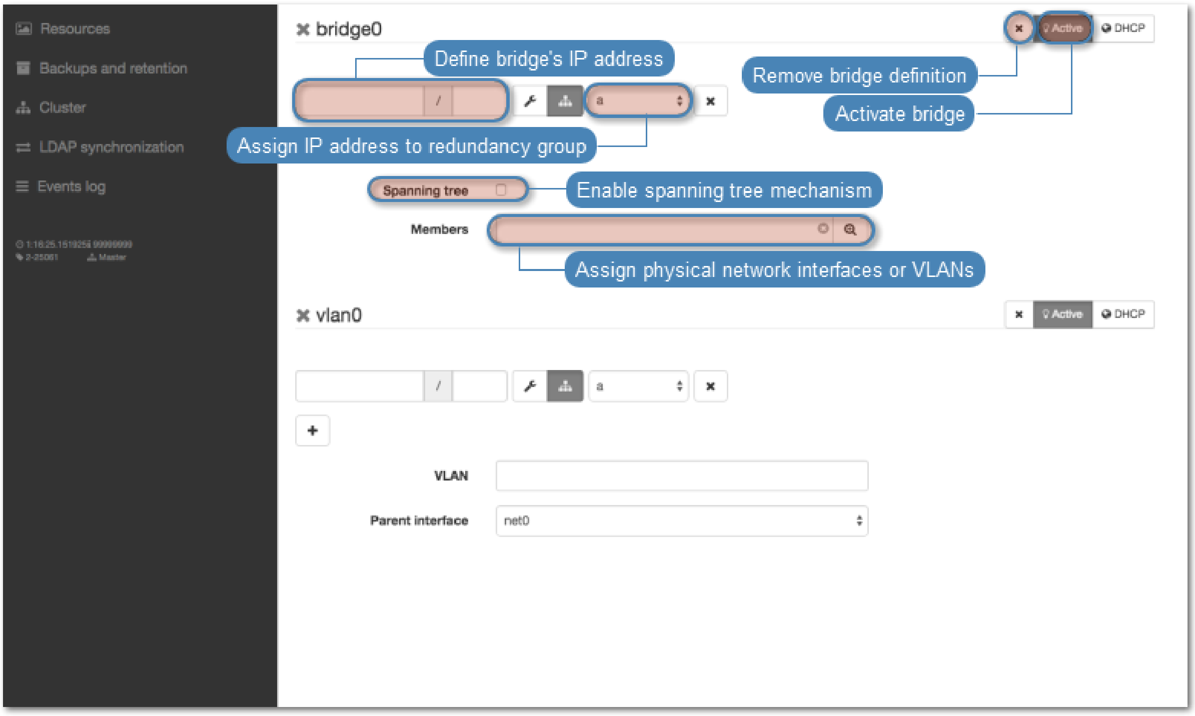
1. Select *Settings > Network configuration.*

2. Click *Bridge.*

3. Assign network interfaces or VLANs to the bridge.

Note: Setting up a network bridge requires removing all IP addresses directly assigned to interfaces which are selected as bridge members.

4. Enter IP address and network subnet in CIDR notation.
5. Select *Spanning tree* option to enable bridge loops prevention.
6. Select the *Management* option if the administration interface should be available under assigned IP addresses and click *Active*.
7. Click *Save*.



15.2.1.4 Setting up virtual networks (VLANs)

VLAN networks allow separating broadcast domains.

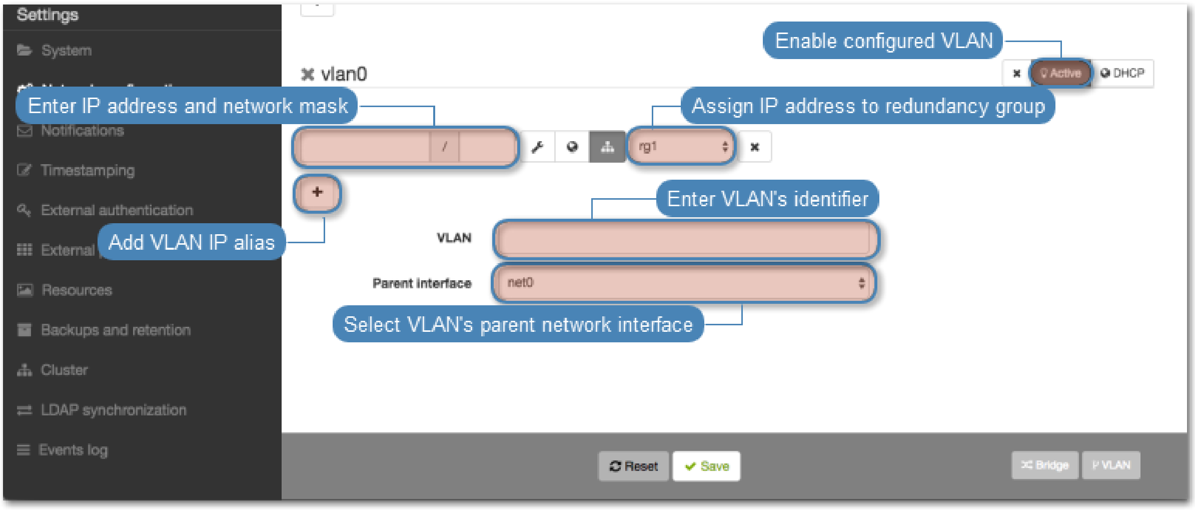
To configure a VLAN on , proceed as follows.

1. Select *Settings > Network configuration*
2. Click *VLAN*.
3. Select the physical interface and define VLAN ID.
4. Add IP addresses to given VLAN.

Note: Select *DHCP* option, to obtain IP address from a DHCP server.

Note: The IP addresses are aliases to the physical interface and are used in *servers configuration* as proxy server address.

5. Click *Active* to activate defined VLAN.
6. Click *Save*.



Enable configured VLAN

Enter IP address and network mask

Assign IP address to redundancy group

Enter VLAN's identifier

Add VLAN IP alias

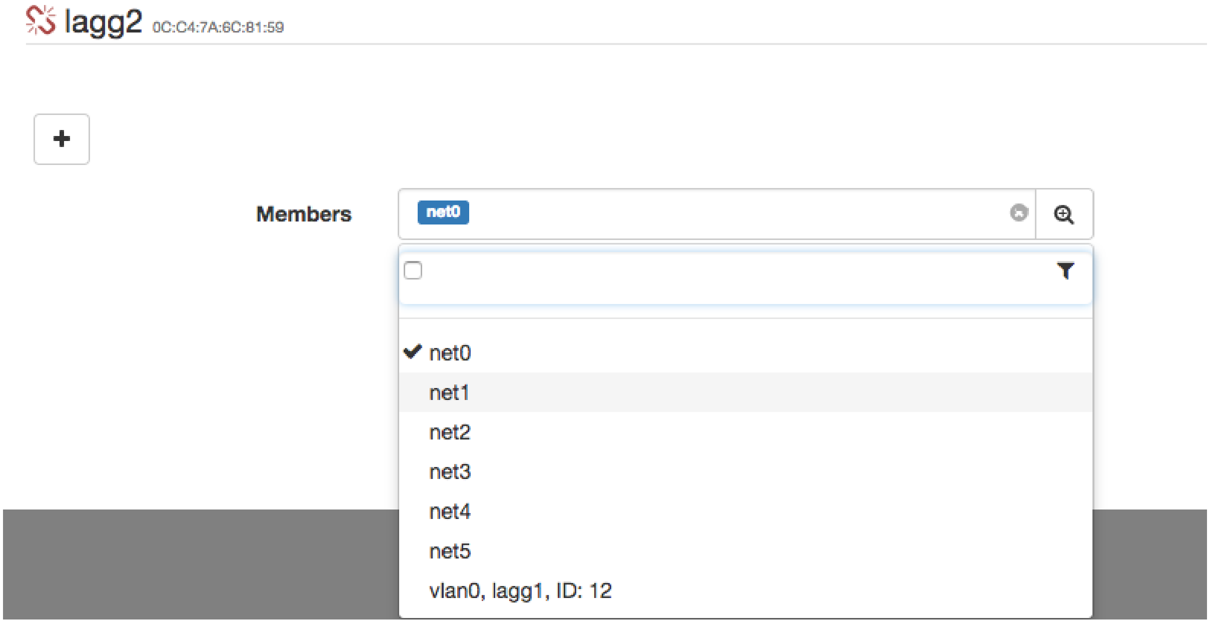
Select VLAN's parent network interface

15.2.1.5 Setting up LACP link aggregation

Link aggregation enables combining a number of network interfaces for improved transfer rates and implementation of failover scenarios in which the services remain available in case of a network switch failure.

To configure a network link aggregation, proceed as follows.

1. Select *Settings > Network configuration*.
2. Click *Link aggregation*.
3. Assign network interfaces.



Note: Setting up a network bridge requires removing all IP addresses directly assigned to interfaces which are selected as bridge members.

4. Enter IP address and network subnet in CIDR notation.
5. Choose additional options for the IP address being defined.

🔧	Enable access to administration panel on given IP address. Note that the management IP address is also used for replicating data between cluster nodes.
🖧	Make the alias a virtual IP address which will be take over by another cluster node in case of the master node's failure.
🌐	Enable access to *User portal* on given IP address.

6. Click *Save*.

Related topics:

- *Servers management*
- *Accounts*

15.2.2 Labeled IP addresses

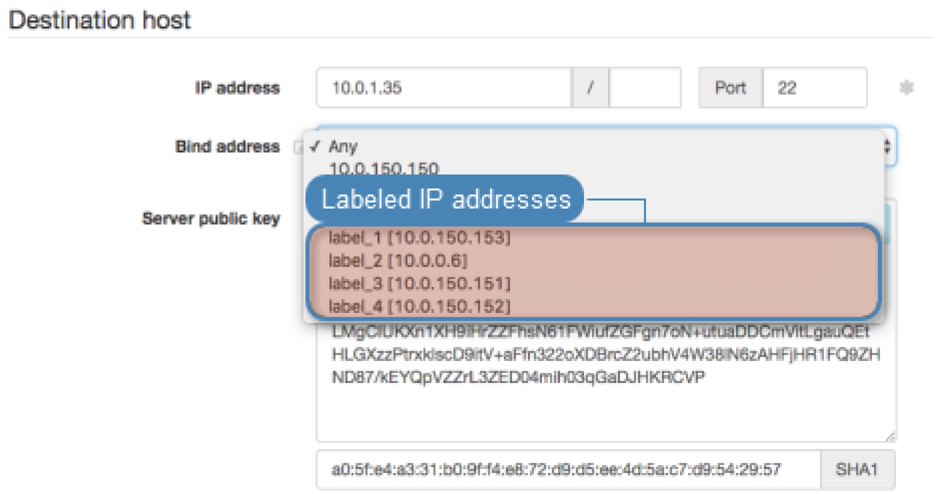
IP address labels are global configuration parameters. They are replicated throughout cluster's nodes, but their assignment is strictly local, applicable to each node separately. Labels enable ensuring constant access to LDAP authentication services in case of a node failure and allow for implementing load balancing scenarios.

Defining a labeled IP address

1. Select *Settings > Network configuration*.
2. Select the *IP labels* tab.
3. Click +.
4. Provide IP address and enter label name.

Note: Label name can comprise small letters, digits, _ and - characters.

5. Click *Save*.
6. Use labeled IP address in listener, server or external authentication source configuration.



Destination host

IP address 10.0.1.35 / Port 22

Bind address
✓ Any
10.0.150.150
label_1 [10.0.150.153]
label_2 [10.0.0.6]
label_3 [10.0.150.151]
label_4 [10.0.150.152]

Server public key

```
LMgCIUKXn1XH9IHrZZFhsN61FWiufZGFgn7oN+utuaDDCmVitLgauQEt
HLGXzzPtrxkIscD9itV+aFfn322oXDBrcZ2ubhV4W38IN6zAHFjHR1FQ9ZH
ND87/kEYQpVZZrL3ZED04mih03qGaDJHKRCVP
```

a0:5f:e4:a3:31:b0:9f:f4:e8:72:d9:d5:ee:4d:5a:c7:d9:54:29:57 SHA1

Related topics:

- *Network interfaces configuration*
- *External authentication*
- *Servers*
- *Listeners*

15.2.3 Bypasses configuration

Bypasses enable to physically re-route network packages in case of a system failure.

Note: Bypasses configuration is not available if Fudo PAM is running in virtualized environment.

1. Select *Settings* > *Network configuration*.
2. Select *Bypasses* tab.
3. Select bypass mode.
   - Bypass mode permanently enabled - this option enforces bypass mode on the network interface card. This mode may be used for maintenance purposes or when troubleshooting network issues.
   - Bypass mode enabled only in case of system failure - network packets are re-routed only in case of a system failure or in case the Fudo PAM is powered off.
   - Bypass mode disabled - in case of system failure, the network packets will not be routed to the next network appliance.
4. Click *Save*.

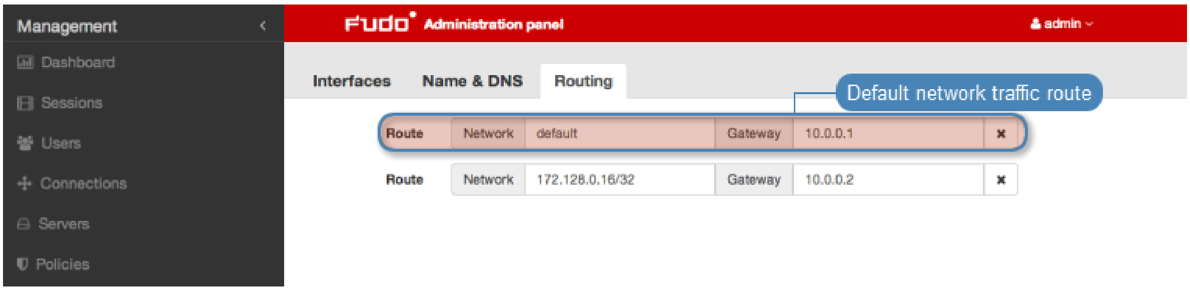
Related topics:

- *Network interfaces configuration*

15.2.4 Routing configuration

In default configuration, 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.



Default network traffic route

Route | Network default | Gateway 10.0.0.1 | ✖

Route | Network 172.128.0.16/32 | Gateway 10.0.0.2 | ✖

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

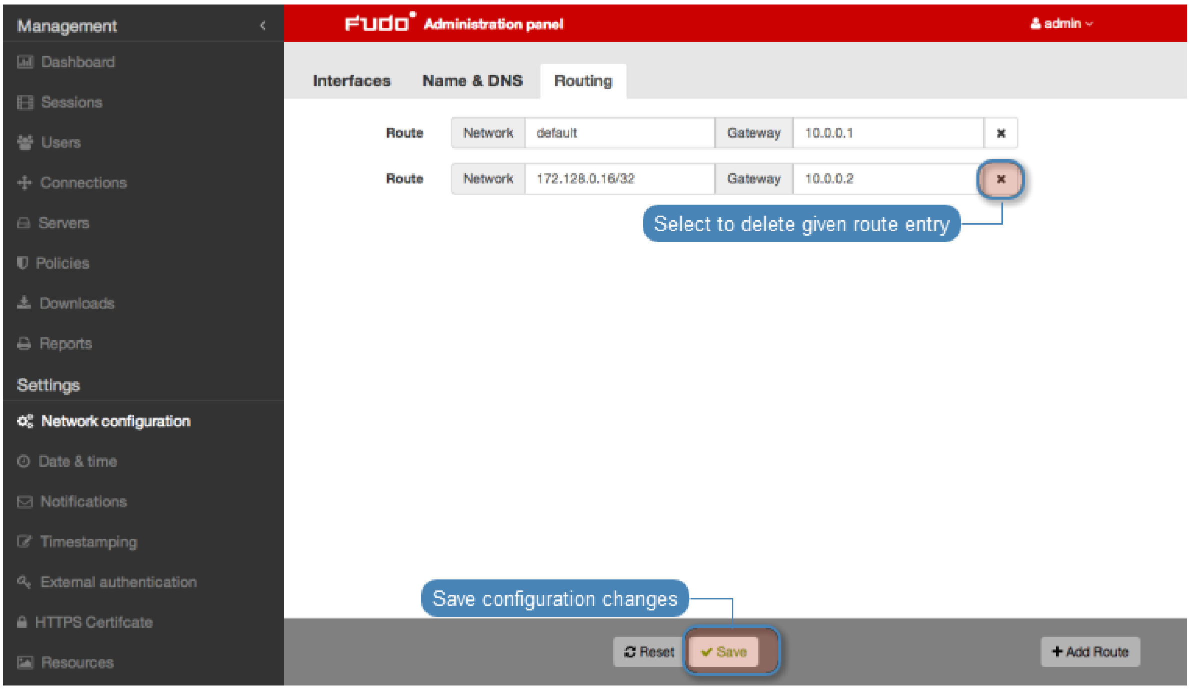
To edit a route, proceed as follows.

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*.



Route: Network default, Gateway 10.0.0.1

Route: Network 172.128.0.16/32, Gateway 10.0.0.2

Select to delete given route entry

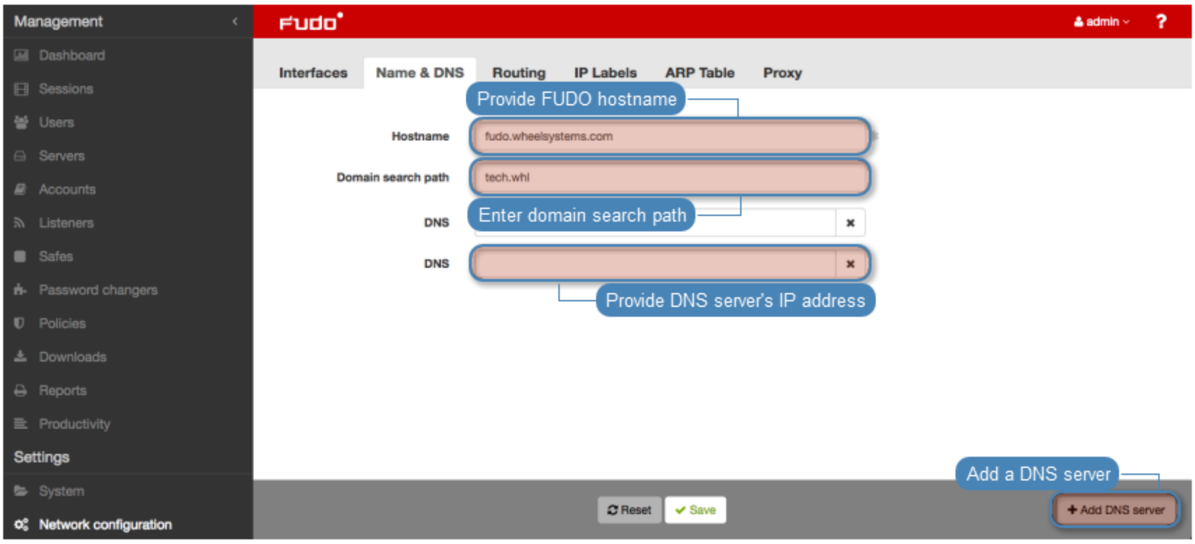
Save configuration changes

Related topics:

- *Network interfaces configuration*
- *Time servers configuration*

15.2.5 DNS configuration

Note: DNS servers enable using mnemonic hosts names instead of IP addresses when configuring various network resources.



Provide FUDO hostname

Hostname: fudo.wheelsystems.com

Domain search path: tech.whl

Enter domain search path

DNS

DNS

Provide DNS server's IP address

Add a DNS server

Defining domain search path

Domain search path enables convenient hosts identification based on short names. For example, defining `tech.whl` as the domain search path, enables defining target host as `ftp` instead of `ftp.tech.whl`.

To define a domain search path, proceed as follows.

1. Select *Settings > Network configuration.*
2. Switch to the *Name & DNS* tab.
3. Enter the domain search path.

Note:

- To define more than one value, enter desired values separated by space character. E.g. `tech.whl wheel.com`
- Protocol implementation enables defining up to six domain search paths.

---

4. Click *Save.*

Adding a DNS server definition

To add a DNS server definition, proceed as follows.

1. Select *Settings > Network configuration.*
2. Switch to the *Name & DNS* tab.
3. Click *Add new* to define new DNS server.
4. Enter DNS server IP address.
5. Click *Save.*

Editing a DNS server definition

To edit DNS server definition, proceed as follows.

1. Select *Settings > Network configuration.*
2. Switch to the *Name & DNS* tab.
3. Find given DNS server and double-click desired field.
4. Change parameter value as needed.
5. Click *Save.*

Deleting a DNS server definition

To delete a DNS server definition, proceed as follows.

Note: Deleting a DNS server definition may cause interruptions in device operation, if system configuration uses hosts names instead of IP addresses.

---

1. Select *Settings > Network configuration.*
2. Switch to the *Name & DNS* tab.
3. Find and select given DNS server definition.
4. Click *Delete.*

5. Click *Save* .

Related topics:

- *Network interfaces configuration*
- *Time servers configuration*

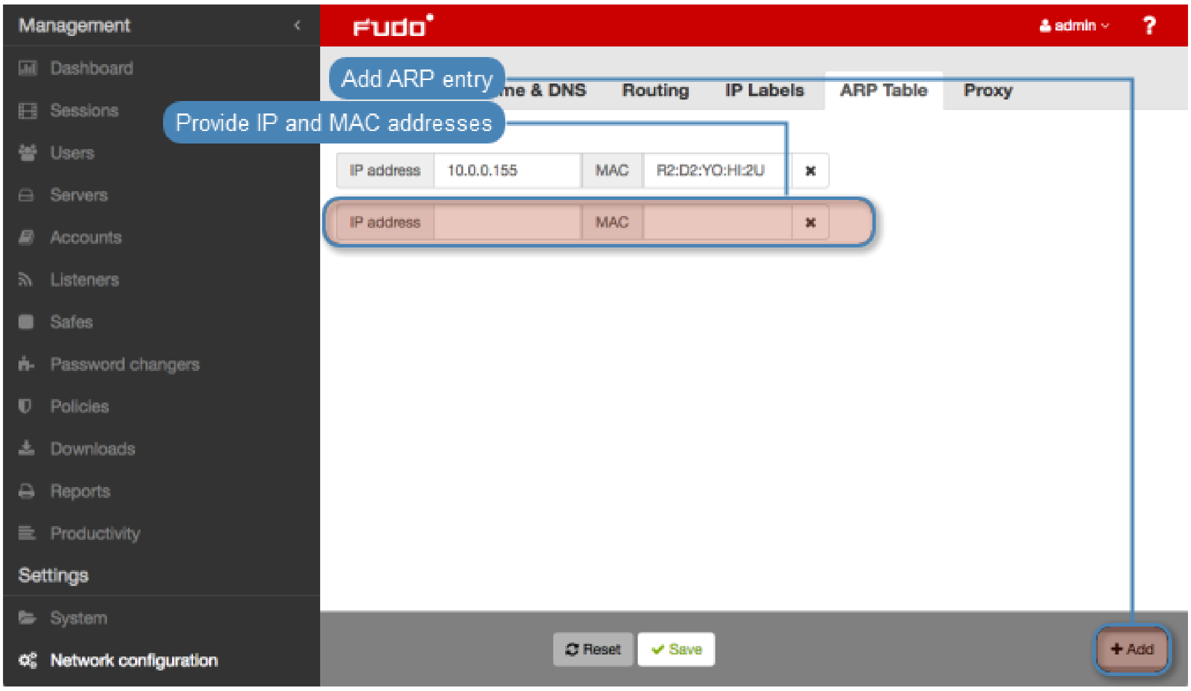
15.2.6 ARP table configuration

Note: Adding an entry to ARP table can resolve network communication issues.

Adding an ARP entry

To add an ARP entry, proceed as follows.

1. Select *Settings > Network configuration.*
2. Switch to the *ARP table* tab.
3. Click *+ Add* to define new ARP table entry.
4. Enter IP address and corresponding MAC address.
5. Click *Save*.



Add ARP entry

Provide IP and MAC addresses

IP address 10.0.0.155 MAC R2:D2:YO:HI:2U

Editing an ARP table entry

To edit an ARP table entry, proceed as follows.

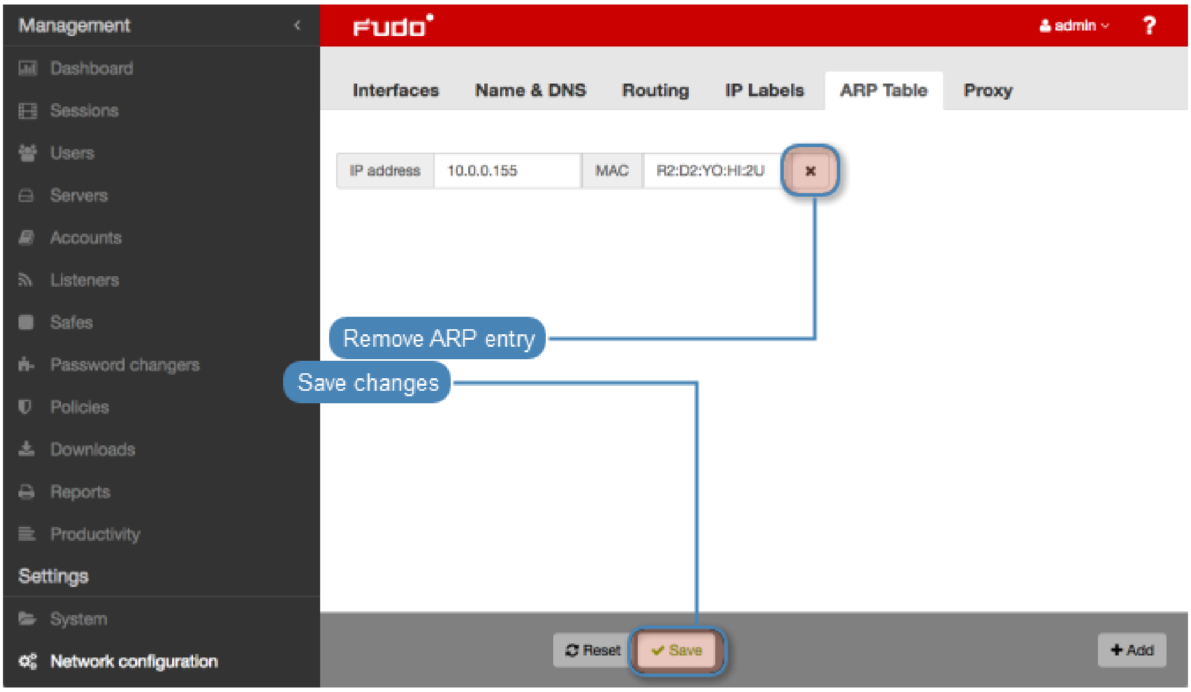
1. Select *Settings > Network configuration.*
2. Switch to the *ARP table* tab.
3. Find and edit desired ARP table entry.
4. Click *Save*.

Deleting an ARP table entry

Note: Deleting an ARP table entry may cause system malfunction due to network communication issues.

To delete an ARP entry, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Switch to the *ARP table* tab.
3. Find desired ARP entry and click the ✖ icon.
4. Click *Save* .



IP address 10.0.0.155 MAC R2:D2:YO:HI:2U

Related topics:

- *Network interfaces configuration*
- *Time servers configuration*

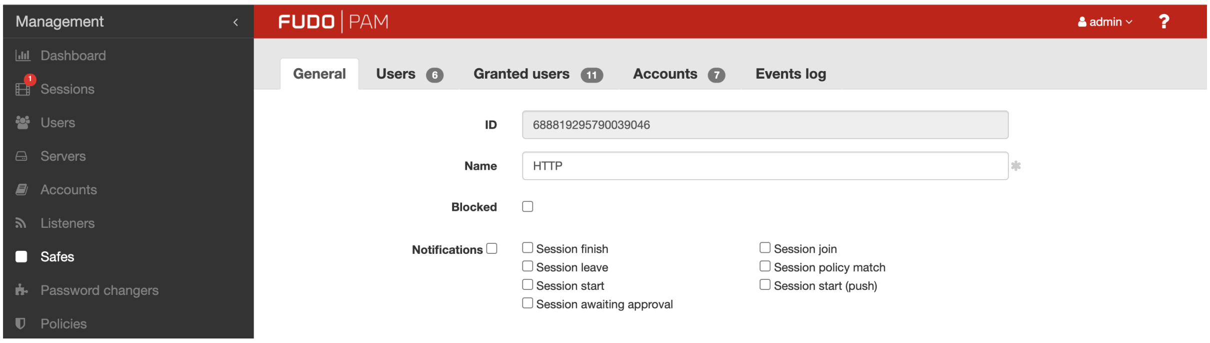
15.3 Notifications

Fudo PAM can send email notifications concerning defined connections (session start, session end, session inject start, session inject end). Notification service is configured when creating new or editing existing connection.

Note:

- Notifications can be received by users with *operator*, *admin* or *superadmin* roles.

- To receive notifications, login to Fudo PAM administration panel and select desired notifications in the Safe's configuration within the *General* section. It is required to log in into each account that should receive the notification and check the corresponding checkboxes.



ID: 688819295790039046

Name: HTTP

Blocked: □

Notifications □
- □ Session finish
- □ Session leave
- □ Session start
- □ Session awaiting approval
- □ Session join
- □ Session policy match
- □ Session start (push)

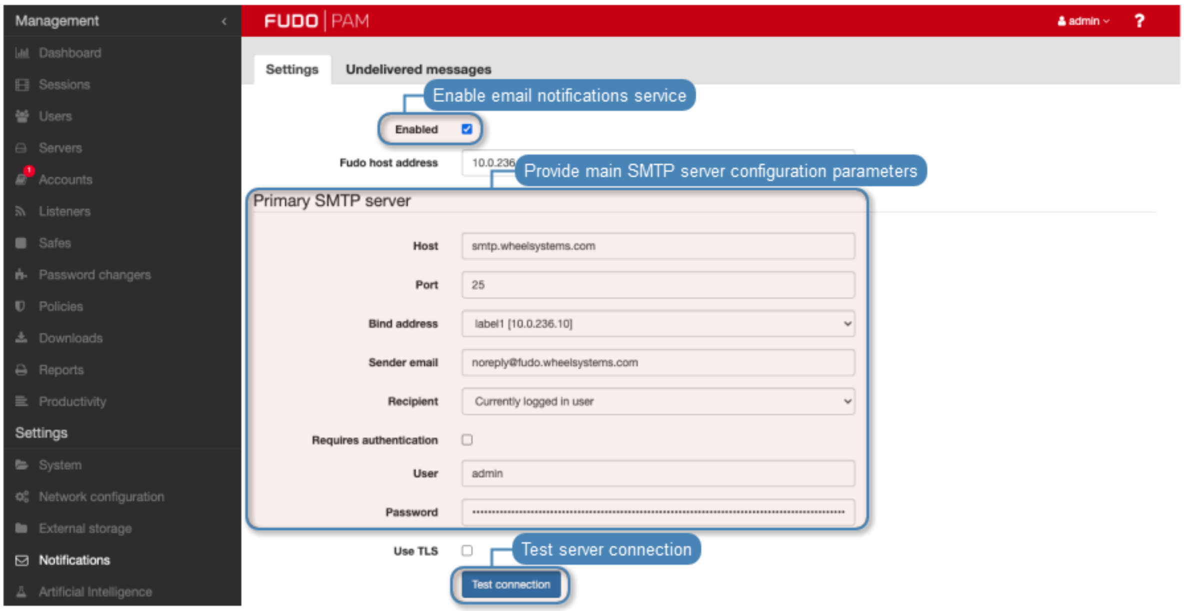
Email notifications service requires configuring SMTP server.

To configure SMTP server, proceed as follows.

1. Select *Settings > Notifications*.
2. Select *Enabled* option.
3. Input *Fudo host address*, which is a Fudo hostname or IP address that will be included in URLs within the sent notifications.

Note: *Fudo host address* is an address to manage notifications from Fudo. Its variable is required for correct configuration of the Session awaiting approval notifications. The variable is responsible for creating a link that will be sent to the user via e-mail for accepting the session.

4. Enter configuration parameters for the Primary SMTP server and optionally for the Secondary SMTP server.



Enable email notifications service

Enabled ☑

Fudo host address: 10.0.236

Provide main SMTP server configuration parameters

Primary SMTP server

Host: smtp.wheelsystems.com

Port: 25

Bind address: label1 [10.0.236.10]

Sender email: noreply@fudo.wheelsystems.com

Recipient: Currently logged in user

Requires authentication □

User: admin

Password: ••

Use TLS □

Test server connection

Parameter	Description
Host	SMTP server address, e.g. `smtp.gmail.com`.
Port	SMTP service port number.
Bind address	SMTP server IP address or interface address.
Sender email	Email address from which the emails will be sent.
Recipient	The recipient of the test message.
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. Additionally, select *Use STARTTLS* option to enable a secure connection.

Note: Click *Test connection* to make sure server parameters are correct.

5. Click ⬆ to upload a CA certificate. Choose the value to show in SHA1 or MD5 format.
6. Click *Save*.

Related Topics:

- *Accounts*

15.4 Artificial Intelligence

Note: *This is an evaluation version of the AI component.*

Fudo PAM creates individual, behavioral users profiles. Based on these, it can detect even the slightest change in their behavior and prevent a security breach.

15.4.1 Configuring models trainers

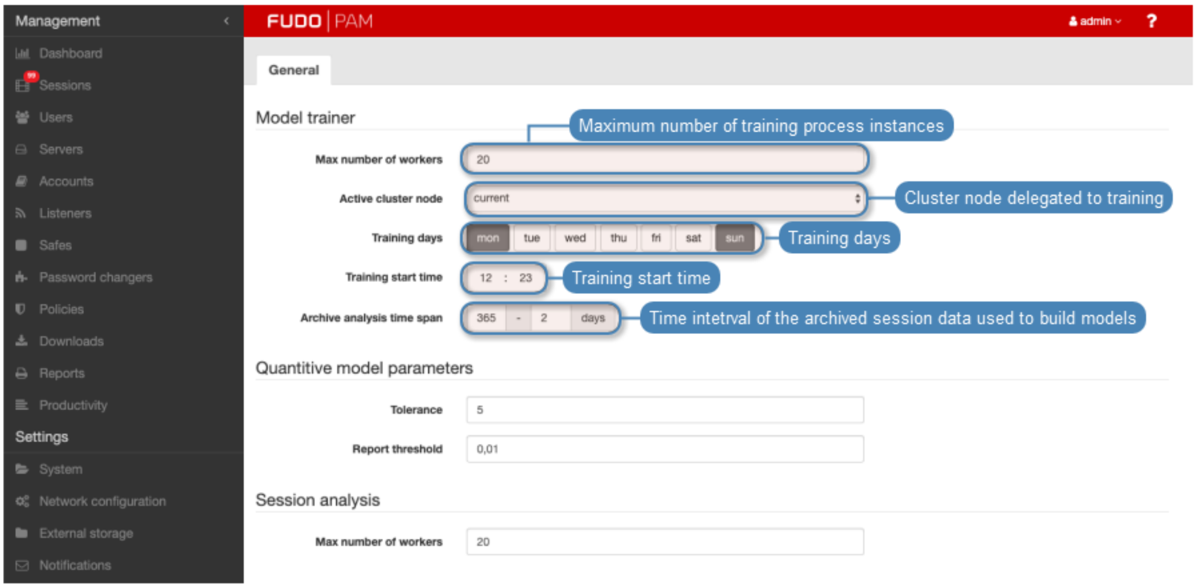
Training models requires processing power. Proper system configuration enables optimal processing of archived sessions while preserving overall system responsiveness in handling current user requests.

To change models trainers configuration, proceed as follows.

1. Select *Settings > Artificial Intelligence*.
2. In the *Model trainer* section, in the *Max number of training instances* field, define the number of processes delegated to constructing user profiles.

Note: Default value is the optimal value based on available hardware resources. The actual number of processes cannot be higher than the number of available CPU cores.

3. From the *Active cluster node* dropdown list, select the node responsible for training models.
4. Select weekdays when the training will take place.
5. Set the training start time.
6. Define the timespan of the data which will be processed to create models.



Model trainer

Max number of workers: 20

Active cluster node: current

Training days: mon tue wed thu fri sat sun

Training start time: 12 : 23

Archive analysis time span: 365 - 2 days

Maximum number of training process instances

Cluster node delegated to training

Training days

Training start time

Time intetrval of the archived session data used to build models

Quantitive model parameters

Tolerance: 5

Report threshold: 0,01

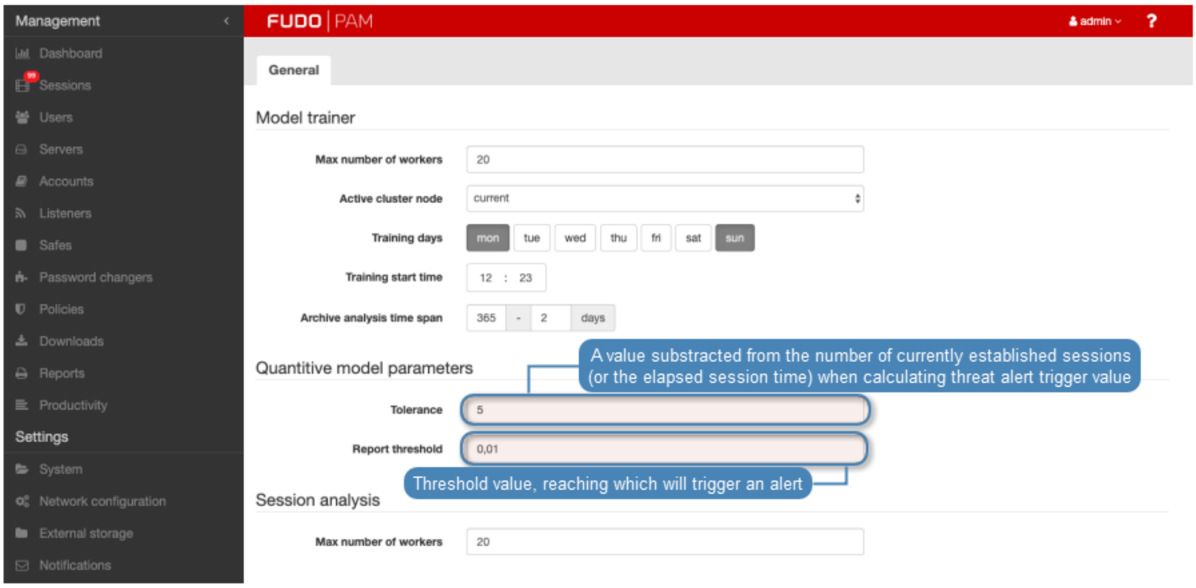
Session analysis

Max number of workers: 20

7. In the *Quantitive model parameters* section, in the *Tolerance* field, define allowed delta regarding the number of connections or the length of a single session.

Note: This parameter is used to calculate the threat risk which triggers the alert. Tolerance value is deducted from the current connections number or the number of minutes of elapsed session time. E.g. if the expected number of connections is 100, the current connection number is 109 and the tolerance value is set to 10, alarm will not be triggered as the calculated value (99) is less than the expected value.

8. In the *Report threshold* field, define the allowed deviation from the expected results.



Model trainer

Max number of workers: 20

Active cluster node: current

Training days: mon tue wed thu fri sat sun

Training start time: 12 : 23

Archive analysis time span: 365 - 2 days

Quantitive model parameters

A value substracted from the number of currently established sessions (or the elapsed session time) when calculating threat alert trigger value

Tolerance: 5

Report threshold: 0,01

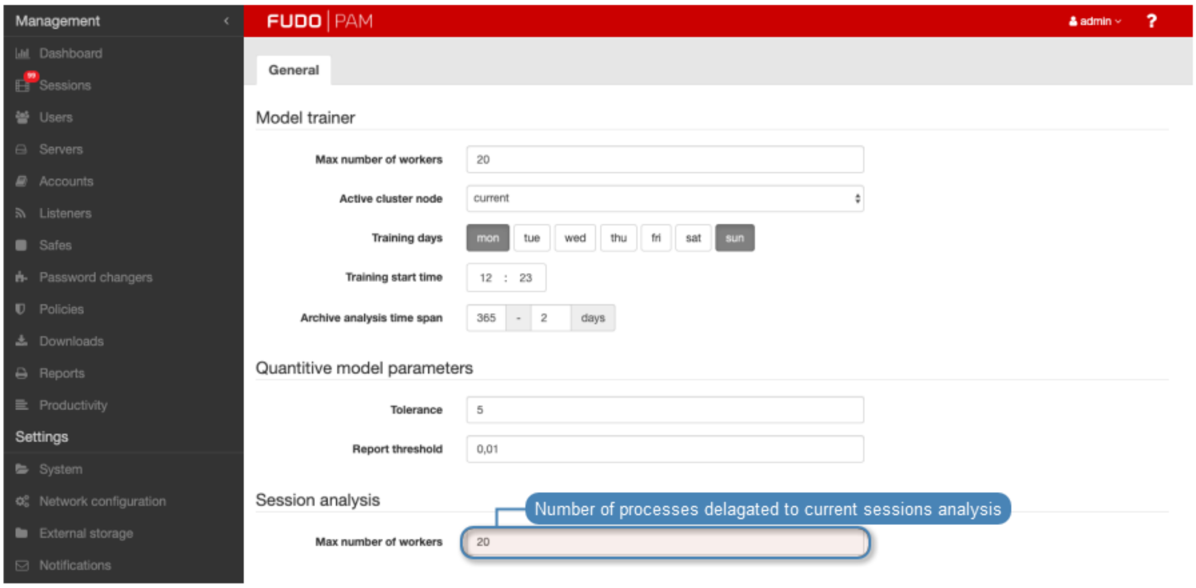
Threshold value, reaching which will trigger an alert

Session analysis

Max number of workers: 20

Note: Report threshold is defined in % and it determines the threshold value when the alert gets triggered on the account of too many sessions or a single connection lasting longer than expected. E.g. with the report threshold set to 1%, the alert will be triggered if the current number of connections has been observed before in 1% of cases.

9. In the *Session analysis* section, in the *Number of analyzing instances*, define the number of processes delegated to session analysis.



Model trainer

Max number of workers: 20

Active cluster node: current

Training days: mon tue wed thu fri sat sun

Training start time: 12 : 23

Archive analysis time span: 365 - 2 days

Quantitive model parameters

Tolerance: 5

Report threshold: 0,01

Session analysis

Number of processes delagated to current sessions analysis

Max number of workers: 20

Note: In case the pool of available data processing processes has been exhausted, online analysis is suspended. After the session is finished the data is picked up by the session analysis processes.

10. Click *Save*.

15.4.2 Configuring behavioral analysis models

Configuration parameters enable fine tuning behavioral models to match the specifics of your IT environment.

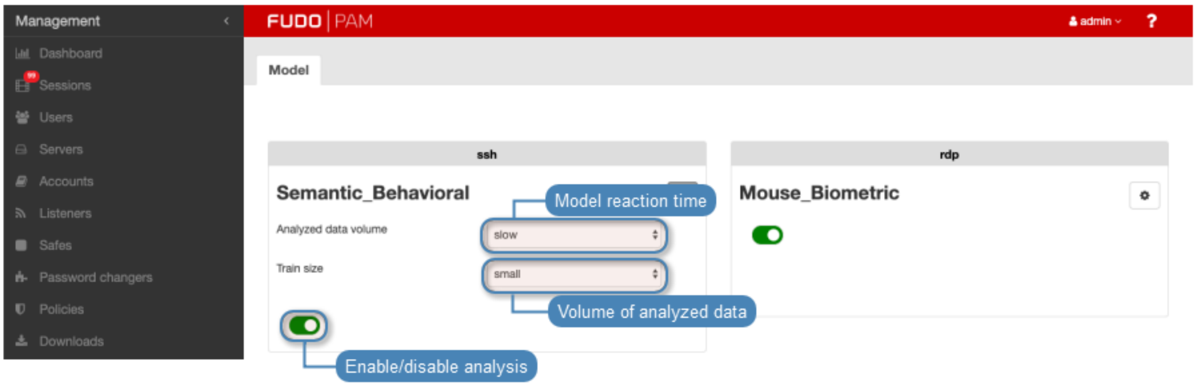
SSH

To change SSH model configuration, proceed as follows.

1. Select *Settings > Artificial Intelligence*.
2. Switch to the *Models* tab.
3. Click the ⚙ icon for the SSH model to display related configuration parameters.
4. From the *Reaction time* drop-down list, select how fast the system should react to delivered analysis results.

Note: Faster reaction time can potentially result in errors due to a smaller data sample.

5. From the *Analyzed data volume* drop-down list, select how much data will be used to build the model.



Semantic_Behavioral

Analyzed data volume: slow

Train size: small

Mouse_Biometric

5. Click *Save*.

RDP

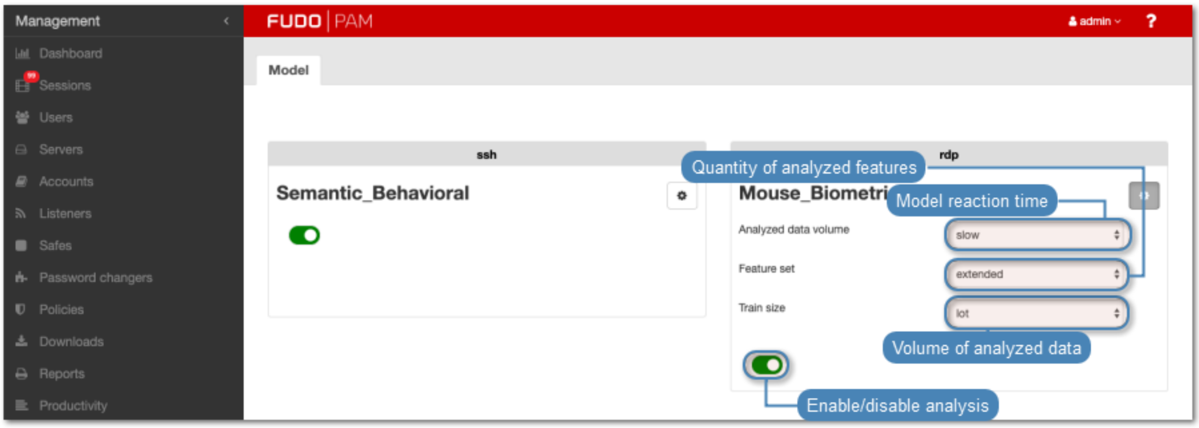
To change RDP model configuration, proceed as follows.

1. Select *Settings > Artificial Intelligence*.
2. Switch to the *Models* tab.
3. Click the ⚙ icon for the RDP model to display related configuration parameters.
4. From the *Reaction time* drop-down list, select how fast the system should react to delivered analysis results.

Note: Faster reaction time can potentially result in errors due to a smaller data sample.

5. From the *Analyzed data volume* drop-down list, select how much data will be used to build the model.
6. From the *Feature set* drop-down list, select how much features should be analyzed.

Note: Feature set determines the collection of features being analyzed. It directly influences the accuracy and the time it takes to construct the model. Analyzing extended feature set will result in a more detailed model but it will take longer to build it.



Semantic_Behavioral

Mouse_Biometri

Analyzed data volume: slow

Feature set: extended

Train size: lot

Quantity of analyzed features

Model reaction time

Volume of analyzed data

Enable/disable analysis

7. Click *Save*.

Related topics:

- *Sessions*
- *AI sessions processing*

15.5 Trusted time-stamping

A trusted timestamp makes recorded session a more convincing evidence in court.

Prerequisites

- Trusted time-stamping feature requires signing a contract with an institution providing time-stamping services.
- Certificate and private key issued by the time-stamping service provider.
- KIR time-stamping service requires a DNS server to be configured. Refer to the *DNS configuration* topic for more information on adding DNS servers.
- Fudo PAM must be able to reach the `http://www.ts.kir.com.pl/HttpTspServer` web address in case of the KIR time-stamping service.
- Fudo PAM must be able to reach the `193.178.164.5` IP address in case of the PWPW time-stamping service.

Enabling and configuring trusted time-stamping

Note: Fudo PAM will also time-stamp sessions recorded before the feature was enabled.

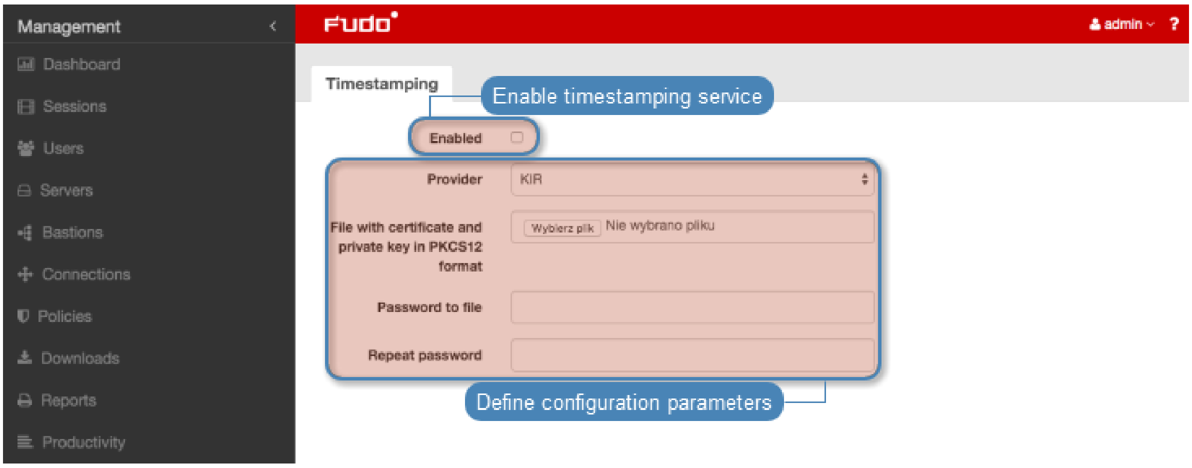
1. Select *Settings > Trusted Timestamping*.
2. Select *Enabled* option.

3. Select from the *Provider* drop-down list the institution providing trusted time-stamping services.

4. Provide the certificate and the private key of the time-stamping service.

Note: You should receive these information from your time-stamping service provider.

5. Click *Save*.



Enable timestamping service

Enabled ☐

Provider: KIR

File with certificate and private key in PKCS12 format: Wybierz plik Nie wybrano pliku

Password to file:

Repeat password:

Define configuration parameters

Related topics:

- *Security measures*

15.6 External authentication

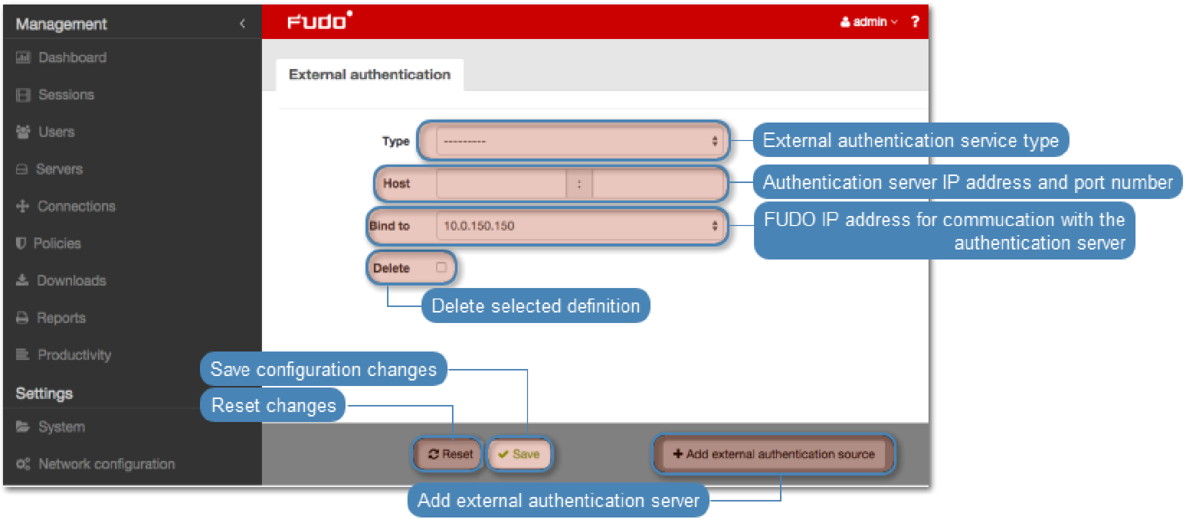
Some of the authentication methods, require defining connections to external authentication servers. These are:

- *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*.


Management
Dashboard
Sessions
Users
Servers
Connections
Policies
Downloads
Reports
Productivity
Settings
System
Network configuration
Fudo
admin
External authentication
Type
Host
Bind to
10.0.150.150
Delete
Reset
Save
+ Add external authentication source
External authentication service type
Authentication server IP address and port number
FUDO IP address for commucation with the authentication server
Delete selected definition
Save configuration changes
Reset changes
Add external authentication server

Adding a new external authentication server

To add an external authentication server, proceed as follows.

1. Select *Settings > External authentication*.
2. Click *+ Add external authentication source*.
3. Select authentication service type.
4. Provide configuration parameters depending on selected authentication system type.

Parameter	Description
CERB	
Host	Server's IP address.
Port	Port used to establish connections with given server.
Bind address	IP address used for sending requests to given host.
Secret	Secret used to establish server connection.
Service	CERB service used for authenticating Fudo PAM users.
RADIUS	
Host	Server's IP address.
Port	Port used to establish connections with given server.
Bind address	IP address used for sending requests to given host.
Secret	Secret used to establish server connection.
NAS ID	RADIUS server NAS-Identifier parameter.
LDAP	
Host	Server's IP address.
Port	Port used to establish connections with given server.
Bind address	IP address used for sending requests to given host.
User DN template	Template containing a path which will be used to create queries to LDAP server.
Active Directory	
Host	Server's IP address.
Port	Port used to establish connections with given server.
Bind address	IP address used for sending requests to given host.
Domain	Domain which will be used for authenticating users in Active Directory.

Note: Labeled IP addresses

In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

5. Click *Save*.

Editing authentication server definition

To edit an authorization server definition, proceed as follows.

1. Select *Settings > External authentication*.
2. Find the server definition and change its configuration as desired.
3. Click *Save*.

Deleting authentication server definition

To delete authentication server definition, proceed as follows.

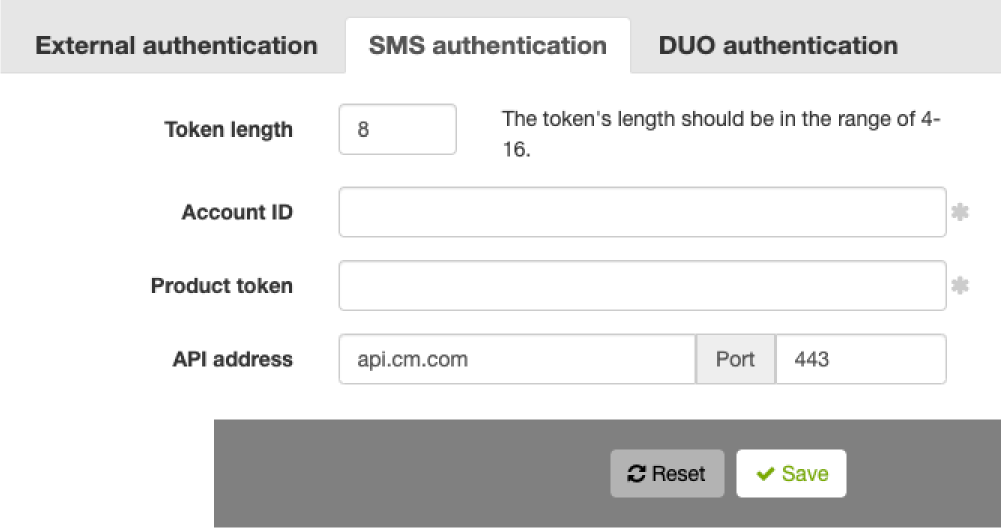
1. Select *Settings > External authentication*.
2. Find desired server definition and select the *Delete* option.
3. Click *Save*.

Another two external authentication methods that require configuration are:

- SMS,
- DUO.

SMS authentication definition

1. Select *Settings > External authentication*.
2. Choose **SMS Authentication** tab.



Token length: 8 — The token's length should be in the range of 4-16.

Account ID: *

Product token: *

API address: api.cm.com Port 443

3. Input *Token length*.

Note: The token's length should be in the range of 4-16.

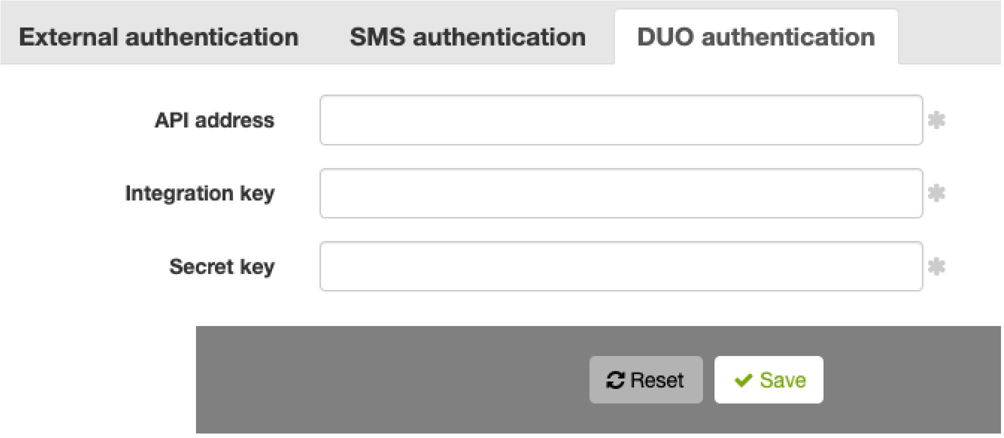
4. Input *Account ID*.
5. Input *Product token*.
6. Input *API address* and its *port*.

Note: The values for *Account ID*, *Product token* and *API address* are given by CM.COM service. You need to have a registered account there to be able to obtain the required information.

7. Go to *Management > Users*.
8. Find and select the user for whom you want to enable SMS authentication
9. Input a phone number in the **Phone** input field.
10. Under **Authentication** section choose *Type: SMS*
11. From a **First factor** drop-down list choose *Static password* and *External authentication* (AD or LDAP).
12. Click *Save*.
13. Log in to the portal with SMS code.

DUO authentication definition

1. Download and install Duo Mobile phone application.
2. Sign up for a personal account on Duo Security.
3. Select *Settings > External authentication* for DUO Authentication configuration.
4. Choose **DUO Authentication** tab.
5. Input from the personal Duo Security profile: *API address*, *Integration key* and *Secret key*.



6. Go to *Management > Users*.
7. Find and select the user for whom you want to enable DUO authentication.

8. Under **Authentication** section choose *Type: DUO*.
9. From a **First factor** drop-down list choose *Static password* or *External authentication* (AD or LDAP).
10. Input *DUO username*.
11. Input *DUO user id*.
12. Click *Save*.
13. Log in to the portal by tapping Accept on push notification from Duo Mobile application.

Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

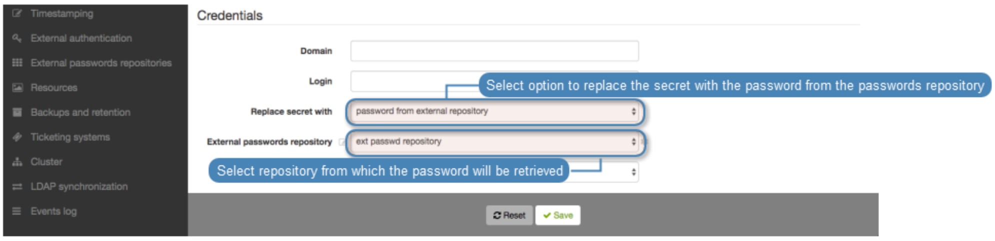
15.7 External passwords repositories

Fudo PAM supports external passwords repositories for managing passwords to monitored servers.

15.7.1 CyberArk Enterprise Password Vault

Adding a new passwords repository

1. Select *Settings > External passwords repositories*.
2. Click *+ Add server*.
3. Select `CyberArk Enterprise Password Vault` from the *Type* drop-down list.
4. Enter object's name.
5. Provide the URL to the passwords server's API.
6. Provide application identification.
7. Define the account format string.
8. Click *Save*.
9. Assign external password repository to an account.
    - Select *Management > Accounts*.
    - Browse objects and click an account to access the settings form.
    - In the *Credentials* section, select *password from external repository* from the *Replace secret with* drop-down list.
    - From the *External passwords repository* select one of the previously defined password repository.



Credentials

Domain

Login

Replace secret with: password from external repository

External passwords repository: ext passwd repository

Select option to replace the secret with the password from the passwords repository

Select repository from which the password will be retrieved

- Click *Save*.

Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

1. Select *Settings > External passwords repositories*.
2. Find the repository definition and change its configuration as desired.
3. Click *Save*.

Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

1. Select *Settings > External passwords repositories*.
2. Find desired repository definition and select the *Delete* option.
3. Click *Save*.

Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

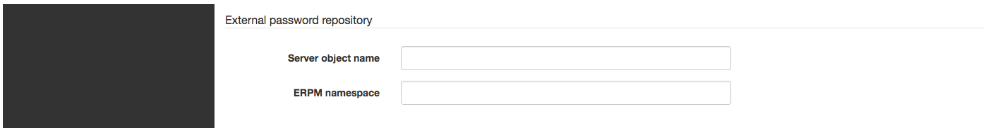
15.7.2 Hitachi ID Privileged Access Manager

Adding a new passwords repository

1. Select *Settings > External passwords repositories*.
2. Click *+ Add server*.
3. Select `Hitachi ID Privileged Access Manager` from the *Type* drop-down list.
4. Enter object's name.
5. Provide the URL to the passwords server's API.
6. Enter user login allowed to access passwords directory.
7. Provide user password in the *Password* and *Repeat password* fields.
8. Click *Save*.
9. Define server's object name and *ERPM namespace* in the *External password repository* sections.

    - Select *Management > Servers*.
    - Browse object and click an server to access the settings form.

- In the *External password repository* section, provide the *Server object name* and *ERPM namespace*.



External password repository

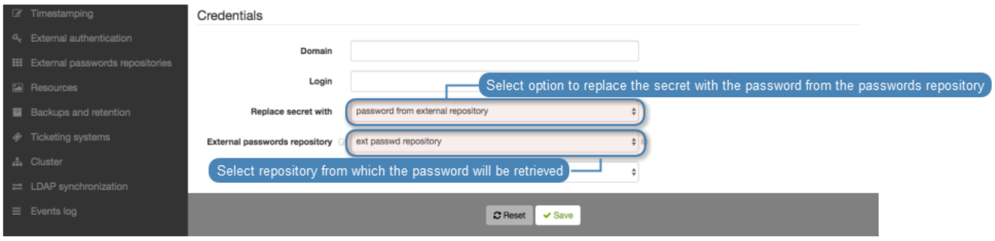
Server object name

ERPM namespace

- Click *Save*

10. Assign external password repository to an account.

    - Select *Management > Accounts*.
    - Browse objects and click an account to access the settings form.
    - In the *Credentials* section, select *password from external repository* from the *Replace secret with* drop-down list.
    - From the *External passwords repository* select one of the previously defined password repository.



Credentials

Domain

Login

Replace secret with: password from external repository

External passwords repository: ext passwd repository

Select option to replace the secret with the password from the passwords repository

Select repository from which the password will be retrieved

- Click *Save*.

Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

1. Select *Settings > External passwords repositories*.
2. Find the repository definition and change its configuration as desired.
3. Click *Save*.

Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

1. Select *Settings > External passwords repositories*.
2. Find desired repository definition and select the *Delete* option.
3. Click *Save*.

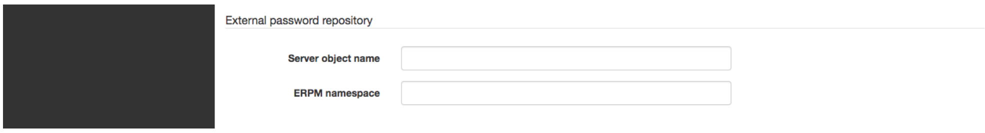
Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

15.7.3 Lieberman Enterprise Random Password Manager

Adding a new passwords repository

1. Select *Settings > External passwords repositories*.
2. Click *+ Add server*.
3. Select `Lieberman Enterprise Random Password Manager` from the *Type* drop-down list.
4. Enter object's name.
5. Provide the URL to the passwords server's API.
6. Define authention module assigned to the user who is allowed to access passwords repository.
7. Enter user login allowed to access passwords repository.
8. Provide user password in the *Password* and *Repeat password* fields.
8. Click *Save*.
9. Define server's object name and *ERPM namespace* in the *External password repository* sections.
    - Select *Management > Servers*.
    - Browse object and click an server to access the settings form.
    - In the *External password repository* section, provide the *Server object name* and *ERPM namespace*.

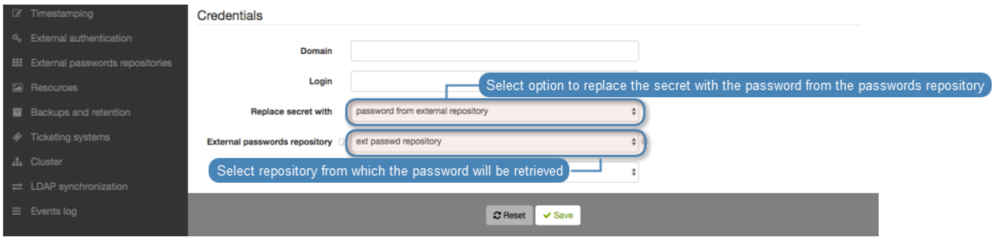


External password repository

Server object name

ERPM namespace

    - Click *Save*
10. Assign external password repository to an account.
    - Select *Management > Accounts*.
    - Browse objects and click an account to access the settings form.
    - In the *Credentials* section, select *password from external repository* from the *Replace secret with* drop-down list.
    - From the *External passwords repository* select one of the previously defined password repository.



Credentials

Domain

Login

Replace secret with: password from external repository

External passwords repository: ext passwd repository

Select option to replace the secret with the password from the passwords repository

Select repository from which the password will be retrieved

    - Click *Save*.

Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

1. Select *Settings > External passwords repositories*.
2. Find the repository definition and change its configuration as desired.
3. Click *Save*.

Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

1. Select *Settings > External passwords repositories*.
2. Find desired repository definition and select the *Delete* option.
3. Click *Save*.

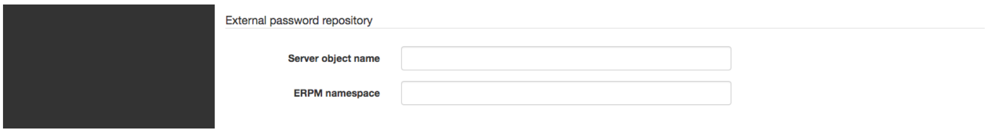
Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

15.7.4 Thycotic Secret Server

Adding a new passwords repository

1. Select *Settings > External passwords repositories*.
2. Click *+ Add server*.
3. Select `Thycotic Secret Server` from the *Type* drop-down list.
4. Enter object's name.
5. Provide the URL to the paswords server's API.
6. Enter user login allowed to access passwords repository.
7. Provide user password in the *Password* and *Repeat password* fields.
8. Define secret string format used for identifying objects on Thycotic Secret Server.
8. Click *Save*.
9. Define server's object name and *ERPM namespace* in the *External password repository* sections.
   - Select *Management > Servers*.
   - Browse object and click an server to access the settings form.
   - In the *External password repository* section, provide the *Server object name* and *ERPM namespace*.



External password repository

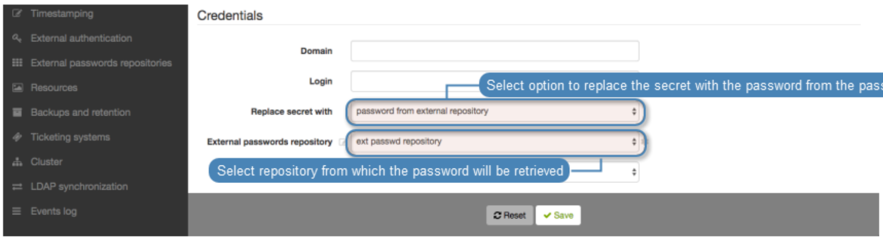
Server object name

ERPM namespace

- Click *Save*

10. Assign external password repository to an account.

    - Select *Management* > *Accounts*.
    - Browse objects and click an account to access the settings form.
    - In the *Credentials* section, select *password from external repository* from the *Replace secret with* drop-down list.
    - From the *External passwords repository* select one of the previously defined password repository.



Credentials

Domain

Login

Replace secret with: password from external repository

External passwords repository: ext passwd repository

Select option to replace the secret with the password from the passwords repository

Select repository from which the password will be retrieved

- Click *Save*.

Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find the repository definition and change its configuration as desired.
3. Click *Save*.

Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

1. Select *Settings* > *External passwords repositories*.
2. Find desired repository definition and select the *Delete* option.
3. Click *Save*.

Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

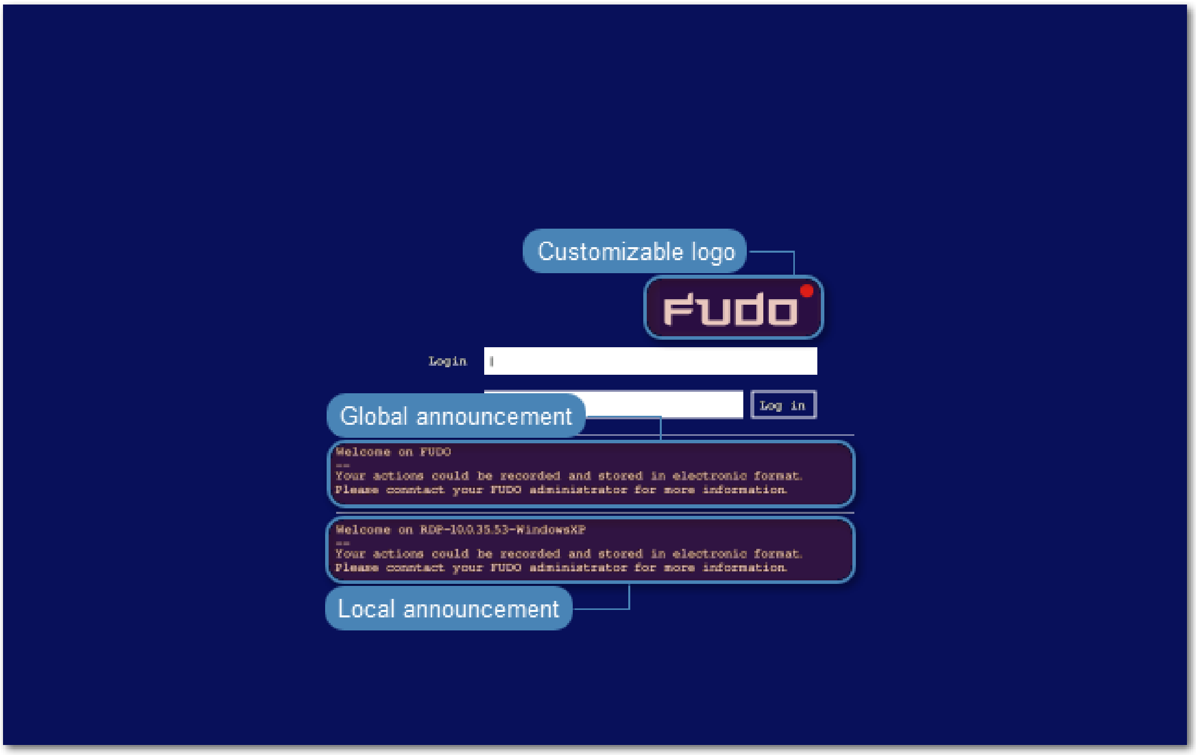
Related topics:

- *User authentication methods and modes*
- *System overview*
- *Integration with CERB server*

15.8 Resources

15.8.1 RDP/VNC login screen configuration

Fudo PAM enables customizing RDP and VNC login screen.



```
Welcome on FUDO
--
Your actions could be recorded and stored in electronic format.
Please contact your FUDO administrator for more information.
```

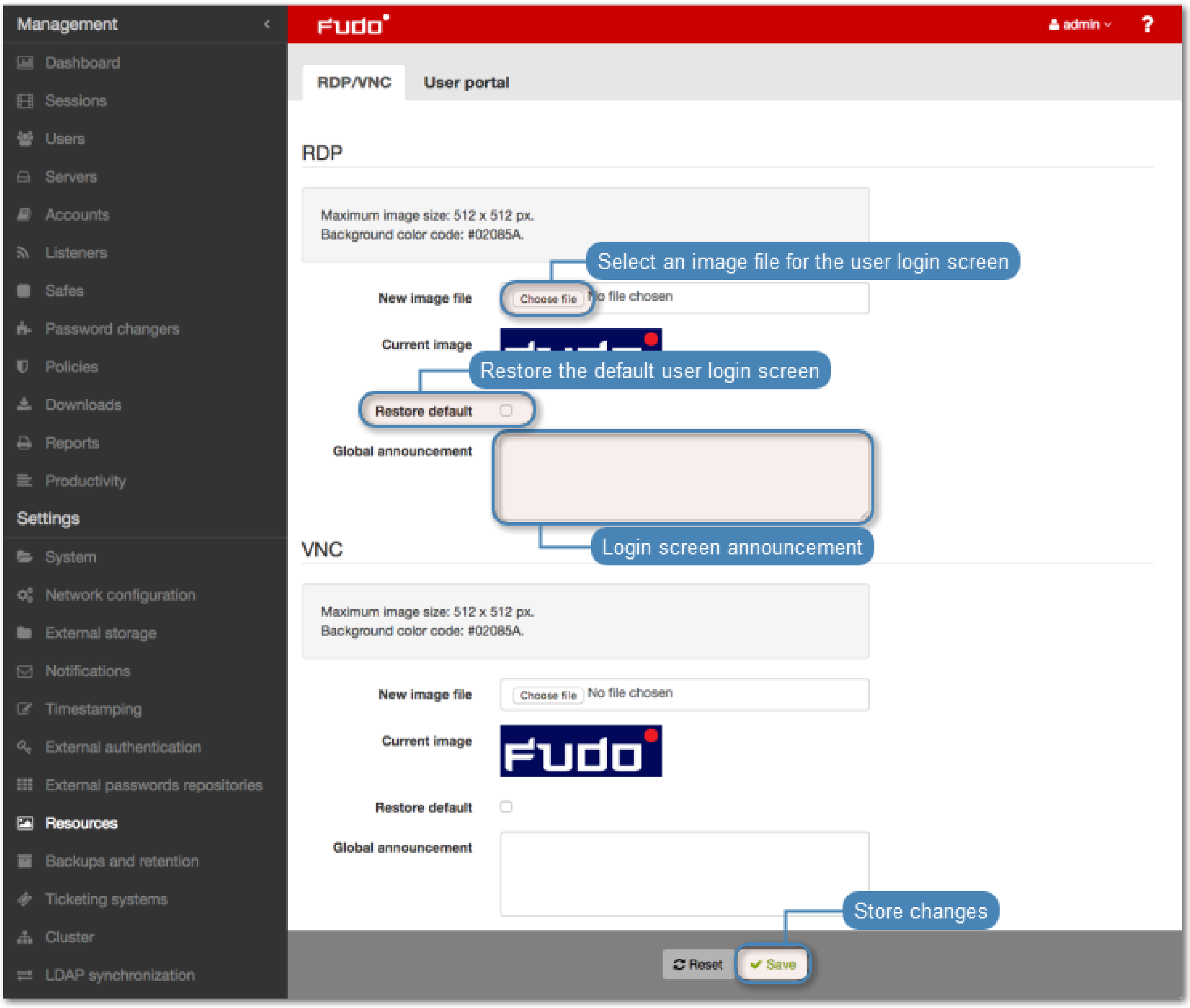
```
Welcome on RDP-10.0.35.53-WindowsXP
--
Your actions could be recorded and stored in electronic format.
Please contact your FUDO administrator for more information.
```

Changing logo

1. Select *Settings > Resources*.
2. Select the *RDP/VNC* tab.
3. In the *RDP* or *VNC* section, click *Choose File* button and select desired image.

Note: Maximum image size is 512 x 512 px.

4. Click *Save*.



Maximum image size: 512 x 512 px.
Background color code: #02085A.

Maximum image size: 512 x 512 px.
Background color code: #02085A.

Select an image file for the user login screen

Restore the default user login screen

Login screen announcement

Store changes

Restoring default logo

1. Select *Settings* > *Resources*.
2. Select *RDP/VNC* tab.
3. In the *RDP* or *VNC* section, select *Restore default* option.
4. Click *Save*.

Defining global announcement

Global announcement is displayed on RDP and VNC login screen.

Note: Apart from global announcement, Fudo PAM also enables configuring local server message in server configuration form.

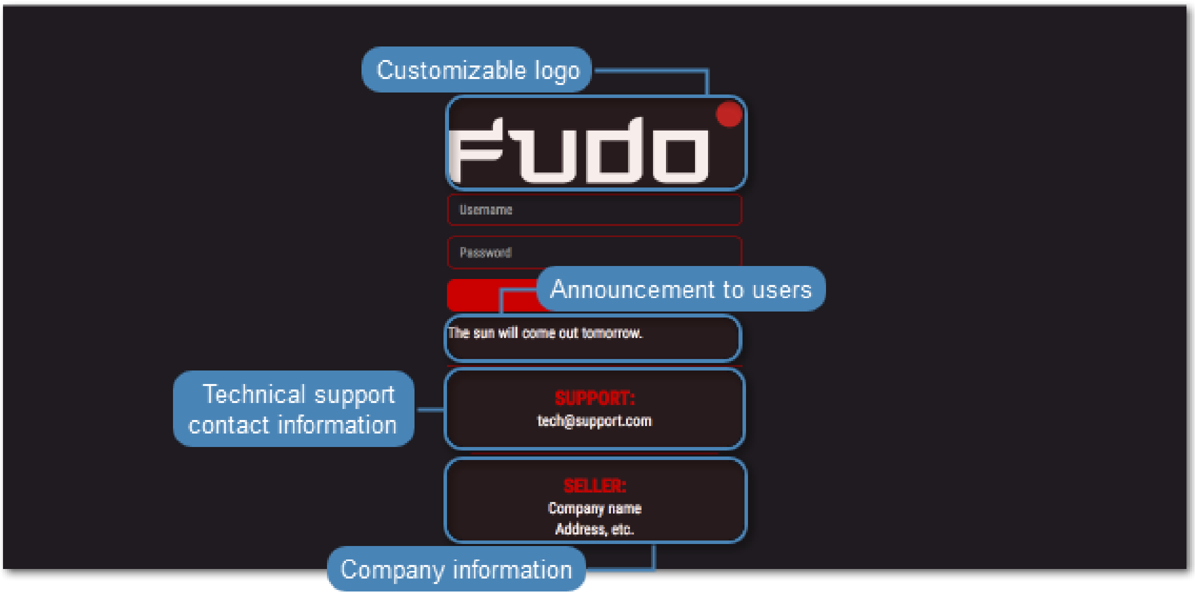
1. Select *Settings* > *Resources*.
2. Select *RDP/VNC* tab.
3. In the *RDP* or *VNC* section, enter desired message in the *Global announcement* field.
4. Click *Save*.

Related topics:

- *Quickstart - RDP*

15.8.2 *User portal* login screen configuration

Fudo PAM enables customizing information displayed on the *User portal* login screen.



1. Select *Settings* > *Resources*.
2. Select the *User portal* tab.
3. In the *User Portal login screen logo* section, click *Choose file*, browse the file system and select a custom logo for the *User portal* login screen.

Note: Maximum image size is 512 x 512 px.

4. Provide company information.

Note: Company information can be five lines, up to 70 characters.

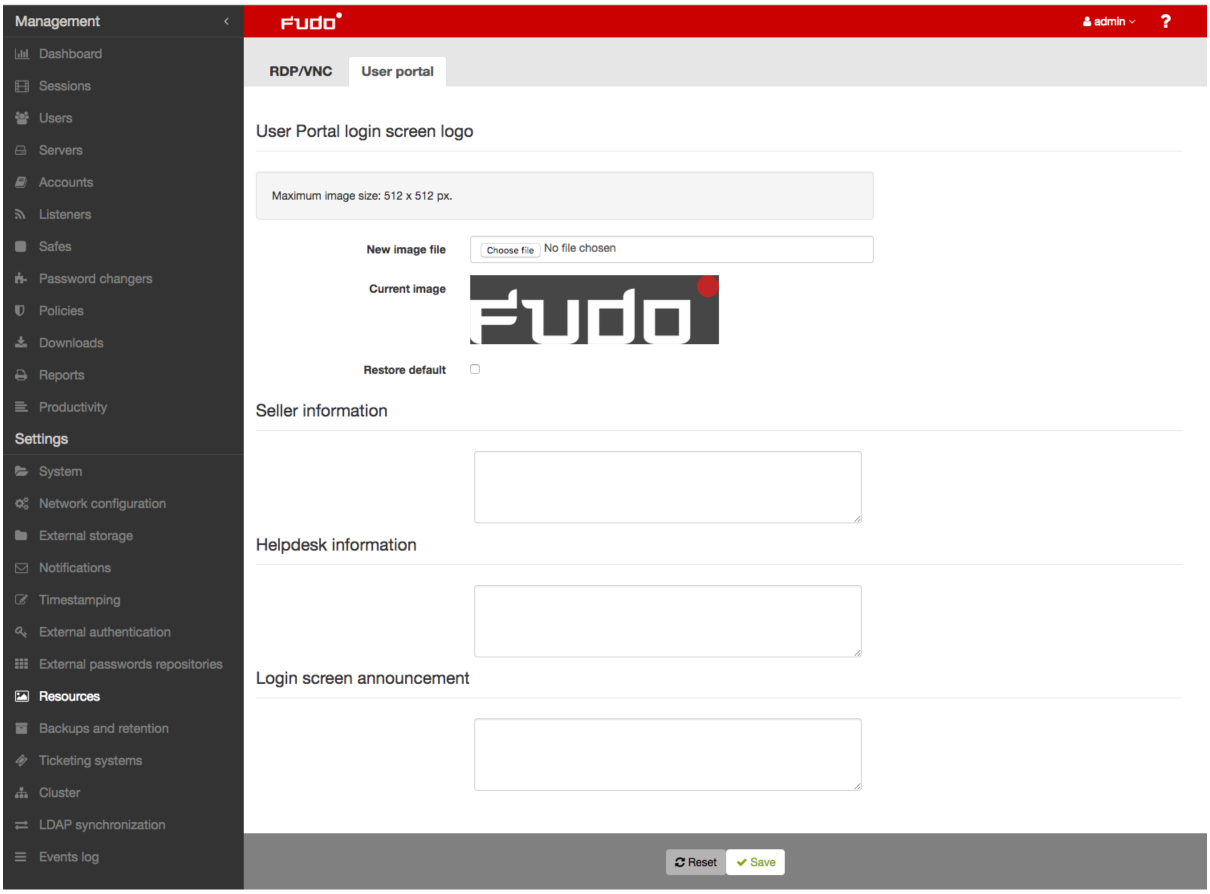
5. Enter help desk contact information.

Note: Helpdesk contact information can be five lines, up to 70 characters.

6. Provide the login screen announcement.

Note: Login screen announcement can be four lines, up to 120 characters.

7. Click *Save*.



User Portal login screen logo

Maximum image size: 512 x 512 px.

New image file: No file chosen

Current image

Restore default □

Seller information

Helpdesk information

Login screen announcement

Related topics:

- *User portal*

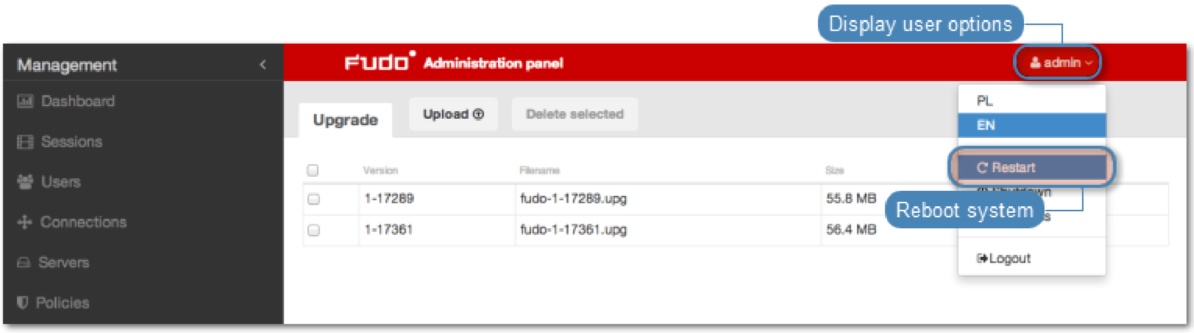
15.9 System version restore

In the case there is a problem with the current system revision, it is possible to restore the system to its previous version.

> **Warning:** Restoring the system to the previous version will bring back the system's state prior the update. Session data and configuration changes in the current system revision will be lost.

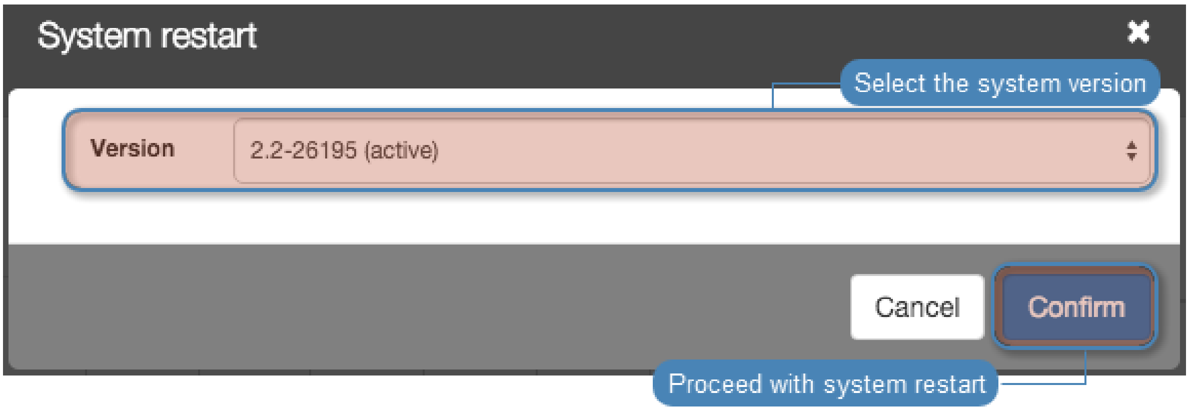
To restore the system to the previous revision, proceed as follows.

1. Connect one of the USB flash drives containing the encryption key.
2. Select *Restart* from user options menu.



3. Select the previous system revision to be loaded after restarting the system.

Note: Current system version is selected by default.



4. Click *Confirm* to proceed with restarting the system to the selected revision.

Warning: Restrating the system will terminate all current users' connections.

Related topics:

- *System initiation*
- *System update*

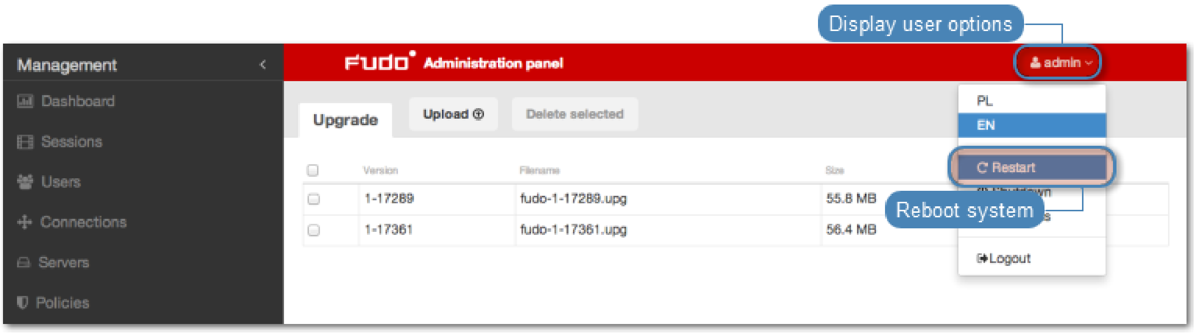
15.10 System restart

Note:

- System restart requires USB flash drive with the encryption key connected to the device.
- Restrating the system will terminate all current users' connections.
- Use the *Deny new connections* option in the *Sessions* section in the system settings menu.

1. Connect one of the USB flash drives containing the encryption key.

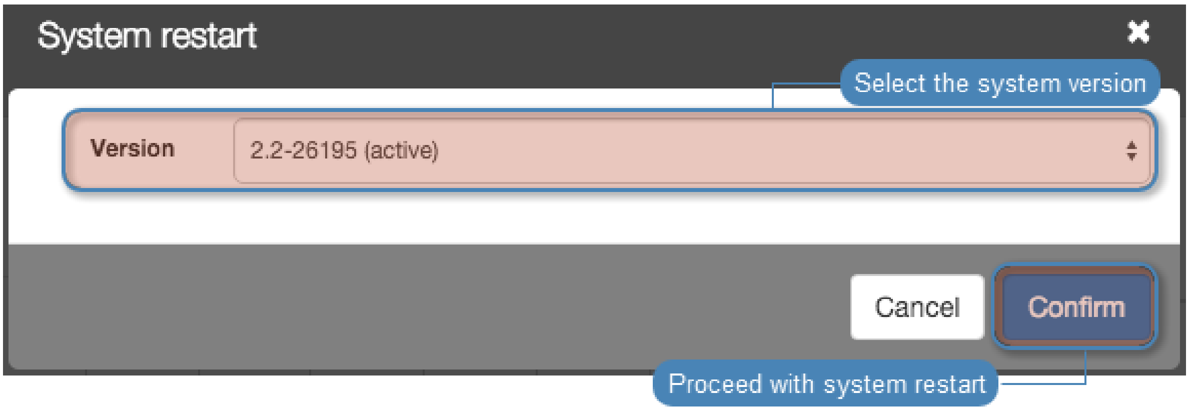
2. Select *Restart* from user options menu.



	Version	Filename	Size
□	1-17289	fudo-1-17289.upg	55.8 MB
□	1-17361	fudo-1-17361.upg	56.4 MB

3. Select the previous system revision to be loaded after restarting the system.

Note: Current system version is selected by default.



Version: 2.2-26195 (active)

4. Click *Confirm* to proceed with restarting the system to the selected revision.

Related topics:

- *System initiation*
- *System version restore*

15.11 SNMP

Fudo PAM's status can be monitored over SNMPv3 protocol.

15.11.1 Configuring SNMP

1. Select *Settings > System*.
2. Select *SNMPv3* option in the *Maintenance and supervision* section.
3. From the *IP address* drop-down list select IP address, which will be used for SNMP communication.
4. Click *Save*.

5. Select *Management > Users*.
6. Click *+ Add*.
7. Select `service` from the *Role* drop-down list and fill in the rest of the *General* section parameters.
8. Select `password` from the *Authentication* drop-down list and enter the password string.

Note:

- SNMP user password must be at least eight characters long.
- SNMP service authenticates the service account using the first defined password.

9. Select *Enabled* option in the *SNMP* section.
10. Select authentication methods from the *Authentication method* drop-down list.
11. Select the SNMP encryption algorithm from the *Encryption* drop-down list.
12. Clikc *Save*.

15.11.2 SNMP MIBs

Fudo PAM supports following MIBs:

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790) - partly supported
- UCD-SNMP-MIB

15.11.3 Getting SNMP readings using `snmpwalk`

Note: Getting SNMP readings requires installing *Net-SNMP 5.7.3*.

Fetching all SNMP information

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}"          -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1
```

Fetching specific SNMP information

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}"          -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1.3.6.1.4.1.24410
```

Data specifier	Description
.1.3.6.1.4.1.24410.1.1.1	Disk status (ZFS status)
.1.3.6.1.4.1.24410.1.1.2	Power supply status **Note:** This feature is not supported on all Fudo PAM units. Contact technical support for more information.
.1.3.6.1.4.1.24410.1.1.3	CPU temperatures
.1.3.6.1.4.1.24410.1.1.4	S.M.A.R.T status

15.11.4 Fudo PAM specific SNMP extensions

Overview

Extensions enable monitoring the number of active sessions, ZFS status, PSU status (if available), CPU temperature on all cores, S.M.A.R.T status such as temperature, health or reallocated sectors.

MIB specification file

The following MIB files can be uploaded to the SNMP manager to enable Fudo PAM specific SNMP extensions.

Warning: The MIB files names has changed in Fudo PAM 4.3. Make sure to replace the old files with the new definitions.

FUDO-SECURITY-COMMON-MIB

FUDO-SECURITY-FUDO-MIB

Related topics:

- *Security measures*
- *Troubleshooting*

15.12 Backups and retention

Data retention

Fudo PAM implements two stage data retention. First data is moved from the internal storage to the external storage connected over fiber channel interface. After defined time period session data is automatically deleted.

Note: Sessions which have been exported and the content is still available for download, will not be deleted automatically. These sessions must be either *deleted manually* or you must delete the exported material in the *Downloads* section for the retention mechanism to delete those session.

To enable data retention service, proceed as follows.

1. Select *Settings > Backups and retention.*
2. Select *Moving session data to external storage enabled* option in the *Data retention* section.
3. Define how long data will be stored locally before it is moved to the external storage.
4. Select *Session data removal enabled* option to have the data automatically removed after specified time period.
5. Define how long data will be stored before being deleted.

Note:

- Global retention parameter values have lower priority than the values set in the *accounts*.
- Global retention settings are replicated within the *cluster configuration*.

6. Click *Save.*

System backup

Warning: Data backup contains confidential information.

Data stored on Fudo PAM can be backed up on an external server running `rsync` service. Backup service has to be enabled on Fudo PAM and requires uploading external server's public SSH key, to authorize access to Fudo PAM.

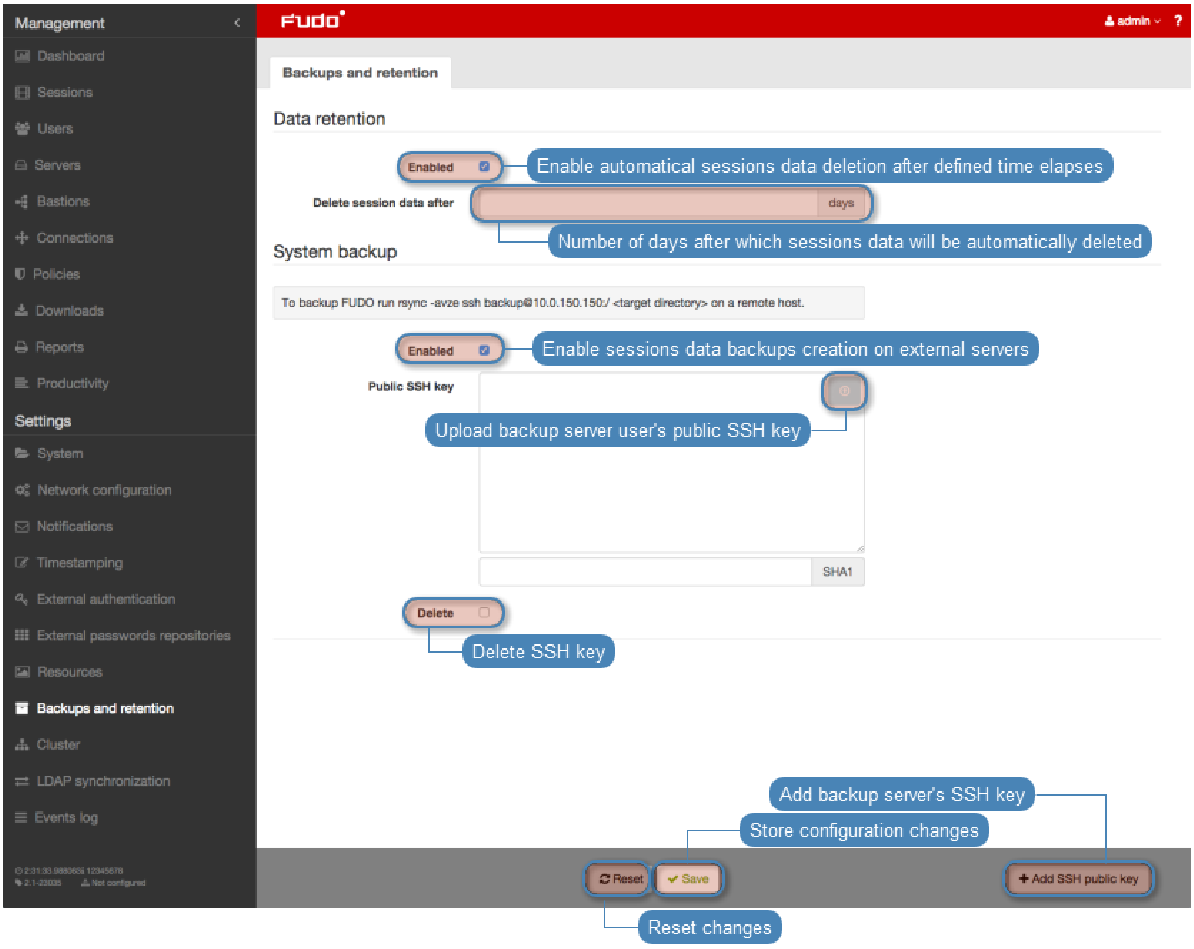
Automated data backup requires configuring `rsync` service on a remote server and granting access rights to data stored on Fudo PAM by uploading to Fudo PAM server's public SSH key.

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 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>
```



Data retention

Enabled ☑

Delete session data after ___ days

System backup

To backup FUDO run rsync -avze ssh backup@10.0.150.150:/ <target directory> on a remote host.

Enabled ☑

Public SSH key

Enable automatical sessions data deletion after defined time elapses

Number of days after which sessions data will be automatically deleted

Enable sessions data backups creation on external servers

Upload backup server user's public SSH key

Delete SSH key

Add backup server's SSH key

Store configuration changes

Reset changes

Restoring system from backup

System restore service is provided by the technical support department on terms agreed in the SLA.

Related topics:

- *Exporting/importing system configuration*
- *Security measures*

15.13 External storage

Fudo PAM enables storing session data on external storage devices connected to Fudo through a fiber channel interface.

Note: External storage in cluster configuration

- In cluster configuration, each node must have a dedicated *WWN* object.
- Data stored externally is not replicated between cluster nodes.

15.13.1 Configuring external storage

1. Select *Settings* > *External storage*.

Note: Fiber channel cards status is depicted by the icons.

- 🟩 - both fiber channel cards are operational.
- 🟨 - external storage volume is degraded - one of the fiber channel card is down.
- 🟥 - both fiber channel cards are down.

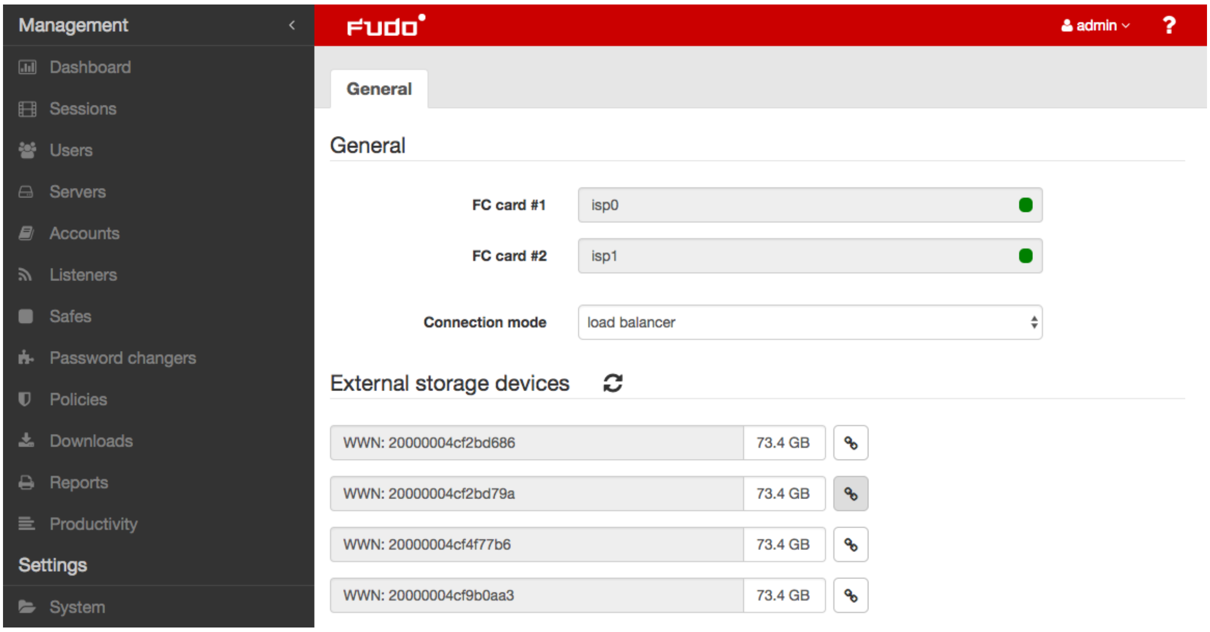
---

2. Select fiber channel cards operating mode.
   - Failover - data is transmitted using one fiber channel interface. If the card fails, the other one takes over ensuring continuous availability of the external storage device.
   - Load balancing - both fiber channel interfaces are used to transfer data between Fudo PAM and the external storage device.
3. In the *External storage devices* section, select desired *WWN* object and click the 🔗 icon.

Note: Click the 🔄 icon to refresh the list of available storage devices.

---

4. Click *Save* and proceed with enabling *session data retention*.



General

FC card #1: isp0 🟩

FC card #2: isp1 🟩

Connection mode: load balancer

External storage devices 🔄

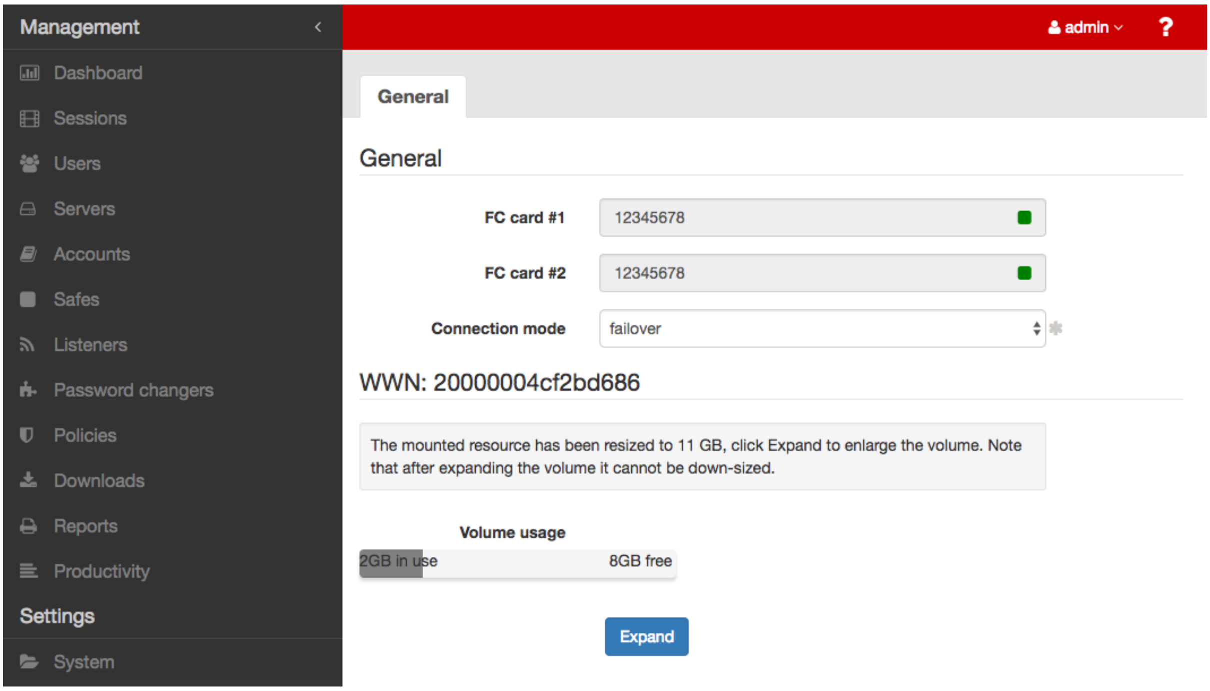
WWN: 20000004cf2bd686	73.4 GB	🔗
WWN: 20000004cf2bd79a	73.4 GB	🔗
WWN: 20000004cf4f77b6	73.4 GB	🔗
WWN: 20000004cf9b0aa3	73.4 GB	🔗

15.13.2 Expanding external storage device

After resizing the WWN object, it must be expanded in Fudo PAM in order to take advantage of the additional storage space.

Warning: The storage device cannot be down-sized after it has been expanded.

1. Select *Settings* > *External storage*.
2. In the section describing the *WWN* object click *Expand*.



General

FC card #1: 12345678 🟩

FC card #2: 12345678 🟩

Connection mode: failover

WWN: 20000004cf2bd686

The mounted resource has been resized to 11 GB, click Expand to enlarge the volume. Note that after expanding the volume it cannot be down-sized.

Volume usage: 2GB in use 8GB free

3. Confirm expanding external storage.
4. Click *Save*.

Related topics:

- *Backups and retention*

15.14 Exporting/importing system configuration

Fudo PAM enables exporting current system state, defined objects and configuration settings, which later can be used to initiate the system.

Warning: Exported configuration data contains confidential information.

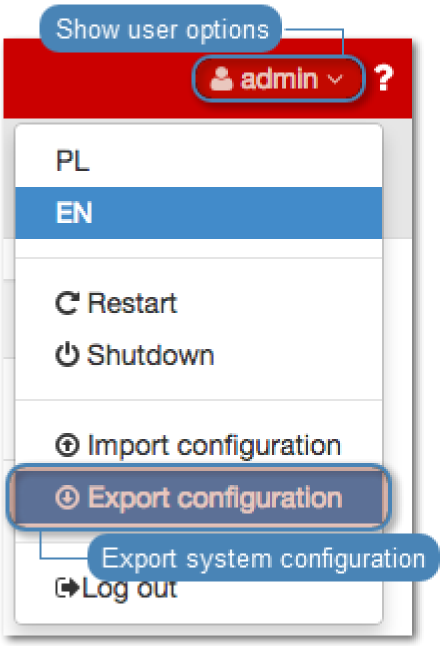
Note: Configuration export and import options are available only for the *superadmin* users.

15.14.1 Exporting system configuration

To export system configuration, proceed as follows.

1. Select *Export configuration* from the user menu.

2. Save the configuration file.



15.14.2 Importing system configuration

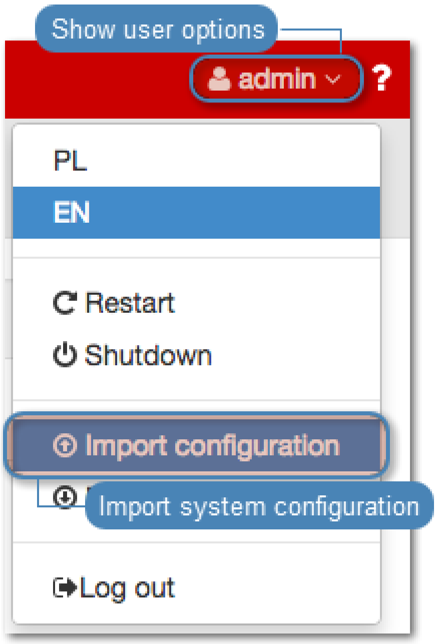
Warning: Importing a configuration file and initiating system with imported data will delete all existing session data.

To import a system configuration file, proceed as follows.

1. Find and decrypt the *Master key file* using *opessl*:

```
openssl smime -decrypt -in path/to/masterkey.pem -inkey privkey.
pem -out masterkey.tar
```

2. Select *Import configuration* from the user menu.



3. Click *Choose file* and select the *Master key* file.

Note: Master key must be decrypted before it's

4. Click *Choose file* and select the configuration file.
5. Click *Confirm*.
6. Click *Confirm* to proceed with initiating the system with the imported data.

Related topics:

- *Configuration encryption*
- *Backups and retention*
- *System initiation*
- *System update*

15.15 Cluster configuration

Fudo PAM cluster ensures uninterrupted access to servers in case of cluster node failure as well as enables implementing static load balancing scenarios.

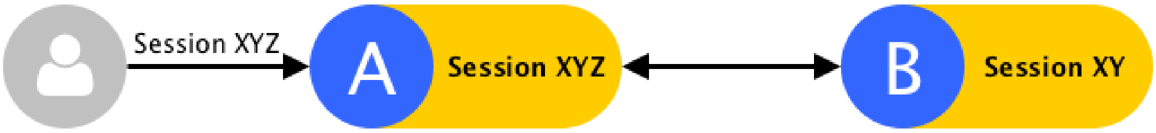
Warning:

- Cluster configuration does not facilitate data backup. If session data is deleted on one of the cluster nodes, it is also deleted from other nodes.
- Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances must not be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

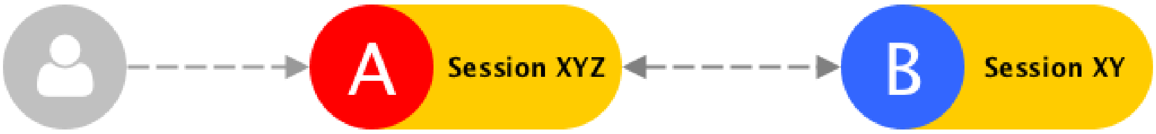
Data replication between cluster nodes is highly customizable. The administrator can choose the node that the data will be replicated to as well as which data (data model objects/session data) is replicated.

In case of a node failure, user access requests will be picked up by another cluster node, determined by the *redundancy group priority*.

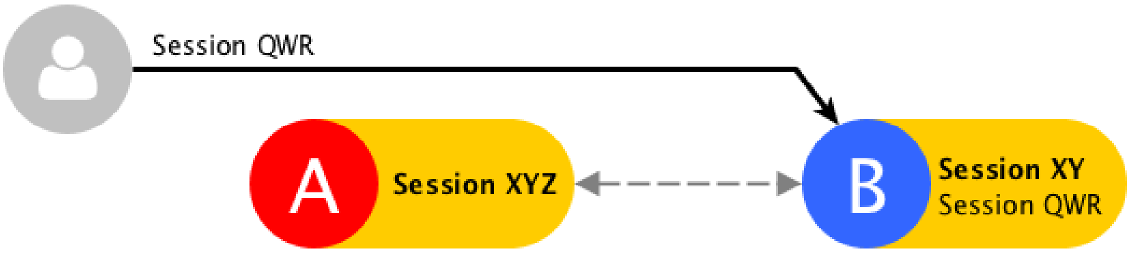
Current session data is replicated to other nodes while the connection is still ongoing.



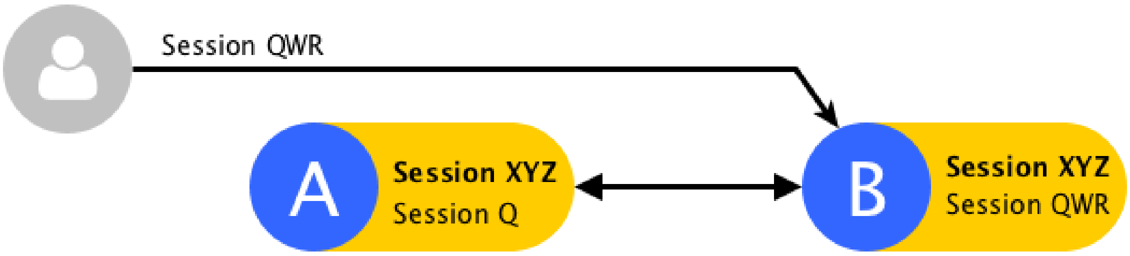
If the node that fails was recording sessions, those sessions will be terminated…



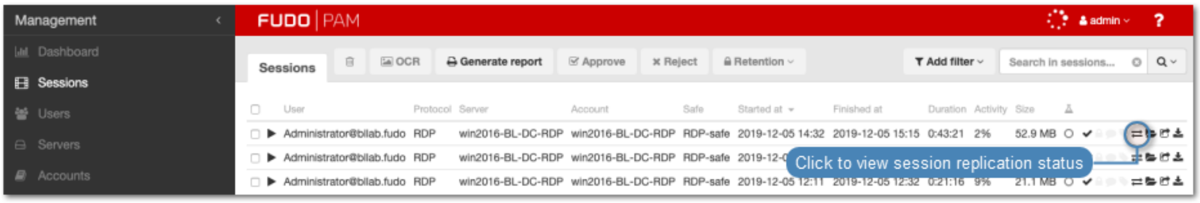
…and users will have to reconnect.



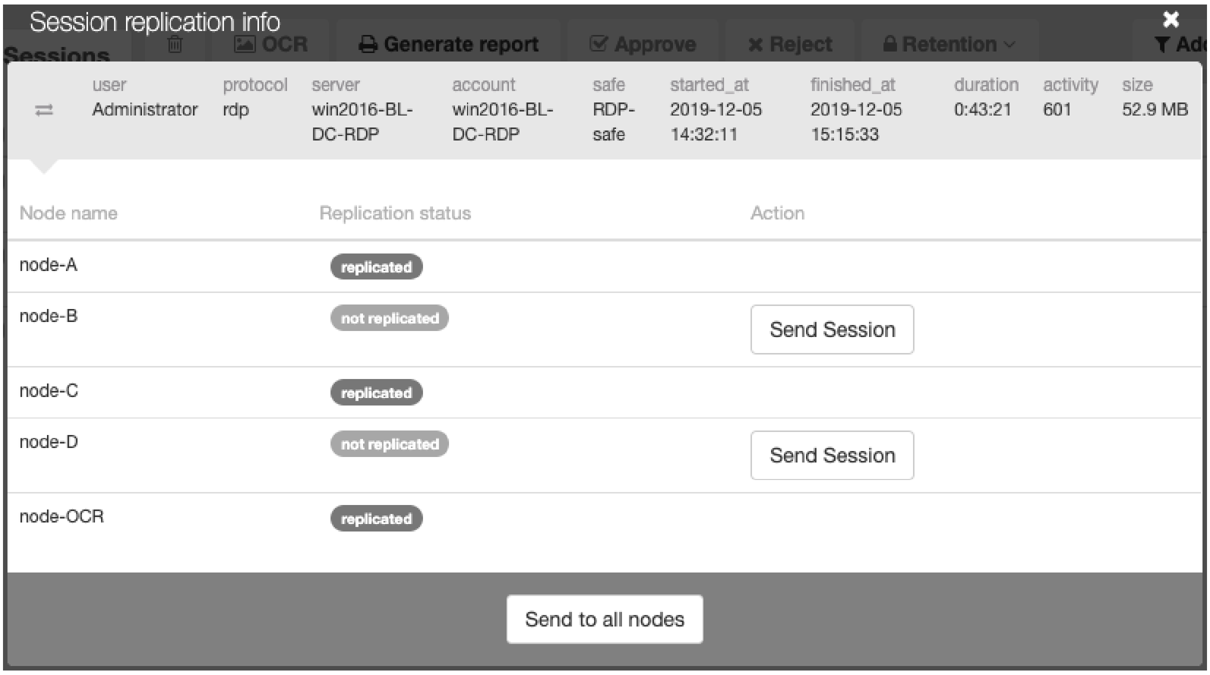
A part of the session data from the node that malfunctioned, which has synchronized, can be accessed on the other nodes, but the session will be fully accessible once the node becomes operational and session data is synchronized between cluster nodes.



Session replication status can be verified by clicking the ⇄ icon on the sessions list.



□	User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
□	▶ Administrator@bllab.fudo	RDP	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 14:32	2019-12-05 15:15	0:43:21	2%	52.9 MB
□	▶ Administrator@bllab.fudo	RDP	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-0				
□	▶ Administrator@bllab.fudo	RDP	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 12:11	2019-12-05 12:32	0:21:16	9%	21.1 MB



user	protocol	server	account	safe	started_at	finished_at	duration	activity	size
Administrator	rdp	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 14:32:11	2019-12-05 15:15:33	0:43:21	601	52.9 MB

Node name	Replication status	Action
node-A	replicated	
node-B	not replicated	Send Session
node-C	replicated	
node-D	not replicated	Send Session
node-OCR	replicated	

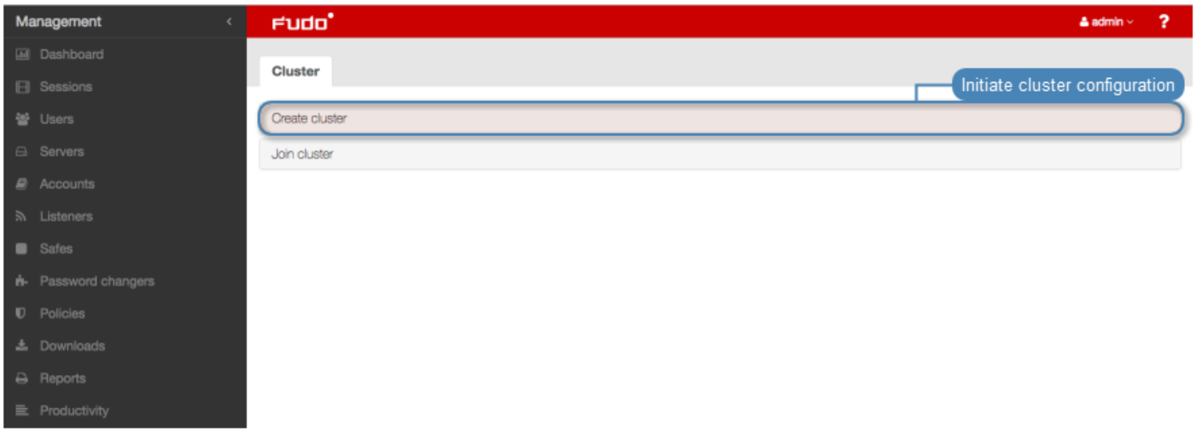
Send to all nodes

15.15.1 Initiating cluster

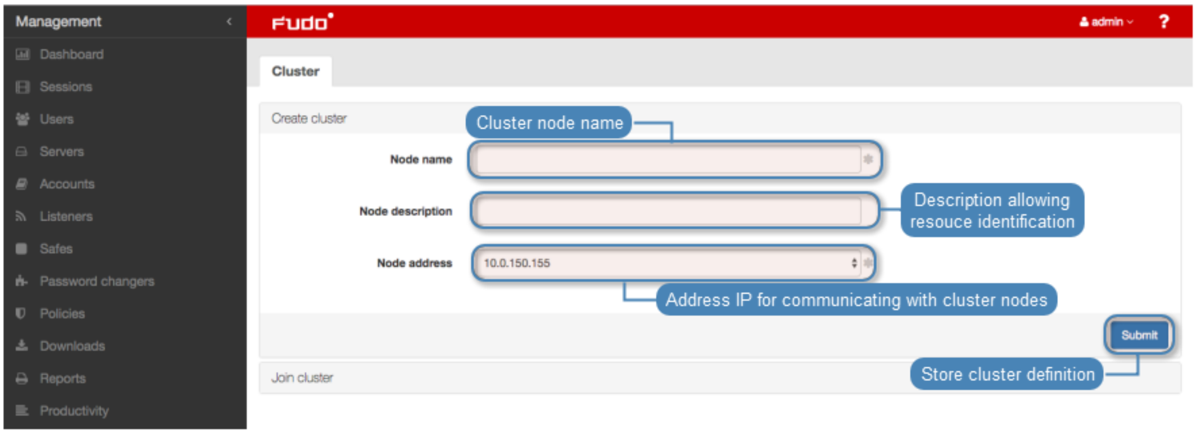
Warning: In cluster configuration all cluster nodes must have *NTP server configured*.

To initiate 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.



Node name

Node description

Node address: 10.0.150.155

Cluster node name

Description allowing resouce identification

Address IP for communicating with cluster nodes

Store cluster definition

Note: Cluster communication address must have the management option enabled 🔧 in the *network configuration*.

---

5. Click *Submit*.

Note: Message concerning cluster key can be ignored when initiating cluster.

Related topics:

- *Adding cluster nodes*
- *Editing cluster nodes*
- *Deleting cluster nodes*
- *Redundancy groups*
- *Cluster configuration*

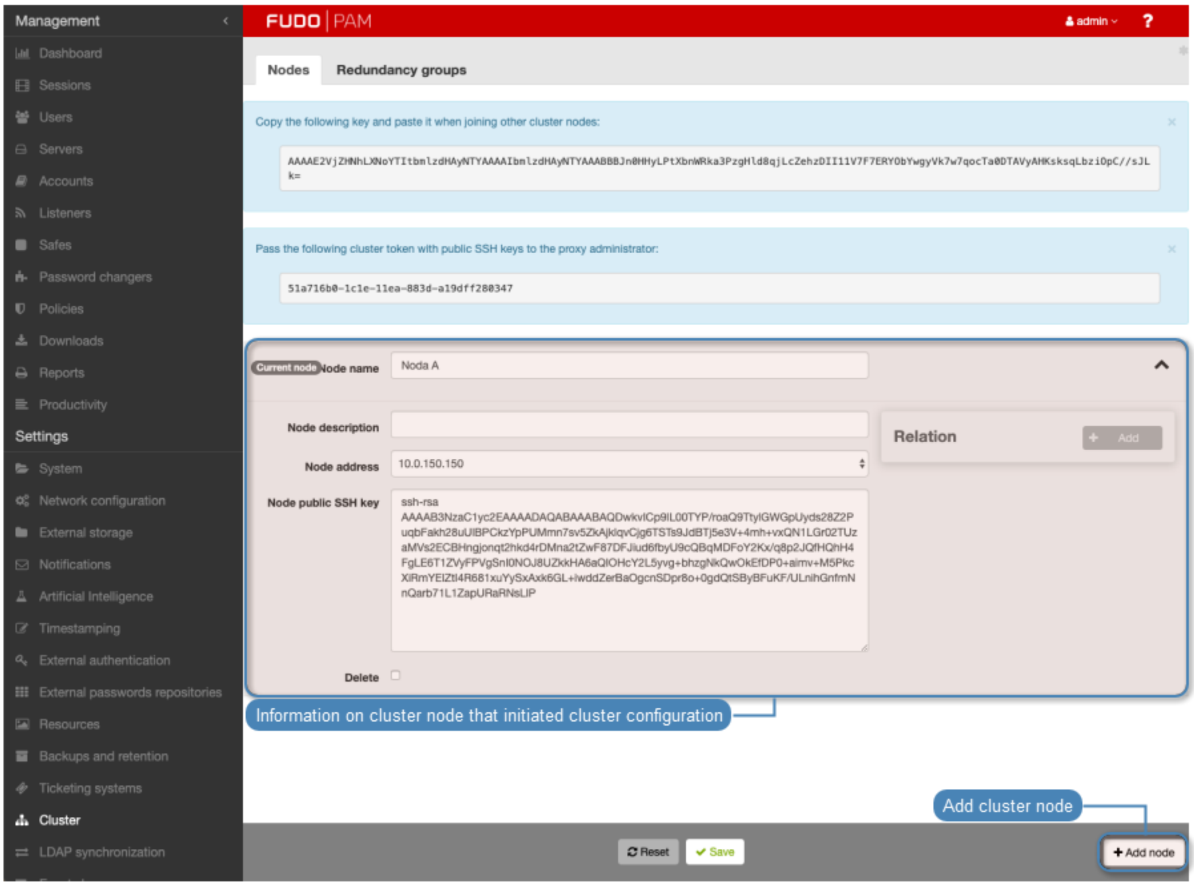
15.15.2 Adding cluster nodes

Warning:

- Session and configuration data (*servers*, *users*, *safes*, *accounts*, *listeners*, *external authentication servers*) of the joining node are deleted and initiated with data replicated from the cluster.
- Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances must not be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

To add a node to Fudo PAM cluster, proceed as follows.

1. Log in to the Fudo PAM administration panel where the cluster has been *initiated*.
2. Select *Settings* > *Cluster*.
3. Click *Add node* to display new node configuration parameters.



Copy the following key and paste it when joining other cluster nodes:

```
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJn0HHyLPtXbnWRka3PzgHld8qjLcZehzDII11V7F7ERYObYwgyVk7w7qocTa0DTAVyAHKsksqLbziOpC//sJL
k=
```

Pass the following cluster token with public SSH keys to the proxy administrator:

```
51a716b0-1c1e-11ea-883d-a19dff280347
```

Node name: Noda A

Node description:

Node address: 10.0.150.150

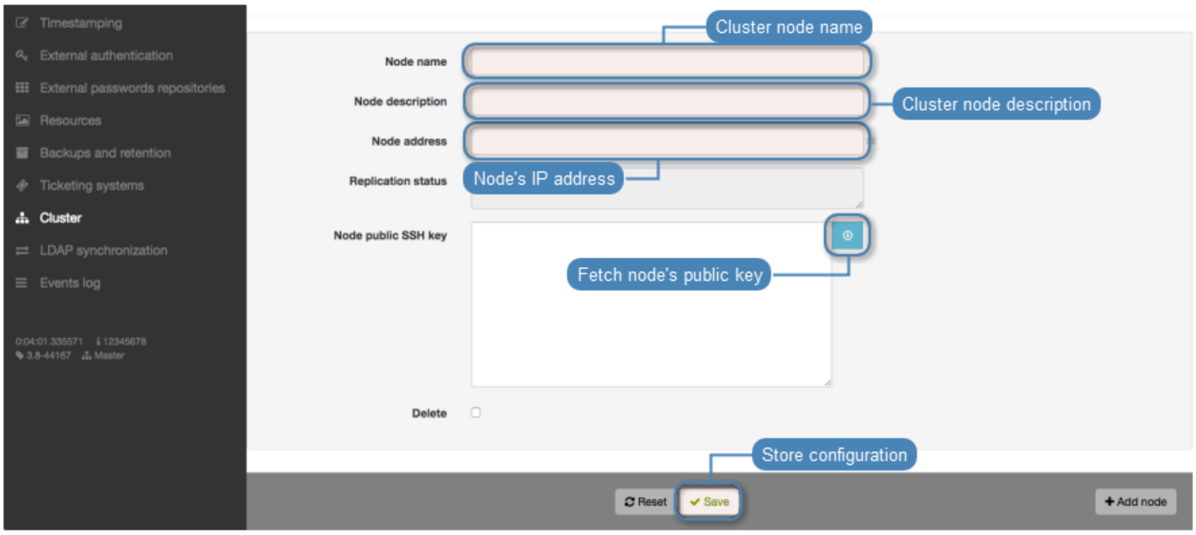
Node public SSH key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDwkvlCp9lL00TYP/roaQ9TtylGWGpUyds28Z2P
uqbFakh28uUlBPCkzYpPUMmn7sv5ZkAjklqvCjg6TSTs9JdBTj5e3V+4mh+vxQN1LGr02TUz
aMVs2ECBHngjonqt2hkd4rDMna2tZwF87DFJiud6fbyU9cQBqMDFoY2Kx/q8p2JQfHQhH4
FgLE6T1ZVyFPVgSnI0NOJ8UZkkHA6aQIOHcY2L5yvg+bhzgNkQwOkEfDP0+aimv+M5Pkc
XiRmYElZtl4R681xuYySxAxk6GL+lwddZerBaOgcnSDpr8o+0gdQtSByBFuKF/ULnihGnfmN
nQarb71L1ZapURaRNsLIP
```

Delete □

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.



Node name

Node description

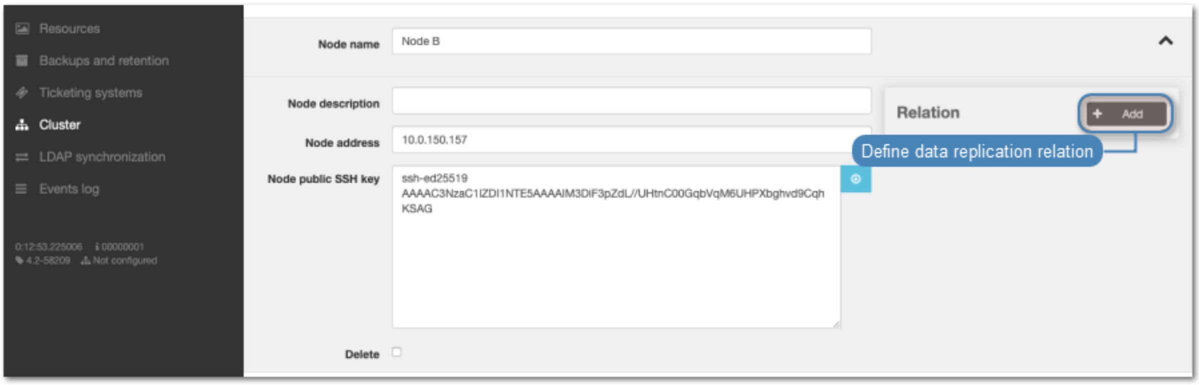
Node address

Replication status

Node public SSH key

Delete □

6. Click ⊙ to download node's public SSH key.
7. In the *Relations* section, click *+ Add*.



Node name: Node B

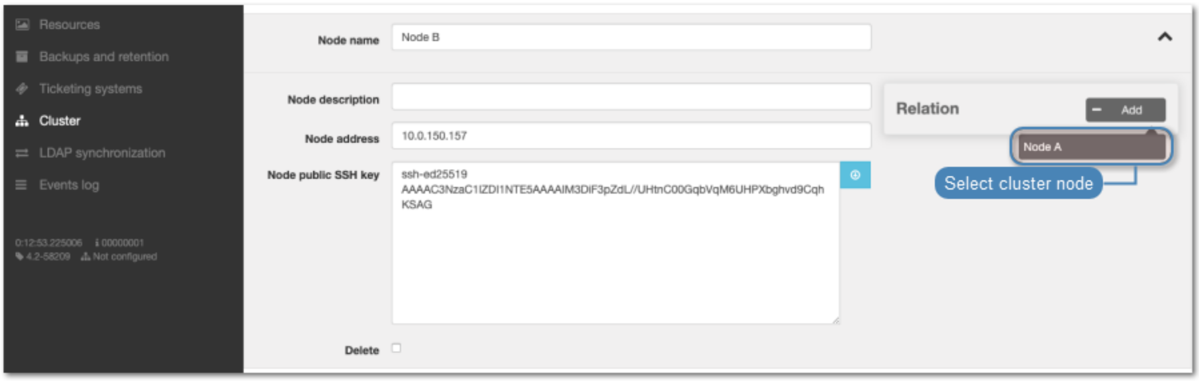
Node description:

Node address: 10.0.150.157

Node public SSH key: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM3DiF3pZdL//UHtnC00GqbVqM6UHPXbghvd9Cqh KSAG

Define data replication relation

8. Select the cluster node to which the data from the given node will be replicated.



Node name: Node B

Node description:

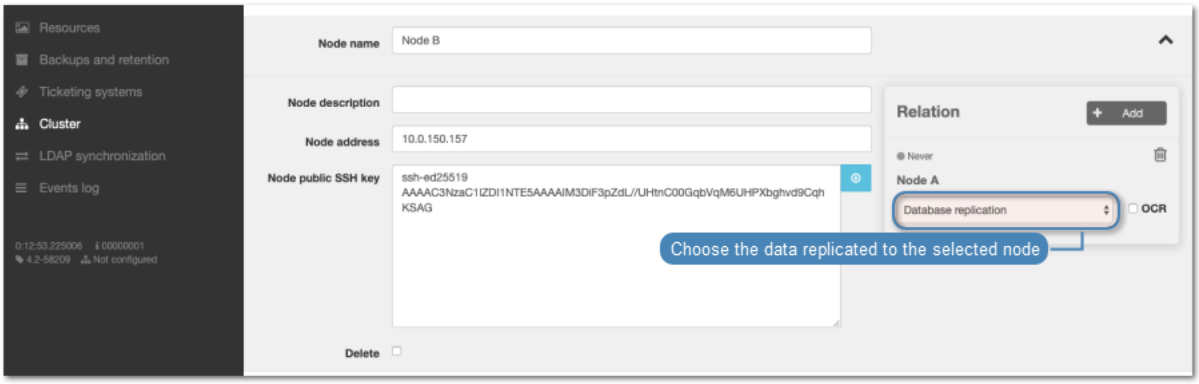
Node address: 10.0.150.157

Node public SSH key: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM3DiF3pZdL//UHtnC00GqbVqM6UHPXbghvd9Cqh KSAG

Node A

Select cluster node

9. Select which data will be replicated.



Node name: Node B

Node description:

Node address: 10.0.150.157

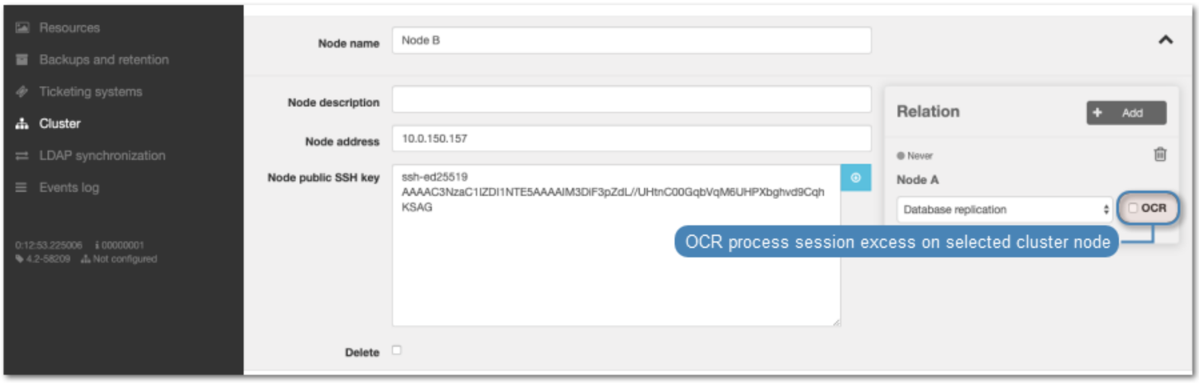
Node public SSH key: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM3DiF3pZdL//UHtnC00GqbVqM6UHPXbghvd9Cqh KSAG

Node A

Database replication □ OCR

Choose the data replicated to the selected node

10. Select *OCR* option to delegate OCR processing in case they cannot be processed locally.



Node name: Node B

Node description:

Node address: 10.0.150.157

Node public SSH key: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM3DiF3pZdL//UHtnC00GqbVqM6UHPXbghvd9Cqh KSAG

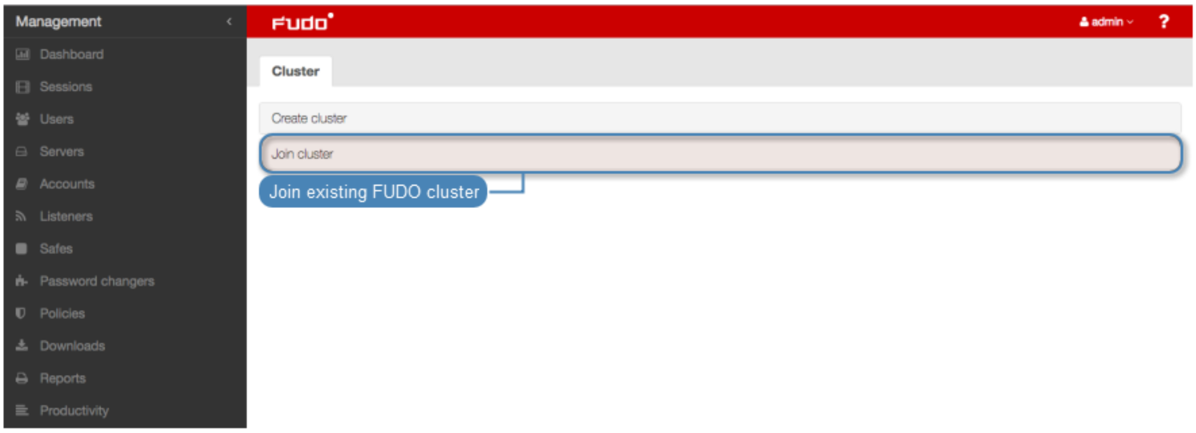
Node A

Database replication □ OCR

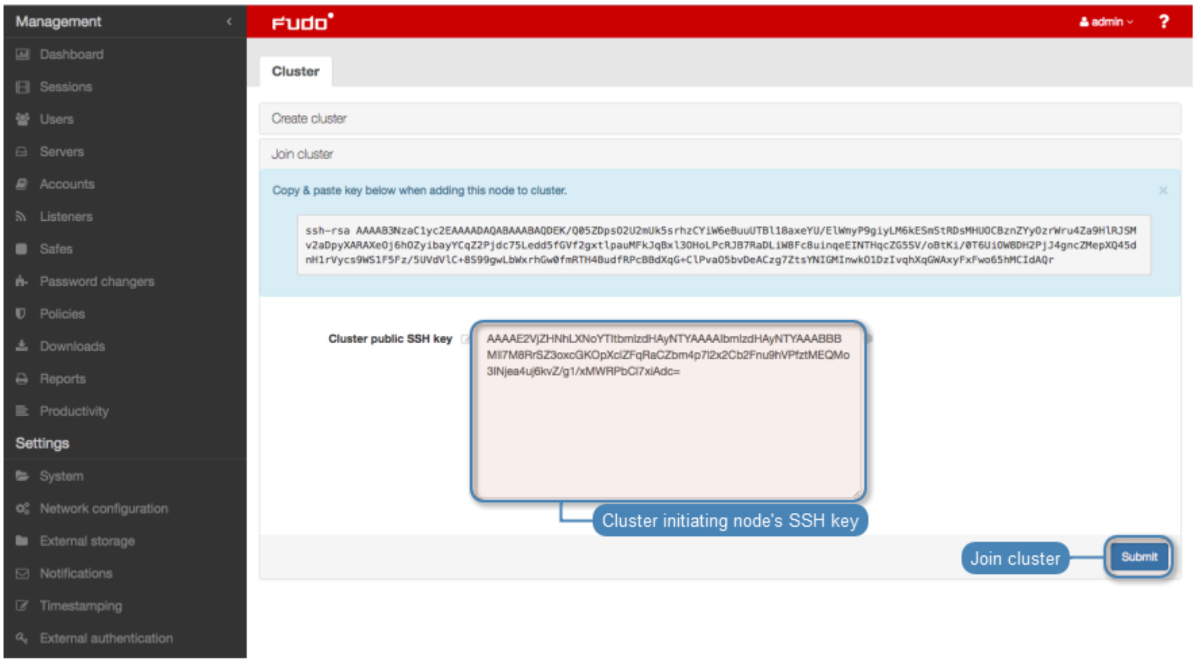
OCR process session excess on selected cluster node

Note: Each Fudo PAM instance has a defined number of resources dedicated to OCR processing. If the *OCR* option is selected, excess of sessions that cannot processed locally at the moment, is forwarded for processing to selected node.

11. In the *Relations* section of the primary node, click *+ Add*.
12. Select the cluster node to which the data from the given node will be replicated.
13. Select which data will be replicated.
14. Click *Save*, to add node definition.
15. Copy cluster key to clipboard.
16. Log in to administration panel of the joining node.
17. Select *Settings > Cluster*.
18. Click *Join cluster*.



19. Paste cluster public SSH key and click *Submit*.



Copy & paste key below when adding this node to cluster.

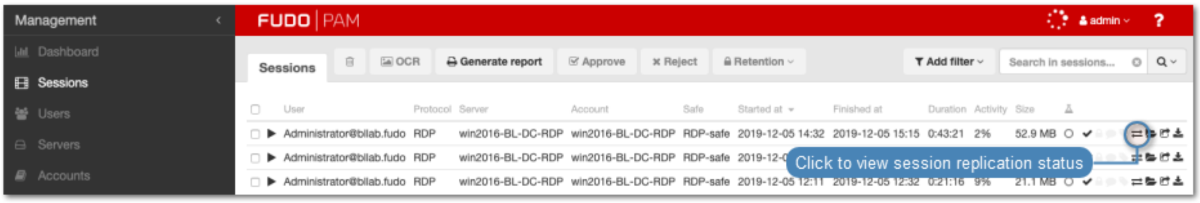
```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDEK/Q05ZDpsO2U2mUk5srhzCYiW6eBuuUTBl18axeYU/ElWmyP9giyLM6kESmStRDsMHUOCBznZYyOzrWru4Za9HlRJSM
v2aDpyXARAXeOj6hOZyibayYCqZ2Pjdc75Ledd5fGVf2gxtlpauMFkJqBxl3OHoLPcRJB7RaDLiW8FcBuinqeEINTHqcZG5SV/oBtKi/0T6UiOW8DH2PjJ4gncZMepXQ45d
nH1rVycs9WS1F5Fz/5UVdVlC+8S99gwLbWxrhGw0fmRTH4BudfRPcB8dXqG+ClPvaO5bvDeACzg7ZtsYNIGMInwkO1DzIvqhXqGWAxyFxFwo65hMCIdAQr
```

Cluster public SSH key

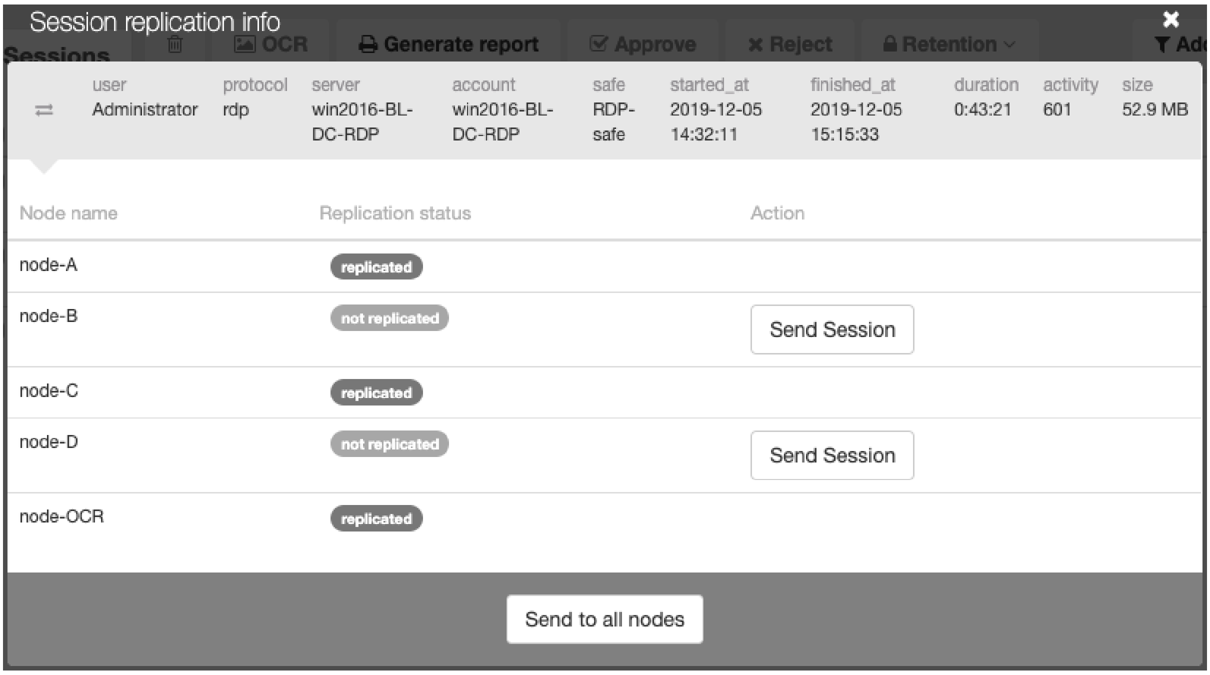
```
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB
MII7M8RrSZ3oxcGKOpXclZFqRaCZbm4p7l2x2Cb2Fnu9hVPfztMEQMo
3INjea4uj6kvZ/g1/xMWRPbCl7xiAdc=
```

20. Click *I understand the consequences, proceed.*

Note: To view session replication status, go to sessions list and click the ⇄ icon.



	User	Protocol	Server	Account	Safe	Started at	Finished at	Duration	Activity	Size
□ ▶	Administrator@bllab.fudo	RDP	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 14:32	2019-12-05 15:15	0:43:21	2%	52.9 MB
□ ▶	Administrator@bllab.fudo	RDP	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-0				
□ ▶	Administrator@bllab.fudo	RDP	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 12:11	2019-12-05 12:32	0:21:16	9%	21.1 MB



	user	protocol	server	account	safe	started_at	finished_at	duration	activity	size
⇄	Administrator	rdp	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 14:32:11	2019-12-05 15:15:33	0:43:21	601	52.9 MB

Node name	Replication status	Action
node-A	replicated	
node-B	not replicated	Send Session
node-C	replicated	
node-D	not replicated	Send Session
node-OCR	replicated	

Related topics:

- *Editing cluster nodes*
- *Deleting cluster nodes*
- *Security: Cluster configuration*

15.15.3 Editing cluster nodes

To modify a cluster node's configuration, proceed as follows.

1. Select *Settings > Cluster.*
2. Find and edit desired node parameters.
3. Click *Submit.*

Related topics:

- *Adding cluster nodes*
- *Deleting cluster nodes*
- *Security: Cluster configuration*

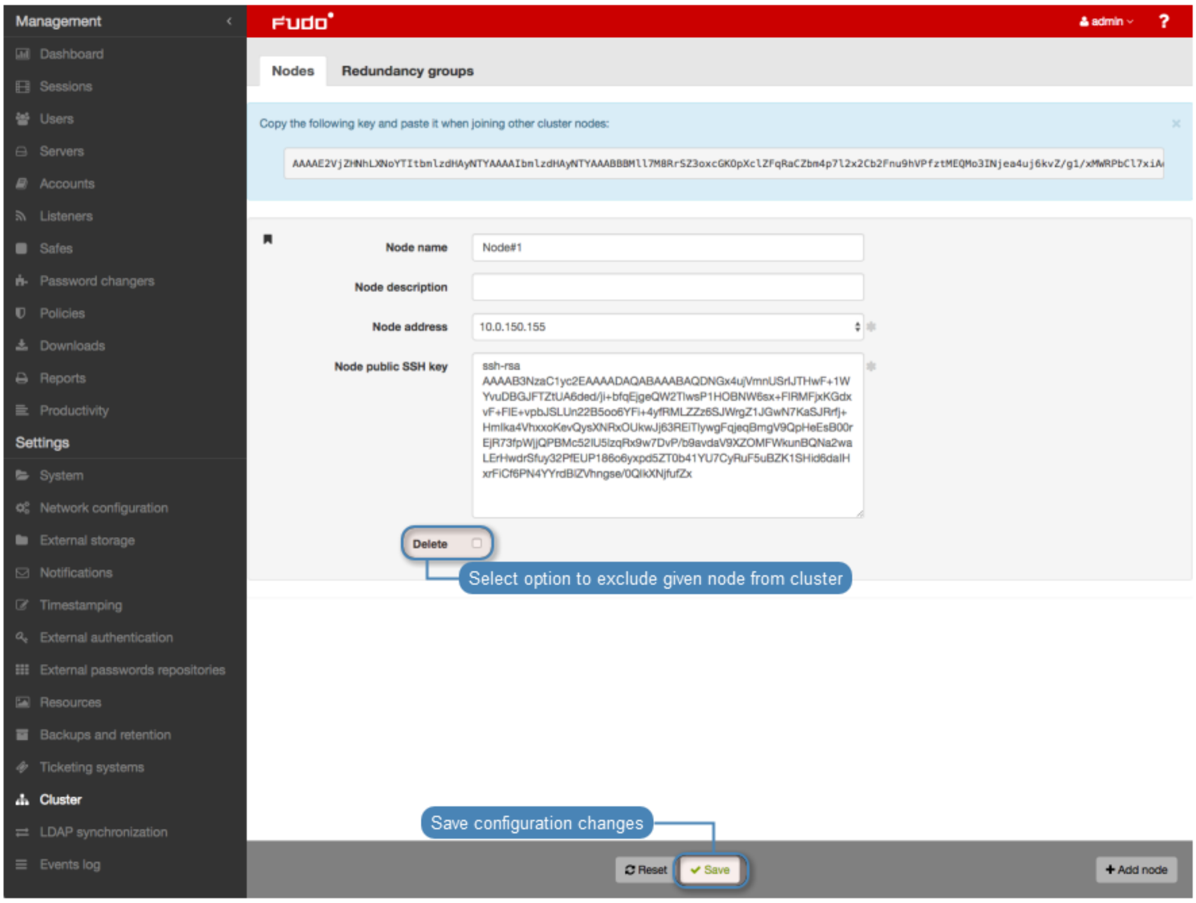
15.15.4 Deleting cluster nodes

Warning:

- Removing a node and re-adding it to a cluster may result in data loss.
- After removing a node, you will no longer be able to delete session data recorded by this node and replicated to other nodes.

To remove a cluster node, proceed as follows.

1. Select *Settings* > *Cluster*.
2. Find desired node and select *Delete*.
3. Click *Submit*.



Copy the following key and paste it when joining other cluster nodes:

```
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMll7M8RrSZ3oxcGKOpXclZFqRaCZbm4p7l2x2Cb2Fnu9hVPfztMEQMo3INjea4uj6kvZ/g1/xMWRPbCl7xiA
```

Node name: Node#1

Node description:

Node address: 10.0.150.155

Node public SSH key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDNGx4ujVmnUSrlJTHwF+1W
YvuDBGJFTZtUA6ded/ji+bfqEjgeQW2TlwsP1HOBNW6sx+FIRMFjxKGdx
vF+FIE+vpbJSLUn22B5oo6YFi+4yfRMLZZz6SJWrgZ1JGwN7KaSJRfj+
Hmlka4VhxxoKevQysXNRxOUkwJj63REiTlywgFqjeqBmgV9QpHeEsB00r
EjR73fpWjjQPBMc52lU5lzqRx9w7DvP/b9avdaV9XZOMFWkunBQNa2wa
LErHwdrSfuy32PfEUP186o6yxpd5ZT0b41YU7CyRuF5uBZK1SHid6dalH
xrFiCf6PN4YYrdBlZVhngse/0QlkXNjfufZx
```

Delete □

Select option to exclude given node from cluster

Save configuration changes

Related topics:

- *Adding cluster nodes*
- *Editing cluster nodes*
- *Security: Cluster configuration*

15.15.5 Redundancy groups

Redundancy groups ensure high system availability. If a master node fails, IP addresses assigned to the redundancy group will be automatically picked up by another node with the highest priority assigned to this group. Assigning different priorities to different redundancy groups enables implementing static load balancing scenario while fully preserving high availability features.

Note: Redundancy groups configuration options are available only after initializing the cluster.

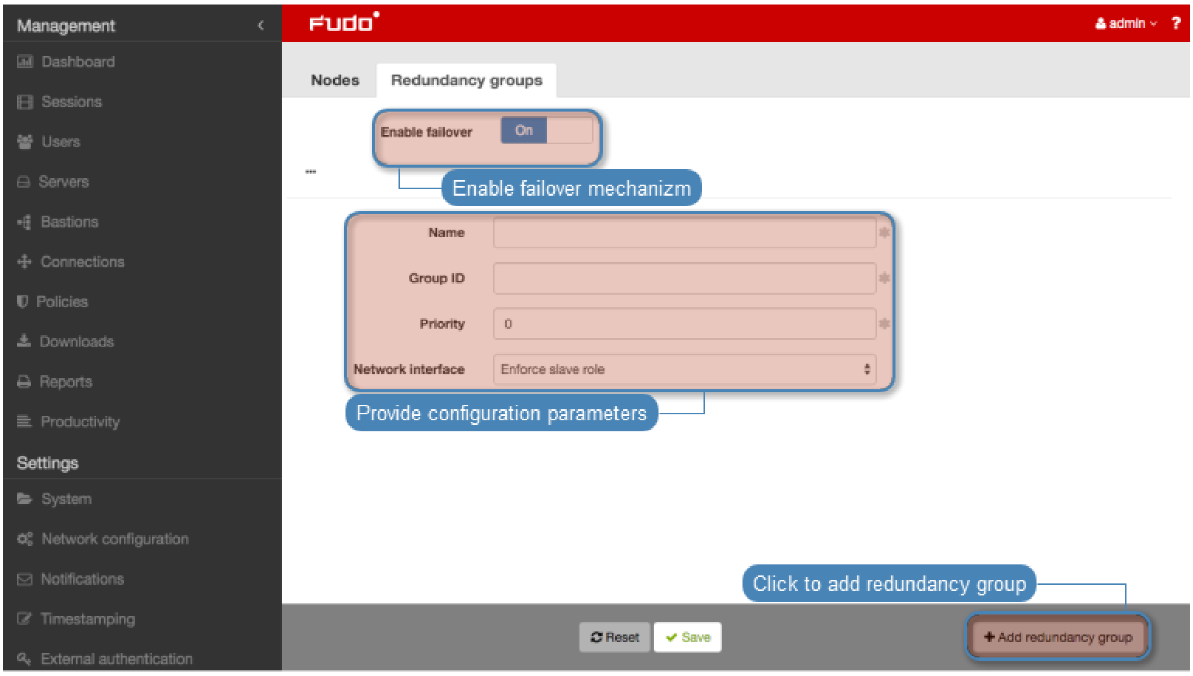
Adding redundancy groups

To add a redundancy group, proceed as follows.

1. Select *Settings > Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Click *+ Add redundancy group*.
4. Define group properties.

Parameter	Description
Name	Descriptive name of the redundancy group.
ID	Redundancy groups identifier (1-255).
Priority	Redundancy group priority (0-254), the lower the number the higher the priority.
	Redundancy group with higher priority assumes the *master* role and handles all requests to monitored servers accessed through IP addresses assigned to this group. In case given cluster node crashes, user requests are directed to on of the remaining nodes with the highest priority defined for given redundancy group.
Interlink interface	Network interface used for monitoring the state of the given redundancy group. The master node broadcasts *keep-alive* packets in the 2nd networking layer informing other nodes that it is up and running while other cluster nodes use the interlink interface to listen for those packets.

Note: By default, once a node takes the *master* role, it will continue on indefinitely as the *master* node.



Enable failover: On

Enable failover mechanizm

Name:

Group ID:

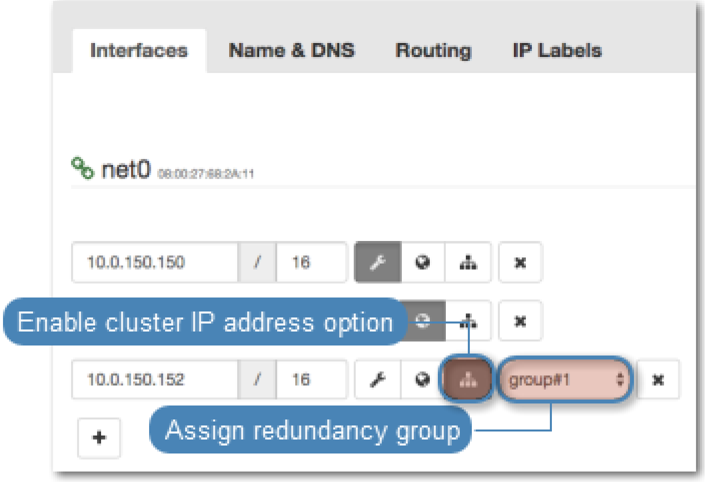
Priority: 0

Network interface: Enforce slave role

Provide configuration parameters

Click to add redundancy group

5. Click *Save*.
6. Select *Settings* > *Network configuration*.
7. Click + to add new IP address.
8. Enter IP address and click the icon to mark the entry as a cluster IP address.
9. Assign previously added redundancy group.
10. Click *Save*.



10.0.150.150 / 16

10.0.150.152 / 16 group#1

Enable cluster IP address option

Assign redundancy group

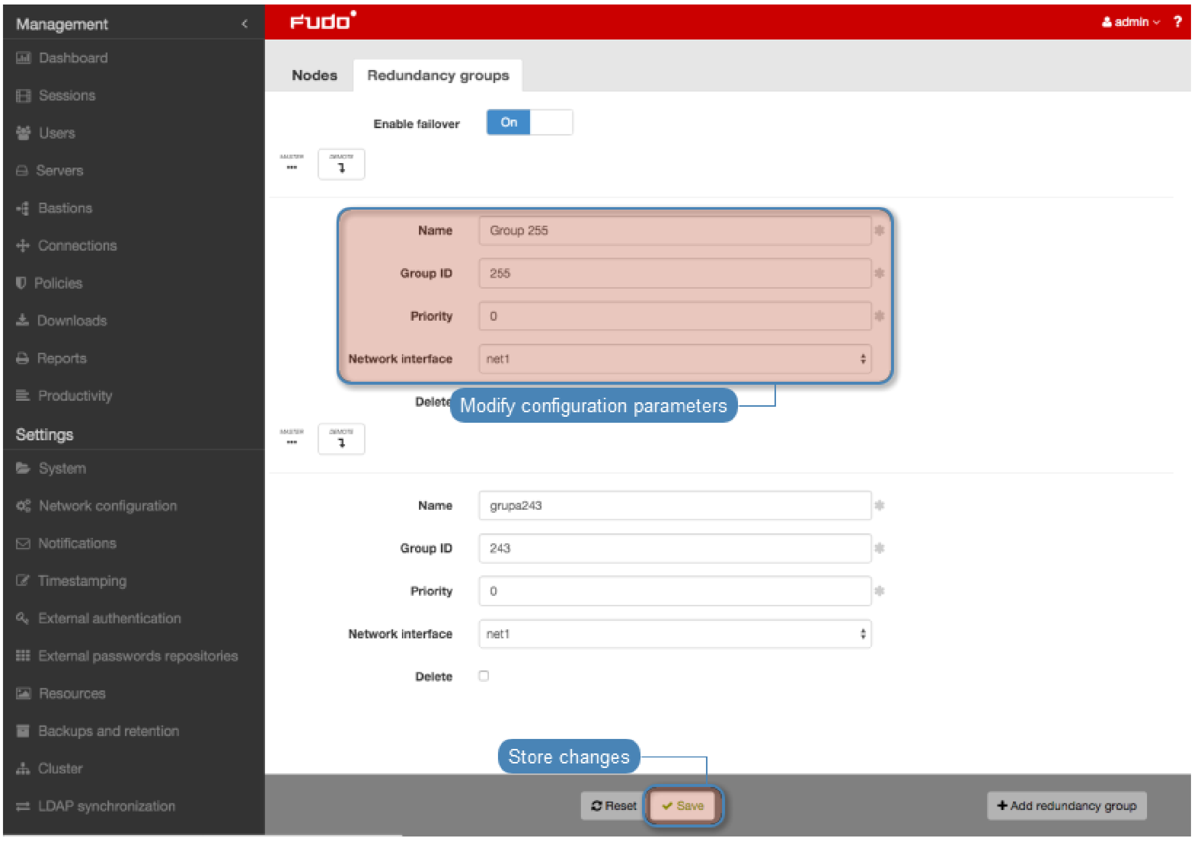
Note: Cluster IP address must be defined on every cluster node.

Editing redundancy groups

To modify a redundancy group, proceed as follows.

1. Select *Settings* > *Cluster*.

2. Switch to the *Redundancy groups* tab.
3. Find and edit desired redundancy group definition.
4. Click *Save*.



Enable failover: On

Name	Group 255
Group ID	255
Priority	0
Network interface	net1
Delete	

Modify configuration parameters

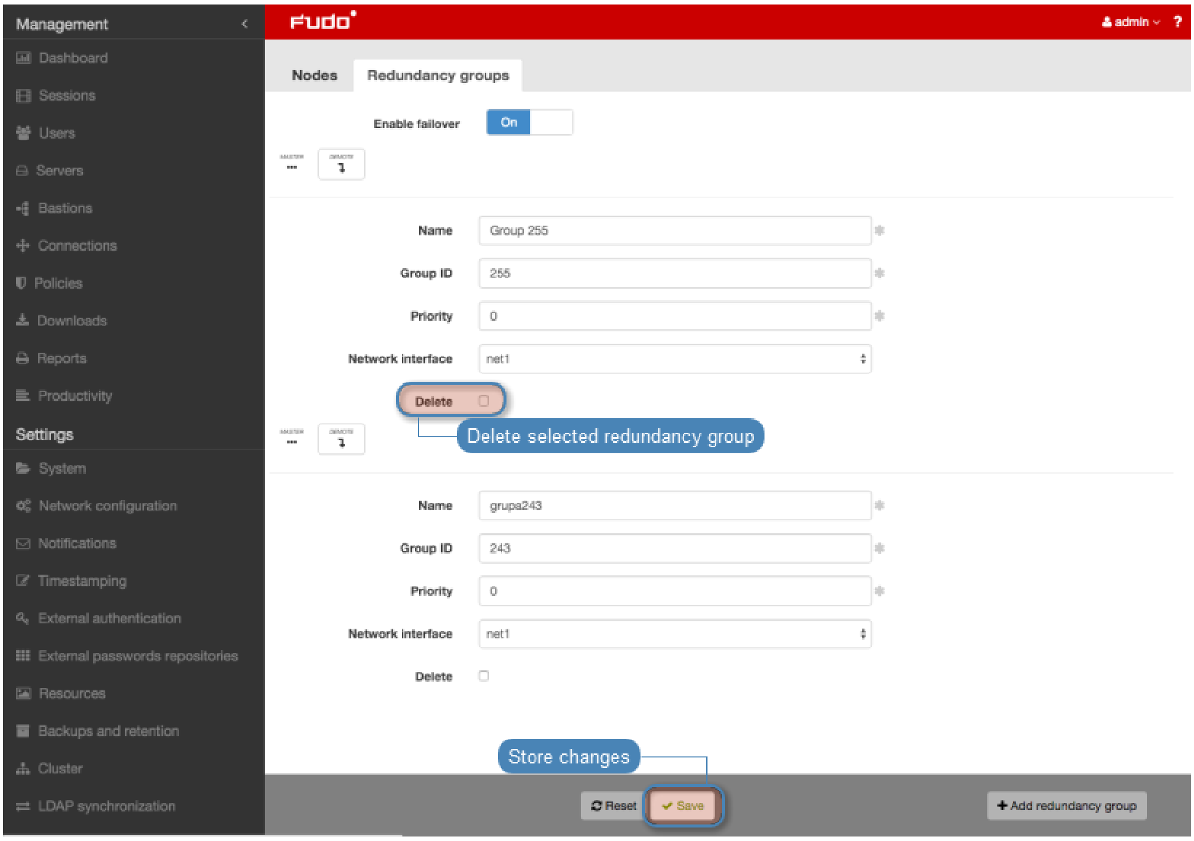
Name	grupa243
Group ID	243
Priority	0
Network interface	net1
Delete	□

Store changes

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*.



Enable failover: On

Name: Group 255

Group ID: 255

Priority: 0

Network interface: net1

Delete □

Delete selected redundancy group

Name: grupa243

Group ID: 243

Priority: 0

Network interface: net1

Delete □

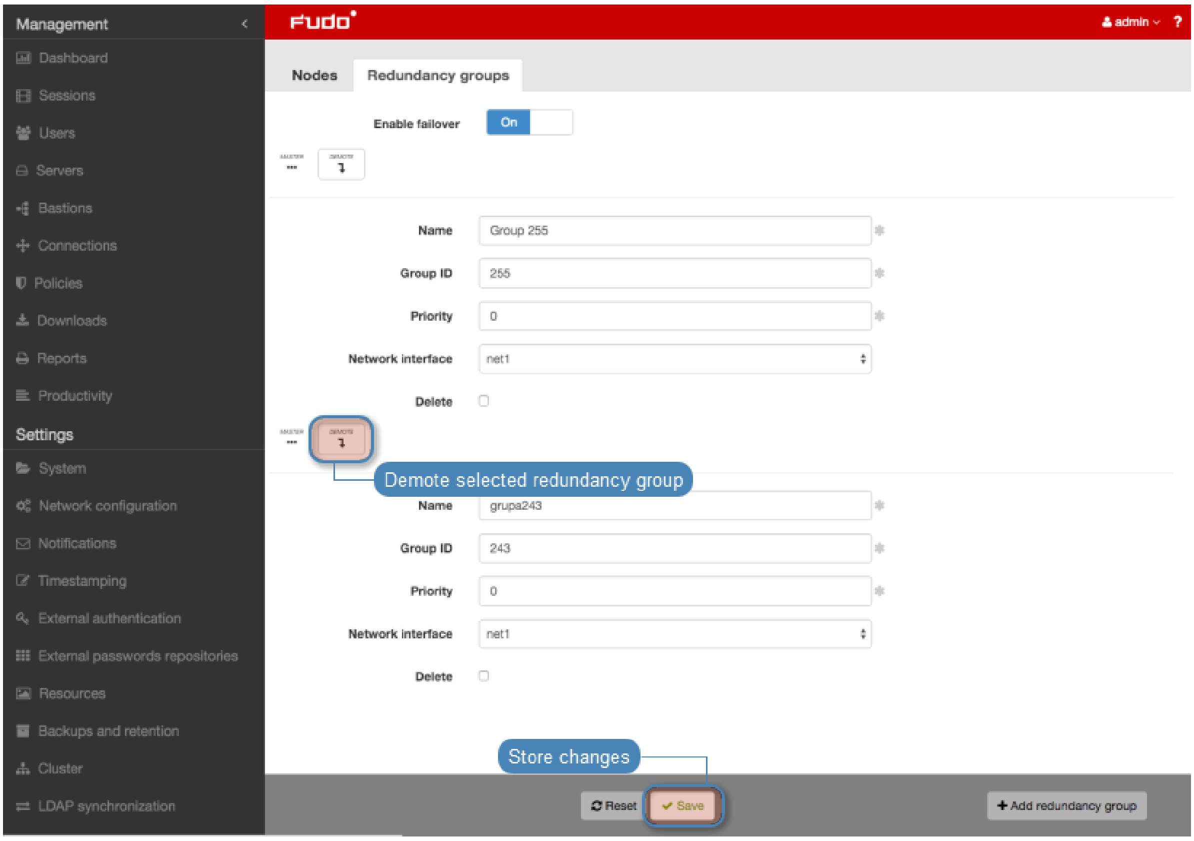
Store changes

Demoting a redundancy group

Note: Demoting redundancy group transfers the master role for given group to another cluster node. The master role is assumed by on of the remaining nodes, on which the given redundancy group has the highest priority defined.

To demote a redundancy group, proceed as follows.

1. Select *Settings* > *Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Click *Demote* next to the desired redundancy group.
4. Click *Confirm*.



Enable failover: On

Name: Group 255
Group ID: 255
Priority: 0
Network interface: net1
Delete: ☐

Demote selected redundancy group

Name: grupa243
Group ID: 243
Priority: 0
Network interface: net1
Delete: ☐

Store changes

Note: If after demoting a redundancy group no other node assumes the master role for the given group, it will be reassigned to the node which previously had this role.

Enforcing a slave role

Note: Enforcing a permanent slave role on a redundancy group ensures that the given node will not assume master role on given redundancy group despite the state that other nodes are in. It's recommended for directing all traffic to other nodes before performing maintenance tasks on given cluster node. A different use case scenario would be a cluster node in a remote location with no 2nd network layer communication with other nodes.

To enforce a permanent slave role on a redundancy group, proceed as follows.

1. Select *Settings > Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Find desired redundancy group and select `Enforce slave mode` from the *Interface* drop-down list.
4. Click *Save*.

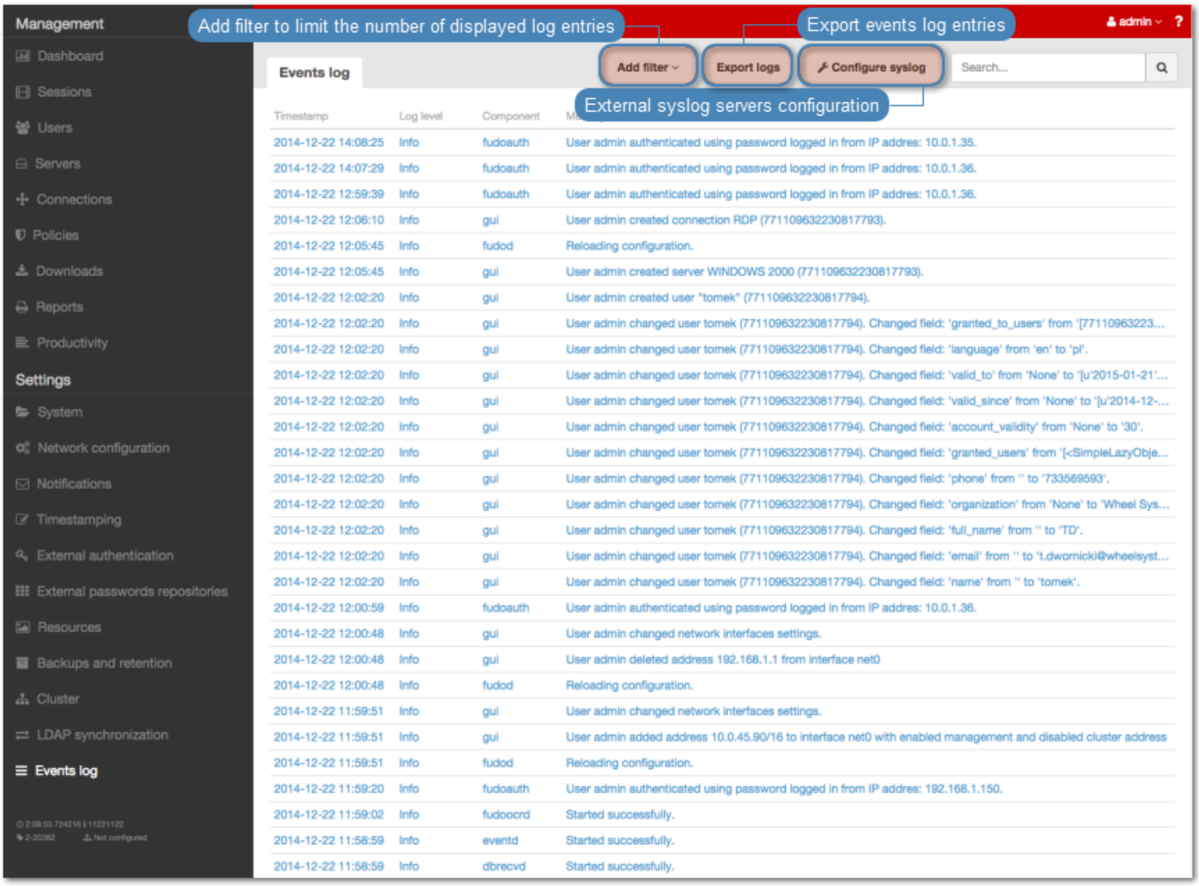
Related topics:

- *Security: Cluster configuration*
- *Initiating cluster*
- *Cluster configuration*

15.16 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.



Add filter to limit the number of displayed log entries

Export events log entries

External syslog servers configuration

Timestamp	Log level	Component	M
2014-12-22 14:08:25	Info	fudoauth	User admin authenticated using password logged in from IP addres: 10.0.1.35.
2014-12-22 14:07:29	Info	fudoauth	User admin authenticated using password logged in from IP addres: 10.0.1.36.
2014-12-22 12:59:39	Info	fudoauth	User admin authenticated using password logged in from IP addres: 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 '[<SimpleLazyObje...
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.dwornicki@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 addres: 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 addres: 192.168.1.150.
2014-12-22 11:59:02	Info	fudoocrd	Started successfully.
2014-12-22 11:58:59	Info	eventd	Started successfully.
2014-12-22 11:58:59	Info	dbrecvd	Started successfully.

15.16.1 External syslog servers

Note:

- Fudo PAM communicates with the syslog server over UDP protocol.
- Messages to the syslog server are send through an interface with the 🔧 option enabled, with an IP address that the target host's network is reachable from or using the default gateway.

Adding a Syslog server

To add a *Syslog* server, proceed as follows.

1. Select *Settings > Events log.*
2. Click *Configure syslog* to display syslog servers configuration settings.

3. Select *Enable events logging on syslog servers* option to activate sending logs to defined syslog servers.
4. Select *Enable sending debug logs* option to activate sending debug logs within messages to defined syslog.
5. Click +.
6. Provide server's IP address and port number.
7. Click *Save*.

Note:

- Log entries sent to syslog servers are formatted as follows:

```
[<log_level>] (<component_name>) (object_name:  object_id) <message>
```

Example:

```
[INFO] (fudordp) (fudo_server:  848388532111147015) (fudo_session:
848388532111147219)          (fudo_user:  848388532111147012) (fudo_connection:
848388532111147014)    User user0 authenticated using password logged in from IP
addres:  10.0.40.101.
```

- For detailed list of log messages, refer to the *Log messages* topic.

Editing Syslog server definition

To edit a *Syslog* server definition, proceed as follows.

1. Select *Settings* > *Events log*.
2. Click *Configure syslog* to display syslog servers configuration settings.
3. Find and edit desired syslog server definition.
4. Click *Save*.

Deleting Syslog server definition

To delete a *Syslog* server definition, proceed as follows.

1. Select *Settings* > *Events log*.
2. Click *Configure syslog* to display syslog servers configuration settings.
3. Find desired server definition and click the i icon.
4. Click *Save*.

15.16.2 Exporting events log

To export events log entries, proceed as follows.

1. Select *Settings* > *Events log*.
2. Click *Export logs* and select where to save exported log entries.

Related topics:

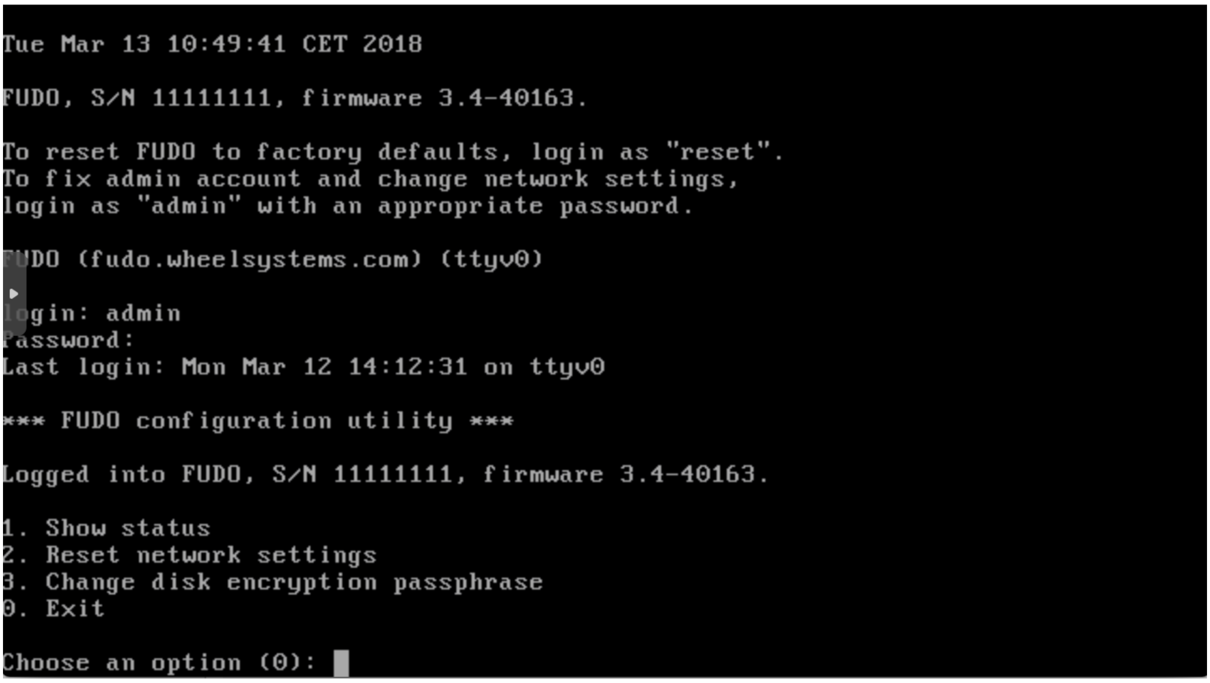
- *Log messages*

- *Security*
- *Managing servers*

15.17 Changing encryption passphrase

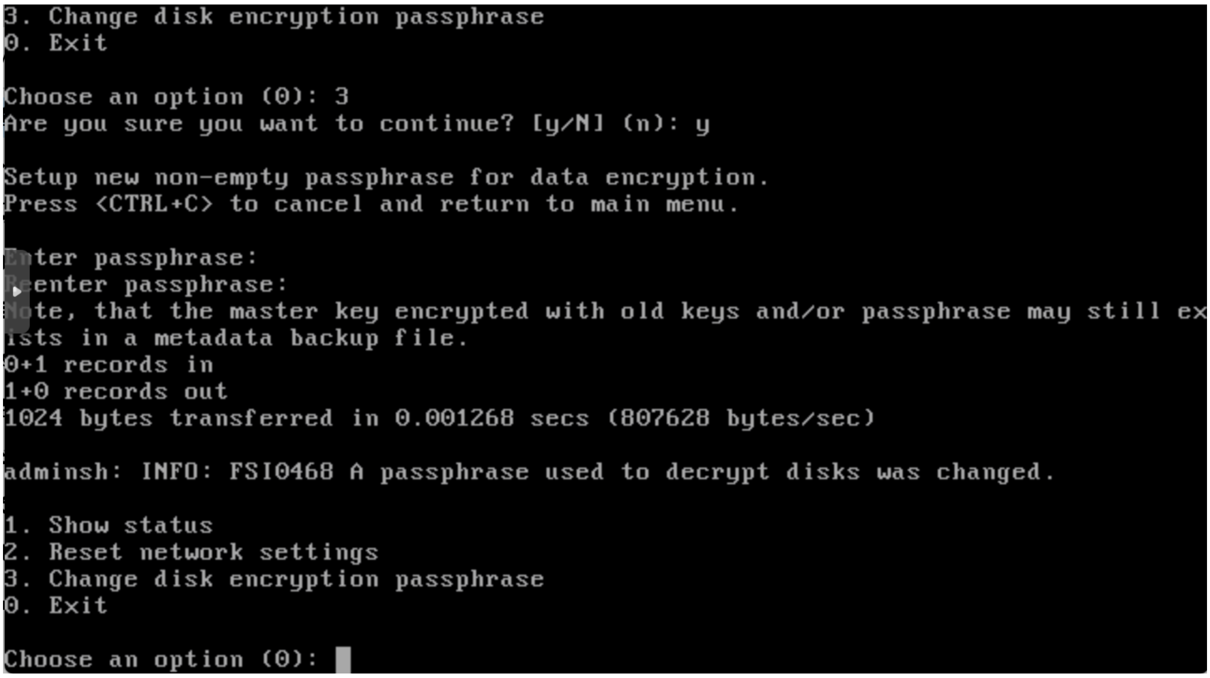
In case of Fudo PAM deployed in a virtual environment, data is encrypted using a passphrase. To change current passphrase, proceed as follow.

1. Log in to system console on an account with *superadmin* privileges.
2. Type in 3 and confirm by pressing the *Enter* key.



```
Tue Mar 13 10:49:41 CET 2018

FUDO, S/N 11111111, firmware 3.4-40163.

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: Mon Mar 12 14:12:31 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 11111111, firmware 3.4-40163.

1. Show status
2. Reset network settings
3. Change disk encryption passphrase
0. Exit

Choose an option (0):
```

3. Type in y and press the *Enter* key, to proceed with changing encryption passphrase.
4. Enter the new passphrase and press the *Enter* key.
5. Enter the passphrase once again and press the *Enter* key.



```
3. Change disk encryption passphrase
0. Exit

Choose an option (0): 3
Are you sure you want to continue? [y/N] (n): y

Setup new non-empty passphrase for data encryption.
Press <CTRL+C> to cancel and return to main menu.

Enter passphrase:
Reenter passphrase:
Note, that the master key encrypted with old keys and/or passphrase may still ex
ists in a metadata backup file.
0+1 records in
1+0 records out
1024 bytes transferred in 0.001268 secs (807628 bytes/sec)

adminsh: INFO: FSI0468 A passphrase used to decrypt disks was changed.

1. Show status
2. Reset network settings
3. Change disk encryption passphrase
0. Exit

Choose an option (0):
```

6. Restart the system to apply changes.

Related topics:

- *System update*
- *Backups and retention*

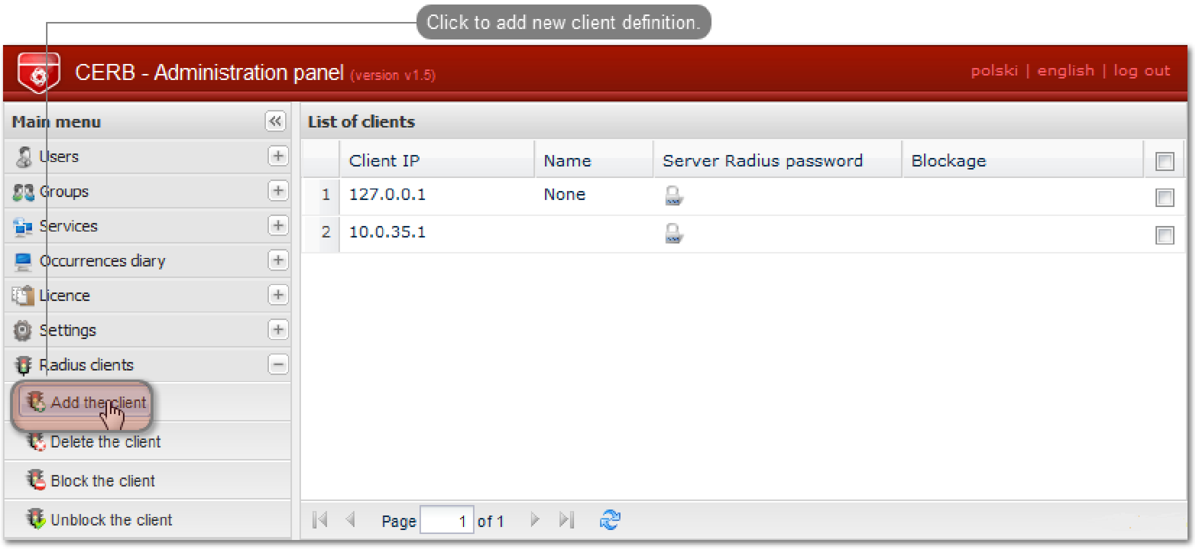
15.18 Integration with CERB server

CERB is complete user authorization solution which supports a number of authorization mechanisms (i.e. mobile token, onetime passwords, etc.). The following procedure describes configuration steps required to enable Fudo PAM to verify users credentials using CERB server.

CERB server configuration

1. Adding RADIUS client.

- Select *RADIUS clients > Add client* to add Fudo PAM as a RADIUS client.

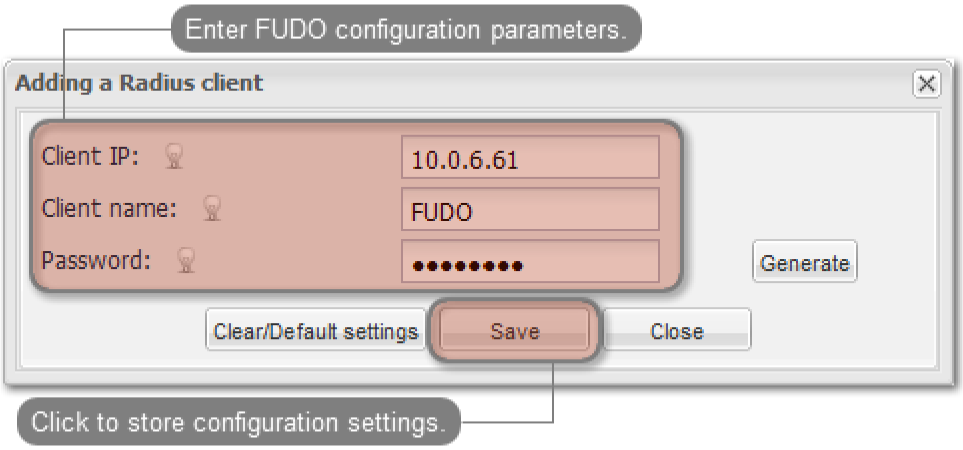


Click to add new client definition.

List of clients

	Client IP	Name	Server Radius password	Blockage	□
1	127.0.0.1	None			□
2	10.0.35.1				□

- Provide Fudo PAM IP address, client's name and password and click *Save*.



Enter FUDO configuration parameters.

Adding a Radius client

Client IP: 10.0.6.61

Client name: FUDO

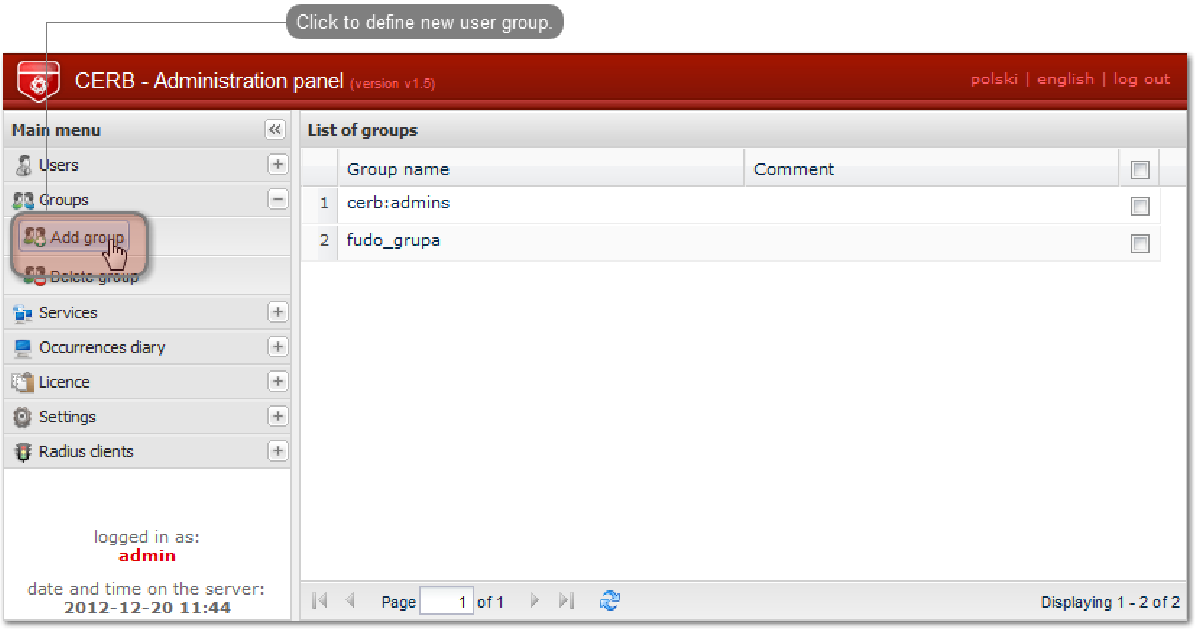
Password: ●●●●●●●●

Click to store configuration settings.

Note: Password will be required to define external authorization server in Fudo PAM administration panel.

2. Adding user group.

- Select *Groups* > *Add group* to define Fudo PAM users who will be authorized by the CERB server.

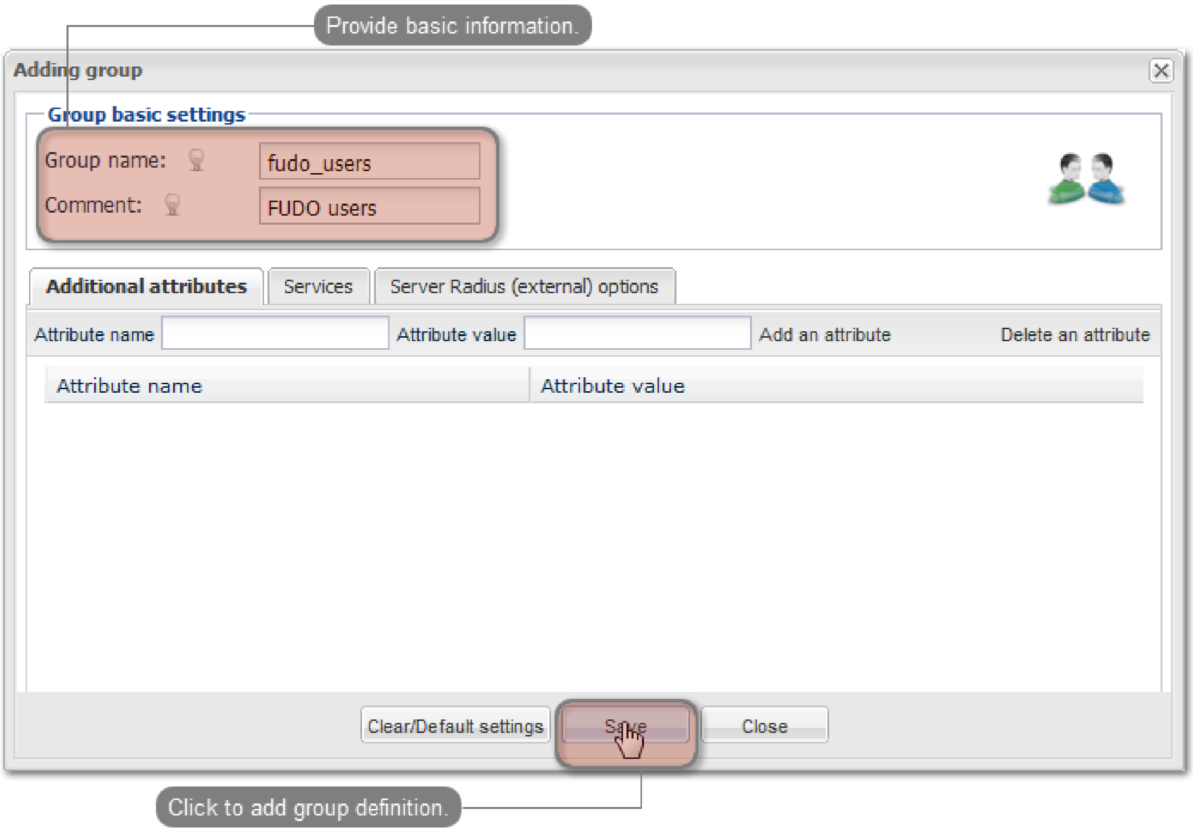


Click to define new user group.

List of groups

	Group name	Comment	□
1	cerb:admins		□
2	fudo_grupa		□

- Enter group’s name (`fudo_users`) and click *Save*.



Provide basic information.

Adding group

Group basic settings

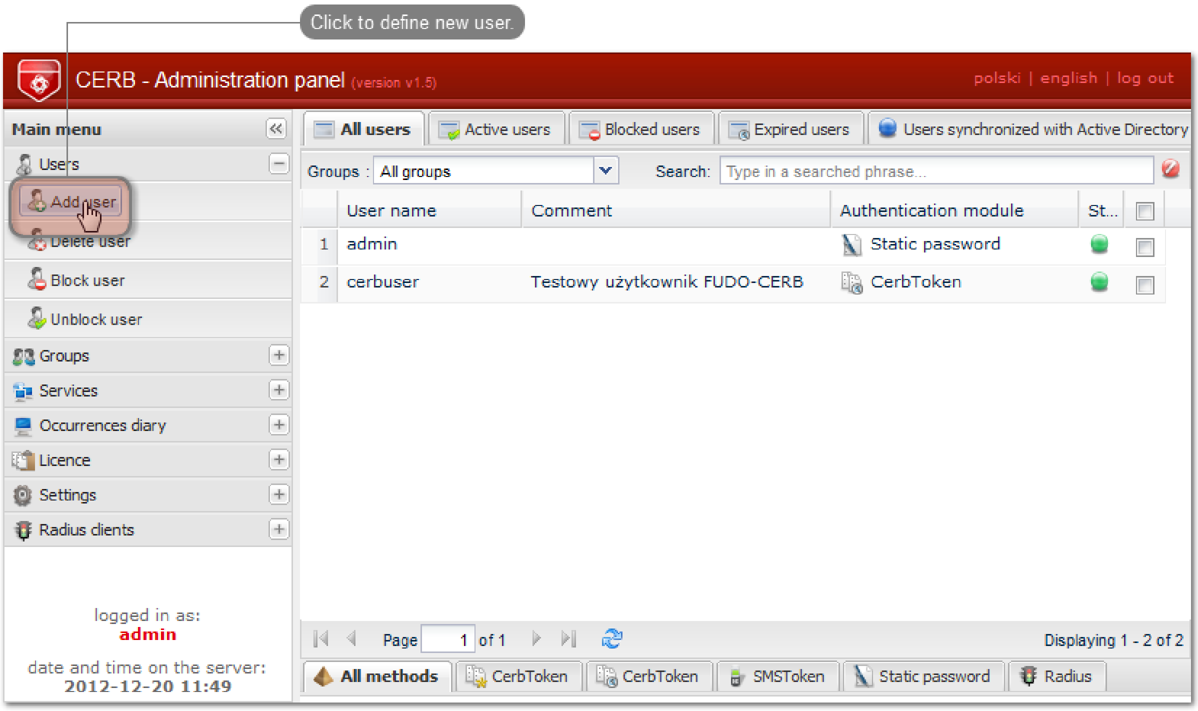
Group name: fudo_users

Comment: FUDO users

Click to add group definition.

3. Adding user.

- Select *Users* > *Add user* to open new user definition window.



Click to define new user.

CERB - Administration panel (version v1.5)

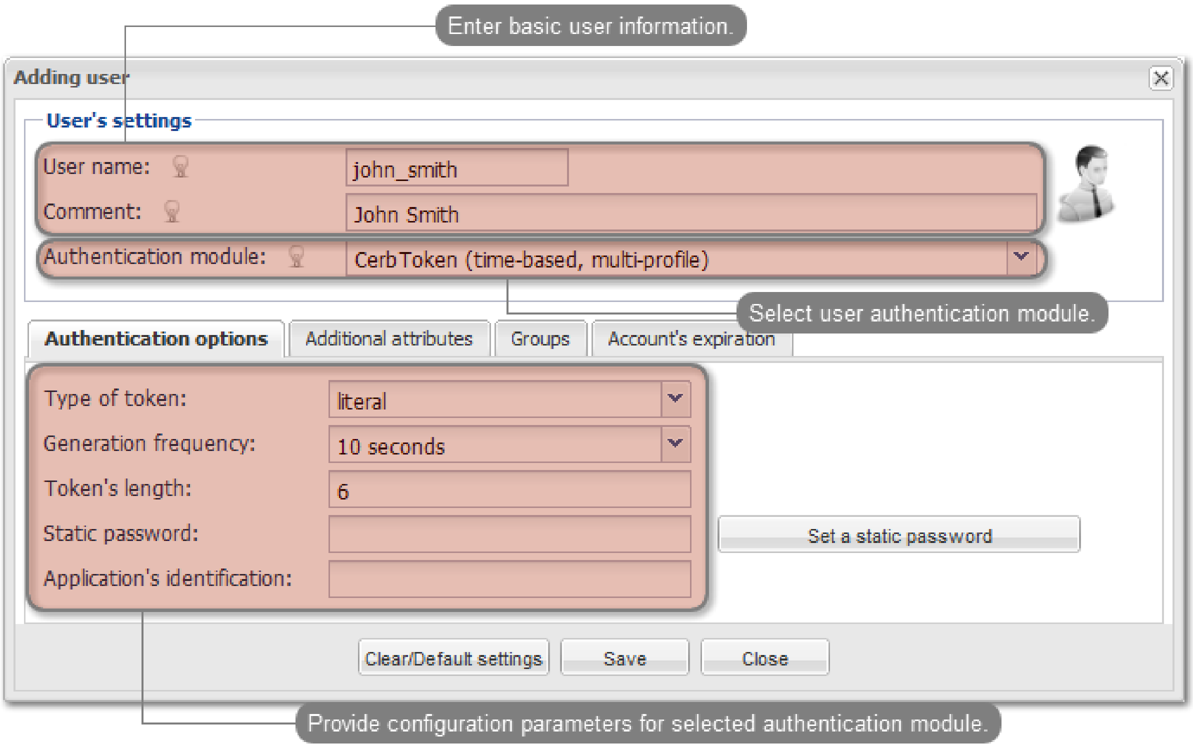
	User name	Comment	Authentication module	St...	□
1	admin		Static password	●	□
2	cerbuser	Testowy użytkownik FUDO-CERB	CerbToken	●	□

Page 1 of 1 Displaying 1 - 2 of 2

logged in as: admin

date and time on the server: 2012-12-20 11:49

- Provide user name, description and select desired authorization module (refer to CERB server documentation form more information on authorization modules).



Enter basic user information.

Adding user

User's settings

User name: john_smith

Comment: John Smith

Authentication module: CerbToken (time-based, multi-profile)

Select user authentication module.

Type of token: literal

Generation frequency: 10 seconds

Token's length: 6

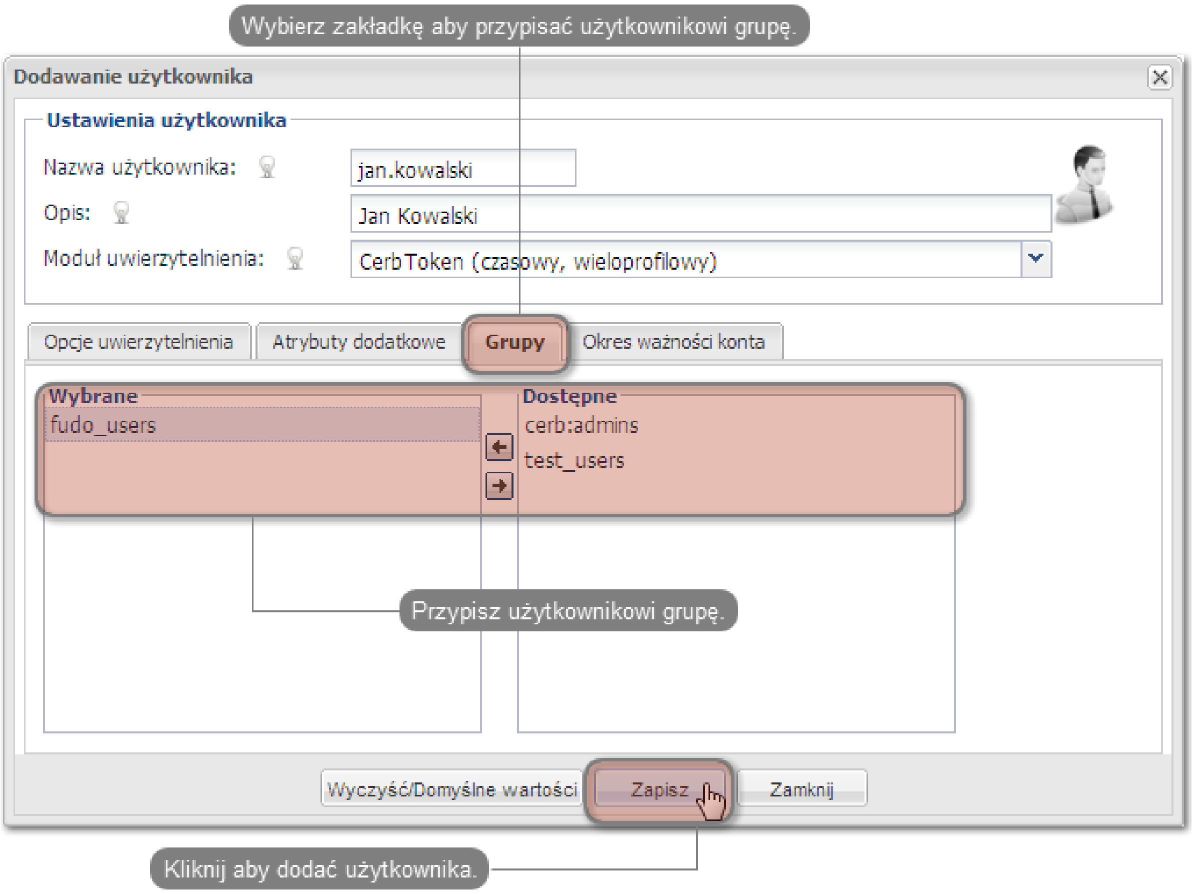
Static password:

Application's identification:

Provide configuration parameters for selected authentication module.

Note: Username is used to authenticate users on Fudo PAM.

- Assign user to previously created `fudo_users` group and click *Save*.



Wybierz zakładkę aby przypisać użytkownikowi grupę.

Dodawanie użytkownika

Ustawienia użytkownika

Nazwa użytkownika: jan.kowalski

Opis: Jan Kowalski

Moduł uwierzytelnienia: CerbToken (czasowy, wieloprofilowy)

Wybrane: fudo_users

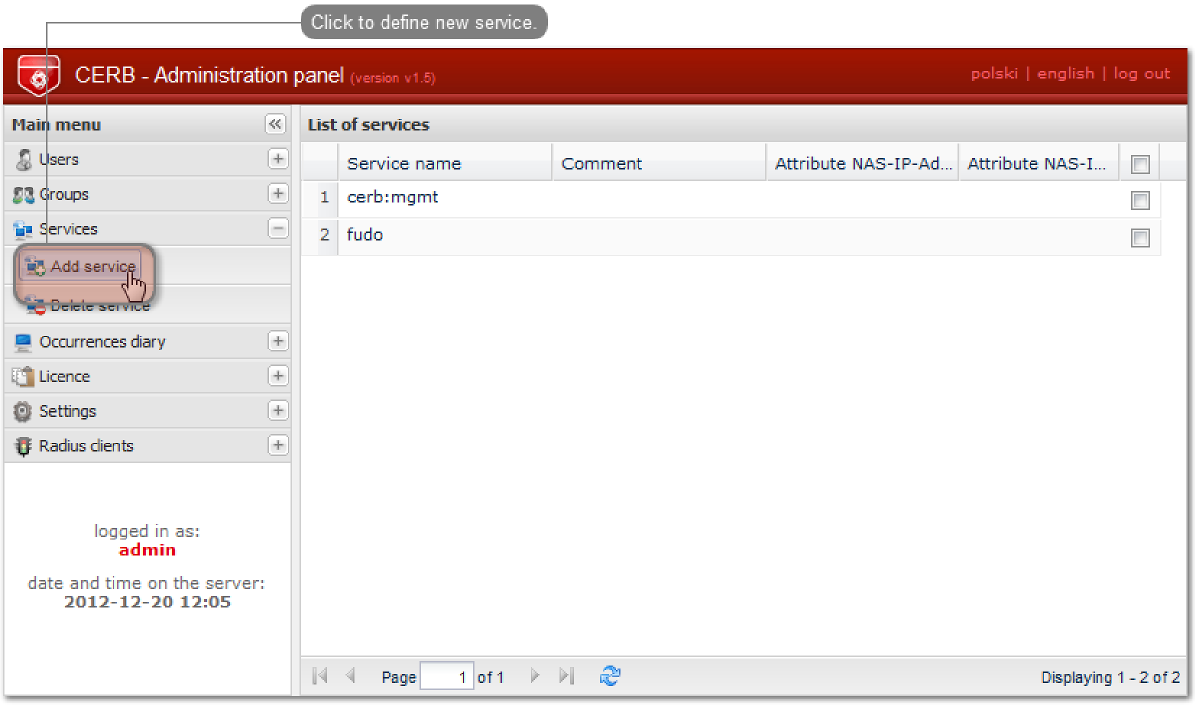
Dostępne: cerb:admins, test_users

Przypisz użytkownikowi grupę.

Kliknij aby dodać użytkownika.

4. Configuring service.

- Select *Services* > *Add service* to open new service definition window.



Click to define new service.

logged in as: **admin**

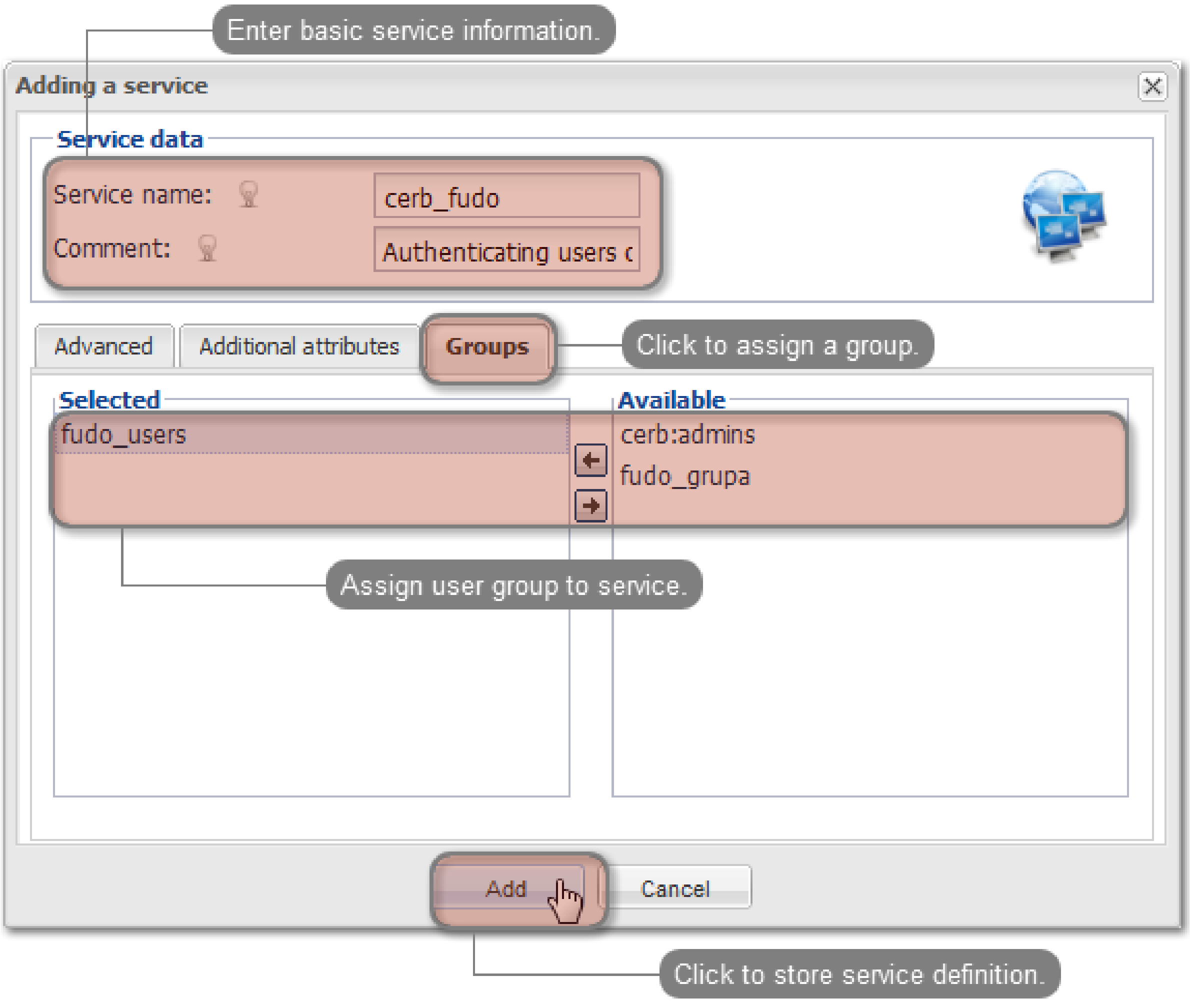
date and time on the server: **2012-12-20 12:05**

List of services

	Service name	Comment	Attribute NAS-IP-Ad...	Attribute NAS-I...	□
1	cerb:mgmt				□
2	fudo				□

- Provide name identifying authorization service (`cerb_fudo`) and service description.

- Add `fudo_users` group to service and click *Add*.



Adding a service

Service data

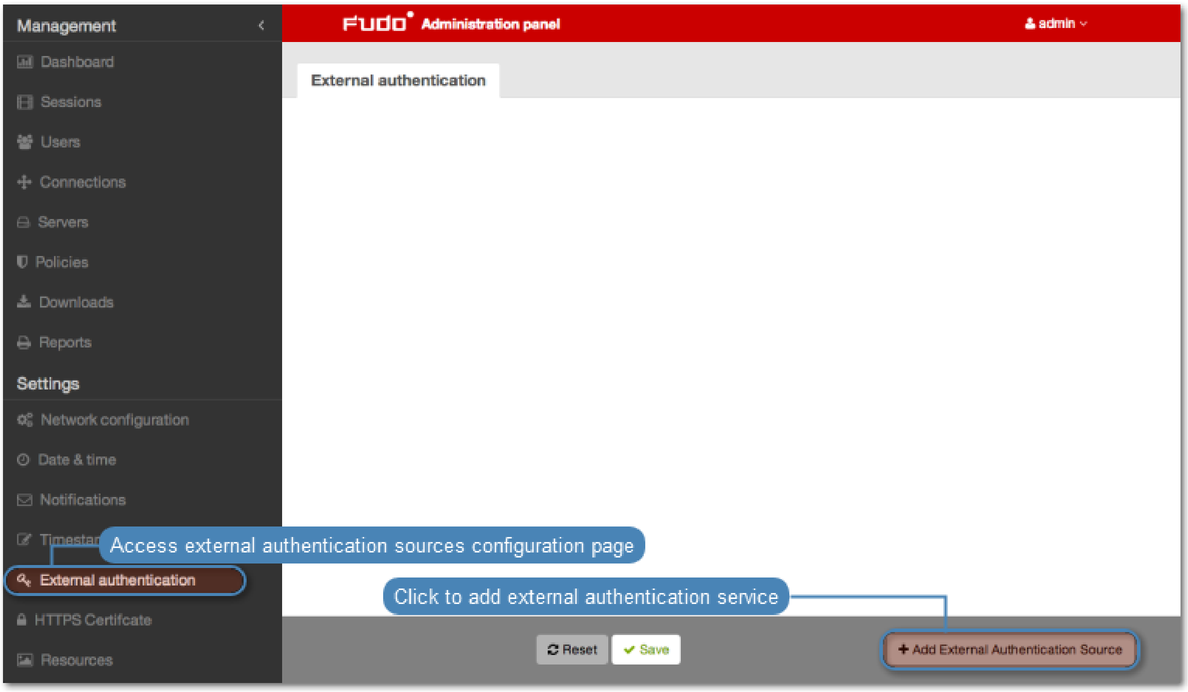
Service name: cerb_fudo

Comment: Authenticating users c

|product_name| server configuration

1. Adding CERB external authorization server.

- Select *Settings > External authentication*.
- Click *Add external authentication source* to add CERB server definition.

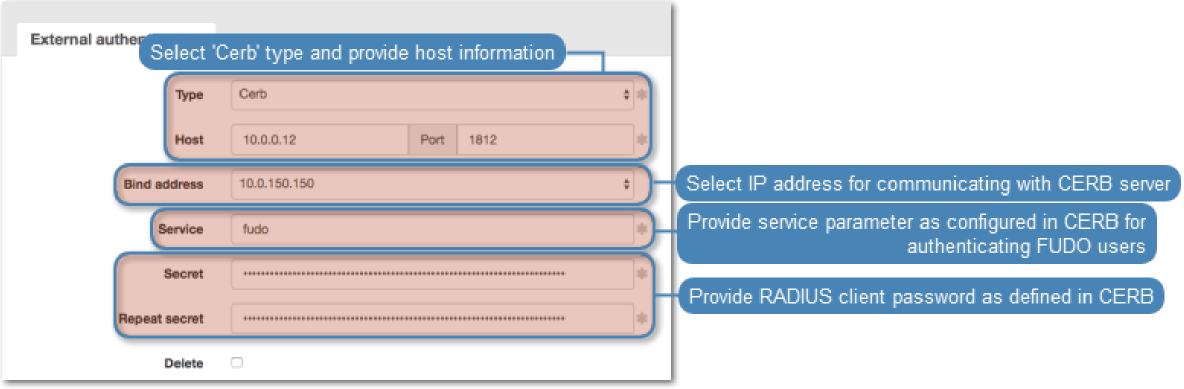


Access external authentication sources configuration page

Click to add external authentication service

- 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



Select 'Cerb' type and provide host information

Type	Cerb
Host	10.0.0.12
Port	1812
Bind address	10.0.150.150
Service	fudo
Secret	••
Repeat secret	••

Select IP address for communicating with CERB server

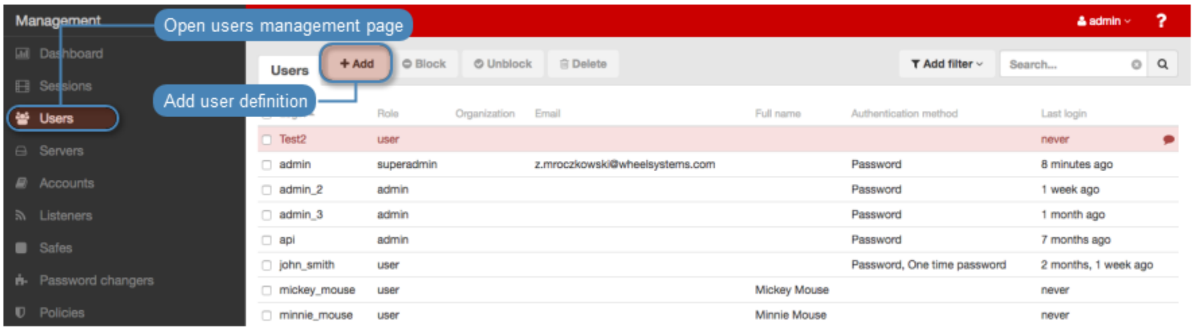
Provide service parameter as configured in CERB for authenticating FUDO users

Provide RADIUS client password as defined in CERB

- Click *Save*.

2. Adding user.

- Select *Management* > *Users*.
- Click *Add*.



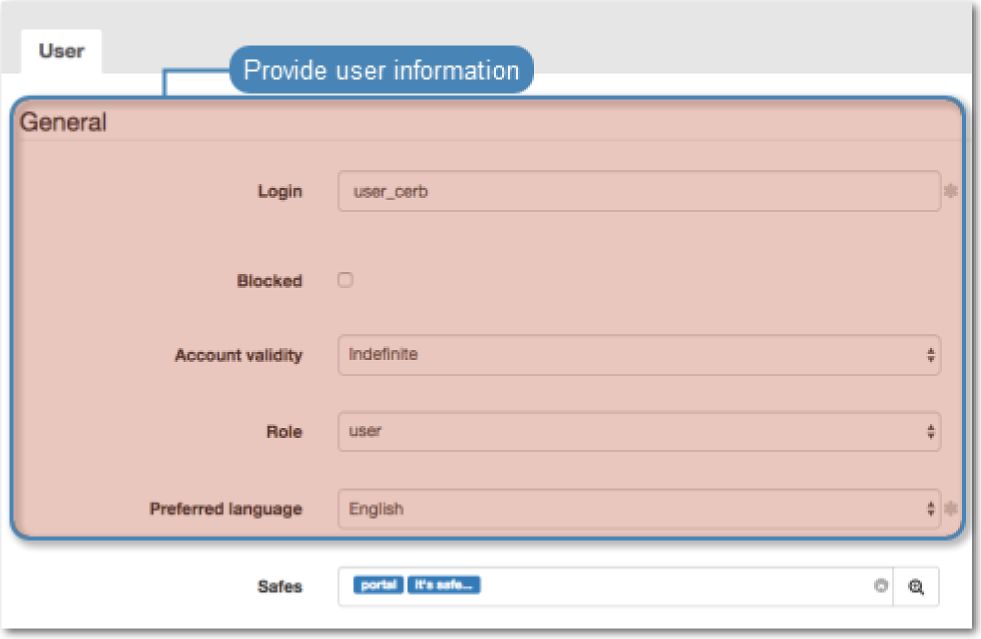
Open users management page

Add user definition

	Role	Organization	Email	Full name	Authentication method	Last login
□ Test2	user					never
□ admin	superadmin		z.mroczkowski@wheelsystems.com		Password	8 minutes ago
□ admin_2	admin				Password	1 week ago
□ admin_3	admin				Password	1 month ago
□ api	admin				Password	7 months ago
□ john_smith	user				Password, One time password	2 months, 1 week ago
□ mickey_mouse	user			Mickey Mouse		never
□ minnie_mouse	user			Minnie Mouse		never

- Provide basic user information.

Note: Username must match the user name defined on CERB server.

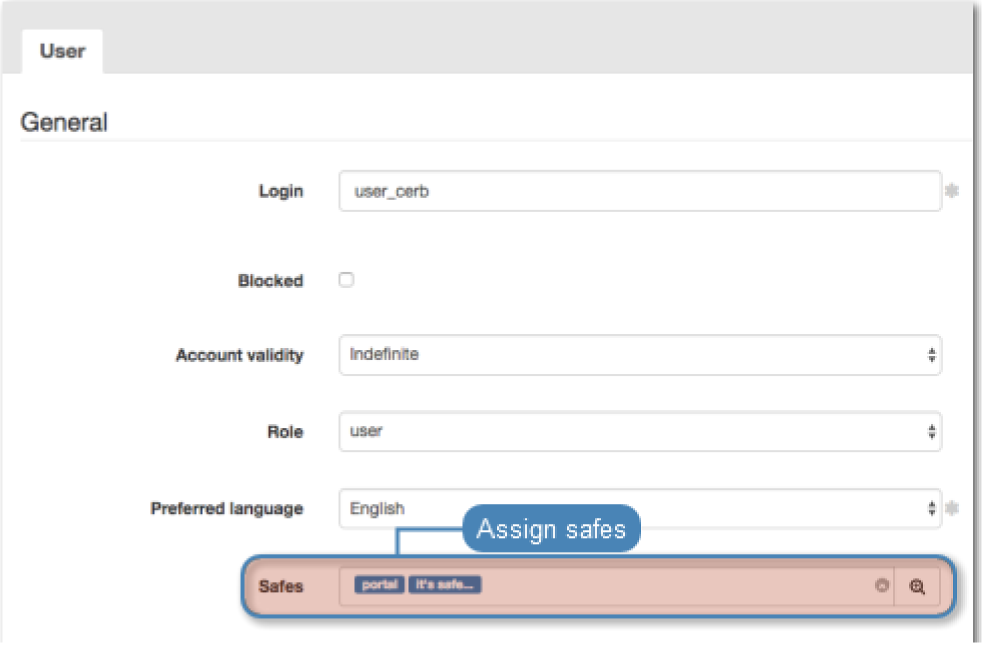


Provide user information

General

Login	user_cerb
Blocked	□
Account validity	Indefinite
Role	user
Preferred language	English
Safes	portal It's safe...

- Add safes that the user will be able to access.



User

General

Login: user_cerb

Blocked: □

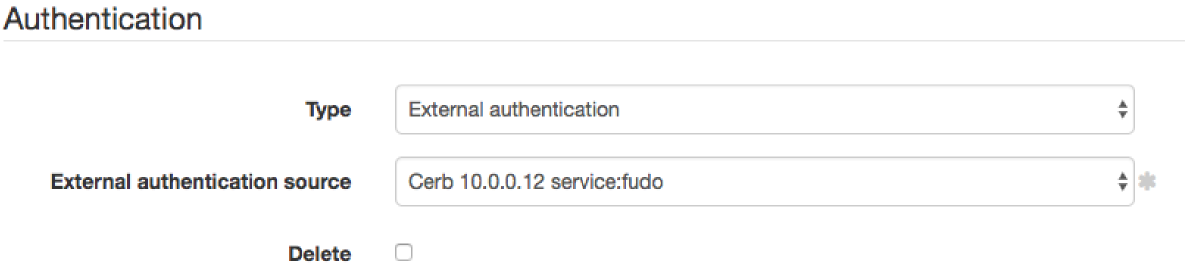
Account validity: Indefinite

Role: user

Preferred language: English

Safes: portal, It's safe...

- In the *Authentication* section, select *External authentication* from the *Type* drop-down list and select previously created Cerb server from the *External authentication source* drop-down list.



Authentication

Type: External authentication

External authentication source: Cerb 10.0.0.12 service:fudo

Delete: □

- Click *Save*.

Related topics:

- *Users*
- *External authentication*
- *User authentication methods and modes*

15.19 System maintenance

The following section contains descriptions of maintenance procedures.

15.19.1 Backing up encryption keys

Encryption keys stored on USB flash drives are necessary to initialize the file system, which stores session data. If the USB flash drive is lost or damaged, it will be impossible to boot the system and access session data.

Microsoft Windows

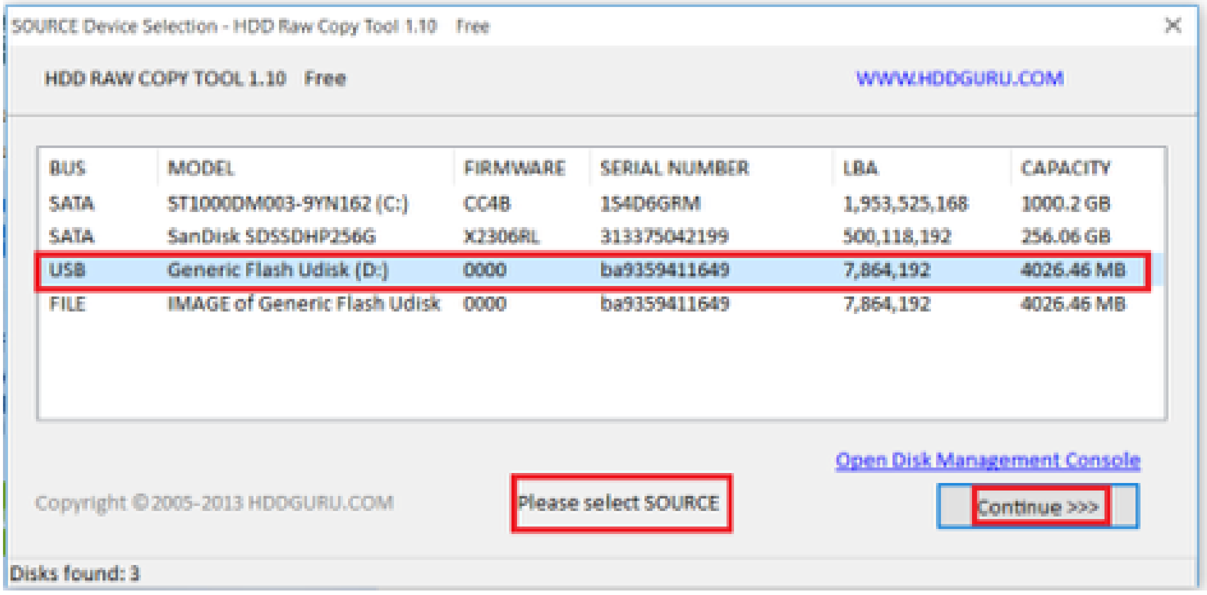
Warning: After connecting the flash drive to your computer, do not initiate or format it. Ignore the system message about it not being able to read data and proceed with the backup procedure.

1. Download and install *HDD Raw Copy Tool*.

   `http://hddguru.com/software/HDD-Raw-Copy-Tool/` (portable version is also available)

2. Start the program.

3. On the source drive selection window, choose the USB drive with the encription key and click *Continue*.

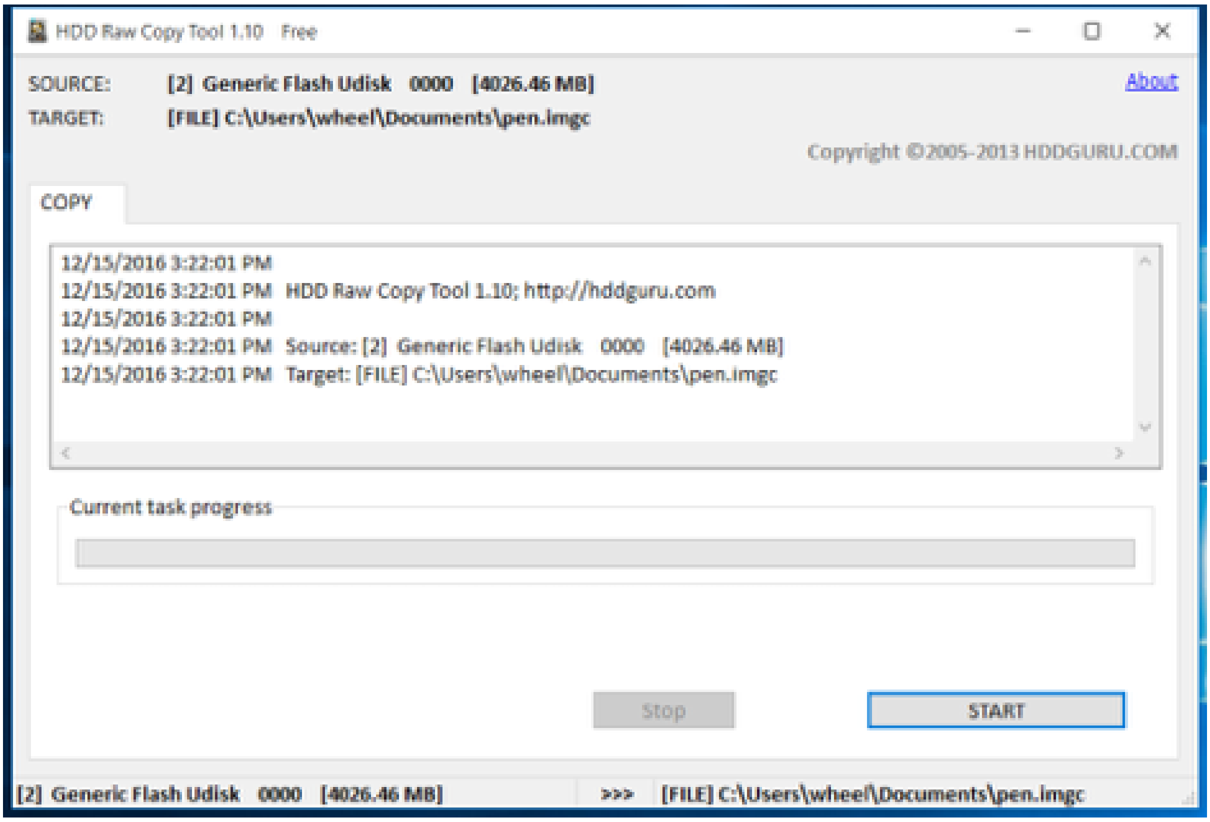

SOURCE Device Selection - HDD Raw Copy Tool 1.10 Free
HDD RAW COPY TOOL 1.10 Free
WWW.HDDGURU.COM
Open Disk Management Console
Copyright ©2005-2013 HDDGURU.COM
Please select SOURCE
Continue >>>

BUS	MODEL	FIRMWARE	SERIAL NUMBER	LBA	CAPACITY
SATA	ST1000DM003-9YN162 (C:)	CC4B	154D6GRM	1,953,525,168	1000.2 GB
SATA	SanDisk SDSSDHP256G	X2306RL	313375042199	500,118,192	256.06 GB
USB	Generic Flash Udisk (D:)	0000	ba9359411649	7,864,192	4026.46 MB
FILE	IMAGE of Generic Flash Udisk	0000	ba9359411649	7,864,192	4026.46 MB

Disks found: 3

4. Click *FILE* twice, select the target image file and click *Continue*.

5. Click *START* to proceed with copying data.



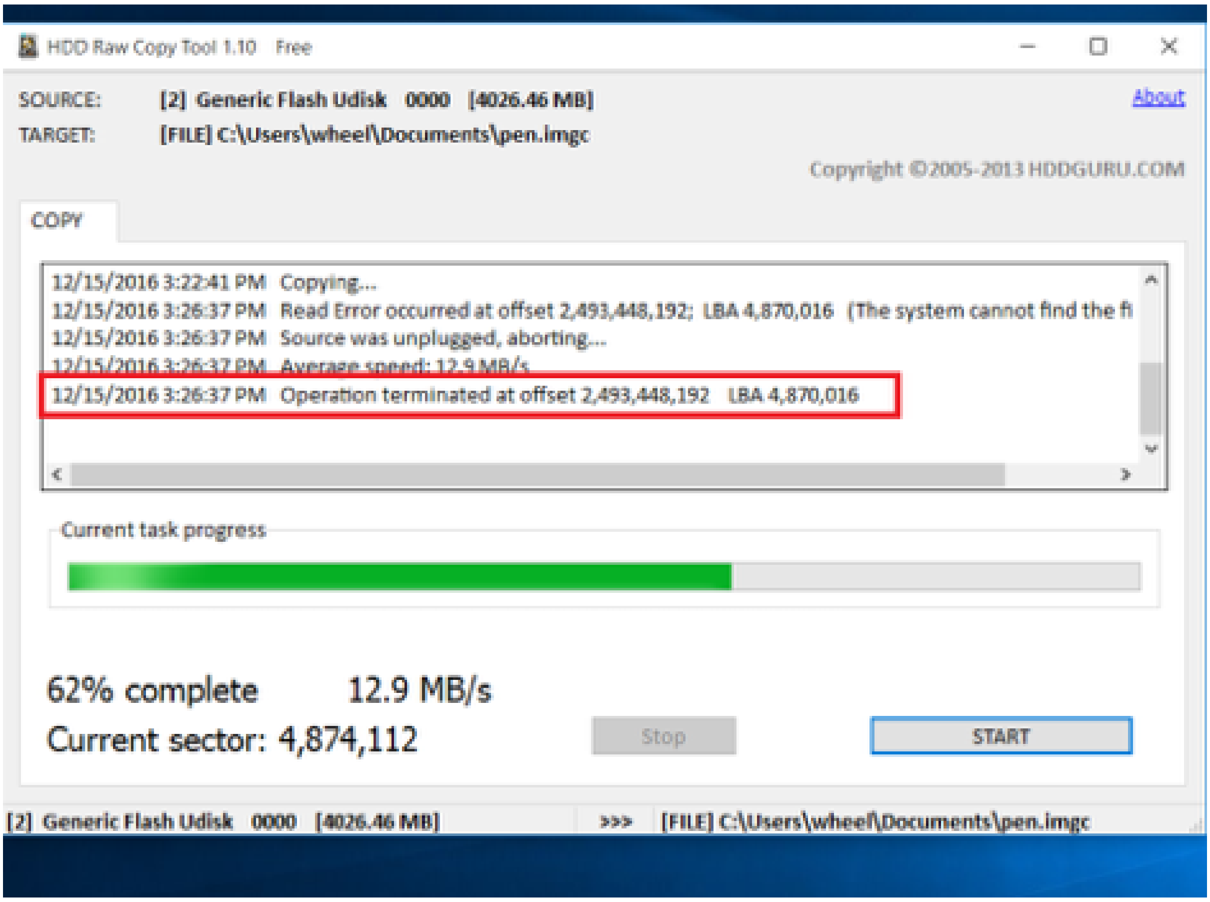
SOURCE: [2] Generic Flash Udisk 0000 [4026.46 MB]
TARGET: [FILE] C:\Users\wheel\Documents\pen.imgc

```
12/15/2016 3:22:01 PM
12/15/2016 3:22:01 PM  HDD Raw Copy Tool 1.10; http://hddguru.com
12/15/2016 3:22:01 PM
12/15/2016 3:22:01 PM  Source: [2]  Generic Flash Udisk   0000   [4026.46 MB]
12/15/2016 3:22:01 PM  Target: [FILE] C:\Users\wheel\Documents\pen.imgc
```

[2] Generic Flash Udisk 0000 [4026.46 MB] >>> [FILE] C:\Users\wheel\Documents\pen.imgc

6. Once the following message occurs

   `Operation terminated at offset...` close the application and disconnect the USB drive.



SOURCE: [2] Generic Flash Udisk 0000 [4026.46 MB]

TARGET: [FILE] C:\Users\wheel\Documents\pen.imgc

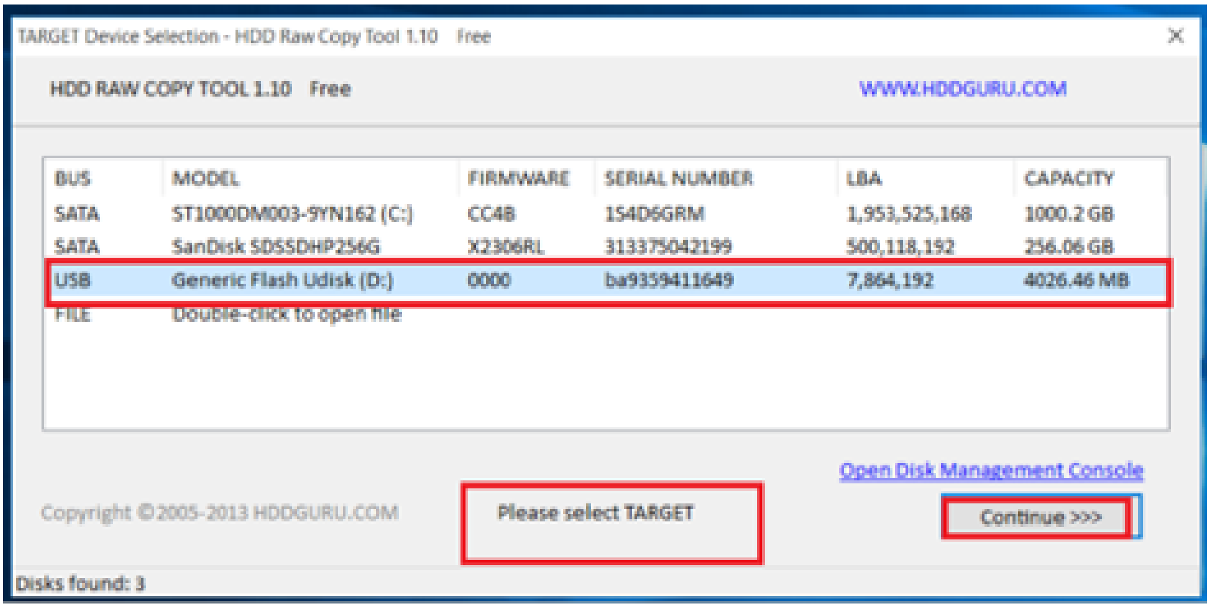
```
12/15/2016 3:22:41 PM  Copying...
12/15/2016 3:26:37 PM  Read Error occurred at offset 2,493,448,192;  LBA 4,870,016  (The system cannot find the fi
12/15/2016 3:26:37 PM  Source was unplugged, aborting...
12/15/2016 3:26:37 PM  Average speed: 12.9 MB/s
12/15/2016 3:26:37 PM  Operation terminated at offset 2,493,448,192   LBA 4,870,016
```

62% complete 12.9 MB/s

Current sector: 4,874,112

[2] Generic Flash Udisk 0000 [4026.46 MB] >>> [FILE] C:\Users\wheel\Documents\pen.imgc

7. Connect another USB drive and start *HDD Raw Copy Tool*.
8. On the source drive selection screen select *FILE* and browse the file system to find the encryption keys image file.
9. Select the newly connected USB flash drive as a target device and click *Continue*.



TARGET Device Selection - HDD Raw Copy Tool 1.10 Free
HDD RAW COPY TOOL 1.10 Free
WWW.HDDGURU.COM

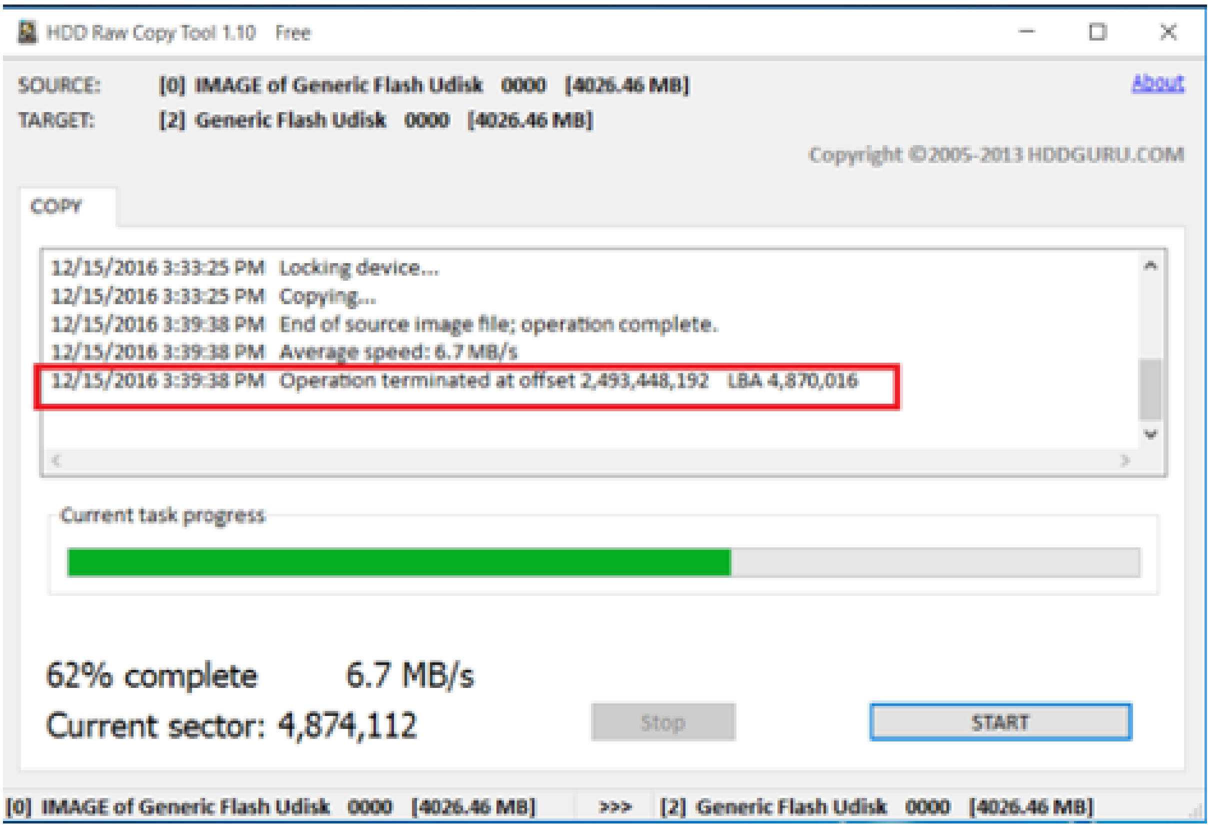
BUS	MODEL	FIRMWARE	SERIAL NUMBER	LBA	CAPACITY
SATA	ST1000DM003-9YN162 (C:)	CC4B	154D6GRM	1,953,525,168	1000.2 GB
SATA	SanDisk SDSSDHP256G	X2306RL	313375042199	500,118,192	256.06 GB
USB	Generic Flash Udisk (D:)	0000	ba9359411649	7,864,192	4026.46 MB
FILE	Double-click to open file				

Open Disk Management Console
Copyright ©2005-2013 HDDGURU.COM
Please select TARGET
Continue >>>
Disks found: 3

10. Click *Continue*.
11. Click *START*.

12. The copying will end once the following message occurs:

```
Operation terminated at offset....
```



SOURCE: [0] IMAGE of Generic Flash Udisk 0000 [4026.46 MB]

TARGET: [2] Generic Flash Udisk 0000 [4026.46 MB]

```
12/15/2016 3:33:25 PM  Locking device...
12/15/2016 3:33:25 PM  Copying...
12/15/2016 3:39:38 PM  End of source image file; operation complete.
12/15/2016 3:39:38 PM  Average speed: 6.7 MB/s
12/15/2016 3:39:38 PM  Operation terminated at offset 2,493,448,192   LBA 4,870,016
```

62% complete 6.7 MB/s

Current sector: 4,874,112

[0] IMAGE of Generic Flash Udisk 0000 [4026.46 MB] >>> [2] Generic Flash Udisk 0000 [4026.46 MB]

13. Close the application and disconnect the USB drive.

Mac OS X

1. Start the terminal.
2. Execute the `sudo -s` command and enter password.
3. Execute the `diskutil list` to list connected drives.
4. Find the drive with the following partitions layout:

```
/dev/disk2 (external, physical):
#: TYPE NAME SIZE IDENTIFIER
0: GUID_partition_scheme *8.0 GB disk2
1: F649773F-1CD6-11E1-9AD2-00262DF29F0D 3.1 KB disk2s1
2: 2B163C2B-1FE5-11E1-8300-00262DF29F0D 1.0 KB disk2s2
```

5. Execute the `dd if=/dev/disk2 of=fudo_pen.img bs=1m` command, where `if` points to the USB drive.
6. Disconnect the flash drive and connect the new one.
7. Execut the `dd if=fudo_pen.img of=/dev/disk2 bs=1m` command.
8. Execute the `sync` command.
9. Disconnect the USB flash drive from your computer.

Linux

1. Start the terminal.
2. Execute the `sudo -s` command and enter password.
3. Execute the `dmesg | less` command to determine the USB flash drive identifier.
4. Execute the `dd if=/dev/disk2 of=fudo_pen.img bs=1m` command, where `if` points to the USB drive.
5. Disconnect the flash drive and connect the new one.
6. Execut the `dd if=fudo_pen.img of=/dev/disk2 bs=1m` command.
7. Execute the `sync` command.
8. Disconnect the USB flash drive from your computer.

Related topics:

- *Events log*
- *Frequently asked questions*

15.19.2 Monitoring system condition

Monitoring system condition allows preventing system failures and overloads, ensuring Fudo PAM Fudo PAM remains operational.

Monitoring active sessions

1. Login to Fudo PAM administration panel.
2. Select *Management > Dashboard*.
3. Check the number of currently running user sessions.

Note: Fudo PAM supports up to 300 RDP connections.

Monitoring network bandwidth

1. Login to Fudo PAM administration panel.
2. Select *Management > Dashboard*.
3. Check current network transfer rate.

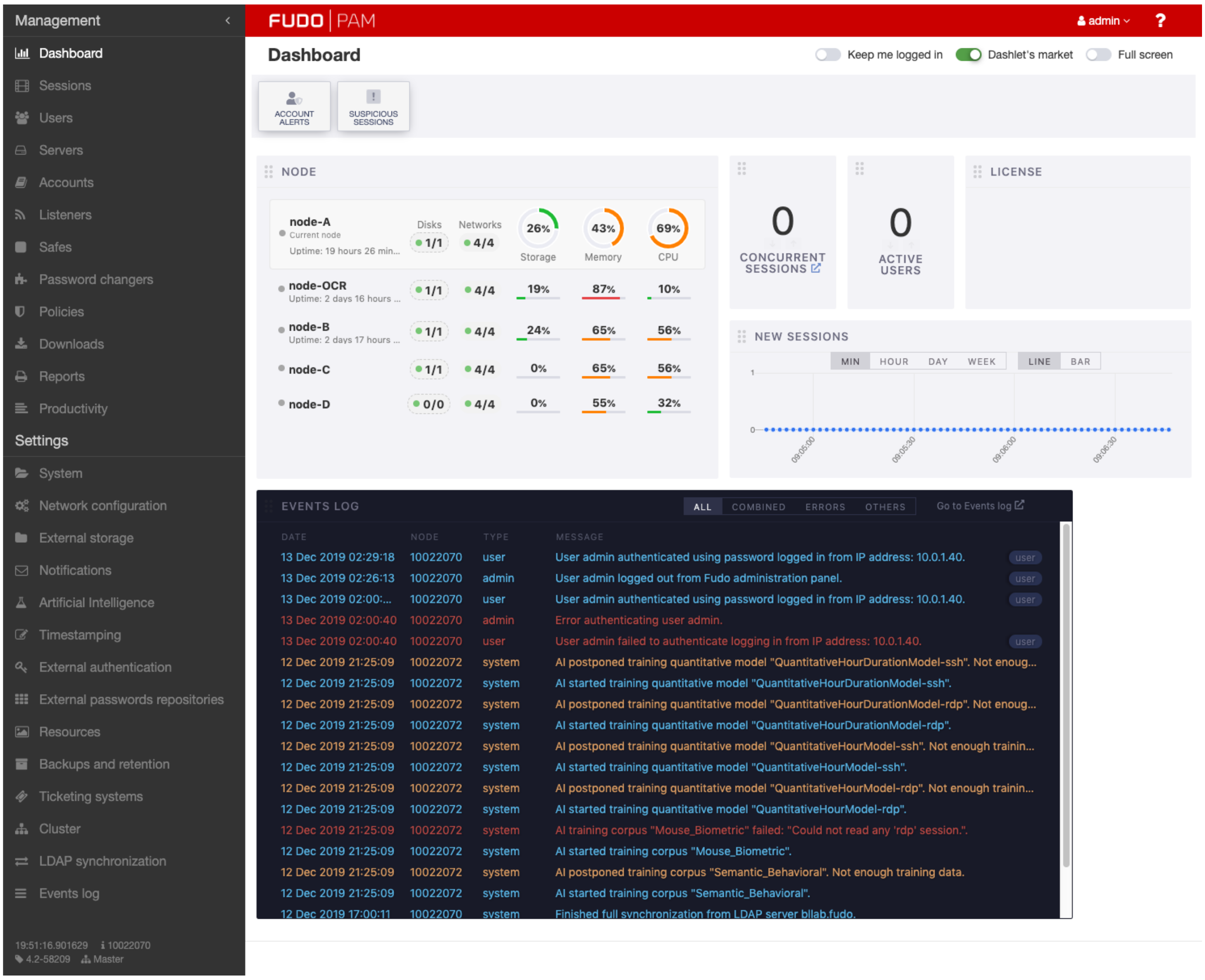
Note: Fudo PAM features 1Gbps network interface cards. In case the current network bandwidth usage exceeds 500Mbps, users may notice a decrease in system communication performance.

Monitoring storage

Warning: Fudo PAM will not allow new connections when storage usage reaches 90%.

1. Login to Fudo PAM administration panel.
2. Select *Management > Dashboard*.

3. Check the storage usage percentage, review and delete archived sessions to free up space if need be.



	Disks	Networks	Storage	Memory	CPU
node-A Current node Uptime: 19 hours 26 min...	● 1/1	● 4/4	26%	43%	69%
node-OCR Uptime: 2 days 16 hours ...	● 1/1	● 4/4	19%	87%	10%
node-B Uptime: 2 days 17 hours ...	● 1/1	● 4/4	24%	65%	56%
node-C	● 1/1	● 4/4	0%	65%	56%
node-D	● 0/0	● 4/4	0%	55%	32%

```
DATE                  NODE      TYPE    MESSAGE
13 Dec 2019 02:29:18  10022070  user    User admin authenticated using password logged in from IP address: 10.0.1.40.      user
13 Dec 2019 02:26:13  10022070  admin   User admin logged out from Fudo administration panel.                               user
13 Dec 2019 02:00:... 10022070  user    User admin authenticated using password logged in from IP address: 10.0.1.40.      user
13 Dec 2019 02:00:40  10022070  admin   Error authenticating user admin.
13 Dec 2019 02:00:40  10022070  user    User admin failed to authenticate logging in from IP address: 10.0.1.40.           user
12 Dec 2019 21:25:09  10022072  system  AI postponed training quantitative model "QuantitativeHourDurationModel-ssh". Not enoug...
12 Dec 2019 21:25:09  10022072  system  AI started training quantitative model "QuantitativeHourDurationModel-ssh".
12 Dec 2019 21:25:09  10022072  system  AI postponed training quantitative model "QuantitativeHourDurationModel-rdp". Not enoug...
12 Dec 2019 21:25:09  10022072  system  AI started training quantitative model "QuantitativeHourDurationModel-rdp".
12 Dec 2019 21:25:09  10022072  system  AI postponed training quantitative model "QuantitativeHourModel-ssh". Not enough trainin...
12 Dec 2019 21:25:09  10022072  system  AI started training quantitative model "QuantitativeHourModel-ssh".
12 Dec 2019 21:25:09  10022072  system  AI postponed training quantitative model "QuantitativeHourModel-rdp". Not enough trainin...
12 Dec 2019 21:25:09  10022072  system  AI started training quantitative model "QuantitativeHourModel-rdp".
12 Dec 2019 21:25:09  10022072  system  AI training corpus "Mouse_Biometric" failed: "Could not read any 'rdp' session.".
12 Dec 2019 21:25:09  10022072  system  AI started training corpus "Mouse_Biometric".
12 Dec 2019 21:25:09  10022072  system  AI postponed training corpus "Semantic_Behavioral". Not enough training data.
12 Dec 2019 21:25:09  10022072  system  AI started training corpus "Semantic_Behavioral".
12 Dec 2019 17:00:11  10022070  system  Finished full synchronization from LDAP server bllab.fudo.
```

Related topics:

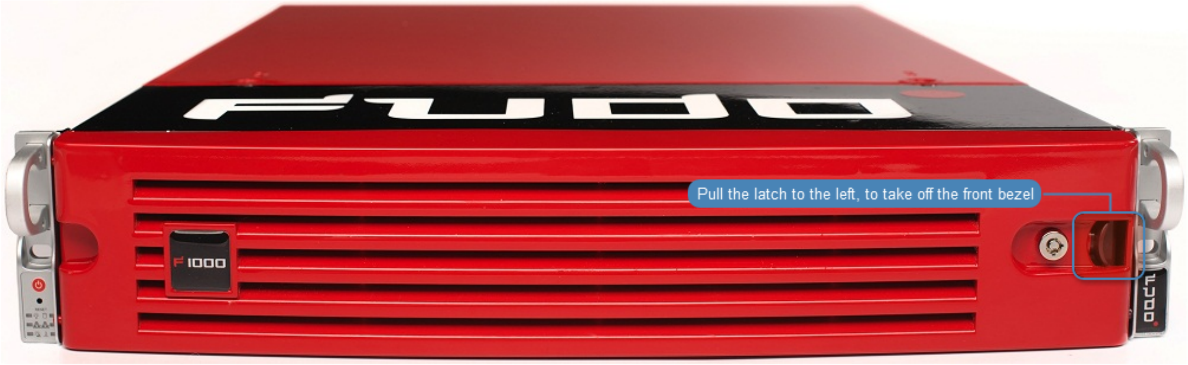
- *System log*
- *Frequently asked questions*

15.19.3 Hard drive replacement

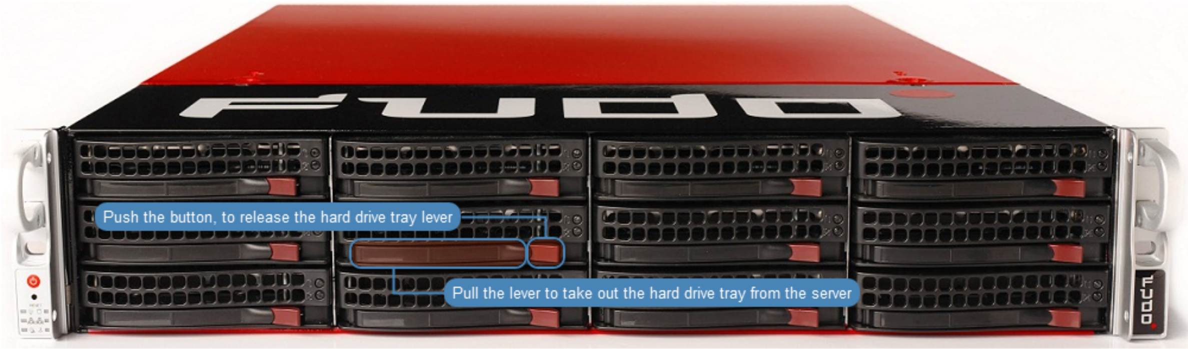
In default configuration, Fudo PAM's storage array comprises 12 hard drives in RAIDZ2 configuration running ZFS file system allowing the system to remain fully operational in case of a failure of two hard drives.

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.


Push the button, to release the hard drive tray lever
Pull the lever to take out the hard drive tray from the server

3. Unscrew the screws securing the hard drive and take out the hard drive from the tray.
4. Install replacement hard drive in the tray and secure it with the screws.
5. Install the hard drive tray back in the server.

Note: Fudo PAM will automatically detect the change in the storage array state and will start rebuilding the data structure. The duration of the array rebuilding process depends on the volume of data stored on the server.

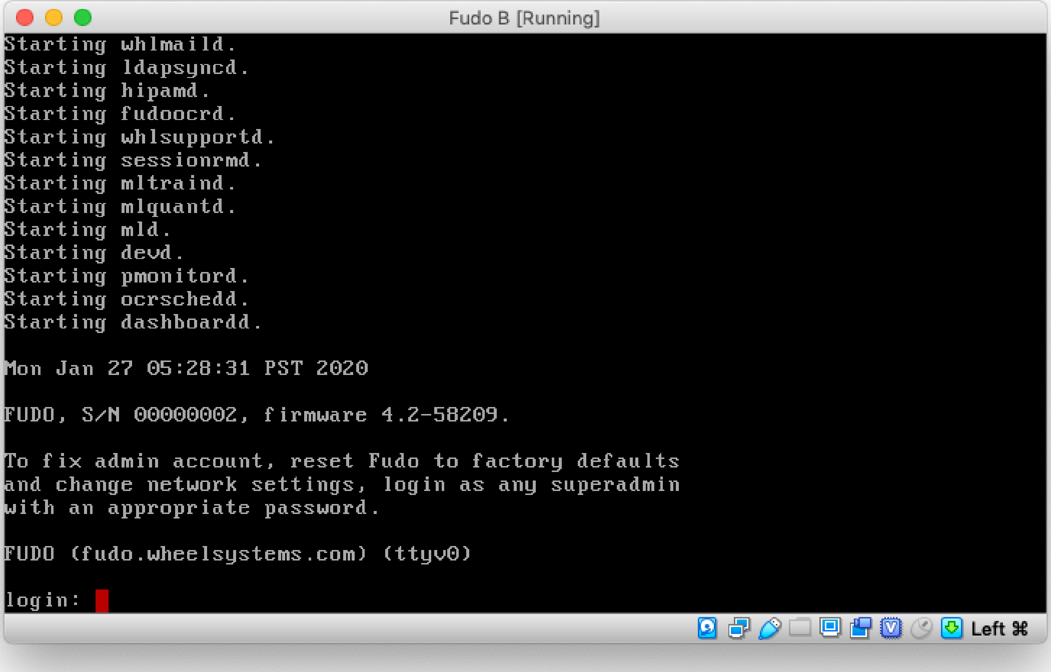
Related topics:

- *Hardware overview*
- *Frequently asked questions*

15.19.4 Resetting configuration to default settings

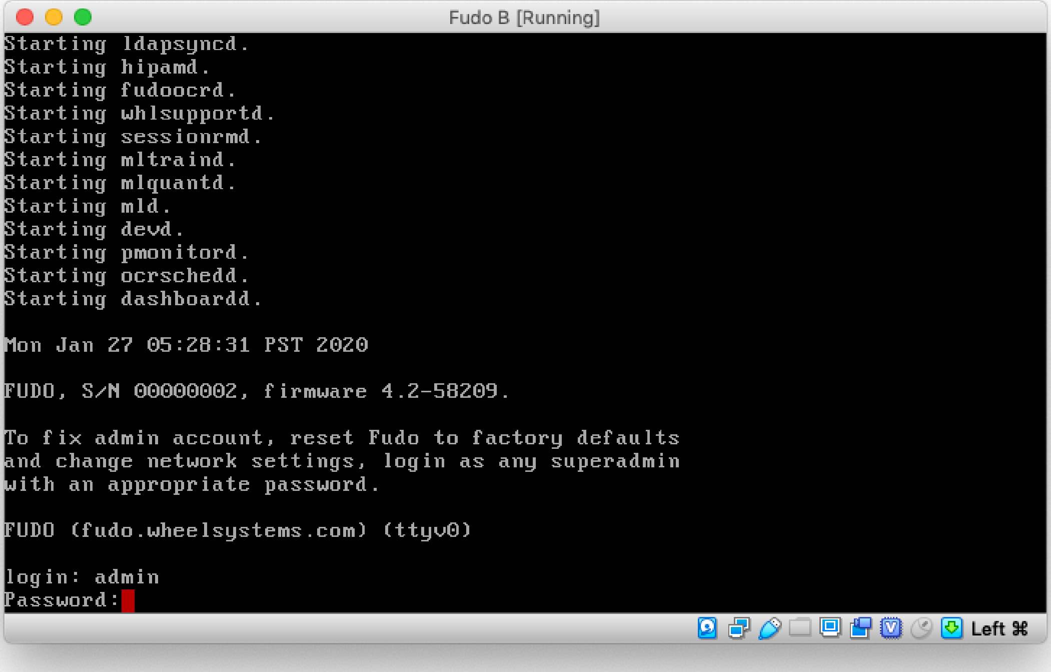
Warning: Configuration reset procedure is irreversible and it results in deleting all recorded sessions, system settings and defined objects. The device needs 2 pendrives plugged in to be properly executed.

1. Access system terminal.
2. Enter administrator account login and press *Enter*.



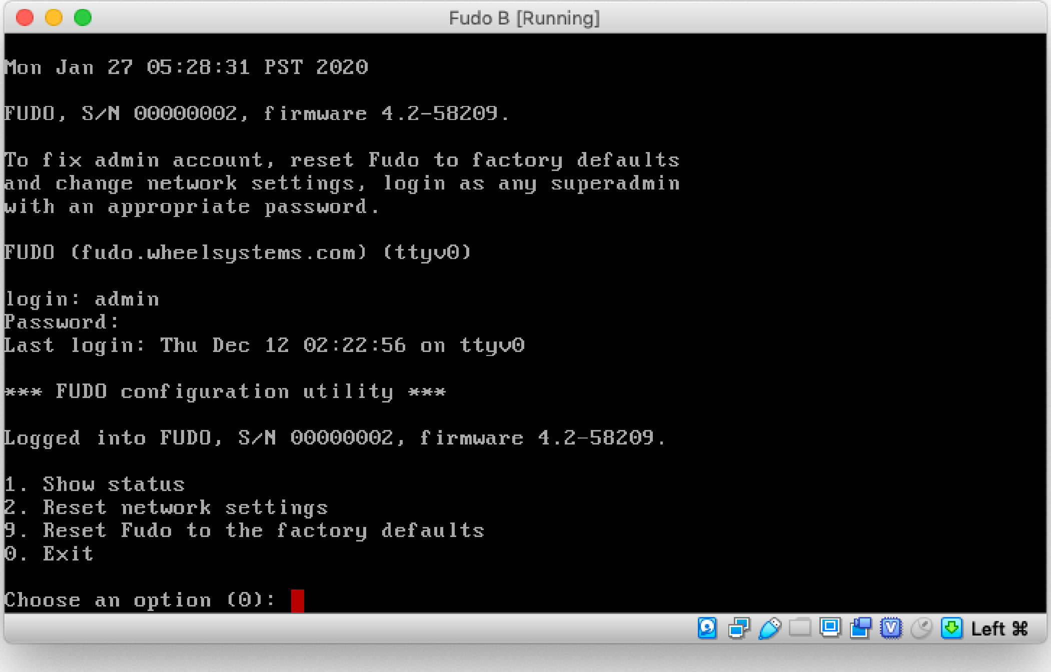
```
Starting whlmaild.
Starting ldapsyncd.
Starting hipamd.
Starting fudoocrd.
Starting whlsupportd.
Starting sessionrmd.
Starting mltraind.
Starting mlquantd.
Starting mld.
Starting devd.
Starting pmonitord.
Starting ocrschedd.
Starting dashboardd.

Mon Jan 27 05:28:31 PST 2020

FUDO, S/N 00000002, firmware 4.2-58209.

To fix admin account, reset Fudo to factory defaults
and change network settings, login as any superadmin
with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login:
```

3. Enter administrator account password and press *Enter*.



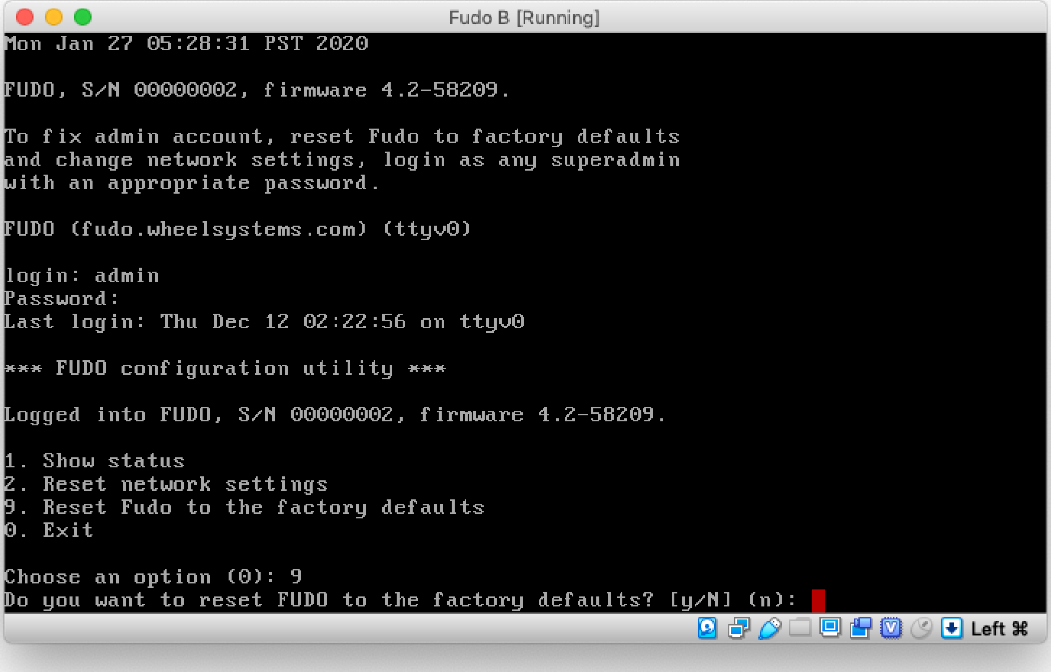
```
Starting ldapsyncd.
Starting hipamd.
Starting fudoocrd.
Starting whlsupportd.
Starting sessionrmd.
Starting mltraind.
Starting mlquantd.
Starting mld.
Starting devd.
Starting pmonitord.
Starting ocrschedd.
Starting dashboardd.

Mon Jan 27 05:28:31 PST 2020

FUDO, S/N 00000002, firmware 4.2-58209.

To fix admin account, reset Fudo to factory defaults
and change network settings, login as any superadmin
with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
```

4. Enter 9 and press *Enter*.



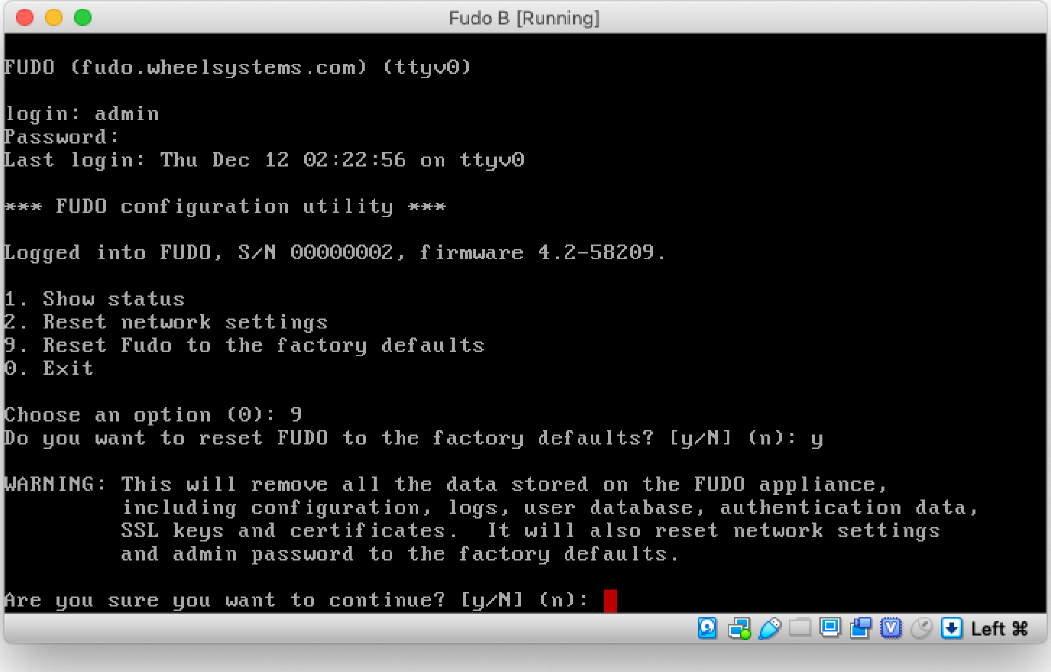
```
Mon Jan 27 05:28:31 PST 2020

FUDO, S/N 00000002, firmware 4.2-58209.

To fix admin account, reset Fudo to factory defaults
and change network settings, login as any superadmin
with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Thu Dec 12 02:22:56 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 00000002, firmware 4.2-58209.

1. Show status
2. Reset network settings
9. Reset Fudo to the factory defaults
0. Exit

Choose an option (0):
```

5. Enter y and press *Enter*.



```
Mon Jan 27 05:28:31 PST 2020

FUDO, S/N 00000002, firmware 4.2-58209.

To fix admin account, reset Fudo to factory defaults
and change network settings, login as any superadmin
with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Thu Dec 12 02:22:56 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 00000002, firmware 4.2-58209.

1. Show status
2. Reset network settings
9. Reset Fudo to the factory defaults
0. Exit

Choose an option (0): 9
Do you want to reset FUDO to the factory defaults? [y/N] (n):
```

6. Enter y and press *Enter* to proceed with factory reset.



```
FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Thu Dec 12 02:22:56 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 00000002, firmware 4.2-58209.

1. Show status
2. Reset network settings
9. Reset Fudo to the factory defaults
0. Exit

Choose an option (0): 9
Do you want to reset FUDO to the factory defaults? [y/N] (n): y

WARNING: This will remove all the data stored on the FUDO appliance,
         including configuration, logs, user database, authentication data,
         SSL keys and certificates.  It will also reset network settings
         and admin password to the factory defaults.

Are you sure you want to continue? [y/N] (n):
```

Note: In case you are returning a demonstration unit, remember to also erase the USB flash drive containing the encryption key.

Related topics:

- *Network interfaces configuration*
- *System maintenance*

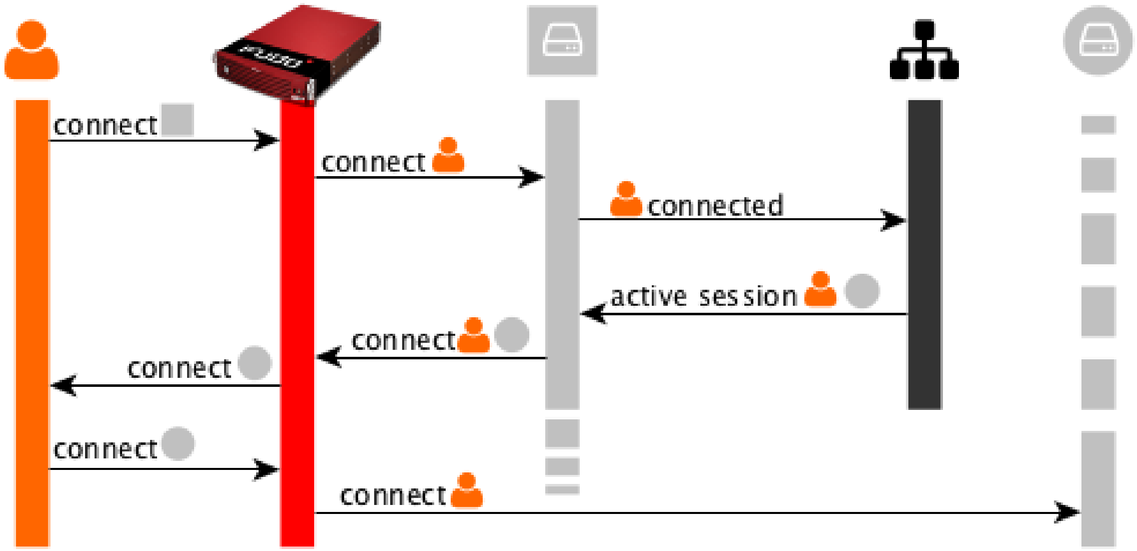
CHAPTER 16

Reference information

16.1 RDP connections broker

Connections broker enables users to reconnect to their existing sessions on a specific server within a pool of load-balanced resources.

If the broker identifies an existing user session on another server, the connection will be redirected to it and the user will be prompted to login again.



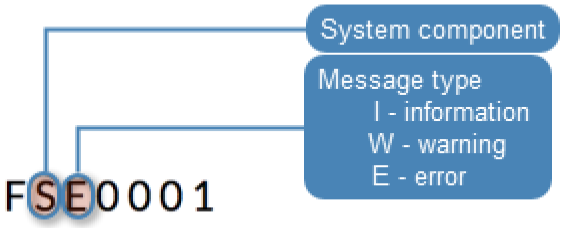
Note: To successfuly redirect a connection, the server identified by the broker must be defined on Fudo PAM, it must listen on default RDP port (3389) and user must be allowed to connect to given server.

Related topics:

- *Data model*
- *RDP*
- *Servers*
- *Accounts*

16.2 Log messages

Note: Message code contains information on the type of the log message and the component that logged the information.



Message code	Message and description
FSE0001	Internal system error.
FSE0002	Fudo certificate error.
FSE0003	Unable to change configuration settings.
FSE0004	Configuration import error.
FSE0005	Unable to initialize ${disk}.
FSE0006	Invalid license.
FSE0007	Unable to find license file.
FSE0008	Unable to attach hard drive ${disk}.
FSE0009	Upgrade failed.
FSE0010	License expired.
FSW0011	Retention module was unable to delete session ${sessid} from database.
FSW0012	Retention module error, session ${sessid} skipped.
FSI0013	Session ${sessid} removed according to retention policy.
FSW0014	Retention module was unable to remove session ${sessid}.
FSI0015	Redundancy group ${name} switched to master role.
FSW0016	Unable to send email, SMTP server not configured.
FSI0017	Redundancy group ${name} switched to slave role.
FSI0018	Hard drive ${disk} initialization started.
FSI0019	Hard drive ${disk} initialization completed. Data synchronization may take a moment.
FSE0020	System backup error.
FSI0021	Hard drive ${disk} attached.
FSI0022	Unsupported hard drive hot-swap.
FSI0023	Manual encryption does not support hard drive hot-swap.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FSE0024	Hard drive belongs to another Fudo (${diskserial}) ${disk}.
FSI0025	Cluster node ${name} (${address}) host key set to ${hostkey}.
FSE0026	Cluster communication error.
FSI0027	Cluster node ${name} initialized.
FSE0028	Unable to join node to cluster.
FSI0029	Resumed data synchronization.
FSI0030	Node ${node} initially synchronized.
FSE0031	Timestamping service communication error.
FSE0032	Unable to timestamp session.
FSE0033	Unknown timestamping service provider.
FSI0034	Session ${SESSION} was timestamped.
FSI0035	Email ${mailname} sent to ${admin_email}.
FSW0036	Unable to send email ${mailname} to ${admin_email} through ${account} server.
FSW0037	Output from SMTP client: ${out}.
FSI0038	Saved email ${mailname} sent to ${admin_email}.
FSI0039	System image version ${FULLNEW} uploaded successfully.
FSE0040	Communication error with cluster node %s (%s): Fudo version mismatch (local: %s, remote: %s).
FSI0041	Initial connection from master cluster node.
FSI0042	Cluster node %s (%s) connected from address %s.
FSI0043	Connection from another cluster node.
FSI0044	Connected to cluster node %s (%s) on address %s.
FSI0045	Initial database replication to cluster node %s (%s) completed.
FSE0046	There is no filter called %s.
FSW0047	Error sending notification.
FSE0048	Error authenticating user over RADIUS.
FUI0049	User %s authenticated using password logged in from IP address: %s.
FUI0050	User %s authenticated using password.
FUI0051	User %s authenticated through %s (Host: %s, Port: %d, %s: %s) logged in from IP address: %s.
FUI0052	User %s authenticated through %s (Host: %s, Port: %d, %s: %s).
FUI0053	User %s authenticated through LDAP (Host: %s, Port: %d) logged in from IP address: %s.
FUI0054	User %s authenticated through LDAP (Host: %s, Port: %d).
FUI0055	User %s (domain %s) authenticated through Active Directory (Host: %s, Port: %d) logged in from IP address: %s.
FUI0056	User %s (domain %s) authenticated through Active Directory (Host: %s, Port: %d).
FUE0057	Authentication method 'password', required by MySQL, requested by the user %s, logging in from IP address %s, was not found.
FUE0058	Authentication method 'password', required by MySQL, requested by the user %s, was not found.
FUW0059	User %s, logging in from IP address %s, has more than one 'password' method, using the first password.
FUW0060	User %s has more than one 'password' method, using the first password.
FSE0061	Incorrect password repository configuration: login is empty.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FSE0062	Incorrect password repository configuration: password is empty.
FSE0063	Incorrect server configuration: ERPM namespace is empty.
FSE0064	Incorrect server configuration: ERPM name is empty.
FSE0065	License configuration error.
FSE0066	Unable to block user %jd.
FSE0067	Error connecting to Lieberman ERPM server %s: incorrect URL in configuration.
FSE0068	Error connecting to Lieberman ERPM server %s: incorrect protocol specified.
FSE0069	Error fetching password from Lieberman ERPM server %s: unable to get sessid for user %s.
FSE0070	Error fetching password from Lieberman ERPM server %s: unable to get password for user %s for the %s/%s server.
FSI0070	Established proxy connection from %s to %s (%s:%u).
FSI0071	Established gateway connection from %s to %s (%s:%u).
FSI0072	Established transparent connection from %s to %s (%s:%u).
FSI0073	Bastion connection from %s to %s (%s:%u).
FSW0074	Connection terminated because license has expired or was not set.
FSW0075	Connection terminated because number of nodes in cluster exceeded license limit.
FSE0076	Unable to establish connection, could not find specified transparent server (tcp://%s:%u).
FSE0077	LDAP authentication error.
FSE0078	LDAP authentication error: unable to connect from %s to %s.
FUE0079	Authentication timeout after %ju key attempt%s and %ju password attempt%s.
FUE0080	Authentication timeout after %lu key attempt%s.
FUE0081	Authentication timeout after %lu password attempt%s.
FSE0082	Unable to establish connection to server %s (%s).
FSE0083	Unable to establish connection from %s to server %s (%s).
FSI0084	Terminating session: %s.
FSI0085	Session finished.
FUI0086	User %s blocked due to connection policy violation.
FUW0087	Session has been terminated due to user %s account expiration.
FUW0088	Session has been terminated due to exceeding the time window defined in the connection %s time policy.
FUE0089	Authentication timeout.
FSE0090	Unable to connect to the passwords repository server %s.
FSE0091	Unable to add server %s.
FSE0092	Passwords repository server %s communication error.
FSE0093	Error connecting to Thycotic server %s: incorrect URL in configuration.
FSE0094	Error connecting to Thycotic server %s: incorrect protocol specified.
FSE0095	Error fetching password from Thycotic server %s: unable to get sessid for user %s.
FSE0096	Error fetching password from Thycotic server %s.
FSE0097	Error fetching password from Thycotic server %s: unable to get secretid for server %s.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FSE0098	Error fetching password from Thycotic server %s: unable to get password for user %s for the %s server.
FUE0099	Connection terminated.
FUI0100	HTTP connection beetwen client and server initiated.
FUE0101	Unable to find matching HTTP connection.
FUI0102	Session terminated by system administrator.
FUE0103	HTTP connection error.
FUI0104	%s connection terminated.
FUI0105	HTTP session inactive, terminating.
FUE0106	Authentication failed: %s.
FUW0107	Invalid inactivity timeout, falling back to %d seconds.
FUE0108	MySQL connection error.
FUI0109	MySQL connection terminated.
FUE0110	Oracle connection error.
FUI0111	Oracle connection terminated.
FUE0112	RDP connection error.
FUE0113	TLS Security configured, but missing TLS private key.
FUE0114	TLS Security configured, but missing TLS certificate.
FUE0115	Standard RDP Security configured, but missing private key.
FUE0116	TLS certificate verification failed.
FUE0117	RSA key verification failed.
FUI0118	Successfully authenticated against the server.
FUI0119	Successfully authenticated against the server as user %s using %s.
FUI0120	Successfully authenticated against the server as user %s within domain %s using %s.
FUI0121	An anonymous user successfully authenticated against the server.
FUI0122	An anonymous user successfully authenticated against the server as user %s.
FUI0123	An anonymous user successfully authenticated against the server as user %s within domain %s.
FUE0124	SSH connection error.
FUE0125	User %s failed to authenticate after %d attempts, disconnecting.
FUI0126	Successfully authenticated against the server as user %s using password.
FUE0127	Invalid authentication method: expected passwordor sshkey, got %s.
FUI0128	User %s authenticated using SSH key.
FUE0129	Failed to authenticate against the server as user %s using %s.
FUE0130	Failed to authenticate against the server as user %s using %s (received %s).
FUW0131	Functionality %s is not allowed.
FUE0132	Client requested incorrect terminal dimensions (%dx%d).
FUE0133	MSSQL connection error.
FUE0134	TN3270 connection error.
FUE0135	Unknown TN3270 command: %02x.
FUW0136	Functionality %s not allowed.
FUE0136	Telnet connection error.
FSE0137	Unable to read private key.
FSE0138	Server's certificate does not match configured certificate.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FUE0139	VNC connection error.
FUE0140	Client version: %s is higher than the client integrated in Fudo: %s.
FUE0141	VNC connection error. Client answered with unsupported security type: %hhu.
FUE0142	VNC connection error. Server version: %s is lower than client version: %s.
FUI0143	VNC connection closed: %s.
FUE0144	User %s failed to authorize logging in from IP address: %s.
FUE0145	User %s failed to authorize.
FUE0146	User %s failed to authenticate logging in from IP address: %s.
FUE0147	User %s failed to authenticate.
FSE0148	Listening on %s:%u failed while adding bastion %s.
FAI0149	User %s deleted previous system version.
FAI0150	User %s changed backup and retention settings.
FAI0151	User %s %s bastion %s.
FAI0152	User %s deleted bastion %s.
FSE0153	Session indexing failure.
FSE0154	Session conversion failure for session %s.
FSI0155	Starting encoding session video %s.
FSI0156	Completed session video %s encoding.
FAI0157	User %s %s failover configuration.
FAI0158	User %s added node %s.
FAI0159	User %s changed %s in node %s.
FAI0160	User %s deleted node %s.
FAI0161	User %s disconnected node from the cluster.
FAI0162	Cluster has no active nodes. Cluster will be disabled.
FAI0163	User %s created new cluster.
FAI0164	User %s attached current node to cluster.
FAE0165	Error authenticating user %s.
FAI0166	User %s restored original logo for protocol %s.
FAI0167	User %s changed logo for protocol %s.
FAI0168	User %s confirmed sensitive feature %s.
FAI0169	User %s removed confirmation for sensitive feature %s.
FAI0170	User %s changed following notifications settings: %s.
FAI0171	User %s enabled email notifications.
FAI0172	User %s disabled email notifications.
FAI0173	User %(username)s is upgrading Fudo.
FAI0174	User %(username)s upgraded Fudo.
FAI0175	User %(username)s uploaded new upgrade image (version: %(version)s, size: %(size)d).
FAI0176	User %(username)s deleted upgrade files.
FAI0177	User %s uploaded license file.
FAW0178	User %(username)s triggered system restart.
FAW0179	User %(username)s triggered system shutdown.
FAW0180	User %s %s remote SSH access.
FAW0181	User %(username)s changed timestamping settings.
FAW0182	User %(username)s uploaded new PKCS12 file.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FAW0183	User %(username)s changed timestamping provider to %(provider)s.
FAW0184	User %(username)s %(action)s timestamping.
FAI0185	User %s imported system configuration.
FAI0186	User %s exported system configuration.
FAI0187	User %s added NTP server %s.
FAI0188	User %s removed NTP server %s.
FAE0189	Error saving NTP servers: "%s".
FAI0190	User %(username)s changed date & time from %(old_date)s to %(new_date)s.
FAI0191	User %s changed timezone to %s.
FAI0192	User %s changed Fudo HTTPS private key and certificate.
FAI0193	User %s %s SSH access.
FAI0194	User %s requested service data.
FAI0195	User %s added %s to %s for %s %s.
FAI0196	User %s removed %s from %s for %s %s.
FAI0197	User %s changed %s from %s to %s for %s %s.
FAI0198	User %(username)s added IP address %(new_inet)s/%(new_netmask)s to interface %(interface)s with %(new_management)s management and %(new_cluster)s cluster address.
FAI0199	User %(username)s changed subnet mask from %(old_netmask)s to %(new_netmask)s on %(new_inet)s/%(new_netmask)s address on interface %(interface)s.
FAI0200	User %(username)s %(new_cluster)s cluster address on %(new_inet)s/%(new_netmask)s address on interface %(interface)s.
FAI0201	User %(username)s %(new_management)s management on %(new_inet)s/%(new_netmask)s address on interface %(interface)s.
FAI0202	User %(username)s deleted IP address %(old_ip)s from interface %(interface)s.
FAI0203	User %(username)s %(action)s interface %(interface)s.
FAI0204	User %(username)s added member %(member)s to bridge %(interface)s.
FAI0205	User %(username)s removed member %(member)s from bridge %(interface)s.
FAI0206	User %(username)s enabled spanning tree propagation on bridge %(interface)s.
FAI0207	User %(username)s disabled spanning tree propagation on bridge %(interface)s.
FAI0208	User %(username)s changed VLAN %(interface)s parent interface from %(old_parent_interface)s to %(new_parent_interface)s.
FAI0209	User %(username)s changed VLAN %(interface)s ID from %(old_vlan)s to %(new_vlan)s.
FAI0210	User %s deleted interface %s.
FAI0211	User %s changed LDAP synchronization settings.
FAW0213	LDAP error during fetching groups: %s.
FAI0214	User %s enforced full LDAP synchronization.
FAI0215	User %s disabled events logging on syslog servers.
FAI0216	User %s removed syslog server: %s:%s.
FAI0217	User %s added syslog server: %s:%s.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FAI0218	User %s removed syslog server %s.
FAI0219	User %s changed remote log dispatch settings.
FAI0220	User %s changed network interfaces settings.
FAI0221	User %s changed hostname from %s to %s.
FAI0222	User %s added DNS server IP address %s.
FAI0223	User %s removed DNS server IP address %s.
FAI0224	User %s added new route for network %s with gateway %s.
FAI0225	User %s changed gateway for network %s from %s to %s.
FAI0226	User %s deleted network %s with gateway %s.
FAI0227	User %s (%s) terminated session.
FAI0228	Anonymous user from IP address %s with access rights granted by user %s joined session.
FAI0229	User %s from IP address %s joined session.
FAI0230	User %s (%s) suspended session.
FAI0231	User %s (%s) resumed session.
FAE0232	MySQL session playback error.
FAI0233	Anonymous user from IP address %s accessed session %s shared by %s with key %s.
FAI0234	User %s from IP address %s accessed session %s.
FAI0235	User %s %s comment %d for session.
FAI0236	User %s generated key %s with %s access.
FAI0237	User %s is viewing user input for session.
FAI0238	User %s blocked server %s.
FAI0239	User %s unblocked server %s.
FAI0240	User %s blocked connection %s.
FAI0241	User %s unblocked connection %s.
FAI0242	User %s addedd new time policy to connection %s for %s from %s to %s.
FAI0243	User %s changed connection %s %s time policy %s from %s to %s.
FAI0244	User %s deleted time policy for %s %s - %s from connection %s.
FAI0247	User %s deleted server %s.
FAI0248	User %s %s server %s.
FAI0251	User %s deleted connection %s.
FAI0252	User %s %s connection %s.
FAI0253	User %s deleted session.
FAI0254	User %s requested OCR processing for session.
FAW0255	User %s tried to disable a non-exisitent sharing key for session.
FAI0256	User %s disabled anonymous access key %s for session.
FAI0259	User %s deleted download %s.
FAI0260	User %s downloaded file %s for session %s.
FAI0261	Anonymous user from IP address %s terminated session shared by %s with key %s.
FAI0262	User %s terminated session.
FAI0263	User %s blocked user %s.
FAI0264	User %s modified policies settings.
FAI0265	User %s modified regular expressions settings.
FSW0266	Failed to send email.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FSE0267	Error generating report %d: %s.
FAI0268	User %s deleted report "%s".
FAW0269	User %s cannot delete report "%s".
FAI0270	Report {} created by user {}.
FAW0271	User %(username)s is blocked.
FAW0272	User %(username)s is not allowed to log in.
FAW0273	User %(username)s logging from IP %(ip)s not found.
FAI0276	User %s unblocked user %s.
FAI0277	User %s deleted user %s.
FAI0278	User %s added user %s to connection %s.
FAI0279	User %s changed user %s.
FAI0281	User %s logged out from Fudo administration panel.
FAI0282	User %s successfully changed his password.
FSE0283	Unable to process pattern: %s
FSW0284	Pattern %s matched on %s with priority %s in session.
FSE0285	Unable to read certificate.
FSE0286	No peer certificate received.
FSW0287	No server key configured, skipping verification.
FSI0288	Server key verification failed.
FUI0289	MSSQL connection terminated.
FSI0290	User %s (%d) was removed. Reason: user wasn't in any of synchronized groups.
FSI0291	System backup initiated, fingerprint: ${fingerprint}.
FSI0292	System backup initiated.
FSI0293	System backup completed, fingerprint: ${fingerprint}.
FSI0294	System backup completed.
FAI0295	User %s blocked bastion %s.
FAI0296	User %s unblocked bastion %s.
FAI0297	User %s created bastion %s.
FAI0298	User %s changed bastion %s.
FAI0299	User %s created server %s.
FAI0300	User %s changed server %s.
FAI0301	User %s changed connection %s.
FAI0302	User %s created connection %s.
FAI0303	User %s created user %s with role %s.
FAI0304	User %s modified %s for %s %s.
FUE0305	Client connection closed: encryption is not available.
FUE0306	Client connection closed.
FSE0307	Error fetching password from HiPAM server %s: unable to get sessid for user %s.
FSE0308	HiPAM server internal error.
FSE0309	Error fetching password from HiPAM server %s: unable to get sessdat for user %s.
FSE0310	Incorrect server configuration: HiPAM name is empty.
FSE0311	Unable to fetch password from HiPAM.
FSE0312	Error connecting to HiPAM server %s: incorrect URL in configuration.
FSE0313	Error connecting to HiPAM server %s: incorrect protocol specified.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FUE0314	Invalid pixel format.
FSE0330	Bad login field configured on LDAP server %s. Error while processing user %s.
FSE0331	Error while processing userAccountControl value of user %s.
FSI0332	User %s will be blocked.
FSI0333	User %s will be unblocked.
FSW0334	User %s has incorrect principal name.
FSI0335	User %s synchronized from LDAP server %s.
FSI0336	Remove pair connection %s user %s.
FSI0337	Add conection %s to user %s.
FSW0338	User %s paired with connection %s, server conflict.
FSI0339	User %s (%s) was removed. Reason: user was not in any of synchronized groups.
FSI0340	Full synchronization from LDAP server %s started.
FSI0341	User %s connections cleared.
FSI0342	User %s will be resynchronized from server %s.
FSI0343	Resynchronized user %s will be removed.
FSW0344	Connection to LDAP server error: %s.
FSI0345	Successfully fetched password from %s.
FUE0346	Client sent a packet bigger than %d bytes.
FSE0348	Unable to get configuration settings.
FAI0349	Anonymous user from IP address %s with access rights granted by user %s left session.
FAI0350	User %s from IP address %s left session.
FUE0351	Client sent unsupported NTLM v1 response.
FSE0352	Bastion requires login and server delimited with one of '%s' (%s).
FAI0353	User %(username)s is deleting upgrade snapshost.
FAI0354	User %(username)s deleted upgrade snapshot.
FSE0355	Inconsistent data, starting recovery replication to cluster node %s (%s).
FUW0356	Unsupported X11 extension: %s.
FUW0357	Server uses higher resolution than the current limit: %dx%d.
FUW0358	Server uses higher color depth than the current limit: %d bpp.
FUE0359	Server rejected X11 connection: %.*s.
FUE0360	Server requires unsupported X11 authentication: %.*s.
FSW0361	Fudo started.
FSE0362	Unable to propagate ARP.
FUE0363	User %s has no access to host %s:%u.
FUI0364	RDP server sent a redirection packet.
FUE0365	RDP server %s:%u has to listen on the default RDP port in order to redirect sessions.
FSE0366	Error connecting to CyberArk server %s: incorrect URL in configuration.
FSE0367	Error connecting to CyberArk server %s: incorrect protocol specified.
FSE0368	Error fetching password from CyberArk server %s.
FSE0369	Error fetching password from CyberArk server %s: unable to get password for user %s for server %s.
FUI0370	User %s authenticated using OTP logged in from IP address: %s.
FUI0371	User %s authenticated using OTP.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FSE0372	Unable to invalidate OTP password %jd.
FUW0373	Session has been terminated due to exceeding the time window defined in a time policy for the user %s and the safe %s.
FSI0374	Established %s connection from %s to %s:%u.
FSE0375	Unable to add listener %s.
FSE0376	Unable to add listener %s because %s is listening on same IP address and port.
FSE0377	Bastion requires login and server to be delimited with one of the '%s' characters (listener: %s, login: %s).
FSE0378	Unable to establish connection: server not found, user not found or user has no access to the server (listener: %s, login: %s).
FSE0379	Unable to establish connection: transparent server (tcp://%s:%u) not found or cannot be reached through listener (listener: %s, login: %s).
FSE0380	Unable to authenticate user %s: server is blocked.
FSE0381	Unable to authenticate user %s: account not found.
FSE0382	Unable to authenticate user %s: account is blocked.
FSE0383	Unable to authenticate user %s: user not found.
FSE0384	Unable to authenticate user %s: user is blocked.
FSE0385	Unable to authenticate user %s: safe not found.
FSE0386	Unable to authenticate user %s: safe is blocked.
FSI0387	Password for account %s verified successfully.
FSI0389	Password for account %s changed successfully.
FAI0393	User %s displayed password history for account %s.
FAI0394	User %s displayed password to account %s changed at %s.
FAI0395	User %s displayed current password for account %s.
FAI0396	User %s blocked safe %s.
FAI0397	User %s unblocked safe %s.
FAI0398	User %s deleted safe %s.
FAI0399	User %s changed safe %s.
FAI0400	User %s created safe %s.
FAI0401	User %s blocked account %s.
FAI0402	User %s unblocked account %s.
FAI0403	User %s deleted account %s.
FAI0404	User %s changed account %s.
FAI0405	User %s created account %s.
FAI0406	User %s blocked listener %s.
FAI0407	User %s unblocked listener %s.
FAI0408	User %s deleted listener %s.
FAI0409	User %s changed listener %s.
FAI0410	User %s created listener %s.
FAI0411	User %s blocked password change policy %s.
FAI0412	User %s unblocked password change policy %s.
FAI0413	User %s deleted password change policy %s.
FAI0414	User %s changed password change policy %s.
FAI0415	User %s created password change policy %s.
FSI0416	Connection between safe %s and user %s has been removed.
FSI0417	Connection between safe %s and user %s has been added.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FSI0418	User %s was removed from safes %s.
FSE0420	Unable to authenticate user %s against server %s.
FAI0421	User %s assigned listener %s to safe %s.
FAI0422	User %s unassigned listener %s from safe %s.
FAI0423	User %s assigned account %s to safe %s.
FAI0424	User %s unassigned account %s from safe %s.
FAI0425	User %s assigned authentication method %s to user %s.
FAI0426	User %s unassigned authentication mathod %s from user %s.
FAI0427	User %s changed authentication mathod %s assigned to user %s.
FAI0428	User %s assigned user %s to safe %s.
FAI0429	User %s unassigned user %s from safe %s.
FAI0430	User %s blocked password changer %s.
FAI0431	User %s unblocked password changer %s.
FAI0432	User %s deleted password changer %s.
FAI0433	User %s changed password changer %s.
FAI0434	User %s created password changer %s.
FSW0435	Password changer timed out for acccount %s.
FUI0436	User %s authenticated using token logged in from IP address: %s.
FUI0437	User %s authenticated using token.
FAW0438	User %s authenticated using new token while the old one still exists.
FAW0439	User %s authenticated using old token.
FAI0440	User %s granted access for account %s to user %s.
FAI0441	User %s revoked access for account %s from user %s.
FAI0442	User %s granted access for listener %s to user %s.
FAI0443	User %s revoked access for listener %s from user %s.
FAI0444	User %s created policy %s.
FAI0445	User %s deleted policy %s.
FAI0446	User %s changed policy %s.
FAI0447	User %s assigned regexp %s to policy %s .
FAI0448	User %s unassigned regexp %s from policy %s.
FAI0449	User %s created regexp %s.
FAI0450	User %s deleted regexp %s.
FAI0451	User %s changed regexp %s.
FAI0452	User %s granted access for safe %s to user %s.
FAI0453	User %s revoked access for safe %s from user %s.
FAI0454	User %s granted access for server %s to user %s.
FAI0455	User %s revoked access for server %s from user %s.
FAI0456	User %s granted access for user %s to user %s.
FAI0457	User %s revoked access for user %s from user %s.
FAI0458	User %s displayed password history for account %s. Reason: %s.
FAI0459	User %s displayed password to account %s changed at %s. Reason: %s.
FAI0460	User %s displayed current password for account %s. Reason: %s
FSE0461	Invalid data from %s LDAP server.
FAI0462	User {} created redundancy group {}.
FAI0463	User {} deleted redundancy group {}.
FAE0464	User %s is not allowed to login from address %s.
FUW0465	Establishing new connections has been disabled.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FSE0466	Fudo versions do not conform.
FUE0467	Client tried to authenticate using an invalid UTF-8 login.
FSI0468	A passphrase used to decrypt disks was changed.
FSE0469	Unexpected number of bastions (%s).
FSE0470	Unexpected number of servers (%s).
FSE0471	Unexpected number of users (%s).
FSE0472	RDP servers %s must all use TLS (NLA) or Standard RDP Security.
FSE0473	Fudo cannot be upgraded to PAM.
FSI0474	Fudo can be upgraded to PAM.
FSE0475	Connection %s replaces a login and forwards a secret for servers %s which is not allowed.
FSE0476	ZVOL with encryption key does not exist.
FSE0477	Replication of encryption key to cluster node %s (%s) failed.
FSE0478	Unable to join cluster's node ${name}. Fudo versions do not conform (local: ${VERSION}, remote: ${rversion}).
FSE0479	Servers %s must all use the same %s settings.
FSE0480	Servers %s must all use the same protocol.
FAI0481	New OTP for user %s has been generated.
FSW0482	Unable to verify password for account %s.
FUI0483	User %s authenticated using Citrix logon ticket logged in from IP address: %s.
FUI0484	User %s authenticated using Citrix logon ticket.
FUE0485	ICA connection error.
FUI0486	ICA server closed connection.
FAI0487	User %s requested timestamping for session.
FAI0488	User %s requested timestamping for account.
FSI0489	Label %s not defined on this node, skipping listener %s.
FAI0490	User %s created external authentication %s.
FAI0491	User %s changed external authentication %s: %s.
FAI0492	User %s deleted external authentication %s.
FSE0493	Unable to establish connection to server %s (%s): label %s not defined on this node.
FSI0494	Label %s not defined on this node, skipping external authentication %s.
FSE0495	Communication error with cluster node %s (%s): connection failure.
FSE0496	Communication error with cluster node %s (%s): unable to replicate a batch with object %jd to table %s.
FSE0497	Communication error with cluster node %s (%s): unable to replicate a batch with object %jd (name: %s) to table %s.
FSE0498	Communication error with cluster node %s (%s): unable to store object %jd in table %s.
FSE0499	Communication error with cluster node %s (%s): unable to store object %jd (name: %s) in table %s.
FSE0500	Communication error with cluster node %s (%s): unable to connect to %s.
FSE0501	Communication error with cluster node %s (%s): failure during handshake.
FSE0502	Database error.

Continued on next page

Table 1 – continued from previous page

Message code	Message and description
FSE0503	Communication error with a cluster node: Fudo version mismatch (local: %s, remote: %s).
FSE0504	Communication error with cluster node %s (%s): %s.
FSE0505	Communication error with a cluster node: failure during handshake.
FSI0508	Successfully replicated encryption key to node %s (%s).
FSE0509	Communication error with cluster node %s (%s): unable to replicate session data.
FSE0510	Communication error with cluster node %s (%s): intial replication failed.
FSW0511	There has been an attempt to reset Fudo to factory defaults. Resetting Fudo to factory defaults has been administratively disabled.
FAI0512	User %s enabled reset account.
FAI0513	User %s disabled reset account.
FAW0514	User %s of role %s tried to view %s, but has insufficient privileges for this action.
FSE0515	Unable to upload backup #${currno} at ${datetime}.
FSI0516	Backup #${currno} at ${datetime} successfully uploaded.
FSE0517	Backup configuration error: %s.
FSE0518	Backup internal error.
FSI0519	${type} backup snapshot ${snapname} successfully taken.
FUE0520	User %s tried to access ICA server %s:%u using Citrix StoreFront which is not permitted.
FUE0521	Citrix StoreFront sent an ICA file without a destination address.
FSW0522	Roolback to ${oldversion} failed.
FSW0523	Upgrade to ${oldversion} failed.
FSW0524	Roolback to ${version} succeeded.
FSW0525	Upgrade to ${version} succeeded.
FSE0526	Error communicating with bypass card. Error setting nextboot mode.
FSE0527	Error communicating with bypass card. Error setting bpe mode.
FSE0528	Error communicating with bypass card. Error switching card mode.
FSE0529	Error communicating with bypass card.
FAI0530	User %s enabled snmp.
FAI0531	User %s disabled snmp.
FSW0532	External storage is unavailable.
FSE0533	Unable to attach external storage.
FSI0534	External storage attached.
FSE0535	External storage is unavailable in this configuration.
FSW0536	External storage detached.
FSI0537	External storage attached successfully.
FAI0538	Set external storage connection mode to %s
FAI0539	Set configured WWN to %s, external storage connection mode to %s
FAI0540	Interface discovery while configuring external storage: %s
FSW0540	Found ${cdisk} paths to fiber channel ${wwn} from ${cscbus} devices.
FSW0541	Retention module was unable to move session ${sessid}.
FAI0542	User %s assigned account %s, listener %s to safe %s.
FAI0543	User %s unassigned account %s, listener %s from safe %s.
FSE0544	Failed to list snapshots.
FSW0545	Unable to change password for account %s.

Continued on next page

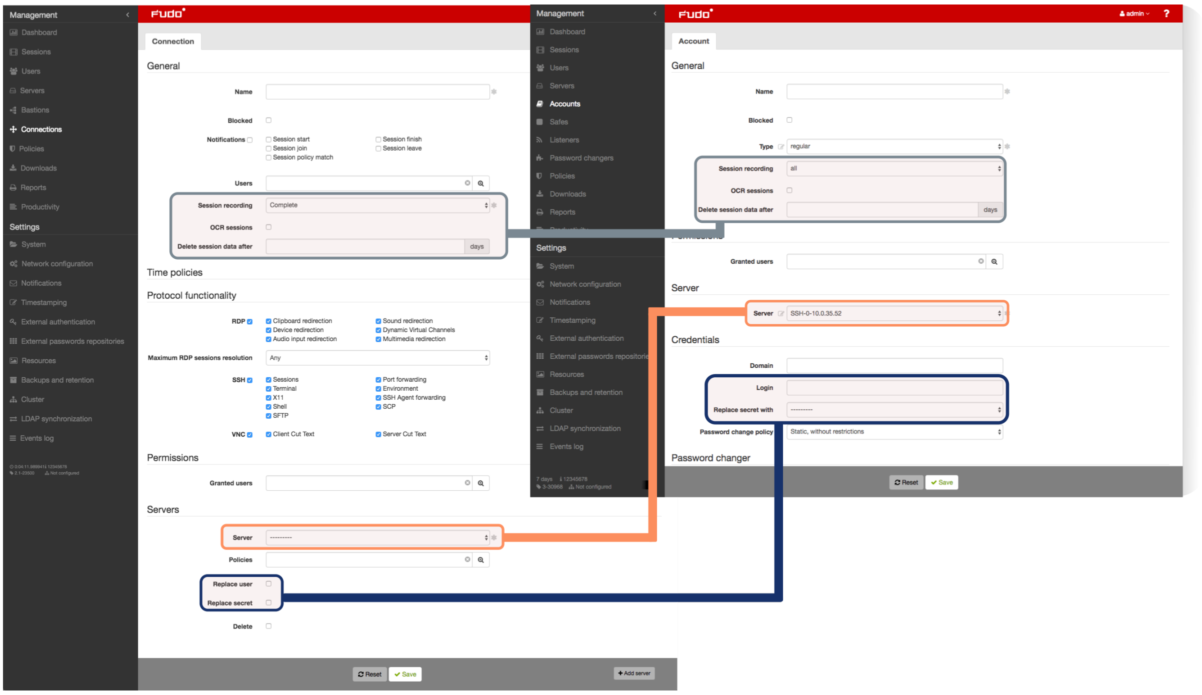
Table 1 – continued from previous page

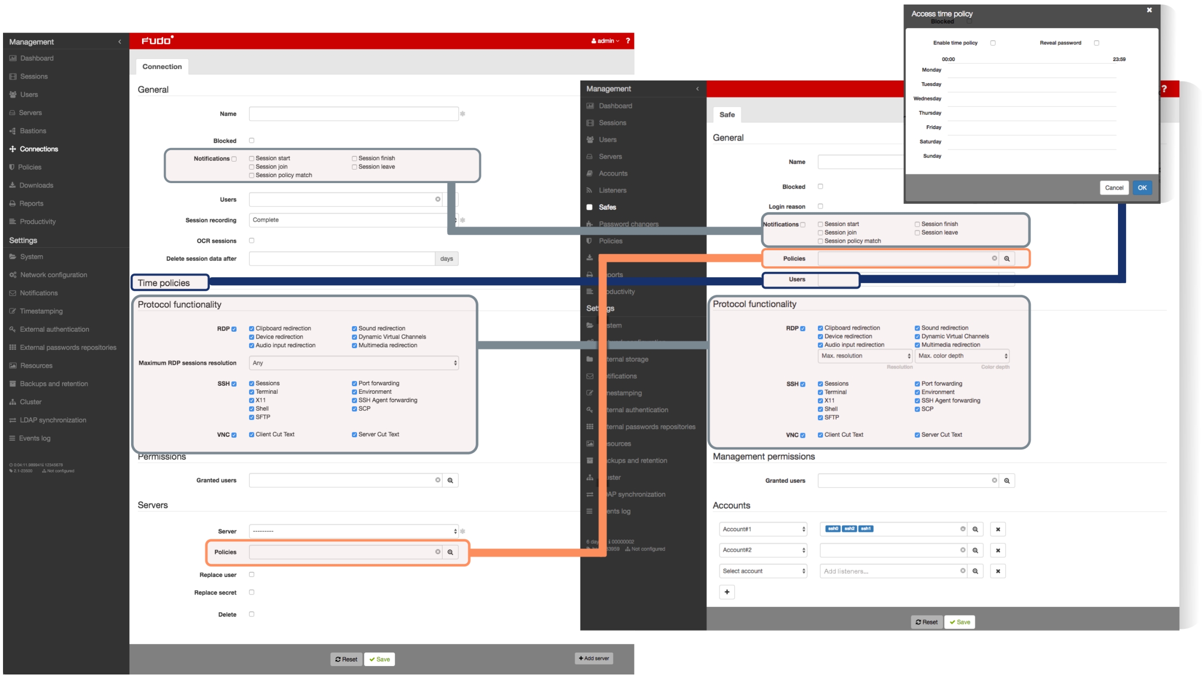
Message code	Message and description
FUI0546	ICA client closed connection.
FAE0547	User %s could not create a ticket requesting an access to safe %s.
FAI0548	User %s created ticket %s requesting an access to safe %s.
FAI0549	User %s approved ticket %s requesting an access for user %s to safe %s.
FAI0550	User %s rejected ticket %s requesting an access for user %s to safe %s.
FAI0551	User %(username)s added member %(member)s to lagg %(interface)s.
FAI0552	User %(username)s removed member %(member)s from lagg %(interface)s.
FSE0553	Unable to extract public key from CA.
FUE0554	SFTP server uses an unsupported version %u.
FAI0555	User %s added address %s to server %s.
FAI0556	User %s removed address %s from server %s.
FAI0557	User %s changed address %s assigned to server %s.
FSI0558	Starting encoding file for session %s.
FSI0559	Completed encoding file for session %s.
FSE0560	Session has not been approved nor rejected.
FSE0561	Unexpected number of connections (%s).
FAI0562	User %s rejected session %s. Reason: %s.
FAI0563	User %s rejected session %s.
FAI0564	User: {} tried to accept session: {} but it was accepted by:
FAI0565	User: {} rejected session: {}
FAI0566	User: {} tried to reject session: {} but it was accepted by:
FAI0567	User: {} tried to reject session: {} but it was rejected by:
FAI0568	User: {} accepted session: {}
FAI0569	User: {} tried to accept session: {} but it was rejected by:
FAI0570	User %s approved session %s.
FSI0571	Proxy connection closed.
FSE0572	Proxy connection error.
FSI0573	Client sent an invalid token.
FSE0574	Unable to resolve ${ip} domain to address.
FSE0575	Unable to convert raw file to pcap.
FAI0576	User {} changed 4 Eyes proxy API certificate settings.
FAI0577	User {} changed 4 Eyes proxy settings.
FSI0578	User %s (%s) was removed. Reason: user's external server dosen't exists any more.
FAI0579	User {} changed 4 Eyes Fudo Mobile settings.
FSE0580	Cluster %s has an invalid token: %s.
FAI0581	User %s changed domain search path from %s to %s.
FSW0582	Disk $cdev was removed.

16.3 Fudo 2.2 to Fudo 3.0 parameters mapping

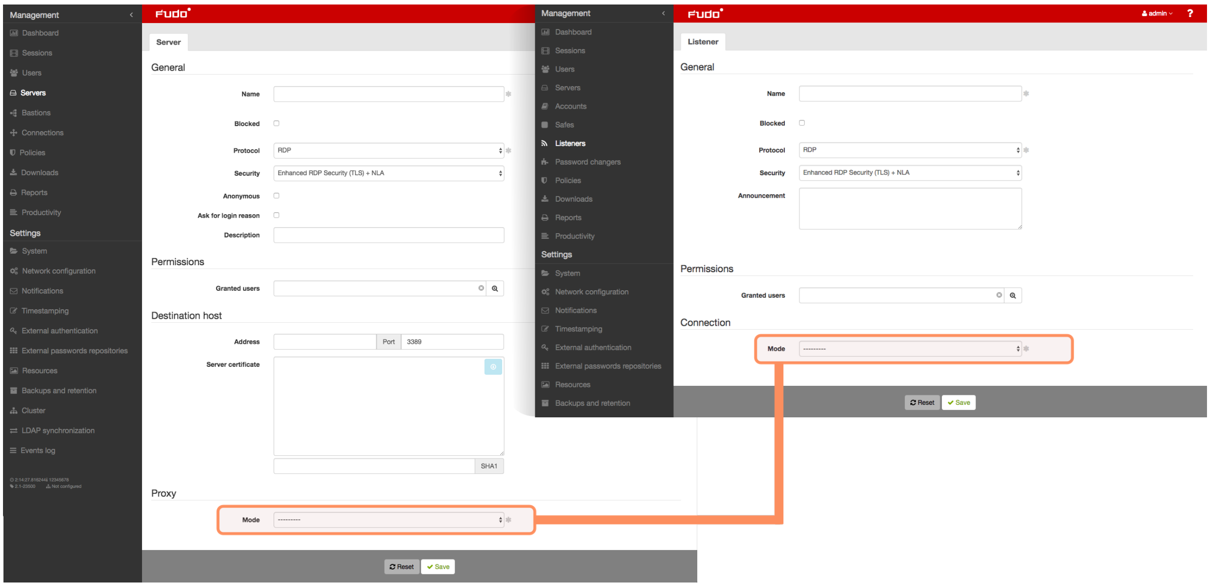
This topic describes how certain parameters from Fudo 2.2 map to Fudo 3.0 data model.

16.3.1 Connection





16.3.2 Server



Server: Protocol: RDP; Security: Enhanced RDP Security (TLS) + NLA; Port: 3389; Mode: ---------

Listener: Protocol: RDP; Security: Enhanced RDP Security (TLS) + NLA; Mode: ---------

16.4 Data model migration from Fudo PAM version 2.2 to 3.0

This topic describes data model migration mechanisms that are applied when performing upgrade from Fudo PAM version 2.2 to 3.0.

Note: In case of unsuccessful upgrade to version 3.0 data model issues which caused upgrade procedure to fail can be found in the system evetns log.

16.4.1 Server

Servers, which have the same IP address and port number assigned are replaced with a single object. Name of the resulting object is a concatenation of the servers' names in ascending order, separated by comma.

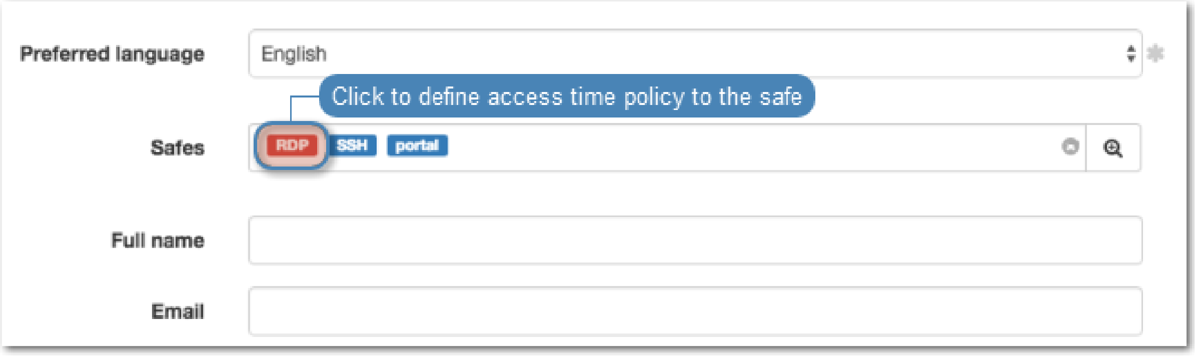
Warning: If there are two servers with the same IP address and port number assigned but with different protocol, description, external password repositorie, RDP security level, HTTP settings, TLS settings, certificates or public keys, upgrade will fail.

16.4.2 Safe (previously *connection*)

- Anonymous connection becomes a *safe* object, which can be deleted.
- For each *bastion* object (a group of servers operating in *bastion* mode, assigned to the same *bastion*) and associated connection, there is a *safe* object created using the following naming convention: `<connection name> > <bastion name>`.

- For each server operating in *gateway*, *proxy* or *transparent* mode, migration procedure creates a *safe* object named `<connection name> > <server name`.
- Automatically created *safe* object inherits connection's access rights, granted privileges, protocols settings, notifications settings and LDAP mapping.
- OCR settings, sessions recording and session data retention parameters are moved to corresponding *account* objects.
- Time policies are replicated as user specific regulations applicable to each safe.

Note: Click selected safe on user's configuration form to display time access settings.



Preferred language: English

Click to define access time policy to the safe

Safes: RDP SSH portal

Full name:

Email:

- After migration, login credentials policies are reflected within the safe.

16.4.3 Account (previously *login credentials*)

For each login credentials sections in every connection, migration mechanism creates a separate *account* object.

- If login credentials contain the user login string the resulting account is of the *regular* type and its name is a combination of the login and server's name - `<login> @ <final server name>`.
- If login credentials do not contain the user login string and concern credentials forwarding connection, the resulting account object is of the *forward* type and it is named `forward for <final server name>`.
- If login credentials do not contain the user login and are used for anonymous connections, the resulting account object is of the *anonymous* type and it is named `anonymous for <final server name>`.
- Duplicated loign credentials are replaced by a single *account* object. Object's management rights, OCR settings, sessions recording settings, session data retention settings are inherited from the connection object that the *account* object derives from.

Warning: If login credentials contain the login string but do not contain the secret (if the login is substituted but the secret field remains empty) the data migration process will fail.

16.4.4 Listener (previously *bastion* or part of a server)

- For each server operating in *proxy*, *transparent* or *gateway* mode, there is a *listener* object created with the same connection mode.
- Newly created object inherits server's access rights, TLS settings and RDP security level parameter.
- Server announcement setting is also passed on to the *listener* object.
- Listener is assigned to all safes that have been created based on connections which were associated with the server that the listener derived from.
- Bastion becomes a listener operating in the *bastion* mode. Access rights and bastion settings are transferred to the listener. The listener is assigned to all safes that have been created based on connections associated with at least one server from the bastion that the listener derived from.

16.4.5 Sessions

- Each session has its safe, server and account identifiers updated accordingly. If a session concerned a server, which was not operating in *bastion* mode, it also has the listener identifier set.

16.5 ICA configuration file

The `.ica` configuration file defines connection parameters for establishing connections with remote host over the ICA protocol.

16.5.1 Non-TLS connections ICA file

```
[ApplicationServers]
<connection name>=

[<connection name>]
ProxyType=SOCKSV5
ProxyHost=<host>:<port>
ProxyUsername=*
ProxyPassword=*
Address=<username>
Username=<username>
ClearPassword=<password>
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

Note: `<connection name>` is for information purpose only and can be any string of characters. Provided value is displayed in the title of the ICA client application window.

16.5.2 TLS connections ICA file

```
[ApplicationServers]
<connection name>=

[<connection name>]
SSLEnable=On
SSLProxyHost=<FQDN>:<port>
Address=<username>
Username=<username>
ClearPassword=<password>
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

Note: `<connection name>` is for information purpose only and can be any string of characters. Provided value is displayed in the title of the ICA client application window.

Related topics:

- *ICA*
- *ICA protocol*
- *Data model*

CHAPTER 17

AAPM (Application to Application Password Manager)

The AAPM module enables secure passwords exchange between applications.

An essential part of the AAPM module is the `fudopv` script. It is installed on the application server and it communicates with the Fudo PAM Secret Manager module to retrieve passwords.

The AAPM module supports Microsoft Windows, Linux and BSD family operating systems.

17.1 Compiling *fudopv* tool

The result of this procedure is `fudopv` application with Python interpreter included.

Note: For information on deploying *fudopv* without compiling sources files, refer to the *Deploying fudopv without compiling source files* topic.

17.1.1 Python

Windows

Download and install Python 3.x environment:

https://www.python.org/downloads/

Note: Make sure to select the option to add `python.exe` to the execution path.

Linux

Install Python environment according to the guide provided by the manufacturer.

Exemplary configuration:

```
./configure \
  --prefix=/opt/python-3.6 \
  --with-ensurepip=install \
  --disable-optimizations \
  --enable-shared
```

Note:

- `--disable-optimizations` - optimizations may result in build failures,
- `--with-ensurepip=install` - installs tools for managing Python's packages,
- `--enable-shared` - one of the `fudopv's` dependencies requires the Python interpreter `.so` library.

17.1.2 Virtual environment

Compiling the package requires the `virtualenv` module.

1. Execute `pip install virtualenv requests` or `easy_install virtualenv requests` command.
2. In the `fudopv/` execute the `virtualenv deps` command.

The environment required for building `fudopv` will be created in the `deps/` folder.

Windows

Run the `deps\Scripts\Activate` command to activate the environment.

Linux

In case of the interpreter build from the source code you can use the included `pip` and `easy_install` tools. You must also set the path to the shared libraries and run the `virtualenv` with the `-p` option:

```
LD_LIBRARY_PATH=/opt/python-3.6/lib
/opt/python-3.6/bin/pip install virtualenv requests
/opt/python-3.6/bin/virtualenv -p /opt/python-3.6/bin/python deps
```

To activate the environment, run the `source deps/bin/activate` command.

17.1.3 Fetching dependencies

In active virtual environment run the `pip install -r requirements.txt` to install `fudopv` dependencies. Dependencies are installed in the `deps/`

Note: If the `ImportError: No module named _markerlib` problem occurs, execute `pip install --upgrade distribute` and install dependencies once again.

Windows

Download and install *pywin32*: https://sourceforge.net/projects/pywin32/files/

Note: Make sure to select the installer for Python 3.x.

After activating the `virtualenv` environment, execute the following command with the path to the *pywin32*:

```
easy_install path\to\pywin32
```

Linux

Linux operating system does not require taking any additional actions.

17.1.4 Package creation script

Execute the `python setup.py` command, which will create package in the *fudopv* folder.

Note: The *PyInstaller* does not support package creation on a privileged account. If the `ERROR: You are running PyInstaller as user root. This is not supported.` error occurs, you can change the `check_not_running_as_root()` function in the `./deps/lib/python3.6/site-packages/PyInstaller/utils/misc.py` so that it return the result without checking anything.

Related topics:

- *Using fudopv*
- *Deploying fudopv without compiling source files*
- *Authentication methods*

17.2 Deploying *fudopv* without compiling source files

To use *fudopv* without compiling source files, proceed as follows.

1. Download and install Python 3.x environment.

Note: It is advised to run *fudopv* in virtual environment.

2. Execute `pip install virtualenv requests` or `easy_install virtualenv requests` command to install virtual environment.
3. In the `fudopv/` execute `virtualenv deps` command.
4. Add *fudopv* to your python search path. Execute `export PYTHONPATH=~/fudopv` where `"~/fudopv"` is the path where you have unpacked the utility and run `virtualenv/easy_install` in.
5. Execute `python -m fudopv`, to start *fudopv*.

Related topics:

- *Using fudopv*

- *Compiling fudopv tool*
- *API interface*

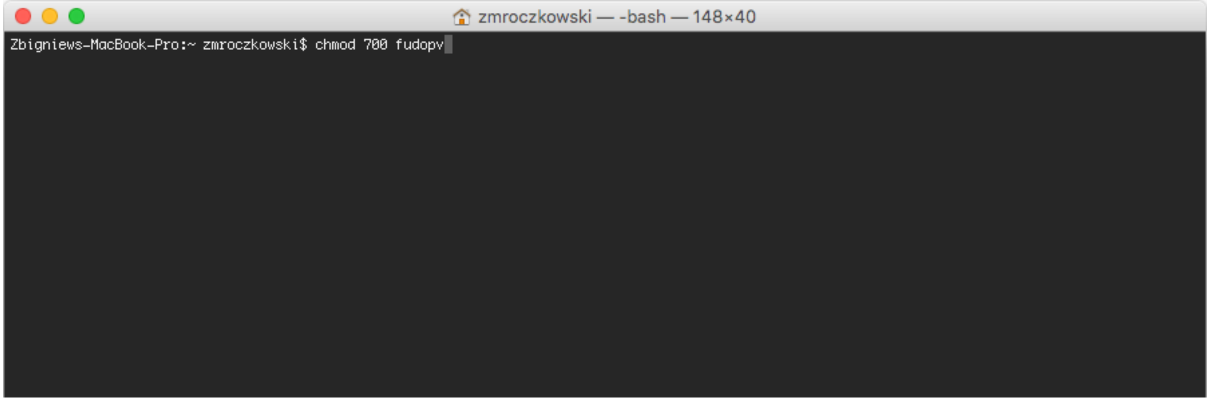
17.3 Using *fudopv*

Execution parameters

`fudopv [<options>] <command> [<parameters>]`

Command/option/parameter	Description
Commands	
`getcert`	Fetch User Portal SSL certificate.
`getpass` <type> <account>	Fetch password to selected account. type: • `direct` - direct, unmonitored connection; • `fudo` - connection monitored by the *PSM* module
Options	
`-c <path>`	Use configuration file from provided path.
`--cfg <path>`	
`-h, --help`	Show options and parameters list.

1. Upload `fudopv` script to the server and change its access rights to allow execution.



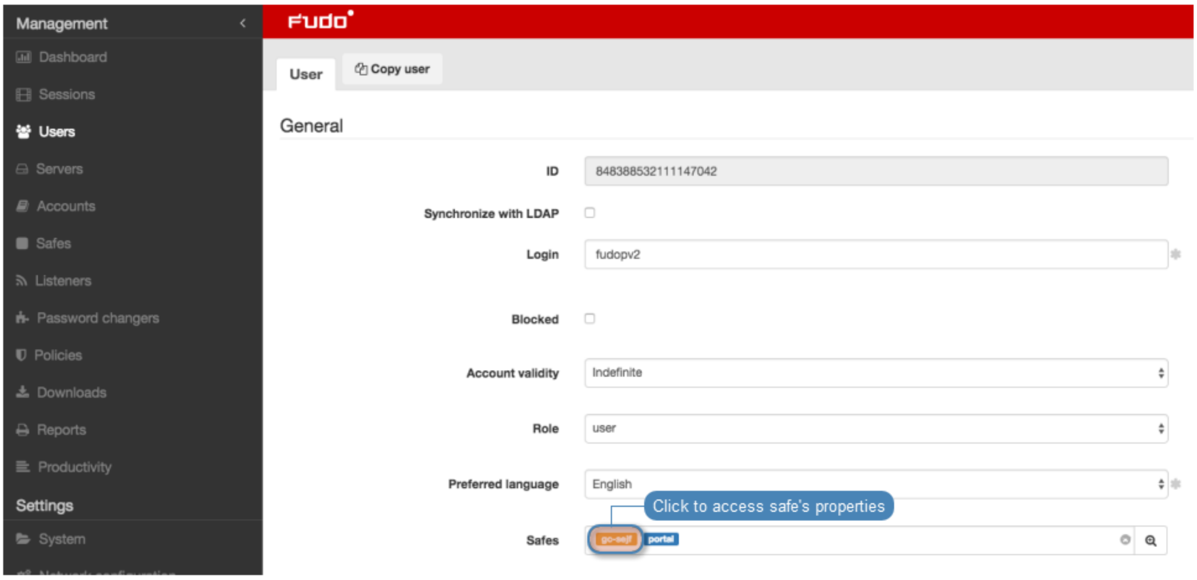
```
Zbigniews-MacBook-Pro:~ zmroczkowski$ chmod 700 fudopv
```

2. Log in to the 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.



General

ID 848388532111147042

Synchronize with LDAP □

Login fudopv2

Blocked □

Account validity Indefinite

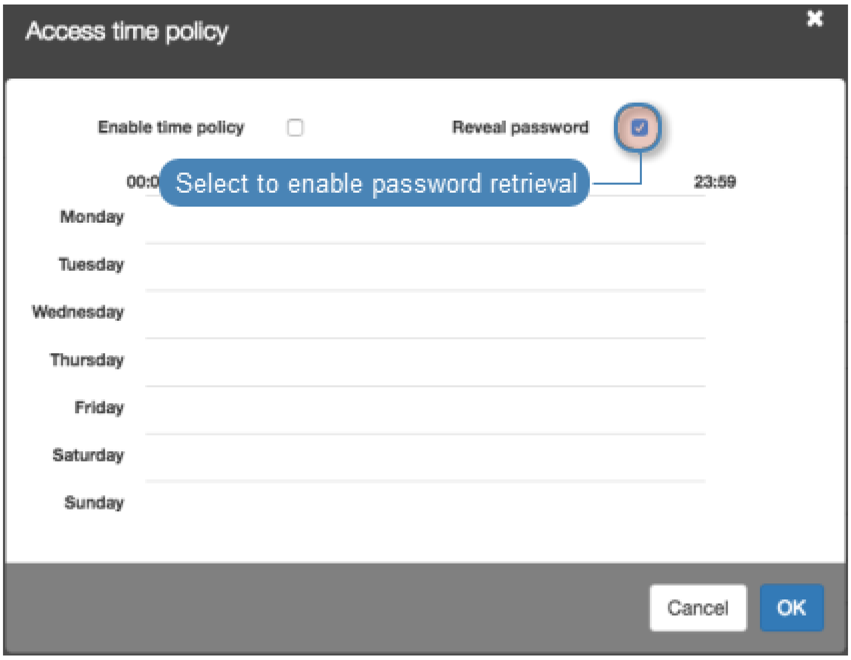
Role user

Preferred language English

Safes go-self portal

Click to access safe's properties

- Select the *Reveal password* option.



Access time policy

Enable time policy □ Reveal password ☑

Select to enable password retrieval

00:0 23:59

Monday

Tuesday

Wednesday

Thursday

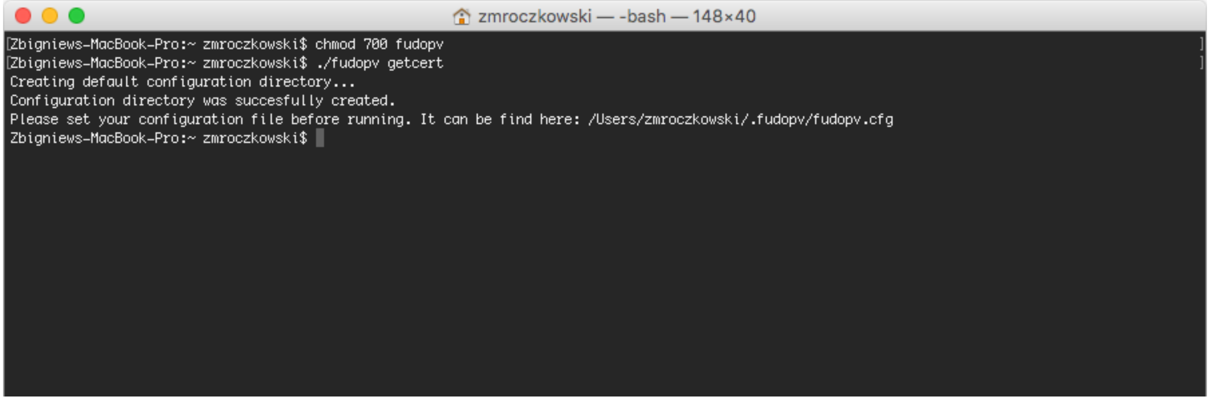
Friday

Saturday

Sunday

- 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.

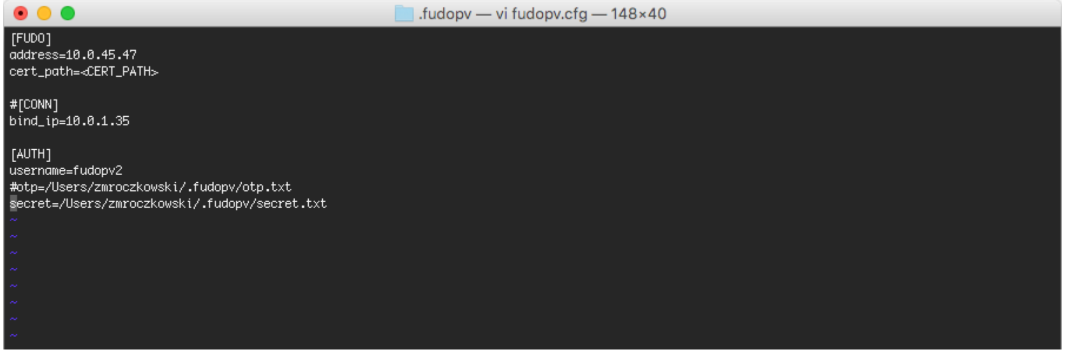


```
Zbigniews-MacBook-Pro:~ zmroczkowski$ chmod 700 fudopv
Zbigniews-MacBook-Pro:~ zmroczkowski$ ./fudopv getcert
Creating default configuration directory...
Configuration directory was succesfully created.
Please set your configuration file before running. It can be find here: /Users/zmroczkowski/.fudopv/fudopv.cfg
Zbigniews-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.

. only:: latex



```
[FUDO]
address=10.0.45.47
cert_path=<CERT_PATH>

#[CONN]
bind_ip=10.0.1.35

[AUTH]
username=fudopv2
#otp=/Users/zmroczkowski/.fudopv/otp.txt
secret=/Users/zmroczkowski/.fudopv/secret.txt
~
~
~
~
~
~
~
~
```

Section	Description
`[FUDO]`	
`address`	User Portal's IP address.
`cert_path`	Path to the User Portal's SSL certificate files.
`[CONN]`	
`bind_ip`	IP address of the server, running the `fudopv` script. The IP address must be the same as the IP address defined in the *API* section in user configuration. This parameter is optional.
`[AUTH]`	
`username`	User login as defined in step 3.
`otp`	Path to the otp.txt file containing the one time password.
`secret`	Path to the secret.txt file containing user's static password.

Note:

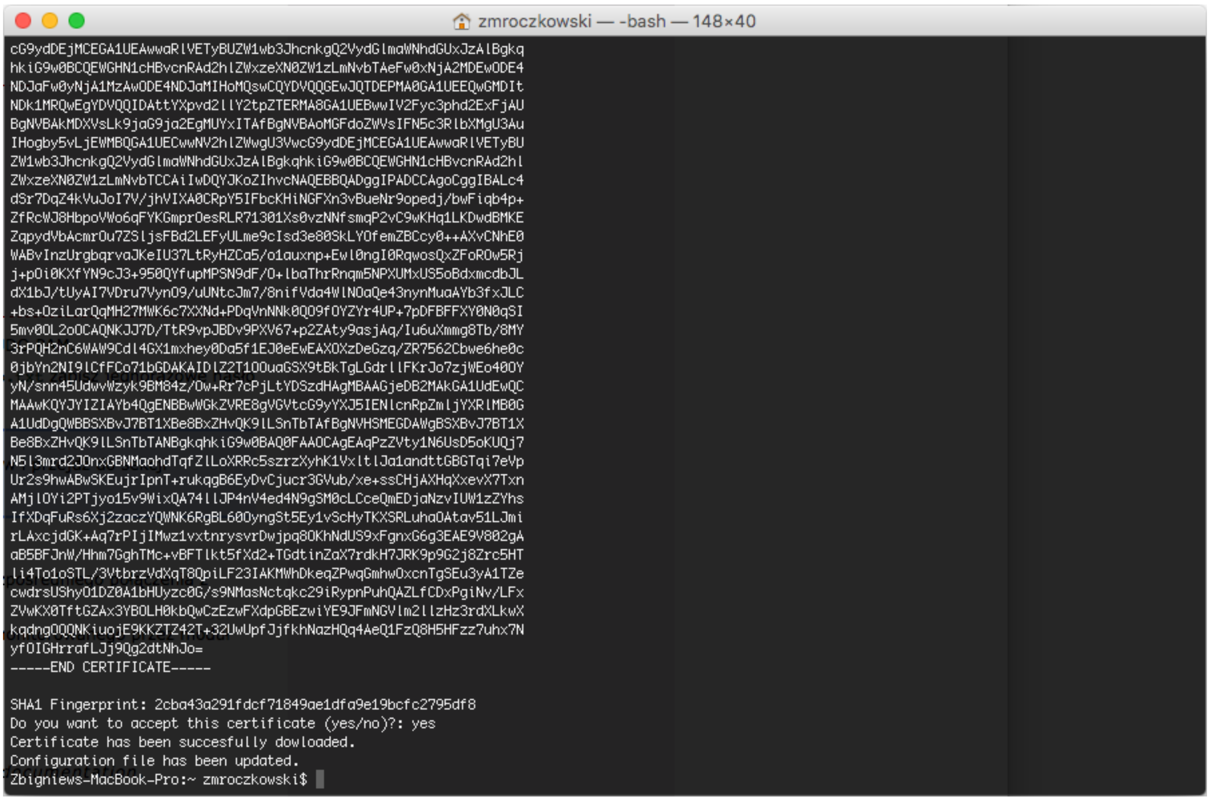
- In the `[FUDO]` section, in the `address` line, enter the User Portal IP address.
- Leave the `cert_path` line as is, it will be updated automatically after successfully running the `fudopv getcert` command.

- If you specified the IP address allowed to access Fudo PAM over API, 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:

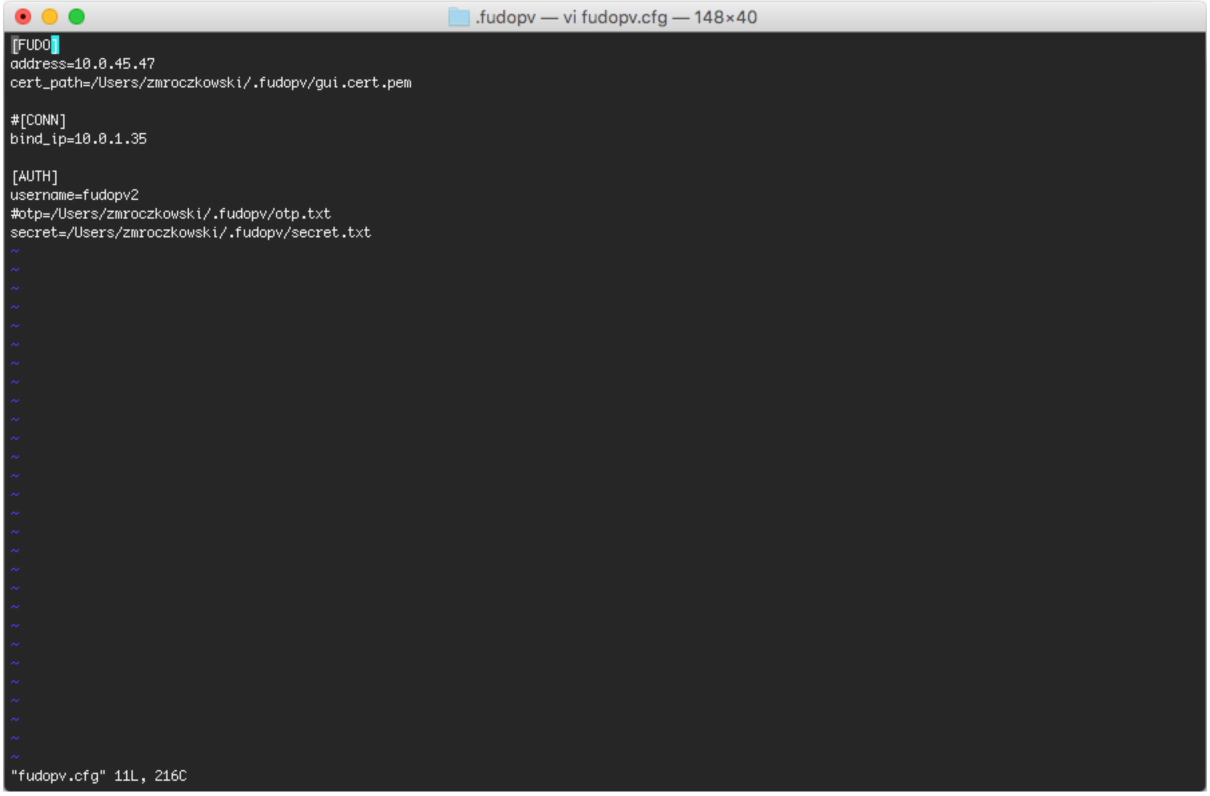
```
[FUDO]
address=10.0.0.8.61
cert_path=<CERT_PATH>

#[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 User Portal's SSL certificate.



```
cG9ydDEjMCEGA1UEAwwaRlVETyBUZW1wb3JhcnkgQ2VydGlmaWNhdGUxJzAlBgkq
hkiG9w0BCQEWGHN1cHBvcnRAd2hlZWxzeXN0ZW1zLmNvbTAeFw0xNjA2MDEwODE4
NDJaFw0yNjA1MzAwODE4NDJaMIHoMQswCQYDVQQGEwJQTDEPMA0GA1UEEQwGMDIt
NDk1MRQwEgYDVQQIDAttYXpvd2llY2tpZTERMA8GA1UEBwwIV2Fyc3phd2ExFjAU
BgNVBAkMDXVsLk9jaG9ja2EgMUYxITAfBgNVBAoMGFdoZWVsIFN5c3RlbXMgU3Au
IHogby5vLjEWMBQGA1UECwwNV2hlZWwgU3VwcG9ydDEjMCEGA1UEAwwaRlVETyBU
ZW1wb3JhcnkgQ2VydGlmaWNhdGUxJzAlBgkqhkiG9w0BCQEWGHN1cHBvcnRAd2hl
ZWxzeXN0ZW1zLmNvbTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALc4
dSr7DqZ4kVuJoI7V/jhVIXA0CRpY5IFbcKHiNGFXn3vBueNr9opedj/bwFiqb4p+
ZfRcWJ8HbpoVWo6qFYKGmprOesRLR71301Xs0vzNNfsmqP2vC9wKHq1LKDwdBMKE
ZqpydVbAcmrOu7ZSljsFBd2LEFyULme9cIsd3e80SkLYOfemZBCcy0++AXvCNhE0
WABvInzUrgbqrvaJKeIU37LtRyHZCa5/o1auxnp+Ewl0ngI0RqwosQxZFoROw5Rj
j+pOi0KXfYN9cJ3+950QYfupMPSN9dF/O+lbaThrRnqm5NPXUMxUS5oBdxmcdbJL
dX1bJ/tUyAI7VDru7VynO9/uUNtcJm7/8nifVda4WlNOaQe43nynMuaAYb3fxJLC
+bs+OziLarQqMH27MWK6c7XXNd+PDqVnNNk0QO9fOYZYr4UP+7pDFBFFXY0N0qSI
5mv0OL2oOCAQNKJJ7D/TtR9vpJBDv9PXV67+p2ZAty9asjAq/Iu6uXmmg8Tb/8MY
3rPQH2nC6WAW9Cdl4GX1mxhey0Da5f1EJ0eEwEAXOXzDeGzq/ZR7562Cbwe6he0c
0jbYn2NI9lCfFCo71bGDAKAIDlZ2T1OOuaGSX9tBkTgLGdrllFKrJo7zjWEo40OY
yN/snn45UdwvWzyk9BM84z/Ow+Rr7cPjLtYDSzdHAgMBAAGjeDB2MAkGA1UdEwQC
MAAwKQYJYIZIAYb4QgENBBwWGkZVRE8gVGVtcG9yYXJ5IENlcnRpZmljYXRlMB0G
A1UdDgQWBBSXBvJ7BT1XBe8BxZHvQK9lLSnTbTAfBgNVHSMEGDAWgBSXBvJ7BT1X
Be8BxZHvQK9lLSnTbTANBgkqhkiG9w0BAQ0FAAOCAgEAqPzZVty1N6UsD5oKUQj7
N5l3mrd2JOnxGBNMaohdTqfZlLoXRRc5szrzXyhK1VxltlJa1andttGBGTqi7eVp
Ur2s9hwABwSKEujrIpnT+rukqgB6EyDvCjucr3GVub/xe+ssCHjAXHqXxevX7Txn
AMjlOYi2PTjyo15v9WixQA74llJP4nV4ed4N9gSM0cLCceQmEDjaNzvIUW1zZYhs
IfXDqFuRs6Xj2zaczYQWNK6RgBL60OyngSt5Ey1vScHyTKXSRLuhaOAtav51LJmi
rLAxcjdGK+Aq7rPIjIMwz1vxtnrysvrDwjpq8OKhNdUS9xFgnxG6g3EAE9V802gA
aB5BFJnW/Hhm7GghTMc+vBFTlkt5fXd2+TGdtinZaX7rdkH7JRK9p9G2j8Zrc5HT
li4To1oSTL/3VtbrzVdXqT8QpiLF23IAKMWhDkeqZPwqGmhwOxcnTgSEu3yA1TZe
cwdrsUShyO1DZ0A1bHUyzc0G/s9NMasNctqkc29iRypnPuhQAZLfCDxPgiNv/LFx
ZVwKX0TftGZAx3YBOLH0kbQwCzEzwFXdpGBEzwiYE9JFmNGVlm2llzHz3rdXLkwX
kqdngOQQNKiuojE9KKZTZ42T+32UwUpfJjfkhNazHQq4AeQ1FzQ8H5HFzz7uhx7N
yfOIGHrrafLJj9Qg2dtNhJo=
-----END CERTIFICATE-----

SHA1 Fingerprint: 2cba43a291fdcf71849ae1dfa9e19bcfc2795df8
Do you want to accept this certificate (yes/no)?: yes
Certificate has been succesfully dowloaded.
Configuration file has been updated.
Zbigniews-MacBook-Pro:~ zmroczkowski$ 
```

Note: After running the script successfully, the path to the certificate in the configuration file will be automatically updated.

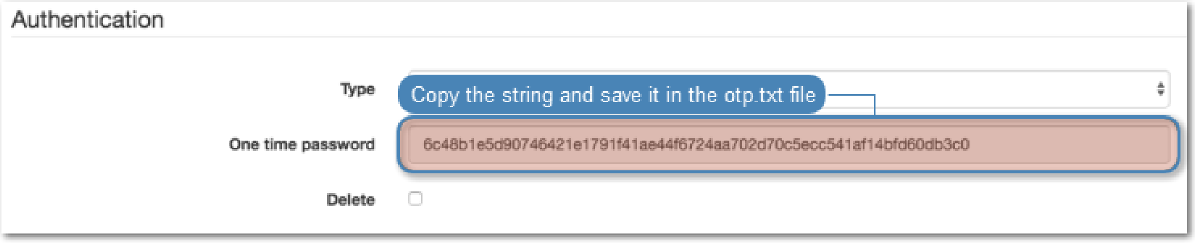


```
[FUDO]
address=10.0.45.47
cert_path=/Users/zmroczkowski/.fudopv/gui.cert.pem

#[CONN]
bind_ip=10.0.1.35

[AUTH]
username=fudopv2
#otp=/Users/zmroczkowski/.fudopv/otp.txt
secret=/Users/zmroczkowski/.fudopv/secret.txt
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"fudopv.cfg" 11L, 216C
```

7. Edit the `secret.txt` file and provide user's static password; or edit the `otp.txt` file and store the one time password.

Note:

- The one time password can be found in user's properties, in the *Authentication* section.



Authentication

Type

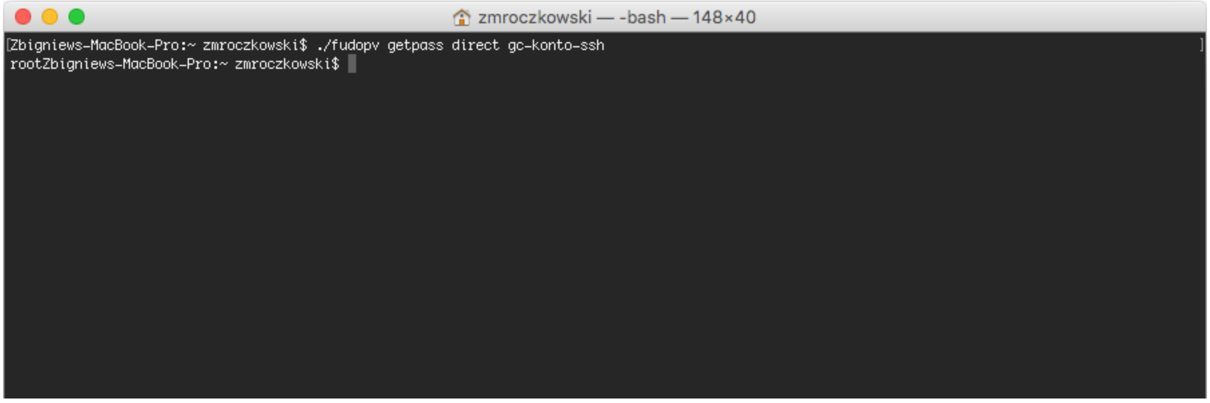
One time password: 6c48b1e5d90746421e1791f41ae44f6724aa702d70c5ecc541af14bfd60db3c0

Delete □

- The `otp.txt` file will be automatically updated each time the `fudopv getpass` command is run.

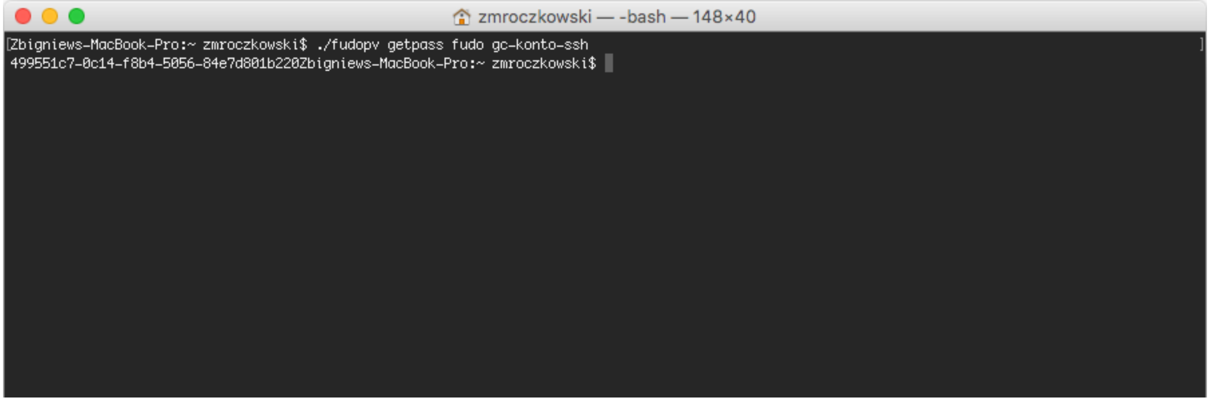
8. Run command:

- `fudopv getpass direct <account_name>`, to fetch password to connect directly to the server.



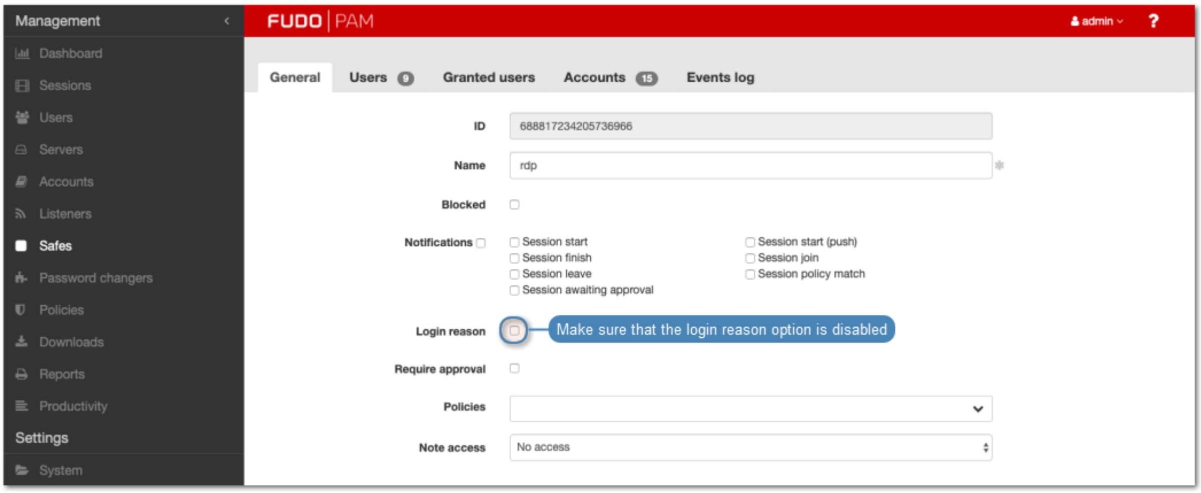
```
[Zbigniews-MacBook-Pro:~ zmroczkowski$ ./fudopv getpass direct gc-konto-ssh
 rootZbigniews-MacBook-Pro:~ zmroczkowski$
```

- `fudopv getpass fudo <account_name>`, to fetch password to establish monitored connection with the target host.



```
[Zbigniews-MacBook-Pro:~ zmroczkowski$ ./fudopv getpass fudo gc-konto-ssh
 499551c7-0c14-f8b4-5056-84e7d801b220Zbigniews-MacBook-Pro:~ zmroczkowski$
```

> **Warning:** Correct operation of the `fudopv` script requires disabling the login reason prompt option in the safe's properties.



ID: 688817234205736966

Name: rdp

Blocked: □

Notifications □
□ Session start
□ Session finish
□ Session leave
□ Session awaiting approval
□ Session start (push)
□ Session join
□ Session policy match

Login reason: □ Make sure that the login reason option is disabled

Require approval: □

Policies:

Note access: No access

Related topics:

- *Compiling fudopv tool*
- *Deploying fudopv without compiling source files*
- *Authentication methods*

- *Data model*
- *System overview*
- *Setting up password changing on a Unix system*

17.4 API interface

AAPM's API interface is described in detail in the *Fudo PAM - API documentation* manual.

Related topics:

- *Compiling fudopv tool*
- *Using fudopv*
- *Deploying fudopv without compiling source files*
- *Data model*
- *System overview*
- *Setting up password changing on a Unix system*

17.5 Authentication methods

Conventions and symbols:

- **url**: `fudo` connection address,
- **->**: `fudopv` request,
- **<-**: response from Fudo PAM,
- **status**: response status,
- **FUDO**: Fudo IP address,
- **USER**: username,
- **SECRET**: password (static/OTP),
- **SESSIONID**: session token,
- **method**: HTTP protocol method: GET/POST/PUT,
- **{"key": "value"}**: JSON included in the request/response.

17.5.1 Static password

Static user password, stored in the `secret.txt` file.

- -> url: https://FUDO/api/portal/login
- -> method: POST
- -> `{"username": "USER", "password": "SECRET"}`
- <- status:

  - 200, OK
    - <- `{"sessionid": "SESSIONID"}`
  - 401, UNAUTHORIZED
  - <- *Not applicable.*

17.5.2 Token

One time password stored in the `otp.txt` file.

- -> url: https://FUDO/api/portal/login
- -> method: POST
- -> `{"username": "USER", "otp": "SECRET"}`
- <- status:
  - 200, OK
    - <- `{"otp": NEW_SECRET, "sessionid": "SESSIONID"}`
  - 401, UNAUTHORIZED
  - <- *Not applicable.*

After saving new password in the `otp.txt`, `fudopv` sends a confirmation message.

- -> url: https://FUDO/api/portal/confirm
- -> method: POST
- -> `{"otp": "NEW_SECRET"}`
- <- status: 204, NO CONTENT

Related topics:

- *Compiling fudopv tool*
- *Deploying fudopv without compiling source files*
- *Using fudopv*

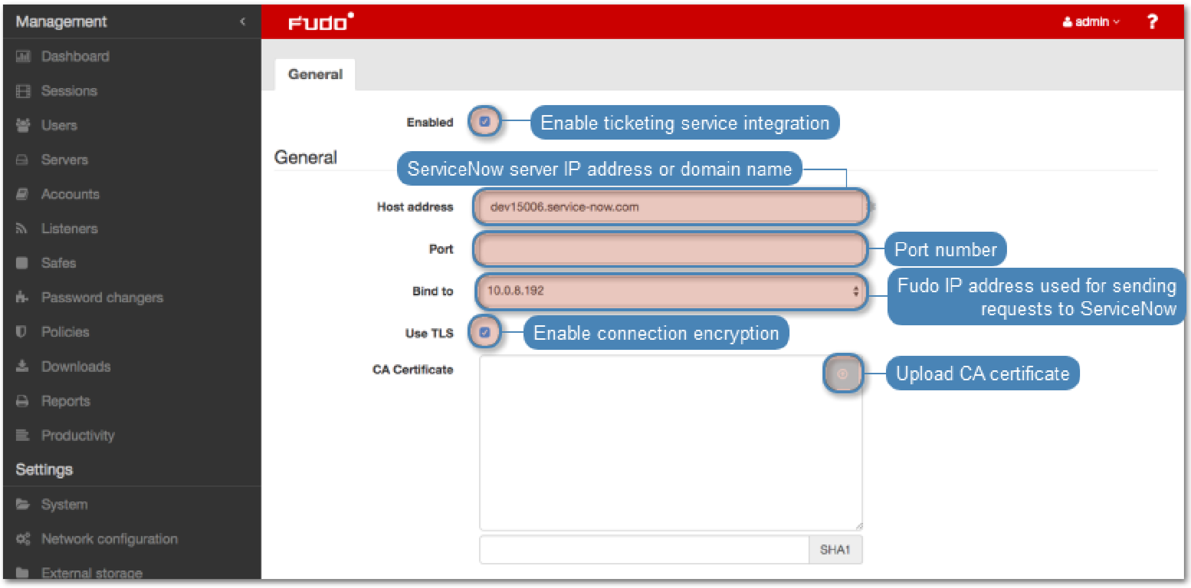
CHAPTER 18

Service Now

18.1 Configuration

To configure *ServiceNow*, proceed as follows.

1. Select *Settings* > *Ticketing system.*
2. Select *Enable* option to enable ticketing service integration.
3. In the *General* section, provide IP address and port number of *ServiceNow* REST API.
4. Select the *Use TLS* option to enable connection encryption.
5. From the *Bind to* drop-down list, select the IP address used by Fudo PAM for sending requests to *ServiceNow* API.



General

Enabled ☑ — Enable ticketing service integration

ServiceNow server IP address or domain name

Host address: dev15006.service-now.com

Port: — Port number

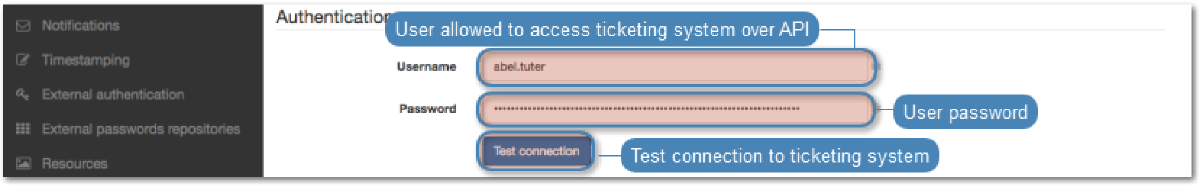
Bind to: 10.0.8.192 — Fudo IP address used for sending requests to ServiceNow

Use TLS ☑ — Enable connection encryption

CA Certificate — Upload CA certificate

6. In the *Authentication* section, provide user credentials allowed to access *ServiceNow* over defined REST API.

Note: Click *Test connection* to verify configuration parameter values. The result of testing will be a ticket in *ServiceNow*, containing the configuration values prefixed with the `test_` string.



Authentication

Username: abel.tuter

Password: ••

User allowed to access ticketing system over API

User password

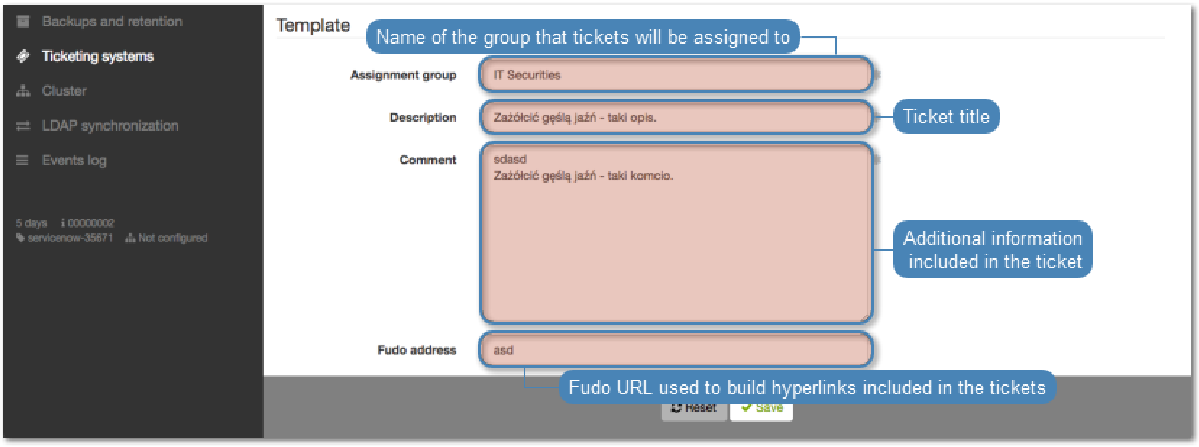
Test connection to ticketing system

7. In the *Template* section, in the *Assignment group*, define the *ServiceNow* users group to which the tickets will be assigned.

8. In the *Description* field, provide the ticket template title.

9. In the *Comment* field, provide additional information to be included in the ticket.

10. Enter Fudo URL that will be used to create quick access hyperlinks included in tickets.



Template

Assignment group: IT Securities

Description: Zażółcić gęślą jaźń - taki opis.

Comment: sdasd
Zażółcić gęślą jaźń - taki komcio.

Fudo address: asd

Name of the group that tickets will be assigned to

Ticket title

Additional information included in the ticket

Fudo URL used to build hyperlinks included in the tickets

11. Click *Save*.

Related topics:

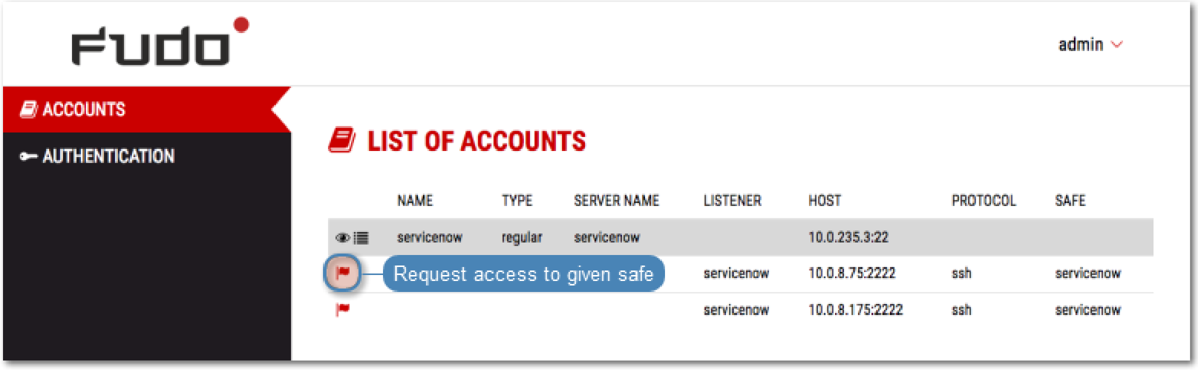
- *Requesting access to safe*
- *Granting access*

18.2 Requesting access to safe

Note: Usernames on Fudo PAM and *ServiceNow* must be the same to ensure correct requests processing.

To request access to safe, proceed as follows.

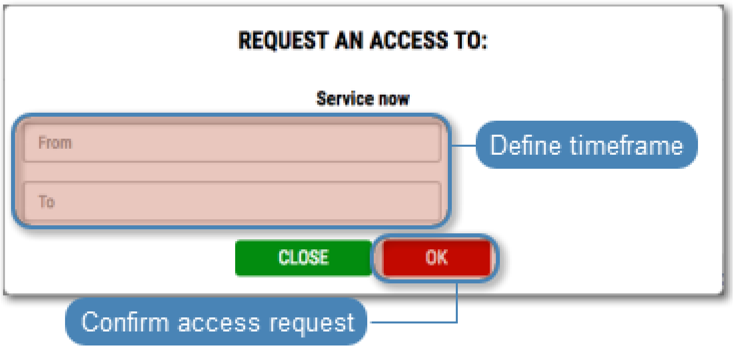
1. Log in to *User Portal*.
2. Find desired safe and click 🚩.



LIST OF ACCOUNTS

	NAME	TYPE	SERVER NAME	LISTENER	HOST	PROTOCOL	SAFE
	servicenow	regular	servicenow		10.0.235.3:22		
				servicenow	10.0.8.75:2222	ssh	servicenow
				servicenow	10.0.8.175:2222	ssh	servicenow

3. Define time period and click *OK*.



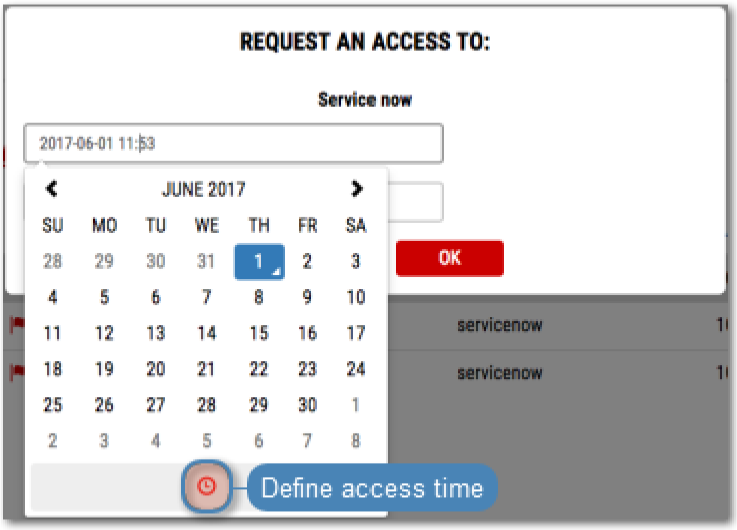
REQUEST AN ACCESS TO:

Service now

From

To

Note: Click the 🕓 icon to access time settings.



REQUEST AN ACCESS TO:

Service now

2017-06-01 11:53

JUNE 2017

SU	MO	TU	WE	TH	FR	SA
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1
2	3	4	5	6	7	8

Related topics:

- *Configuration*
- *Granting access*

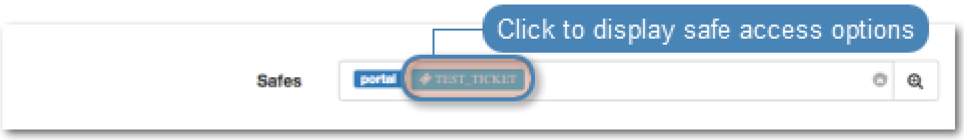
18.3 Granting access

To grant access based on a *ServiceNow* ticket, proceed as follows.

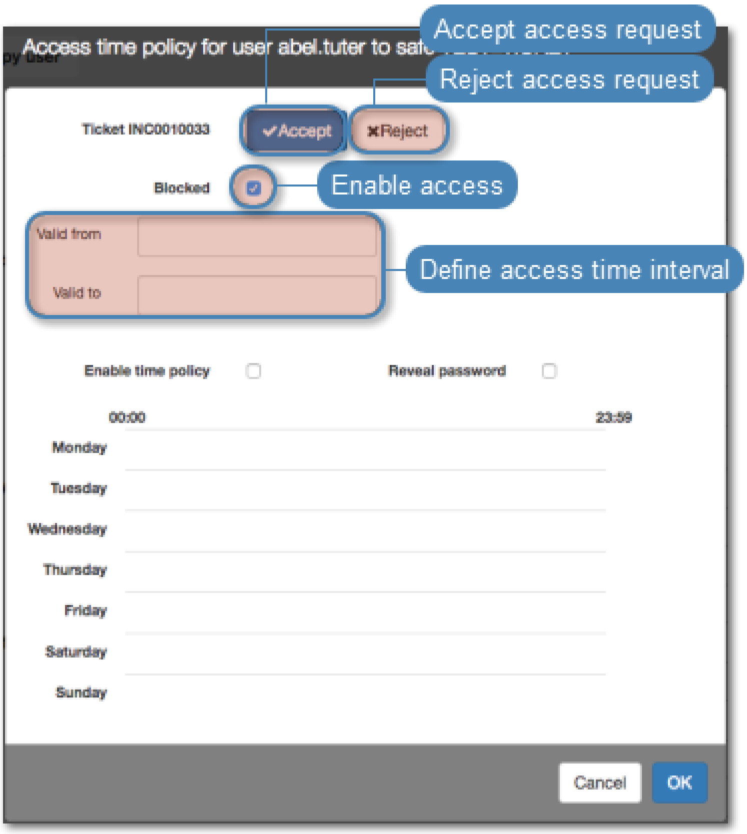
1. Select *Management* > *Users*.
2. Find and click user requesting access.

Note: Users with pending access requests are marked with 🎫 icon.

3. In the *Safes* field, find and click the object that the user requests to access.


Click to display safe access options

4. Deselect *Blocked* option and define access time period.
5. Click *Accept*.


Accept access request

Reject access request

Enable access

Define access time interval

Note: Safe access management options can be also accessed from within the safe edit form.

Related topics:

- *Configuration*

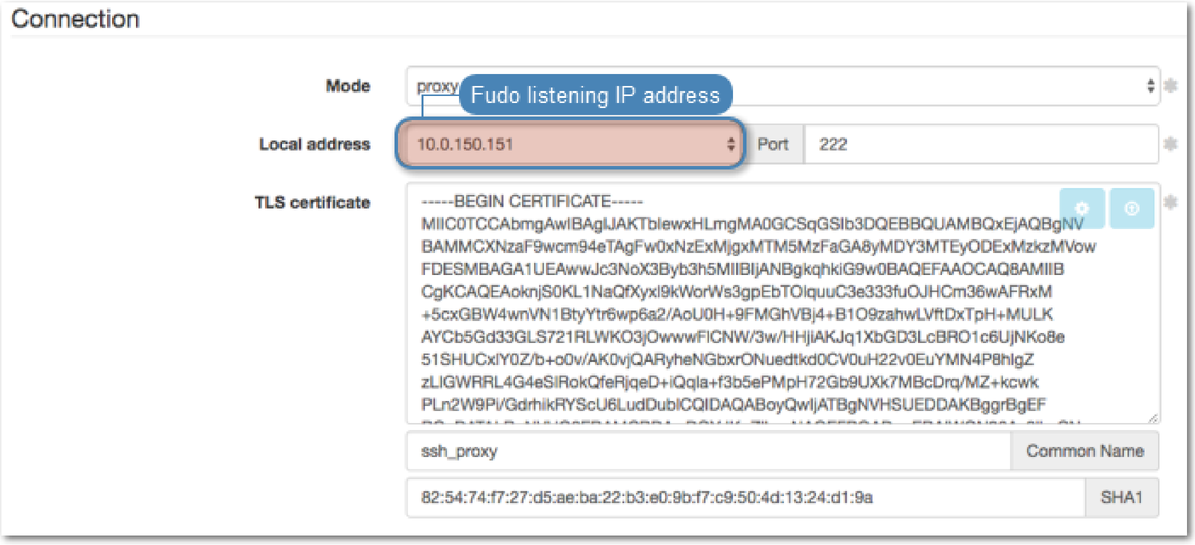
- *Requesting access to safe*

CHAPTER 19

Client applications

19.1 PuTTY

1. Download and launch PuTTY.
2. In the *Host Name (or IP address)* field, enter IP address defined in the listener.



Connection

Mode: proxy

Fudo listening IP address

Local address: 10.0.150.151 Port 222

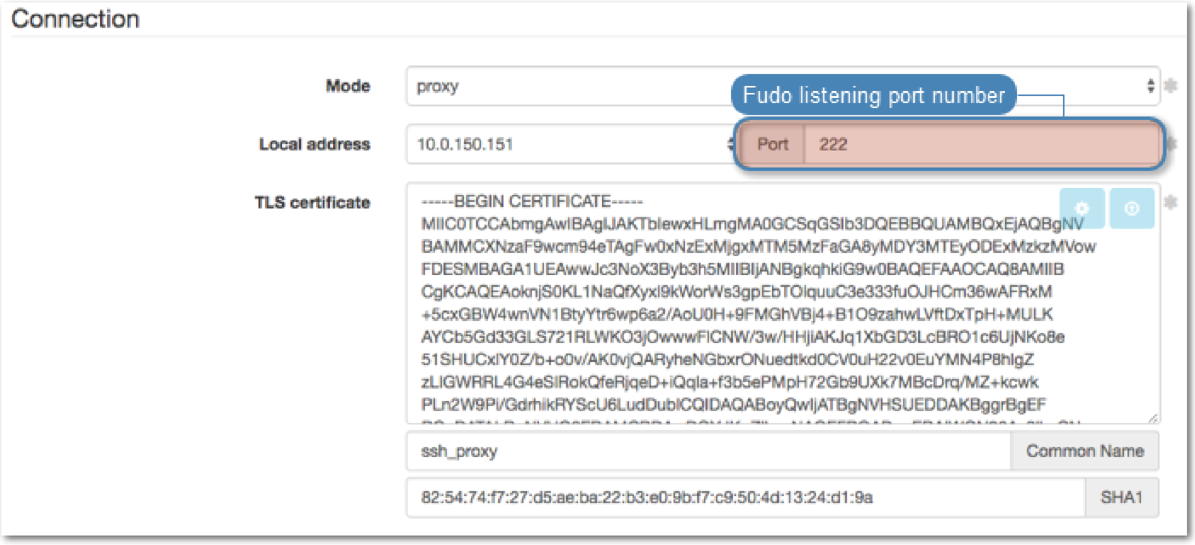
TLS certificate:

```
-----BEGIN CERTIFICATE-----
MIIC0TCCAbmgAwIBAgIJAKTblewxHLmgMA0GCSqGSIb3DQEBBQUAMBQxEjAQBgNV
BAMMCXNzaF9wcm94eTAgFw0xNzExMjgxMTM5MzFaGA8yMDY3MTEyODExMzkzMVow
FDESMBAGA1UEAwwJc3NoX3Byb3h5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAoknjS0KL1NaQfXyxl9kWorWs3gpEbTOlquuC3e333fuOJHCm36wAFRxM
+5cxGBW4wnVN1BtyYtr6wp6a2/AoU0H+9FMGhVBj4+B1O9zahwLVftDxTpH+MULK
AYCb5Gd33GLS721RLWKO3jOwwwFlCNW/3w/HHjiAKJq1XbGD3LcBRO1c6UjNKo8e
51SHUCxlY0Z/b+o0v/AK0vjQARyheNGbxrONuedtkd0CV0uH22v0EuYMN4P8hlgZ
zLIGWRRL4G4eSIRokQfeRjqeD+iQqla+f3b5ePMpH72Gb9UXk7MBcDrq/MZ+kcwk
PLn2W9Pi/GdrhikRYScU6LudDubICQIDAQABoyQwIjATBgNVHSUEDDAKBggrBgEF
```

ssh_proxy Common Name

82:54:74:f7:27:d5:ae:ba:22:b3:e0:9b:f7:c9:50:4d:13:24:d1:9a SHA1

3. In the *Port number* field, enter port number defined in the listener.



Connection

Mode: proxy

Local address: 10.0.150.151 Port 222

Fudo listening port number

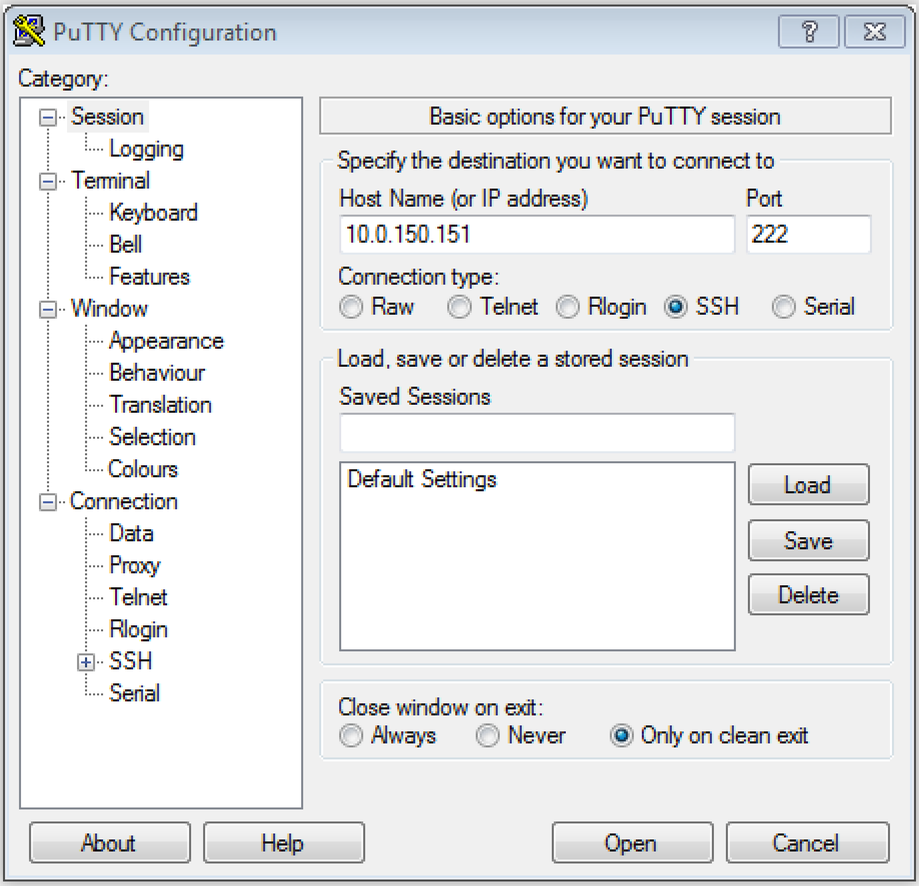
TLS certificate:

```
-----BEGIN CERTIFICATE-----
MIIC0TCCAbmgAwIBAgIJAKTblewxHLmgMA0GCSqGSIb3DQEBBQUAMBQxEjAQBgNV
BAMMCXNzaF9wcm94eTAgFw0xNzExMjgxMTM5MzFaGA8yMDY3MTEyODExMzkzMVow
FDESMBAGA1UEAwwJc3NoX3Byb3h5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAoknjS0KL1NaQfXyxl9kWorWs3gpEbTOlquuC3e333fuOJHCm36wAFRxM
+5cxGBW4wnVN1BtyYtr6wp6a2/AoU0H+9FMGhVBj4+B1O9zahwLVftDxTpH+MULK
AYCb5Gd33GLS721RLWKO3jOwwwFICNW/3w/HHjiAKJq1XbGD3LcBRO1c6UjNKo8e
51SHUCxlY0Z/b+o0v/AK0vjQARyheNGbxrONuedtkd0CV0uH22v0EuYMN4P8hlgZ
zLIGWRRL4G4eSIRokQfeRjqeD+iQqla+f3b5ePMpH72Gb9UXk7MBcDrq/MZ+kcwk
PLn2W9Pi/GdrhikRYScU6LudDubICQIDAQABoyQwIjATBgNVHSUEDDAKBggrBgEF
```

ssh_proxy Common Name

82:54:74:f7:27:d5:ae:ba:22:b3:e0:9b:f7:c9:50:4d:13:24:d1:9a SHA1

4. Select the SSH connection type.



Specify the destination you want to connect to

Host Name (or IP address): 10.0.150.151

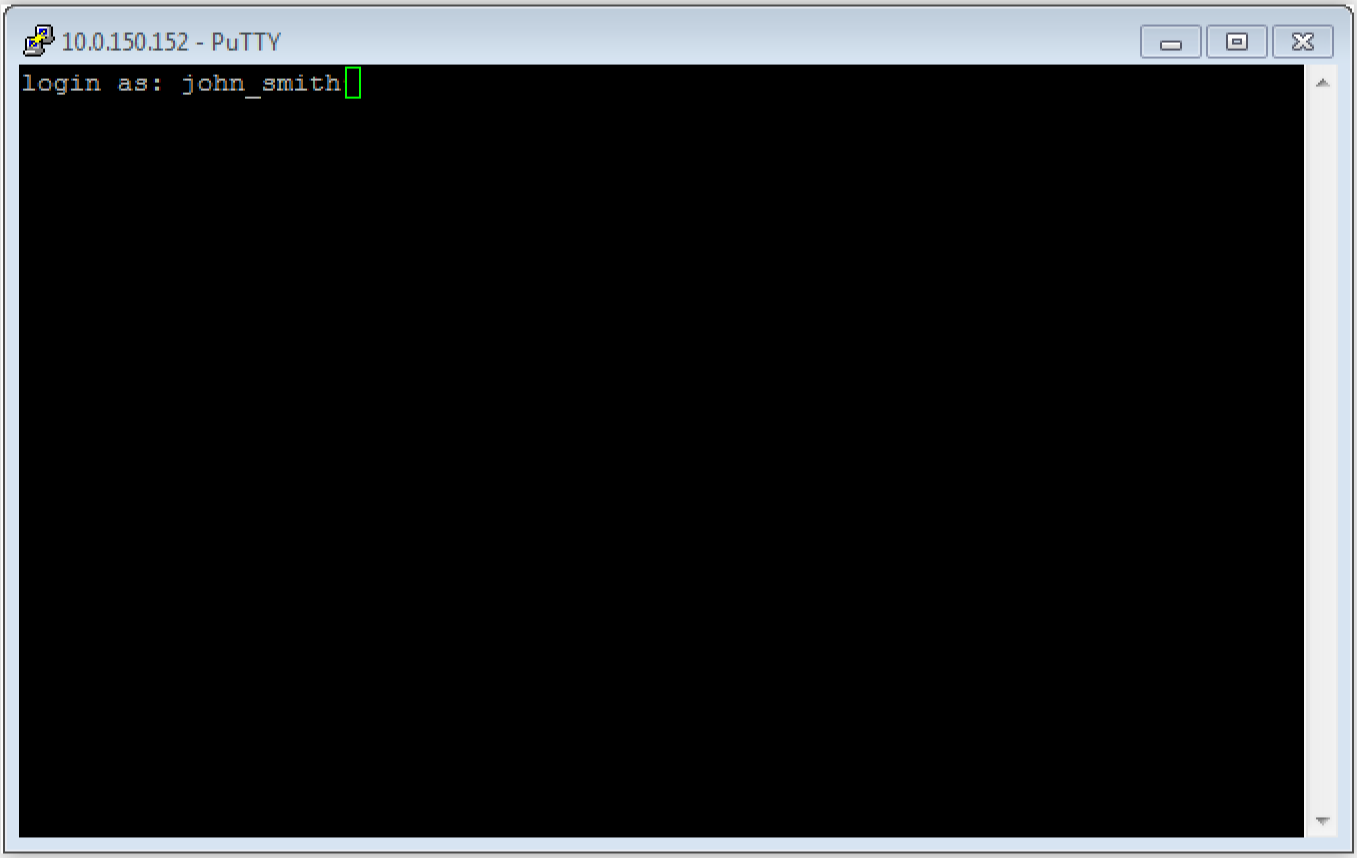
Port: 222

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

5. Click *Open*.

6. Enter username.



```
login as: john_smith
```

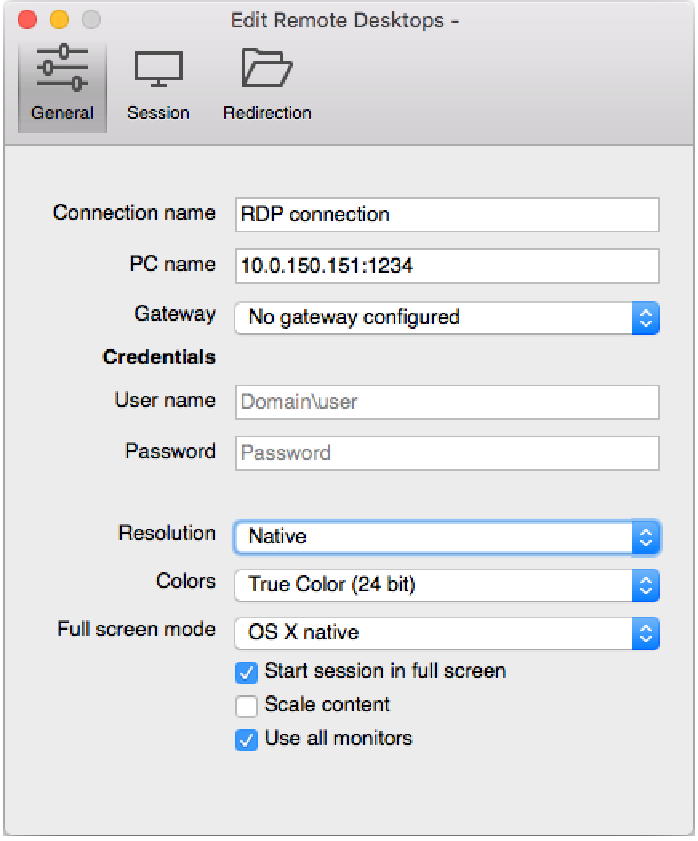
7. Enter password.

Related topics:

- *SSH*
- *Creating an SSH server*
- *Creating an SSH listener*

19.2 Microsoft Remote Desktop

1. Launch *Microsoft Remote Desktop*.
2. Enter connection name.
3. Provide destination host IP address and RDP service port number in the *PC name* field as defined in the listener object.



Edit Remote Desktops -

Connection name: RDP connection

PC name: 10.0.150.151:1234

Gateway: No gateway configured

Credentials

User name: Domain\user

Password: Password

Resolution: Native

Colors: True Color (24 bit)

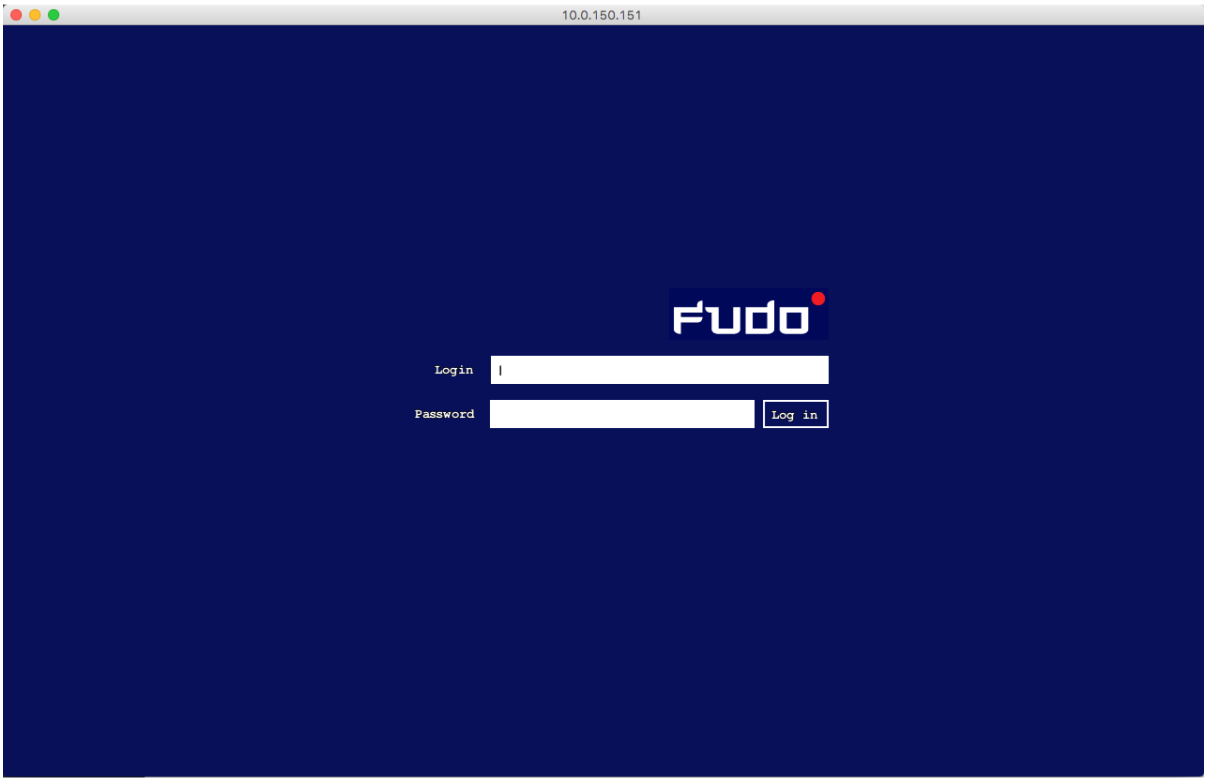
Full screen mode: OS X native

☑ Start session in full screen

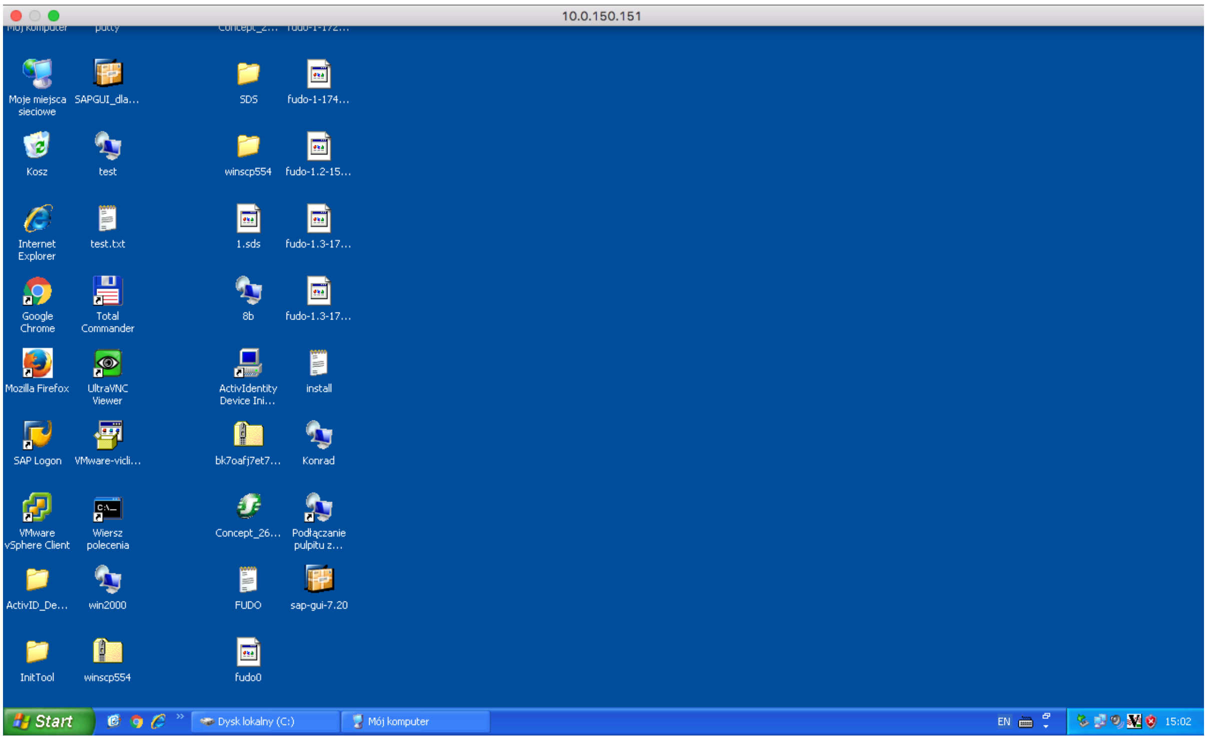
□ Scale content

☑ Use all monitors

3. Enter user login and password and press the [Enter] keyboard key.



Note: Fudo PAM enables using custom login, no access and session termination screens for RDP and VNC connections. For more information on user defined images for graphical remote sessions, refer to the *Resources* topic.

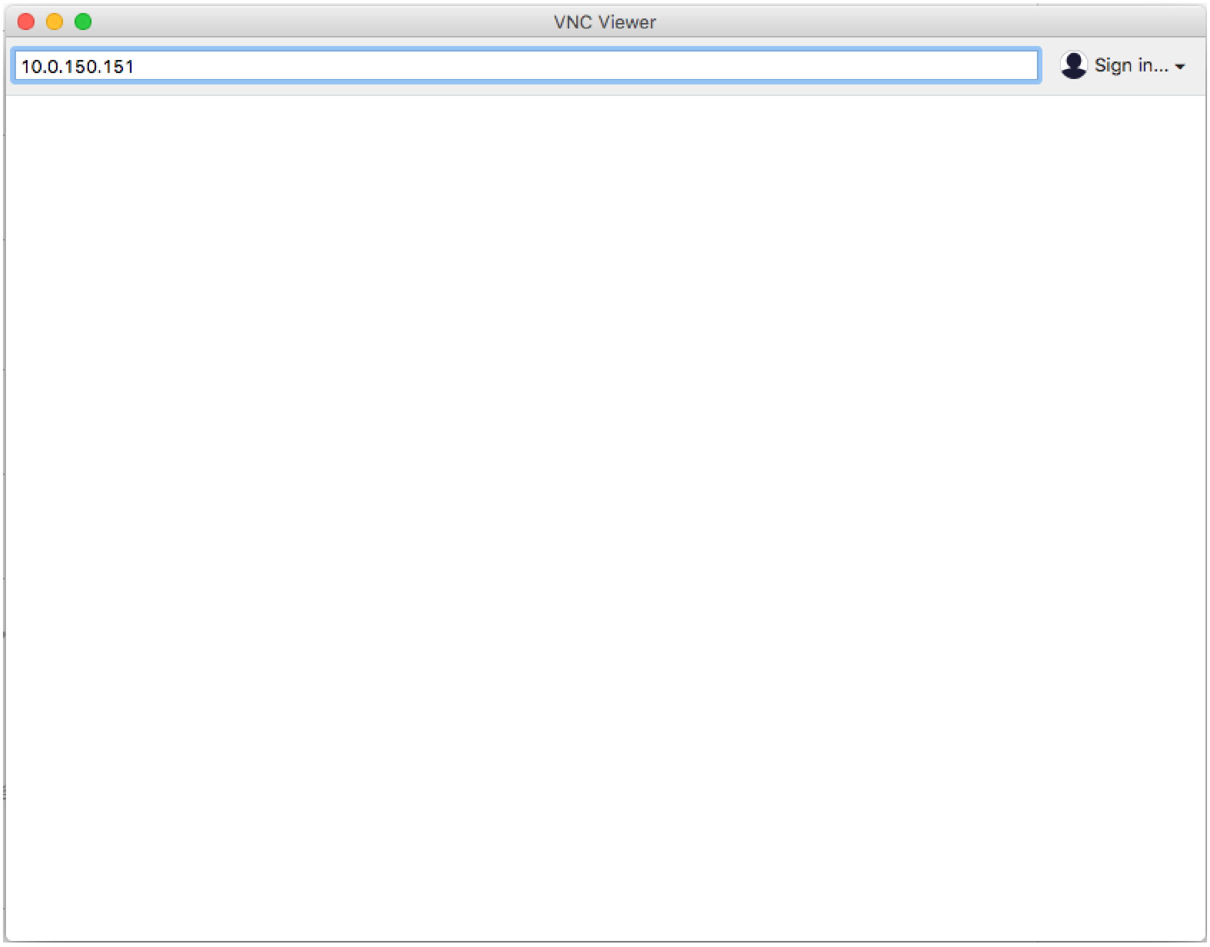


Related topics:

- *RDP*
- *Creating an RDP server*
- *Creating an RDP listener*

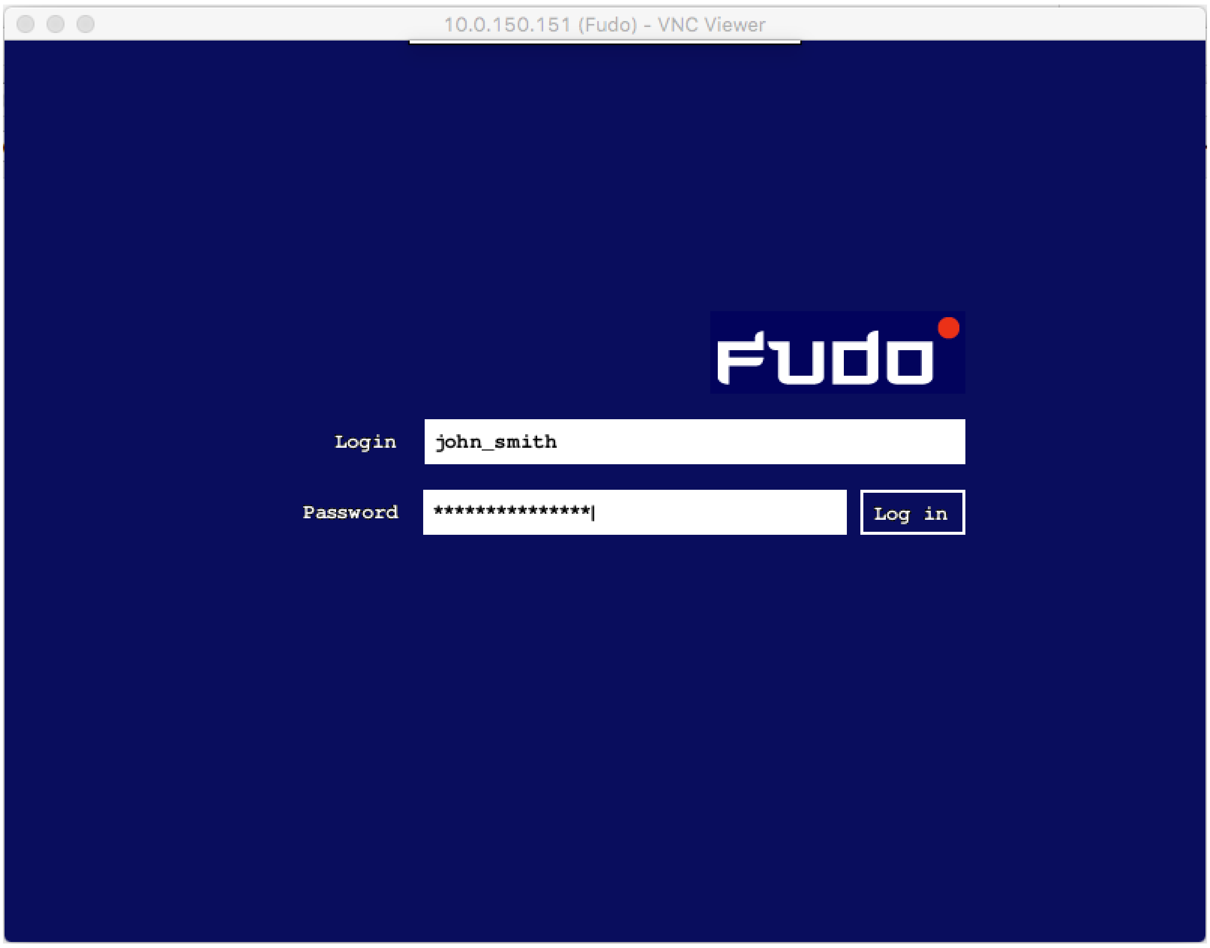
19.3 VNC Viewer

1. Launch *VNC Viewer*.
2. Enter IP address in the server address field as defined in the listener object.



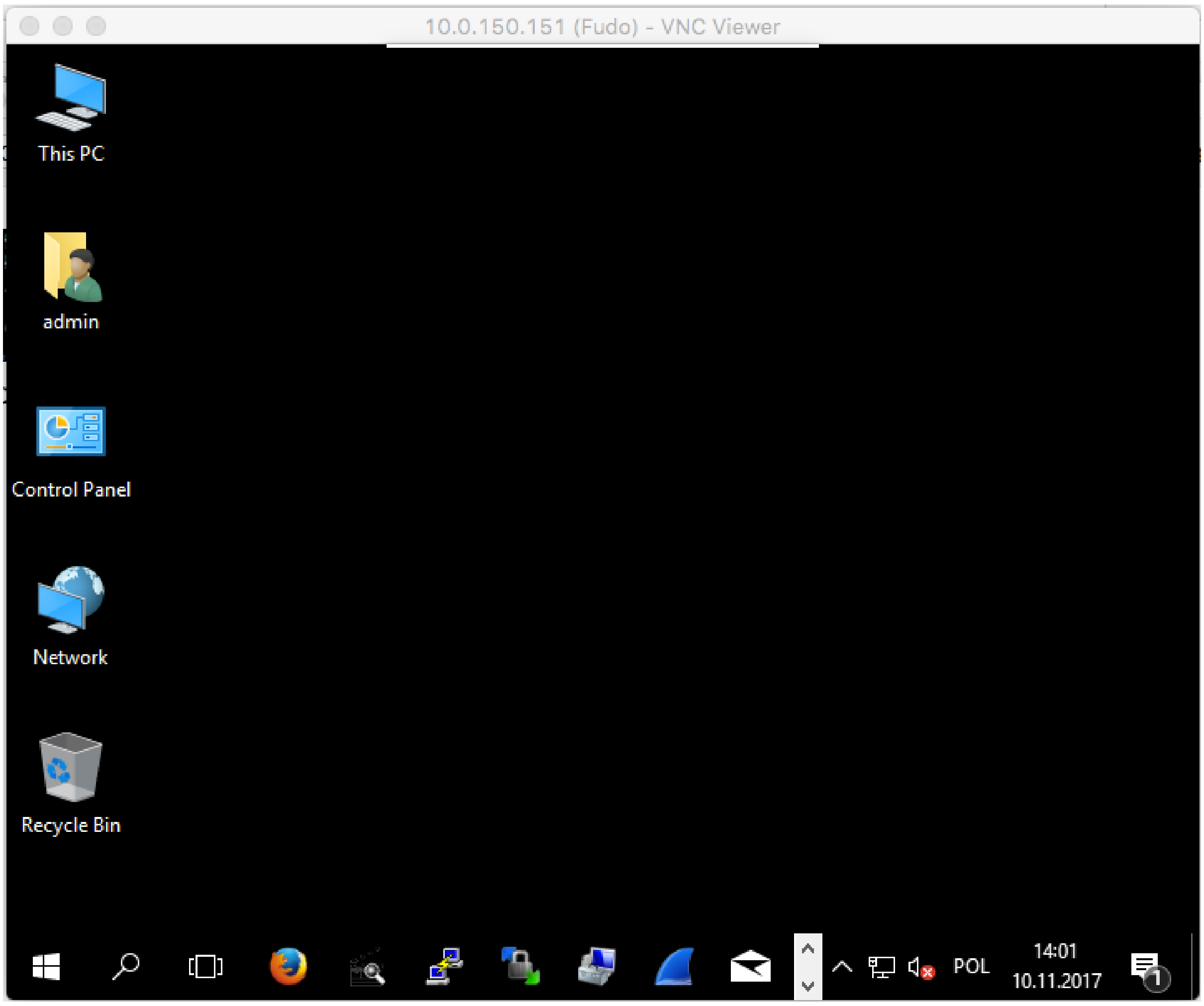
10.0.150.151

3. Enter username and password and press the enter key.



Login john_smith

Password ****************

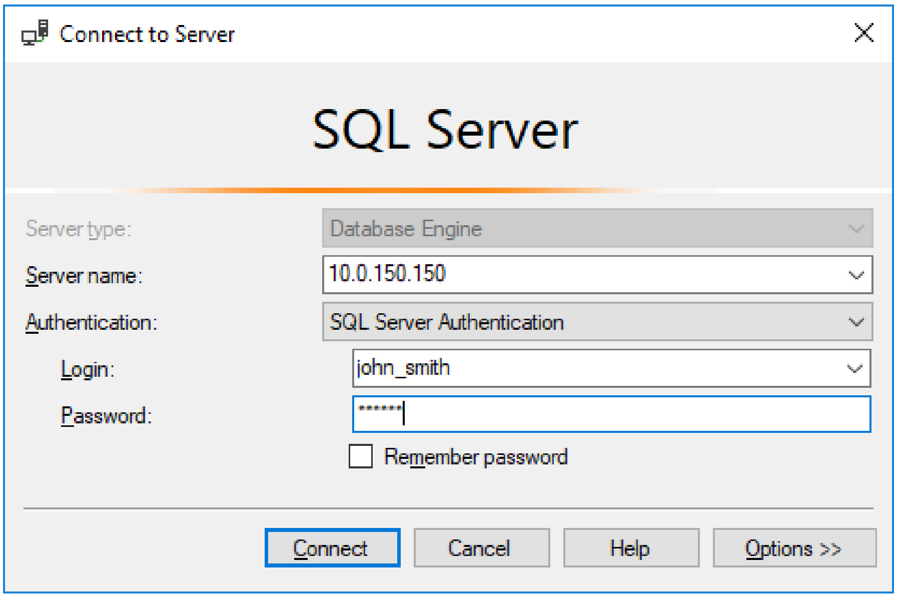


Related topics:

- *VNC*
- *Creating a VNC server*
- *Creating a VNC listener*

19.4 SQL Server Management Studio

1. Start *SQL Server Management Studio*.
2. Enter IP address as defined in the listener object.
3. From the *Authentication* drop-down list, select *SQL Server Authentication*.
4. Enter user login and password.
5. Click *Connect*.



Server type: Database Engine

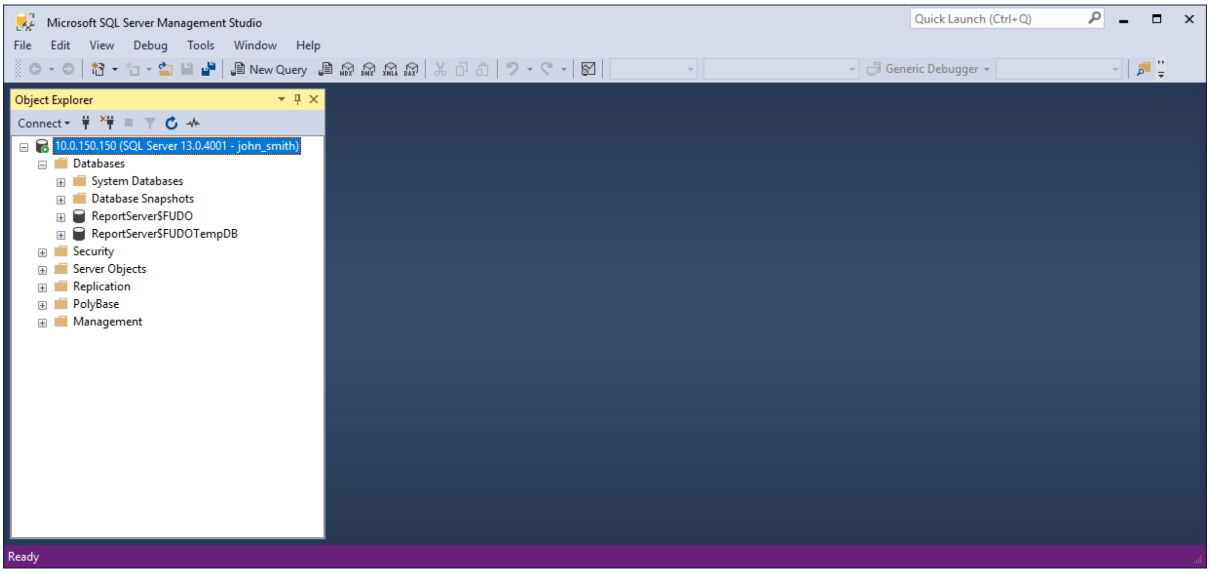
Server name: 10.0.150.150

Authentication: SQL Server Authentication

Login: john_smith

Password: ******

□ Remember password



Related topics:

- *MS SQL*
- *Creating a MS SQL server*
- *Creating a MS SQL listener*

CHAPTER 20

Troubleshooting

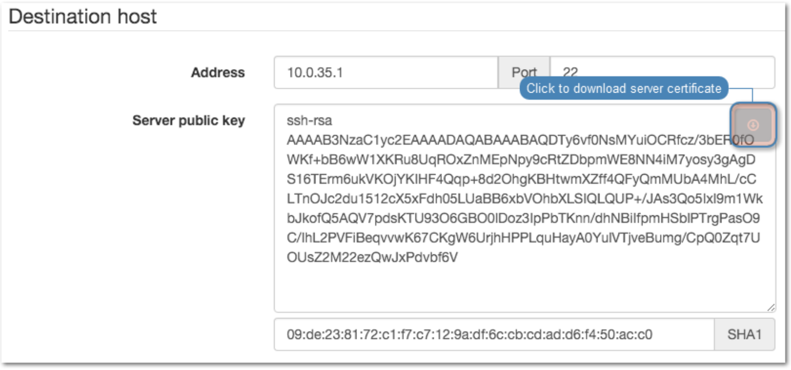
20.1 Booting up

Problem	Symptoms and solution
Fudo PAM does not boot up	• Make sure that both power supplies are connected to power outlets. Not connecting both power supplies will result in sound alarm. • Make sure that encryption key is properly connected. • In case the problem is a result of unsuccessful system update, wait a few minutes. During that time, Fudo PAM will detect the problem and will restore previous system revision.

20.2 Connecting to servers

Problem	Symptoms and solution
Cannot connect to server	**Symptoms:** • User cannot log in. • Events log entry: *Authentication failed: Invalid username kowalski or password.*
	Solution: • Verify that user definition exists in Fudo PAM database. • Make the login credentials are correct. • Make sure that the client software does not have outdated credentials stored. • Check if the user has a domain defined and make sure it is provided when attempting to log in. • If there are two users with the same login, one of which has the domain configured the same as the *default domain*, and the other does not have the domain defined, Fudo PAM will report authentication problem as it cannot determine which user is trying to connect.
	Symptoms: events log entry: *Unable to establish connection to server zbigniew (10.0.35.53:3399).*
	Cause: incorrect server configuration.
	Solution: • Verify that the server in question is properly configured (IP address, port number). • Check if the server is reachable from Fudo PAM: 1. Log in to Fudo PAM administration panel. 2. Select *Settings > System*, *Diagnostics* tab. 3. Enter server address in the *Ping* section and execute command and test host's availability. • Check if the server is reachable on given port number: 1. Log in to Fudo PAM administration panel. 2. Select *Settings > System*, *Diagnostics* tab. 3. Enter server address along with the port number in the *Netcat* section and execute command.
	Symptoms: Message in client software: *Cannot establish new connection because the capacity of the filesystem has been reached.*
	Cause: Storage usage has reached 90%.
	Solution: *Delete sessions* to free up storage space.

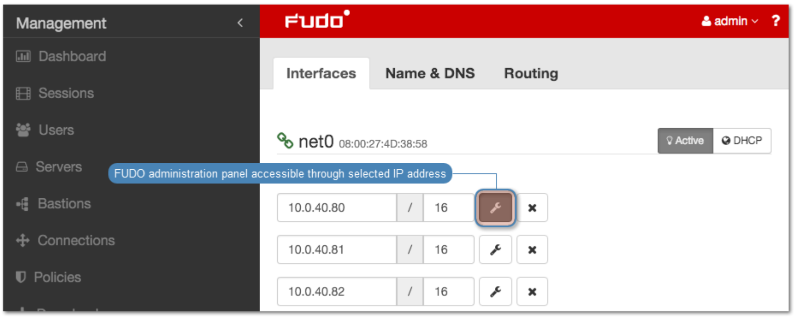
Problem	Symptoms and solution
When logging in not all of the users see the Fudo PAM logon screen.	**Cause:** - Credentials stored in RDP client result in users being automatically logged in to remote host. - Credentials stored in RDP client, user is successfully authenticated against credentials stored so the Fudo PAM logon screen is not displayed. Next, Fudo PAM forwards user credentials to target server but they are no longer valid which results in Windows gina being displayed.
	Symptoms: - Client software message: *Connection closed by remote host.* - Events log entry: *Failed to authenticate against the server as user root using password.*
	Cause: incorrect login credentials.
	Solution: provide correct login credentials in server configuration.
	Symptoms: - RDP client message: *Connection refused.* - SSH client message: *ssh: connect to host 10.0.1.111 port 10011: Connection refused*
	Cause: server has been blocked.
	Solution: log in to Fudo PAM administration panel and unblock the server.

Problem	Symptoms and solution
Connection is terminated	**Symptoms:** • User tries to log in to server monitored by Fudo PAM, after entering username and password session is immediately terminated. • Events log entry: *TLS certificate verification failed.*
	Solution:
	Download new target host certificate in the *Target host* section.
	 Destination host Address: 10.0.35.1 Port: 22 Server public key: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDTy6vf0NsMYuiOCRfcz/3bER0fO WKf+bB6wW1XKRu8UqROxZnMEpNpy9cRtZDbpmWE8NN4iM7yosy3gAgD S16TErm6ukVKOjYKIHF4Qqp+8d2OhgKBHtwmXZff4QFyQmMUbA4MhL/cC LTnOJc2du1512cX5xFdh05LUaBB6xbVOhbXLSIQLQUP+/JAs3Qo5Ixl9m1Wk bJkofQ5AQV7pdsKTU93O6GBO0IDoz3IpPbTKnn/dhNBilfpmHSblPTrgPasO9 C/IhL2PVFiBeqvvwK67CKgW6UrjhHPPLquHayA0YulVTjveBumg/CpQ0Zqt7U OUsZ2M22ezQwJxPdvbf6V 09:de:23:81:72:c1:f7:c7:12:9a:df:6c:cb:cd:ad:d6:f4:50:ac:c0 SHA1
	Symptoms: • After entering username and password the connection is terminated. • Events log entry: *RDP connection error.*
	Solution: check if in the *General* tab in TCP-Rdp properties, the *Encryption level* option is not set to `FIPS Compliant`.
Cannot connect to server	**Symptoms:** • Cannot log in to server with error message *User user0 not allowed to connect to server.* • Events log entry: *Authentication failed: User user0 not allowed to connect to server.*
	Cause: user is not assigned to proper connection.
	Solution: add user to appropriate connection object.

Problem	Symptoms and solution
	Symptoms: - After entering username and password, the screen freezes. - Events log entry *Terminating session: User user0 (id=848388532111147010) is blocked.*
	Cause: user is blocked.
	Solution: log in to Fudo PAM administration panel and unblock the user in question.
User has to provide login credentials twice	**Symptoms:** user connecting over RDP protocol enters login credentials and immediately afterwards is asked again for the same login information.
	Cause: server is a part of an infrastructure managed by connections broker which has detected an active user's session on another server.
	Symptoms: user connecting over SSH protocol enters login credentials and immediately afterwards is asked again for login information.
	Cause: in *connection* object options for login and password substitution are enabled but the input fields are left blank which results in two fold authentication - first time against Fudo PAM and second time against the target host.
Cannot connect to server over RDP protocol	**Symptoms:** - User connecting over RDP is disconnected a moment after establishing connection. - Events log entry: *RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.*
	Cause: connection is redirected to a host which does not listen on port number 3389.
	Solution: configure server in question so it accepts user connections on port number 3389.
	Symptoms: - Events log entry: *User user0 has no access to host 192.168.0.1:3389*
	Cause: connections broker determines an existing user session on another server and redirects user to that host but it is not configured on Fudo PAM or the user does not have sufficient access rights to connect to given server.
	Solution: - Make sure that the server object exists. - Add user to proper *safe* object.

Problem	Symptoms and solution
Cannot connect to Telnet5250 server using PC5250 client revision 20091005 S/20111019 S	**Symptoms:** cannot establish connection to target host.
	Cause: in case of aforementioned client applications, Fudo PAM requires setting up additional objects to enable TCP traffic on ports number 449, 8470 and 8476.
	Soluiton: • Add Telnet TN5250 server with default port number. • Add three server objects with `TCP` protocol and following port numbers 449, 8470 and 8476. • Add `TN5250` listener, in `Proxy` mode with default port number. • Add three `TCP` listener objects, in `Proxy` mode, with port numbers 449, 8470 and 8476. • Add `regular` account, define authentication parameters and assign it to the main TN5250 server definition. • Add three `anonymous` accounts and assign each to one of supporting servers. • Add safe and assign account with corresponding listeners.

20.3 Logging to administration panel

Problem	Symptoms and solution
Cannot log in to administration panel	• Make sure that Fudo PAM IP address is correct. • Set Fudo PAM IP address from the console as described in the *|product_name| System documentation* in the *Network interfaces configuration* topic. • Make sure that the IP address in question has the management access option enabled.  Management Dashboard Sessions Users Servers Bastions Connections Policies Fudo admin ? Interfaces Name & DNS Routing net0 08:00:27:4D:38:58 Active DHCP FUDO administration panel accessible through selected IP address 10.0.40.80 / 16 10.0.40.81 / 16 10.0.40.82 / 16

20.4 Session playback

Problem	Symptoms and solution
Cannot playback exported video	**Cause:** required video codecs are missing.
	Solution: install correct video codecs.
Administrator user does not see sessions	**Symptoms:** session list does not contain expected entries.
	Cause: insufficient access rights.
	Solution: grant access rights to specific user, server and connection objects.
Cannot playback session in session player	**Symptoms:** message: `Could not find session data.`
	Cause: recording has been disabled in connection properties when given session transpired.
	Solution: enable session recording to be able to playback session material in future.

20.5 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.

20.6 Trusted timestamping

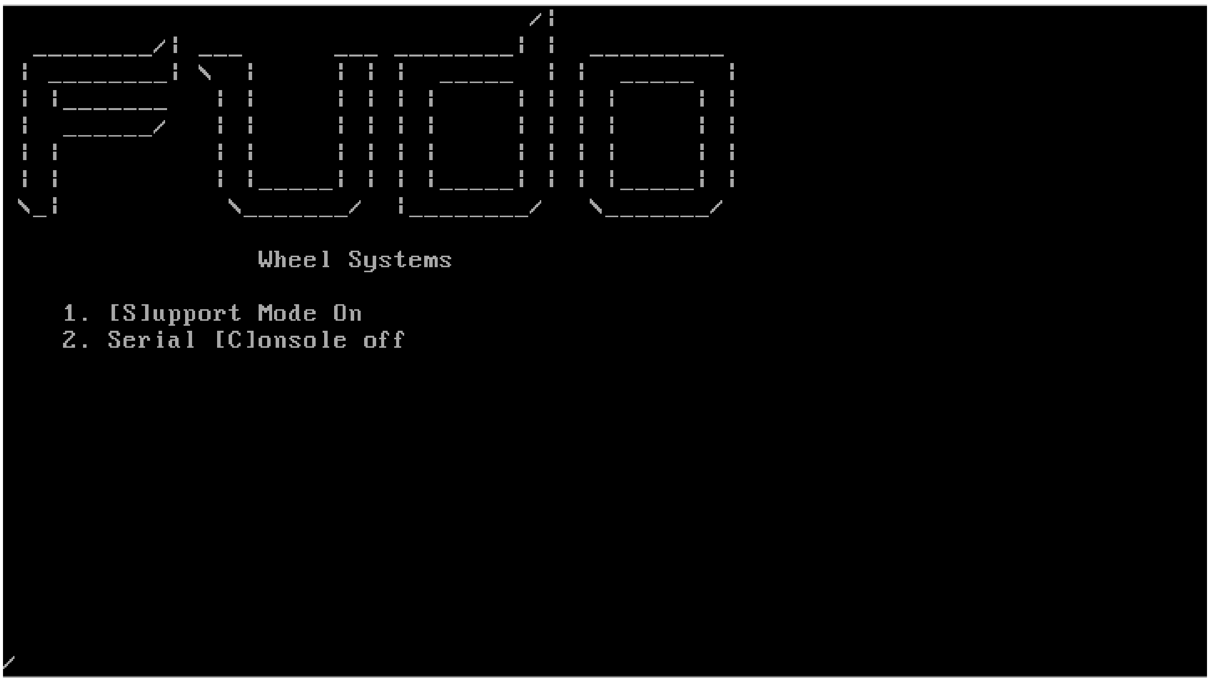
Problem	Symptoms and solution
Session are not timestamped	**Symptoms:** • System log entry: *Timestamping service communication error.*
	Reason: Time-stamping host is not reachable by Fudo.
	Solution: Make sure that firewall settings allow traffic to the time-stamping service server. • PWPW time-stamping service IP address: `193.178.164.5` • KIR time-stamping service IP address: `http://www.ts.kir.com.pl/HttpTspServer`
	Symptoms: • System log entry: *Unable to timestamp session.* • No session timestamp icon 🕒 on sessions list.
	Reason: Time-stamping service misconfiguration.
	Solution: Make sure that time-stamping service has been *configured properly*.

20.7 Support mode

Support mode enables remote access to Fudo PAM in case it cannot boot up properly.

Enabling support mode

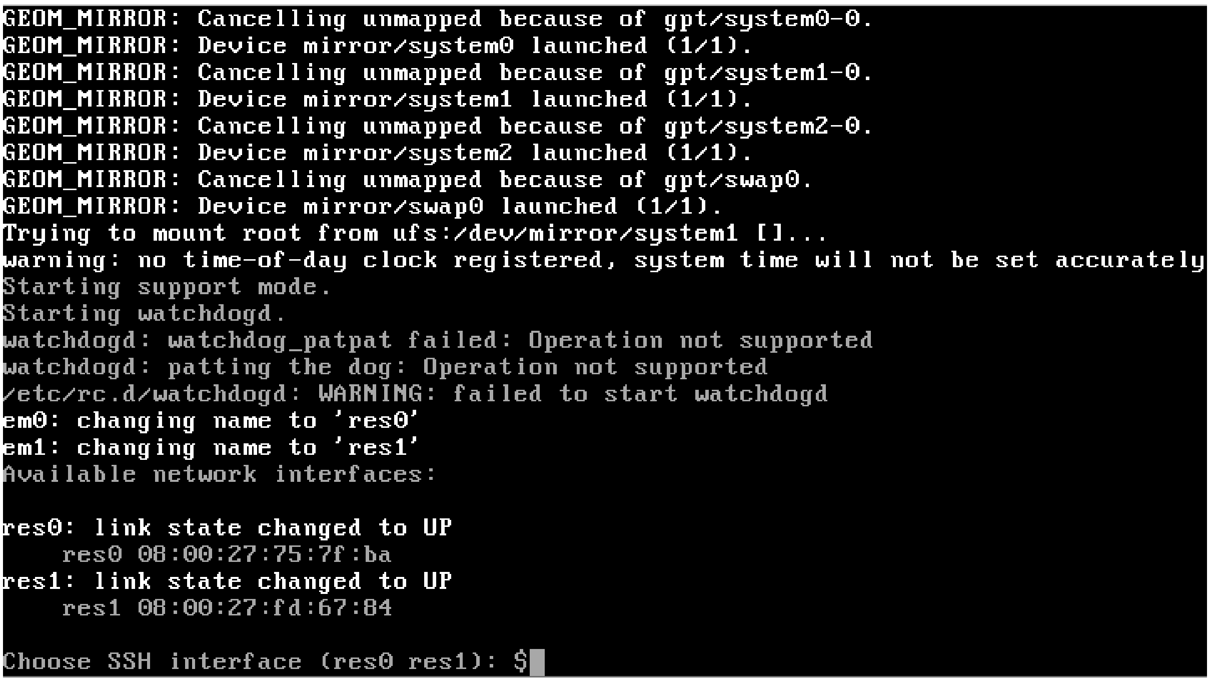
1. Access the system terminal.
2. During the boot up, enter `1` and press the *Enter* key to confirm.



```
                 Wheel Systems

    1. [S]upport Mode On
    2. Serial [C]onsole off
```

3. Select network interface.

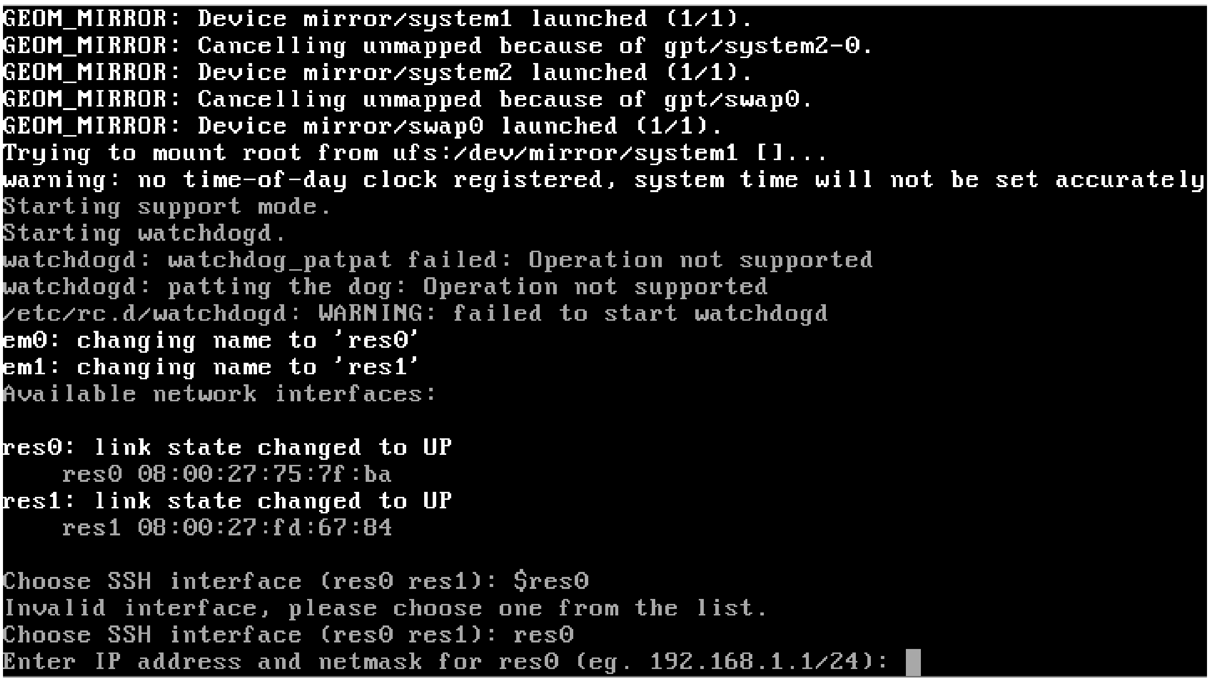
Note: In support mode, network interfaces are named `res*` instead of `net*`.



```
GEOM_MIRROR: Cancelling unmapped because of gpt/system0-0.
GEOM_MIRROR: Device mirror/system0 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/system1-0.
GEOM_MIRROR: Device mirror/system1 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/system2-0.
GEOM_MIRROR: Device mirror/system2 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/swap0.
GEOM_MIRROR: Device mirror/swap0 launched (1/1).
Trying to mount root from ufs:/dev/mirror/system1 []...
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $
```

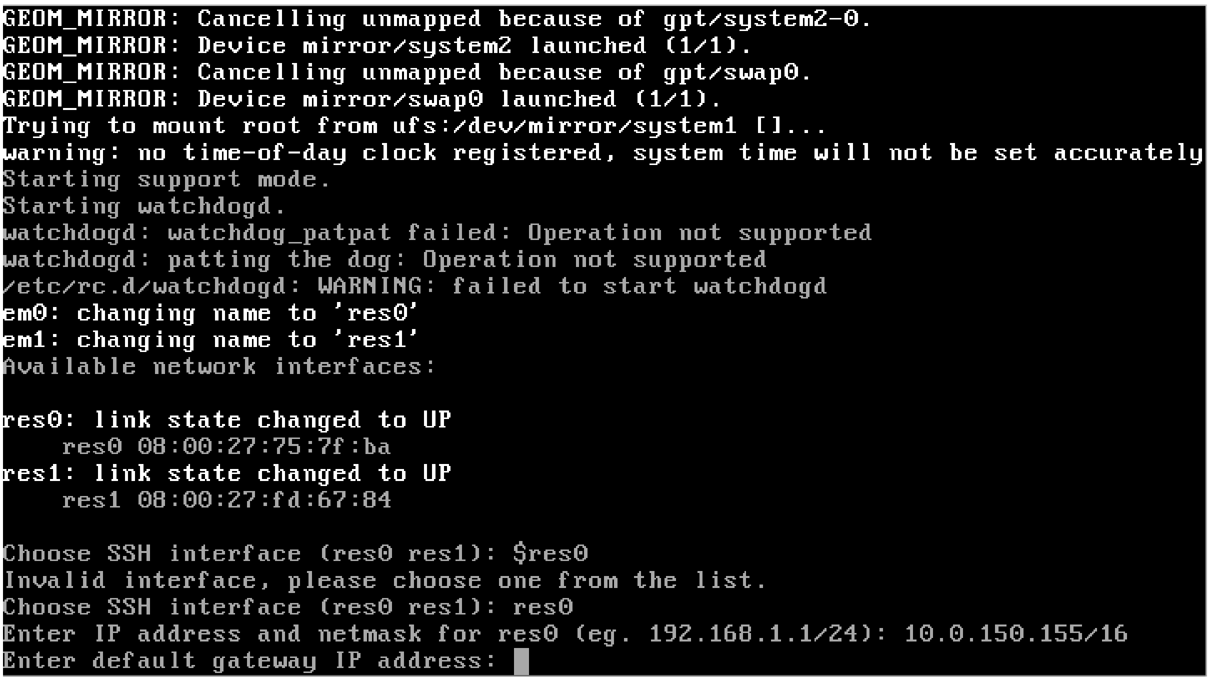
4. Enter the IP address along with network mask, eg. `10.0.0.8/16`.

Note: The IP address is used for establishing remote SSH connection, thus it must be reachable by the technical support specialist. If possible, the IP address should be the same as before the system's malfunction.



```
GEOM_MIRROR: Device mirror/system1 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/system2-0.
GEOM_MIRROR: Device mirror/system2 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/swap0.
GEOM_MIRROR: Device mirror/swap0 launched (1/1).
Trying to mount root from ufs:/dev/mirror/system1 []...
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24):
```

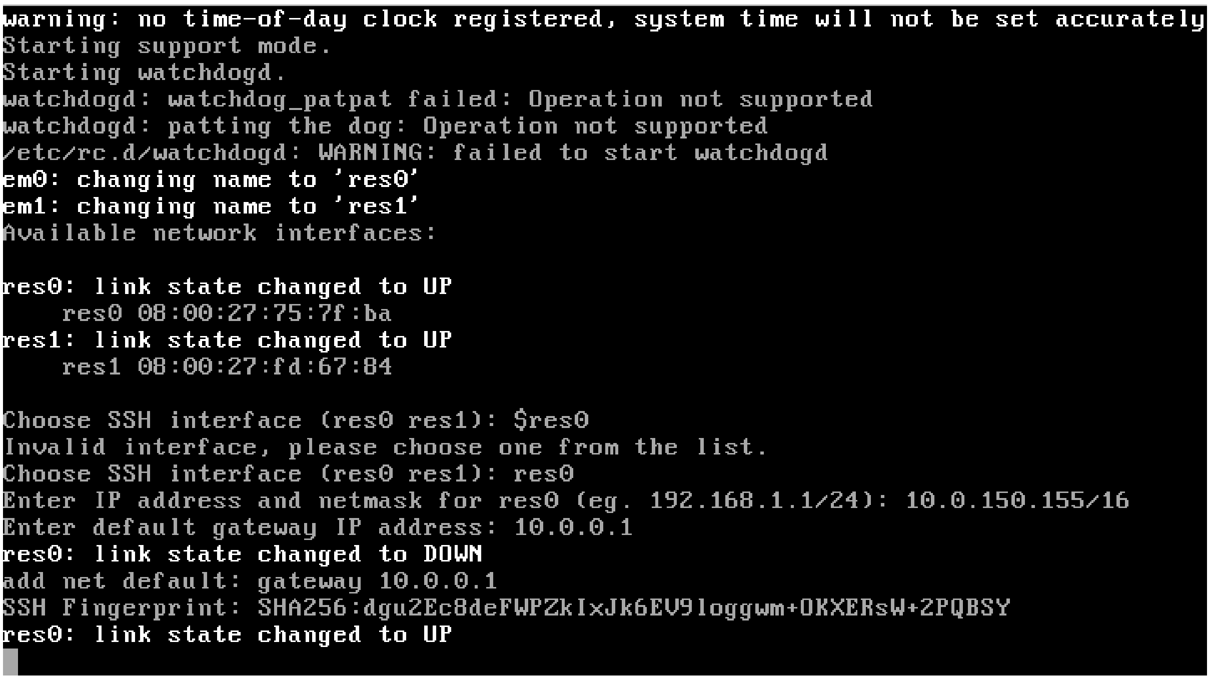
5. Enter the gateway's IP address and press enter to enable connection to your Fudo PAM.



```
GEOM_MIRROR: Cancelling unmapped because of gpt/system2-0.
GEOM_MIRROR: Device mirror/system2 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/swap0.
GEOM_MIRROR: Device mirror/swap0 launched (1/1).
Trying to mount root from ufs:/dev/mirror/system1 []...
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24): 10.0.150.155/16
Enter default gateway IP address:
```

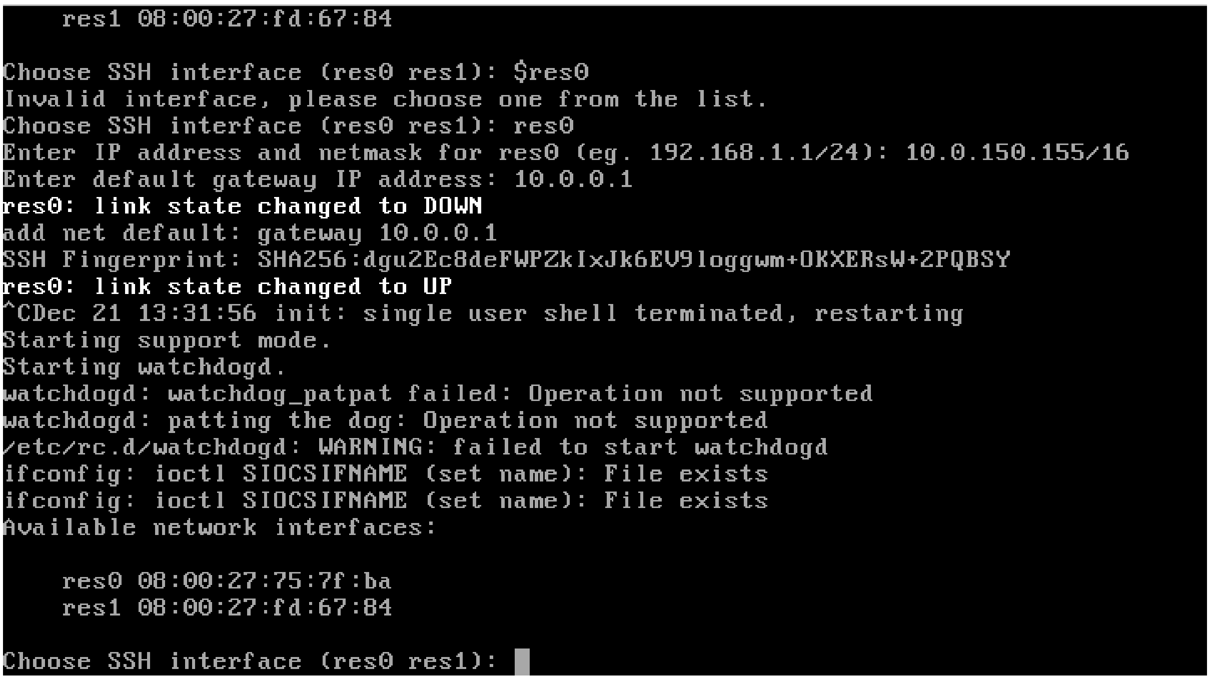
Note:

- Fingerprint allows for verifying that the connection has been established with the correct remote host.



```
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24): 10.0.150.155/16
Enter default gateway IP address: 10.0.0.1
res0: link state changed to DOWN
add net default: gateway 10.0.0.1
SSH Fingerprint: SHA256:dgu2Ec8deFWPZkIxJk6EV9loggwm+OKXERsW+2PQBSY
res0: link state changed to UP
```

6. Once the work is done and the connection is no longer needed, press `[Ctrl]` + `C` keys to close it and reset the network settings.



```
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24): 10.0.150.155/16
Enter default gateway IP address: 10.0.0.1
res0: link state changed to DOWN
add net default: gateway 10.0.0.1
SSH Fingerprint: SHA256:dgu2Ec8deFWPZkIxJk6EV9loggwm+OKXERsW+2PQBSY
res0: link state changed to UP
^CDec 21 13:31:56 init: single user shell terminated, restarting
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
ifconfig: ioctl SIOCSIFNAME (set name): File exists
ifconfig: ioctl SIOCSIFNAME (set name): File exists
Available network interfaces:

    res0 08:00:27:75:7f:ba
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1):
```

Related topics:

- *Network interfaces configuration*
- *System maintenance*

CHAPTER 21

Frequently asked questions

1. How many user sessions can be stored on at once?

2. How 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 Fudo PAM?

5. How to determine unauthorized access attempts to supervised servers?

6. Is it possible to hide the login screen when connecting over the RDP protocol?

7. Why the users list in the connection's properties is incomplete?

8. Why is a user removed from the LDAP/AD server still present on the users list?

9. How frequently are users' definitions synchronized with an LDAP/AD server?

*10. I see * instead of the keystrokes in the session player. Is it possible to see the actual keyboard input?*

11. Can I deactivate a session URL?

12. What should I do before returning a demonstration unit after testing?

AI session processing

13. How long does it take for the model to learn? How many sessions do I have to record to see results?

14. We have 20 accounts and 20 users in our company - how long will it take to see differences?

15. If I connect to different servers, does Fudo create a separate model for each of them?

16. If I give my login credentials to another person, will the AI detect that someone else has logged in and terminate the session?

17. Session status icon is yellow all the time - what does it mean?

18. Five users use the same account to establish connections - will the system be able to determine who and when has logged in onto the server?

19. How will the system determine that it wasn't me if we all use the same commands?

20. Sessions are not analyzed, why is that?

1. How many user sessions can be stored at once?

Fudo PAM F1000 series is delivered with 24 TB of RAW hard drive space (15.9 TB usable) while the F3000 series appliances come with 96 TB of RAW storage space (59.9 TB usable) dedicated for storing users sessions.

Size of the stored session is determined by user's activity. An hour of recorded connection takes on average:

RDP	218 MB active user session (no activity generates almost no data). Definite session size depends on the screen resolution, color depth and actual user activity.
SSH	41.5 MB active session.

Given that assumptions, internal storage space enables recording of:

	RDP	SSH
F1000	28.6 years	150.2 years
F3000	112.8 years	592.5 years

Note:

- Disk usage figures include space taken up by the filesystem's redundancy mechanism. The filesystem reserves a portion of available storage, which results in some of the storage space being reported as used on a newly initiated system.
- Fudo 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 Fudo PAM supports sessions archiving?

All sessions are stored on Fudo PAM internal storage space. In addition to that, 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 the Fudo PAM?

In case of the SSH protocol, 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 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 login screen when connecting over the RDP protocol?

Hiding the 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 users list?

Deleting a user object from an AD or an LDAP server requires performing the full synchronization to reflect those changes on 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.

12. What should I do before returning a demonstration unit after testing?

After testing Fudo, you should delete all session and configuration data by *resetting configuration to default settings* and erase the flash drive with the encryption key.

13. How long does it take for the model to learn? How many sessions do I have to record to see results?

Models are trained as scheduled in the *AI system settings*.

- For the SSH model the minimum are 65 sessions (with at least 25 different commands) and 5 unique predictors (e.g. users). Optimal results require 300 sessions per predictor (e.g. user) and 10 unique predictors (e.g. users).
- For the RDP model, the minimum are 5 hours of session recordings per predictor (e.g. user). Optimal results require 30 hors of session recordings and 10 unique predictors (e.g. users).

14. We have 20 accounts and 20 users in our company - how long will it take to see differences?

This solely depends on the availability of session data. If there is enough session information available to build models, you can expect model to be trained the next day after first predictor session is recorded.

- For SSH model the minimum are 65 sessions (with at least 25 different commands) and 5 unique predictors (e.g. users). Optimal results require 300 sessions per predictor (e.g. user) and 10 unique predictors (e.g. users).
- For RDP model, the minimum are 5 hours of session recordings per predictor (e.g. user). Optimal results require 30 hours of session recordings and 10 unique predictors (e.g. users).

15. If I connect to different servers, does Fudo create a separate model for each of them?

Fudo creates and maintains one RDP and one SSH model for a single user.

16. If I give my login credentials to another person, will the AI detect that someone else has logged in and terminate the session?

Fudo PAM will detect that someone else has logged in and will set the session risk status to high, but it will not terminate the session.

17. Session status icon is yellow all the time - what does it mean?

Yellow color indicates that the model could not determine whether the session poses a threat or not. Under normal circumstances, these sessions should be considered as non-threatening. But if you suspect there has been a security incident, these sessions should be reviewed.

18. Five users use the same account to establish connections - will the system be able to determine who and when has logged in onto the server?

Users must have individual accounts created on Fudo PAM so it can correctly determine if an account security has been breached.

19. How will the system determine that it wasn't me if we all use the same commands?

Every user runs the same commands differently. E.g. one user will execute `ls -la` and another will run `ls -al`. Combination of such subtle differences allows for determining a if the currently logged in user matches the profile.

20. Sessions are not analyzed, why is that?

In order for a session to be analyzed, there must be a matching model available. Also, session has to meet volumetric requirements - it must be long enough and carry enough information. Refer to *AI sessions processing* for more information.

CHAPTER 22

Glossary

AAPM AAPM (Application to Application Password Manager) module enables secure password exchange between applications.

account

accounts Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); password changing policy as well as the password changer itself.

Active Directory Users authorization and authentication in Windows domain.

AD Active Directory - users authorization and authentication in Windows domain.

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.

ARP Address Resolution Protocol - protocol used for mapping Internet layer addresses (IP addresses) to the physical - link layer addresses (MAC addresses).

CERB Complete user authentication and authorization solution, supporting different authentication methods i.e., mobile token (mobile phone application), static password, SMS one-time passwords, etc.

CIDR Short notation of network addressing, in which the IP address is written according to the IPv4 standard, and the subnet mask is provided as a number of *1* in the subnet mask in binary system (192.168.1.1 - 255.255.255.0; 192.168.1.1/24).

data retention Data retention mechanism automatically deletes session data after define time period transpires.

DHCP Mechanism for dynamic IP addressing management i LAN networks.

DNS Domain Name Server - name server service which maps IP addresses to hosts names which are easier to remember.

DUO is a mobile application that works with Duo Security's two-factor authentication service. The application generates passcodes for login and can receive push notifications for authentication.

Efficiency Analyzer Efficiency Analyzer module delivers statistical information on users' activity.

external authentication server Server storing user data used for verification of user login credentials when connecting to Fudo PAM or the monitored server.

Fingerprint Characters string being a result of a hash function on input data, allowing to determine if the input data has been altered.

fudopv AAPM module script, installed on the server, which enables secure password exchange between applications.

heartbeat Network packet used for informing other cluster nodes about machine's current state. If a cluster node does not receive a heartbeat packet in a given timeframe, it will take over the master node role and will start processing users' requests.

hot-swap Hot-swap mechanism enables replacing hardware components without the necessity to turn the system off.

LDAP Lightweight Directory Access Protocol - distributed catalog services management and access protocol in IP networks.

listener Listener determines server connection mode (proxy, gateway, transparent, bastion) as well as its specifics.

OATH Open Authentication - open standard enabling implementation of strong, two-factor user and devices authentication.

OCR Optical Character Recognition - image processing for identifying and indexing text.

password changer Tool which enables facilitating automated password changing on a server.

passwords repository Passwords repository manages password to privileged accounts on monitored hosts.

policy Mechanism which enables defining patterns which in case of being detected will trigger defined actions.

PSM (Privileged Session Management) PSM module is used for recording remote access sessions.

PSM PSM (Privileged Session Monitoring) module enables monitoring and recording remote access sessions.

Public key Authentication method which uses a pair of keys - private (held only by the user) and public (publicly available) to determine user's identity.

RADIUS Remote Authentication Dial In User Service - networking protocol used to control access to different services within IT infrastructure.

RDP Remote Desktop Protocol - remote access protocol to computer systems running Microsoft operating system.

RDP connections broker Remote sessions management mechanism for server farms.

redundancy group Defined group of IP addresses, which in case of a system failure, will be seamlessly carried over to another cluster node to maintain the availability of the services.

safe Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

server

servers Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

shared session User session which was joined by another user.

SMS is a text messaging service component of most telephone, and mobile device systems.

SSH Secure Shell - networking protocol for secure communication with remote systems.

SSH access Service access to Fudo PAM over SSH protocol.

Static password Basic user authorization method which uses login and password combination to determine users's identity.

Syslog Events logging standard in computer systems. Syslog server collects and stores log data from networked devices, which can be later used for analysis and reporting.

time policy Time policy mechanism enables defining time periods during which users are allowed to connect to monitored hosts.

timestamp Session data hash value, which enables verifying that the data has not been modified.

user User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

VLAN Virtual networks mechanism, enabling separation of broadcast domains.

VNC Remote access protocol to graphical user interfaces.

WWN World Wide Name - unique object identifier in external storage solutions.

Index