Fudo Enterprise 5.3 - System Documentation

Fudo Security

December 13, 2024

Contents

CHAPTER 1

About documentation

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

Documentation Structure

1. About documentation

This chapter provides information about the documentation.

2. Layout themes of the Admin Panel

This chapter provides information on how to change layout themes for the Fudo Enterprise's Admin Panel.

3. Introduction

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

4. System deployment

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

5. Quick start

This chapter contains typical configuration examples.

6. Users

This chapter covers users management topics.

7. Servers

This chapter covers servers management topics.

8. Pools

This chapter covers pools management topics.

9. Remote applications

This chapter covers remote applications management topics.

10. Accounts

This chapter covers accounts management topics.

11. Listeners

This chapter covers listeners management topics.

12. Safes

This chapter covers safes management topics.

13. Discovery

This chapter covers the Discovery functionality and management topics.

14. Password changers

This chapter contains information on automated password changing feature.

15. Policies

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

16. Account activity in the Access Gateway

This chapter covers the functionality of *Resource in use* option.

17. Access requests

This chapter covers the functionality of granting access to the resources via the request.

18. Sessions

This chapter contains information on stored access sessions.

19. Reports

This chapter contains topics related to generating reports.

20. Productivity

This chapter describes Fudo Enterprise's Productivity Analyzer module.

21. Administration

This chapter contains administration procedures.

22. Reference information

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

23. Fudo Officer 1.0

This chapter describes the Fudo Officer 1.0 application functionality.

24. AAPM (Application to Application Password Manager)

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

25. Ticketing systems

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

26. Client applications

This chapter contains client applications configuration instructions for selected protocols.

27. Troubleshooting

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

28. Frequently asked questions

This chapter contains frequently requested information about Fudo Enterprise.

29. 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

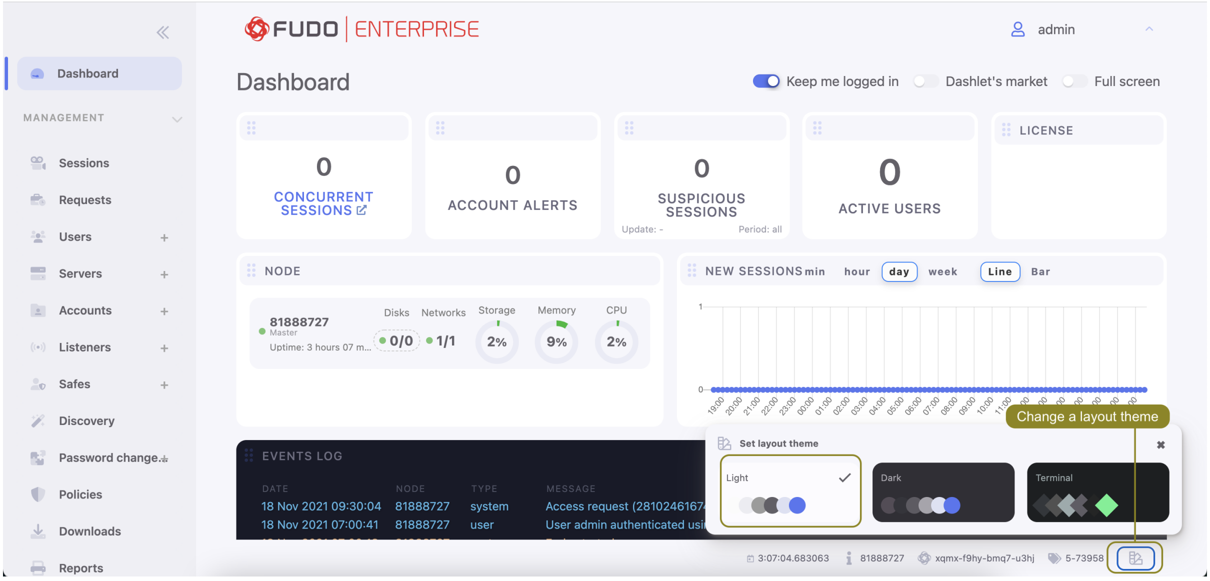
All trademarks, product names, and company names or logos cited in this document are the property of their respective owners and are used for information purpose only.

CHAPTER 2

Layout themes of the Admin Panel

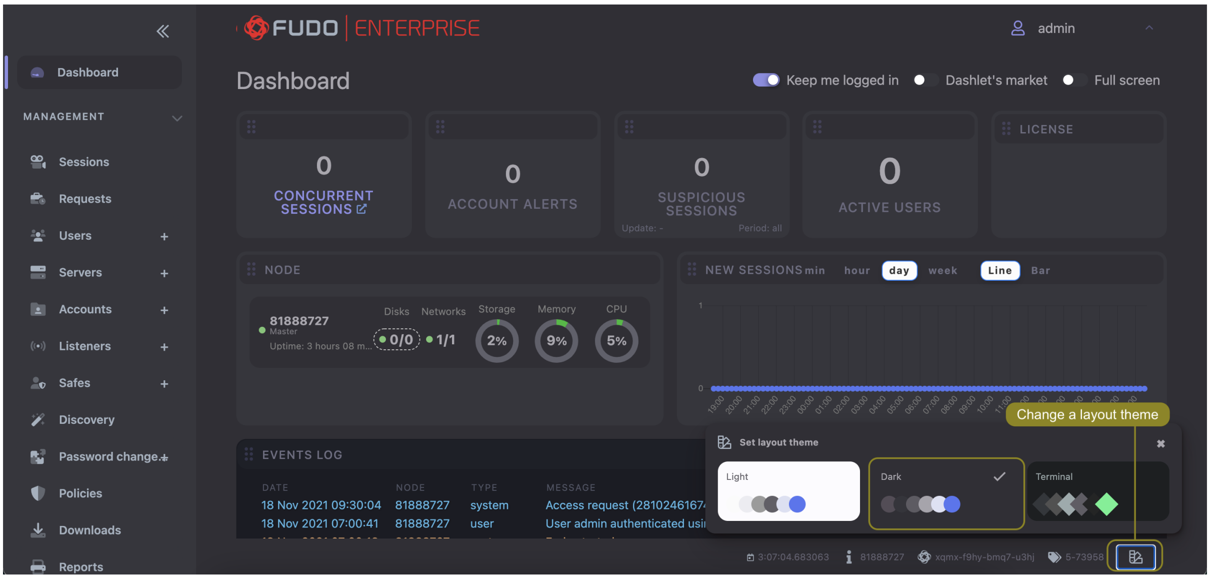
There are three layout themes available to choose for the Admin Panel. Click the icon in the lower right corner of the screen to access the list of variants.

Light theme:



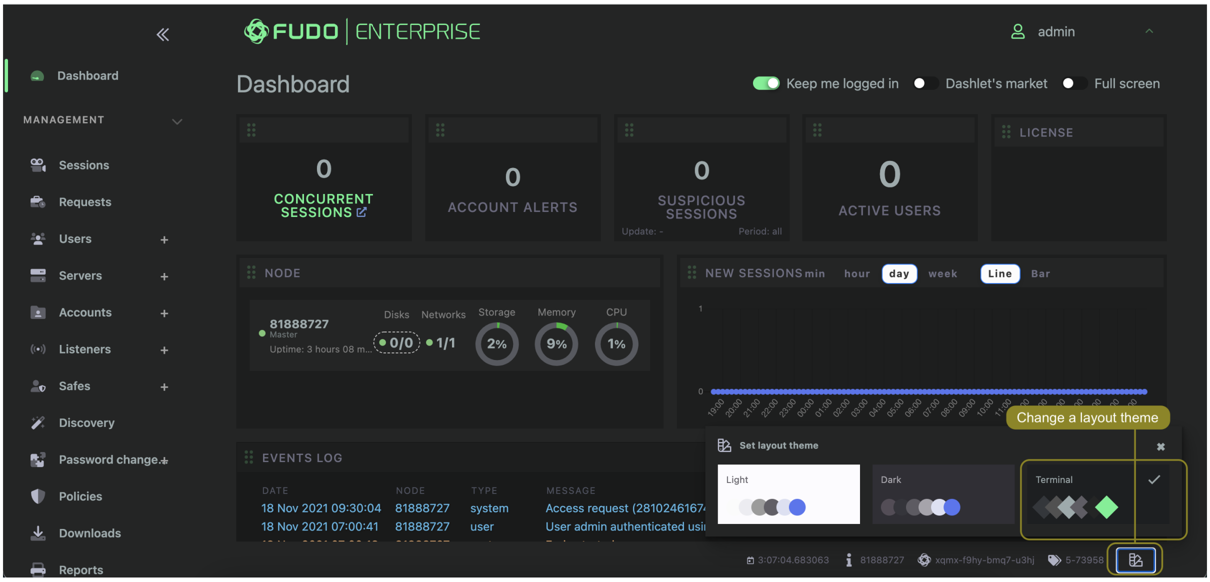
DATE	NODE	TYPE	MESSAGE
18 Nov 2021 09:30:04	81888727	system	Access request (2810246167
18 Nov 2021 07:00:41	81888727	user	User admin authenticated usi

Dark theme:



DATE	NODE	TYPE	MESSAGE
18 Nov 2021 09:30:04	81888727	system	Access request (28102461674
18 Nov 2021 07:00:41	81888727	user	User admin authenticated usi

Terminal theme:



DATE	NODE	TYPE	MESSAGE
18 Nov 2021 09:30:04	81888727	system	Access request (28102461674
18 Nov 2021 07:00:41	81888727	user	User admin authenticated usi

Related topics:

- *Introduction*

CHAPTER 3

Introduction

3.1 System overview

Fudo Enterprise is a complete solution for managing remote privileged access. Fudo Enterprise includes a range of features, each dedicated to different aspects of remote access management:

- *Session Monitoring & Recording*
- *Secret Management*
- *Just-in-Time (JIT) Access*
- *Single Sign-On (SSO)*
- *Agentless Convenient Access*
- *AI-Powered Prevention*
- *Productivity Analyzer*
- *Rapid Deployment*
- *Compliance Support*

3.1.1 Session Monitoring & Recording

Fudo Enterprise provides administrators with advanced tools to monitor and manage sessions in real-time. Administrators can join, share, pause, or terminate sessions, ensuring swift action in response to potentially suspicious activities.

The platform supports resource sharing over 10+ protocols, including RDP, SSH, and HTTPS, enabling secure access to critical systems. Fudo Enterprise records complete network traffic along with meta data, enabling precise session playback and full-text content search. This functionality provides a comprehensive audit trail to enhance security and ensure compliance.

Fudo Enterprise acts as a proxy between users and monitored servers and it registers users' actions, including mouse pointer moves, keystrokes and transferred files.

Data stored on Fudo can be timestamped which makes session material a more reliable evidence in court.

Fudo Enterprise session monitoring module supports following system configurations:

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

3.1.2 Secret Management

Fudo Enterprise provides a secure and flexible system for managing privileged account credentials. Credentials are stored securely and never leave the system, ensuring robust protection.

Administrators can utilize predefined templates to quickly set up password changers within minutes. These password changers operate on a separate transport layer, such as SSH, LDAP, Telnet, or WinRM, allowing integration with various systems.

Fudo Enterprise supports password changing on following systems:

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

Beyond the built-in examples, custom scripts can be created to enhance functionality, offering precise control over credential management on monitored servers. For more information, refer to the *Password changers* section.

3.1.3 Just-in-Time (JIT) Access

Fudo Enterprise supports Just-in-Time (JIT) access workflows, enabling organizations to implement a Zero-Trust security approach. Through the *request management* section, administrators can define and schedule specific time windows for resource availability, granting access only when necessary. This ensures adherence to the zero-standing-privileges principle, minimizing security risks by limiting prolonged access to critical systems.

3.1.4 Single Sign-On (SSO)

Fudo Enterprise provides Single Sign-On (SSO) functionality for both the Admin Panel and the User Access Gateway. SSO streamlines authentication by automatically logging users into the system, enhancing usability and efficiency while maintaining robust security standards.

3.1.5 Agentless Convenient Access

Fudo Enterprise offers flexible and agentless access to resources, allowing users to choose their preferred method of connection. Users can continue using their favorite native clients for a seamless experience or take advantage of the built-in, browser-based Webclient provided by Fudo Enterprise. This flexibility ensures ease of use for both technical and non-technical users alike.

3.1.6 AI-Powered Prevention

Fudo Enterprise incorporates *AI-driven capabilities* to assist in daily security management tasks. The system provides actionable guidelines to support verification and monitoring processes, simplifying the responsibilities of security teams and CISOs. By analyzing behavioral and semantic patterns, Fudo Enterprise detects potential credential compromises and sends notifications, enabling swift response to mitigate risks and enhance overall security posture.

3.1.7 Productivity Analyzer

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

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

3.1.8 Rapid Deployment

Fudo Enterprise is designed as an all-in-one solution, eliminating the need for additional software or hidden costs to initiate your instance. Whether deployed as an appliance or a virtual machine, all necessary components are included within the core system. This streamlined approach ensures a quick and efficient installation process, enabling full deployment in as little as one day.

3.1.9 Compliance Support

Fudo Enterprise is designed to help organizations meet a wide range of compliance requirements, including PCI-DSS, SOX, HIPAA, NIST, GDPR, and ISA/IEC 62443. By providing robust security and auditing features, Fudo Enterprise ensures adherence to industry standards and regulatory frameworks, simplifying compliance management for your organization.

Related topics:

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

3.2 Available GUI Languages

The Fudo Enterprise interface is offered in the following languages:

- English
- Polish
- Ukrainian
- Russian
- Kazakh

Related topics:

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

3.3 Supported protocols

3.3.1 HTTP

Supported connection modes:

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

Supported OCR languages for the rendered HTTP session:

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

Supported algorithms when TLS encryption selected and the option *Legacy ciphers* disabled:

- `ecdhe-ecdsa-aes256-gcm-sha384`
- `ecdhe-rsa-aes256-gcm-sha384`
- `ecdhe-ecdsa-chacha20-poly1305`
- `ecdhe-rsa-chacha20-poly1305`
- `ecdhe-ecdsa-aes256-sha384`

- `dhe-rsa-aes256-gcm-sha384`

Notes:

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

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

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

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

Additionally, in the non-rendered mode:

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

Additionally, in the rendered mode:

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

3.3.2 Modbus

Supported connection modes:

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

Notes:

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

3.3.3 MS SQL (TDS)

Due to the fact that MS SQL Studio may create multiple connections for sending internal queries, the sessions, connected via the TDS layer protocol using MS SQL Studio are getting aggregated by Fudo Enterprise.

Fudo Enterprise follows an algorithm that verifies if there is an already connected session on a current node. If the algorithm identifies that the main connection objects (`listener`, `account`, `server address (server)`, `user`, and `safe`) of the new session are correlating with already existing session, both sessions are aggregated into one.

If the main connection objects of the new session are not correlating with any of already existing sessions, a new session is created.

This makes multiple queries to be grouped within one session. Every query has a unique tag that allows filtering important connections with users' queries in the Fudo Enterprise player.

Supported connection modes:

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

Supported client applications:

- SQL Server Management Studio,
- sqsh.

Notes:

- Session joining is not supported.

3.3.4 MySQL

Supported connection modes:

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

Supported client applications:

- Official MySQL client,
- PyMySQL libraries for Python.

Notes:

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

3.3.5 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

Supported algorithms

- when TLS encryption selected and the option *Legacy ciphers* is disabled:
  - `TLS_AES_256_GCM_SHA384`
  - `TLS_CHACHA20_POLY1305_SHA256`
  - `TLS_AES_128_GCM_SHA256`
  - `ECDHE-ECDSA-CHACHA20-POLY1305`
  - `ECDHE-RSA-CHACHA20-POLY1305`
  - `ECDHE-ECDSA-AES256-GCM-SHA384`
  - `ECDHE-RSA-AES256-GCM-SHA384`
  - `ECDHE-ECDSA-AES256-SHA384`
  - `ECDHE-RSA-AES256-SHA384`
  - `DHE-RSA-AES256-GCM-SHA384`
  - `AES256-GCM-SHA384`
  - `AES128-GCM-SHA256`
  - `AES128-SHA256`
- when TLS encryption selected and the option *Legacy ciphers* is enabled:
  - `TLS_AES_256_GCM_SHA384`

  - `TLS_CHACHA20_POLY1305_SHA256`
  - `TLS_AES_128_GCM_SHA256`
  - `ECDHE-ECDSA-AES256-GCM-SHA384`
  - `ECDHE-RSA-AES256-GCM-SHA384`
  - `DHE-RSA-AES256-GCM-SHA384`
  - `ECDHE-ECDSA-CHACHA20-POLY1305`
  - `ECDHE-RSA-CHACHA20-POLY1305`
  - `DHE-RSA-CHACHA20-POLY1305`
  - `ECDHE-ECDSA-AES128-GCM-SHA256`
  - `ECDHE-RSA-AES128-GCM-SHA256`
  - `DHE-RSA-AES128-GCM-SHA256`
  - `ECDHE-ECDSA-AES256-SHA384`
  - `ECDHE-RSA-AES256-SHA384`
  - `DHE-RSA-AES256-SHA256`
  - `ECDHE-ECDSA-AES128-SHA256`
  - `ECDHE-RSA-AES128-SHA256`
  - `DHE-RSA-AES128-SHA256`
  - `ECDHE-ECDSA-AES256-SHA`
  - `ECDHE-RSA-AES256-SHA`
  - `DHE-RSA-AES256-SHA`
  - `ECDHE-ECDSA-AES128-SHA`
  - `ECDHE-RSA-AES128-SHA`
  - `DHE-RSA-AES128-SHA`
  - `AES256-GCM-SHA384`
  - `AES128-GCM-SHA256`
  - `AES256-SHA256`
  - `AES128-SHA256`
  - `AES256-SHA`
  - `AES128-SHA`

Notes:

- RDP protocol implementation supports user authentication over RADIUS in challenge-response mode.
- For RDP servers are supported NLA mode and TLS mode.
- For RDP listeners, besides the standard security level, the *Enhanced RDP Security with TLS* option is supported.

- In case the *NLA* option enabled, Fudo Enterprise requires NTLM protocol version 2 or newer. To properly handle NLA authentication connections, enable option to only send NTLMv2 response both on client and server side.
    1. Click *Start* > *All Programs* > *Accessories* > *Run*.
    2. Type `secpol.msc` in the *Open* input field and click *OK*.
    3. Select *Local Policies* > *Security Options* and double-click *Network Security: LAN Manager authentication level*.
    4. Select *Send NTLMv2 response only. Refuse LM & NTLM* from the drop-down list.
    5. Click *Apply*.
- Fudo Enterprise verifies input language settings when negotiation connection and does not support dynamic language change on the login screen.

RemoteApp

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

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

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

3.3.6 SSH

Supported connection modes:

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

Supported features:

- Connections multiplexing (video export, session termination, pause, join, playback, raw data),
- SCP (raw data, session termination, extracting separate files),
- SFTP,
- 2FA,
- Port redirection (video export, session termination, pause, session join, playback, raw data),
- SSH Agent forwarding (transparent, not recorded),
- X11 - within SSH protocol (video export, session termination, pause, session join, playback, raw data),
- Shell (video export, session termination, pause, session join, playback, raw data),

- Terminal (video export, session termination, pause, session join, playback, raw data).

Supported encryption algorithms:

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

Supported hashing algorithms:

- MD5
- SHA256

Supported types of SSH keys:

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

Supported encoding: UTF-8

Supported ciphers:

- Supported *key exchange* algorithms:
  - `curve25519-sha256`
  - `curve25519-sha256@libssh.org`
  - `ecdh-sha2-nistp256`
  - `ecdh-sha2-nistp384`
  - `ecdh-sha2-nistp521`
  - `diffie-hellman-group-exchange-sha256`
  - `diffie-hellman-group16-sha512`
  - `diffie-hellman-group18-sha512`
  - `diffie-hellman-group14-sha256`
- additionally, there are 3 more *key exchange* algorithms supported when the *Legacy ciphers* option is enabled:
  - `diffie-hellman-group14-sha1`
  - `diffie-hellman-group1-sha1`
  - `diffie-hellman-group-exchange-sha1`
- Supported *host key* algorithms:
  - `ecdsa-sha2-nistp256-cert-v01@openssh.com`
  - `ecdsa-sha2-nistp384-cert-v01@openssh.com`
  - `ecdsa-sha2-nistp521-cert-v01@openssh.com`
  - `ssh-ed25519-cert-v01@openssh.com`
  - `rsa-sha2-512-cert-v01@openssh.com`

- rsa-sha2-256-cert-v01@openssh.com
- ssh-rsa-cert-v01@openssh.com
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519
- rsa-sha2-512
- rsa-sha2-256
- ssh-rsa

- plus, there are 2 more *host key* algorithms supported when the *Legacy ciphers* option is enabled:
  - ssh-dss
  - ssh-dss-cert-v01@openssh.com
- Supported *encryption* algorithms:
  - chacha20-poly1305@openssh.com
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - aes128-gcm@openssh.com
  - aes256-gcm@openssh.com
- additionally, there are 10 more *encryption* algorithms supported when the *Legacy ciphers* option is enabled:
  - aes128-cbc
  - aes192-cbc
  - aes256-cbc
  - rijndael-cbc@lysator.liu.se
  - 3des-cbc
  - arcfour256
  - arcfour128
  - arcfour
  - blowfish-cbc
  - cast128-cbc
- Supported *MAC* algorithms:
  - umac-64-etm@openssh.com
  - umac-128-etm@openssh.com

  - `hmac-sha2-256-etm@openssh.com`
  - `hmac-sha2-512-etm@openssh.com`
  - `umac-64@openssh.com`
  - `umac-128@openssh.com`
  - `hmac-sha2-256`
  - `hmac-sha2-512`

- plus, there are 11 more *MAC* algorithms supported when the *Legacy ciphers* option is enabled:
  - `hmac-sha1`
  - `hmac-sha1-etm@openssh.com`
  - `hmac-sha1-96-etm@openssh.com`
  - `hmac-sha1-96`
  - `hmac-ripemd160`
  - `hmac-ripemd160@openssh.com`
  - `hmac-ripemd160-etm@openssh.com`
  - `hmac-md5`
  - `hmac-md5-96`
  - `hmac-md5-etm@openssh.com`
  - `hmac-md5-96-etm@openssh.com`

Notes:

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

3.3.7 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.

3.3.8 Telnet 5250

Supported connection modes:

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

Supported client applications:

- IBM Personal Communications,
- tn5250.

Notes:

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

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

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

3.3.9 Telnet

Supported connection modes:

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

Notes:

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

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

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

3.3.10 VNC

Supported connection modes:

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

Suggested client applications:

- TightVNC,
- RealVNC.

Supported OCR languages:

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

Notes:

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

Connection specifics - VNC server requires authentication

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

Connection specifics - server does not require authentication

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

3.3.11 X11

X11 protocol is supported within the SSH protocol.

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

Supported servers:

- Xorg,
- Xming,
- XQuartz.

Supported fonts:

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

3.3.12 TCP

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

Supported connection modes:

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

Notes:

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

3.3.13 Secret Checkout

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

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

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

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

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

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

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

Notes:

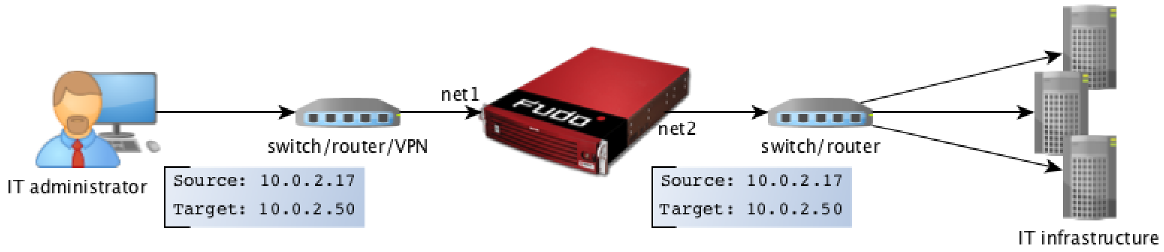
- *Session joining* feature is not supported.
- Playback is not supported.

3.4 Deployment scenarios

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

Bridge

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



```
Source: 10.0.2.17
Target: 10.0.2.50
```

```
Source: 10.0.2.17
Target: 10.0.2.50
```

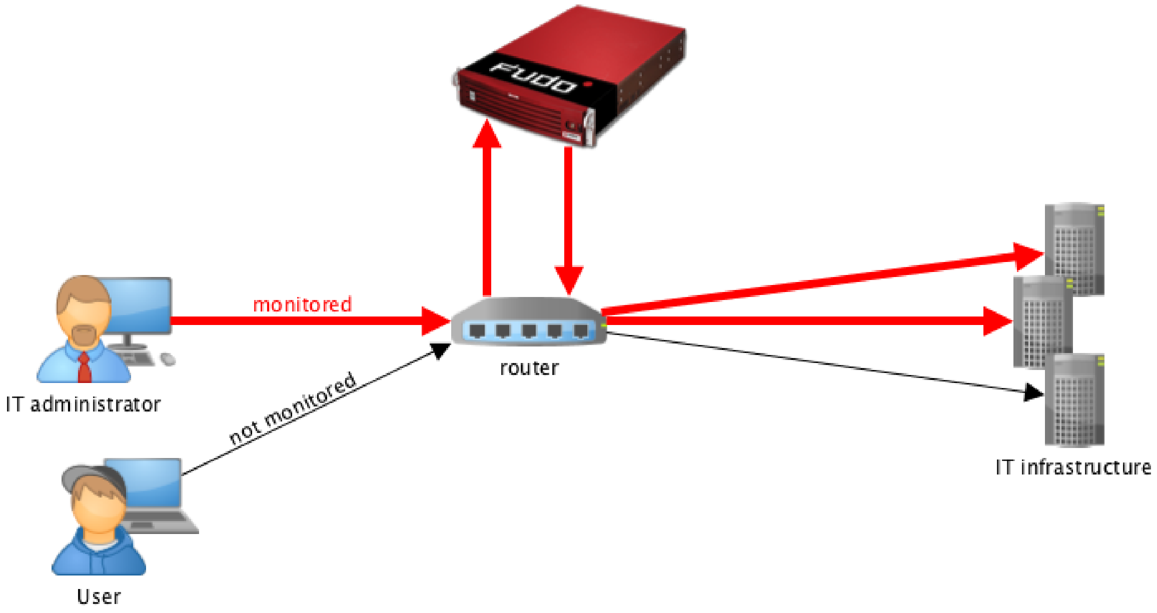
Mediating packages transfer, Fudo Enterprise preserves source IP address when forwarding requests to destination servers.

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

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

Forced routing

Forced routing mode requires using a properly configured router. Such solution allows controlling network traffic in third ISO/OSI network layer, so only administrative requests are routed through Fudo Enterprise and the rest of the traffic is forwarded directly to the destination server.



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

Related topics:

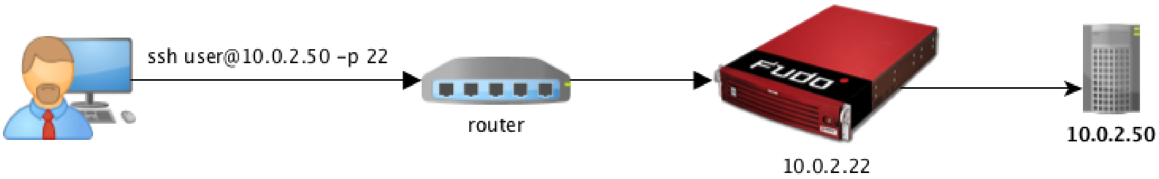
- *Connection modes*
- *Managing servers*
- *User authentication methods and modes*
- *System overview*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*

- *Initial boot up*

3.5 Connection modes

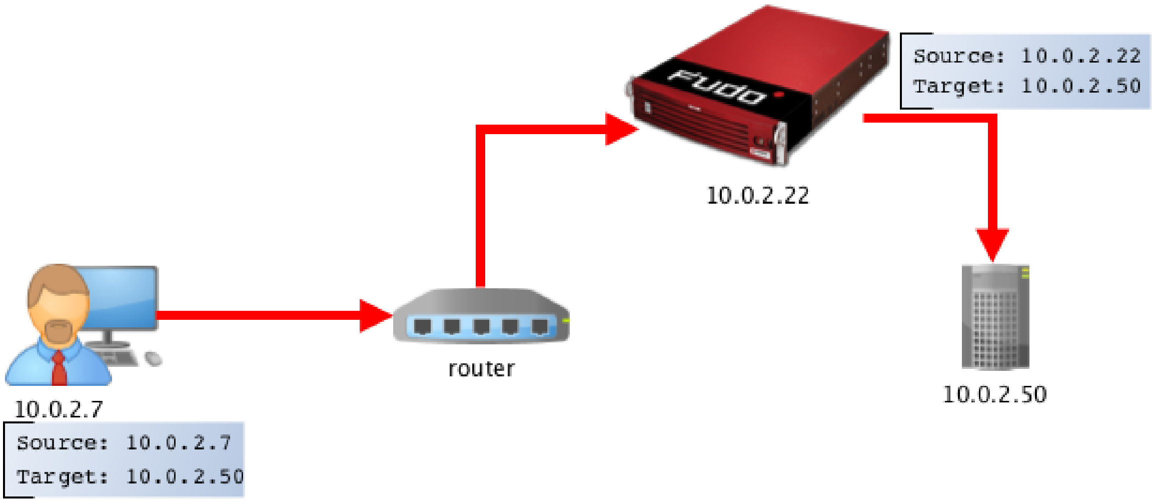
Transparent

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



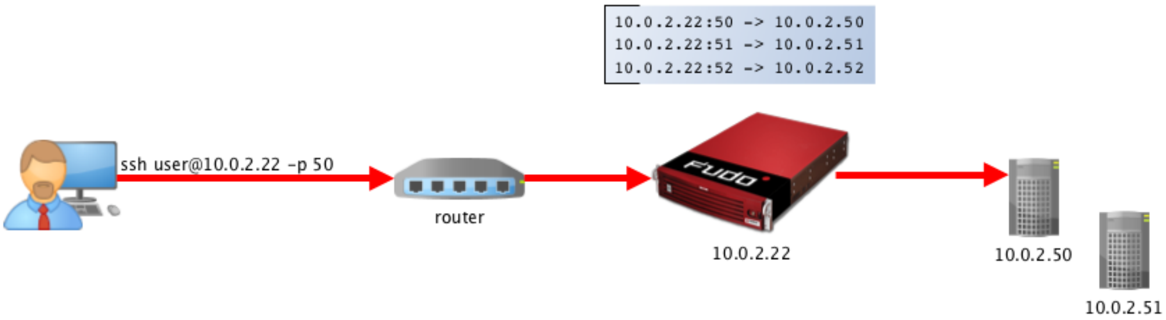
Gateway

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



Proxy

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

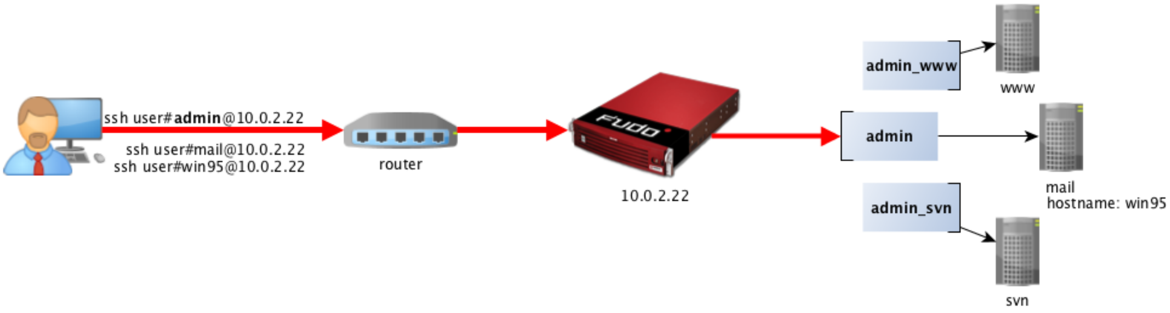


Such approach enables concealing actual IP addressing and allows configuring servers to only accept requests sent from Fudo Enterprise.

Bastion

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

In bastion mode, the target host is specified within the string identifying the user and the server their are trying to connect to, e.g. `ssh -l johndoe#root#example.server.org`. This enables facilitating access to a group of monitored servers through the same IP address and port number combination.



While connecting, the Fudo Enterprise expects:

`<username>[@domain][#<serverlogin>#<address>[:<port>]]`, where:

- `<username>`: User's login on Fudo Enterprise,
- `[@domain]` is optional,
- `<serverlogin>`: user's login on the target server,
- `<address>`: server address on the target server (the `<port>` can be omitted if native for protocol).

Warning: # character in between is required.

Target object string is matched in the following sequence:

1. Exact username - Fudo Enterprise tries to match the string with object defined in the local database.

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

Note: If an account object doesn't have a *login* defined, the Fudo Enterprise system will ask for a *login* while connecting to the target server.

Related topics:

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

3.6 User authentication methods and modes

User authentication methods

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

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

Note:

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

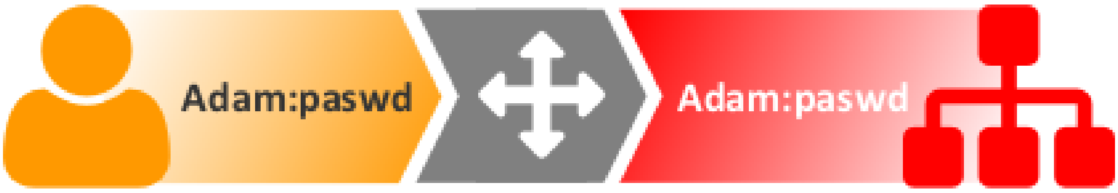
Authentication modes

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

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

Authentication with original login and password

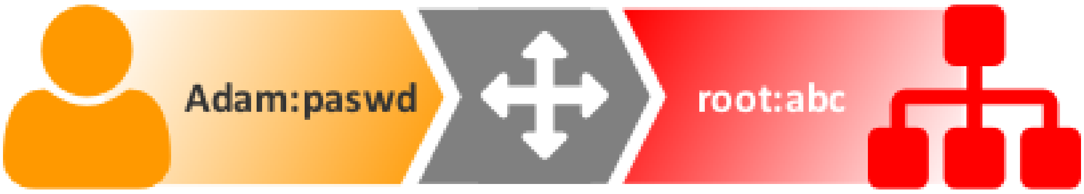
In this authentication mode, Fudo uses login and password provided by the user upon logon to authenticate the user on the target system.



Authentication with login and password substitution

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

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



Note:

- The password to the target system can be either explicitly defined in the *account* or can be obtained from internal or external password vault upon each access request. For more information, refer to the *Password changers* and *External passwords repositories* topics.

- Due to specifics of VNC protocol, which authenticates the user using password only, the login entered as the substitution string is ignored when establishing a VNC connection.

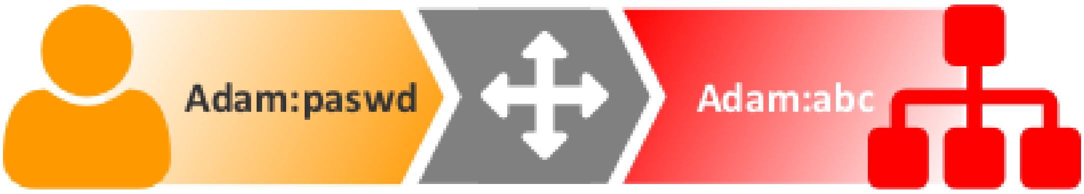
Note: In case of Oracle database, the user password and the privileged account password must be both either shorter than 16 characters or 16-32 characters long.

Two-fold authentication

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

Authentication with password substitution

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



Note:

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

Authentication by target server

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

Administrator approved access

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

Related topics:

- *Creating a safe*
- *Approving pending user requests*

- *Declining pending requests*
- *System overview*
- *External authentication servers configuration*
- *Security measures*

3.7 Security measures

3.7.1 Data encryption

Data stored on Fudo Enterprise is encrypted with AES-XTS algorithm using 256 bit encryption keys. AES-XTS algorithm is most effective hard drive encryption solution.

Appliance

Encryption keys are stored on two USB flash drives. Flash drives delivered with Fudo Enterprise are uninitialized. Keys initialization takes place during initial system boot-up, during which both flash drives have to be connected (initiation procedure is described in chapter *System initiation*).

After encryption keys have been initiated and Fudo Enterprise has booted up, both USB flash drives can be removed and placed somewhere safe. During daily operation, encryption key is required only for system boot up. If safety procedures allow, one USB flash drive can stay connected to Fudo Enterprise, which will allow Fudo Enterprise to boot up automatically in case of a power outage or system reboot after software update.

Virtual machine distribution

Fudo Enterprise's file system, running in virtual environment is encrypted using an encryption phrase, which is set up during system initiation and has to be entered each time the system boots up.

Database

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

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

3.7.2 Backups

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

3.7.3 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.

3.7.4 Sandboxing

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

3.7.5 Reliability

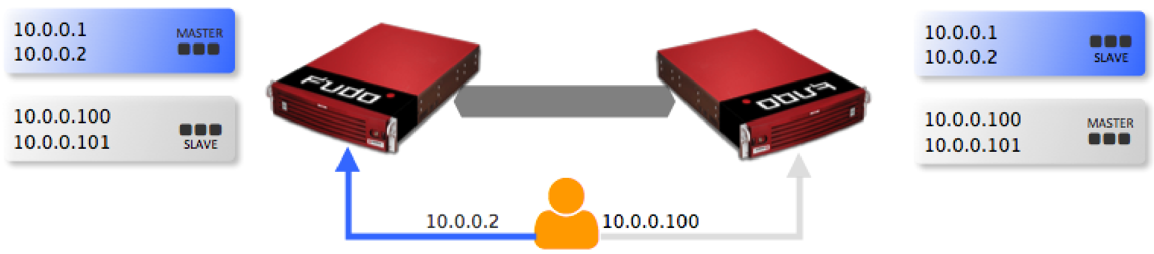
System hardware configuration is optimized to deliver high performance and high availability.

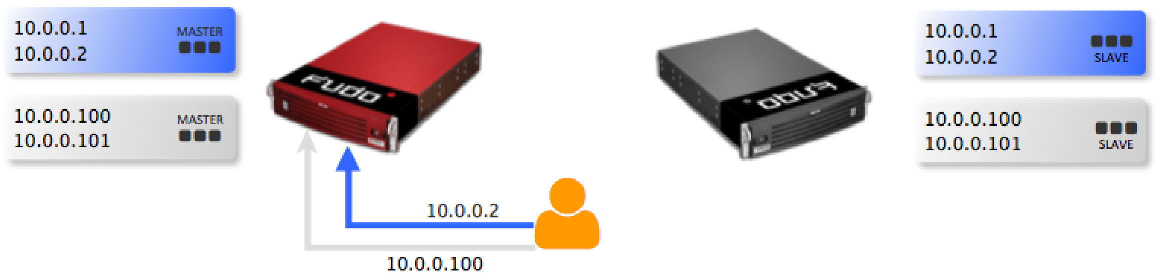
3.7.6 Cluster configuration

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

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

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





Related topics:

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

3.8 Data model

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

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

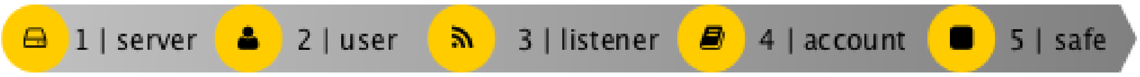
Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

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

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

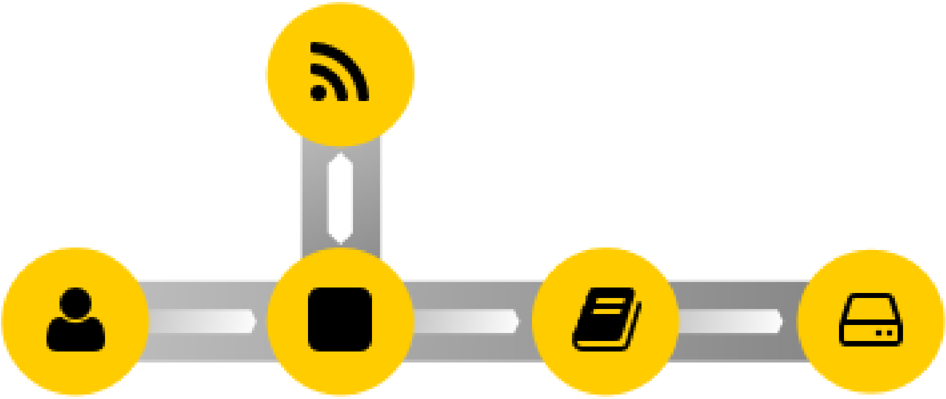
Listener determines server connection mode (proxy, gateway, transparent, bastion) as well as its specifics.

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



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

Objects relations chart



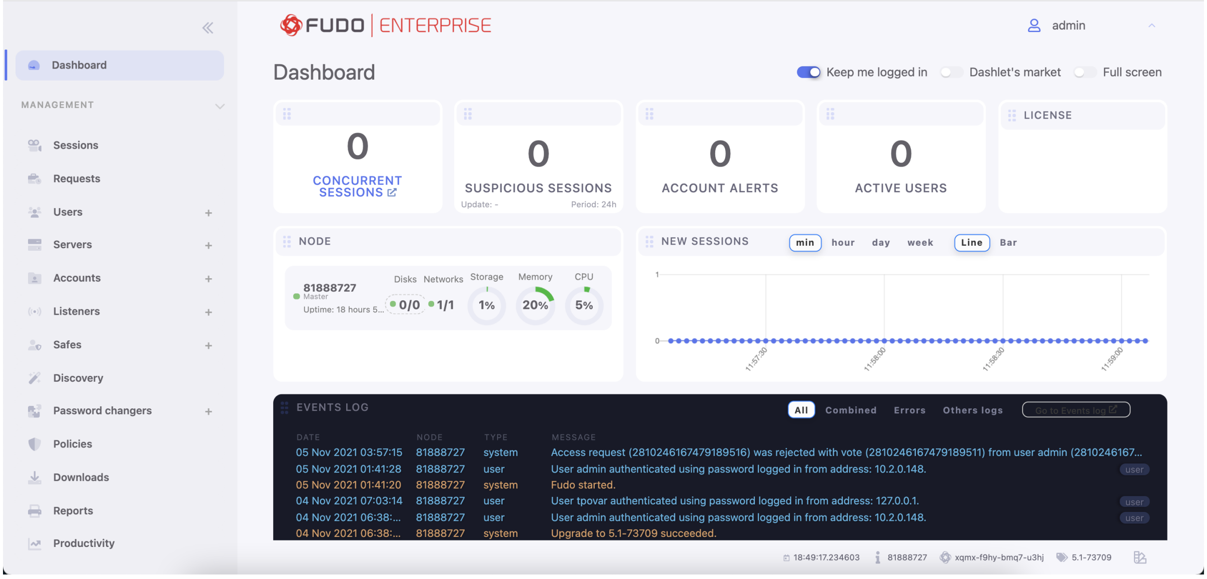
Safe is the central data model object. It regulates access to monitores servers by specifying privileged accounts on monitored servers along with the listeners which determine the actual connection parameters (e.g. IP address, port number) depending on the given protocol. This kind of data model allows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

Related topics:

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

3.9 Dashboard

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



```
DATE                  NODE      TYPE    MESSAGE
05 Nov 2021 03:57:15  81888727  system  Access request (2810246167479189516) was rejected with vote (2810246167479189511) from user admin (2810246167...
05 Nov 2021 01:41:28  81888727  user    User admin authenticated using password logged in from address: 10.2.0.148.                              user
05 Nov 2021 01:41:20  81888727  system  Fudo started.
04 Nov 2021 07:03:14  81888727  user    User tpovar authenticated using password logged in from address: 127.0.0.1.                              user
04 Nov 2021 06:38:... 81888727  user    User admin authenticated using password logged in from address: 10.2.0.148.                              user
04 Nov 2021 06:38:... 81888727  system  Upgrade to 5.1-73709 succeeded.
```

Note:

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

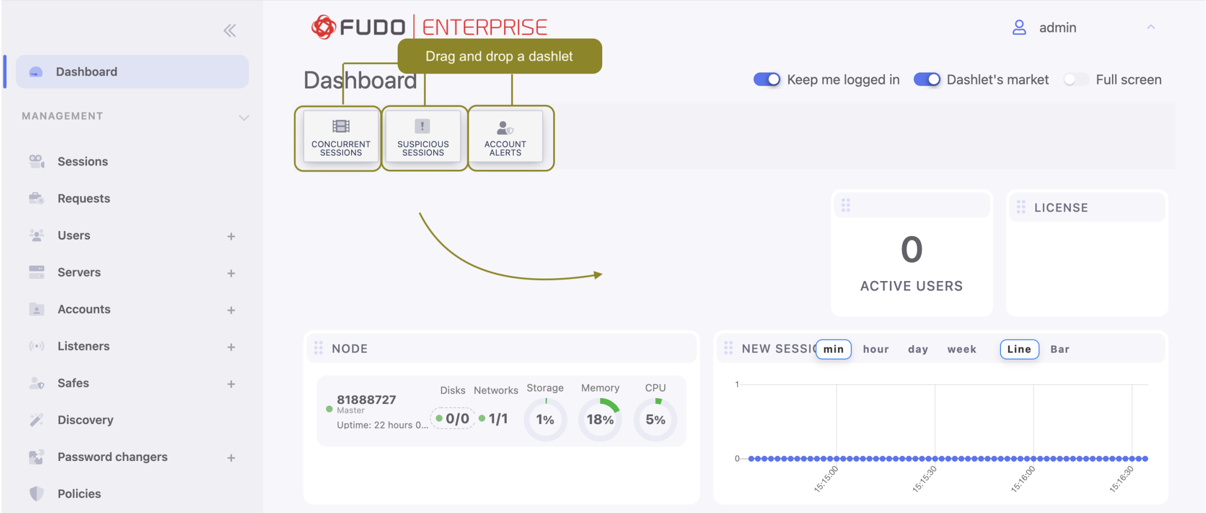
3.9.1 Widgets

New sessions	Chart depicting the number of newly established connections in a given time interval.
Concurrent sessions	The current number of user sessions.
Suspicious sessions	High-threat level sessions. The widget allows the following timeline configurations for the sessions: last 12 hours, last day, last week, and last month. The Suspicious sessions widget also provides an URL to the filtered Sessions list with `Threat level: High` criteria set so that administrator can check what's going on and quickly react.
Account alerts	Number of accounts at risk of a security breach.
Active users	Nubmer of currently connected users.
License	Information on the active license.
Node	Status information on the current Fudo Enterprise instance as well as other nodes.
System logs	Recent system events.

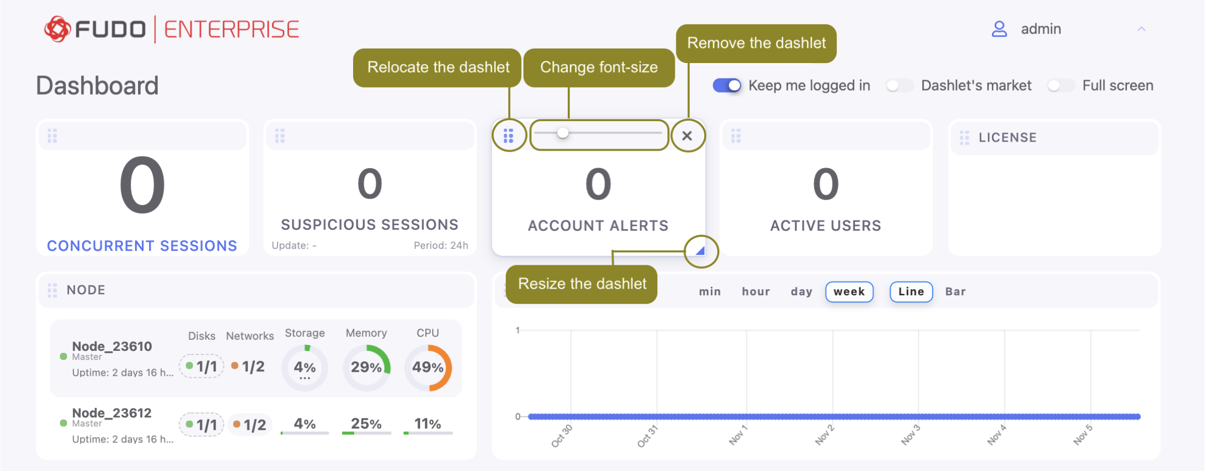
Note: Available widgets depend on the *user role*.

3.9.2 Adding, customizing and removind dashlets

1. Click the *Dashlet's market* switcher to display available dashlets.



2. Drag and drop a dashlet onto the workspace.

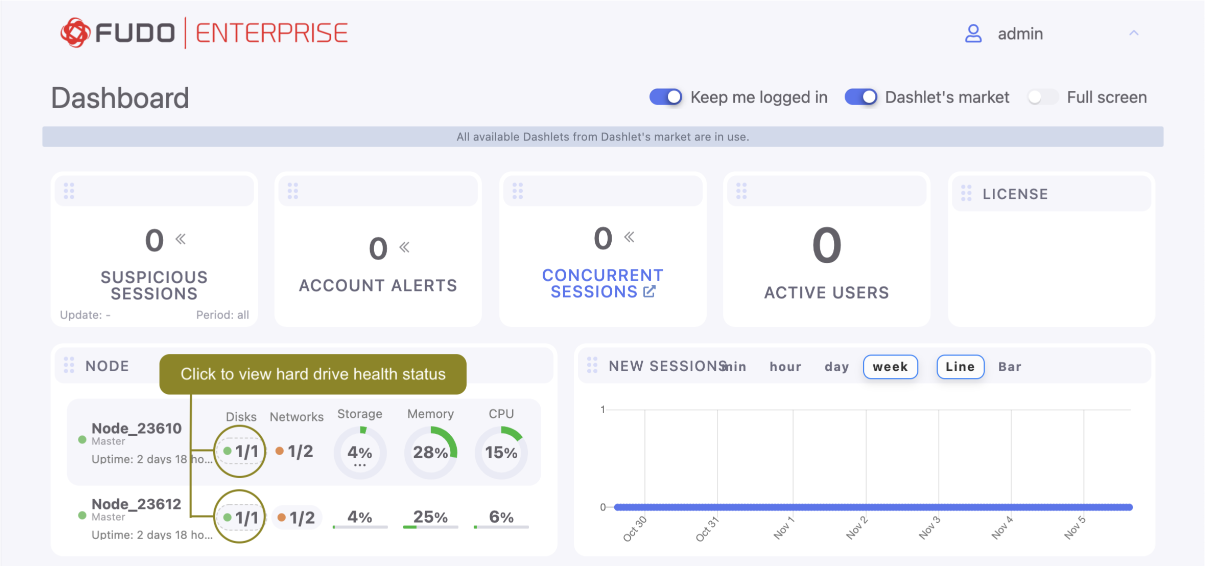


- Click and drag bottom-right corner of the dashlet to resize it.
- Click and drag the top-left corner to relocate the dashlet.
- Click arrows to change font-size.
- Click ✖ icon in the top-right corner. Then, click *Remove* to remove selected dashlet.

Note: Removed dashlets appear in the dashlets market area.

3.9.3 Hard drives status information

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



Click to view hard drive health status

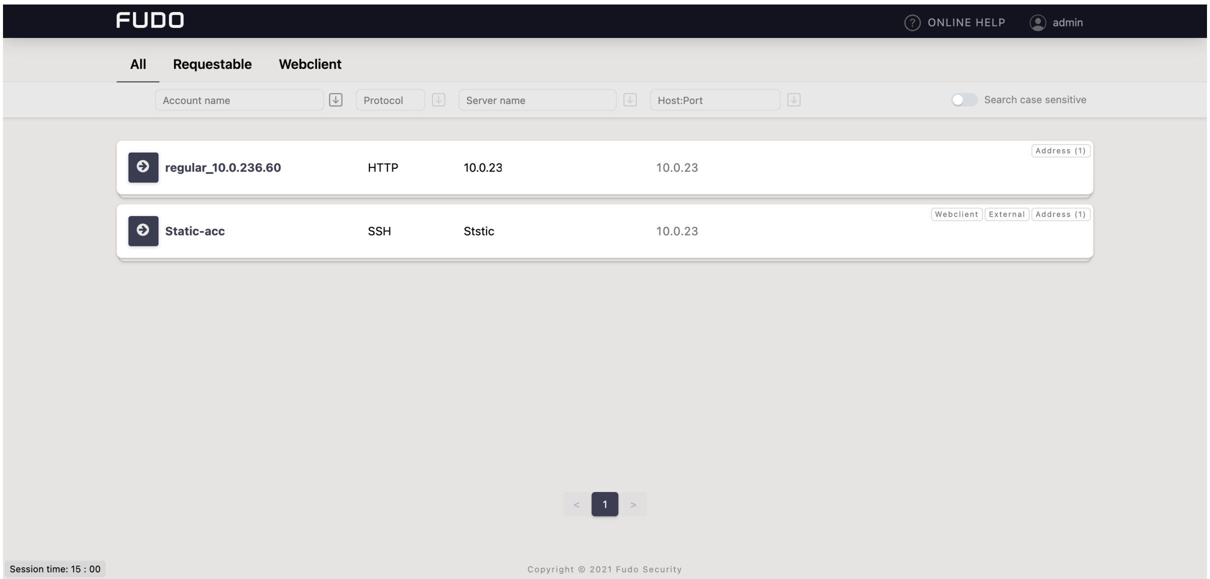
🟢	Hard drive operates properly.
🔵	Data on the hard drive is being synchronized.
🟠	Data read/write errors - the hard drive does not operate properly and it is likely to fail - contact the technical support to discuss hard drive replacement.
🔴	Hard drive failure - the hard drive must be replaced - contact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

Related topics:

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

3.10 User Portal (Access Gateway)

Access Gateway enables browsing available resources and initiating connections with monitored servers using selected listener.



Account name	Protocol	Server name	Host:Port
regular_10.0.236.60	HTTP	10.0.23	10.0.23
Static-acc	SSH	Ststic	10.0.23

Related topics:

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

3.11 Third-Party Licenses

This section contains third-party license information for certain third-party products included with Fudo Enterprise.

All the relevant licenses for third-party tools we depend on to deliver our product are available here. Please click on the link to view copies of the licenses text.

If the indicated location does not contain a license for specific product, it means that it was not provided by the developer.

CHAPTER 4

System deployment

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

4.1 Requirements

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 Enterprise on port 443/TCP, for administration purposes.
- Ability to establish an outgoing connection from Fudo Enterprise to the server `home.fudosecurity.com` on port 22/TCP for the *Call Home* service purpose.
- Ability for users to connect to Fudo Enterprise and for Fudo Enterprise to connect to target systems.
- Proper *time server configuration*.

Default ports used at startup

Port	Description
443/TCP	Required for administration purposes.
65522/TCP	Necessary for SSH-based administrative connections.
22/TCP	Utilized for SSH listener, added by default in the configuration, and for Fudo Officer mobile app using *Call Home* service.
3389/TCP	Used for RDP listener, added by default in the configuration.

Hardware requirements

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

Virtual appliance requirements

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

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

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

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

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

Target virutalization environments:

- VMware Tools
- VirtualBox
- Proxmox
- Hyper-V
- Azure

VNC software client requirements

VNC connections require 24-bit (true color) mode, with encryption disabled.

4.2 Hardware overview

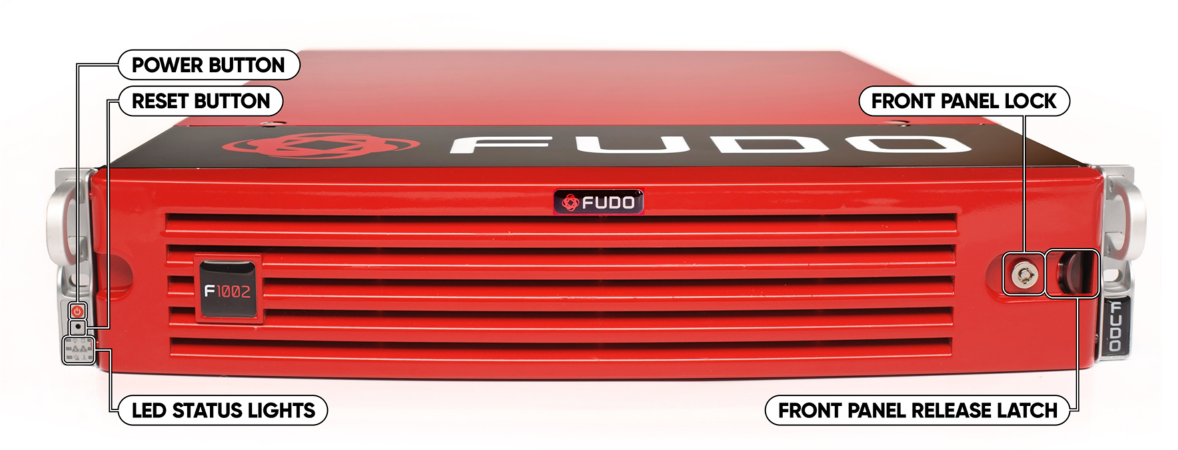
Fudo Enterprise is delivered in a 2U (F100x), 3U (F300x) or 4U (F500x) 19” rack server case.

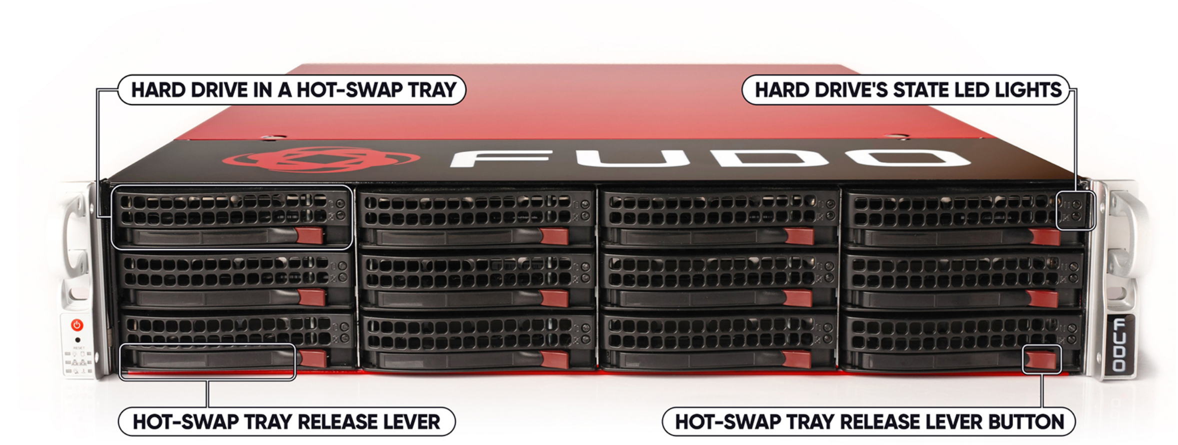
Fudo Enterprise F1002

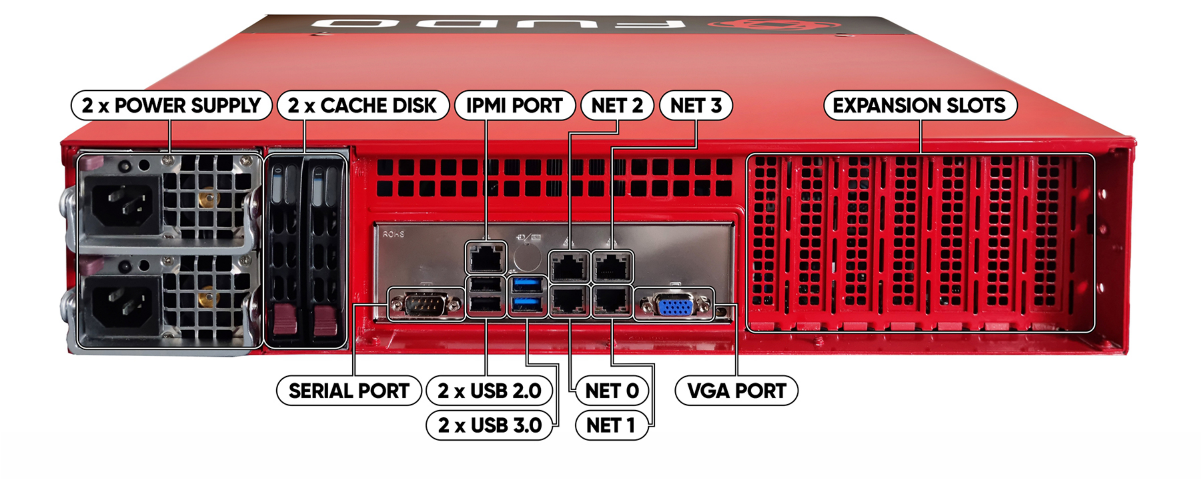
- Chassis: 19” 2U
- Dimensions: 89 mm (height), 437 mm (width), 647 mm (depth)
- PSU: 2x 920 W
- System memory: 32 GB
- Internal storage: 12x 2 TB, 2x 480 GB SSD
- Network interfaces:
  - 4 x RJ45 Gigabit Ethernet LAN ports

- 1 x RJ45 Dedicated IPMI LAN port

The situation might be different, depending on the use of the expansion cards.




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

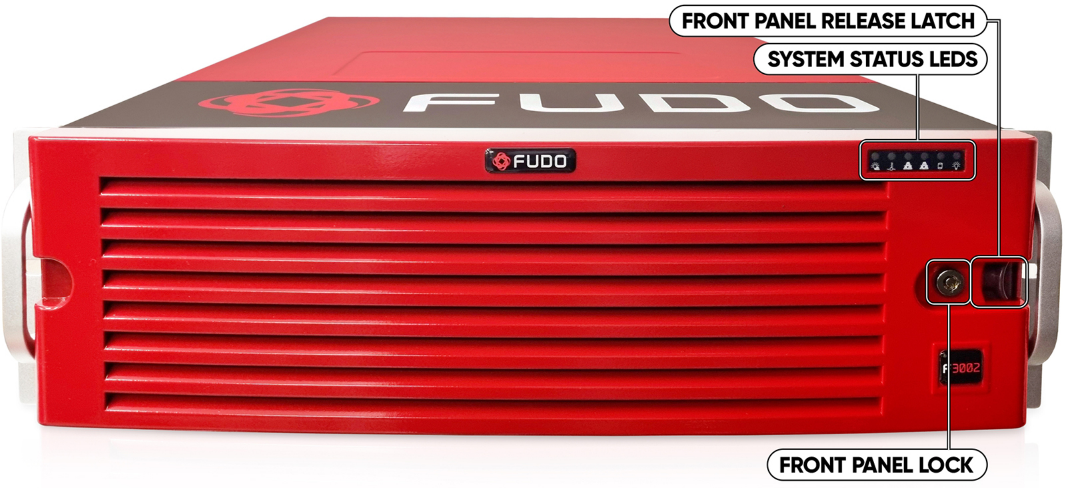


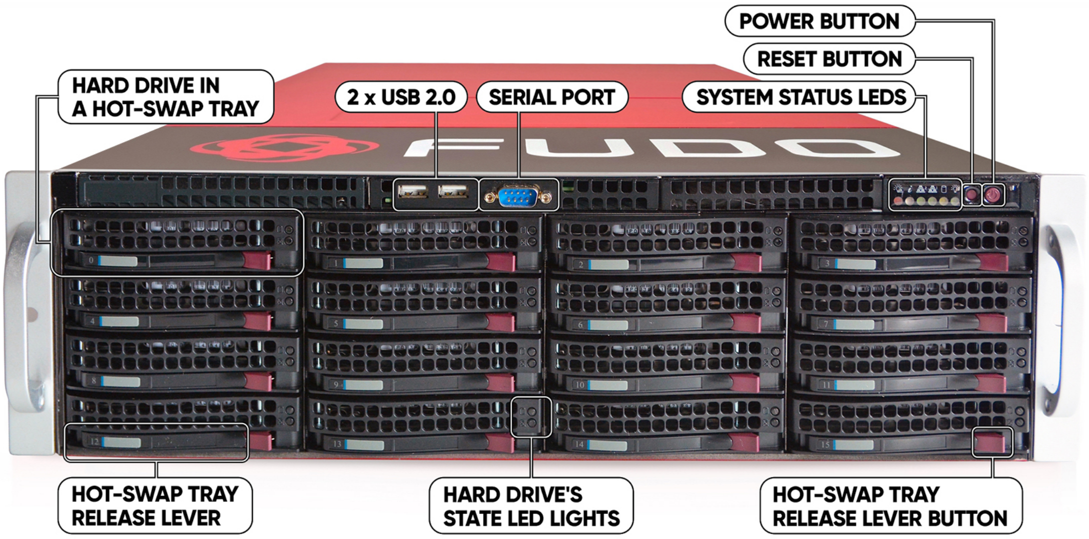
Fudo Enterprise F3002

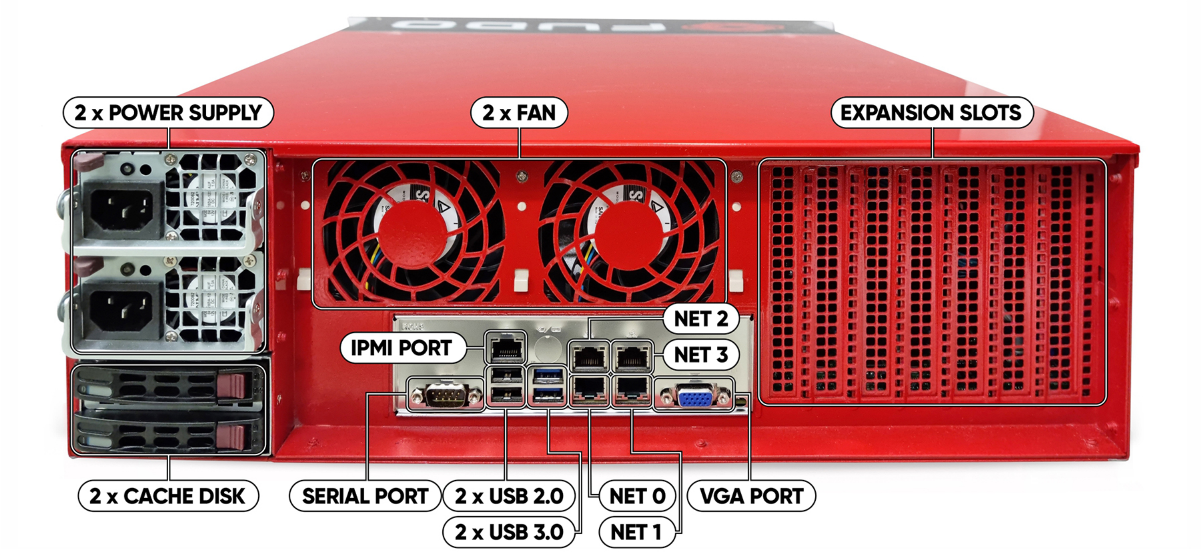
- Chassis: 19" 3U
- Dimensions: 132 mm (height), 437 mm (width), 647 mm (depth)

- PSU: 2x 1000 W
- System memory: 64 GB
- Internal storage: 16x 6 TB HDD, 2x 480 GB SSD
- Network interfaces:
  - 4 x RJ45 Gigabit Ethernet LAN ports
  - 1 x RJ45 Dedicated IPMI LAN port

  The situation might be different, depending on the use of the expansion cards.



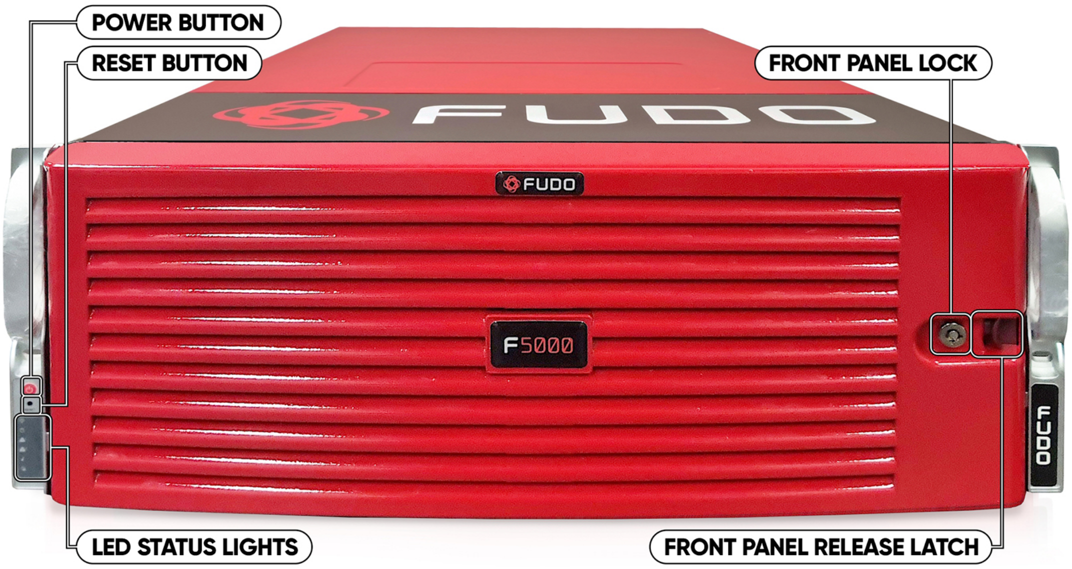

POWER BUTTON
RESET BUTTON
HARD DRIVE IN A HOT-SWAP TRAY
2 x USB 2.0
SERIAL PORT
SYSTEM STATUS LEDS
HOT-SWAP TRAY RELEASE LEVER
HARD DRIVE'S STATE LED LIGHTS
HOT-SWAP TRAY RELEASE LEVER BUTTON

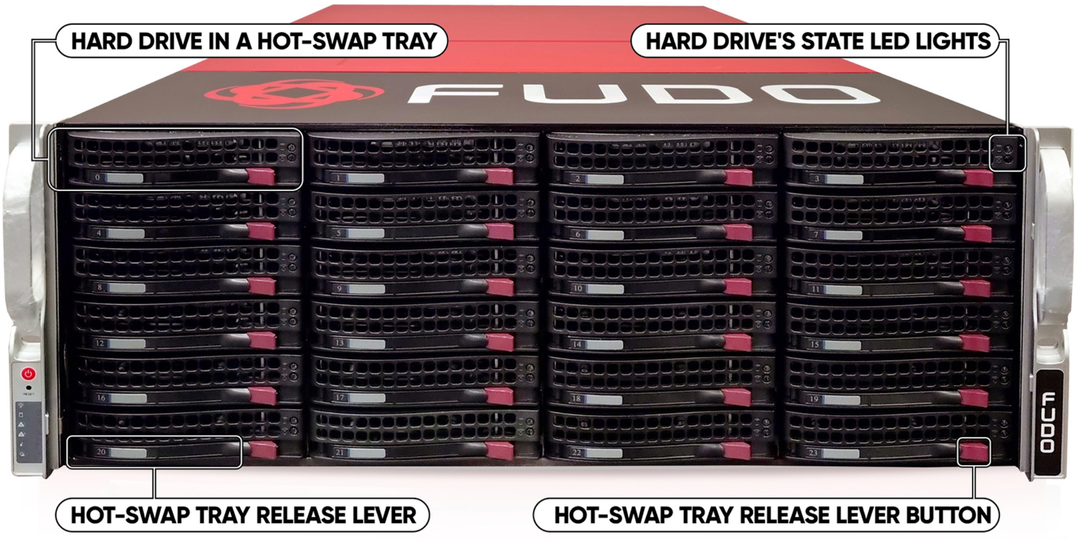


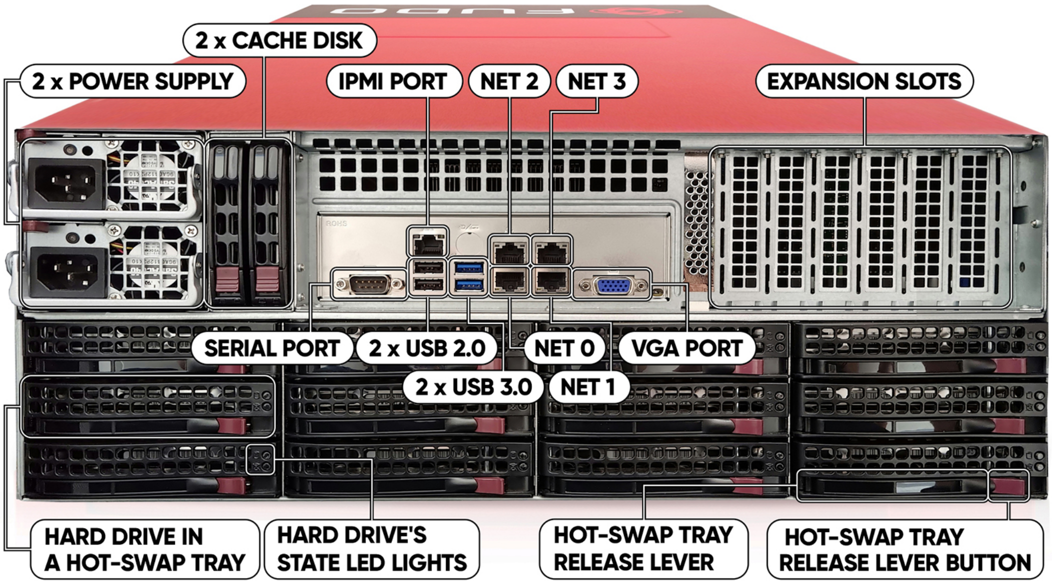
Fudo Enterprise F5000

- Chassis: 19" 4U
- Dimensions: 178 mm (height), 437 mm (width), 699 mm (depth)
- PSU: 2x 1280 W
- System memory: 128 GB
- Internal storage: 36x 8 TB, 2x 480 GB SSD
- Network interfaces:
  - 4 x RJ45 Gigabit Ethernet LAN ports
  - 1 x RJ45 Dedicated IPMI LAN port

  The situation might be different, depending on the use of the expansion cards.




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


2 x CACHE DISK
2 x POWER SUPPLY
IPMI PORT
NET 2
NET 3
EXPANSION SLOTS
SERIAL PORT
2 x USB 2.0
NET 0
VGA PORT
2 x USB 3.0
NET 1
HARD DRIVE IN A HOT-SWAP TRAY
HARD DRIVE'S STATE LED LIGHTS
HOT-SWAP TRAY RELEASE LEVER
HOT-SWAP TRAY RELEASE LEVER BUTTON

Related topics:

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

4.3 System initiation

Appliance

Fudo Enterprise is delivered with two uninitiated USB flash drives. During initial boot up, Fudo Enterprise generates encryption keys, which are stored on enclosed USB flash drives. More information on encryption keys can be found in the *Security measures* chapter.

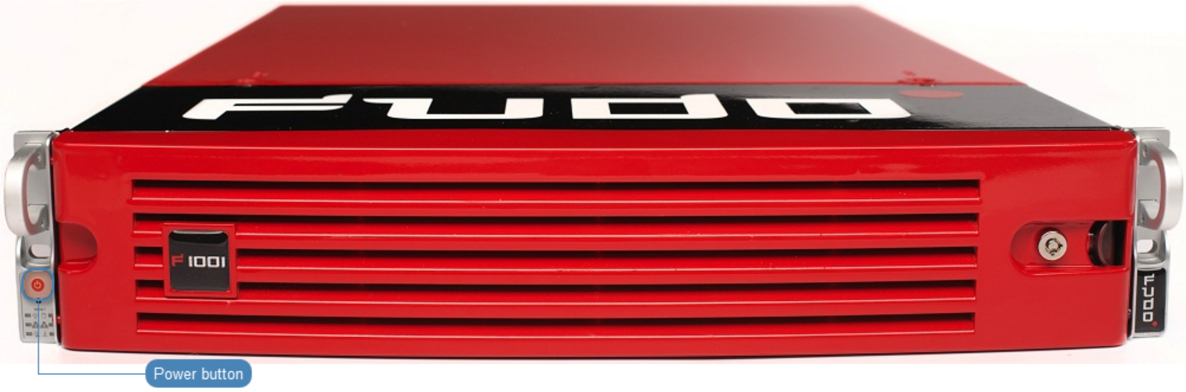
1. Install device in 19" rack cabinet.
2. Connect both power supply units to 230V/110V power outlets.

Note: Connecting both power supplies is necessary to start the system.

3. Connect network cable to one of the RJ-45 ports.
4. Connect both of the USB flash drives delivered with Fudo Enterprise.

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

5. Press the power button on the front panel.



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

Warning:

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

Note:

- In daily operation, one encryption key is required to start the system after which it can be disconnected.

- It is advised to make a backup copy of the encryption key.

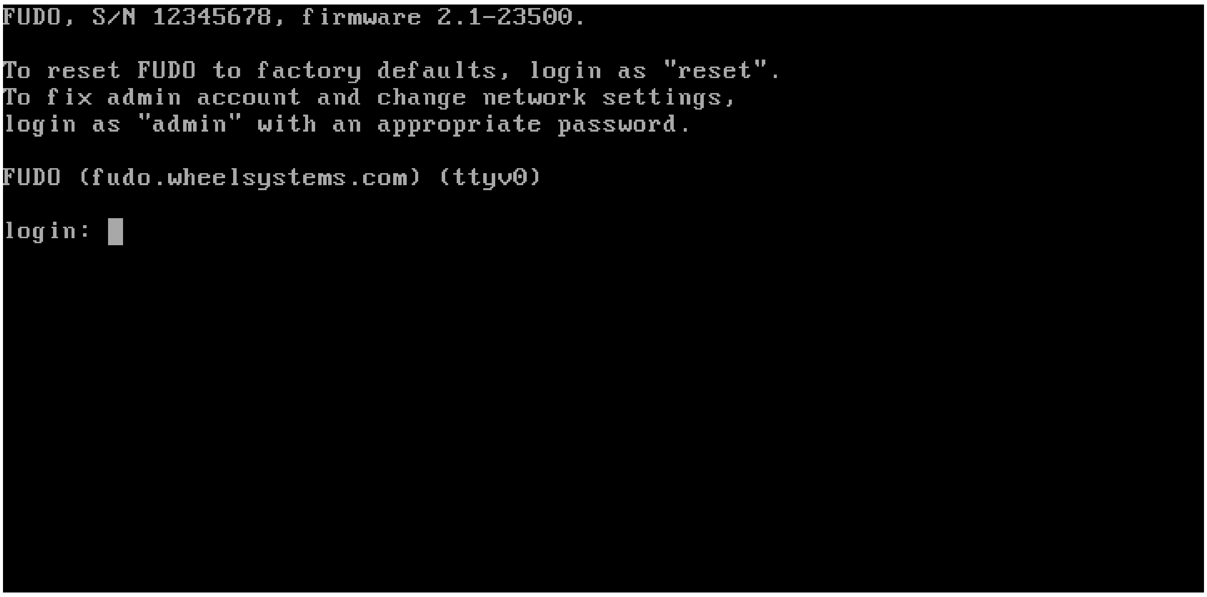
Setting IP address using system console

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

Note: Default login credentials:

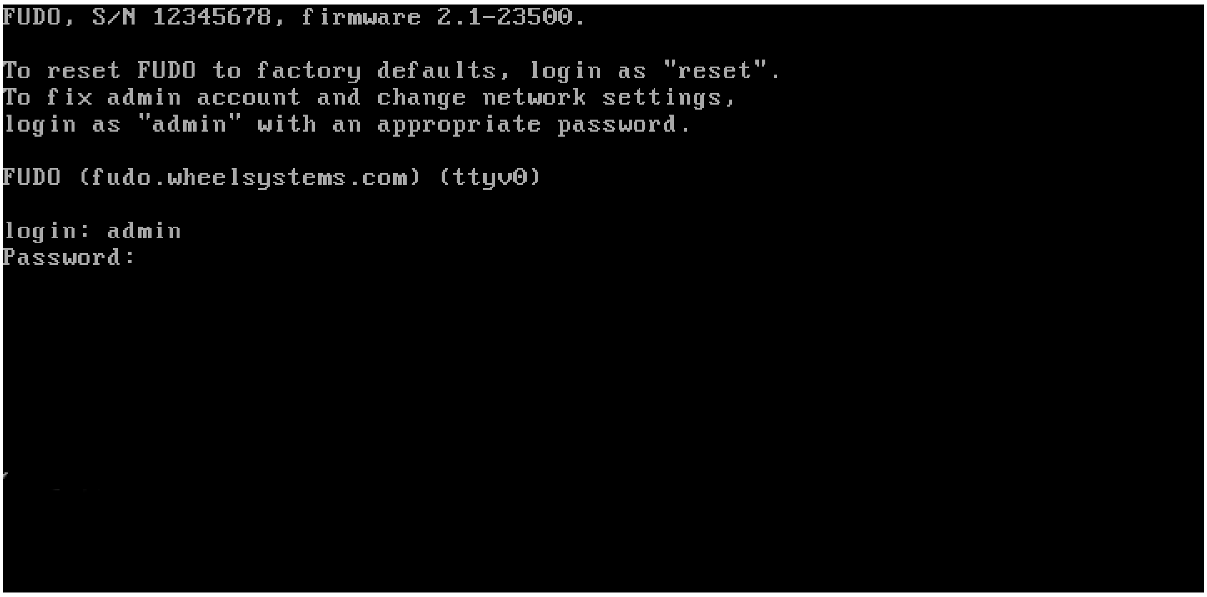
login: admin
password: proxycrypto

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



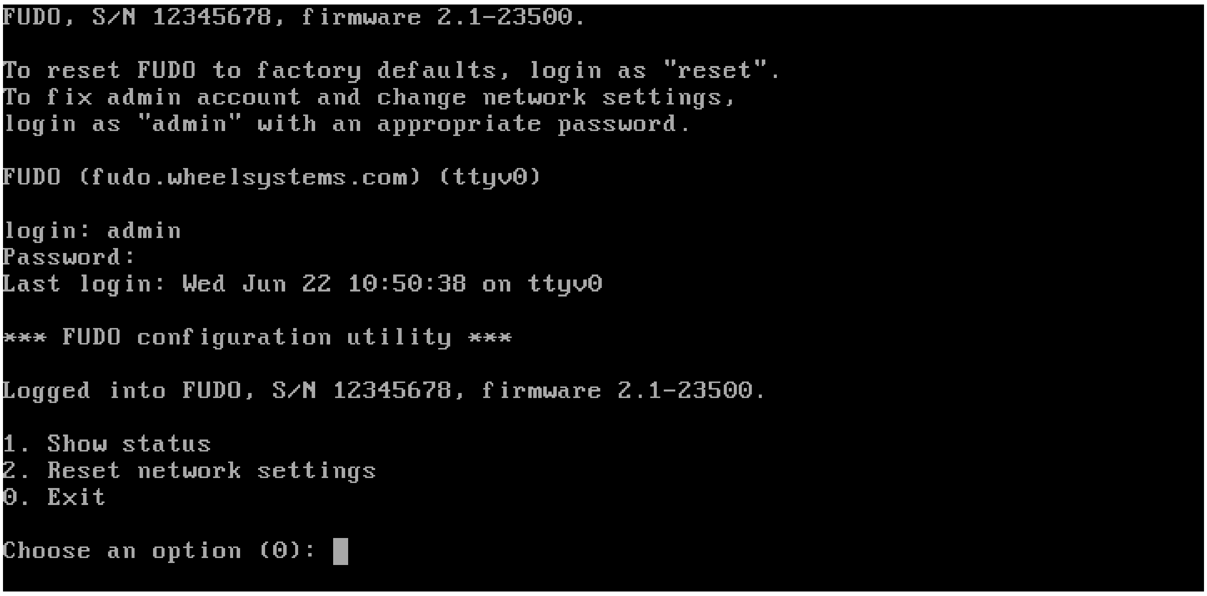
```
FUDO, S/N 12345678, firmware 2.1-23500.

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*.



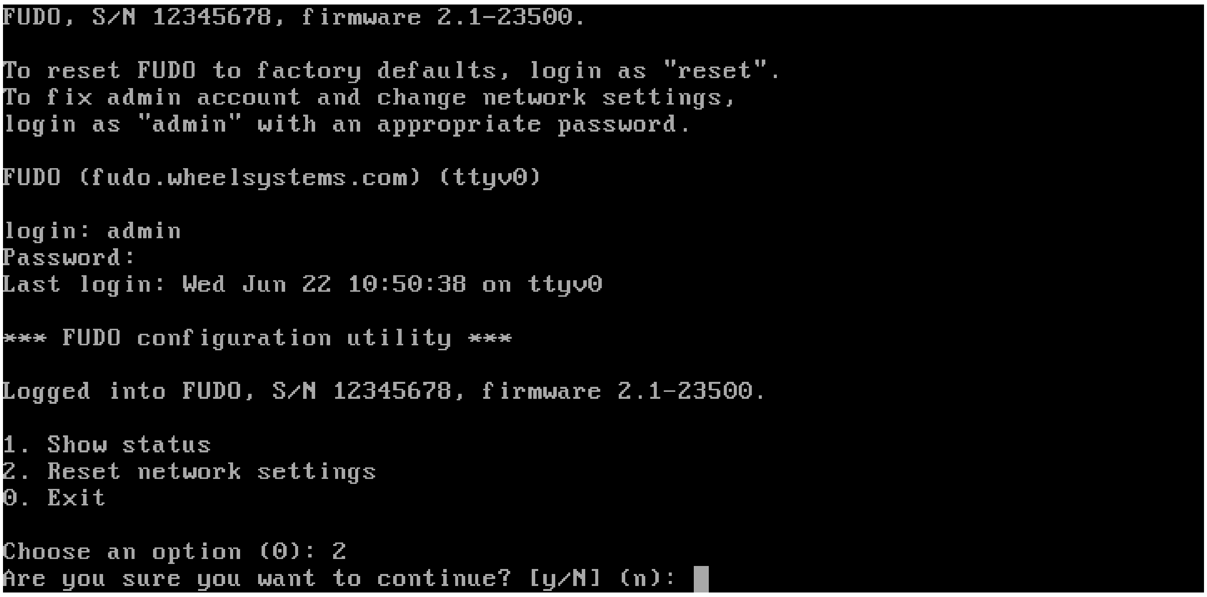
```
FUDO, S/N 12345678, firmware 2.1-23500.

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.



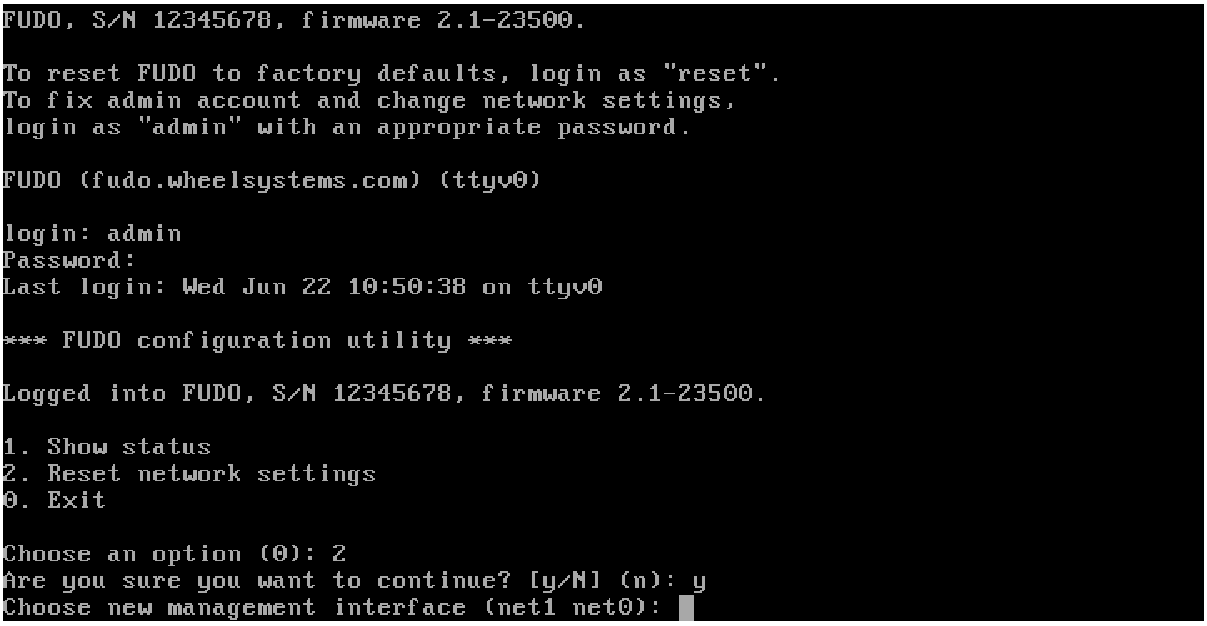
```
FUDO, S/N 12345678, firmware 2.1-23500.

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.



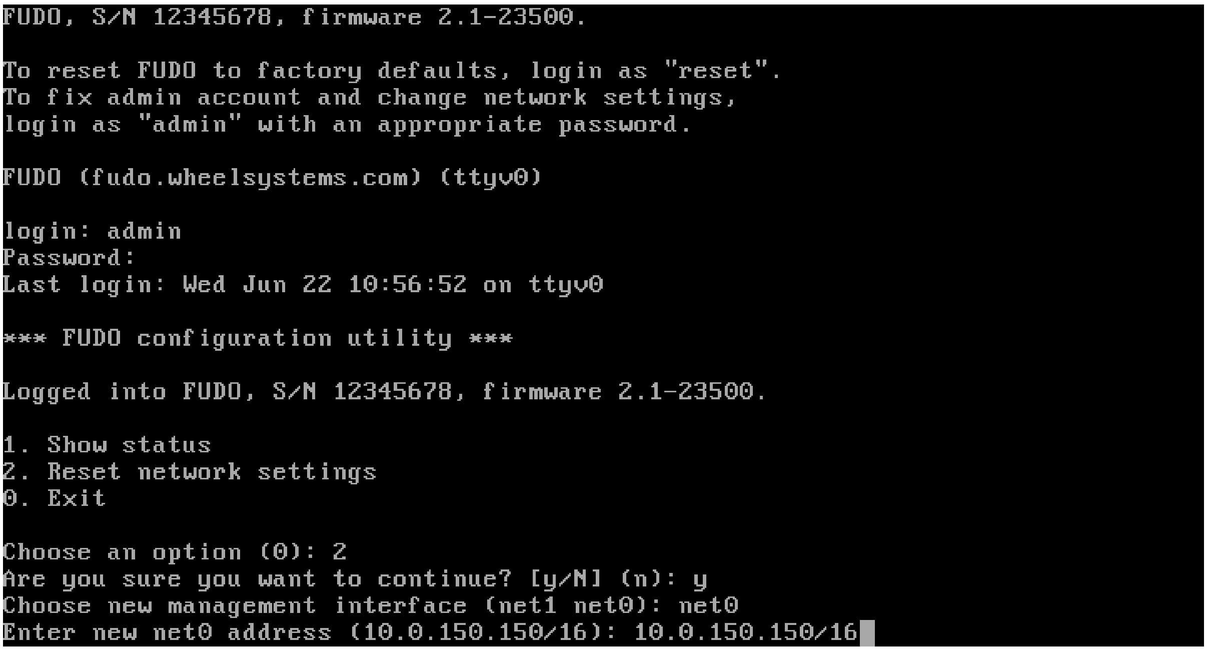
```
FUDO, S/N 12345678, firmware 2.1-23500.

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 Enterprise web interface is accessible through the management interface).



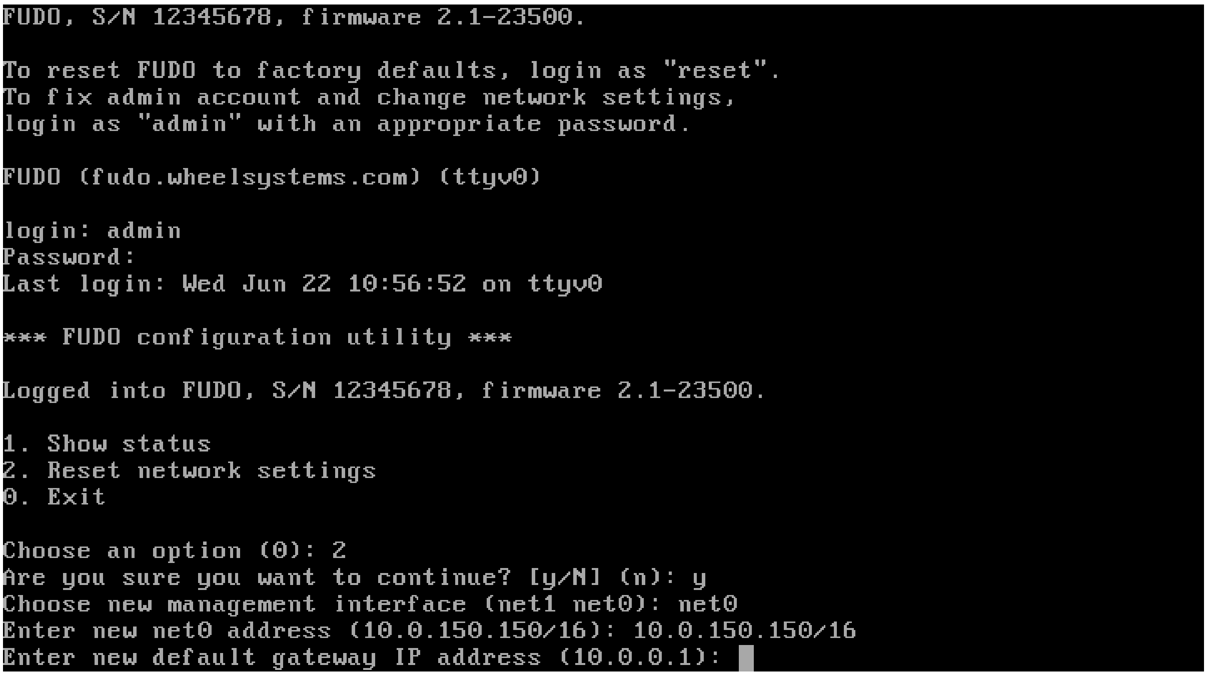
```
FUDO, S/N 12345678, firmware 2.1-23500.

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): 
```

7. Enter IP address along with the network subnet mask separated with / (e.g. `10.0.0.8/24`) and press *Enter*.



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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

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

8. Enter network gate and press *Enter*.



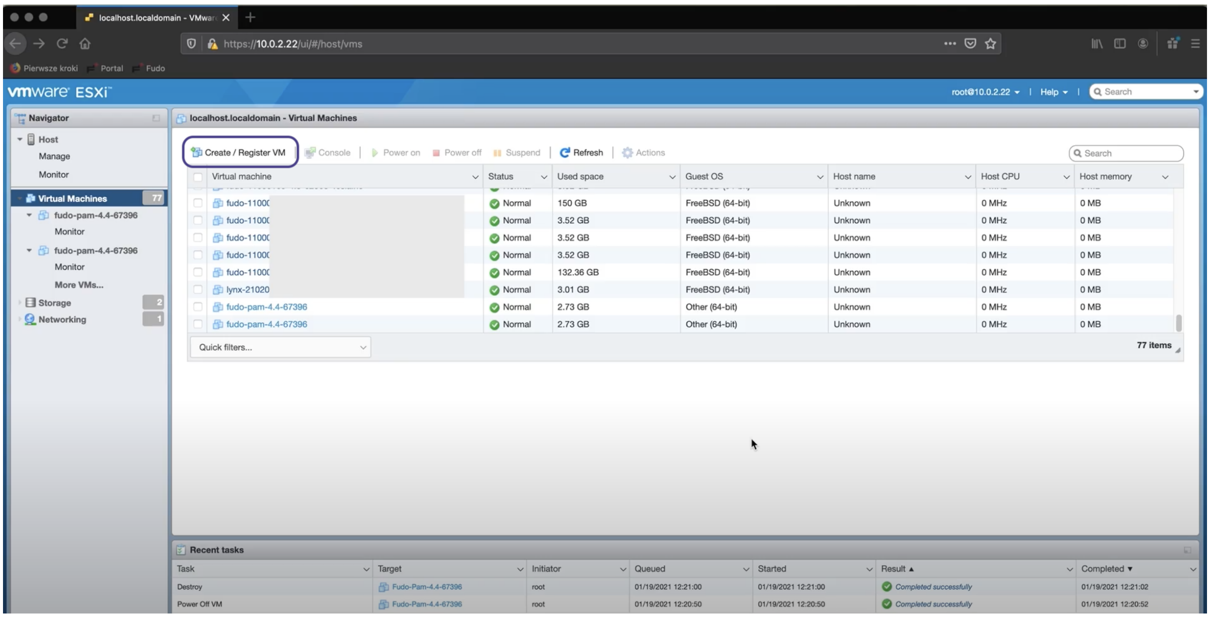
```
FUDO, S/N 12345678, firmware 2.1-23500.

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

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

4.3.1 Virtual machine

Local Fudo Enterprise deployment is based on uploading the OVA / OVF file into virtualization tool and running the Fudo Enterprise instance on browser. Please follow below chapters to deploy Fudo Enterprise using the VMware or Proxmox virtualization tools. In order to proceed the deployment, the OVA or OVF file is needed.

VMware Installation with OVA file

1. Click the *Create / Register VM* button.

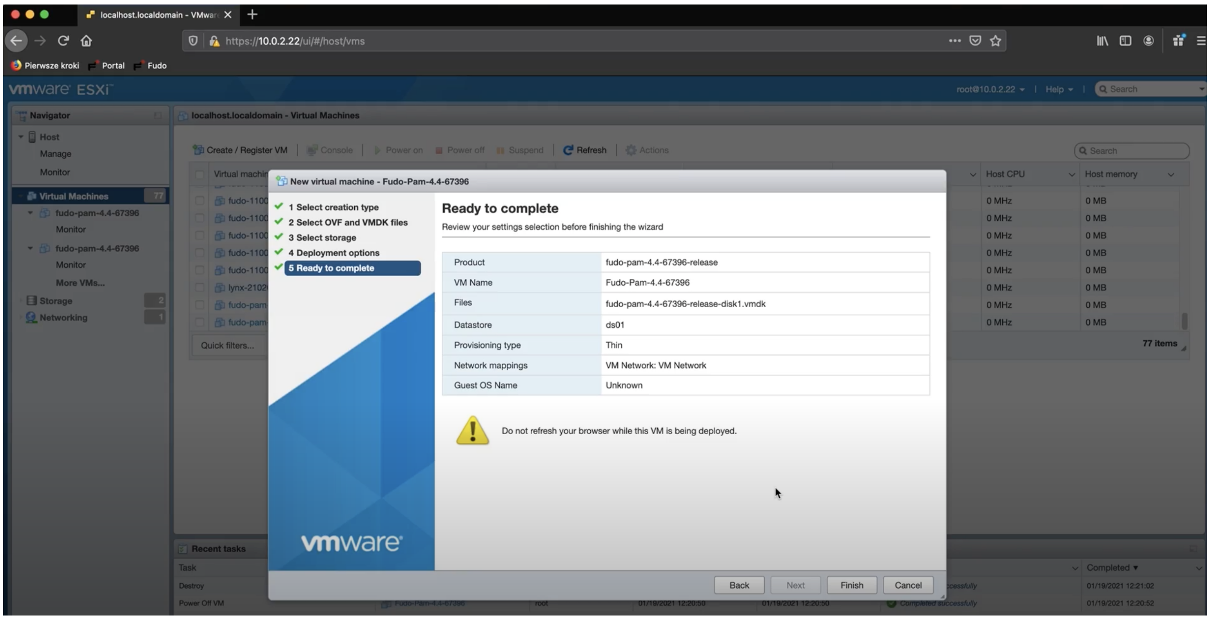


Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
fudo-1100[redacted]	Normal	150 GB	FreeBSD (64-bit)	Unknown	0 MHz	0 MB
fudo-1100[redacted]	Normal	3.52 GB	FreeBSD (64-bit)	Unknown	0 MHz	0 MB
fudo-1100[redacted]	Normal	3.52 GB	FreeBSD (64-bit)	Unknown	0 MHz	0 MB
fudo-1100[redacted]	Normal	3.52 GB	FreeBSD (64-bit)	Unknown	0 MHz	0 MB
fudo-1100[redacted]	Normal	132.36 GB	FreeBSD (64-bit)	Unknown	0 MHz	0 MB
lynx-21020[redacted]	Normal	3.01 GB	FreeBSD (64-bit)	Unknown	0 MHz	0 MB
fudo-pam-4.4-67396	Normal	2.73 GB	Other (64-bit)	Unknown	0 MHz	0 MB
fudo-pam-4.4-67396	Normal	2.73 GB	Other (64-bit)	Unknown	0 MHz	0 MB

Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼
Destroy	Fudo-Pam-4.4-67396	root	01/19/2021 12:21:00	01/19/2021 12:21:00	Completed successfully	01/19/2021 12:21:02
Power Off VM	Fudo-Pam-4.4-67396	root	01/19/2021 12:20:50	01/19/2021 12:20:50	Completed successfully	01/19/2021 12:20:52

2. In the modal window, select the *Deploy a virtual machine from an OVF or OVA file* option.
3. Select the downloaded OVA file and upload it, or just drag and drop it into the upload area.

4. Enter a name for the virtual machine.
5. Select the storage option.
6. Select deployment options.



New virtual machine - Fudo-Pam-4.4-67396

✓ 1 Select creation type
✓ 2 Select OVF and VMDK files
✓ 3 Select storage
✓ 4 Deployment options
✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	fudo-pam-4.4-67396-release
VM Name	Fudo-Pam-4.4-67396
Files	fudo-pam-4.4-67396-release-disk1.vmdk
Datastore	ds01
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

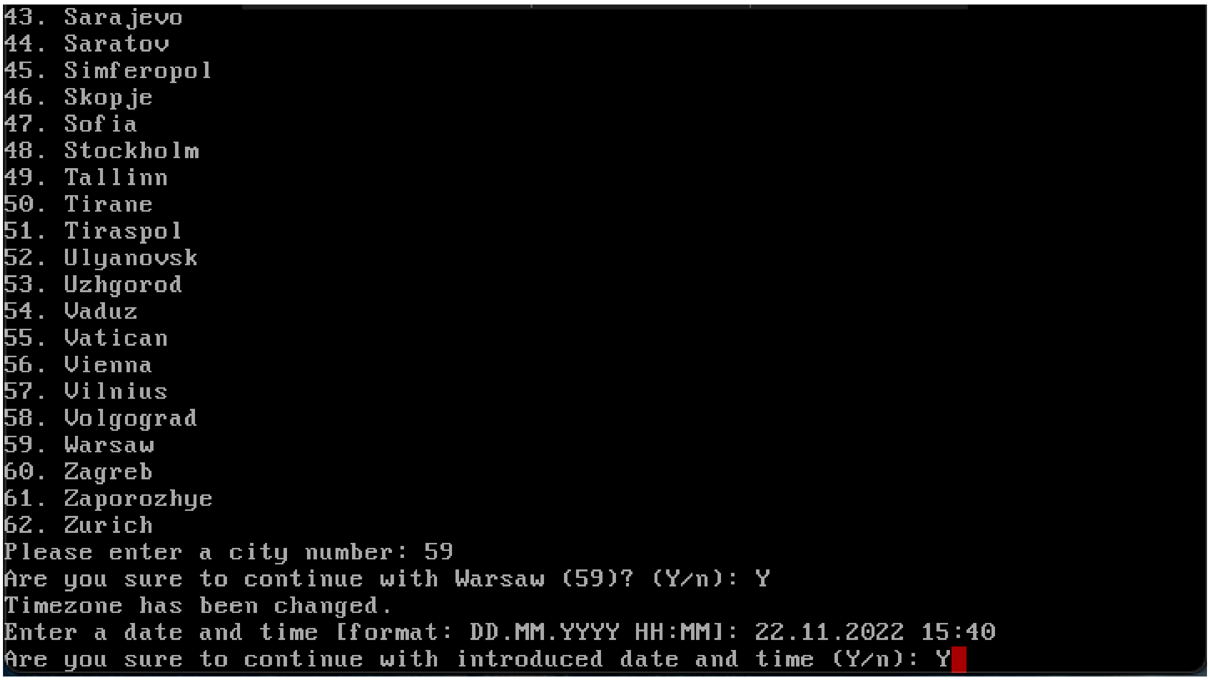
Do not refresh your browser while this VM is being deployed.

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

Note: The password is optional and can be left empty. However, if the password is provided, the Fudo system encrypts it and asks for it every time the VM is rebooted.

---

11. Select the region and city by providing respective codes and confirming your choice.
12. Enter date and time in `DD.MM.YYYY HH:MM` format.



```
43. Sarajevo
44. Saratov
45. Simferopol
46. Skopje
47. Sofia
48. Stockholm
49. Tallinn
50. Tirane
51. Tiraspol
52. Ulyanovsk
53. Uzhgorod
54. Vaduz
55. Vatican
56. Vienna
57. Vilnius
58. Volgograd
59. Warsaw
60. Zagreb
61. Zaporozhye
62. Zurich
Please enter a city number: 59
Are you sure to continue with Warsaw (59)? (Y/n): Y
Timezone has been changed.
Enter a date and time [format: DD.MM.YYYY HH:MM]: 22.11.2022 15:40
Are you sure to continue with introduced date and time (Y/n): Y
```

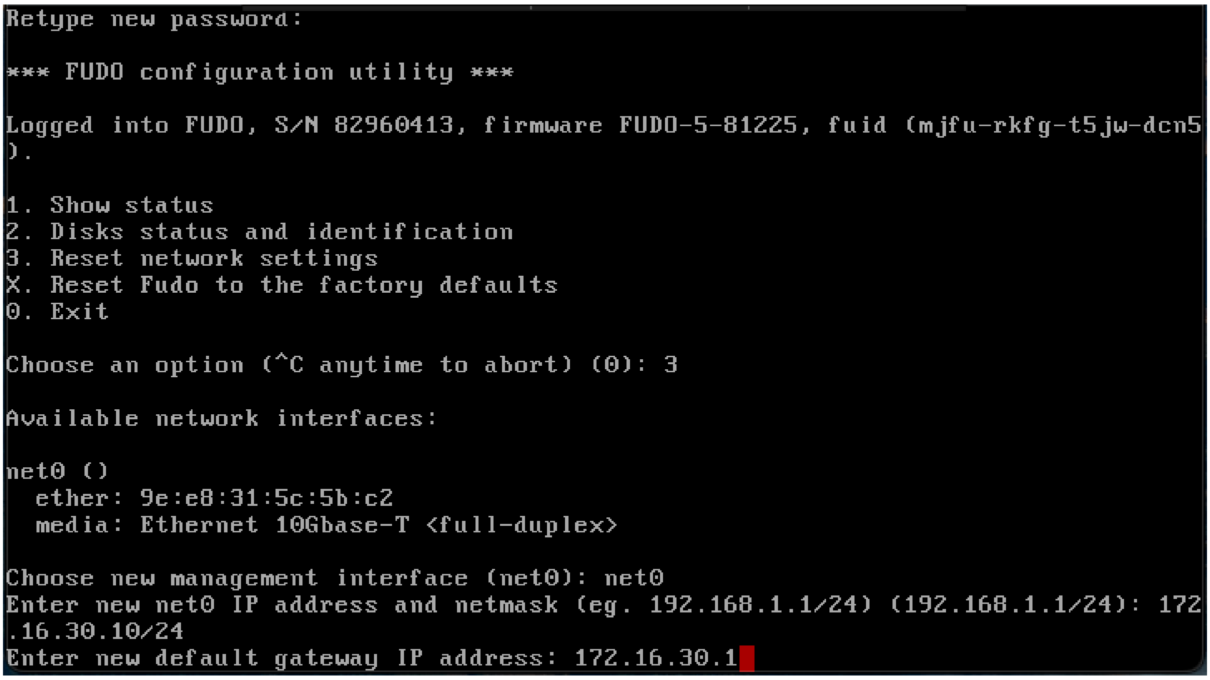
13. Set the network configuration:

    a. Sign in as an administrator:

        login: admin
        password: proxycrypto

    b. From the list of the *Fudo configuration utility*, select option *3 - Reset network settings*.

    c. Select new management interface and enter the IP address.



```
Retype new password:

*** FUDO configuration utility ***

Logged into FUDO, S/N 82960413, firmware FUDO-5-81225, fuid (mjfu-rkfg-t5jw-dcn5
).

1. Show status
2. Disks status and identification
3. Reset network settings
X. Reset Fudo to the factory defaults
0. Exit

Choose an option (^C anytime to abort) (0): 3

Available network interfaces:

net0 ()
  ether: 9e:e8:31:5c:5b:c2
  media: Ethernet 10Gbase-T <full-duplex>

Choose new management interface (net0): net0
Enter new net0 IP address and netmask (eg. 192.168.1.1/24) (192.168.1.1/24): 172
.16.30.10/24
Enter new default gateway IP address: 172.16.30.1
```

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

Proxmox Installation with OVF file

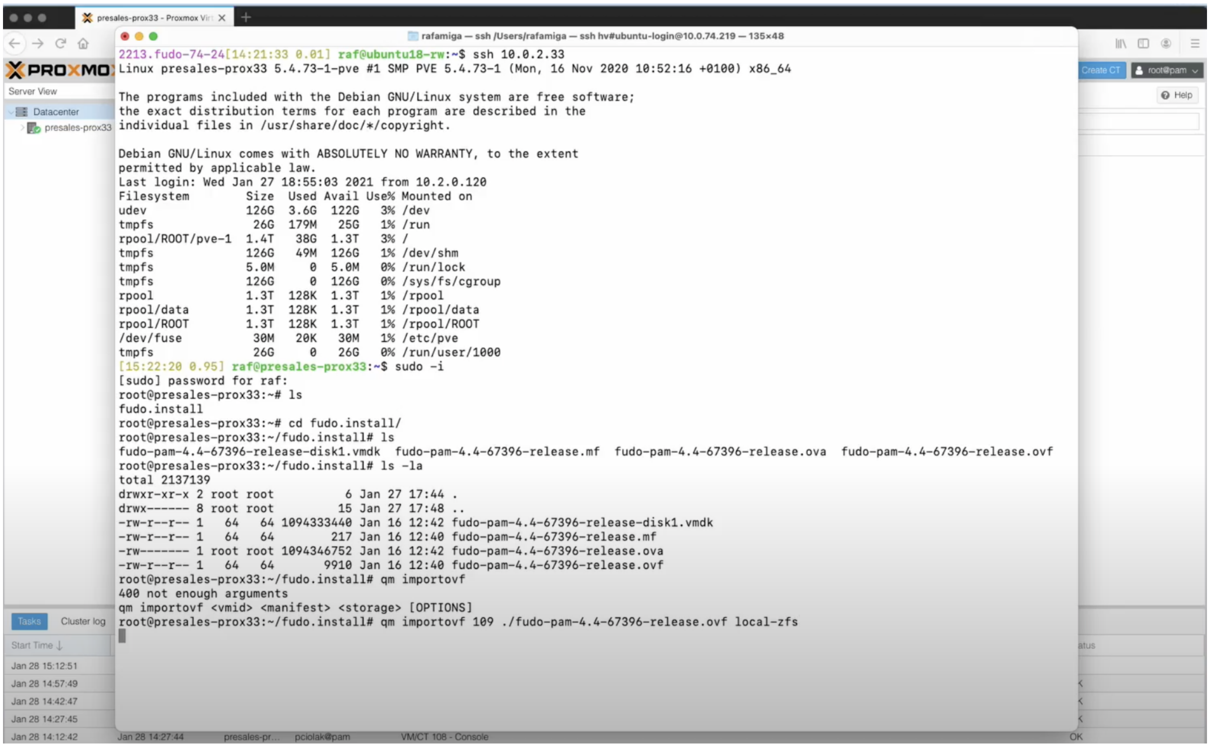
1. Create a new machine using cores, memory and VM name as read from the OVF manifest, and import the disks to the local-zfs storage:

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

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

   for example:

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



```
2213.fudo-74-24[14:21:33 0.01] raf@ubuntu18-rw:~$ ssh 10.0.2.33
Linux presales-prox33 5.4.73-1-pve #1 SMP PVE 5.4.73-1 (Mon, 16 Nov 2020 10:52:16 +0100) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jan 27 18:55:03 2021 from 10.2.0.120
Filesystem        Size  Used Avail Use% Mounted on
udev              126G  3.6G  122G   3% /dev
tmpfs              26G  179M   25G   1% /run
rpool/ROOT/pve-1  1.4T   38G  1.3T   3% /
tmpfs             126G   49M  126G   1% /dev/shm
tmpfs             5.0M     0  5.0M   0% /run/lock
tmpfs             126G     0  126G   0% /sys/fs/cgroup
rpool             1.3T  128K  1.3T   1% /rpool
rpool/data        1.3T  128K  1.3T   1% /rpool/data
rpool/ROOT        1.3T  128K  1.3T   1% /rpool/ROOT
/dev/fuse          30M   20K   30M   1% /etc/pve
tmpfs              26G     0   26G   0% /run/user/1000
[15:22:20 0.95] raf@presales-prox33:~$ sudo -i
[sudo] password for raf:
root@presales-prox33:~# ls
fudo.install
root@presales-prox33:~# cd fudo.install/
root@presales-prox33:~/fudo.install# ls
fudo-pam-4.4-67396-release-disk1.vmdk  fudo-pam-4.4-67396-release.mf  fudo-pam-4.4-67396-release.ova  fudo-pam-4.4-67396-release.ovf
root@presales-prox33:~/fudo.install# ls -la
total 2137139
drwxr-xr-x 2 root root          6 Jan 27 17:44 .
drwx------ 8 root root         15 Jan 27 17:48 ..
-rw-r--r-- 1   64   64 1094333440 Jan 16 12:42 fudo-pam-4.4-67396-release-disk1.vmdk
-rw-r--r-- 1   64   64        217 Jan 16 12:40 fudo-pam-4.4-67396-release.mf
-rw------- 1 root root 1094346752 Jan 16 12:42 fudo-pam-4.4-67396-release.ova
-rw-r--r-- 1   64   64       9910 Jan 16 12:40 fudo-pam-4.4-67396-release.ovf
root@presales-prox33:~/fudo.install# qm importovf
400 not enough arguments
qm importovf <vmid> <manifest> <storage> [OPTIONS]
root@presales-prox33:~/fudo.install# qm importovf 109 ./fudo-pam-4.4-67396-release.ovf local-zfs
```

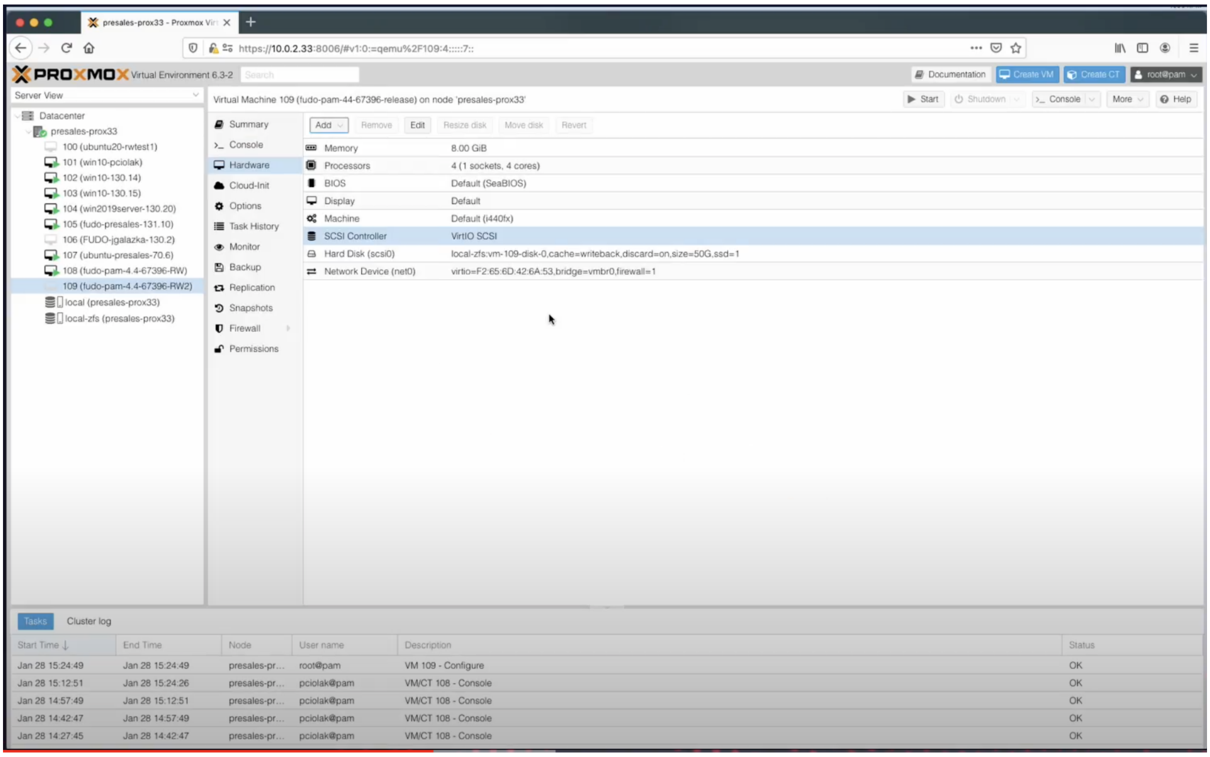
2. Wait for the manifest data to be imported.

3. In the Proxmox client find your server and open settings for your `109 (fudo-one-36271-release)` virtual machine.

4. In the *Hardware section*, change the *Hard Disk* options into the *Write back* cache, and in *Advanced section* check the *SSD emulation* option, then the *Discard* option. Click *OK*.

5. In the *SCSI Controller* section, select the *VirtIO SCSI* option as a SCSI controller type.

6. Add a new Network Device and in the *Model* field select the *VirtIO (paravirtualized)* option.



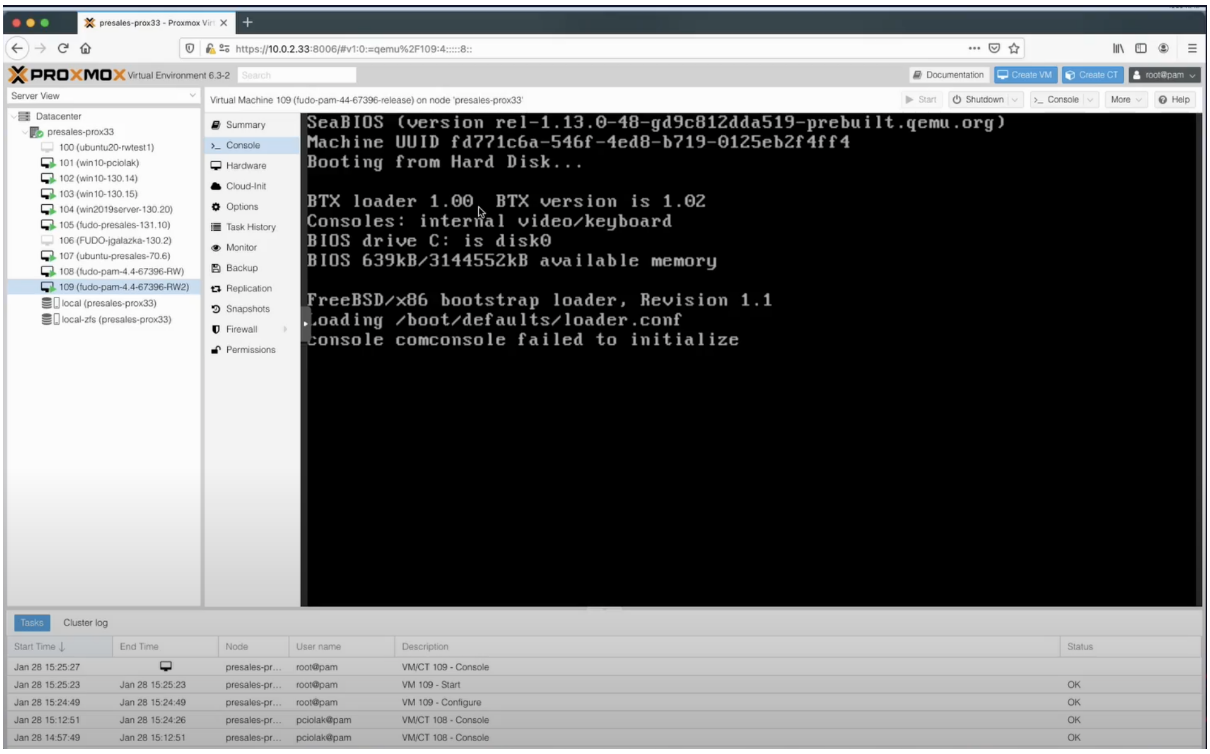
Virtual Machine 109 (fudo-pam-44-67396-release) on node 'presales-prox33'

Memory	8.00 GiB
Processors	4 (1 sockets, 4 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
Hard Disk (scsi0)	local-zfs:vm-109-disk-0,cache=writeback,discard=on,size=50G,ssd=1
Network Device (net0)	virtio=F2:65:6D:42:6A:53,bridge=vmbr0,firewall=1

Start Time ↓	End Time	Node	User name	Description	Status
Jan 28 15:24:49	Jan 28 15:24:49	presales-pr...	root@pam	VM 109 - Configure	OK
Jan 28 15:12:51	Jan 28 15:24:26	presales-pr...	pciolak@pam	VM/CT 108 - Console	OK
Jan 28 14:57:49	Jan 28 15:12:51	presales-pr...	pciolak@pam	VM/CT 108 - Console	OK
Jan 28 14:42:47	Jan 28 14:57:49	presales-pr...	pciolak@pam	VM/CT 108 - Console	OK
Jan 28 14:27:45	Jan 28 14:42:47	presales-pr...	pciolak@pam	VM/CT 108 - Console	OK

7. Click the *Start* option.

8. Go to the *Console*.



Virtual Machine 109 (fudo-pam-44-67396-release) on node 'presales-prox33'

```
SeaBIOS (version rel-1.13.0-48-gd9c812dda519-prebuilt.qemu.org)
Machine UUID fd771c6a-546f-4ed8-b719-0125eb2f4ff4
Booting from Hard Disk...

BTX loader 1.00  BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 639kB/3144552kB available memory

FreeBSD/x86 bootstrap loader, Revision 1.1
.oading /boot/defaults/loader.conf
console comconsole failed to initialize
```

Start Time ↓	End Time	Node	User name	Description	Status
Jan 28 15:25:27		presales-pr...	root@pam	VM/CT 109 - Console	
Jan 28 15:25:23	Jan 28 15:25:23	presales-pr...	root@pam	VM 109 - Start	OK
Jan 28 15:24:49	Jan 28 15:24:49	presales-pr...	root@pam	VM 109 - Configure	OK
Jan 28 15:12:51	Jan 28 15:24:26	presales-pr...	pciolak@pam	VM/CT 108 - Console	OK
Jan 28 14:57:49	Jan 28 15:12:51	presales-pr...	pciolak@pam	VM/CT 108 - Console	OK

9. Select the region and city by providing respective codes and confirming your choice.

10. Enter date and time in `DD.MM.YYYY HH:MM` format.

11. Set the network configuration:

    a. Sign in as an administrator:

login: admin
password: proxycrypto

b. From the list of the *Fudo configuration utility*, select the option *3 - Reset network settings*.

c. Select new management interface and enter the IP address with a mask.

d. Enter a new default gateway IP address.

Note: Your Fudo Enterprise instance has been successfully initiated!

12. Enter the registered IP address in your browser bar and sign in as an administrator.
13. In the *Network configuration settings* input a name for the Access Gateway address. Click *Save*.
14. Add a new DNS server address in the Name & DNS sub-tab. Click *Save*.
15. In the System settings, add a new NTP server address. Click *Save*.
16. From the contextual menu in the upper right corner, select the *Restart* option.
17. Wait for the system to be restarted and sign in back again.

Note: Now you can start with your first configuration!

Related topics:

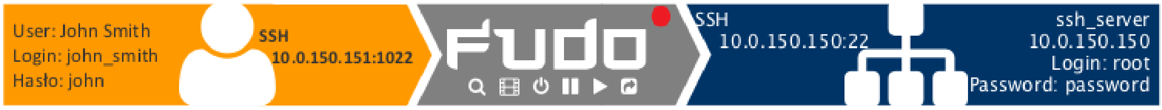
- *Requirements*
- *Quick start - SSH connection configuration*
- *Quick start - RDP connection configuration*
- *System overview*
- *Security measures*

CHAPTER 5

Quick start

5.1 SSH

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



5.1.1 Prerequisites

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

5.1.2 Configuration

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 server.*
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`ssh_server`
Description	✗
Blocked	✗
Protocol	`SSH`
Legacy ciphers	✗
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.150.151`
Mask	`32`
Port	`22`
Server verification	`None`

4. Click *Save* or *Save and close.*

Adding a user

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

1. Select *Management > Users.*

2. Click *+ Add*.

3. Provide essential user information:

Parameter	Value
General	
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	`10.0.150.152`
Port	`1022`
External address	✗
External port	✗

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

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

5. Click *Save*.

Adding an account

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

1. Select *Management > Accounts*.

2. Click *+ Add*.

3. Provide essential configuration parameters:

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

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

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

5. Click *Save*.

Defining a safe

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

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

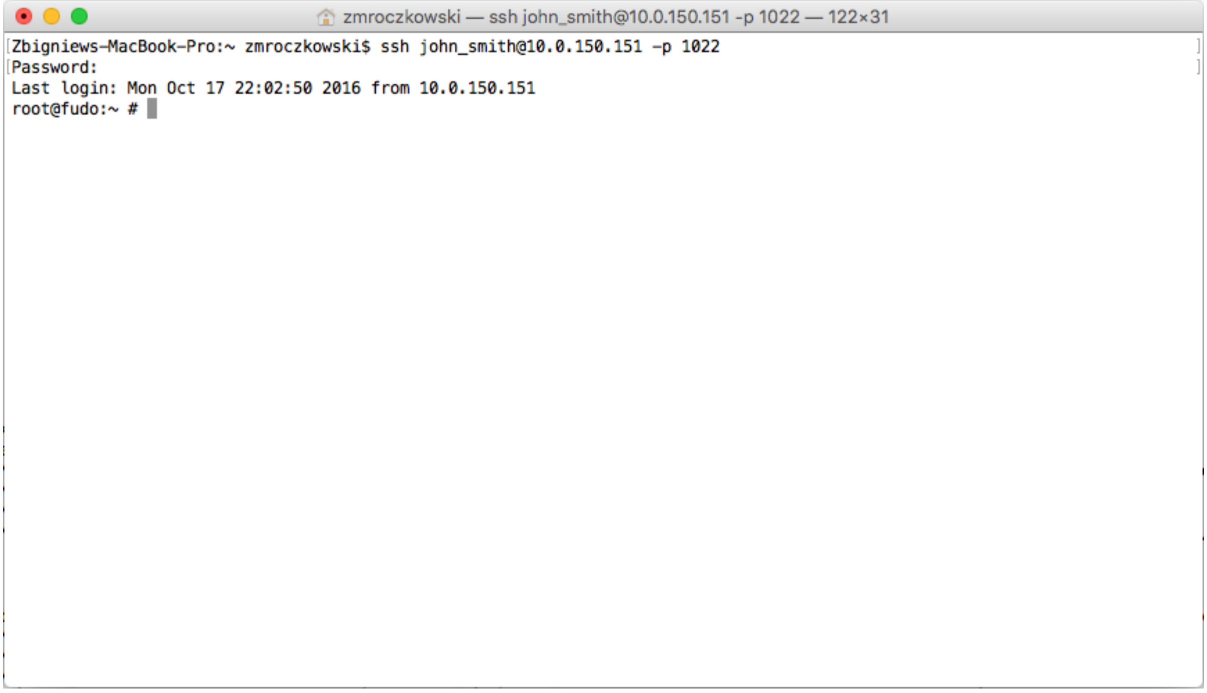
Parameter	Value
General	
Name	`ssh_safe`
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✓
VNC	✗

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

5.1.3 Establishing connection

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

Example:



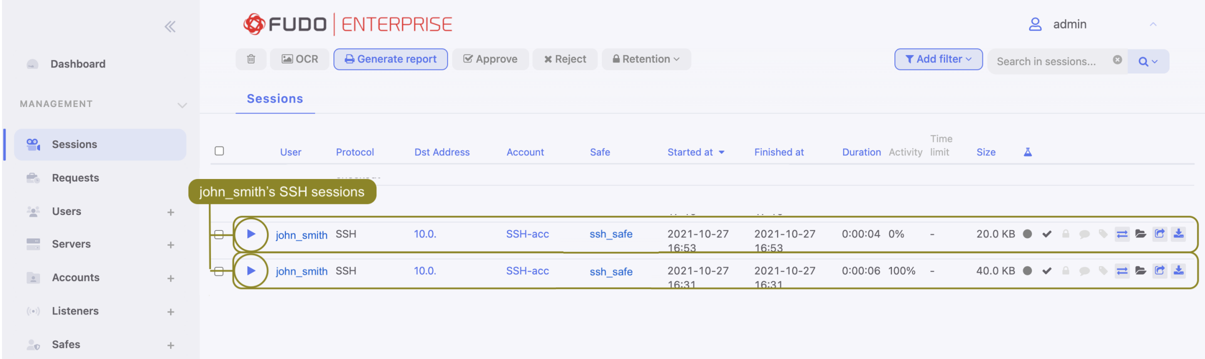
```
Zbigniews-MacBook-Pro:~ zmroczkowski$ ssh john_smith@10.0.150.151 -p 1022
Password:
Last login: Mon Oct 17 22:02:50 2016 from 10.0.150.151
root@fudo:~ #
```

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 Enterprise starts recording user's activities.

5.1.4 Viewing user session

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



□		User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
□	▶	john_smith	SSH	10.0.	SSH-acc	ssh_safe	2021-10-27 16:53	2021-10-27 16:53	0:00:04	0%	-	20.0 KB
□	▶	john_smith	SSH	10.0.	SSH-acc	ssh_safe	2021-10-27 16:31	2021-10-27 16:31	0:00:06	100%	-	40.0 KB

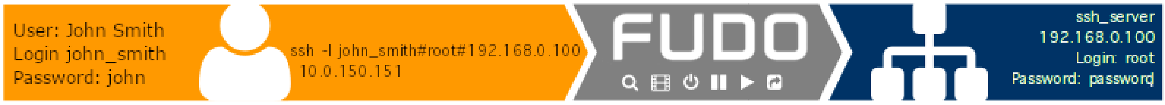
Related topics:

- *PuTTY*
- *Requirements*

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

5.2 SSH in bastion mode

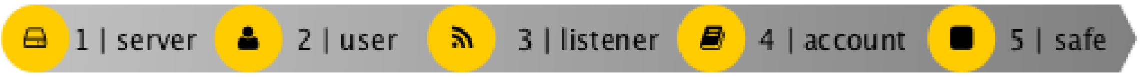
This chapter contains an example of a basic Fudo Enterprise configuration, to monitor SSH access in bastion mode. In this scenario, the user connects to the remote server over the *SSH* protocol and logs in to the Fudo Enterprise using an individual login and password combination (`john_smith`/`john`). The user specifies user name along with account login on the target server and target server address in the login string (`john_smith#root#192.168.0.110`) and connects to it over default SSH port number. Upon establishing connection, login credentials are substituted with the previously defined values: `root`/`password` (authentication modes are described in the *User authentication modes* section).



5.2.1 Prerequisites

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

5.2.2 Configuration



Adding a server

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

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

Parameter	Value
General	
Name	`ssh_server`
Description	❌
Blocked	❌
Protocol	`SSH`
Legacy ciphers	❌
Bind address	`Any`
Permissions	
Granted users	❌
Destination	
Address	`192.168.0.100`
Mask	`32`
Port	`22`
Server verification	`None`

4. In the *Server verification* section select *Server public key* and provide respective public key data or click *Get public key*.

5. Click *Save* or *Save and close*.

Adding a user

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

1. Select *Management > Users*.

2. Click *+ Add*.

3. Provide essential user information:

Parameter	Value
General	
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.

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

5. Click *Save*.

Adding an account

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

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

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

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

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

5. Click *Save*.

Defining a safe

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

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

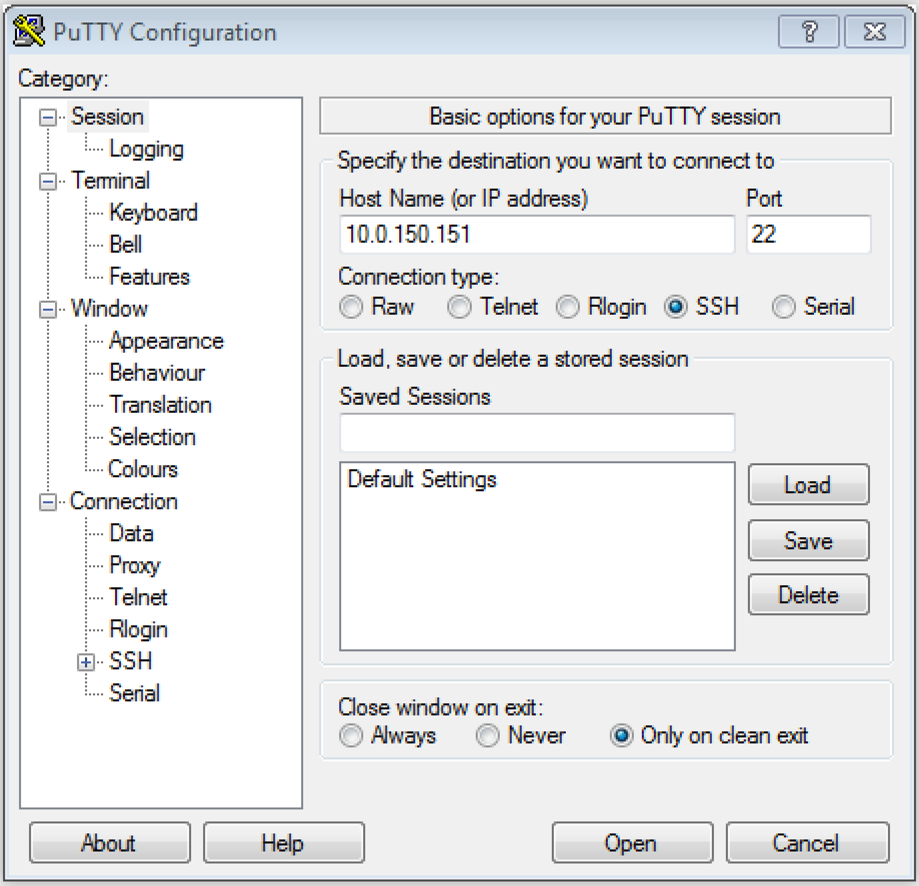
Parameter	Value
General	
Name	`ssh_safe`
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✗
SSH	✓
VNC	✗

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

5.2.3 Establishing connection

PuTTY - SSH client for Microsoft Windows

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



PuTTY Configuration

Category: Session, Logging, Terminal, Keyboard, Bell, Features, Window, Appearance, Behaviour, Translation, Selection, Colours, Connection, Data, Proxy, Telnet, Rlogin, SSH, Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.0.150.151

Port: 22

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

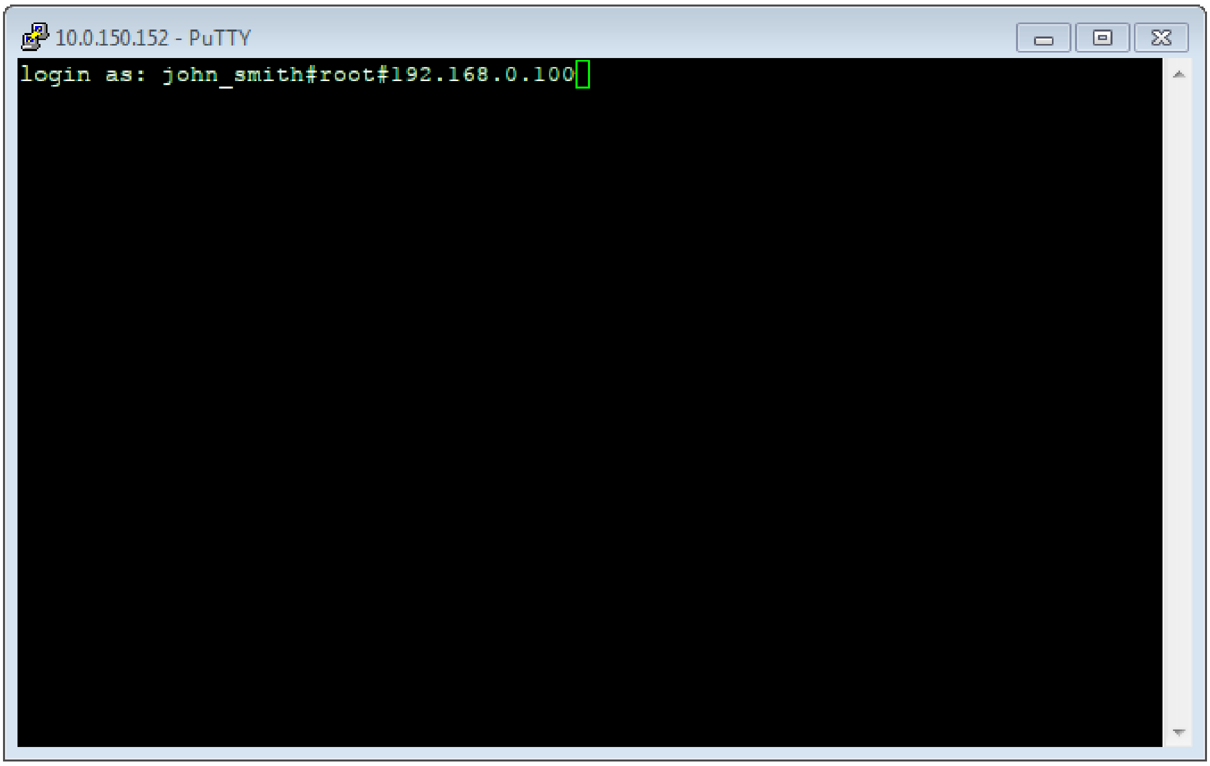
Load, save or delete a stored session

Saved Sessions: Default Settings

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

4. Click *Open*.

5. Enter user name along with account login on the target server and target server address.



10.0.150.152 - PuTTY

```
login as: john_smith#root#192.168.0.100
```

6. Enter password.

Command line interface

Launch terminal and run ssh command using following format:

```
ssh -l <fudo-user>#<server-user>#<server-address> <fudo-address>
```

Example:

```
ssh -l john_smith#root#192.168.0.110 10.0.150.151
```

5.2.4 Viewing user session

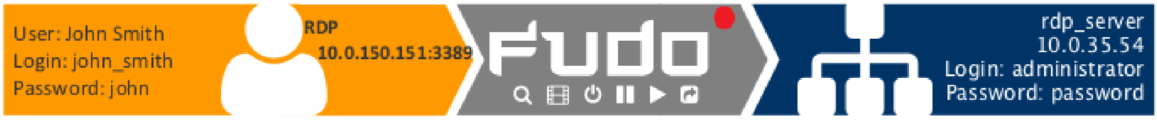
1. Open a web browser and enter the Fudo Enterprise administrator panel IP address.
2. Enter the login and password to login to the Fudo Enterprise administration panel.
3. Select *Management > Sessions*.
4. Find *John Smith's* session and click the playback icon.

Related topics:

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

5.3 RDP

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor RDP access to a remote server. In this scenario, the user connects to the remote server over the *RDP* protocol and logs in to the Fudo Enterprise using an individual login and password combination (`john_smith`/`john`). When establishing the connection with the remote server, Fudo Enterprise substitutes the login with specified in *Account* and the password with the password managed by a password changer (authentication modes are described in the *User authentication modes* section).



5.3.1 Prerequisites

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

5.3.2 Configuration

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 server*.
3. Provide essential configuration parameters:

Parameter	Value
Name	`rdp_server`
Description	✗
Blocked	✗
Protocol	`RDP`
TLS enabled	✓
NLA enabled	✗
Legacy ciphers	✗
Inform about existing connection	✗
Bind address	`10.0.150.151`
Permissions	
Granted users	✗
Destination	
Address	`10.0.35.54`
Mask	`32`
Port	`3389`
Server verification	`None`

4. Click *Save* or *Save and close*.

Adding a user

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.)

enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

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

Parameter	Value
General	
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.

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

5. Click *Save*.

Adding an account

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

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

Parameter	Value
General	
Name	`admin_rdp_server`
Blocked	✗
Type	`regular`
Session recording	`all`
OCR sessions	✓
OCR Language	`English`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`rdp_server`
Credentials	
Domain	✗
Login	`administrator`
Replace secret with	`with password`
Password	`password`
Repeat password	`password`
Password change policy	`Static, without restrictions`

4. Click *Save*.

Defining a safe

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

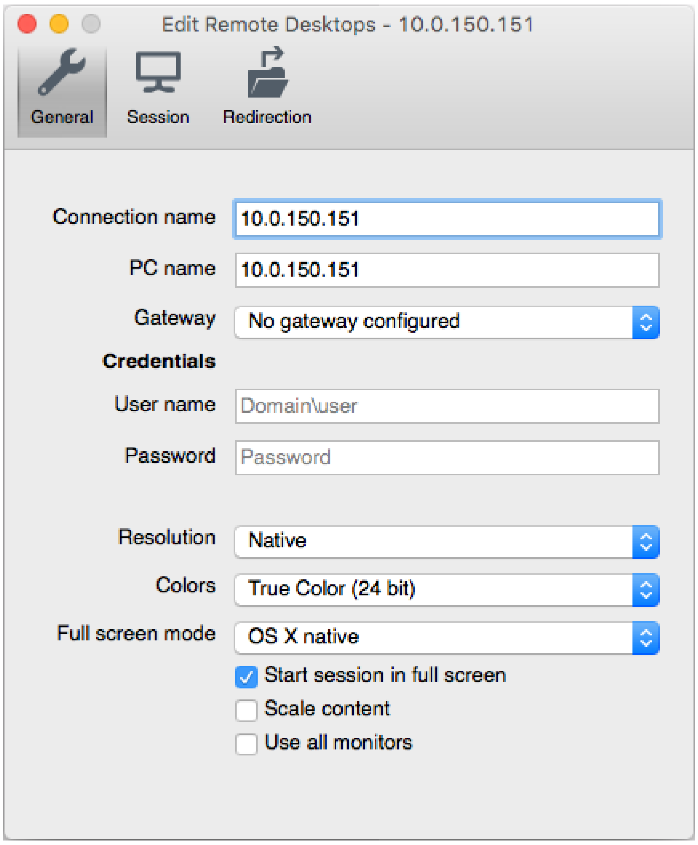
1. Select *Management > Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

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

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

5.3.3 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.



Edit Remote Desktops - 10.0.150.151

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)

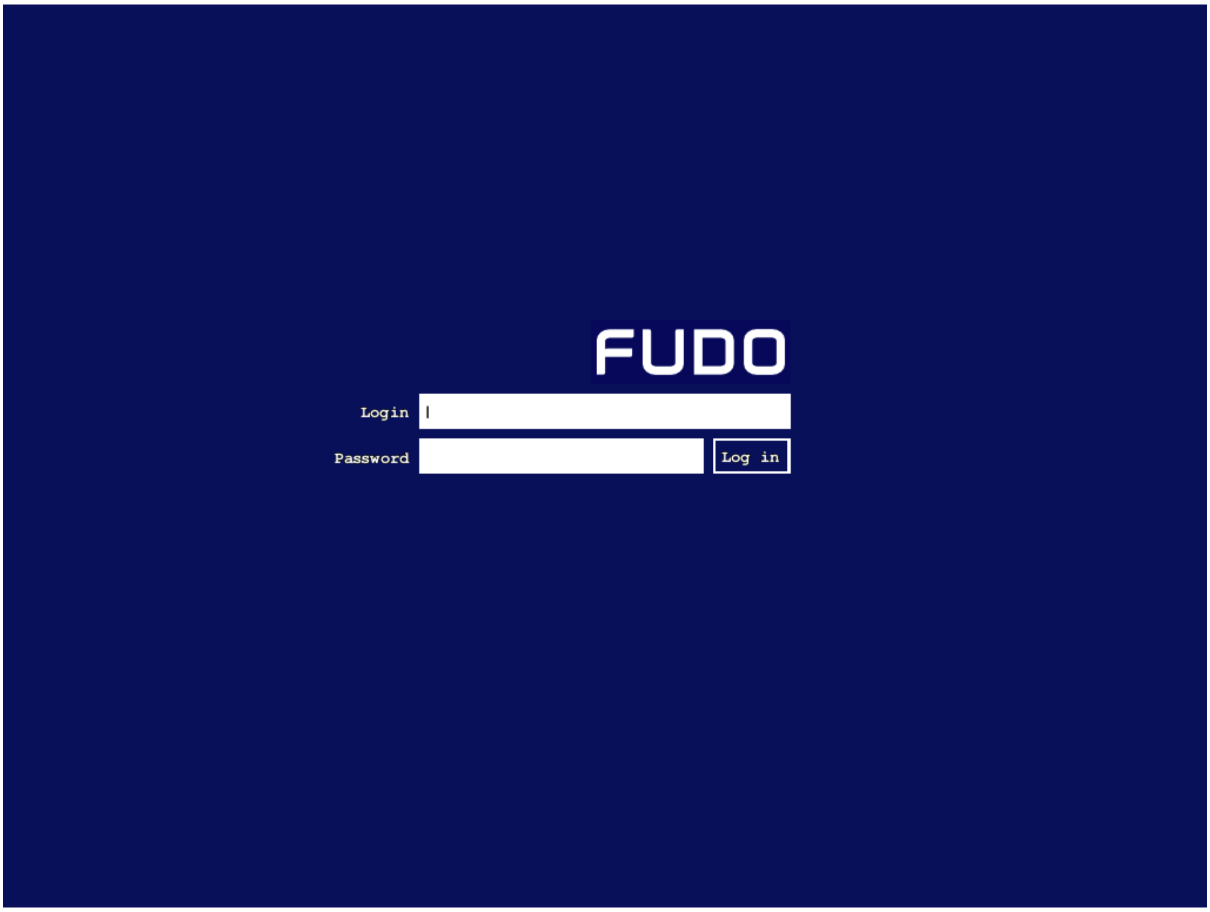
Full screen mode: OS X native

☑ Start session in full screen

□ Scale content

□ Use all monitors

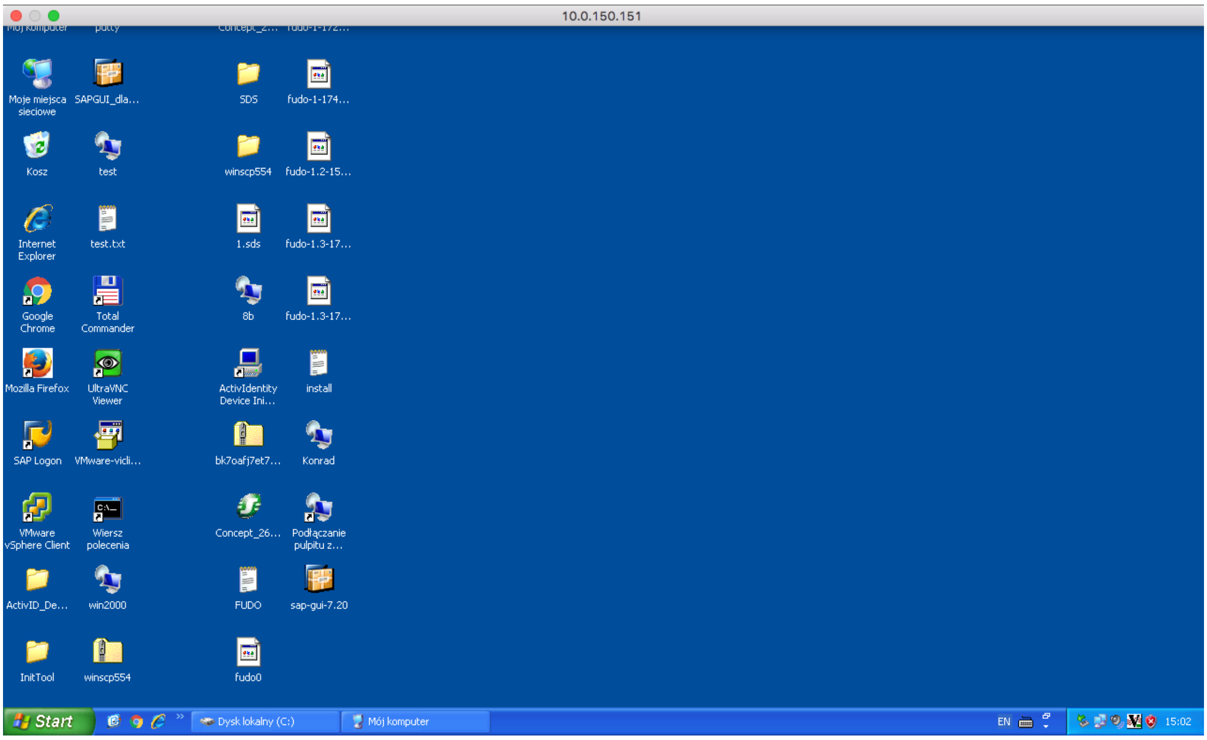
3. Enter user login and password and press the [Enter] keyboard key.



Login: l

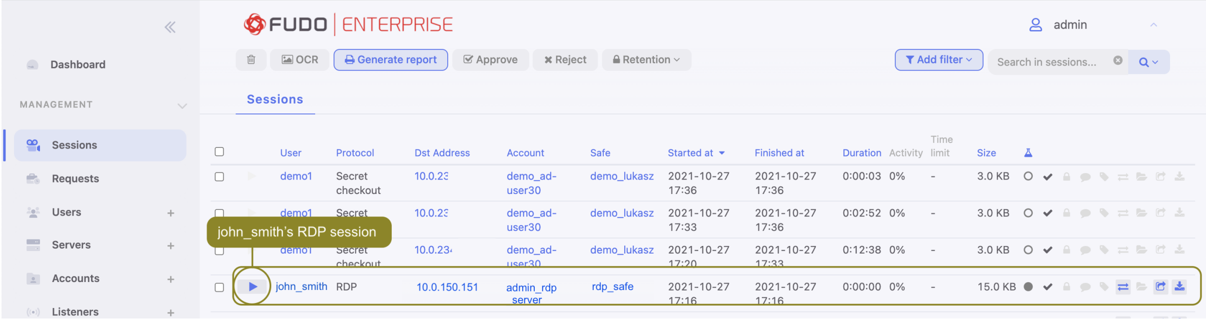
Password:

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



5.3.4 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 Enterprise administration panel.
3. Select *Management > Sessions*.
4. Find *John Smith's* session and click the playback icon.



☐		User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
☐	▶	demo1	Secret checkout	10.0.23	demo_ad-user30	demo_lukasz	2021-10-27 17:36	2021-10-27 17:36	0:00:03	0%	-	3.0 KB
☐	▶	demo1	Secret	10.0.23	demo_ad-user30	demo_lukasz	2021-10-27 17:33	2021-10-27 17:36	0:02:52	0%	-	3.0 KB
☐		demo1	Secret checkout	10.0.23	demo_ad-user30	demo_lukasz	2021-10-27 17:20	2021-10-27 17:33	0:12:38	0%	-	3.0 KB
☐	▶	john_smith	RDP	10.0.150.151	admin_rdp server	rdp_safe	2021-10-27 17:16	2021-10-27 17:16	0:00:00	0%	-	15.0 KB

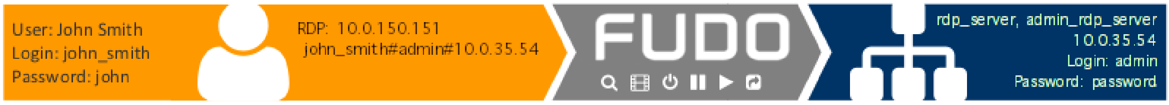
Related topics:

- *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*

5.4 RDP in bastion mode

This chapter contains an example of a basic Fudo Enterprise configuration, to monitor RDP access to a remote server. In this scenario, the user connects to the remote server in bastion mode by specifying the user name along with account login on the target server and target server address in the login string. Bastion mode enables facilitating privileged accounts monitoring while preserving default protocols port numbers.



5.4.1 Prerequisites

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

5.4.2 Configuration

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 server*.
3. Provide essential configuration parameters:

Parameter	Value
Name	`rdp_server`
Description	✗
Blocked	✗
Protocol	`RDP`
TLS enabled	✓
NLA enabled	✗
Legacy ciphers	✗
Inform about existing connection	✗
Bind address	`10.0.150.151`
Permissions	
Granted users	✗
Destination	
Address	`10.0.35.54`
Mask	`32`
Port	`3389`
Server verification	`None`

4. Click *Save* or *Save and close.*

Adding a user

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

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

Parameter	Value
General	
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.

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

5. Click *Save*.

Adding an account

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

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

Parameter	Value
General	
Name	`admin_rdp_server`
Blocked	✗
Type	`regular`
Session recording	`all`
OCR sessions	✓
OCR Language	`English`
Notes	✗
Data retention	
Override global retention settings	✗
Delete session data after	`61` days
Permissions	
Granted users	✗
Server	
Server	`rdp_server`
Credentials	
Domain	✗
Login	`admin`
Replace secret with	`with password`
Password	`password`
Repeat password	`password`
Password change policy	`Static, without restrictions`

4. Click *Save*.

Defining a safe

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

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

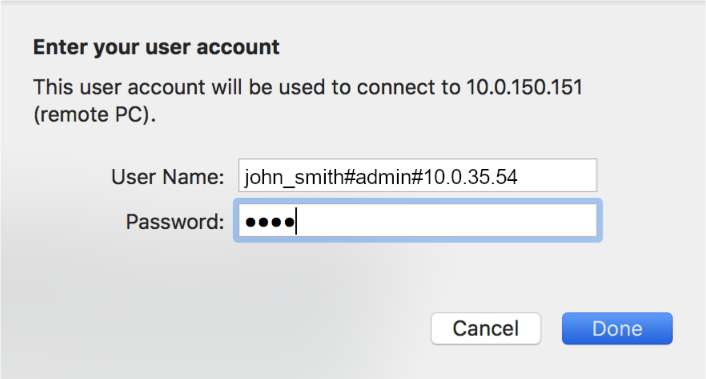
Parameter	Value
General	
Name	`rdp_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Protocol functionality	
RDP	✓
SSH	✗
VNC	✗

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

5.4.3 Establishing an RDP connection with a remote host

1. Launch RDP client of your choice.
2. Enter destination host IP address and RDP service port number.
3. Enter user name along with account login on the target server (server login) and target server address (`john_smith#admin#10.0.35.54`) and provide password.

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



Enter your user account

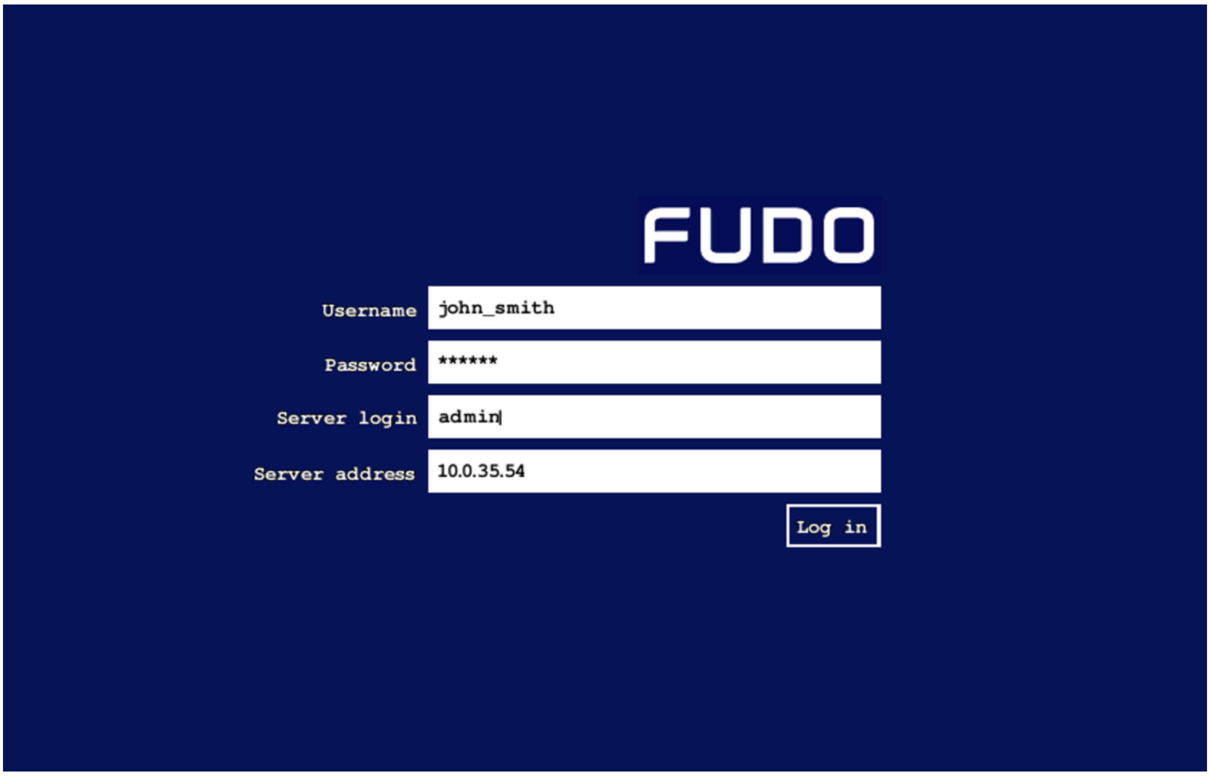
This user account will be used to connect to 10.0.150.151 (remote PC).

User Name: john_smith#admin#10.0.35.54

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.
- When connecting using the forward account, where the Username and Server login are identical, the Server login field may be omitted on the login screen.
- In case the specified account is not found, Fudo Enterprise will try to match the name with a server object. If a matching server is not found, system tries to match the string to a host's DNS name.
- Fudo Enterprise enables using a custom logo on the login screen for RDP and VNC connections. For more information refer to the *Resources* topic.

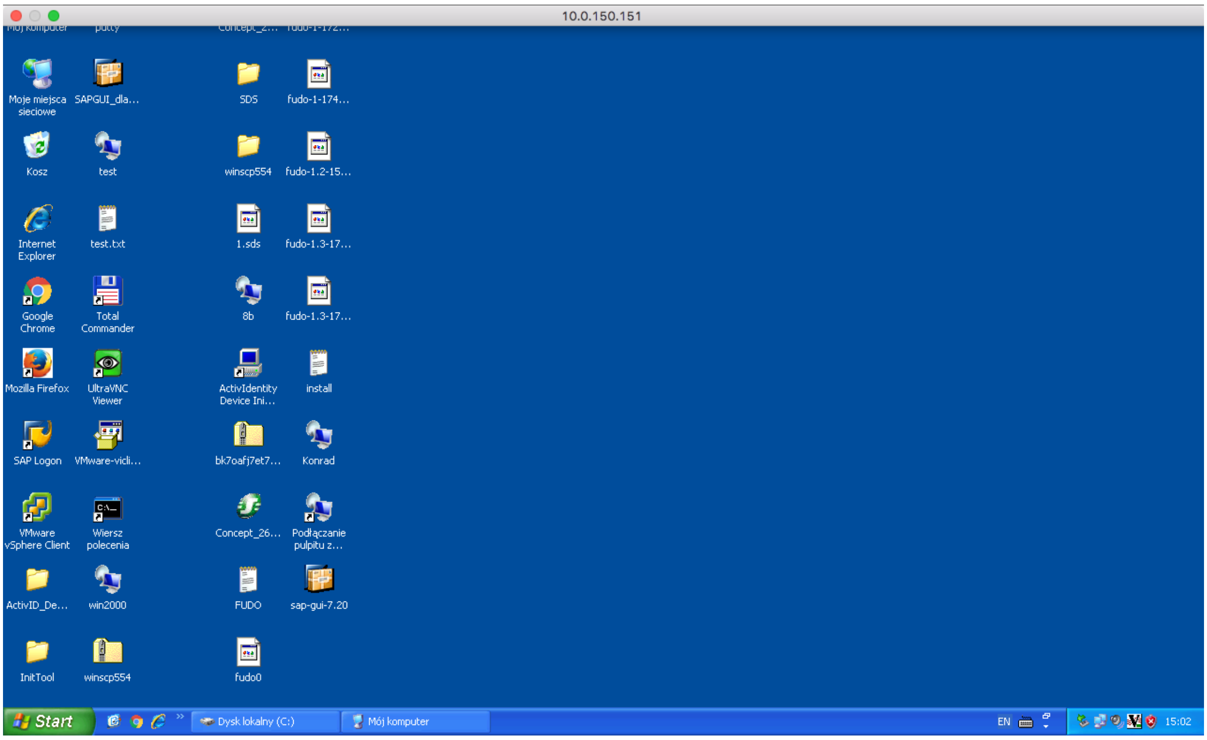


Username john_smith

Password ******

Server login admin

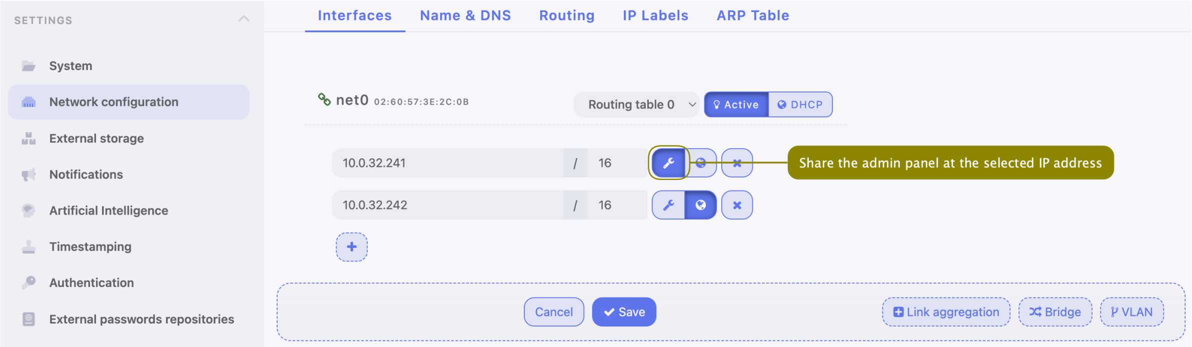
Server address 10.0.35.54



5.4.4 Viewing user session

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

Note: Make sure that the entered IP address has the control panel sharing option enabled in the *Network configuration* settings.



net0 02:60:57:3E:2C:0B

Routing table 0

Active

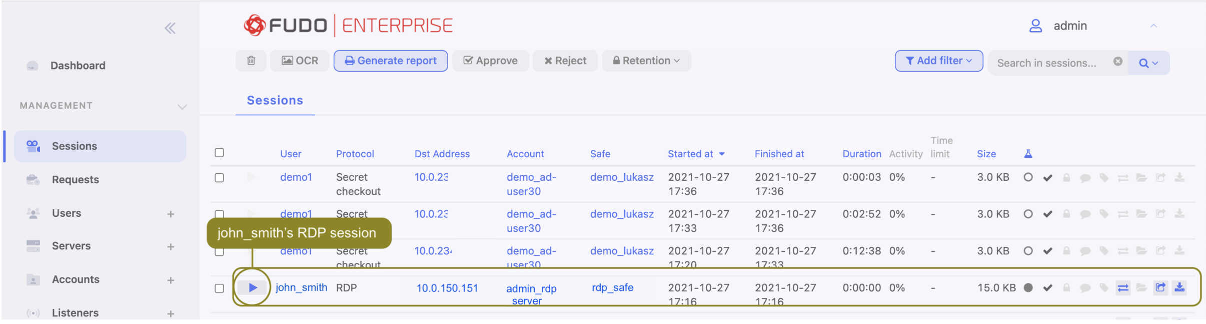
DHCP

10.0.32.241 / 16

Share the admin panel at the selected IP address

10.0.32.242 / 16

2. Enter the login and password to login to the Fudo Enterprise administration panel.
3. Select *Management > Sessions*.
4. Find *John Smith's* session and click the playback icon.



john_smith's RDP session

		User	Protocol	Dst Address	Account	Safe	Started at ▾	Finished at	Duration	Activity	Time limit	Size
□		demo1	Secret checkout	10.0.23	demo_ad-user30	demo_lukasz	2021-10-27 17:36	2021-10-27 17:36	0:00:03	0%	-	3.0 KB
□		demo1	Secret checkout	10.0.23	demo_ad-user30	demo_lukasz	2021-10-27 17:33	2021-10-27 17:36	0:02:52	0%	-	3.0 KB
□		demo1	Secret checkout	10.0.23	demo_ad-user30	demo_lukasz	2021-10-27 17:20	2021-10-27 17:33	0:12:38	0%	-	3.0 KB
□	▶	john_smith	RDP	10.0.150.151	admin_rdp server	rdp_safe	2021-10-27 17:16	2021-10-27 17:16	0:00:00	0%	-	15.0 KB

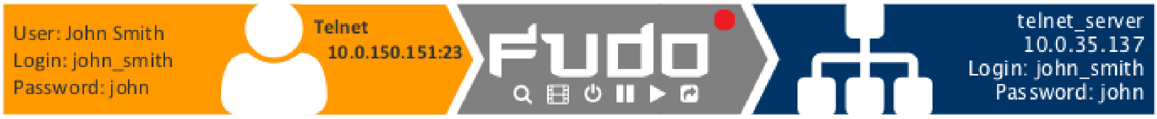
Related topics:

- *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*

5.5 Telnet

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

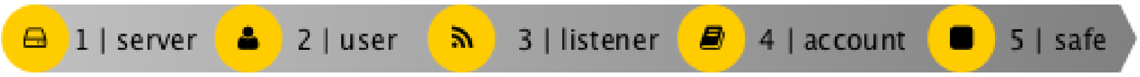
Note: Telnet connections do not support login credentials forwarding and login credentials substitution. When connecting to target host over telnet protocol, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise and then again, to connect to the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



5.5.1 Prerequisites

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

5.5.2 Configuration



Adding a server

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

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

Parameter	Value
General	
Name	`telnet_server`
Description	✗
Blocked	✗
Protocol	`Telnet 5250`
TLS enabled	✗
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.35.137`
Mask	32
Port	23

4. Click *Save* or *Save and close*.

Adding a user

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

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

3. Provide essential user information:

Parameter	Value
General	
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*.

5.5.3 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 Enterprise:

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

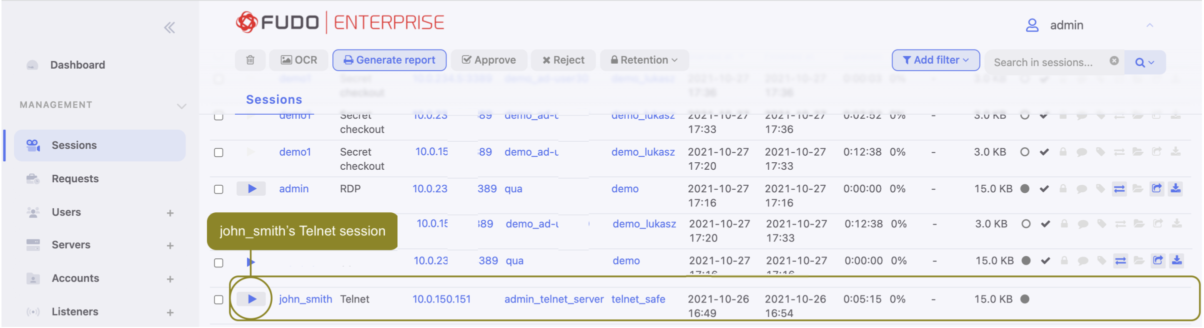
4. Provide user authentication information defined on the target host:

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

Note: Telnet connections do not support user credentials substitution.

5.5.4 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 Enterprise administration panel.
3. Select *Management > Sessions*.
4. Find *John Smith's* session and click the playback icon.



john_smith's Telnet session

□		demo1	Secret checkout	10.0.23	89	demo_ad-u	demo_lukasz	2021-10-27 17:33	2021-10-27 17:36	0:02:52	0%	-	3.0 KB ○ ✓
□		demo1	Secret checkout	10.0.15	89	demo_ad-u	demo_lukasz	2021-10-27 17:20	2021-10-27 17:33	0:12:38	0%	-	3.0 KB ○ ✓
□	▶	admin	RDP	10.0.23	389	qua	demo	2021-10-27 17:16	2021-10-27 17:16	0:00:00	0%	-	15.0 KB ● ✓
				10.0.15	89	demo_ad-u	demo_lukasz	2021-10-27 17:20	2021-10-27 17:33	0:12:38	0%	-	3.0 KB ○ ✓
□	▶			10.0.23	389	qua	demo	2021-10-27	2021-10-27	0:00:00	0%	-	15.0 KB ● ✓
□	▶	john_smith	Telnet	10.0.150.151		admin_telnet_server	telnet_safe	2021-10-26 16:49	2021-10-26 16:54	0:05:15	0%	-	15.0 KB ●

Related topics:

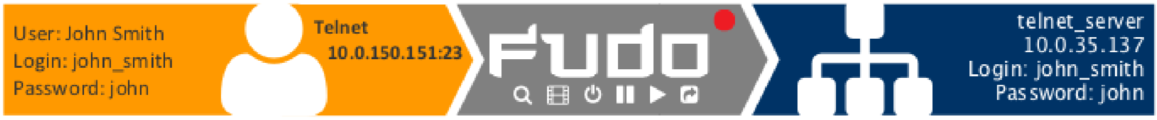
- *Quick start - SSH connection configuration*
- *Quick start - HTTP connection configuration*
- *Quick start - MySQL connection configuration*
- *Quick start - RDP connection configuration*
- *Requirements*

- *Data model*
- *Resources*

5.6 Telnet 5250

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

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



5.6.1 Prerequisites

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

5.6.2 Configuration

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 5250`
TLS enabled	❌
Bind address	`Any`
Permissions	
Granted users	❌
Destination	
Address	`10.0.35.137`
Mask	`32`
Port	`23`

4. Click *Save* or *Save and close*.

Adding a user

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

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

Parameter	Value
General	
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	✗

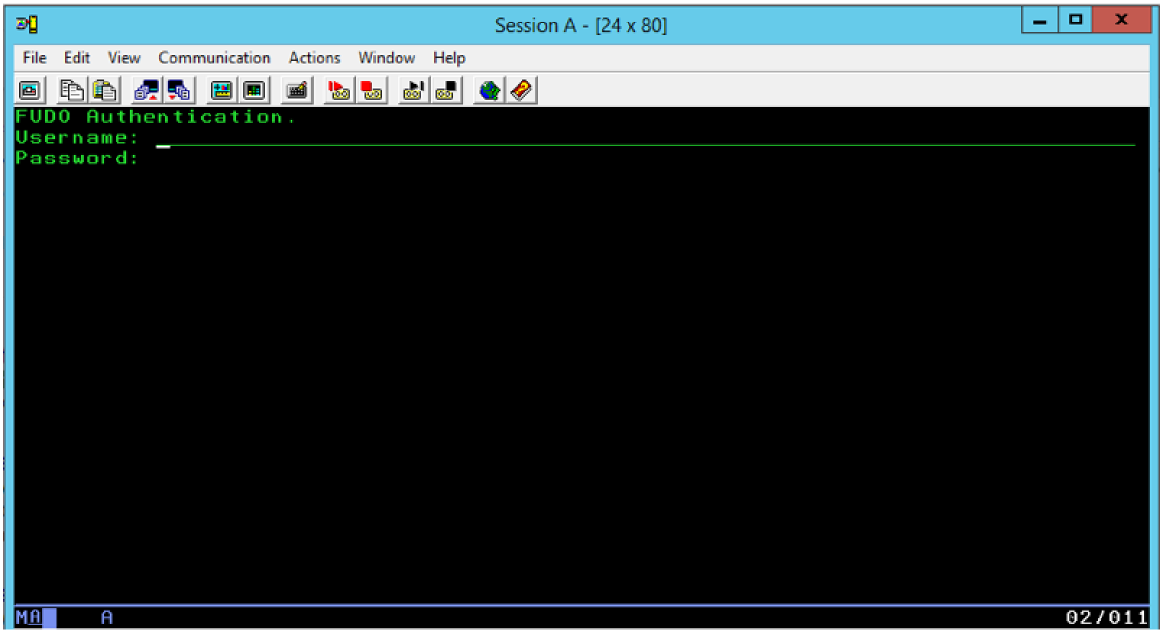
4. Select *Users* tab.
5. Click *+ Add user*.
6. Find *John* and click +.
7. Click *OK*.
8. Select *Accounts* tab.
9. Click *+ Add account*.
10. Find the `admin_telnet_server` object and click +.
11. Click *OK*.
12. Click ✎ in the *Listeners* column.
13. Find the `telnet_listener` object and click +.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

5.6.3 Establishing a telnet connection with the remote host

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

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

3. Provide user authentication information defined on Fudo Enterprise:

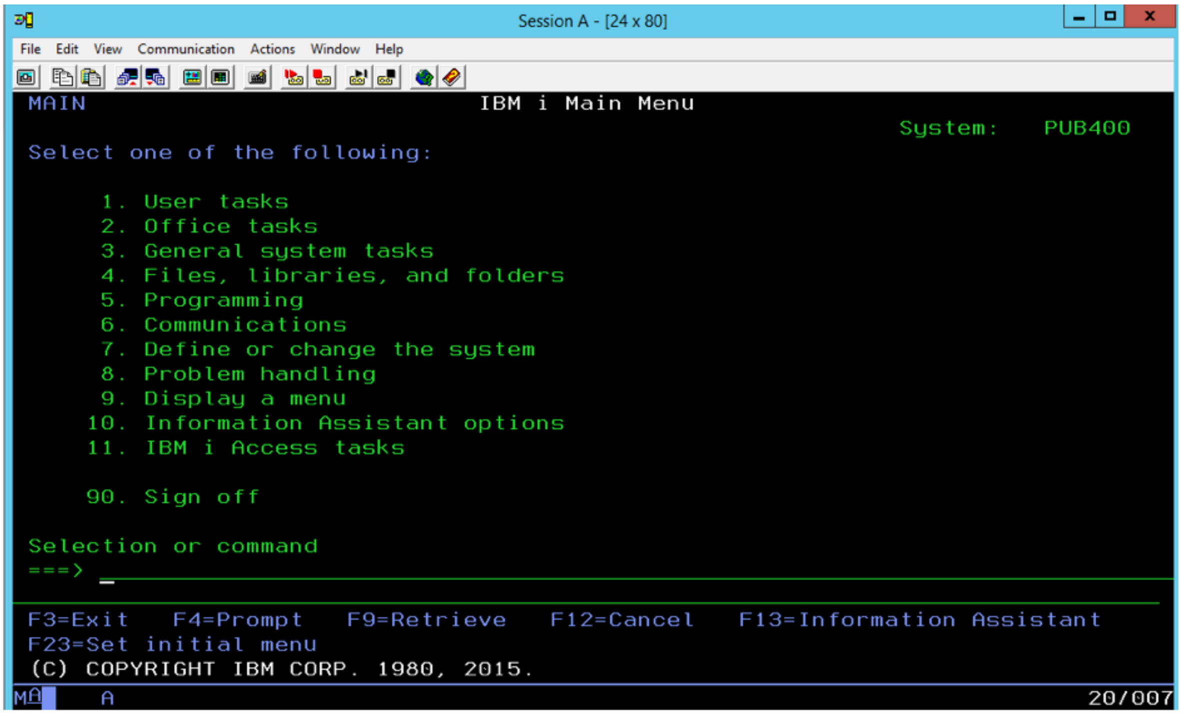


```
FUDO Authentication.
Username:
Password:
```

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

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

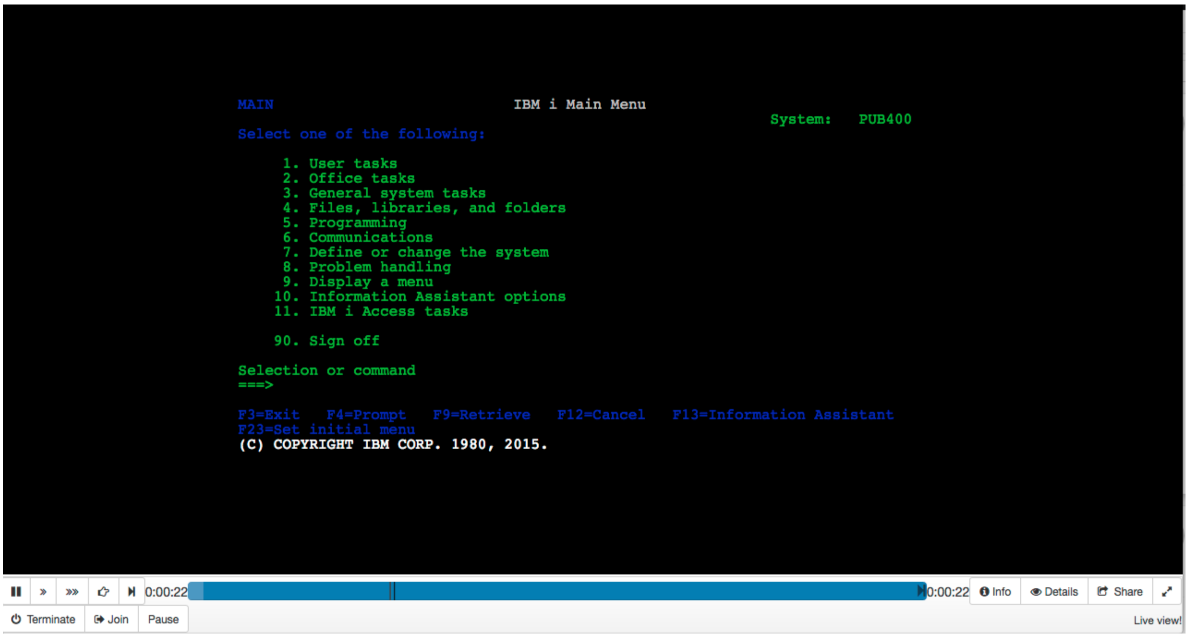
Note: Telnet connections do not support user credentials substitution.



```
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
```

5.6.4 Viewing user's session

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



```
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:

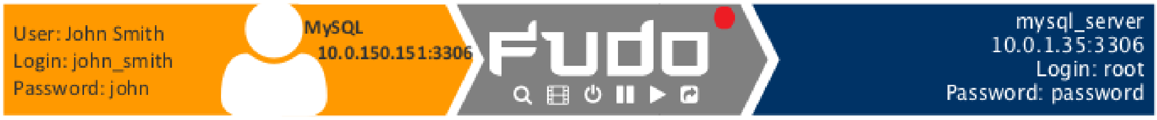
- *Quick start - SSH connection configuration*

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

5.7 MySQL

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

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



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

5.7.1 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.

5.7.2 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 server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`mysql_server`
Description	✗
Blocked	✗
Protocol	`MySQL`
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.1.35`
Mask	32
Port	3306

4. Click *Save* or *Save and close*.

Adding a user

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

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

Parameter	Value
General	
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.

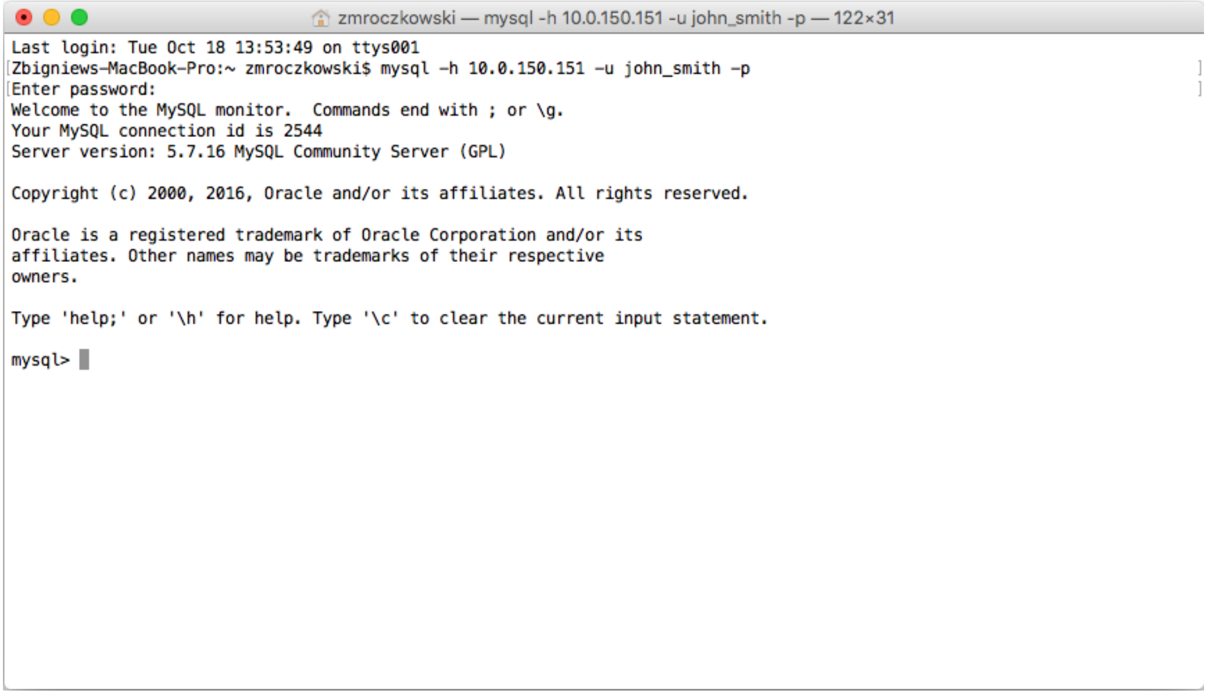
1. Select *Management > Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

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*.

5.7.3 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.

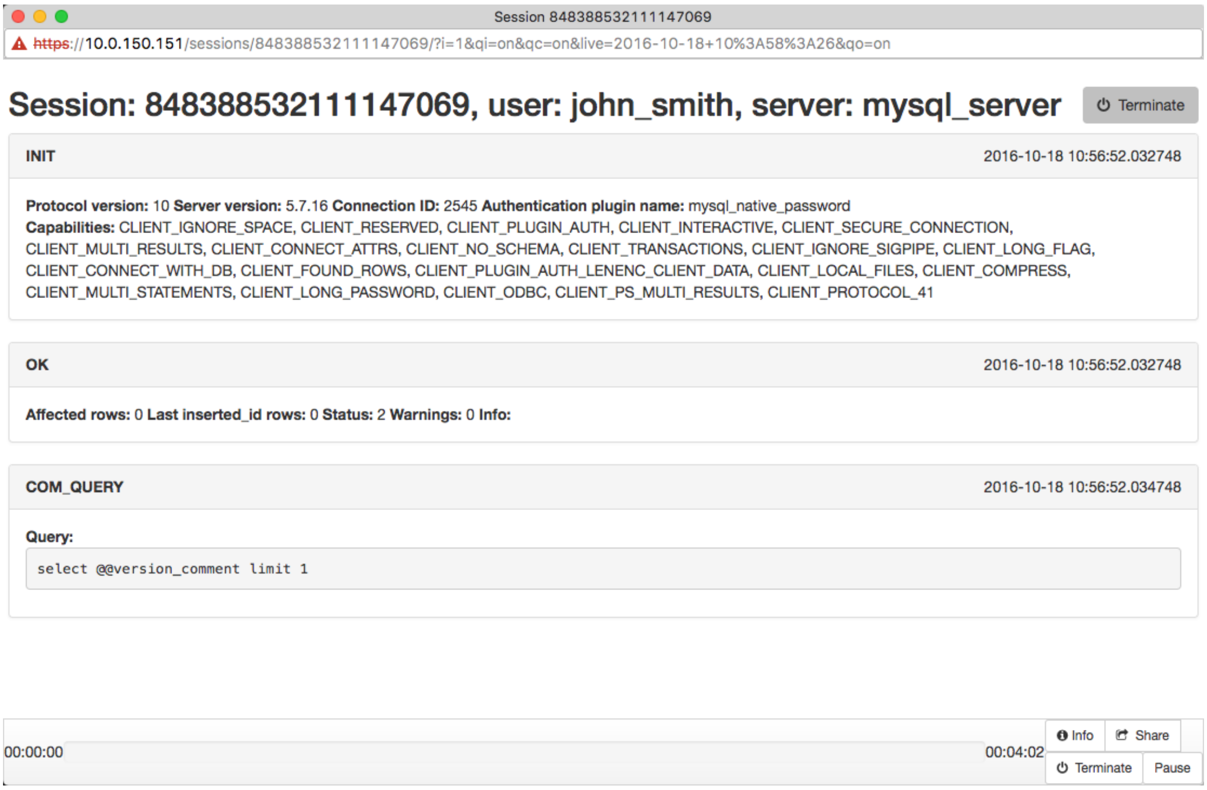

zmroczkowski — mysql -h 10.0.150.151 -u john_smith -p — 122×31

```
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.

5.7.4 Viewing user session

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


Session 848388532111147069
https://10.0.150.151/sessions/848388532111147069/?i=1&qi=on&qc=on&live=2016-10-18+10%3A58%3A26&qo=on
Terminate
00:00:00
00:04:02
Info
Share
Terminate
Pause

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
```

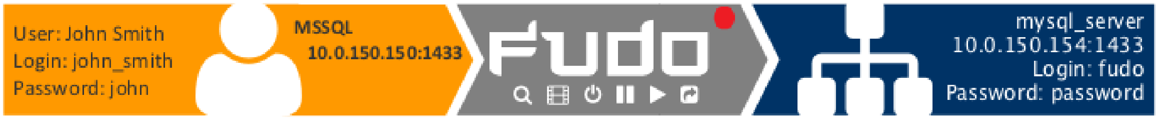
Related topics:

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

5.8 MS SQL

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

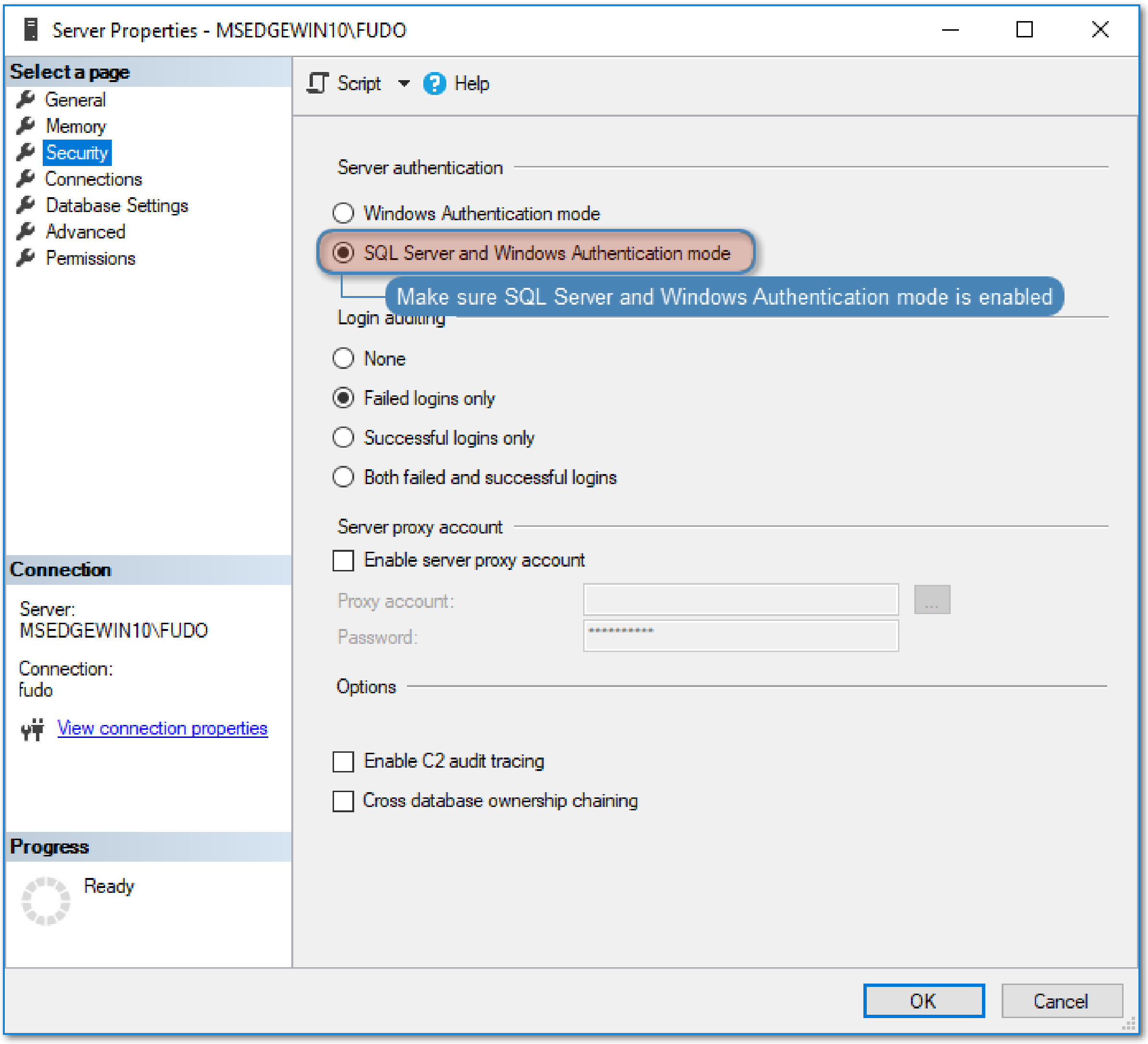
In this scenario, the user connects to a MS SQL database using individual login and password using *SQL Server Management Studio*. When establishing the connection with the remote server, Fudo Enterprise substitutes the login and the password with the previously defined values: `fudo`/`password` (authorization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



5.8.1 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

Script ▾ Help

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

View connection properties

Progress

Ready

OK Cancel

5.8.2 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 server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`mssql_server`
Description	✗
Blocked	✗
Protocol	`MS SQL (TDS)`
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.150.154`
Mask	`32`
Port	`1433`

4. Click *Save* or *Save and close*.

Adding a user

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

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

Parameter	Value
General	
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.

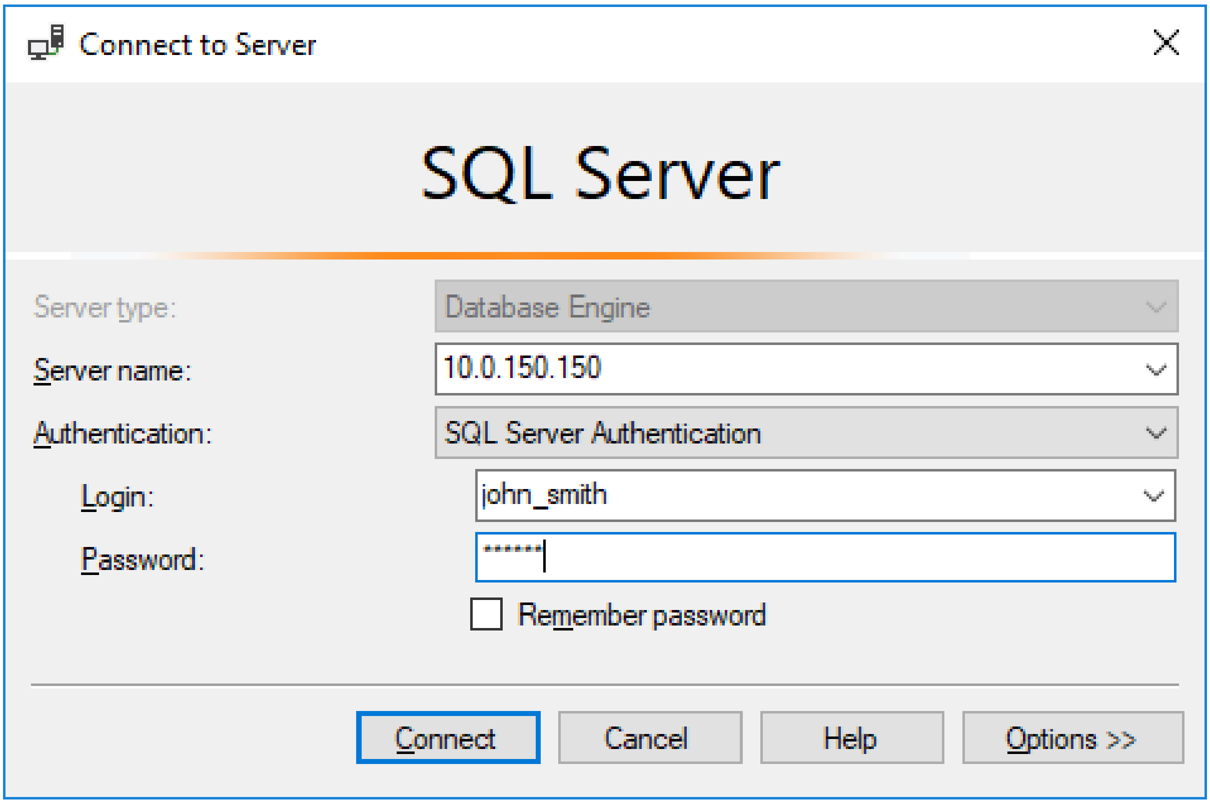
1. Select *Management > Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

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*.

5.8.3 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*.



Connect to Server

SQL Server

Server type: Database Engine

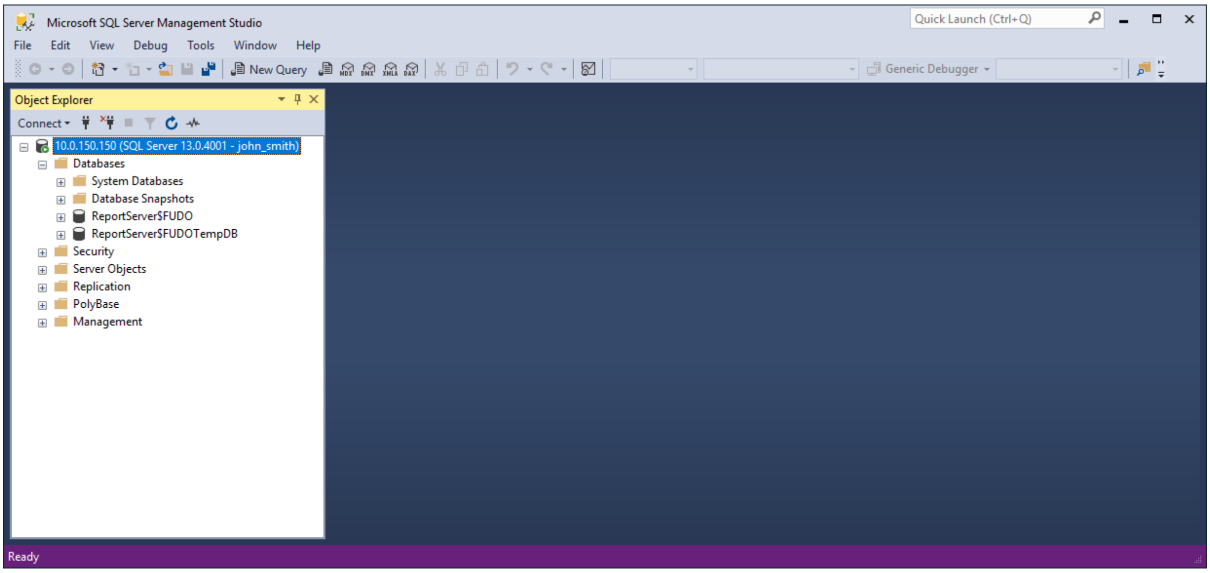
Server name: 10.0.150.150

Authentication: SQL Server Authentication

Login: john_smith

Password: ******

□ Remember password



10.0.150.150 (SQL Server 13.0.4001 - john_smith)
- Databases
  - System Databases
  - Database Snapshots
  - ReportServer$FUDO
  - ReportServer$FUDOTempDB
- Security
- Server Objects
- Replication
- PolyBase
- Management

5.8.4 Viewing user session

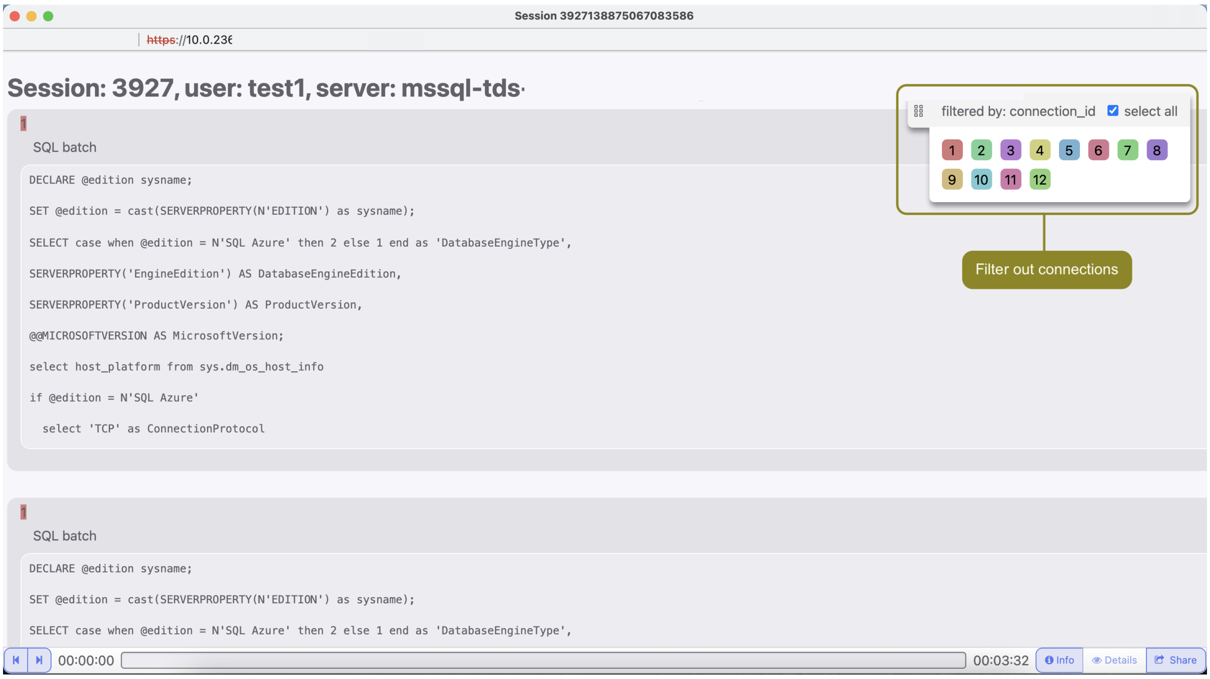
1. Open a web browser and go to the Fudo Enterprise administration page.
2. Enter user login and password to log in to Fudo Enterprise administration panel.
3. Select *Management* > *Sessions*.
4. Find *John Smith's* session and click ▶.

Note: Due to the fact that MS SQL Studio may create multiple connections for sending internal queries, the sessions, connected via the TDS layer protocol using MS SQL Studio are getting aggregated by Fudo Enterprise.

Fudo Enterprise follows an algorithm that verifies if there is an already connected session on a current node. If the algorithm identifies that the main connection objects (`listener`, `account`, `server address (server)`, `user`, and `safe`) of the new session are correlating with already existing session, both sessions are aggregated into one.

If the main connection objects of the new session are not correlating with any of already existing sessions, a new session is created.

This makes multiple queries to be grouped within one session. Every query has a unique tag that allows filtering important connections with users' queries in the Fudo Enterprise player.


Session 3927138875067083586
https://10.0.236
Session: 3927, user: test1, server: mssql-tds
filtered by: connection_id
☑ select all
1
2
3
4
5
6
7
8
9
10
11
12
Filter out connections
00:00:00
00:03:32
Info
Details
Share

1

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',

SERVERPROPERTY('EngineEdition') AS DatabaseEngineEdition,

SERVERPROPERTY('ProductVersion') AS ProductVersion,

@@MICROSOFTVERSION AS MicrosoftVersion;

select host_platform from sys.dm_os_host_info

if @edition = N'SQL Azure'

  select 'TCP' as ConnectionProtocol
```

1

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',
```

Related topics:

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

5.9 HTTP

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

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

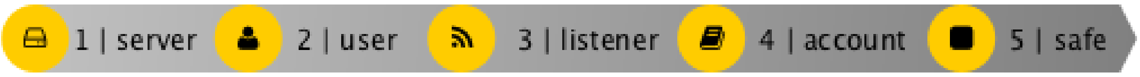
Model	Maximum recommended number of concurrent HTTP sessions*
F100x	2
F300x	5
F500x	10

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

5.9.1 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.

5.9.2 Configuration



Adding a server

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

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

Parameter	Value
General	
Name	`twitter`
Description	✗
Blocked	✗
Protocol	`HTTP`
TLS enabled	✓
Legacy ciphers	✗
HTTP host	✗
HTTP timeout	`900`
HTTP Authentication	`Twitter`
Bind address	`10.0.236.70`
Permissions	
Granted users	✗
Destination	
Address	`twitter.com`
Port	`443`
Server verification	`None`

4. Click *Save* or *Save and close*.

Adding a user

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

1. Select *Management > Users*.

2. Click *+ Add*.

3. Provide essential user information:

Parameter	Value
General	
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:

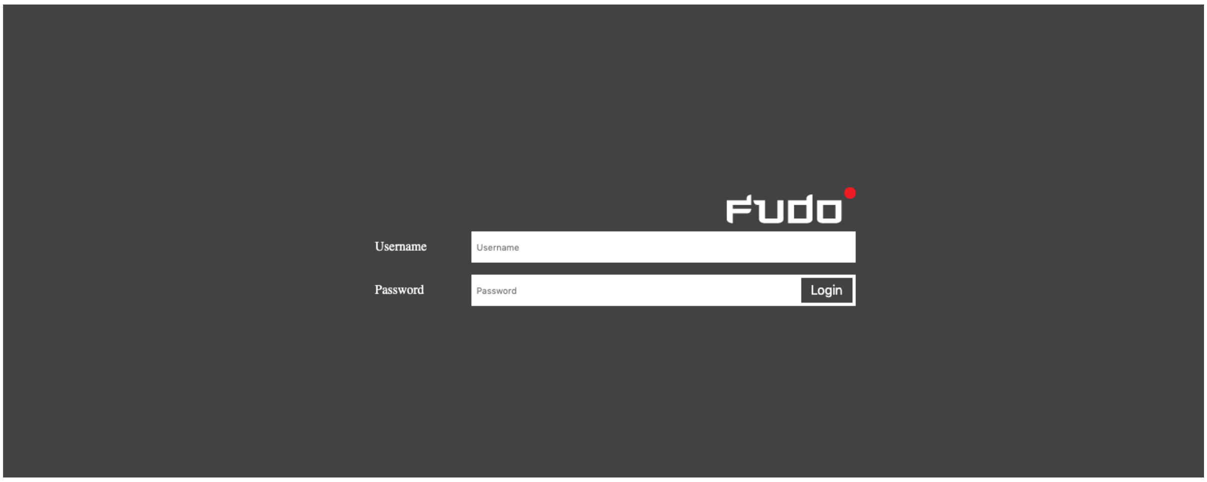
Parameter	Value
General	
Name	`twitter_safe`
Blocked	✗
Notifications	✗
Login reason	✗
Require approval	✗
Policies	✗
Note access	`No access`
Users	`john_smith`
Protocol functionality	
RDP	✗
SSH	✗
VNC	✗

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*.

5.9.3 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.

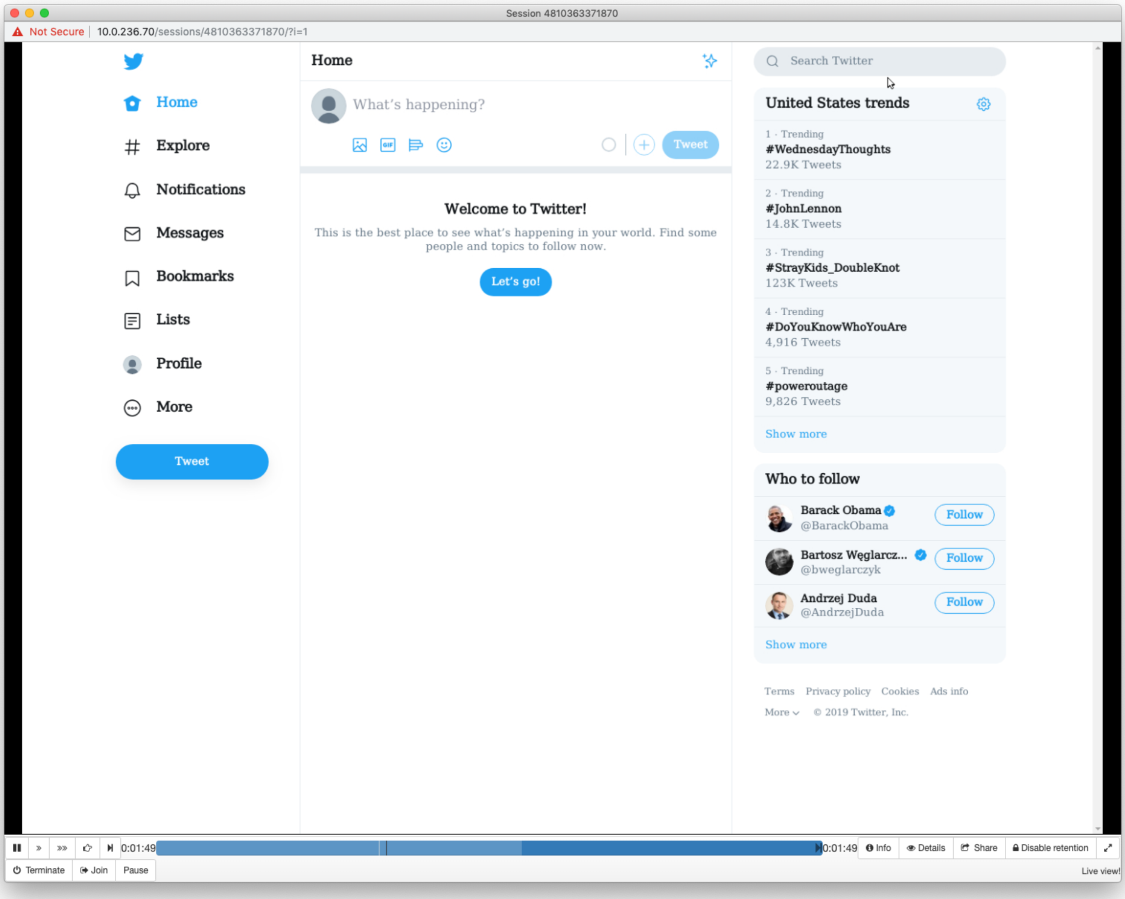
Note: In case you are authenticating using two factors, input your static password along with the dynamic factor (token value) in the password field as a single string of characters.



4. Continue browsing the website.

5.9.4 Viewing user session

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



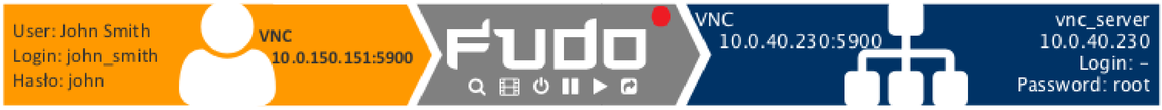
Related topics:

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

5.10 VNC

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

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



5.10.1 Prerequisites

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

5.10.2 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 server*.
3. Provide essential configuration parameters:

Parameter	Value
General	
Name	`vnc_server`
Description	✗
Blocked	✗
Protocol	`VNC`
Bind address	`Any`
Permissions	
Granted users	✗
Destination	
Address	`10.0.40.230`
Mask	32
Port	5900

4. Click *Save* or *Save and close*.

Adding a user

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

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

Parameter	Value
General	
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.

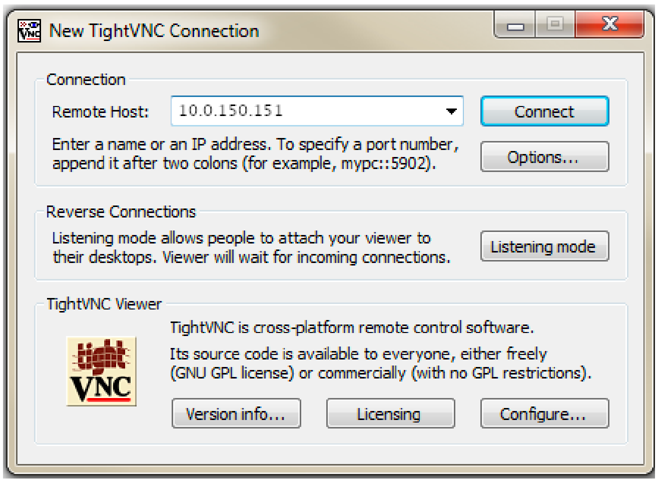
1. Select *Management > Safes*.
2. Click *+ Add*.
3. Provide essential configuration parameters:

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*.

5.10.3 Establishing connection

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



New TightVNC Connection

Connection

Remote Host: 10.0.150.151

Enter a name or an IP address. To specify a port number, append it after two colons (for example, mypc::5902).

Reverse Connections

Listening mode allows people to attach your viewer to their desktops. Viewer will wait for incoming connections.

TightVNC Viewer

TightVNC is cross-platform remote control software.

Its source code is available to everyone, either freely (GNU GPL license) or commercially (with no GPL restrictions).

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

5.10.4 Viewing user session

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

Related topics:

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

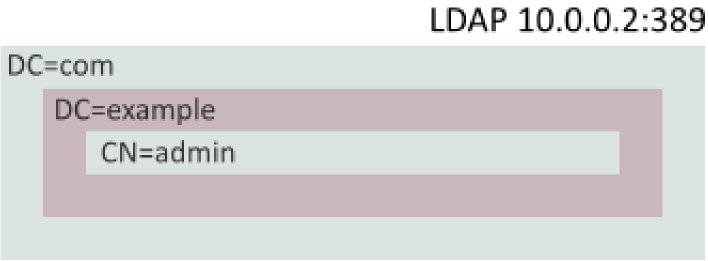
5.11 User authentication against external LDAP server

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

5.11.1 Prerequisites

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

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

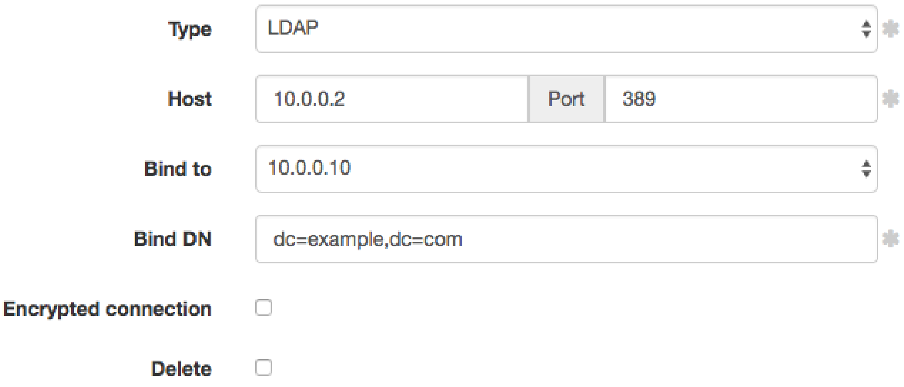


5.11.2 Configuration

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*.

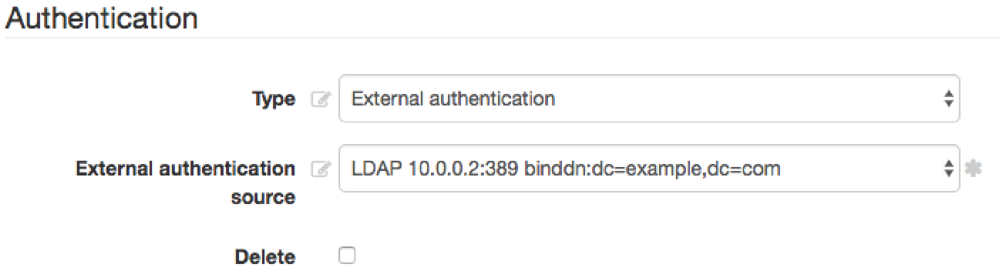
Adding user authentication method

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*.

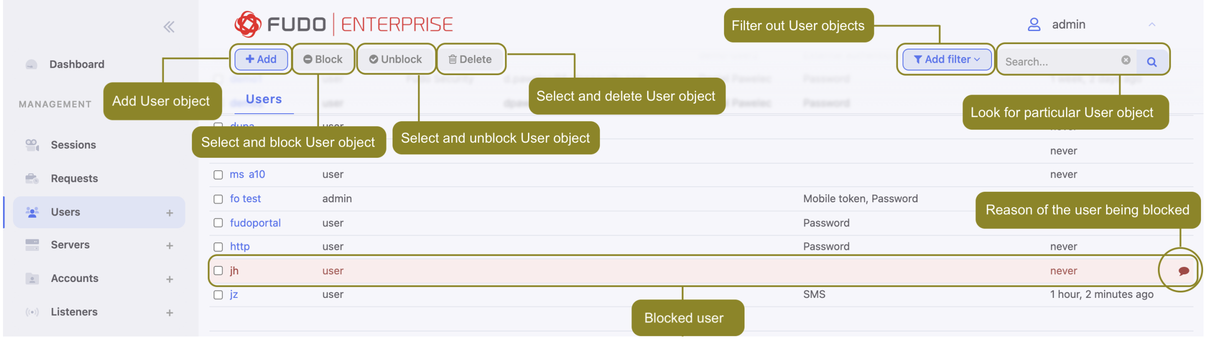
Related topics:

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

CHAPTER 6

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.



☐ ms a10	user		never
☐ fo test	admin	Mobile token, Password	
☐ fudoportal	user	Password	
☐ http	user	Password	never
☐ jh	user		never
☐ jz	user	SMS	1 hour, 2 minutes ago

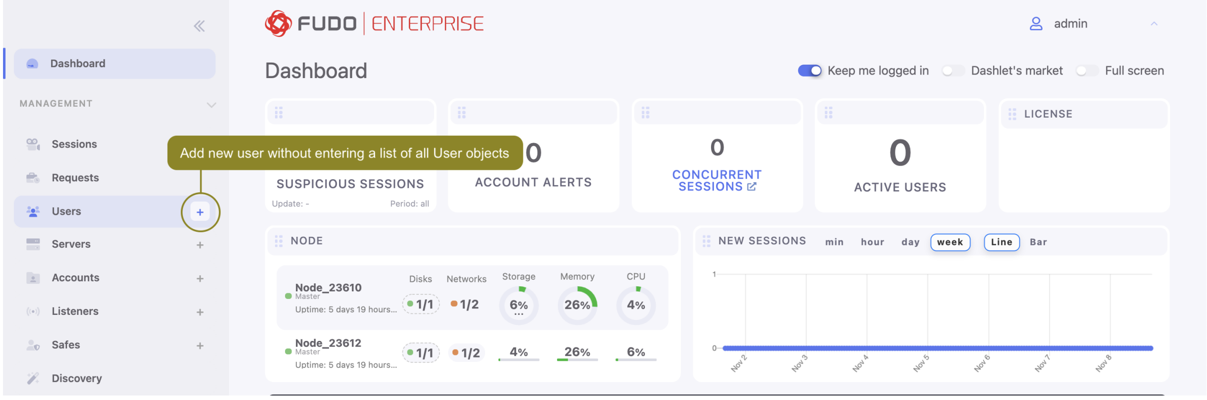
Note: Fudo Enterprise allows importing users definitions from directory services such as Active Directory or LDAP. For more information on users synchronization service, refer to the *Users synchronization* topic.

6.1 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 Enterprise. Supportable MySQL plugins by Fudo Enterprise are `mysql_native_password` and `mysql_old_password`. Server plugin should be set to `mysql_native_password` in `/etc/mysql/mysql.conf.d/mysqld.cnf` and a User object is created with `mysql_native_password` plugin.

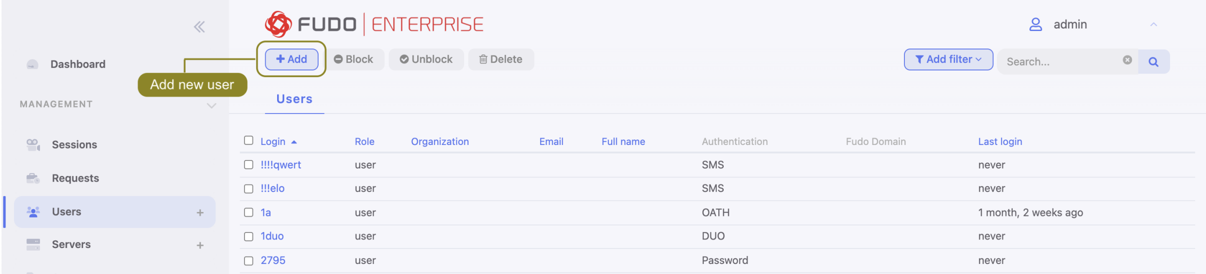
1. Click + icon next to the *Users* tab of the *Management* sub-section,



Add new user without entering a list of all User objects

or

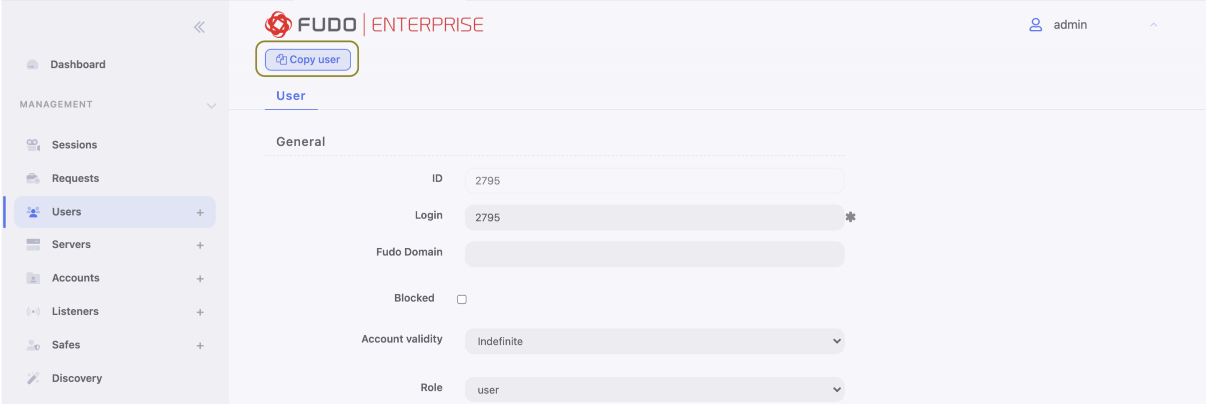
1. Select *Management* > *Users* and then click + *Add*.



Add new user

Login	Role	Organization	Email	Full name	Authentication	Fudo Domain	Last login
!!!!qwert	user				SMS		never
!!!elo	user				SMS		never
1a	user				OATH		1 month, 2 weeks ago
1duo	user				DUO		never
2795	user				Password		never

Note: Fudo Enterprise 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.



General

ID: 2795

Login: 2795 *

Fudo Domain:

Blocked: □

Account validity: Indefinite

Role: user

---

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.

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

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 Enterprise.
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.

Continued on next page

Table 1 – continued from previous page

Role	Access rights
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. • Managing 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.
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.

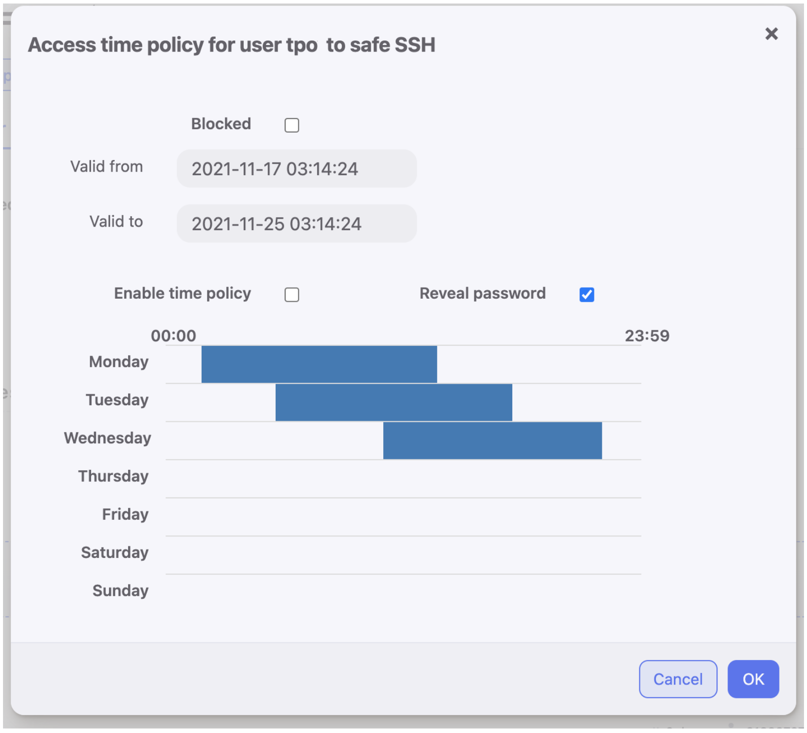
8. Select user's preferred language in Fudo Enterprise administration panel.

Note: List of available languages is specified in the license.

9. Grant access to safes.

Note:

- Drag and drop safe objects to change the order in which safes are processed upon establishing connection.
- Click safe to define *time access policy*.
- Click *Reveal password* option to enable displaying password on User Portal (Access Gateway).



Access time policy for user tpo to safe SSH

Blocked □

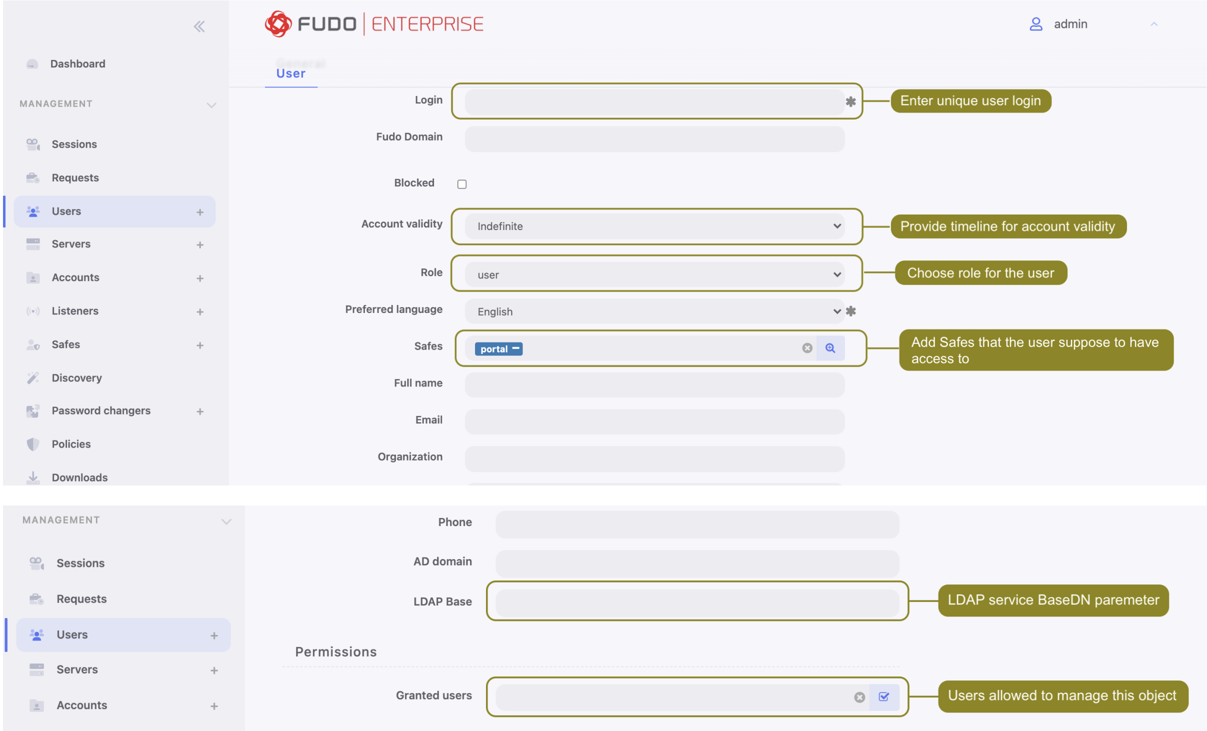
Valid from 2021-11-17 03:14:24

Valid to 2021-11-25 03:14:24

Enable time policy □ Reveal password ☑

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 Enterprise will report authentication problem as it cannot determine which user is trying to connect.



Login: Enter unique user login

Fudo Domain

Blocked □

Account validity: Indefinite — Provide timeline for account validity

Role: user — Choose role for the user

Preferred language: English

Safes: portal — Add Safes that the user suppose to have access to

Full name

Email

Organization

Phone

AD domain

LDAP Base: LDAP service BaseDN paremeter

Granted users: Users allowed to manage this object

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

Note:

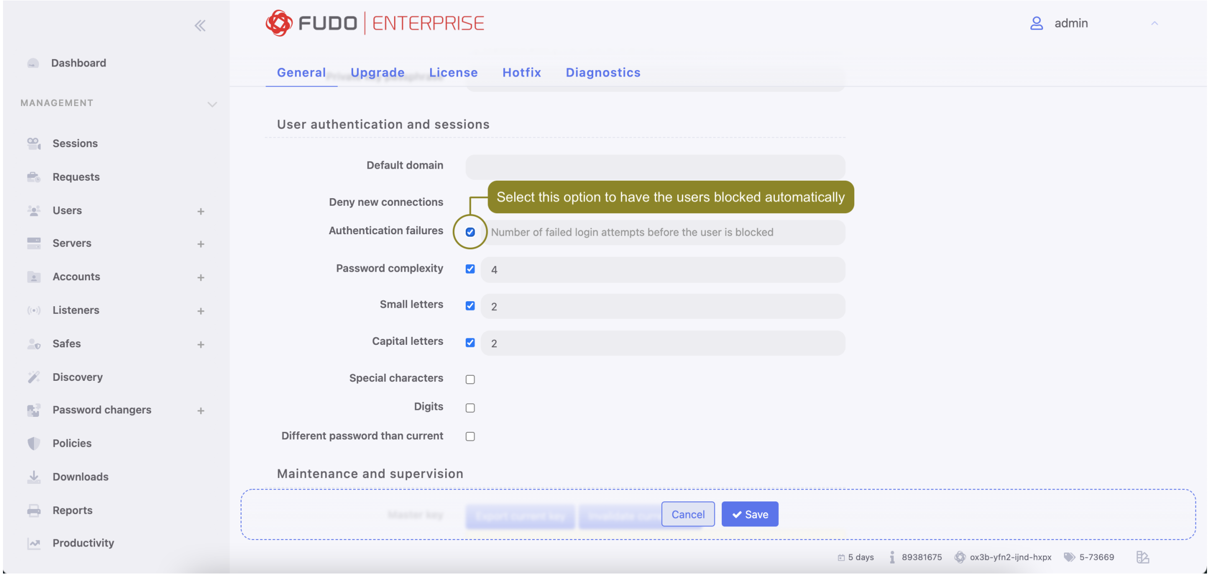
- LDAP base is necessary for authenticating the user using the Active Directory service.
- E.g. for `example.com` domain, the LDAP base parameter value should be `dc=example, dc=com`.

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.



User authentication and sessions

Default domain

Deny new connections

Authentication failures ☑ Number of failed login attempts before the user is blocked

Password complexity ☑ 4

Small letters ☑ 2

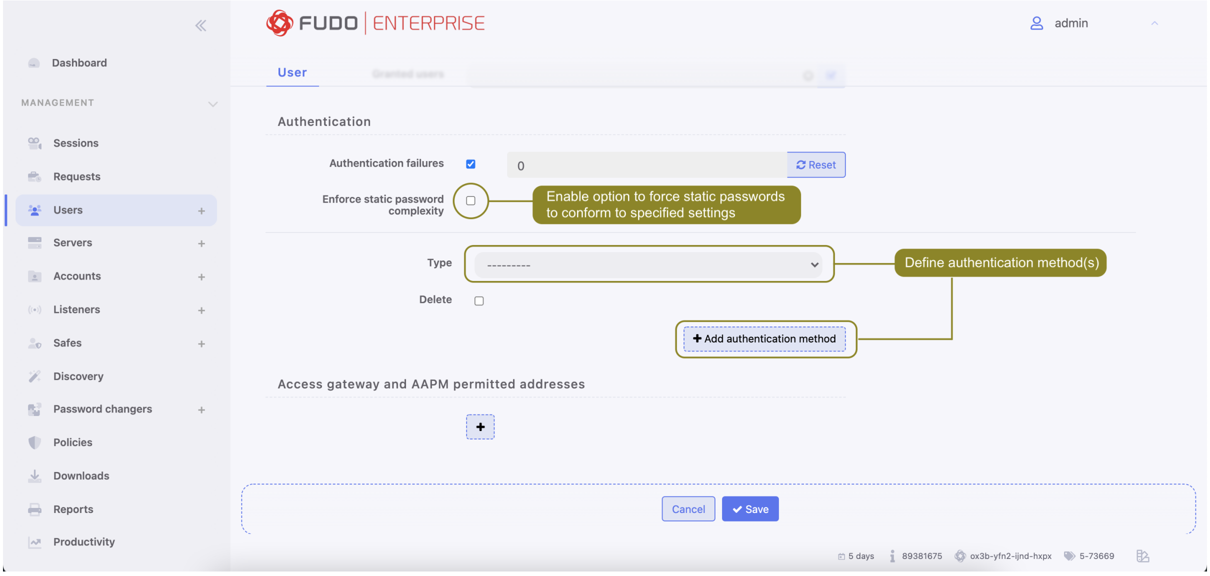
Capital letters ☑ 2

Special characters □

Digits □

Different password than current □

Maintenance and supervision



Authentication

Authentication failures ☑ 0

Enforce static password complexity □

Type ---------

Delete □

Access gateway and AAPM permitted addresses

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.

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

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

Certificate

- Provide *Subject* that complies with the RFC 2253 or RFC 4514 requirements.

Note: Additionally, the CA certificate is required to be uploaded in the *Settings > System* tab. For more info about authentication with certificate, refer to the *Certificate-based authentication scheme* topic.

DUO

- From a **First factor** drop-down list choose `Static password` or `External authentication` (AD or LDAP).
- Input *DUO username.*
- Input *DUO user id.*

Note: For more info about DUO authentication configuration, refer to the *DUO authentication definition* topic.

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 (Access Gateway)*.

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.

SMS

- Input a phone number in the **Phone** input field in the *General* section above.
- From a **First factor** drop-down list choose `Static password` or `External authentication` (AD or LDAP).

Note: For more info about SMS authentication configuration, refer to the *SMS authentication definition* topic.

OATH

Refer to the *Two-factor OATH authentication with Google Authenticator* page.

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

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

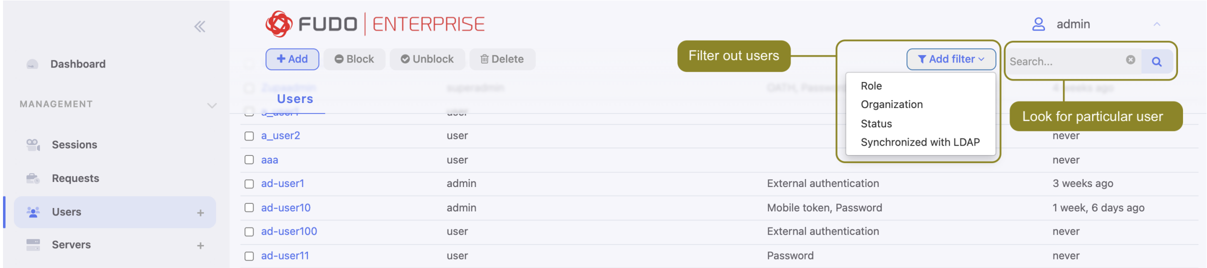
21. In the *Access gateway and AAPM permitted addresses*, click + and define IP address used by the User Portal (Access Gateway) and the AAPM to communicate with Fudo Enterprise.
22. Click *Save*.

Related topics:

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

6.2 Editing a user

1. Select *Management > Users*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.

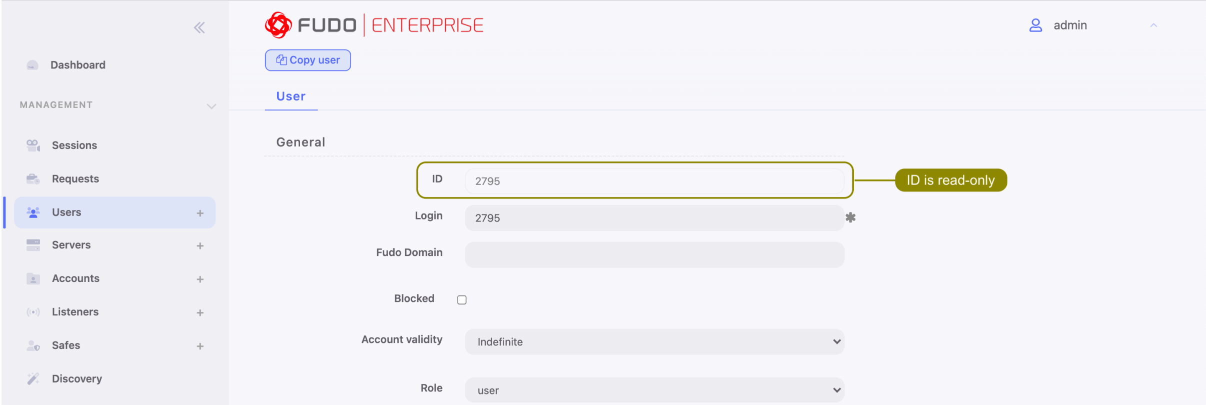


a_user2	user		never
aaa	user		never
ad-user1	admin	External authentication	3 weeks ago
ad-user10	admin	Mobile token, Password	1 week, 6 days ago
ad-user100	user	External authentication	never
ad-user11	user	Password	never

3. Find and click desired user's name to access its configuration parameters.

Note:

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



ID: 2795

Login: 2795 ✱

Fudo Domain:

Blocked: □

Account validity: Indefinite

Role: user

4. Modify configuration values as needed.
5. Click *Save*.

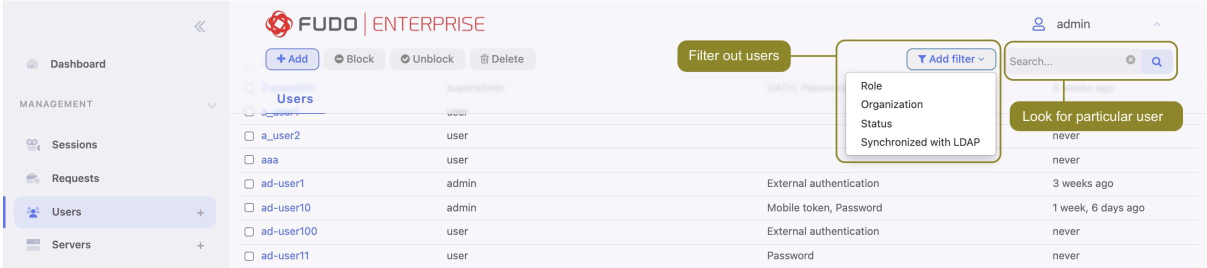
Related topics:

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

6.3 Blocking a user

Warning: Blocking a user will terminate its current connections.

1. Select *Management* > *Users*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.

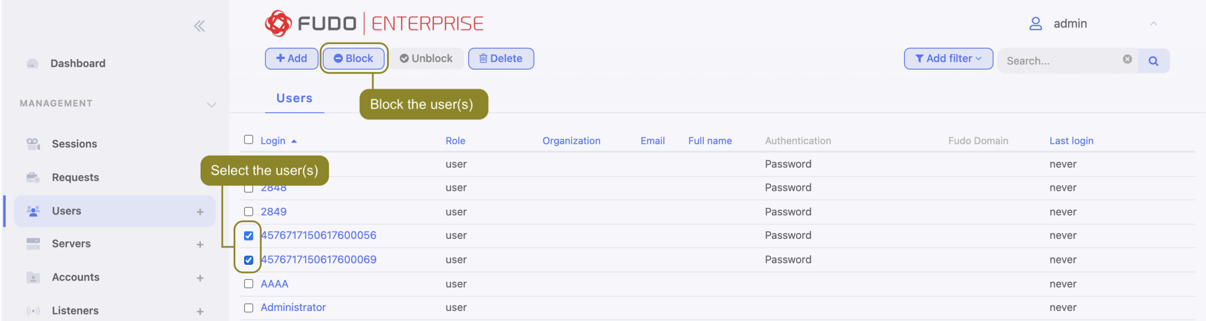


Filter out users

Look for particular user

□ a_user2	user		never
□ aaa	user		never
□ ad-user1	admin	External authentication	3 weeks ago
□ ad-user10	admin	Mobile token, Password	1 week, 6 days ago
□ ad-user100	user	External authentication	never
□ ad-user11	user	Password	never

3. Select the user you want to block and click *Block*.



Block the user(s)

Select the user(s)

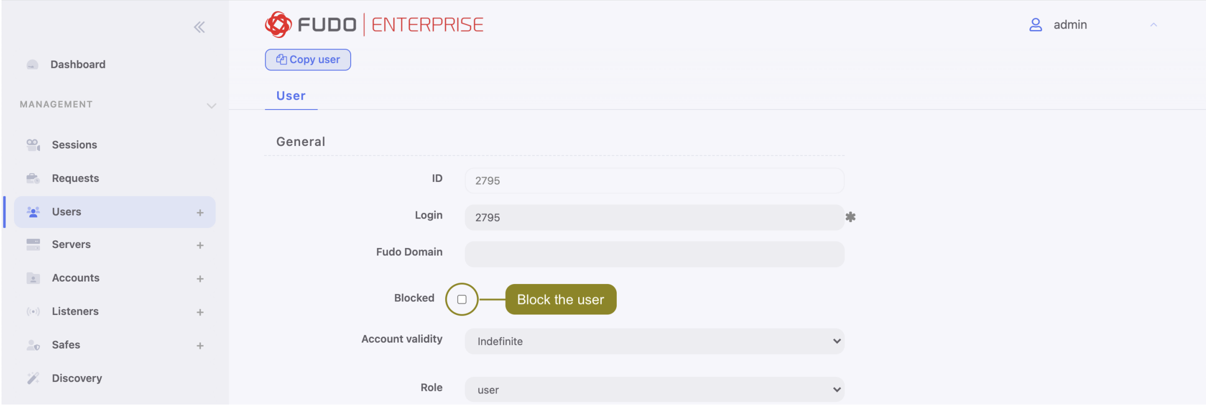
□ Login	Role	Organization	Email	Full name	Authentication	Fudo Domain	Last login
	user				Password		never
□ 2848	user				Password		never
□ 2849	user				Password		never
☑ 4576717150617600056	user				Password		never
☑ 4576717150617600069	user				Password		never
□ AAAA	user						never
□ Administrator	user						never

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

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

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

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



General

ID	2795
Login	2795
Fudo Domain	
Blocked	□
Account validity	Indefinite
Role	user

Block the user

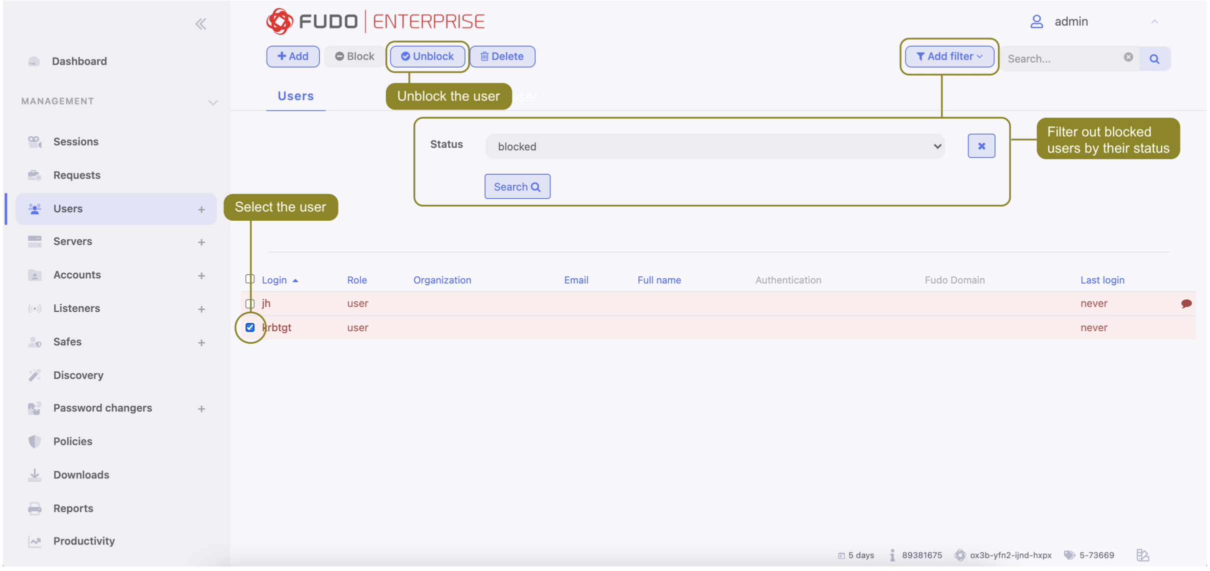
5. Click *Save*.

Related topics:

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

6.4 Unblocking a user

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



Unblock the user

Filter out blocked users by their status

Status: blocked

Select the user

☐	Login	Role	Organization	Email	Full name	Authentication	Fudo Domain	Last login
☐	jh	user						never
☑	krbtgt	user						never

4. Click *Confirm* to unblock selected objects.

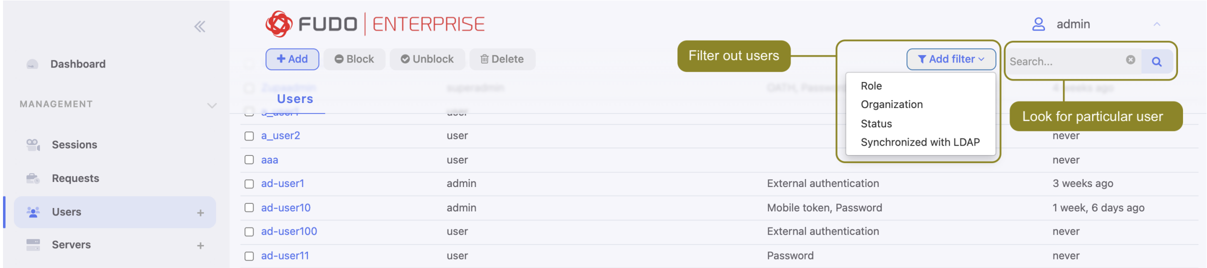
Related topics:

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

6.5 Deleting a user

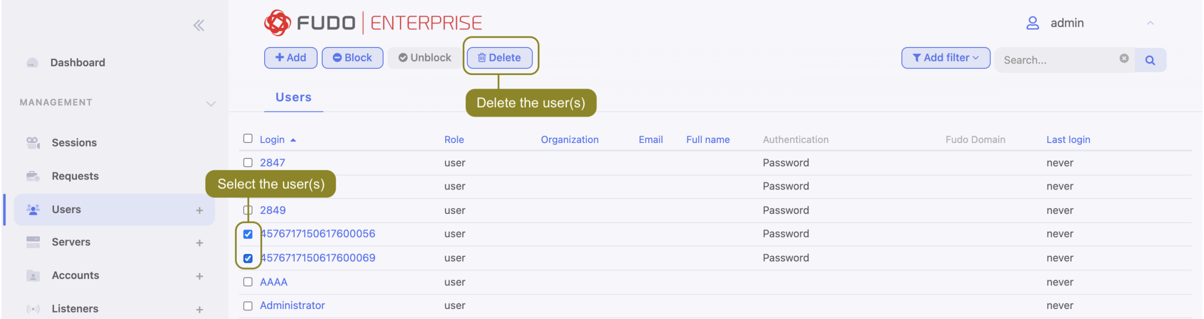
Warning: Deleting a user definition will terminate its current connections.

1. Select *Management > Users*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



□ a_user2	user		never
□ aaa	user		never
□ ad-user1	admin	External authentication	3 weeks ago
□ ad-user10	admin	Mobile token, Password	1 week, 6 days ago
□ ad-user100	user	External authentication	never
□ ad-user11	user	Password	never

3. Click *Delete*.



□ Login	Role	Organization	Email	Full name	Authentication	Fudo Domain	Last login
□ 2847	user				Password		never
	user				Password		never
□ 2849	user				Password		never
☑ 4576717150617600056	user				Password		never
☑ 4576717150617600069	user				Password		never
□ AAAA	user						never
□ Administrator	user						never

4. Confirm deleting selected objects.

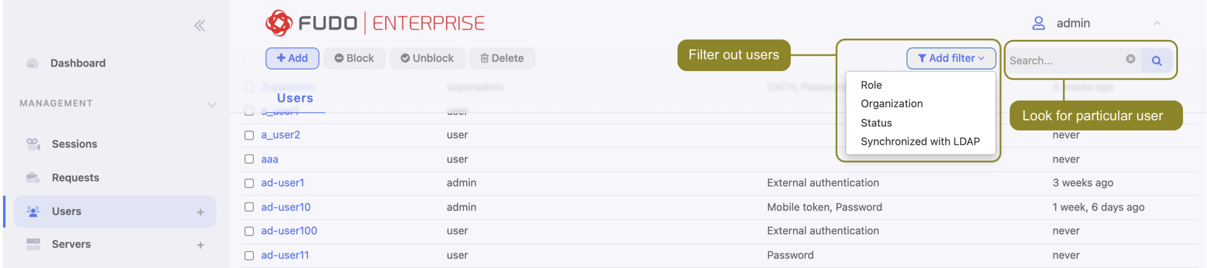
Related topics:

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

6.6 Time access policy

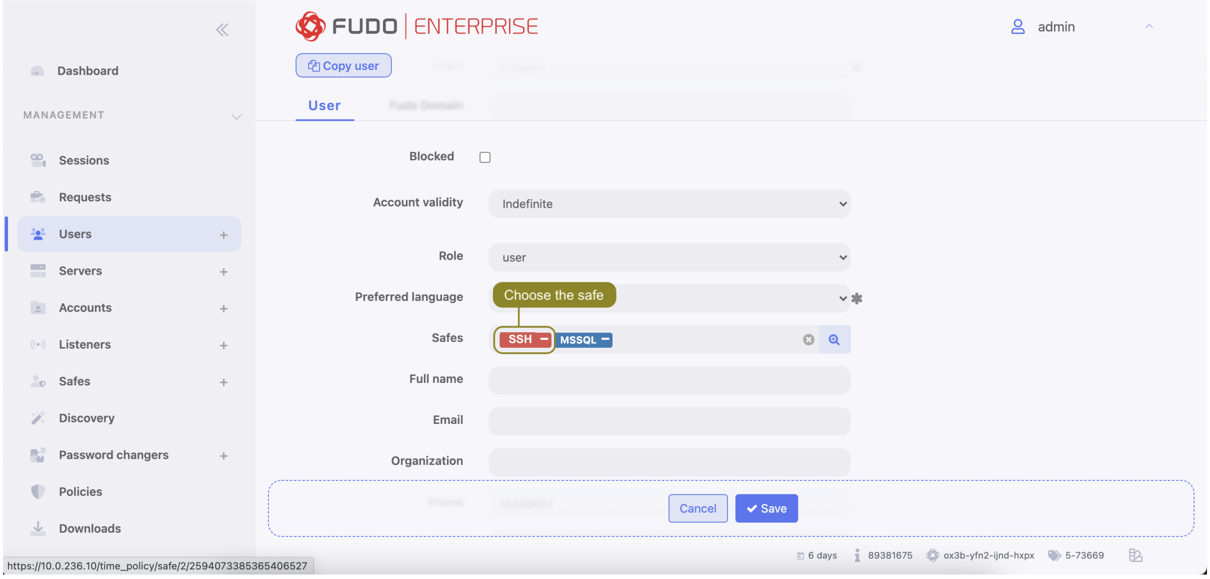
Fudo Enterprise can regulate access to safes based on time. To define time based safe access, proceed as follows.

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



□ a_user2	user		never
□ aaa	user		never
□ ad-user1	admin	External authentication	3 weeks ago
□ ad-user10	admin	Mobile token, Password	1 week, 6 days ago
□ ad-user100	user	External authentication	never
□ ad-user11	user	Password	never

3. Find and click desired user's name to access its configuration parameters.
4. Click desired safe object.



Blocked □

Account validity: Indefinite

Role: user

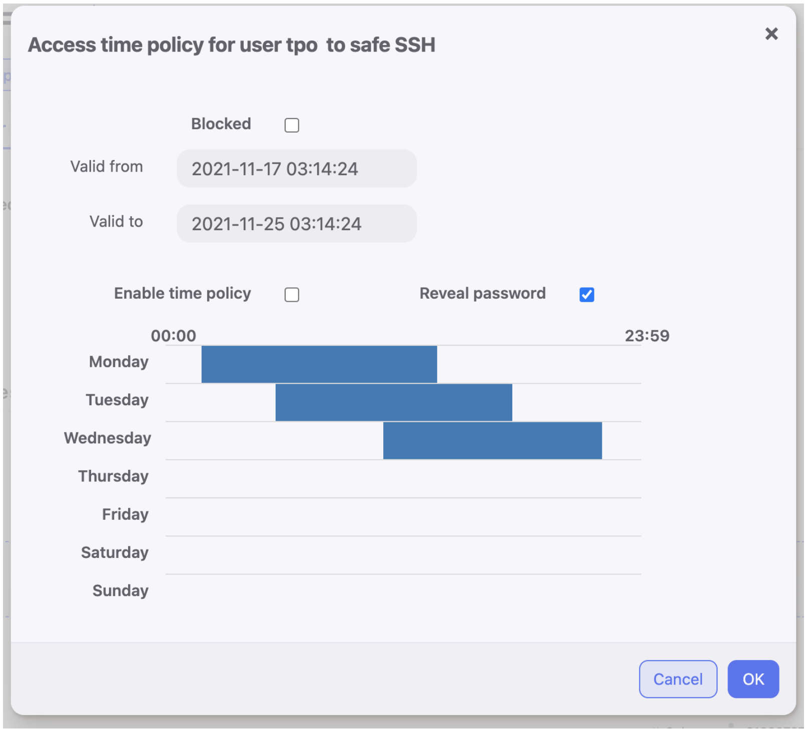
Preferred language

Safes: SSH, MSSQL

Full name

Email

Organization



Access time policy for user tpo to safe SSH

Blocked □

Valid from: 2021-11-17 03:14:24

Valid to: 2021-11-25 03:14:24

Enable time policy □ Reveal password ☑

5. 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.

6. 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.

7. Select the *Enable time policy* option.

8. 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 (Access Gateway)*.

9. Click the weekly calendar to define time interval.
10. Click *OK*.
11. Click *Save*.

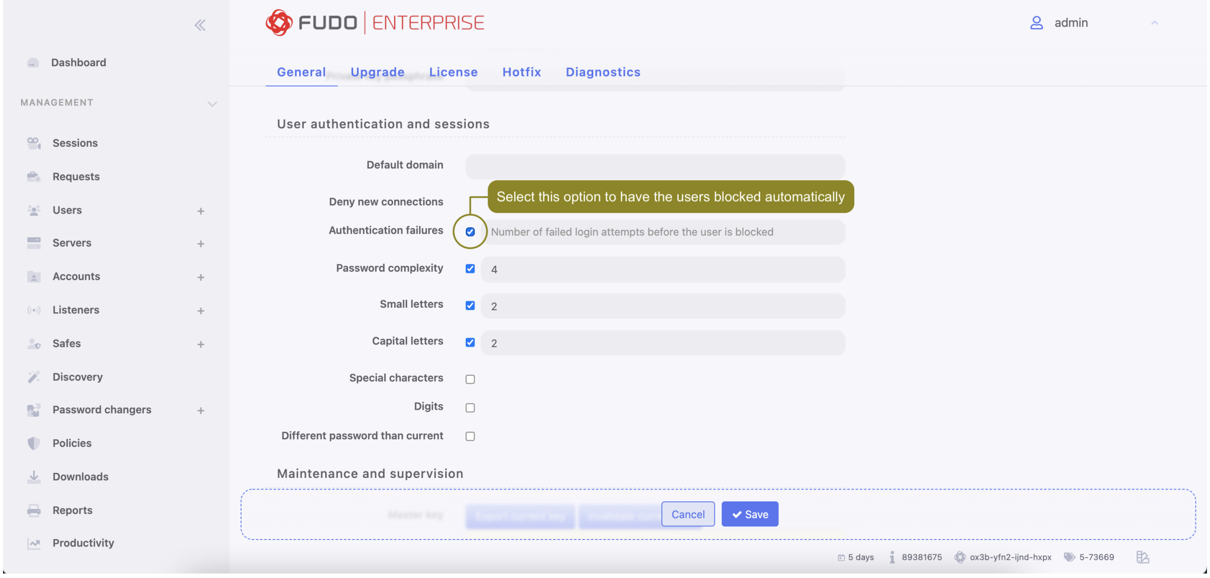
Related topics:

- *Creating a user*
- *Servers*
- *Accounts*

6.7 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

Select this option to have the users blocked automatically

Authentication failures ☑ Number of failed login attempts before the user is blocked

Password complexity ☑ 4

Small letters ☑ 2

Capital letters ☑ 2

Special characters □

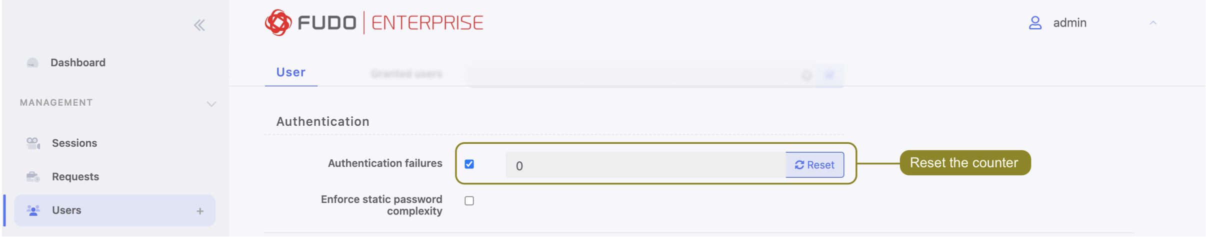
Digits □

Different password than current □

Maintenance and supervision

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.



Authentication

Authentication failures ☑ 0 Reset

Enforce static password complexity □

Related topics:

- *User authentication methods and modes*

6.8 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. • Managing 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.

Continued on next page

Table 2 – continued from previous page

Role	Access rights
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*

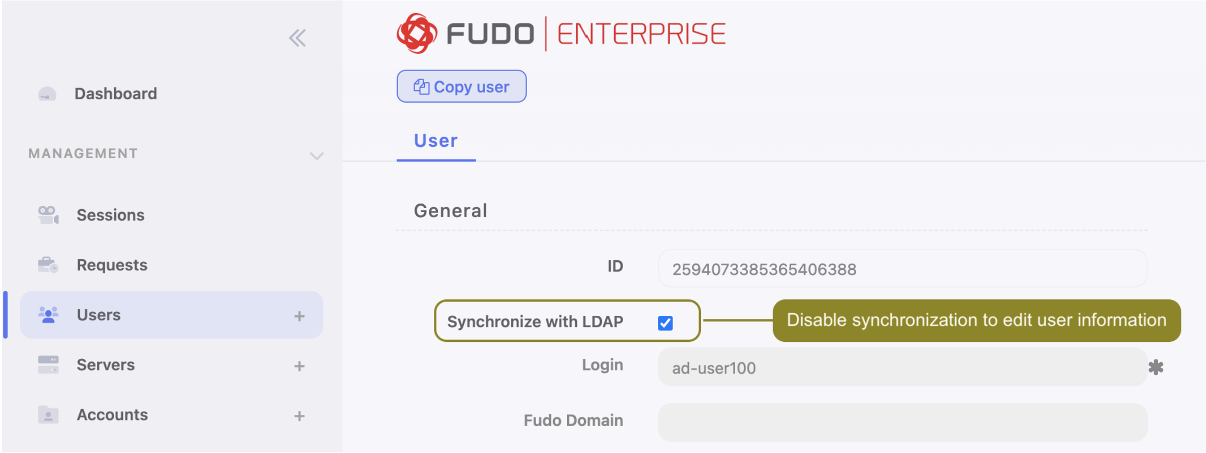
6.9 Users synchronization

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

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

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

- Fudo Enterprise supports nested LDAP groups.
- Also, Fudo Enterprise allows synchronizing the user's data with the LDAP service source. The `Synchronize with LDAP` option is responsible for this process. When this option is checked for the given user, an administrator can't edit the user's data manually but can add or edit their authentication methods. If the `Synchronize with LDAP` option is unchecked, the user is no longer synchronized with LDAP source, and can be edited by an administrator. The administrator can still check the option and reinstate synchronization with LDAP, but any change made manually will disappear with the next synchronisation attempt. Only the added authentication methods won't change.



ID 2594073385365406388

Synchronize with LDAP ☑

Disable synchronization to edit user information

Login ad-user100

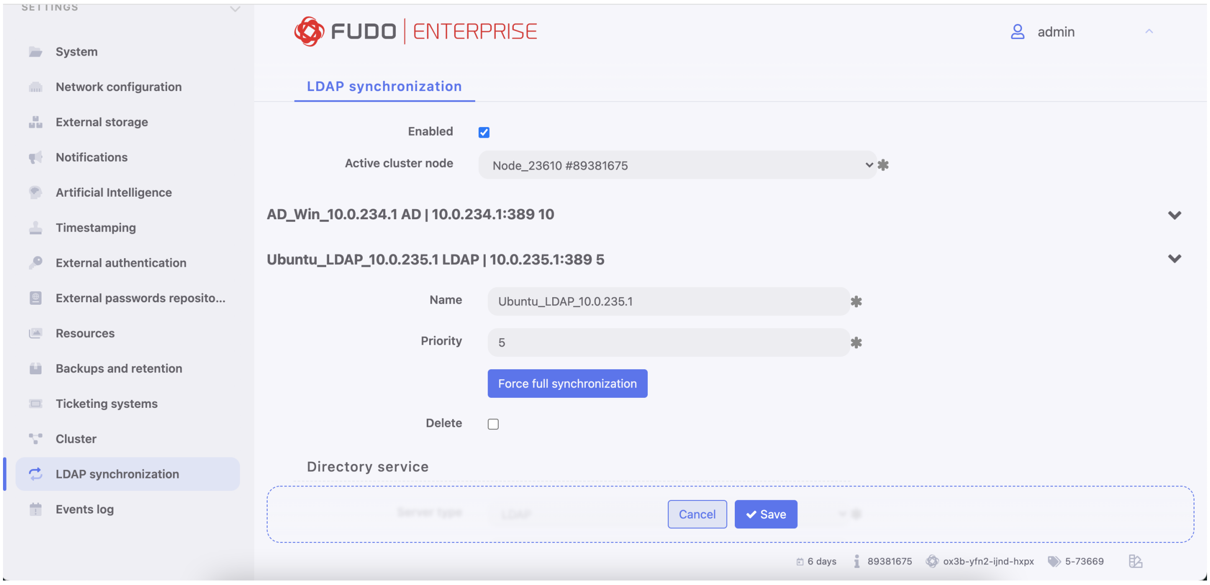
Fudo Domain

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.



LDAP synchronization

Enabled ☑

Active cluster node: Node_23610 #89381675

AD_Win_10.0.234.1 AD | 10.0.234.1:389 10

Ubuntu_LDAP_10.0.235.1 LDAP | 10.0.235.1:389 5

Name: Ubuntu_LDAP_10.0.235.1

Priority: 5

Force full synchronization

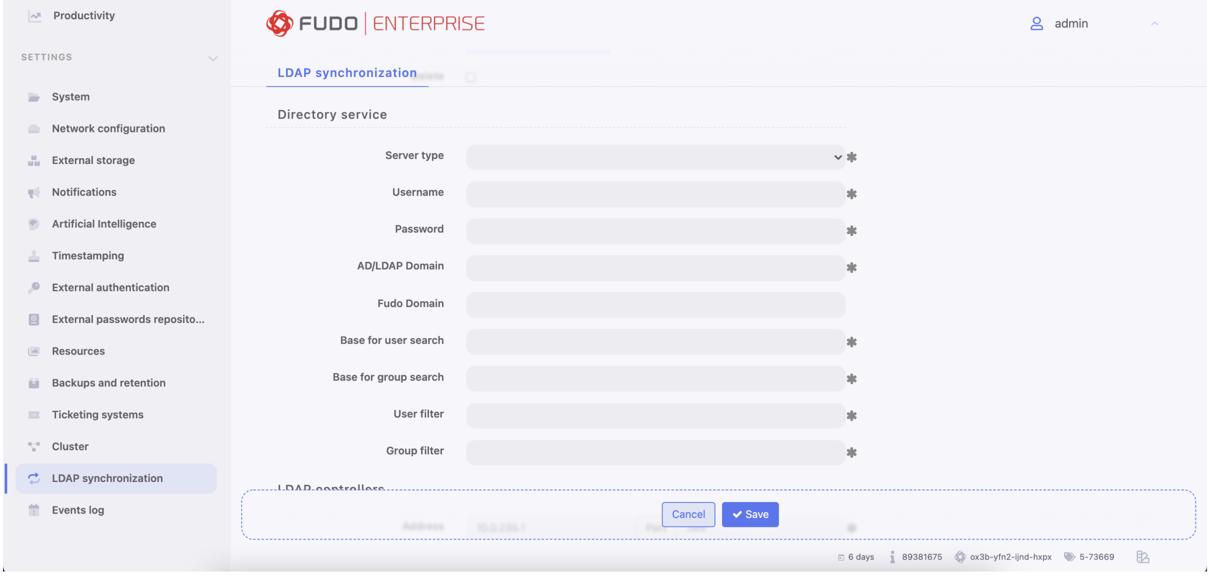
Delete □

Directory service

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.



LDAP synchronization

Directory service

Server type

Username

Password

AD/LDAP Domain

Fudo Domain

Base for user search

Base for group search

User filter

Group filter

LDAP controllers

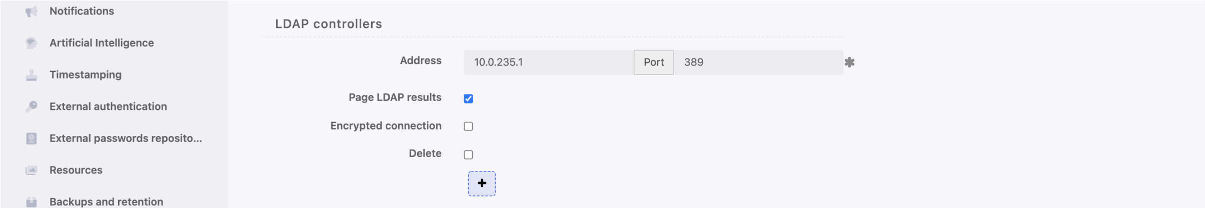
14. Click + in the *LDAP controllers* section to define directory service server.

15. Provide IP address and port number.

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

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

Note: Click + to add more directory servers.



LDAP controllers

Address: 10.0.235.1 Port: 389 ✱

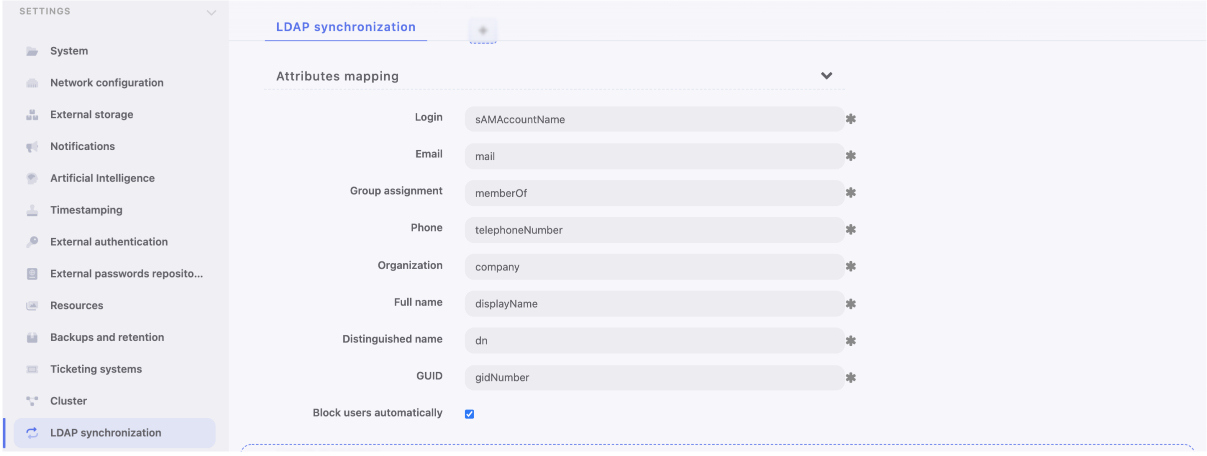
Page LDAP results ☑

Encrypted connection □

Delete □

18. Define user information mapping.

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

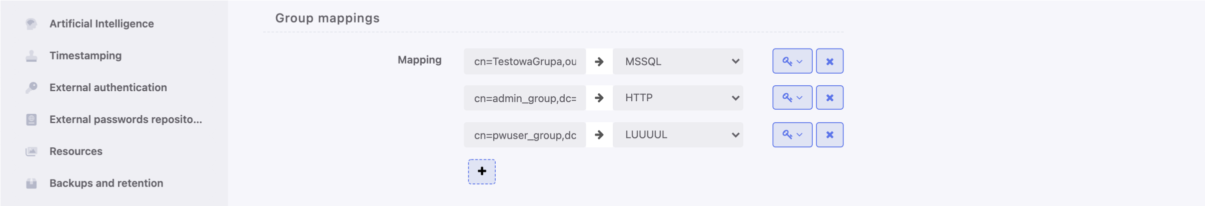


LDAP synchronization

Attributes mapping

Login	sAMAccountName ✱
Email	mail ✱
Group assignment	memberOf ✱
Phone	telephoneNumber ✱
Organization	company ✱
Full name	displayName ✱
Distinguished name	dn ✱
GUID	gidNumber ✱
Block users automatically	☑

19. Select *Block automatically* to automatically block local users' accounts blocked in the directory.
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=TestowaGrupa,ou → MSSQL
cn=admin_group,dc= → HTTP
cn=pwuser_group,dc → LUUUUL

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 Enterprise will be authenticating him against external authentication sources starting from those defined in the first group mapping defined.

For example:

A user is assigned to groups A and B. Group B is mapped to `Safe RDP` and has `CERB` and `Radius` authentication sources assigned. Group A is second in order and it is mapped to `Safe SSH` and has `AD` authentication source assigned.

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

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

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 Enterprise supports nested LDAP groups.

Related topics:

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

6.10 Two-factor OATH authentication with Google Authenticator

Google Authenticator generates verification code as a dynamic component to a static password to increase account security.

Fudo Enterprise allows configuring default settings for the OATH authentication so they are automatically added to the user definition, when administrator selects `OATH` as an active authentication method.

6.10.1 Protocols Supporting OATH Authentication Method

When logging in, OATH authentication can be performed either in *Challenge-Response* mode or by concatenating the dynamic code generated by Google Authenticator to the end of the static password defined in the authentication method, such as `password481418`. Please note that not all protocols support this authentication method.

Table 3: `OATH Availability Across Protocols`

Platform or Protocol	Challenge-Response Mode	Password + Dynamic Code
Logging into Access Gateway	available	available
Logging into Admin Panel	available	available
VNC	available	available
SSH	available	available
RDP	available	available
Telnet 3270	not available	available
Telnet 5250	not available	available
Telnet	not available	available
MS SQL(TDS)	not available	not available
HTTP/S	not available	not available
TCP	not available	not available
MySQL	not available	not available
X11	not available	not available
Modbus	not available	not available

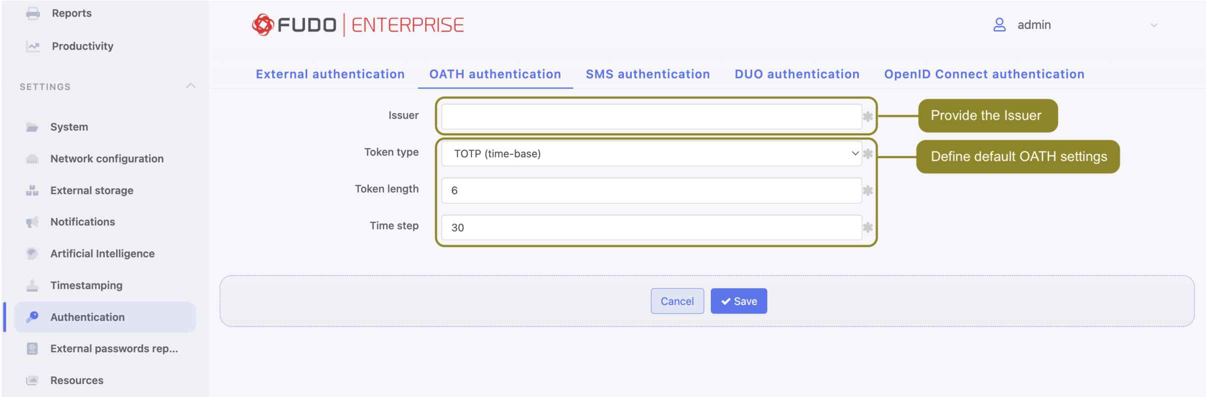
6.10.2 Configuring the OATH Authentication Method

In order to configure default settings for the OATH authentication method, follow the instruction:

1. Select *Settings > Authentication > OATH authentication*.
2. Fill out the *Issuer* field.
3. From the *Token type* field select `TOTP (time-base)` or `HOTP (counter-base)`.
4. Fill out the *Token length* field.

5. Input *Time step* if selected *Token type* was `TOTP (time-base)`.

6. Click *Save*.



Issuer:

Token type: TOTP (time-base)

Token length: 6

Time step: 30

Provide the Issuer

Define default OATH settings

In order to configure OATH as an active authentication method for a user, follow the steps:

1. Select *Management* > *Users*.

2. Find and click the user for whom you want to add the OATH authentication method.

3. Scroll down to the *Authentication* section.

4. From the *Type* drop-down list, select `OATH`.

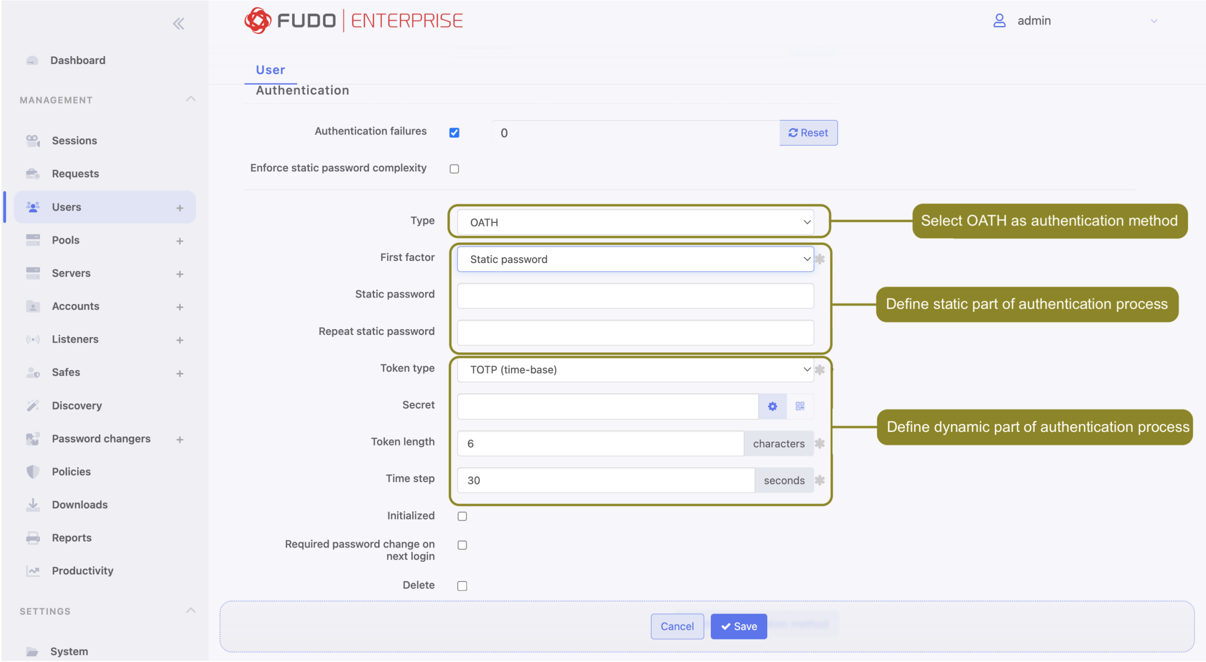
5. Choose the first factor: `Password` or `External authentication`.

If `Password` is chosen:

- Enter password's static part.

- Fields *Token type*, *Token length* and *Time step* will be filled out automatically as default settings claim. Their value is editable.

- Enter a secret that will be used by *Google Authenticator*. Note, that the secret must be a `Base32` encoded value. Alternatively, click ⚙ to generate it automatically. Click to show the *QR code*.



Authentication failures ☑ 0

Enforce static password complexity □

Type: OATH

First factor: Static password

Static password:

Repeat static password:

Token type: TOTP (time-base)

Secret:

Token length: 6 characters

Time step: 30 seconds

Initialized □

Required password change on next login □

Delete □

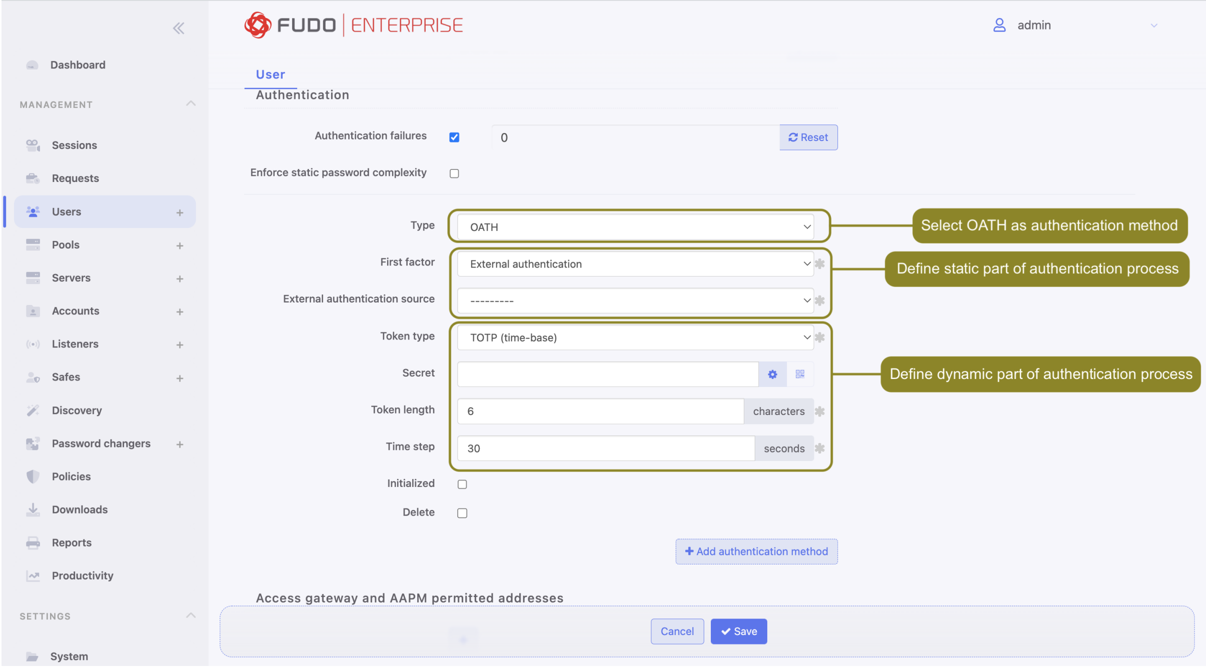
Select OATH as authentication method

Define static part of authentication process

Define dynamic part of authentication process

If `External authentication` is chosen:

- Select External authentication source.
- Fields *Token type*, *Token length* and *Time step* will be filled out automatically as default settings claim. Their value is editable.
- Enter a secret that will be used by *Google Authenticator*. Note, that the secret must be a `Base32` encoded value. Alternatively, click ⚙ to generate it automatically. Click to show the *QR code*.



Authentication failures ☑ 0

Enforce static password complexity □

Type: OATH

First factor: External authentication

External authentication source: ---------

Token type: TOTP (time-base)

Secret:

Token length: 6 characters

Time step: 30 seconds

Initialized □

Delete □

Access gateway and AAPM permitted addresses

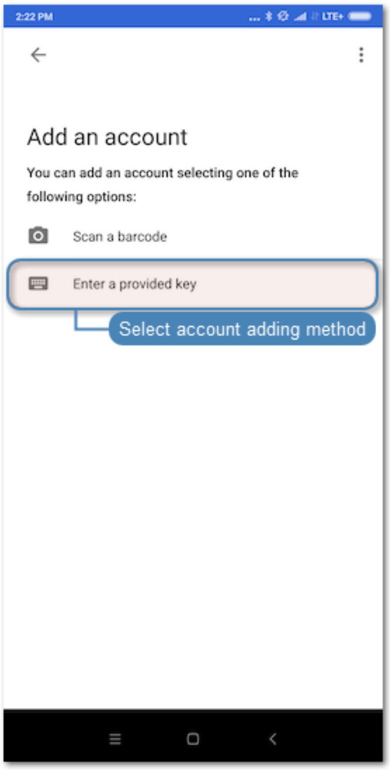
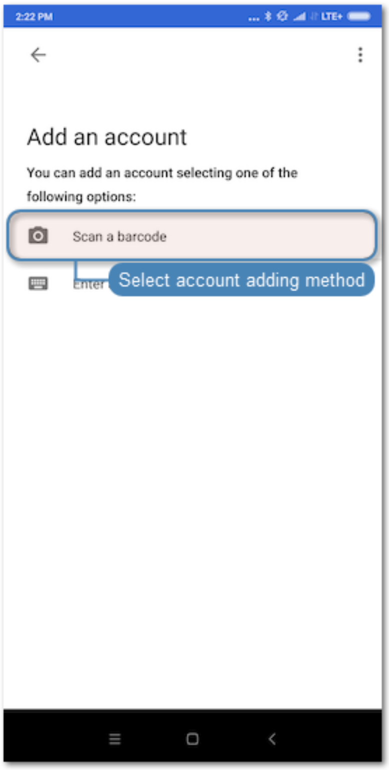
Select OATH as authentication method

Define static part of authentication process

Define dynamic part of authentication process

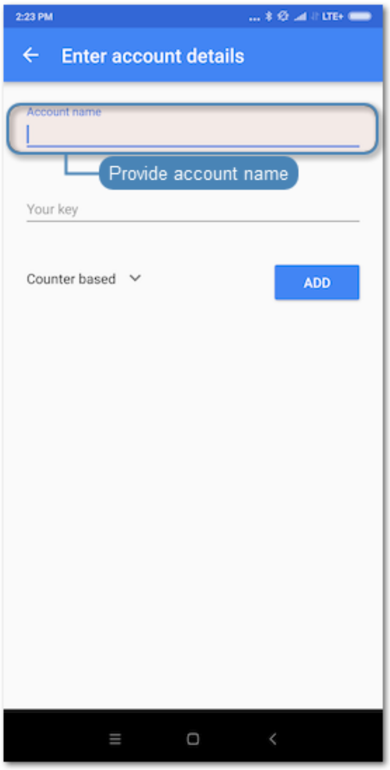
Note: The *Initialized* option serves for the user's initialization via the QR code. When their *static password* as a *First factor* setting is filled or *External authentication* source if configured, the QR code is displayed during their first connection. After successful first authentication the *Initialized* option becomes checked and takes uneditable state.

6. Click *Save*.
7. Launch *Google Authenticator*.

Manual entry	QR Code
• Select *Enter a provided key*.  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.  Add an account You can add an account selecting one of the following options: Scan a barcode Enter Select account adding method

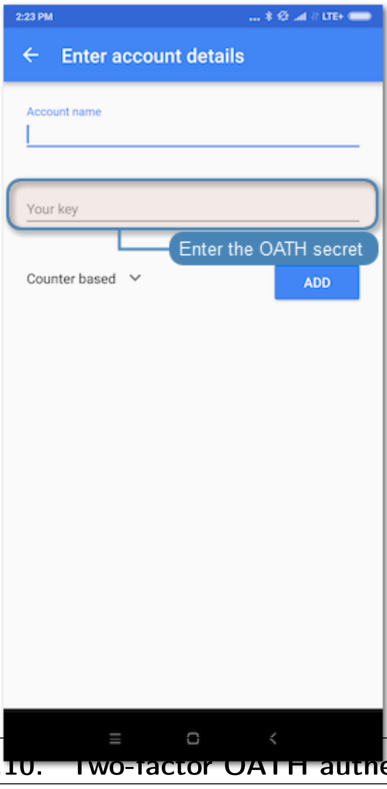
Manual entry	QR Code

- Enter account name.



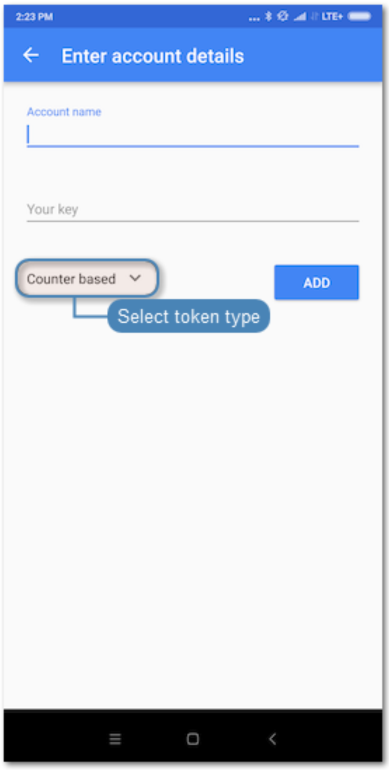
- Enter the secret defined in OATH authentication method.

Note: Click 👁 on the user configuration form in the *Authentication* section to reveal the secret.

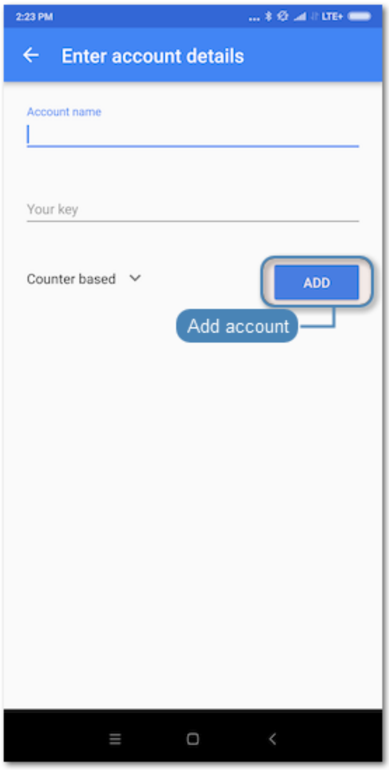


<table>
<tr><th>Manual entry</th><th>QR Code</th></tr>
<tr><td>

- Select *Counter based*.

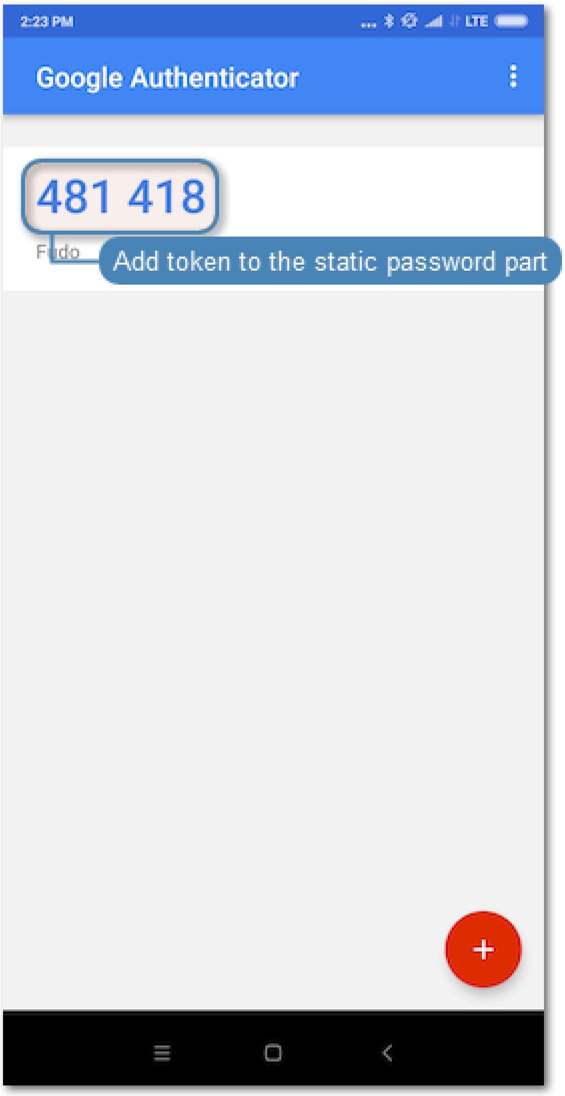


- Select ADD.



</td><td></td></tr>
</table>

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



Related topics:

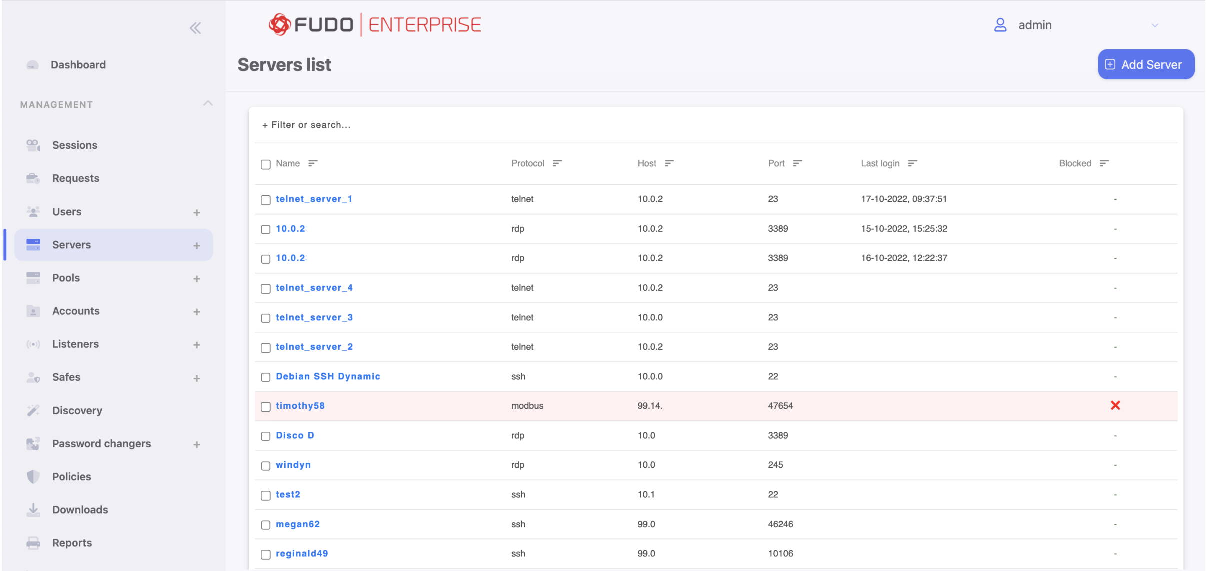
- *User authentication methods and modes*

CHAPTER 7

Servers

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

- Fudo Enterprise allows configuring a server with one unique address and a server with a group of addresses to be connected within a specified network.
- Once the server definition is configured and saved, the Fudo Enterprise allows grouping multiple servers within one Server Pool so all the added servers are managed as one server within other objects.



Servers list

Name	Protocol	Host	Port	Last login	Blocked
telnet_server_1	telnet	10.0.2	23	17-10-2022, 09:37:51	-
10.0.2	rdp	10.0.2	3389	15-10-2022, 15:25:32	-
10.0.2	rdp	10.0.2	3389	16-10-2022, 12:22:37	-
telnet_server_4	telnet	10.0.2	23		-
telnet_server_3	telnet	10.0.0	23		-
telnet_server_2	telnet	10.0.2	23		-
Debian SSH Dynamic	ssh	10.0.0	22		-
timothy58	modbus	99.14.	47654		✗
Disco D	rdp	10.0	3389		-
windyn	rdp	10.0	245		-
test2	ssh	10.1	22		-
megan62	ssh	99.0	46246		-
reginald49	ssh	99.0	10106		-

7.1 Creating a server

7.1.1 Creating an HTTP server

Note:

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

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

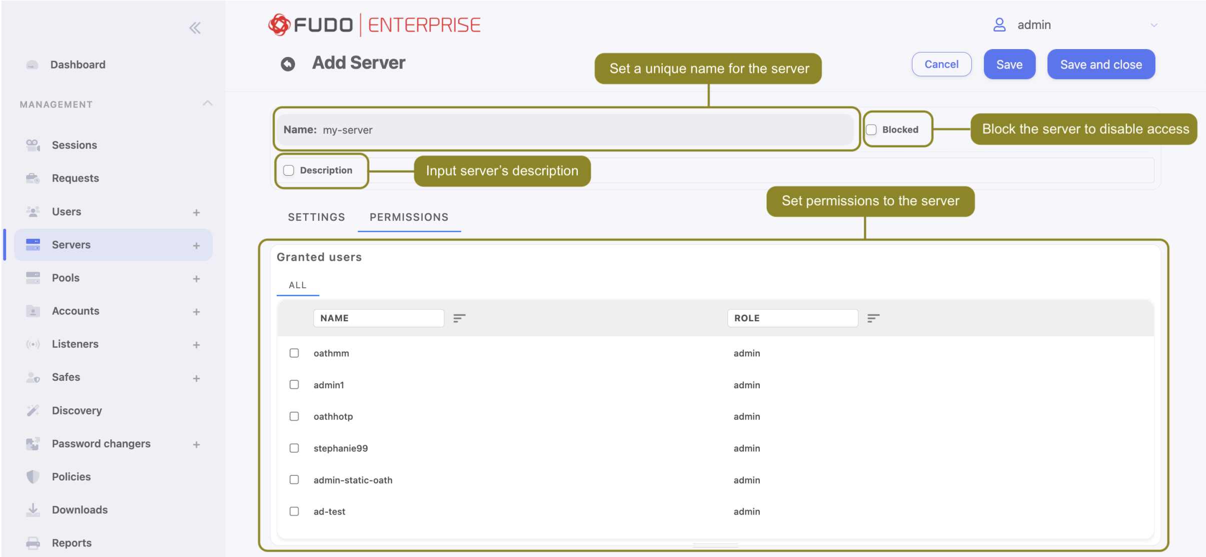
Model	Maximum recommended number of concurrent HTTP sessions*
F100x	2
F300x	5
F500x	10

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

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

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

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



Set a unique name for the server

Name: my-server

□ Blocked

Block the server to disable access

□ Description

Input server's description

Set permissions to the server

Granted users

ALL

	NAME	ROLE
□	oathmm	admin
□	admin1	admin
□	oathhotp	admin
□	stephanie99	admin
□	admin-static-oath	admin
□	ad-test	admin

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

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

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

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

8. In the *HTTP host* field provide the HTTP host header value.

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

9. Enter value of the *HTTP timeout* parameter, determining the time period of inactivity (expressed in seconds), after which the user will have to authenticate again.
10. Click the *HTTP Authentication* option to enable additional verification process and select one of the available platforms. If `None` is selected, provide custom login page details:
    - *Login page URL*,
    - *Username* and *Password*,
    - optionally, check the *Press the enter key prior to password* option.

Note: HTTP authentication is active only when the *Render sessions* option is enabled in the HTTP listener settings. To enable *Render sessions* option, please refer to the *Creating a HTTP listener* topic.

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

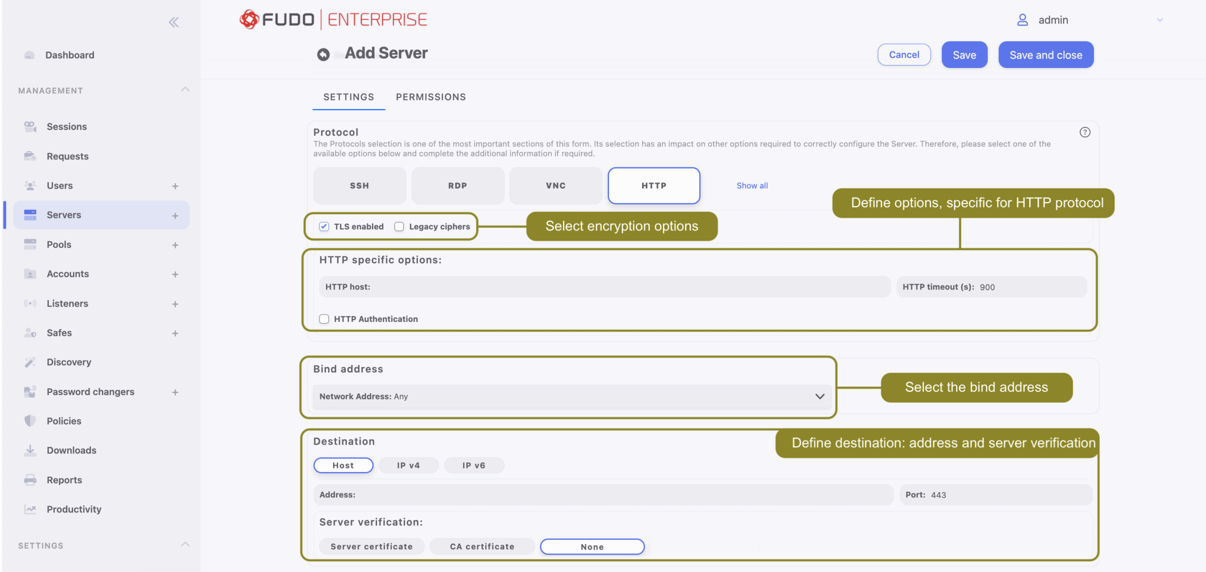
Note:

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

12. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.

- If the *TLS enabled* was checked, in the *Server verification* section select one of the following options:`Server certificate` or `CA certificate` and provide respective certificate data. Select `None` to disable server verification.



Protocol

The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

☑ TLS enabled ☐ Legacy ciphers

Select encryption options

Define options, specific for HTTP protocol

HTTP specific options:

HTTP host:

HTTP timeout (s): 900

☐ HTTP Authentication

Bind address

Network Address: Any

Select the bind address

Destination

Define destination: address and server verification

Address:

Port: 443

Server verification:

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

Related topics:

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

7.1.2 Creating a Modbus server

Note:

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

---

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

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

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

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

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

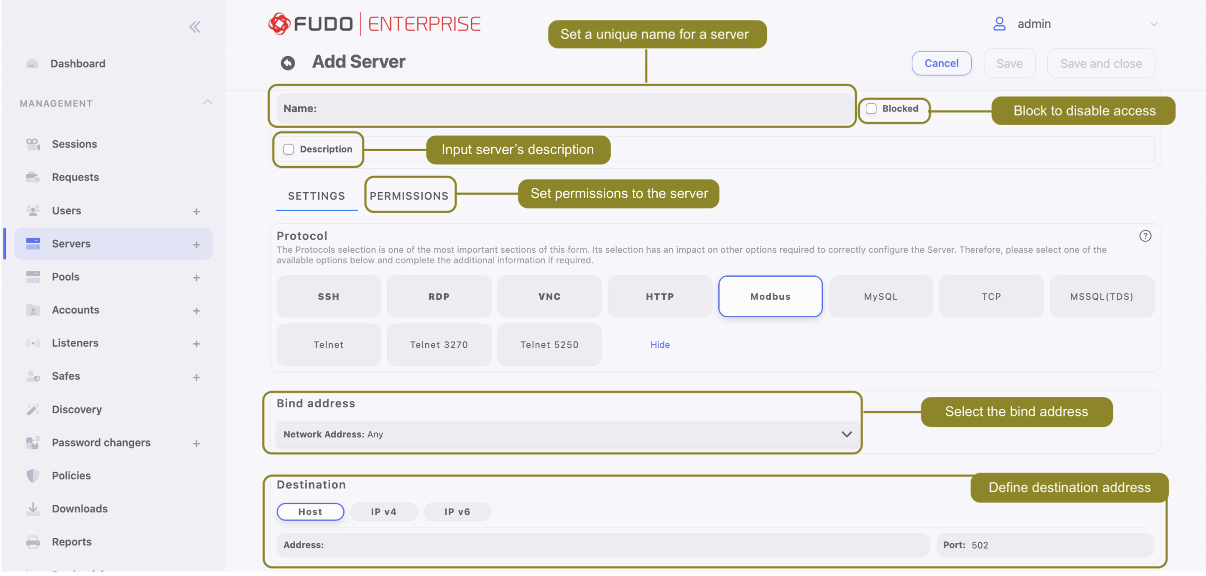
7. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

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

8. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.



Set a unique name for a server

Name:

☐ Blocked

Block to disable access

☐ Description

Input server's description

Set permissions to the server

Protocol

The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

Bind address

Network Address: Any

Select the bind address

Destination

Define destination address

Address:

Port: 502

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

Related topics:

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

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

7.1.3 Creating a MS SQL server

Note:

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

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

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

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

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

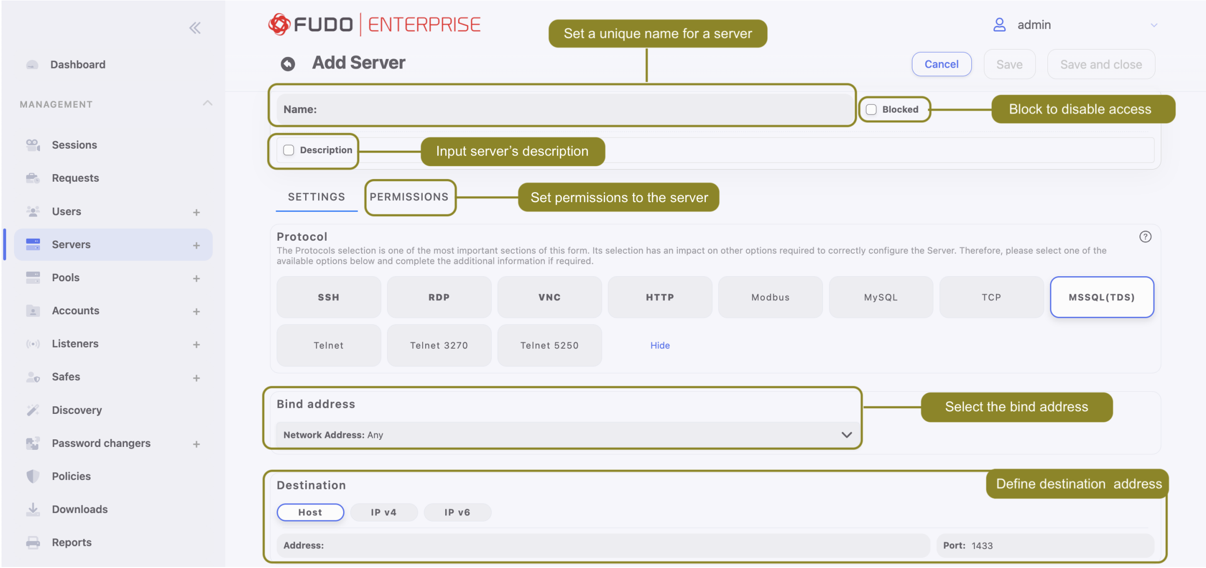
7. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

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

8. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.



Set a unique name for a server

Name:

□ Blocked

Block to disable access

□ Description

Input server's description

Set permissions to the server

Protocol

The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

Bind address

Network Address: Any

Select the bind address

Destination

Define destination address

Address:

Port: 1433

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

Related topics:

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

7.1.4 Creating a MySQL server

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

Note:

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

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

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

2. Enter server's unique name.

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

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

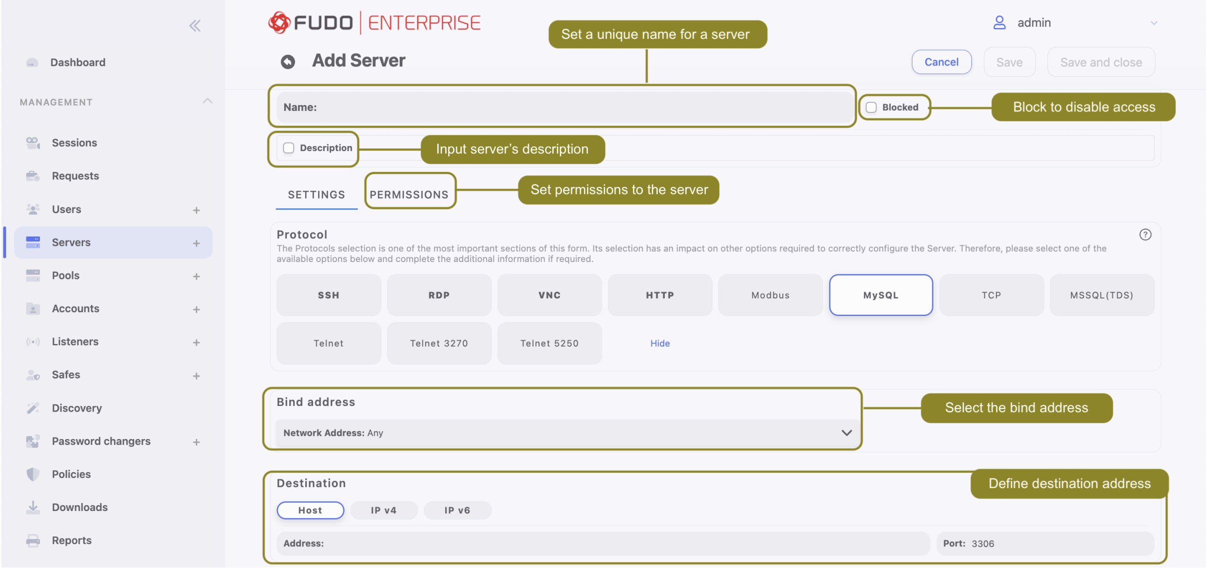
7. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

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

8. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.



Add Server

Set a unique name for a server

Name:

□ Blocked

Block to disable access

□ Description

Input server's description

Set permissions to the server

Protocol

The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

Bind address

Network Address: Any

Select the bind address

Destination

Define destination address

Address:

Port: 3306

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

Related topics:

- *Pools*

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

7.1.5 Creating an RDP server

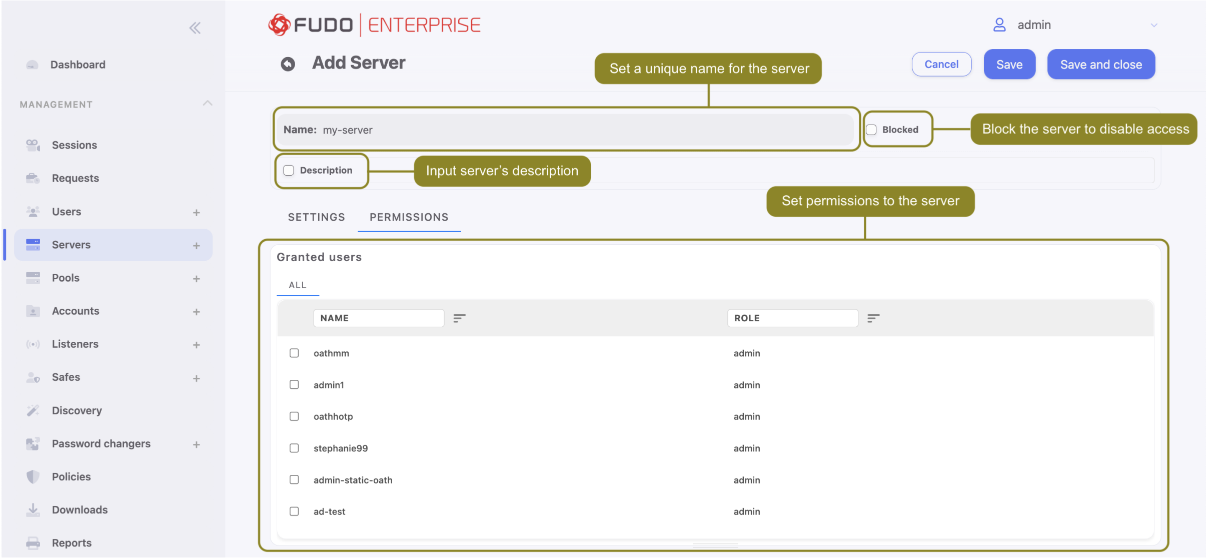
Note:

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

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

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

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



Set a unique name for the server

Block the server to disable access

Input server's description

Set permissions to the server

Name: my-server

Granted users

NAME	ROLE
□ oathmm	admin
□ admin1	admin
□ oathhotp	admin
□ stephanie99	admin
□ admin-static-oath	admin
□ ad-test	admin

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

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

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

   - Check the *NLA enabled* option for additional security.

   Note: Security mode must match the security mode setting in the *RDP listener configuration*. The *NLA enabled* option within a server corresponds to the *Enhanced RDP Security (TLS)* option within the listener.

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

   8. Check the *Inform about existing connection* option to have the users informed that other users are connected to the server, they are trying to connect to.

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

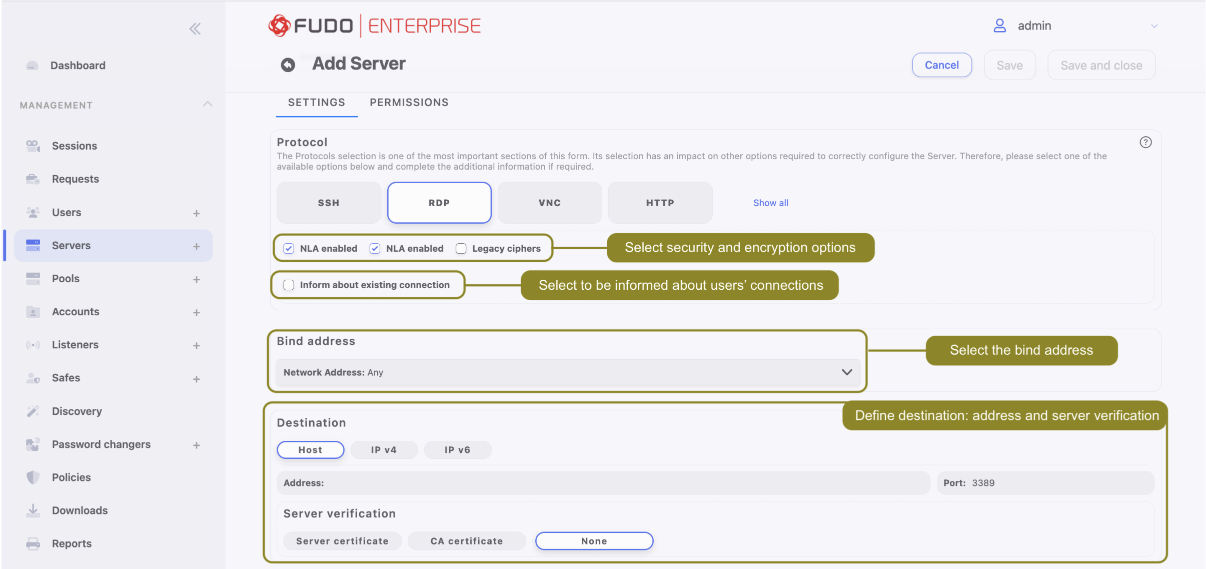
Note:

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

10. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.

- If the *TLS enabled* has been checked, in the *Server verification* section select one of the following options:`Server certificate` or `CA certificate` and provide respective certificate data. Select `None` to disable server verification.
- Otherwise, provide *server key*.



Add Server

Protocol

The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

☑ NLA enabled ☑ NLA enabled □ Legacy ciphers — Select security and encryption options

□ Inform about existing connection — Select to be informed about users' connections

Bind address

Network Address: Any — Select the bind address

Destination — Define destination: address and server verification

Host | IP v4 | IP v6

Address:

Port: 3389

Server verification

Server certificate | CA certificate | None

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

Related topics:

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

7.1.6 Creating an SSH server

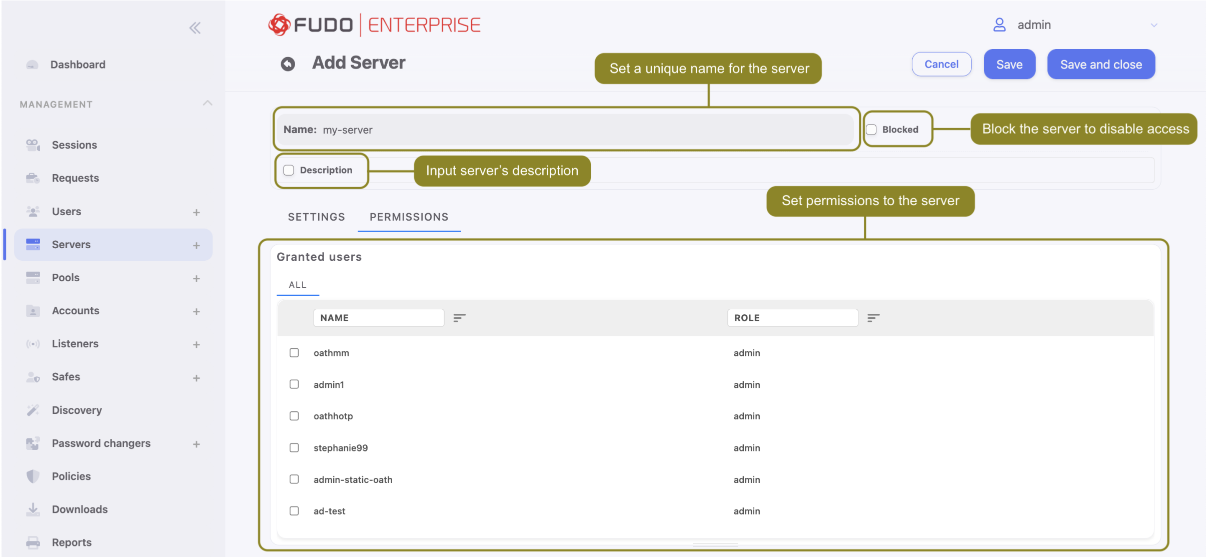
Note:

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

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

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

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



Set a unique name for the server

Name: my-server

□ Blocked

Block the server to disable access

□ Description

Input server's description

Set permissions to the server

Granted users

	NAME	ROLE
□	oathmm	admin
□	admin1	admin
□	oathhotp	admin
□	stephanie99	admin
□	admin-static-oath	admin
□	ad-test	admin

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

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

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

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

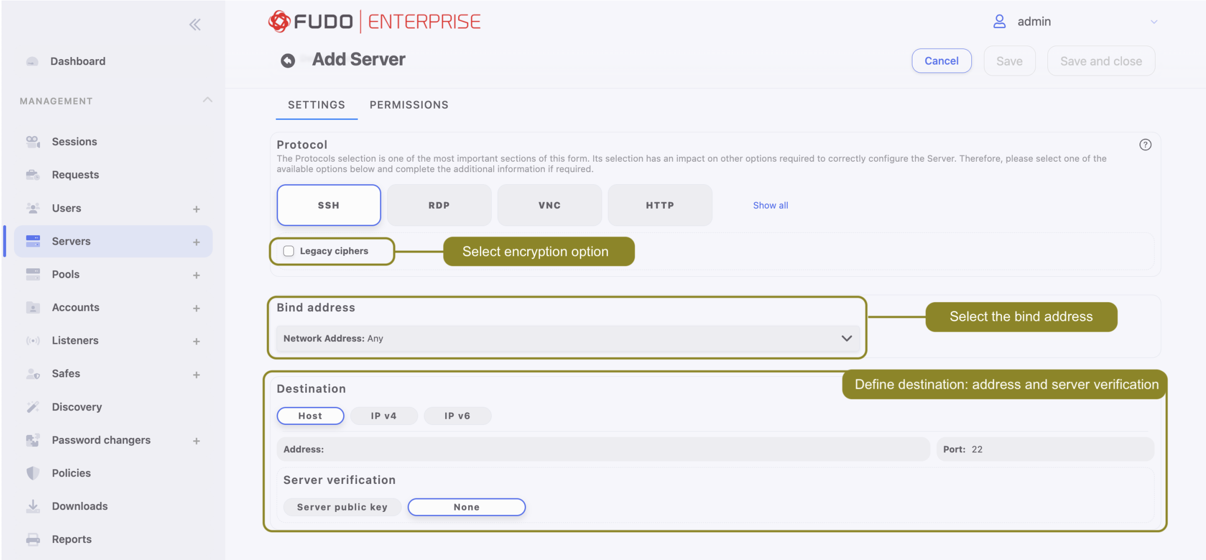
Note:

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

13. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.

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



Add Server

Protocol

The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

☐ Legacy ciphers

Select encryption option

Bind address

Network Address: Any

Select the bind address

Destination

Define destination: address and server verification

Address:

Port: 22

Server verification

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

Related topics:

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

7.1.7 Creating a Telnet server

Note:

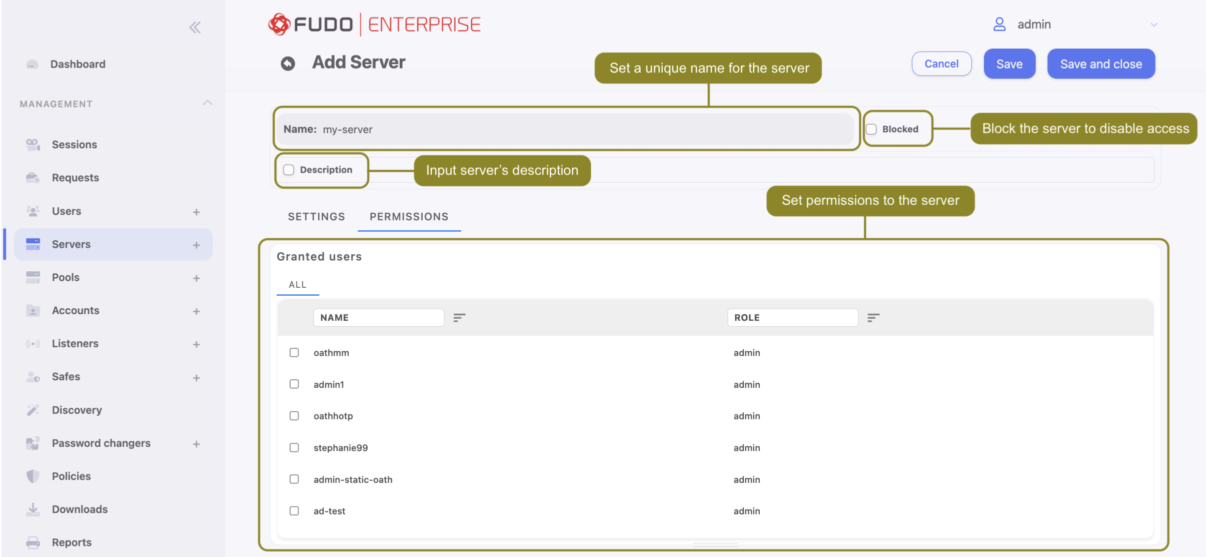
- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- In case of Telnet connections over *forward* and *regular* accounts, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise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

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

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

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

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



Set a unique name for the server

Name: my-server

Block the server to disable access

Input server's description

Set permissions to the server

Granted users

NAME	ROLE
□ oathmm	admin
□ admin1	admin
□ oathhotp	admin
□ stephanie99	admin
□ admin-static-oath	admin
□ ad-test	admin

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

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

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

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

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

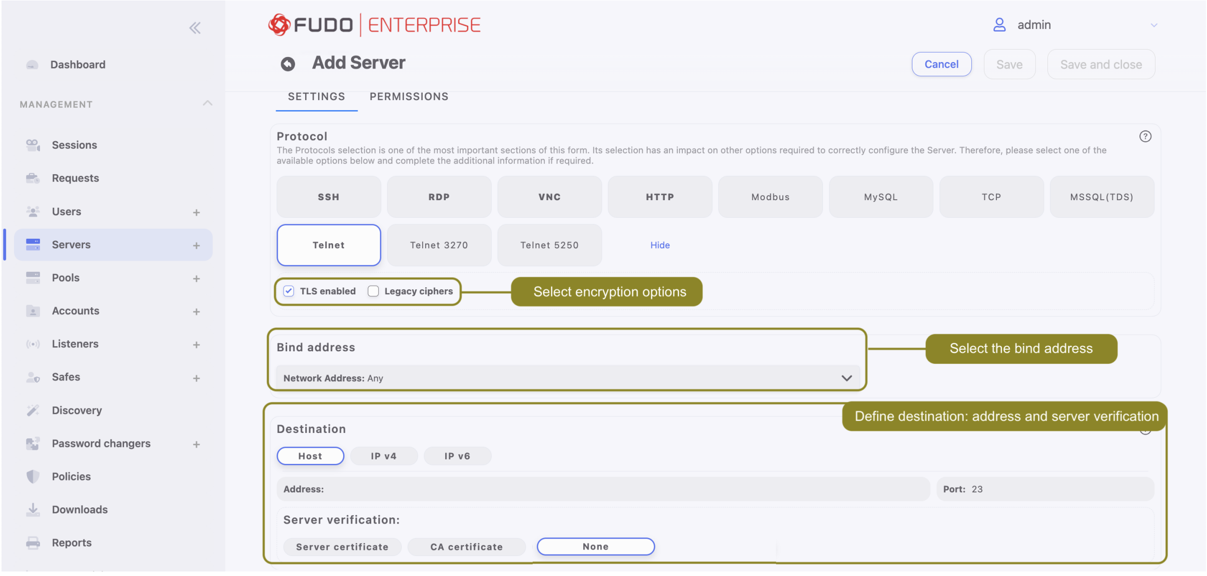
Note:

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

9. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.

- If the *TLS enabled* was checked, in the *Server verification* section select one of the following options:`Server certificate` or `CA certificate` and provide respective certificate data. Select `None` to disable server verification.



Protocol

The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

☑ TLS enabled □ Legacy ciphers

Select encryption options

Bind address

Network Address: Any

Select the bind address

Define destination: address and server verification

Destination

Address:

Port: 23

Server verification:

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

Related topics:

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

7.1.8 Creating a Telnet 3270 server

Note:

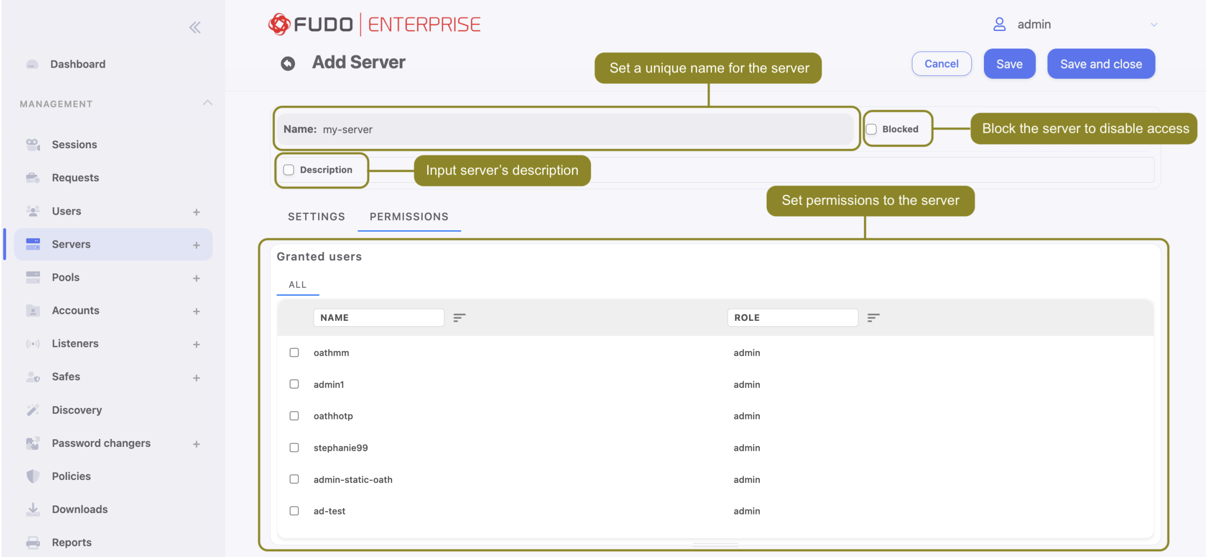
- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- In case of Telnet connections over *forward* and *regular* accounts, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise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

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

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

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

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



Set a unique name for the server

Block the server to disable access

Input server's description

Set permissions to the server

NAME	ROLE
□ oathmm	admin
□ admin1	admin
□ oathhotp	admin
□ stephanie99	admin
□ admin-static-oath	admin
□ ad-test	admin

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

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

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

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

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

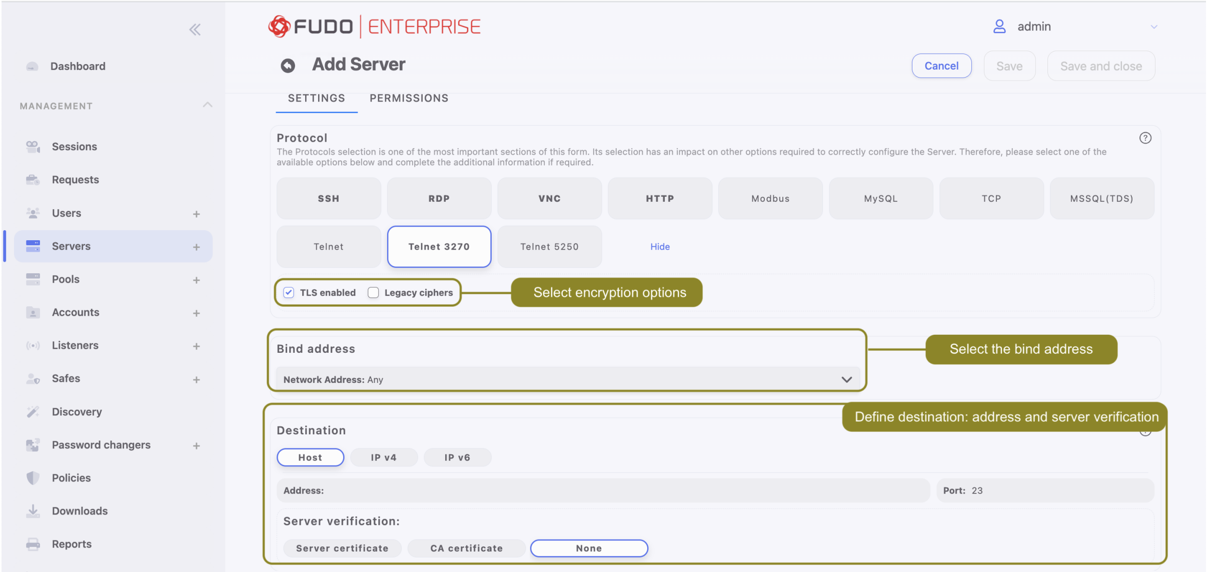
Note:

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

9. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.

- If the *TLS enabled* was checked, in the *Server verification* section select one of the following options:`Server certificate` or `CA certificate` and provide respective certificate data. Select `None` to disable server verification.



Protocol

The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

☑ TLS enabled ☐ Legacy ciphers

Select encryption options

Bind address

Network Address: Any

Select the bind address

Destination

Define destination: address and server verification

Address:

Port: 23

Server verification:

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

Related topics:

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

7.1.9 Creating a Telnet 5250 server

Note:

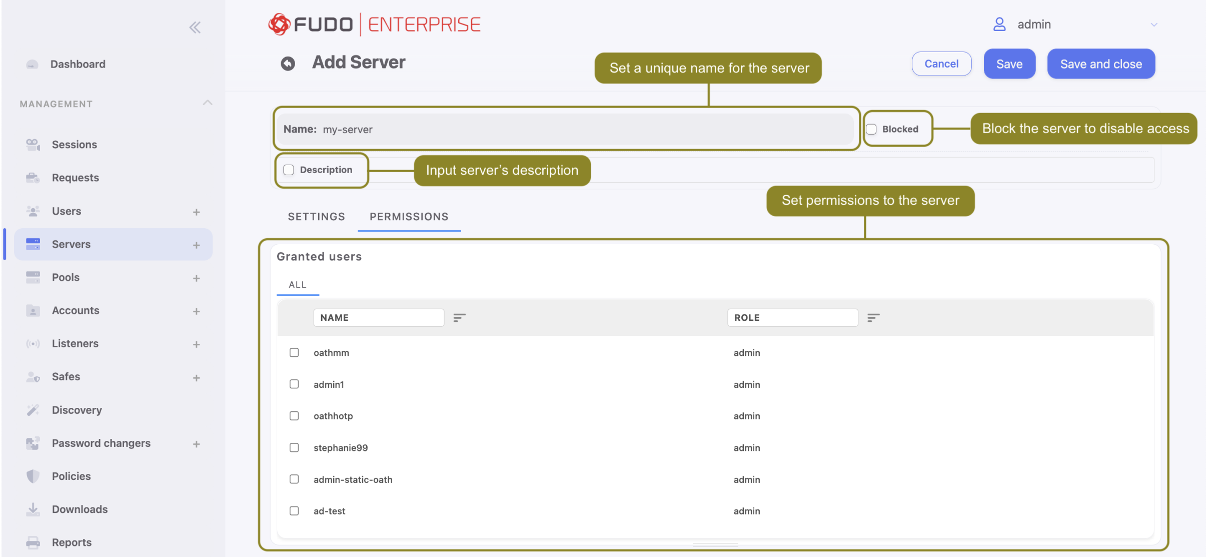
- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- In case of Telnet connections over *forward* and *regular* accounts, users are asked to provide their login credentials twice. First time to authenticate against Fudo Enterprise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

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

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

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

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



Set a unique name for the server

Name: my-server

□ Blocked

Block the server to disable access

□ Description

Input server's description

Set permissions to the server

Granted users

	NAME	ROLE
□	oathmm	admin
□	admin1	admin
□	oathhotp	admin
□	stephanie99	admin
□	admin-static-oath	admin
□	ad-test	admin

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

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

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

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

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

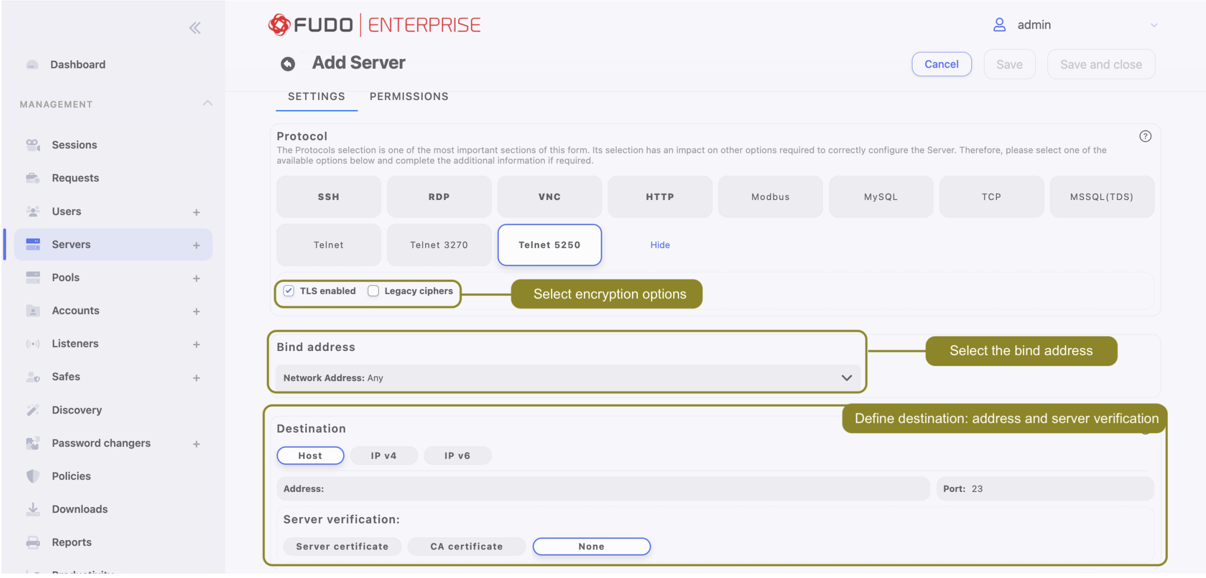
Note:

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

9. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.

- If the *TLS enabled* was checked, in the *Server verification* section select one of the following options:`Server certificate` or `CA certificate` and provide respective certificate data. Select `None` to disable server verification.



Protocol

The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

☑ TLS enabled ☐ Legacy ciphers

Select encryption options

Bind address

Network Address: Any

Select the bind address

Destination

Define destination: address and server verification

Address:

Port: 23

Server verification: None

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

Related topics:

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

7.1.10 Creating a VNC server

Note:

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

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

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

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

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

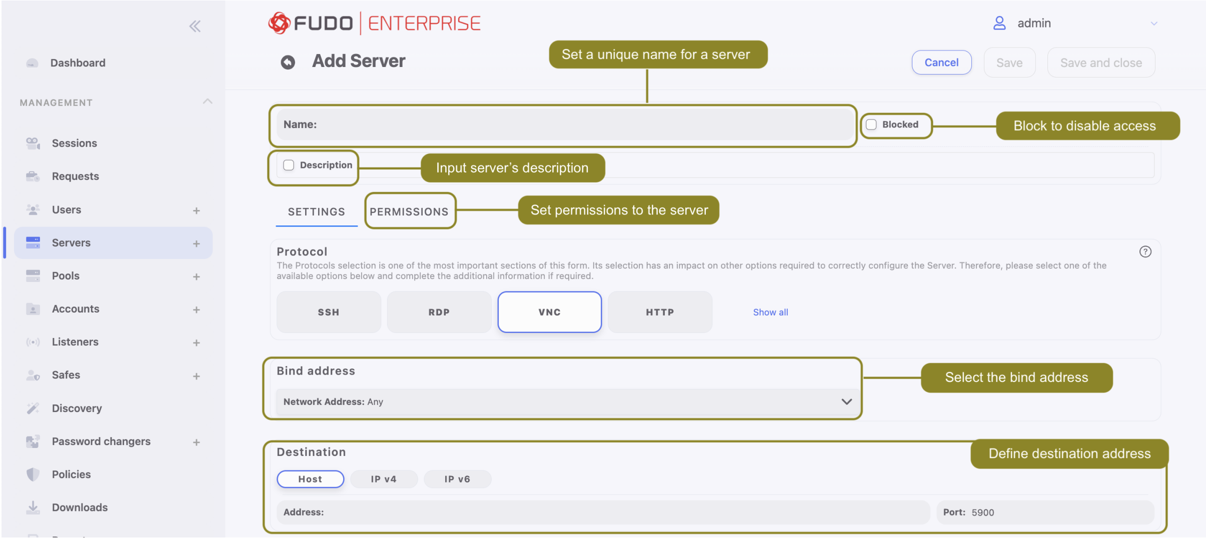
7. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

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

8. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.



The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

Network Address: Any

Address:

Port: 5900

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

Related topics:

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

- *Accounts*

7.1.11 Creating a TCP server

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

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

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

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

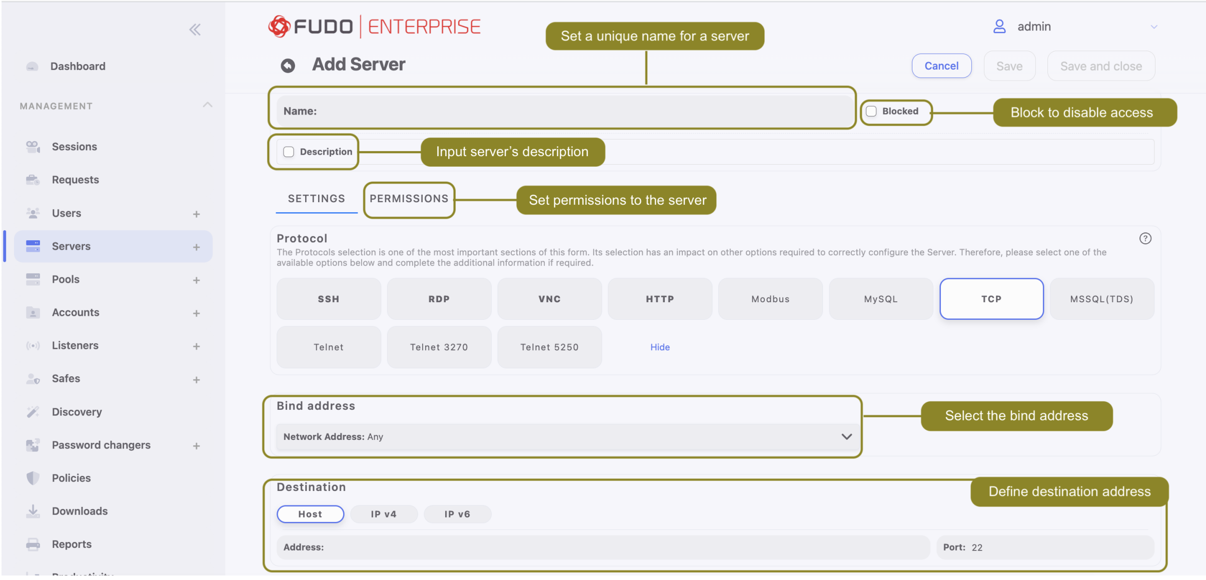
7. From the *Bind address* drop-down list, select Fudo Enterprise IP address used for communicating with this server.

Note:

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

8. In the *Destination* section select `Host`, `IPv4` or `IPv6`. Enter server's IP address.

Note: Depending on selected option, default values for the *Mask* and *Port* fields are filled out automatically. This way the Fudo Enterprise system detects server as one with unique address. In order to set up address for entire subnet, provide a dedicated value for the *Address* and the *Mask* fields.



The Protocols selection is one of the most important sections of this form. Its selection has an impact on other options required to correctly configure the Server. Therefore, please select one of the available options below and complete the additional information if required.

Set a unique name for a server

Block to disable access

Input server's description

Set permissions to the server

Select the bind address

Define destination address

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

Related topics:

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

7.2 Editing a server

1. Select *Management* > *Servers*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.
3. Find and click desired object's name to open its configuration page.
4. Modify configuration parameters as needed.
5. Click *Save*.

Related topics:

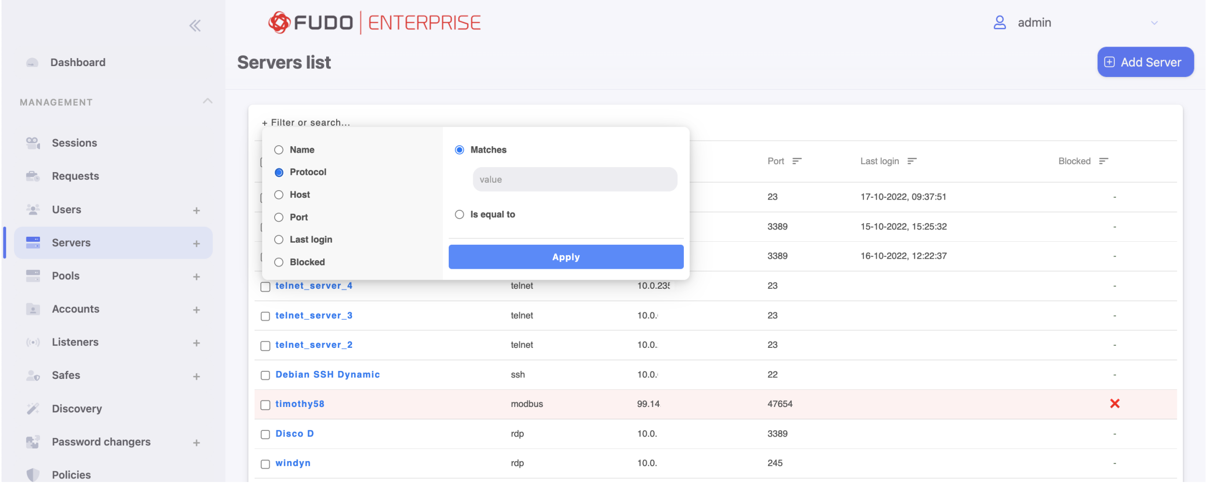
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*

7.3 Blocking a server

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

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

1. Select *Management > Servers*.
2. Define filters to limit the number of objects displayed on the list, or select a server that needs to be blocked right from the list.



Servers list

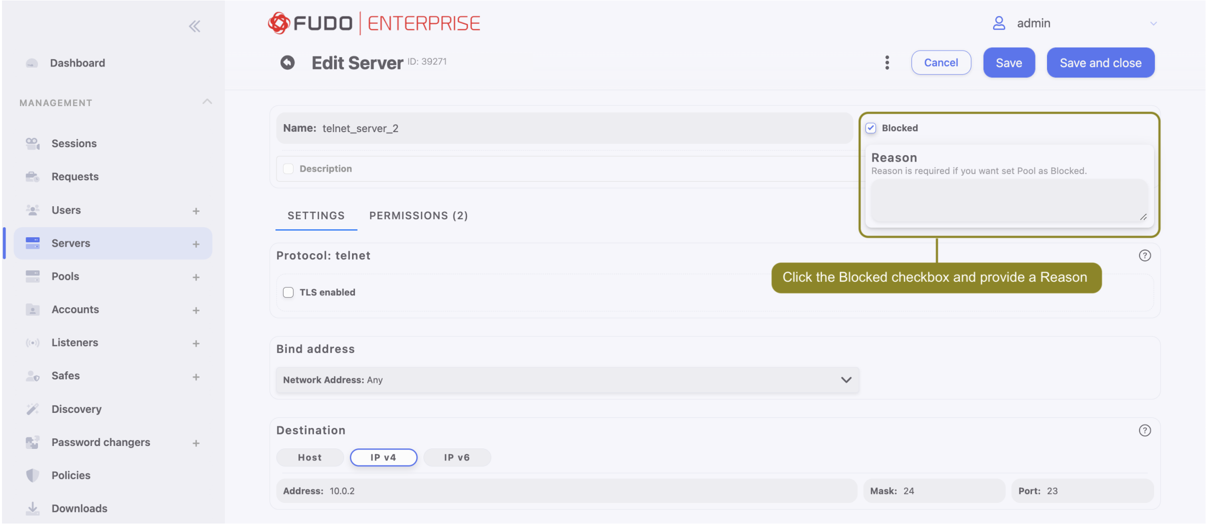
+ Filter or search...

○ Name
● Protocol
○ Host
○ Port
○ Last login
○ Blocked

● Matches
value
○ Is equal to

			Port	Last login	Blocked
			23	17-10-2022, 09:37:51	-
			3389	15-10-2022, 15:25:32	-
			3389	16-10-2022, 12:22:37	-
□	telnet_server_4	telnet	10.0.23	23		-
□	telnet_server_3	telnet	10.0.	23		-
□	telnet_server_2	telnet	10.0.	23		-
□	Debian SSH Dynamic	ssh	10.0.	22		-
□	timothy58	modbus	99.14	47654		✗
□	Disco D	rdp	10.0.	3389		-
□	windyn	rdp	10.0.	245		-

3. Select the object and click the *Blocked* option.
4. Provide blocking reason and click *Set Reason*.



Edit Server ID: 39271

Name: telnet_server_2

Description

☑ Blocked

Reason
Reason is required if you want set Pool as Blocked.

Click the Blocked checkbox and provide a Reason

Protocol: telnet

□ TLS enabled

Bind address

Network Address: Any

Destination

Address: 10.0.2 Mask: 24 Port: 23

5. Click *Save* or *Save and close.*

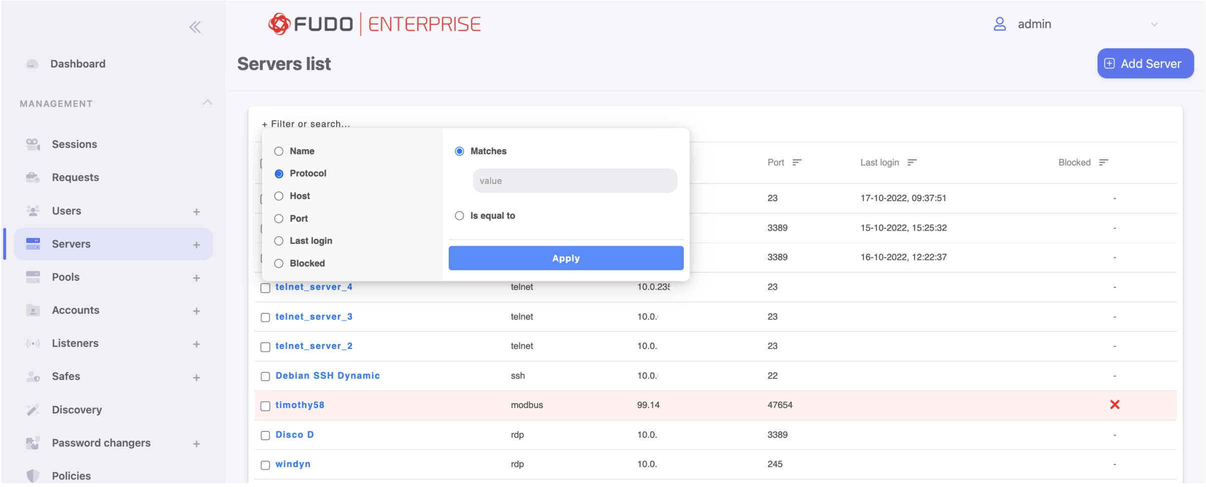
Related topics:

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

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

7.4 Unblocking a server

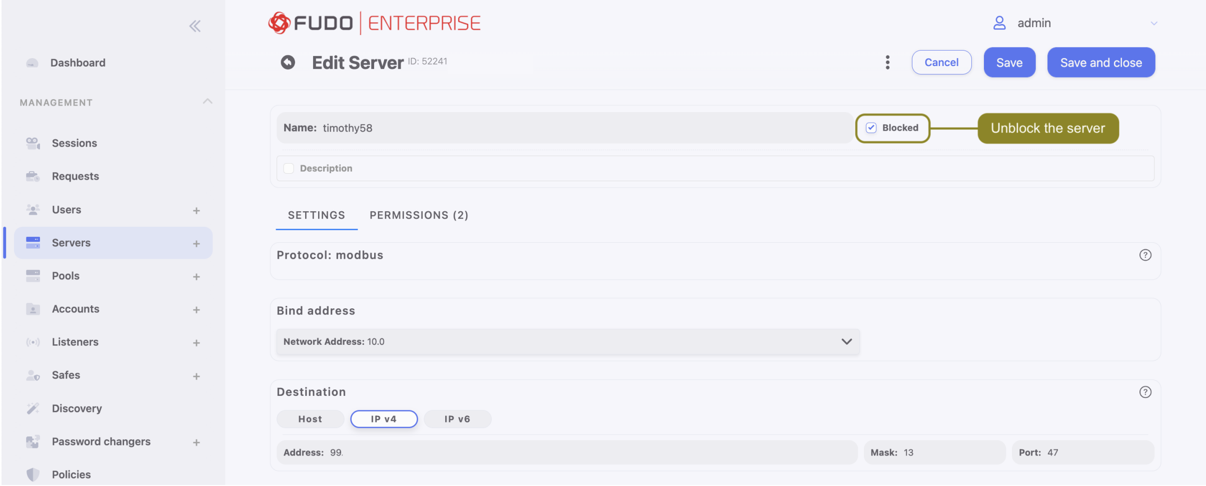
1. Select *Management > Servers*.
2. Define filters to limit the number of objects displayed on the list, or select a server that needs to be unblocked right from the list.



Servers list

			Port	Last login	Blocked
			23	17-10-2022, 09:37:51	-
			3389	15-10-2022, 15:25:32	-
			3389	16-10-2022, 12:22:37	-
□ telnet_server_4	telnet	10.0.235	23		-
□ telnet_server_3	telnet	10.0.	23		-
□ telnet_server_2	telnet	10.0.	23		-
□ Debian SSH Dynamic	ssh	10.0.	22		-
□ timothy58	modbus	99.14	47654		✗
□ Disco D	rdp	10.0.	3389		-
□ windyn	rdp	10.0.	245		-

3. Select the server and click the *Blocked* option.



Edit Server ID: 52241

Name: timothy58

☑ Blocked

Description

Protocol: modbus

Bind address

Network Address: 10.0

Destination

Address: 99.

Mask: 13

Port: 47

4. Click *Save* or *Save and close*.

Related topics:

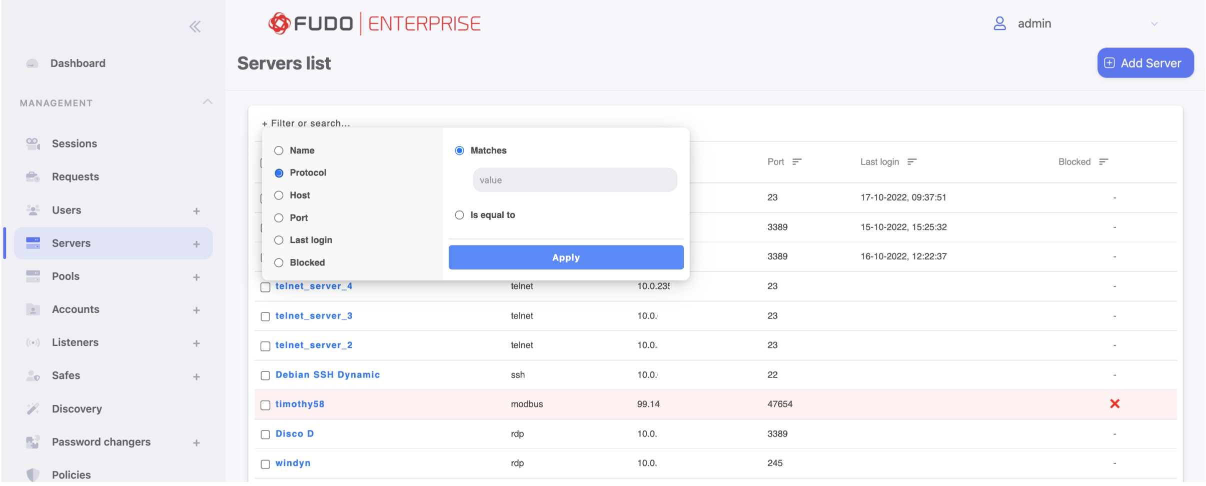
- *Data model*
- *System initiation*
- *Users*
- *Listeners*

- *Safes*
- *Accounts*

7.5 Deleting a server

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

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

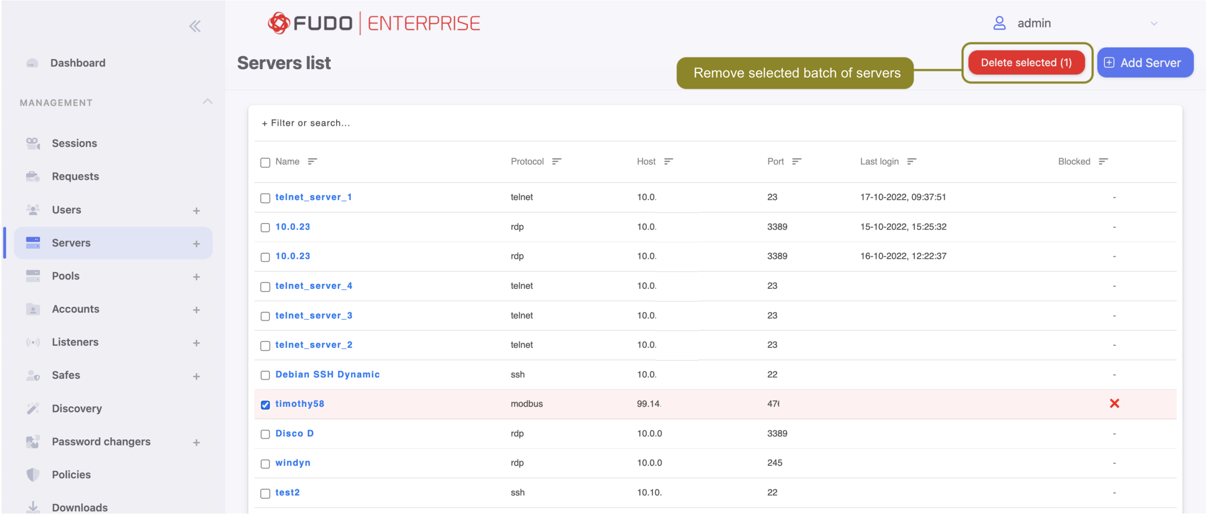


○ Name
● Protocol
○ Host
○ Port
○ Last login
○ Blocked

● Matches: value
○ Is equal to

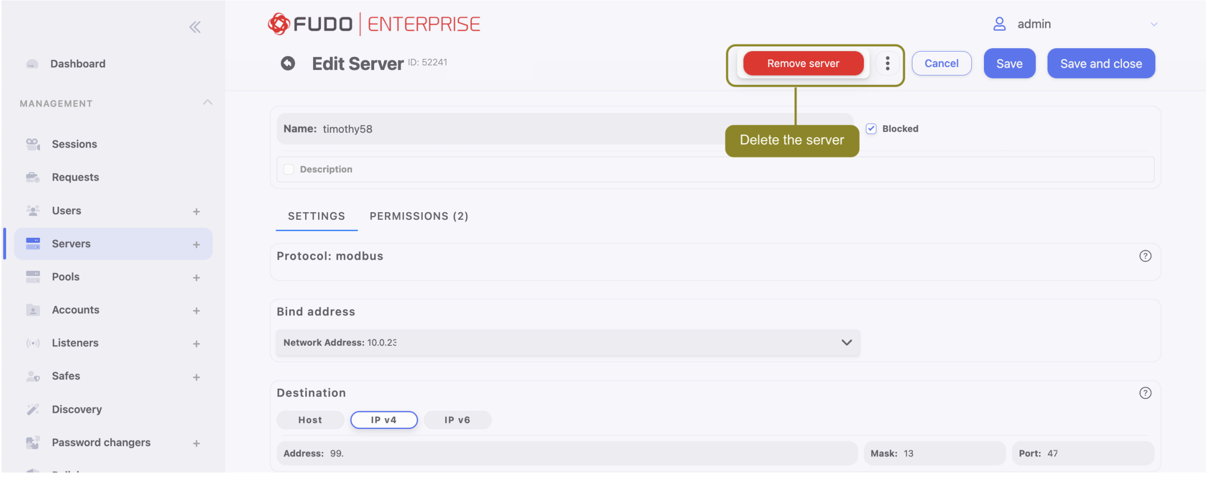
			Port	Last login	Blocked
			23	17-10-2022, 09:37:51	-
			3389	15-10-2022, 15:25:32	-
			3389	16-10-2022, 12:22:37	-
□ telnet_server_4	telnet	10.0.23	23		-
□ telnet_server_3	telnet	10.0.	23		-
□ telnet_server_2	telnet	10.0.	23		-
□ Debian SSH Dynamic	ssh	10.0.	22		-
□ timothy58	modbus	99.14	47654		✗
□ Disco D	rdp	10.0.	3389		-
□ windyn	rdp	10.0.	245		-

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



□ Name	Protocol	Host	Port	Last login	Blocked
□ telnet_server_1	telnet	10.0.	23	17-10-2022, 09:37:51	-
□ 10.0.23	rdp	10.0.	3389	15-10-2022, 15:25:32	-
□ 10.0.23	rdp	10.0.	3389	16-10-2022, 12:22:37	-
□ telnet_server_4	telnet	10.0.	23		-
□ telnet_server_3	telnet	10.0.	23		-
□ telnet_server_2	telnet	10.0.	23		-
□ Debian SSH Dynamic	ssh	10.0.	22		-
☑ timothy58	modbus	99.14	47		✗
□ Disco D	rdp	10.0.0	3389		-
□ windyn	rdp	10.0.0	245		-
□ test2	ssh	10.10.	22		-

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



Name: timothy58

☑ Blocked

□ Description

Protocol: modbus

Bind address

Network Address: 10.0.23

Destination

Host | IP v4 | IP v6

Address: 99.

Mask: 13

Port: 47

4. Confirm server(s) deleting.

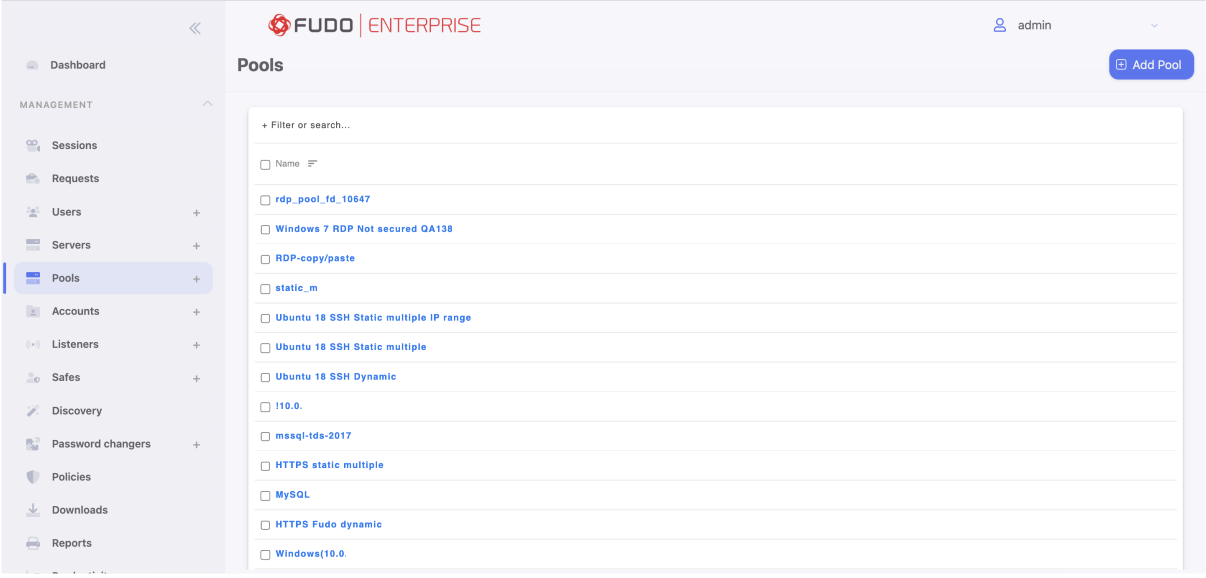
Related topics:

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

CHAPTER 8

Pools

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



□ Name
□ rdp_pool_fd_10647
□ Windows 7 RDP Not secured QA138
□ RDP-copy/paste
□ static_m
□ Ubuntu 18 SSH Static multiple IP range
□ Ubuntu 18 SSH Static multiple
□ Ubuntu 18 SSH Dynamic
□ !10.0.
□ mssql-tds-2017
□ HTTPS static multiple
□ MySQL
□ HTTPS Fudo dynamic
□ Windows(10.0.

8.1 Creating a pool

In order to create a pool, follow the instructions:

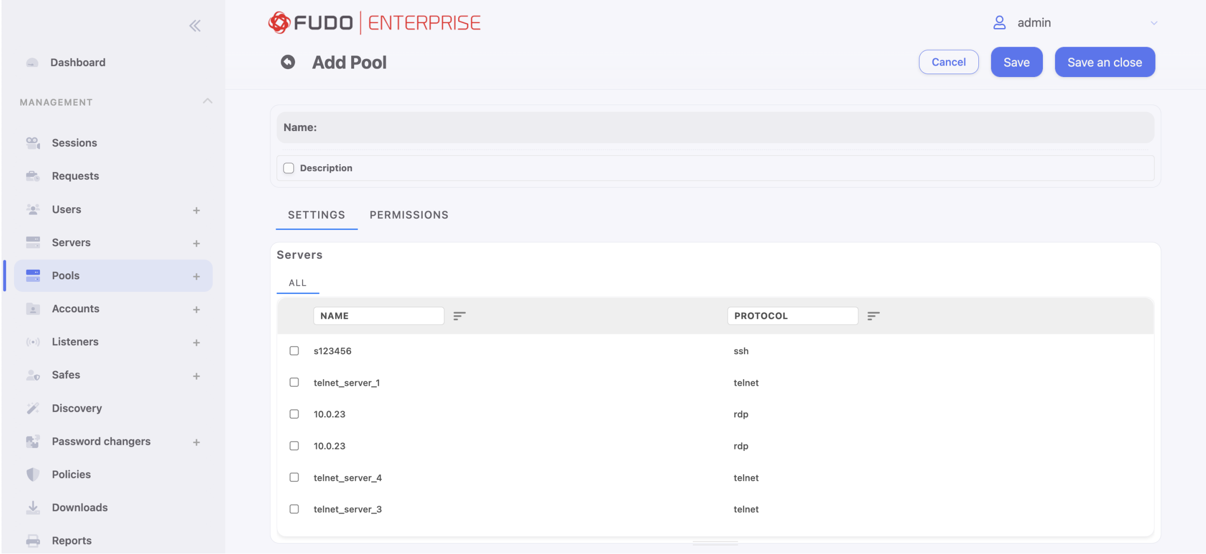
1. Click + icon in the main menu next to the *Pools* tab, or

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

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

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

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



NAME	PROTOCOL
□ s123456	ssh
□ telnet_server_1	telnet
□ 10.0.23	rdp
□ 10.0.23	rdp
□ telnet_server_4	telnet
□ telnet_server_3	telnet

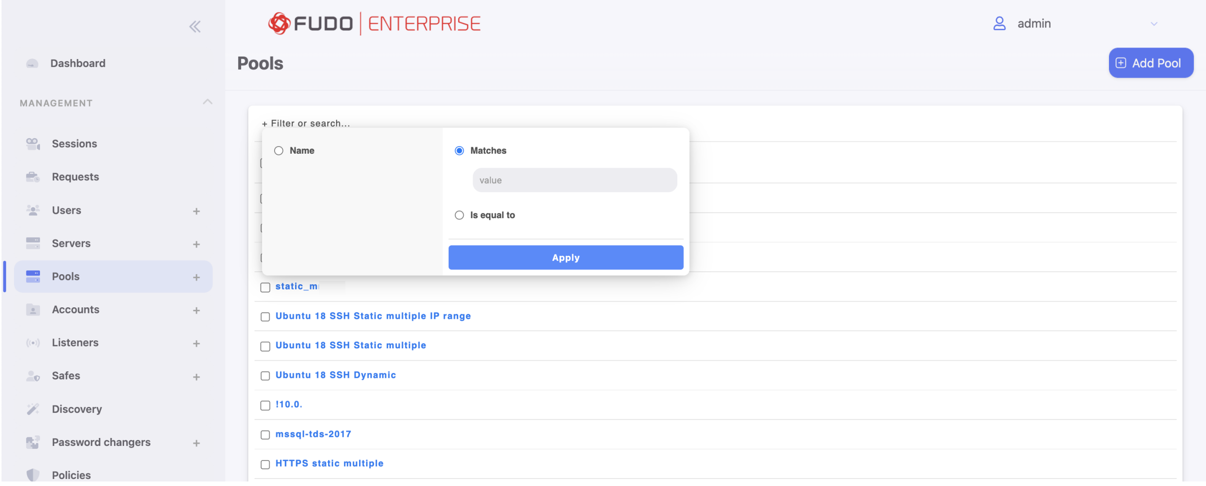
6. Click *Save* or *Save and close*.

8.2 Deleting a pool

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

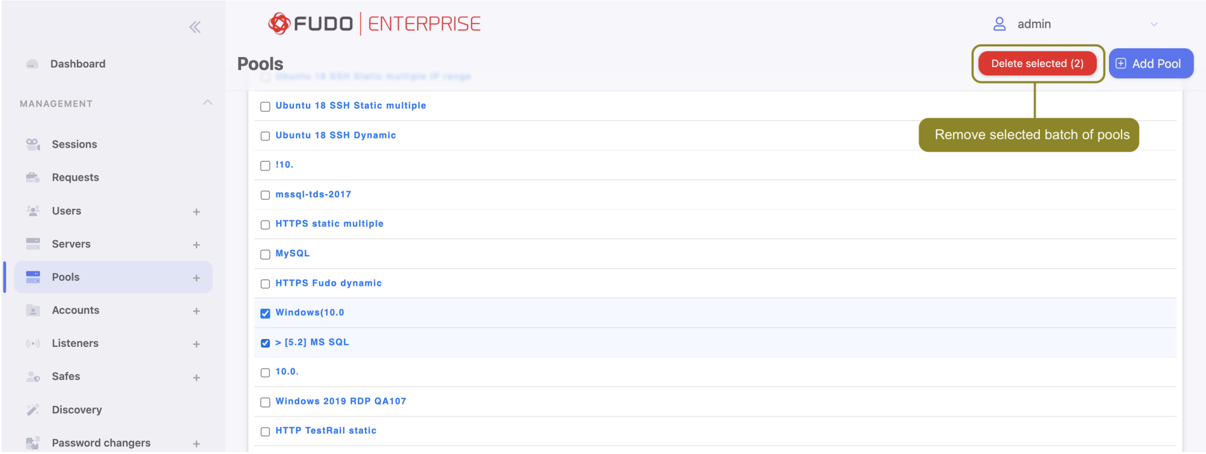
In order to delete a pool, follow the instructions:

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



□ static_m
□ Ubuntu 18 SSH Static multiple IP range
□ Ubuntu 18 SSH Static multiple
□ Ubuntu 18 SSH Dynamic
□ !10.0.
□ mssql-tds-2017
□ HTTPS static multiple

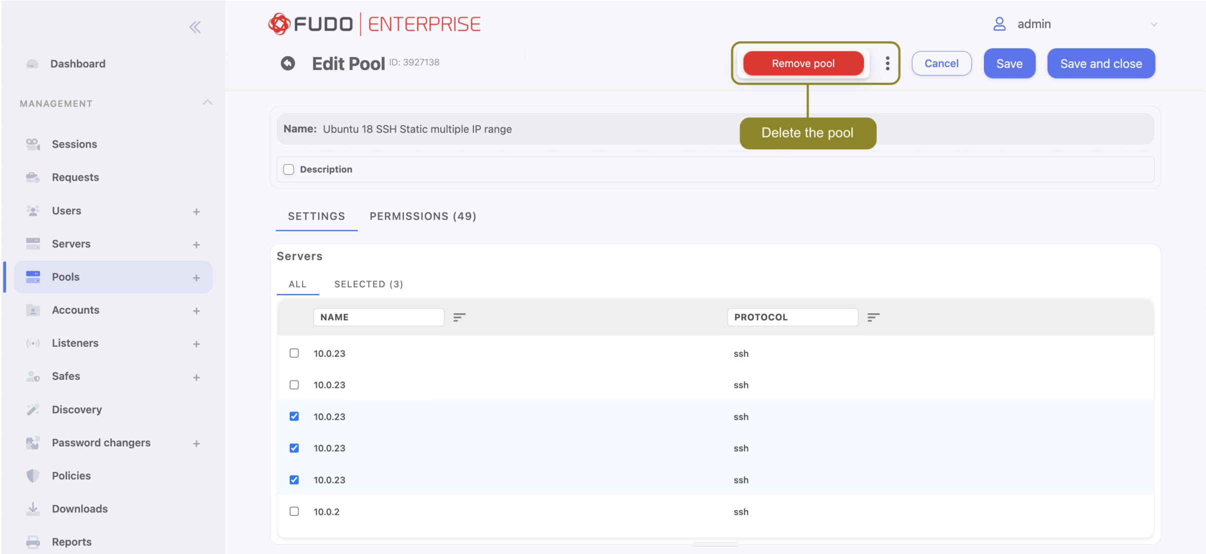
3. Use checkboxes next to the pool(s) and click *Delete selected*.



Remove selected batch of pools

- ☐ Ubuntu 18 SSH Static multiple
- ☐ Ubuntu 18 SSH Dynamic
- ☐ !10.
- ☐ mssql-tds-2017
- ☐ HTTPS static multiple
- ☐ MySQL
- ☐ HTTPS Fudo dynamic
- ☑ Windows(10.0
- ☑ > [5.2] MS SQL
- ☐ 10.0.
- ☐ Windows 2019 RDP QA107
- ☐ HTTP TestRail static

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



Delete the pool

Name: Ubuntu 18 SSH Static multiple IP range

☐ Description

	NAME	PROTOCOL
☐	10.0.23	ssh
☐	10.0.23	ssh
☑	10.0.23	ssh
☑	10.0.23	ssh
☑	10.0.23	ssh
☐	10.0.2	ssh

4. Confirm pool(s) deleting.

Related topics:

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

CHAPTER 9

Remote applications

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

You can configure remote application entries for specific resource for its future connection by a user via Access Gateway and Remote Desktop Protocol client.

9.1 Adding remote application

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

1. Select *Management > Remote applications*.
2. Click the *Add remote application* button.
3. Provide remote application configuration:

- Enter application's *Name*,
- provide *Path* to the executable file, and
- the *Arguments* within two %% symbols, e.g., `%%variable%%`. Defining variable shows additional configuration row where you can define which object and what property of object to use,
- select *Object type* and *Object property* for each of your Arguments,
- encrypt given arguments by selecting *Encrypt* option.

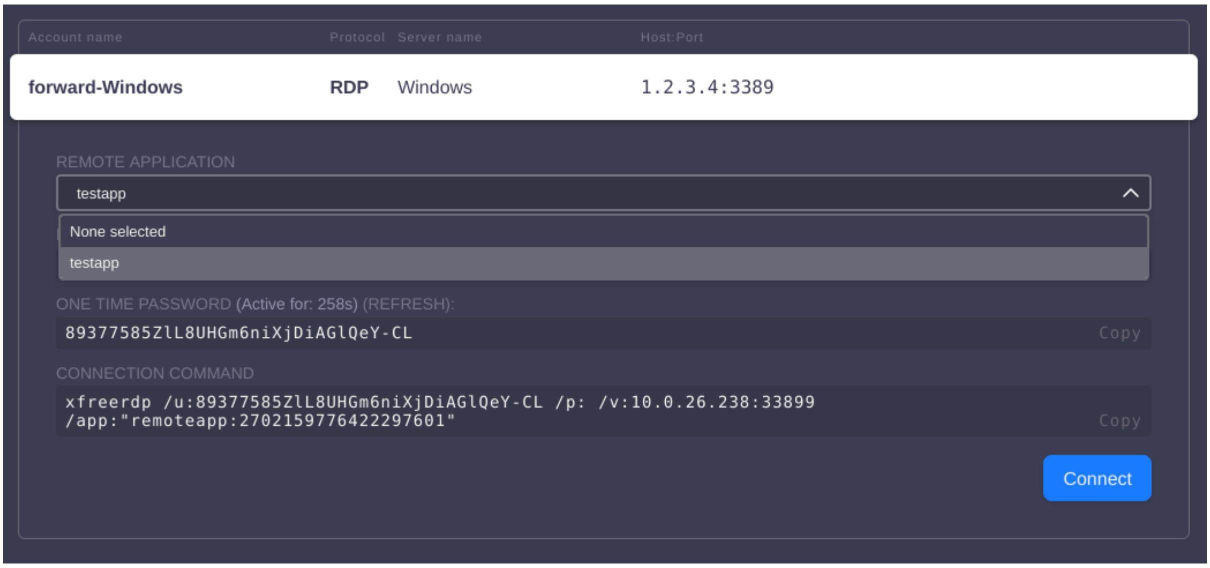
4. Click *Save* or *Save and close*.
5. Add the predefined remote application to the Account with access to the RDP server:

- Select *Management > Accounts*,
- select the account with access to the RDP server or create a new one,

- in the *Remote applications* section click the *Add remote application* button and select the predefined remote application.
- click the button *Save*.

9.2 Connecting to remote application via Access Gateway

In order to establish a connection, sign in to the Access Gateway and select the respective account and a listener to be connected using the predefined remote application. Select the Native client option.



Account name	Protocol	Server name	Host:Port
forward-Windows	RDP	Windows	1.2.3.4:3389

REMOTE APPLICATION: testapp

ONE TIME PASSWORD (Active for: 258s) (REFRESH):

```
89377585ZlL8UHGm6niXjDiAGlQeY-CL
```

CONNECTION COMMAND

```
xfreerdp /u:89377585ZlL8UHGm6niXjDiAGlQeY-CL /p: /v:10.0.26.238:33899
/app:"remoteapp:2702159776422297601"
```

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

9.3 Deleting remote application

Deleting a definition of the remote application

In order to delete a remote application definition, follow the instructions:

1. Select *Management > Remote applications*.
2. Select a remote application definition that needs to be deleted right from the list.
3. In the edit mode click on the vertical three-dot icon.
4. Press the *Remove Application* button.
5. Confirm the remote application removal.

Deleting a remote application from the Account definition

In order to delete a predefined remote application from the Account definition, follow the instructions:

1. Select *Management > Accounts*.

2. Select the account that has the predefined remote application configured.
3. In the *Remote applications* section the *Delete* option to remove the predefined remote application.
4. Click the button *Save*.

Related topics:

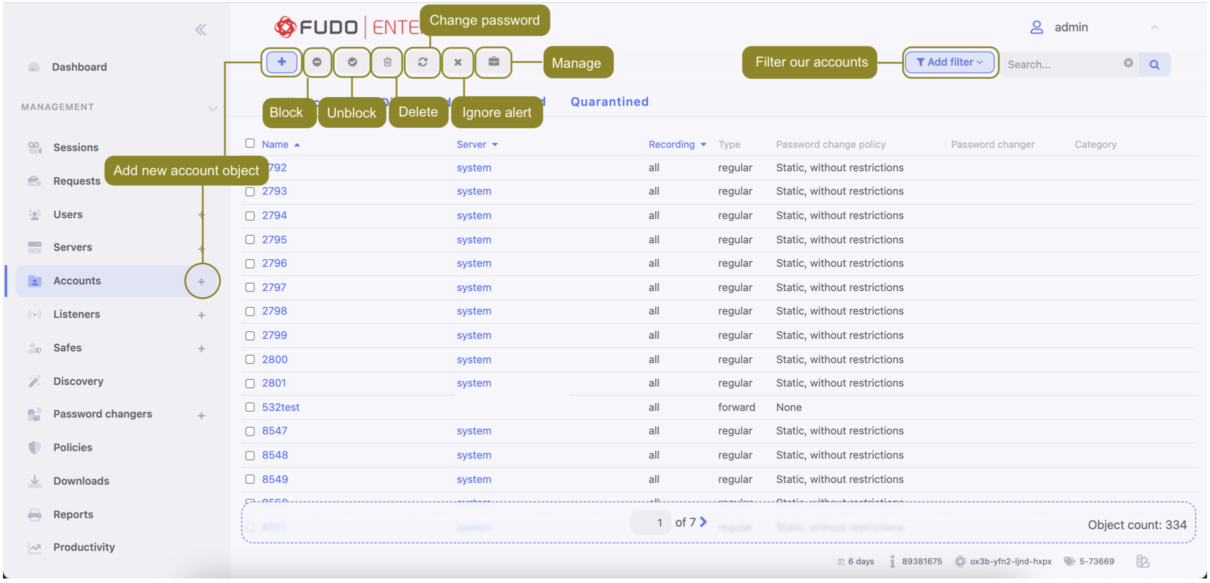
- *Data model*
- *System initiation*
- *Users*
- *Listeners*
- *Safes*
- *Accounts*
- *Creating an account*

CHAPTER 10

Accounts

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

Note: In case of Telnet connections, user has to go through authentication process twice. First time to authenticate against Fudo Enterprise and then to connect to the target host.



Name	Server	Recording	Type	Password change policy	Password changer	Category
792	system	all	regular	Static, without restrictions		
2793	system	all	regular	Static, without restrictions		
2794	system	all	regular	Static, without restrictions		
2795	system	all	regular	Static, without restrictions		
2796	system	all	regular	Static, without restrictions		
2797	system	all	regular	Static, without restrictions		
2798	system	all	regular	Static, without restrictions		
2799	system	all	regular	Static, without restrictions		
2800	system	all	regular	Static, without restrictions		
2801	system	all	regular	Static, without restrictions		
532test		all	forward	None		
8547	system	all	regular	Static, without restrictions		
8548	system	all	regular	Static, without restrictions		
8549	system	all	regular	Static, without restrictions		

1 of 7 Object count: 334

6 days 89381675 ox3b-yfn2-ijnd-hxpx 5-73669

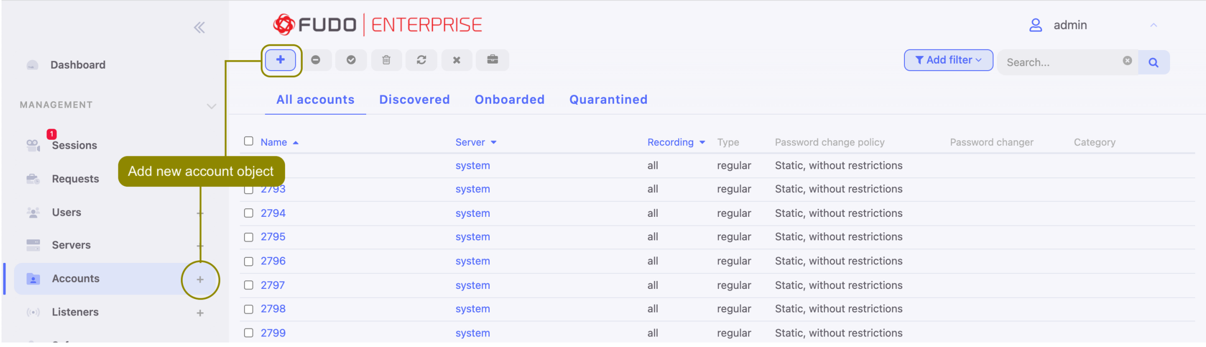
10.1 Creating an account

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.

10.1.1 Creating an *anonymous* account

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

Select *Management* > *Accounts* and then click + *Add*.

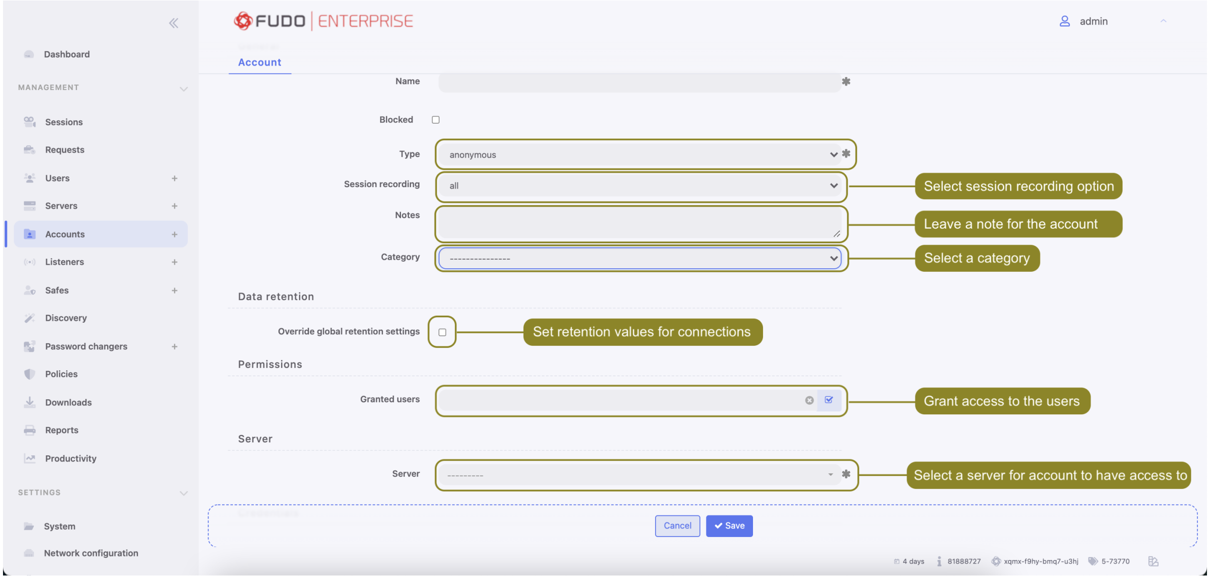


Add new account object

Name	Server	Recording	Type	Password change policy	Password changer	Category
	system	all	regular	Static, without restrictions		
2793	system	all	regular	Static, without restrictions		
2794	system	all	regular	Static, without restrictions		
2795	system	all	regular	Static, without restrictions		
2796	system	all	regular	Static, without restrictions		
2797	system	all	regular	Static, without restrictions		
2798	system	all	regular	Static, without restrictions		
2799	system	all	regular	Static, without restrictions		

2. Define object's name.

3. Select *Blocked* option to disable account after it's created.



Name	
Blocked	□
Type	anonymous
Session recording	all
Notes	
Category	---------------

Data retention

Override global retention settings	□

Permissions

Granted users	

Server

Server	---------

Select session recording option

Leave a note for the account

Select a category

Set retention values for connections

Grant access to the users

Select a server for account to have access to

4. Select `anonymous` from the *Type* drop-down list.

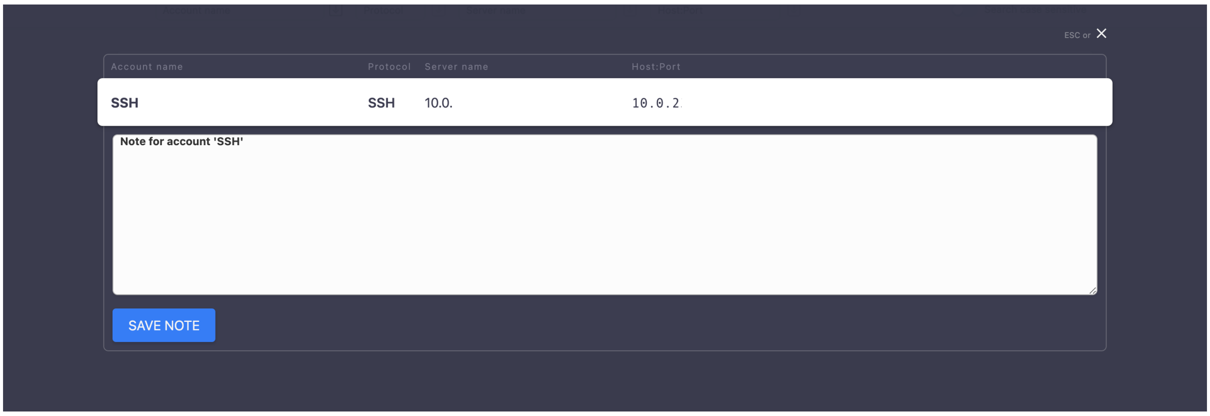
5. Select desired session recording option.

    - `all` - Fudo Enterprise saves session metadata (basic session information), records raw network traffic (RAW file) and stores session data in internal file format (FBS). The latter enables session playback using the built-in session player, as well as exporting sessions to a selection of video file formats.

- `raw` - Fudo Enterprise saves session metadata (basic session information) and records raw network traffic (RAW file). The raw data can be downloaded but it cannot be played back in graphical form using the built-in session player (session player only depicts the networks packet exchange between the client and the target host).
- `noraw` - Fudo Enterprise records the session data in a non-raw format that could be played back using the built-in session player.
- `none` - Fudo Enterprise saves only session metadata (basic session information).

6. In the *Notes* field, enter a message to *User Portal (Access Gateway)* users. If permissions are granted, notes can be also edited.

Note: Account notes can be displayed in the *User Portal (Access Gateway)*.



Account name	Protocol	Server name	Host:Port
SSH	SSH	10.0.	10.0.2

Note for account 'SSH'

7. In the *Category* field select `privileged` or `non-privileged` account category. The category serves an informational purpose.
8. In the *Data retention* section, define automatic data removal settings.
   - Select *Override global retention settings* option to set other than *global retention values* for connections established using this account.
   - Check the *Delete session data* option to exclude sessions from retention mechanism.
   - Next to the *Delete session data* field, define the number of days after which the session data will moved to external storage device. Default value when the option is checked, is 30 days.

Note: Data retention for sessions established using this account will only be active if global retention is enabled. To change global retention settings see chapter *Data Retention*.

9. In the *Permissions* section, add users allowed to manage this object.
10. In the *Server* section, assign account to a specific server or a server pool by selecting it from the *Server* drop-down list.
11. 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.

12. Click *Save*.

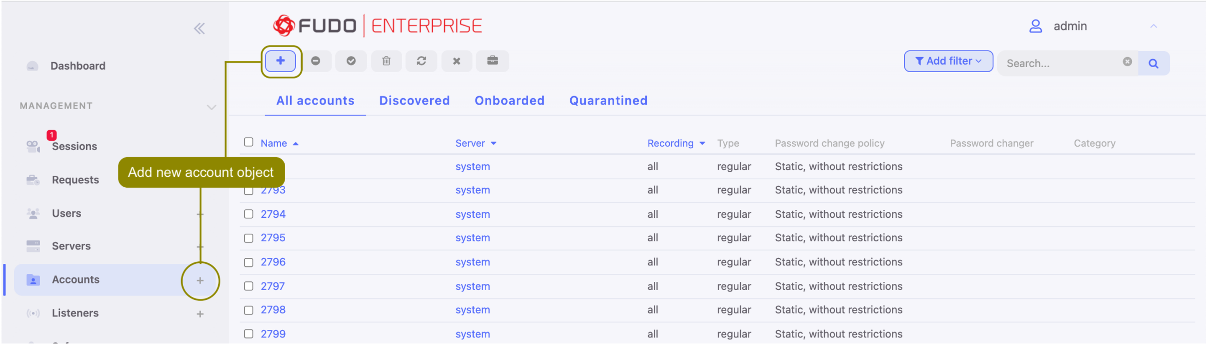
Related topics:

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

10.1.2 Creating a *forward* account

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

Select *Management* > *Accounts* and then click + *Add*.

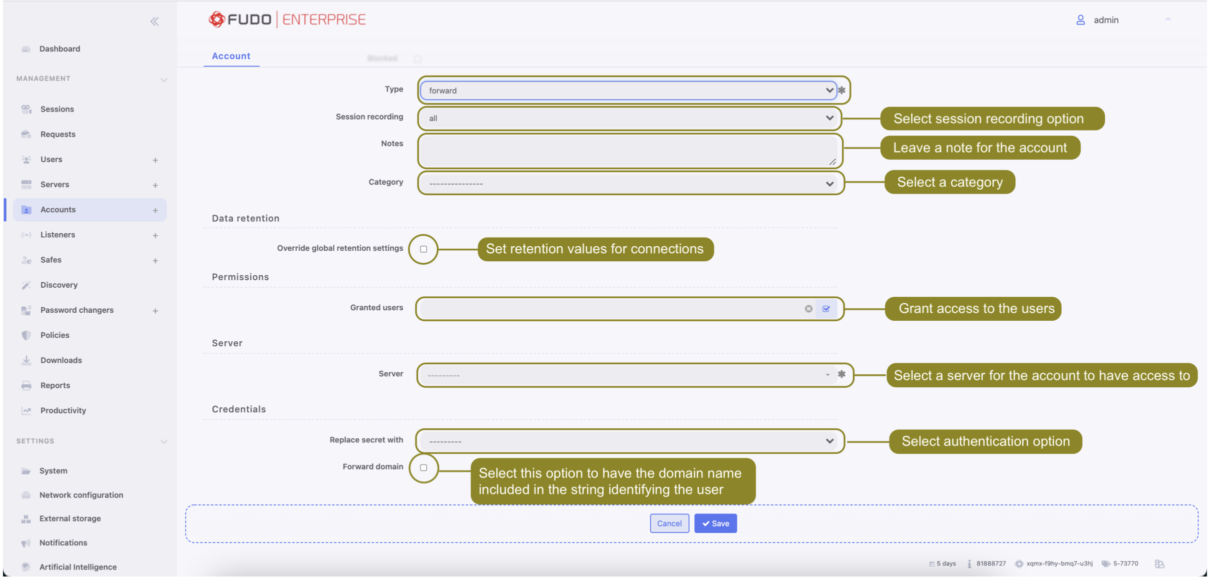


Add new account object

Name	Server	Recording	Type	Password change policy	Password changer	Category
	system	all	regular	Static, without restrictions		
2793	system	all	regular	Static, without restrictions		
2794	system	all	regular	Static, without restrictions		
2795	system	all	regular	Static, without restrictions		
2796	system	all	regular	Static, without restrictions		
2797	system	all	regular	Static, without restrictions		
2798	system	all	regular	Static, without restrictions		
2799	system	all	regular	Static, without restrictions		

2. Define object's name.

3. Select *Blocked* option to disable account after it's created.



Type: forward

Session recording: all — Select session recording option

Notes — Leave a note for the account

Category: --------------- — Select a category

Data retention

Override global retention settings ☐ — Set retention values for connections

Permissions

Granted users — Grant access to the users

Server

Server: --------- — Select a server for the account to have access to

Credentials

Replace secret with: --------- — Select authentication option

Forward domain ☐ — Select this option to have the domain name included in the string identifying the user

4. Select `forward` from the *Type* drop-down list.

5. Select desired session recording option.

   - `all` - Fudo Enterprise saves session metadata (basic session information), records raw network traffic (RAW file) and stores session data in internal file format (FBS). The latter enables session playback using the built-in session player, as well as exporting sessions to a selection of video file formats.

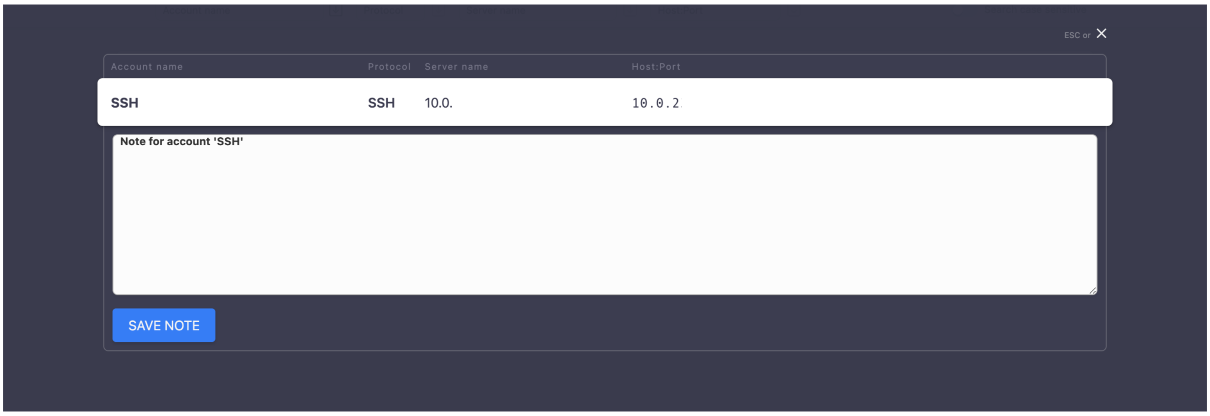
   - `raw` - Fudo Enterprise saves session metadata (basic session information) and records raw network traffic (RAW file). The raw data can be downloaded but it cannot be played back in graphical form using the built-in session player (session player only depicts the networks packet exchange between the client and the target host).

   - `noraw` - Fudo Enterprise records the session data in a non-raw format that could be played back using the built-in session player.

   - `none` - Fudo Enterprise saves only session metadata (basic session information).

6. In the *Notes* field, enter a message to *User Portal (Access Gateway)* users. If permissions are granted, notes can be also edited.

Note: Account notes can be displayed in the *User Portal (Access Gateway)*.



ESC or ×

Account name	Protocol	Server name	Host:Port
SSH	SSH	10.0.	10.0.2

Note for account 'SSH'

7. In the *Category* field select `privileged` or `non-privileged` account category. The category serves an informational purpose.

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

   - Select *Override global retention settings* option to set other than *global retention values* for connections established using this account.

   - Check the *Delete session data* option to exclude sessions from retention mechanism.

   - Next to the *Delete session data* field, define the number of days after which the session data will moved to external storage device. Default value when the option is checked, is 30 days.

Note: Data retention for sessions established using this account will only be active if global retention is enabled. To change global retention settings see chapter *Data Retention*.

9. In the *Permissions* section, add users allowed to manage this object.
10. In the *Server* section, assign account to a specific server or a server pool by selecting it from the *Server* drop-down list.
11. From the *Replace secret with* drop down list in the *Credentials*, 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.

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 Enterprise and once again for accessing target system.

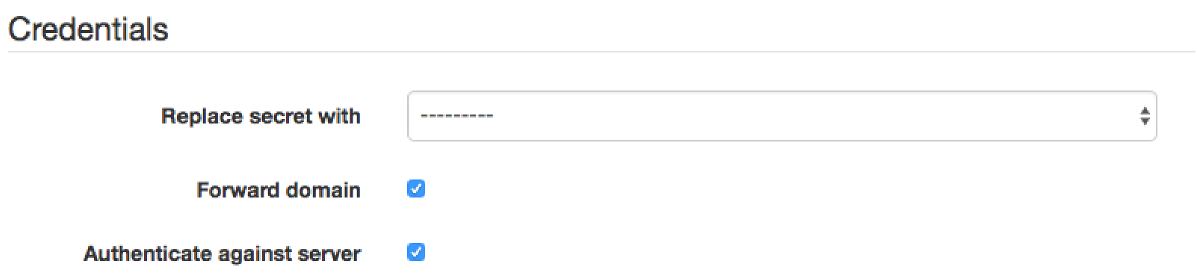
To enable two-fold authentication, select `password` from the *Replace secret with* drop-down list and leave the password and login fields empty.

`password from external repository`

- Select external repository.

Note: *Authentication by the server*

With the *Authentication against server* option enabled, Fudo Enterprise does not verify the correctness of user credentials. Login information is forwarded to the target host, which verifies whether the user is allowed to access it. Verification status is returned to Fudo, which establishes monitored connection. To enable this authentication scenario, select the *Authenticate against server* option in the *Credentials* section (available only for SSH servers and RDP hosts with the *Enhanced RDP Security (TLS) + NLA* security option selected).



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.

12. Select *Forward domain* option to have the domain name included in the string identifying the user.
13. For SSH connections, select the *SSH Agent forwarding* option to authenticate the user against the target host using client's SSH key. Use -A option for connecting to SSH server.
14. Click *Save*.

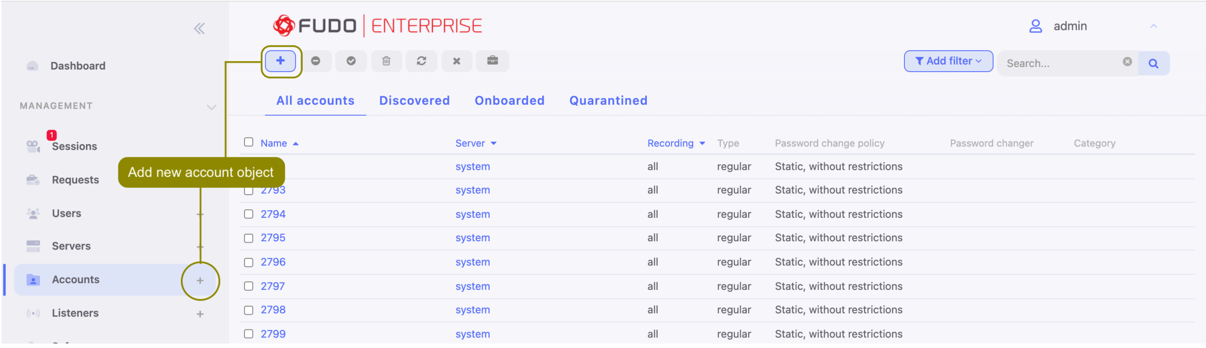
Related topics:

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

10.1.3 Creating a *regular* account

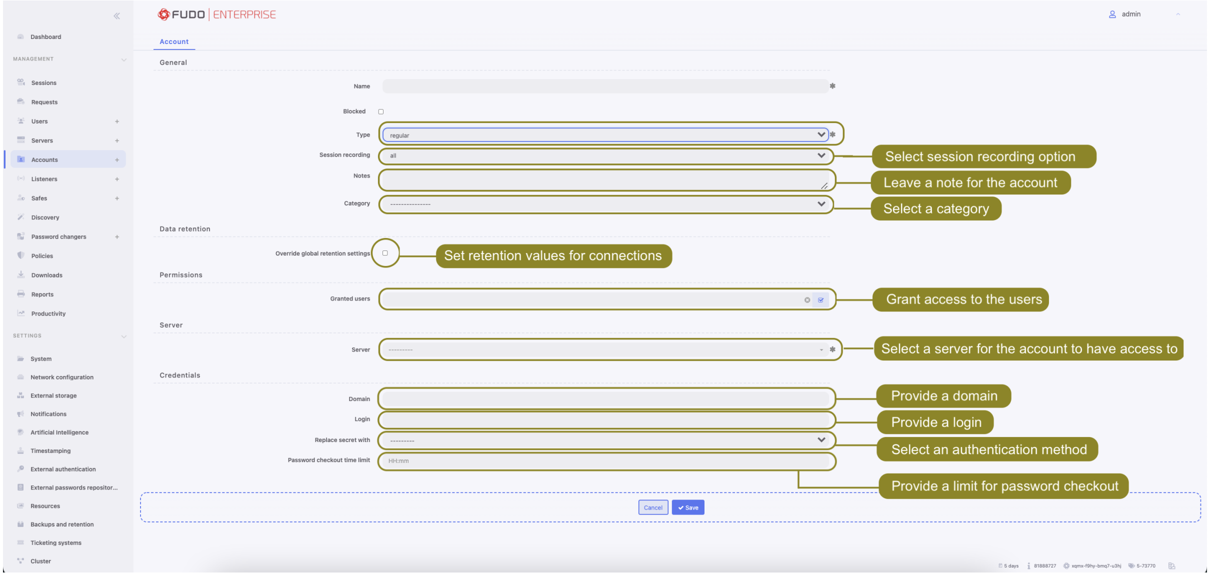
1. Click + icon in the main menu next to the *Accounts* tab, or

Select *Management* > *Accounts* and then click + *Add*.



□ Name	Server	Recording	Type	Password change policy	Password changer	Category
	system	all	regular	Static, without restrictions		
□ 2793	system	all	regular	Static, without restrictions		
□ 2794	system	all	regular	Static, without restrictions		
□ 2795	system	all	regular	Static, without restrictions		
□ 2796	system	all	regular	Static, without restrictions		
□ 2797	system	all	regular	Static, without restrictions		
□ 2798	system	all	regular	Static, without restrictions		
□ 2799	system	all	regular	Static, without restrictions		

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



General

Name *

Blocked □

Type: regular *

Session recording: all — Select session recording option

Notes — Leave a note for the account

Category: --------------- — Select a category

Data retention

Override global retention settings □ — Set retention values for connections

Permissions

Granted users — Grant access to the users

Server

Server: --------- * — Select a server for the account to have access to

Credentials

Domain — Provide a domain

Login — Provide a login

Replace secret with: --------- — Select an authentication method

Password checkout time limit: HH:mm — Provide a limit for password checkout

4. Select `regular` from the *Type* drop-down list.

5. Select desired session recording option.

   - `all` - Fudo Enterprise saves session metadata (basic session information), records raw network traffic (RAW file) and stores session data in internal file format (FBS). The latter enables session playback using the built-in session player, as well as exporting sessions to a selection of video file formats.

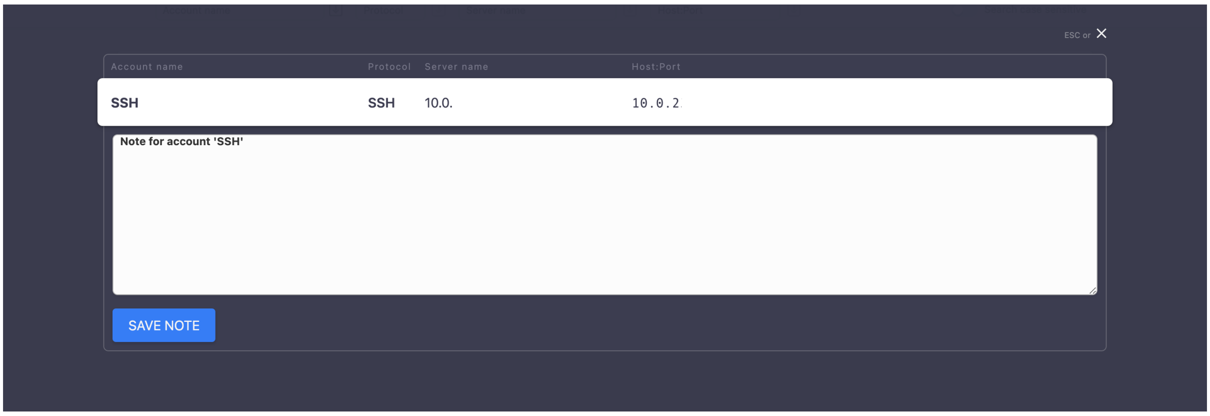
   - `raw` - Fudo Enterprise saves session metadata (basic session information) and records raw network traffic (RAW file). The raw data can be downloaded but it cannot be played back in graphical form using the built-in session player (session player only depicts the networks packet exchange between the client and the target host).

   - `noraw` - Fudo Enterprise records the session data in a non-raw format that could be played back using the built-in session player.

   - `none` - Fudo Enterprise saves only session metadata (basic session information).

6. In the *Notes* field, enter a message to *Access Gateway* users. If permissions are granted, notes can be also edited.

Note: Account notes can be displayed in the *User Portal (Access Gateway)*.



Account name	Protocol	Server name	Host:Port
SSH	SSH	10.0.	10.0.2

Note for account 'SSH'

7. In the *Category* field select `privileged` or `non-privileged` account category. The category serves an informational purpose.

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

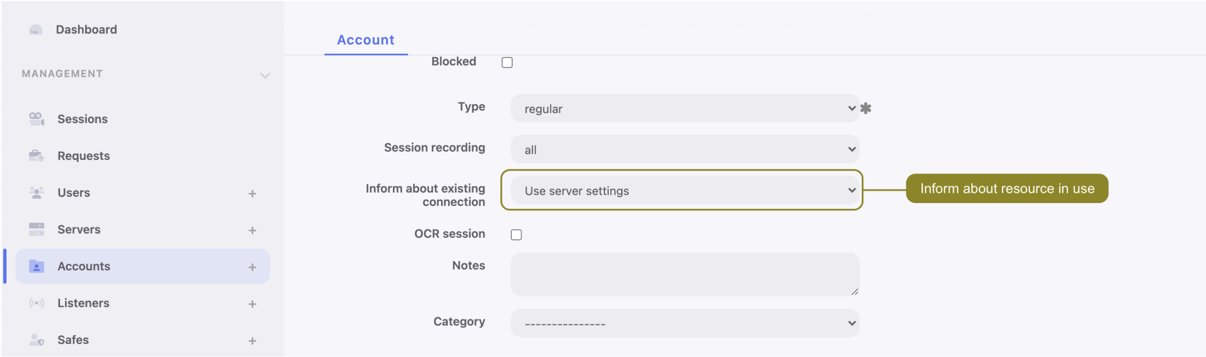
   - Select *Override global retention settings* option to set other than *global retention values* for connections established using this account.
   - Check the *Delete session data* option to exclude sessions from retention mechanism.
   - Next to the *Delete session data* field, define the number of days after which the session data will moved to external storage device. Default value when the option is checked, is 30 days.

Note: Data retention for sessions established using this account will only be active if global retention is enabled. To change global retention settings see chapter *Data Retention*.

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

10. In the *Server* section, assign account to a specific server or a server pool by selecting it from the *Server* drop-down list.

Configuring an account with access to the RDP server, an additional option will show up. In the *Inform about existing connection* field select to set server settings / disable or enable this option.



Blocked ☐
Type: regular
Session recording: all
Inform about existing connection: Use server settings
OCR session ☐
Notes
Category: ---------------

Note: More about this feature under this link: *Account activity in the Access Gateway*.

11. In the *Credentials* section, enter privileged account domain.
12. Type in login to the privileged account.
13. 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 from external repository`

    - Select external repository.

    `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 Enterprise and once again for accessing target system.

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

14. In the *Password checkout time limit* field, define the time after which the password is returned automatically.

Note: Defining the password checkout time limit automatically enables the Secret Checkout feature for the particular Safe.

15. For SSH connections, select the *SSH Agent forwarding* option to authenticate the user against the target host using client's SSH key. Use -A option for connecting to SSH server.

If `password` option was chosen as an authentication method, provide additional configuration:

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

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

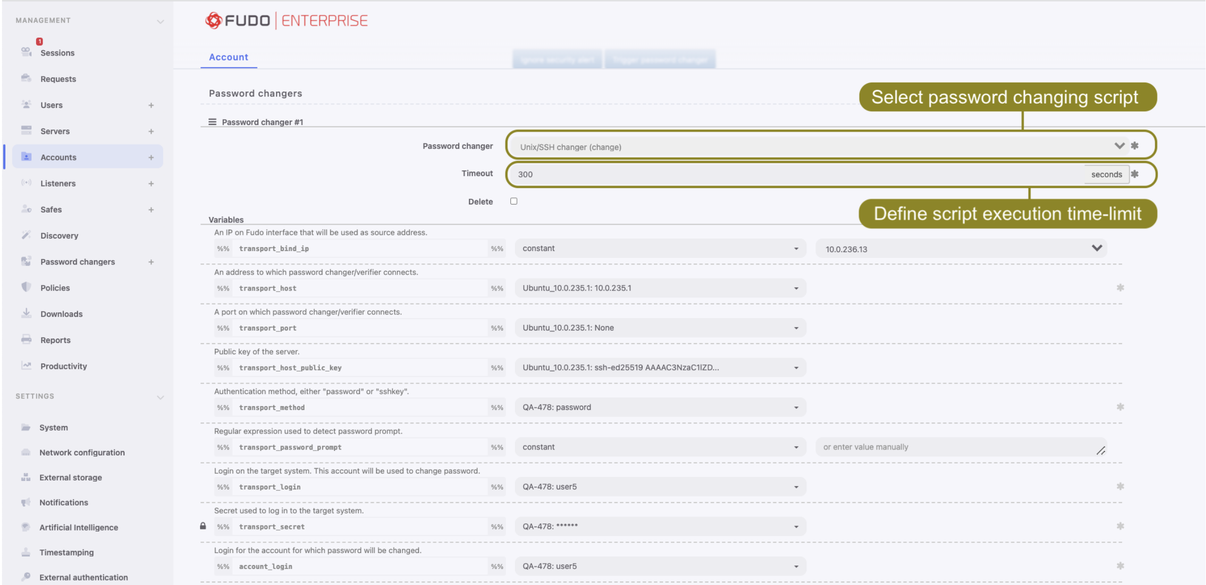
Note: This option requires to choose at least one *Password changer* and a *Password change policy* any other than `Static, without restrictions`.

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

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

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

- Click + *Add password changer*, to have the password to the account changed automatically according to the *password policy*.
- In the *Password changers* section, from the *Password changer* drop-down list select password changer specific for given account.
- In the *Timeout* field, define the script's execution time limit.
- In the *Variables* section, assign attributes to variables.



Select password changing script

Define script execution time-limit

Password changers

Password changer #1

Password changer: Unix/SSH changer (change)

Timeout: 300 seconds

Delete ☐

Variables

An IP on Fudo interface that will be used as source address.
%% transport_bind_ip %% constant 10.0.236.13

An address to which password changer/verifier connects.
%% transport_host %% Ubuntu_10.0.235.1: 10.0.235.1

A port on which password changer/verifier connects.
%% transport_port %% Ubuntu_10.0.235.1: None

Public key of the server.
%% transport_host_public_key %% Ubuntu_10.0.235.1: ssh-ed25519 AAAAC3NzaC1lZD...

Authentication method, either "password" or "sshkey".
%% transport_method %% QA-478: password

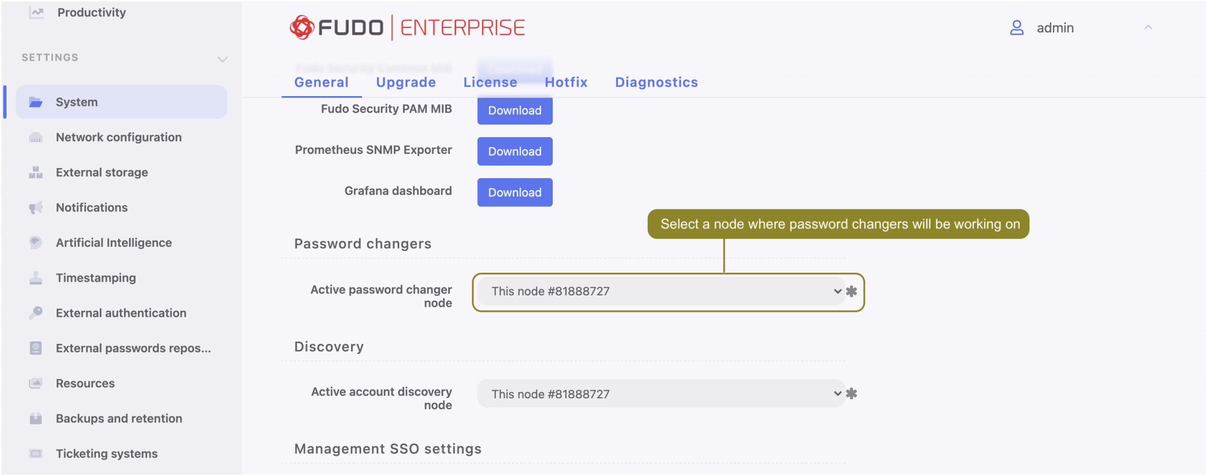
Regular expression used to detect password prompt.
%% transport_password_prompt %% constant or enter value manually

Login on the target system. This account will be used to change password.
%% transport_login %% QA-478: user5

Secret used to log in to the target system.
%% transport_secret %% QA-478: ******

Login for the account for which password will be changed.
%% account_login %% QA-478: user5

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



Fudo Security PAM MIB

Prometheus SNMP Exporter

Grafana dashboard

Select a node where password changers will be working on

Password changers

Active password changer node: This node #81888727

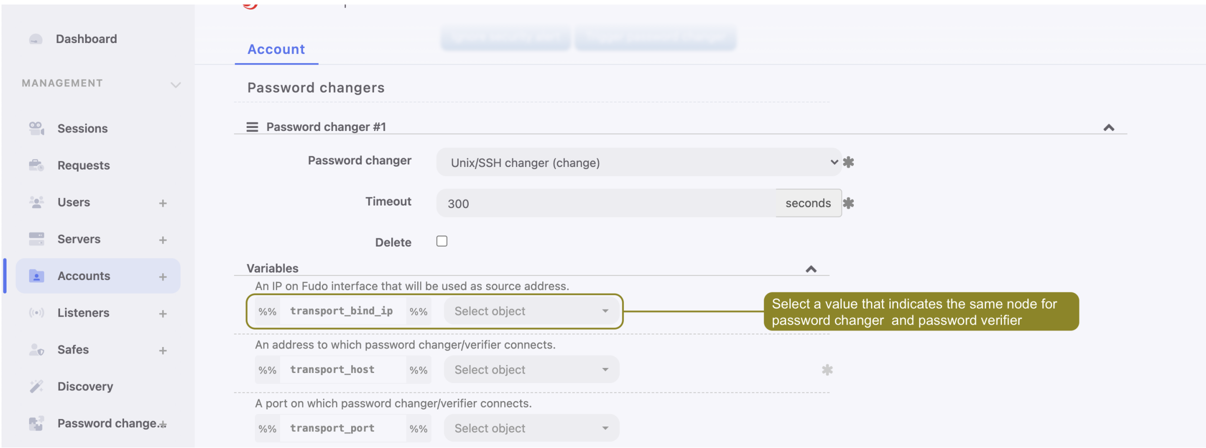
Discovery

Active account discovery node: This node #81888727

Management SSO settings

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

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



Password changers

Password changer #1

Password changer: Unix/SSH changer (change)

Timeout: 300 seconds

Delete □

Variables

An IP on Fudo interface that will be used as source address.
%% transport_bind_ip %% Select object

Select a value that indicates the same node for password changer and password verifier

An address to which password changer/verifier connects.
%% transport_host %% Select object

A port on which password changer/verifier connects.
%% transport_port %% Select object

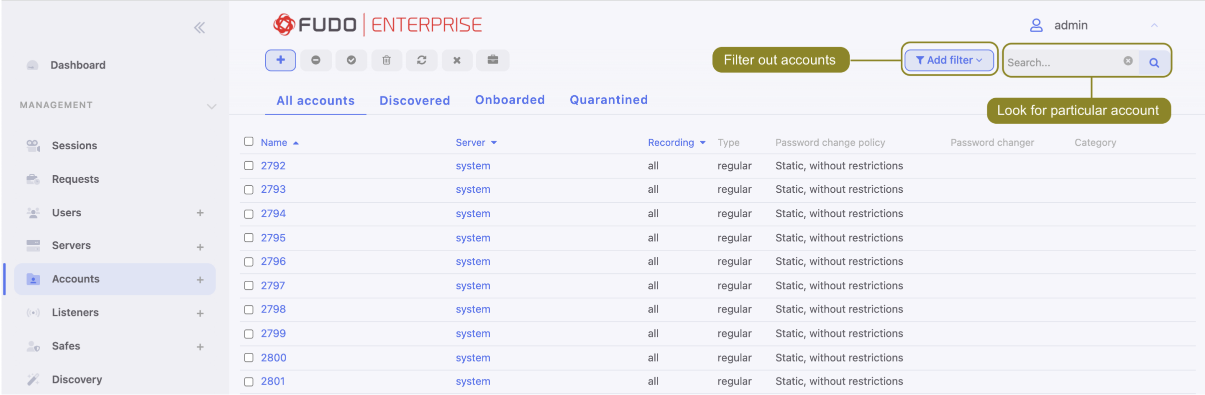
If the `transport_bind_ip` variable values indicate different cluster nodes, the configured password changer/verifier will be running on a node that set as an *Active cluster node for Password changers*.

Related topics:

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

10.2 Editing an account

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



Name	Server	Recording	Type	Password change policy	Password changer	Category
2792	system	all	regular	Static, without restrictions		
2793	system	all	regular	Static, without restrictions		
2794	system	all	regular	Static, without restrictions		
2795	system	all	regular	Static, without restrictions		
2796	system	all	regular	Static, without restrictions		
2797	system	all	regular	Static, without restrictions		
2798	system	all	regular	Static, without restrictions		
2799	system	all	regular	Static, without restrictions		
2800	system	all	regular	Static, without restrictions		
2801	system	all	regular	Static, without restrictions		

3. Find and click desired object's name to open its configuration page.
4. Modify configuration parameters as needed.
5. Click *Save*.

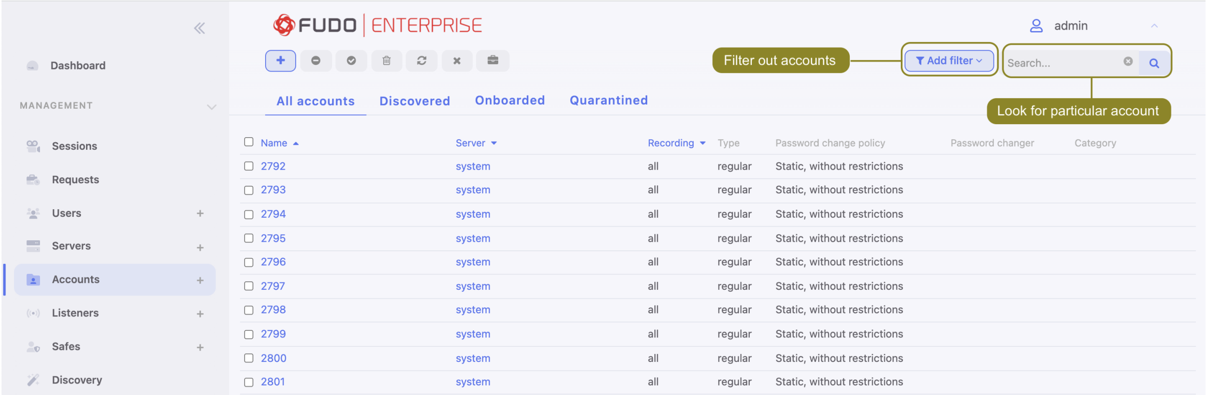
Related topics:

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

10.3 Blocking an account

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

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.

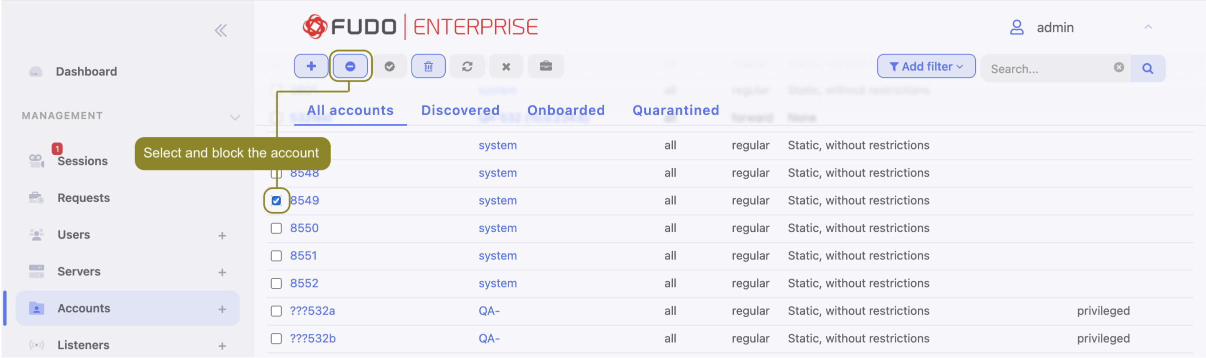


Filter out accounts

Look for particular account

□	Name	Server	Recording	Type	Password change policy	Password changer	Category
□	2792	system	all	regular	Static, without restrictions		
□	2793	system	all	regular	Static, without restrictions		
□	2794	system	all	regular	Static, without restrictions		
□	2795	system	all	regular	Static, without restrictions		
□	2796	system	all	regular	Static, without restrictions		
□	2797	system	all	regular	Static, without restrictions		
□	2798	system	all	regular	Static, without restrictions		
□	2799	system	all	regular	Static, without restrictions		
□	2800	system	all	regular	Static, without restrictions		
□	2801	system	all	regular	Static, without restrictions		

3. Click *Block*.



Select and block the account

		system	all	regular	Static, without restrictions	
□	8548	system	all	regular	Static, without restrictions	
☑	8549	system	all	regular	Static, without restrictions	
□	8550	system	all	regular	Static, without restrictions	
□	8551	system	all	regular	Static, without restrictions	
□	8552	system	all	regular	Static, without restrictions	
□	???532a	QA-	all	regular	Static, without restrictions	privileged
□	???532b	QA-	all	regular	Static, without restrictions	privileged

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

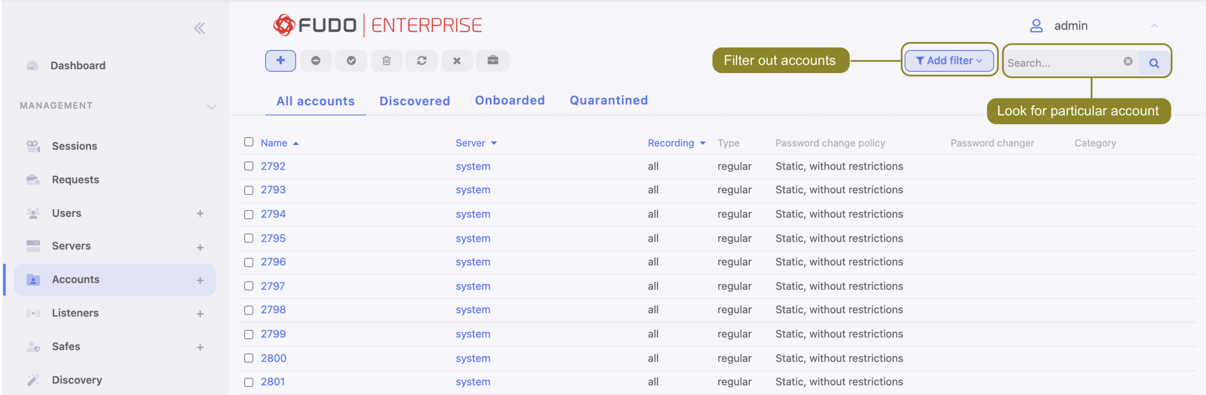
Note: To view the blocking reason, place the cursor over the 💬 icon on the accounts list.

Related topics:

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

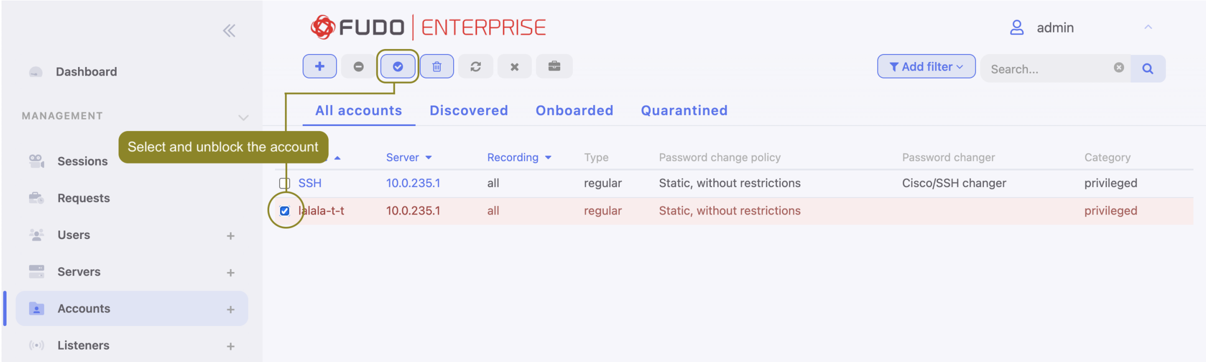
10.4 Unblocking an account

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



Name	Server	Recording	Type	Password change policy	Password changer	Category
2792	system	all	regular	Static, without restrictions		
2793	system	all	regular	Static, without restrictions		
2794	system	all	regular	Static, without restrictions		
2795	system	all	regular	Static, without restrictions		
2796	system	all	regular	Static, without restrictions		
2797	system	all	regular	Static, without restrictions		
2798	system	all	regular	Static, without restrictions		
2799	system	all	regular	Static, without restrictions		
2800	system	all	regular	Static, without restrictions		
2801	system	all	regular	Static, without restrictions		

3. Click *Unblock*.



	Server	Recording	Type	Password change policy	Password changer	Category
□ SSH	10.0.235.1	all	regular	Static, without restrictions	Cisco/SSH changer	privileged
☑ lalala-t-t	10.0.235.1	all	regular	Static, without restrictions		privileged

4. Confirm unblocking selected objects.

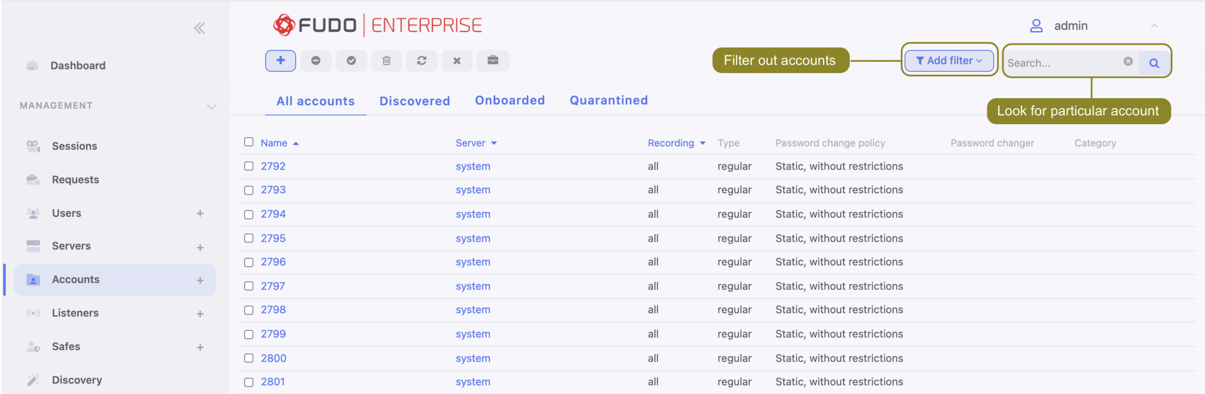
Related topics:

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

10.5 Deleting an account

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

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.

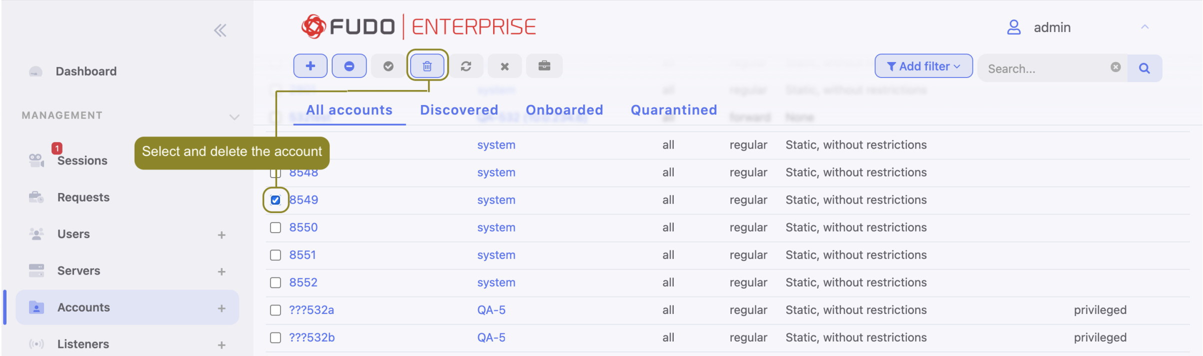


Filter out accounts

Look for particular account

	Name	Server	Recording	Type	Password change policy	Password changer	Category
□	2792	system	all	regular	Static, without restrictions		
□	2793	system	all	regular	Static, without restrictions		
□	2794	system	all	regular	Static, without restrictions		
□	2795	system	all	regular	Static, without restrictions		
□	2796	system	all	regular	Static, without restrictions		
□	2797	system	all	regular	Static, without restrictions		
□	2798	system	all	regular	Static, without restrictions		
□	2799	system	all	regular	Static, without restrictions		
□	2800	system	all	regular	Static, without restrictions		
□	2801	system	all	regular	Static, without restrictions		

3. Click *Delete*.



Select and delete the account

		system	all	regular	Static, without restrictions	
□	8548	system	all	regular	Static, without restrictions	
☑	8549	system	all	regular	Static, without restrictions	
□	8550	system	all	regular	Static, without restrictions	
□	8551	system	all	regular	Static, without restrictions	
□	8552	system	all	regular	Static, without restrictions	
□	???532a	QA-5	all	regular	Static, without restrictions	privileged
□	???532b	QA-5	all	regular	Static, without restrictions	privileged

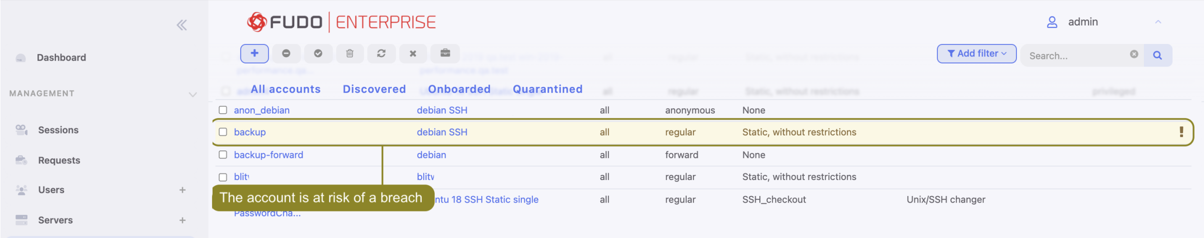
4. Confirm deletion of selected objects.

Related topics:

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

10.6 Managing security alerts

Fudo Enterprise tracks user's action in *User Portal (Access Gateway)* and registers every password viewing. Blocking a user who has seen the current password is a potential security breach. Fudo Enterprise identifies such events and communicates them to system's administrators.



□	anon_debian	debian SSH	all	anonymous	None		
□	backup	debian SSH	all	regular	Static, without restrictions		!
□	backup-forward	debian	all	forward	None		
□	blitv	blitv	all	regular	Static, without restrictions		
	PasswordCha...	ntu 18 SSH Static single	all	regular	SSH_checkout	Unix/SSH changer	

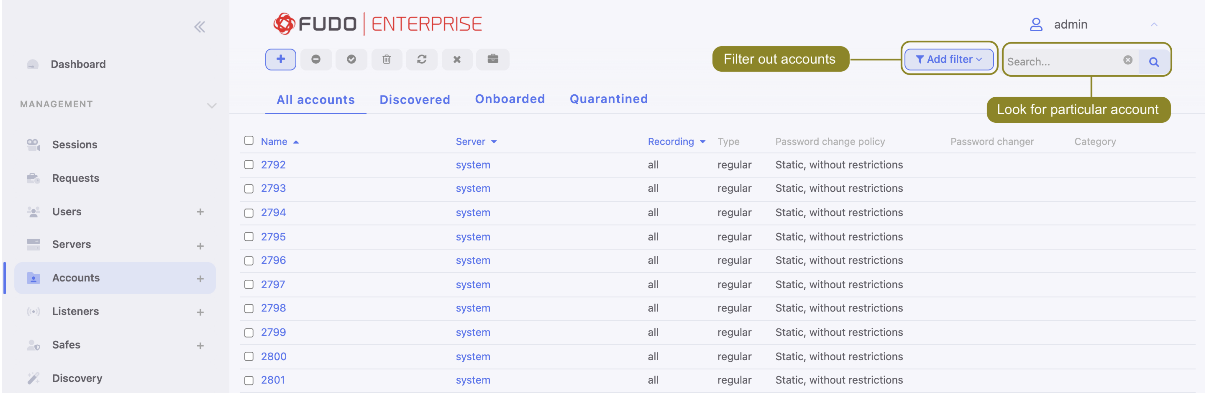
The account is at risk of a breach

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

10.6.1 Triggering password change

Triggering password change on the accounts list

1. Select *Management > Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.

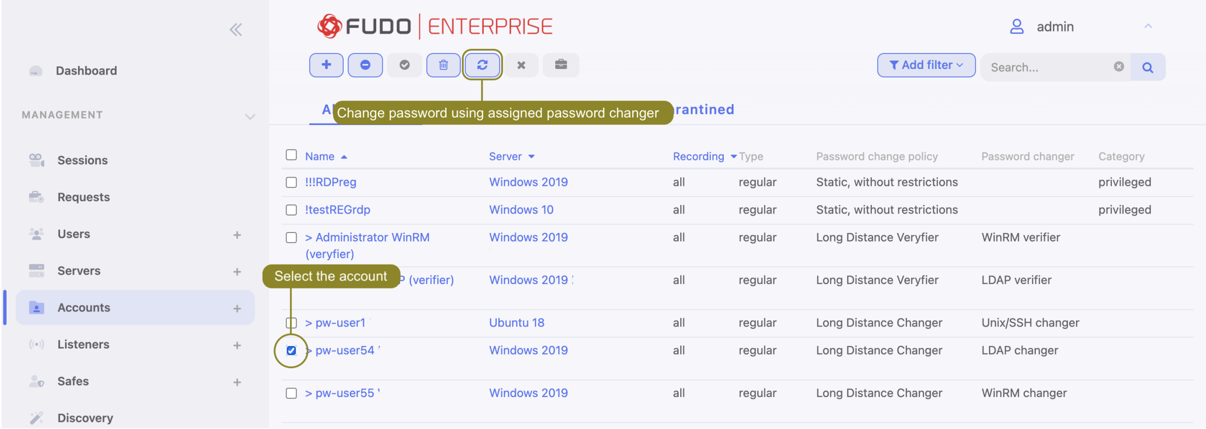


Filter out accounts

Look for particular account

Name	Server	Recording	Type	Password change policy	Password changer	Category
2792	system	all	regular	Static, without restrictions		
2793	system	all	regular	Static, without restrictions		
2794	system	all	regular	Static, without restrictions		
2795	system	all	regular	Static, without restrictions		
2796	system	all	regular	Static, without restrictions		
2797	system	all	regular	Static, without restrictions		
2798	system	all	regular	Static, without restrictions		
2799	system	all	regular	Static, without restrictions		
2800	system	all	regular	Static, without restrictions		
2801	system	all	regular	Static, without restrictions		

3. Click *Change password*.



Change password using assigned password changer

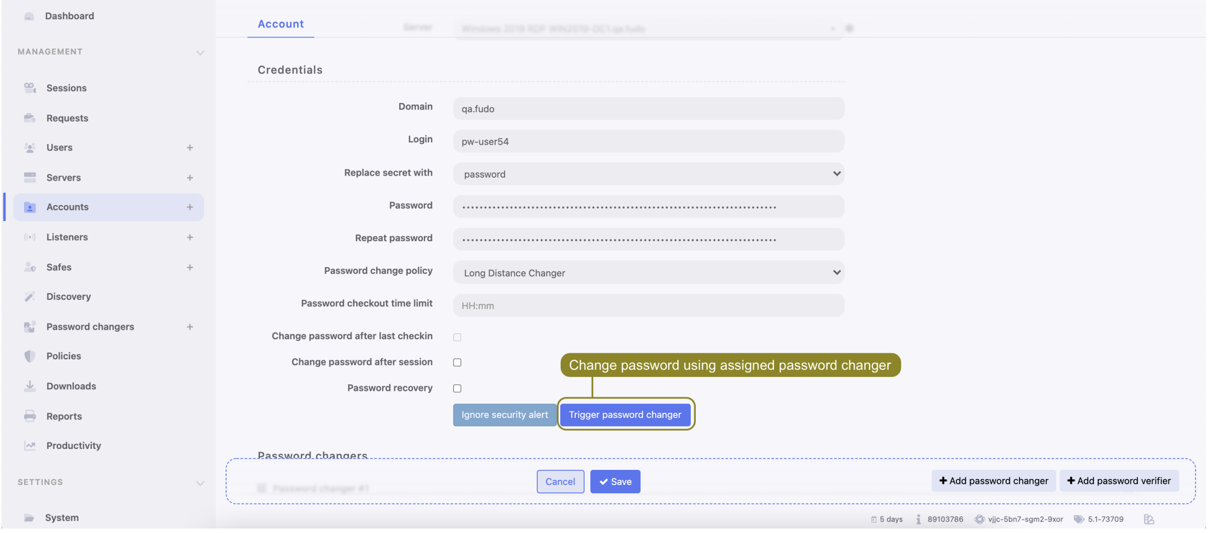
Select the account

Name	Server	Recording	Type	Password change policy	Password changer	Category
□ !!!RDPreg	Windows 2019	all	regular	Static, without restrictions		privileged
□ !testREGrdp	Windows 10	all	regular	Static, without restrictions		privileged
□ > Administrator WinRM (veryfier)	Windows 2019	all	regular	Long Distance Veryfier	WinRM verifier	
P (verifier)	Windows 2019	all	regular	Long Distance Veryfier	LDAP verifier	
□ > pw-user1	Ubuntu 18	all	regular	Long Distance Changer	Unix/SSH changer	
☑ > pw-user54 '	Windows 2019	all	regular	Long Distance Changer	LDAP changer	
□ > pw-user55 '	Windows 2019	all	regular	Long Distance Changer	WinRM changer	

4. Confirm changing password to selected accounts.

Triggering password change from account form

In the *Credentials* section, click *Trigger password changer*.



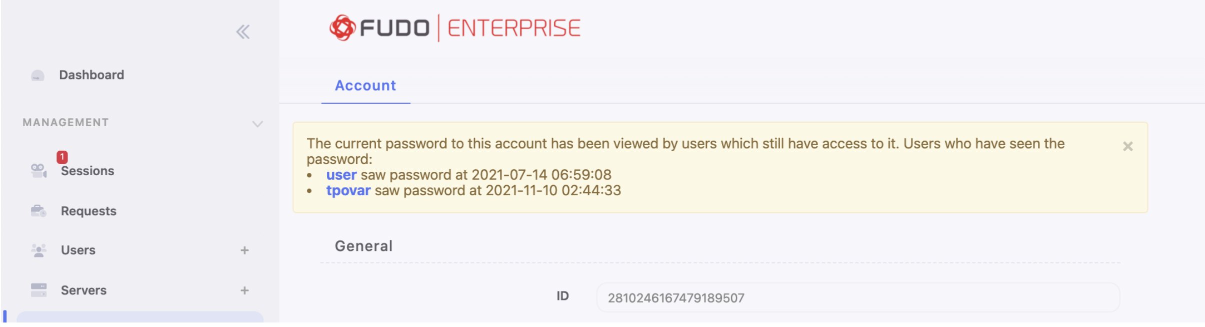
Credentials

Domain	qa.fudo
Login	pw-user54
Replace secret with	password
Password	•••
Repeat password	•••
Password change policy	Long Distance Changer
Password checkout time limit	HH:mm
Change password after last checkin	□
Change password after session	□
Password recovery	□

Ignore security alert | Trigger password changer

Change password using assigned 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 users which still have access to it. Users who have seen the password:

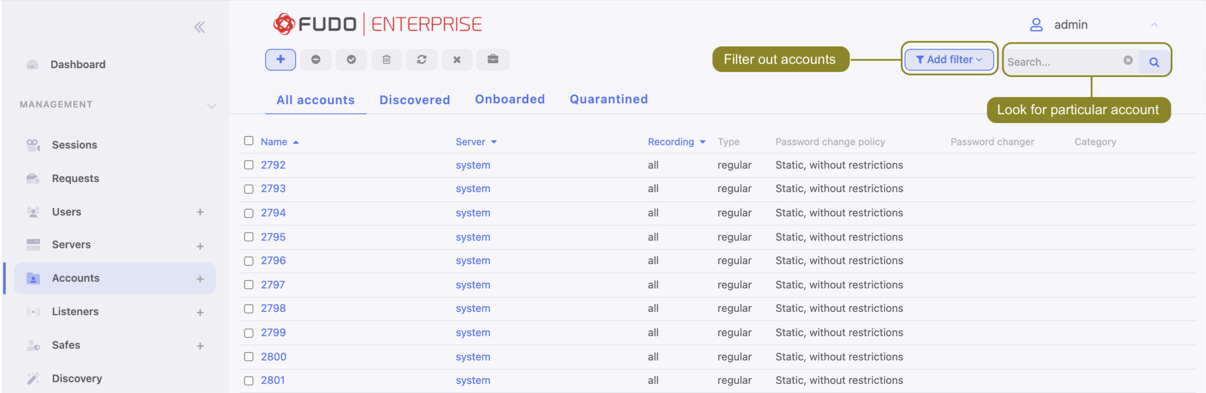
- **user** saw password at 2021-07-14 06:59:08
- **tpovar** saw password at 2021-11-10 02:44:33

ID 2810246167479189507

10.6.2 Ignoring security alert

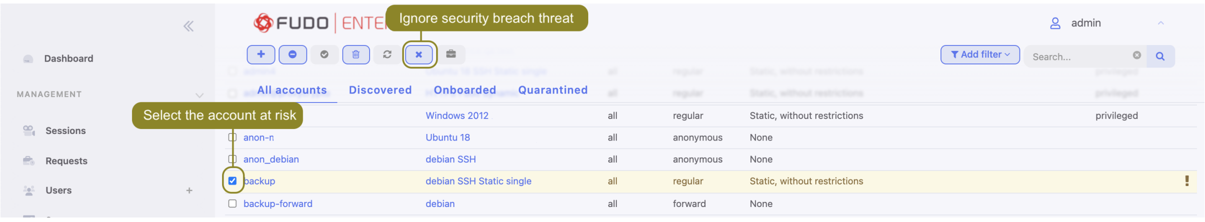
Ignoring security alert on the accounts list

1. Select *Management* > *Accounts*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



Name	Server	Recording	Type	Password change policy	Password changer	Category
2792	system	all	regular	Static, without restrictions		
2793	system	all	regular	Static, without restrictions		
2794	system	all	regular	Static, without restrictions		
2795	system	all	regular	Static, without restrictions		
2796	system	all	regular	Static, without restrictions		
2797	system	all	regular	Static, without restrictions		
2798	system	all	regular	Static, without restrictions		
2799	system	all	regular	Static, without restrictions		
2800	system	all	regular	Static, without restrictions		
2801	system	all	regular	Static, without restrictions		

3. Click *Ignore alert.*

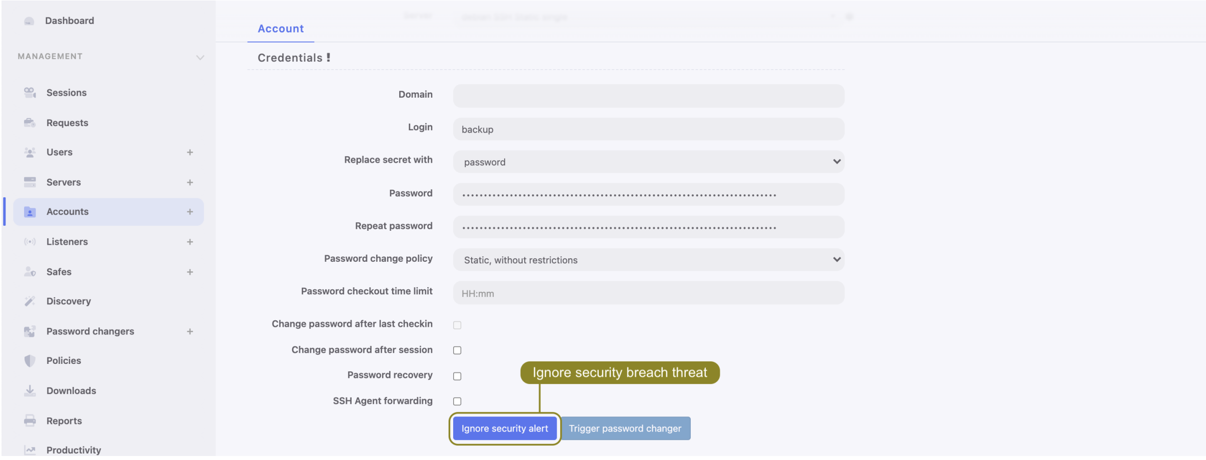


		Windows 2012	all	regular	Static, without restrictions	privileged
□	anon-n	Ubuntu 18	all	anonymous	None	
□	anon_debian	debian SSH	all	anonymous	None	
☑	backup	debian SSH Static single	all	regular	Static, without restrictions	!
□	backup-forward	debian	all	forward	None	

4. Confirm ignoring security alerts for selected accounts.

Ignoring security alert from the account form

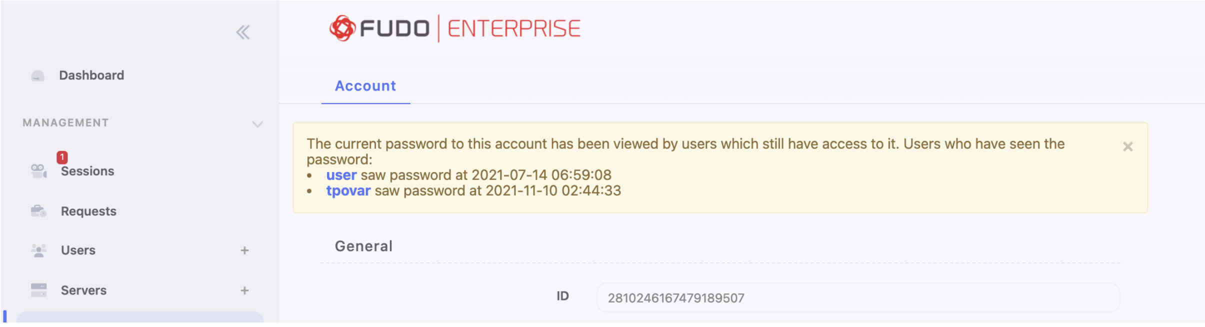
In the *Credentials* section, click *Ignore security alert.*



Credentials !

Domain	
Login	backup
Replace secret with	password
Password	•••
Repeat password	•••
Password change policy	Static, without restrictions
Password checkout time limit	HH:mm
Change password after last checkin	□
Change password after session	□
Password recovery	□
SSH Agent forwarding	□

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 users which still have access to it. Users who have seen the password:

- **user** saw password at 2021-07-14 06:59:08
- **tpovar** saw password at 2021-11-10 02:44:33

ID 2810246167479189507

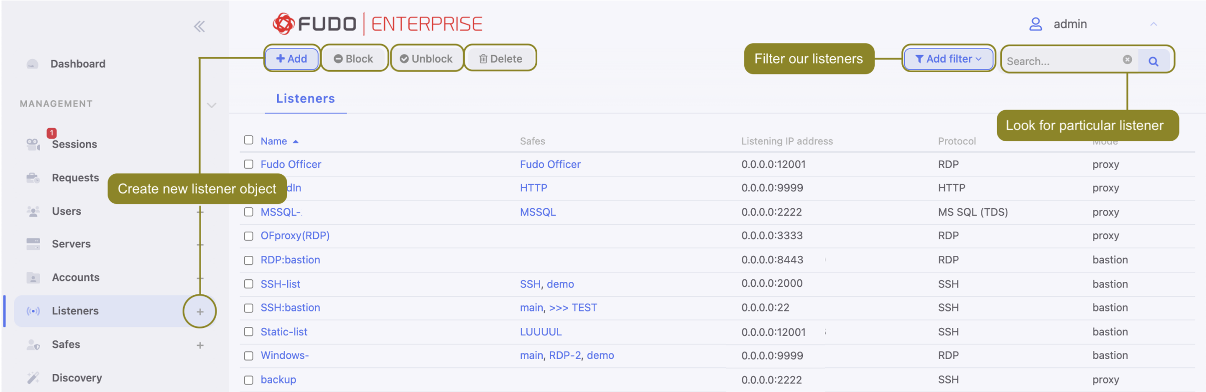
Related topics:

- *Password changers*
- *User Portal (Access Gateway)*

CHAPTER 11

Listeners

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



Create new listener object

Filter our listeners

Look for particular listener

Name	Safes	Listening IP address	Protocol	Mode
Fudo Officer	Fudo Officer	0.0.0.0:12001	RDP	proxy
dIn	HTTP	0.0.0.0:9999	HTTP	proxy
MSSQL-	MSSQL	0.0.0.0:2222	MS SQL (TDS)	proxy
OFproxy(RDP)		0.0.0.0:3333	RDP	proxy
RDP:bastion		0.0.0.0:8443	RDP	bastion
SSH-list	SSH, demo	0.0.0.0:2000	SSH	bastion
SSH:bastion	main, >>> TEST	0.0.0.0:22	SSH	bastion
Static-list	LUUUUL	0.0.0.0:12001	SSH	bastion
Windows-	main, RDP-2, demo	0.0.0.0:9999	RDP	bastion
backup		0.0.0.0:2222	SSH	proxy

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*.

11.1 Creating a listener

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

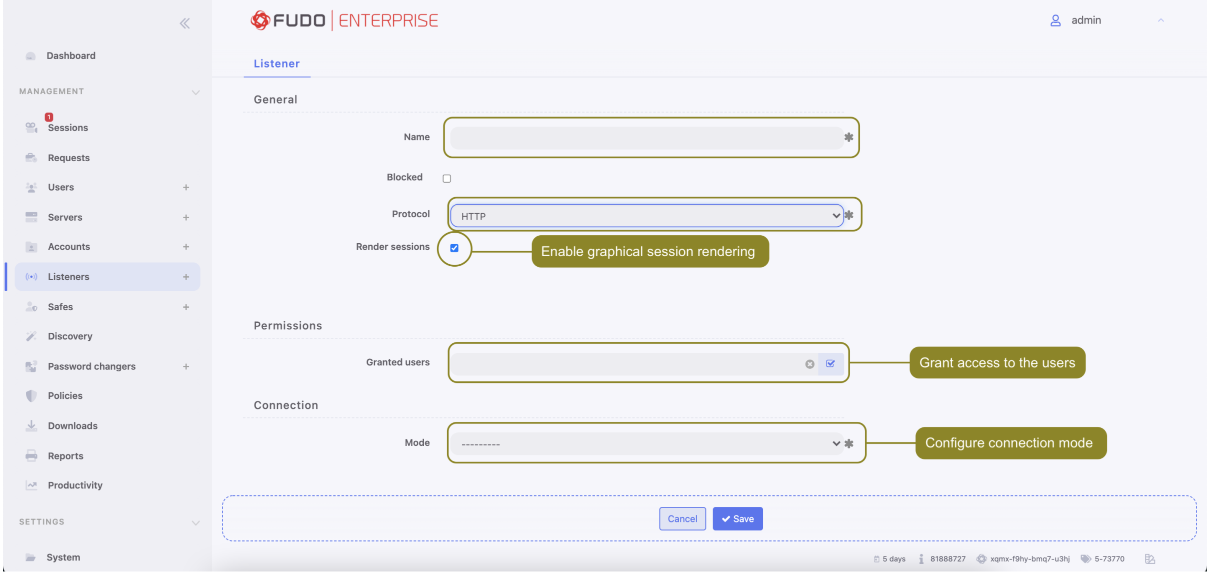
> **Warning:** Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances must not be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

11.1.1 Creating a HTTP listener

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

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

2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.
4. Select `HTTP` from the *Protocol* drop-down list.



General

Name

Blocked □

Protocol HTTP

Render sessions ☑

Enable graphical session rendering

Permissions

Granted users

Grant access to the users

Connection

Mode ---------

Configure connection mode

5. Select `Render sessions` to enable graphical session rendering.

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

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

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

Note:

- In case of rendered HTTP sessions, raw protocol data is not recorded.
- *Render sessions* option must be enabled to activate authentication in the HTTP servers (refer to the *Creating an HTTP server* topic).
- To understand the difference between rendered and raw HTTP sessions, please refer to the *Viewing sessions* topic.

6. In the *Permissions* section, add users allowed to manage this object.
7. 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.

   gateway

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

   - Select `gateway` 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 Enterprise IP address and port number which unambiguously identifies target host.

   - 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.

  transparent

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

  - Select `transparent` 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.

- Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing connections.
- In the *TLS certificate* field, click ⚙ to generate TLS certificate, or click ⇧ to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.

9. Click *Save*.

Related topics:

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

11.1.2 Creating a Modbus listener

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

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

2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.
4. Select `Modbus` from the *Protocol* drop-down list.
5. In the *Permissions* section, add users allowed to manage this object.
6. In the *Connection* section, select desired connection mode.

   gateway

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

   - Select `gateway` 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 Enterprise IP address and port number which unambiguously identifies target host.

   - 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 Enterprise moderates the connection with the remote host using user's IP address.

This option requires deploying Fudo Enterprise in the *bridge mode*.

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

7. Click *Save*.

Related topics:

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

11.1.3 Creating a MySQL listener

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

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

2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.
4. Select `MySQL` from the *Protocol* drop-down list.
5. In the *Permissions* section, add users allowed to manage this object.
6. In the *Connection* section, select desired connection mode.

gateway

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

- Select `gateway` 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 Enterprise IP address and port number which unambiguously identifies target host.

- 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 Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

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

7. Click *Save*.

Related topics:

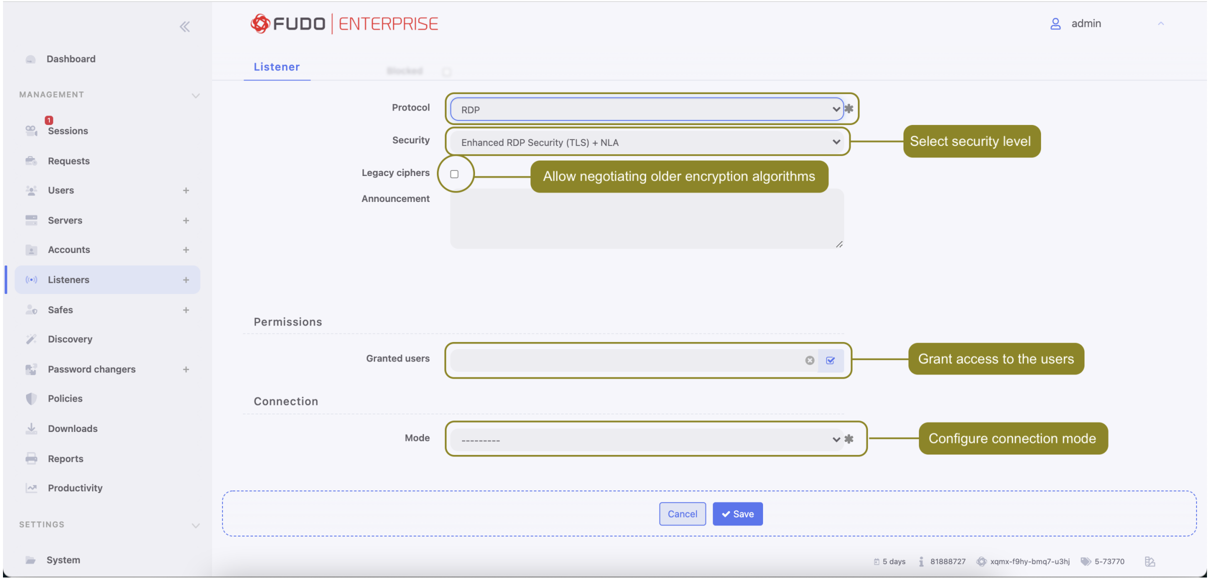
- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

11.1.4 Creating an RDP listener

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

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

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



Protocol: RDP

Security: Enhanced RDP Security (TLS) + NLA

Select security level

Legacy ciphers: □

Allow negotiating older encryption algorithms

Announcement

Permissions

Granted users

Grant access to the users

Connection

Mode: ---------

Configure connection mode

4. Select `RDP` from the *Protocol* drop-down list.
5. 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 the *Enhanced RDP Security (TLS)* option is chosen, select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing RDP connections.

---

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*).

- 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.

gateway

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

- Select `gateway` 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 Enterprise IP address and port number which unambiguously identifies target host.

- 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.

transparent

Note: User connects to the target host by providing its actual IP address. Fudo Enterprise moderates the connection with the remote host using user's IP address.

This option requires deploying Fudo Enterprise in the *bridge mode*.

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

9. In the *TLS certificate* field, click ⚙ to generate TLS certificate, or click ⇧ to upload server certificate file with private key pasted at the end of the file. The rest of the required fields will be filled automatically. Allowed format of the server certificate file is PEM, although besides `.pem`, accepted file extensions are `.txt` and `.cert`.
10. Click *Save*.

Related topics:

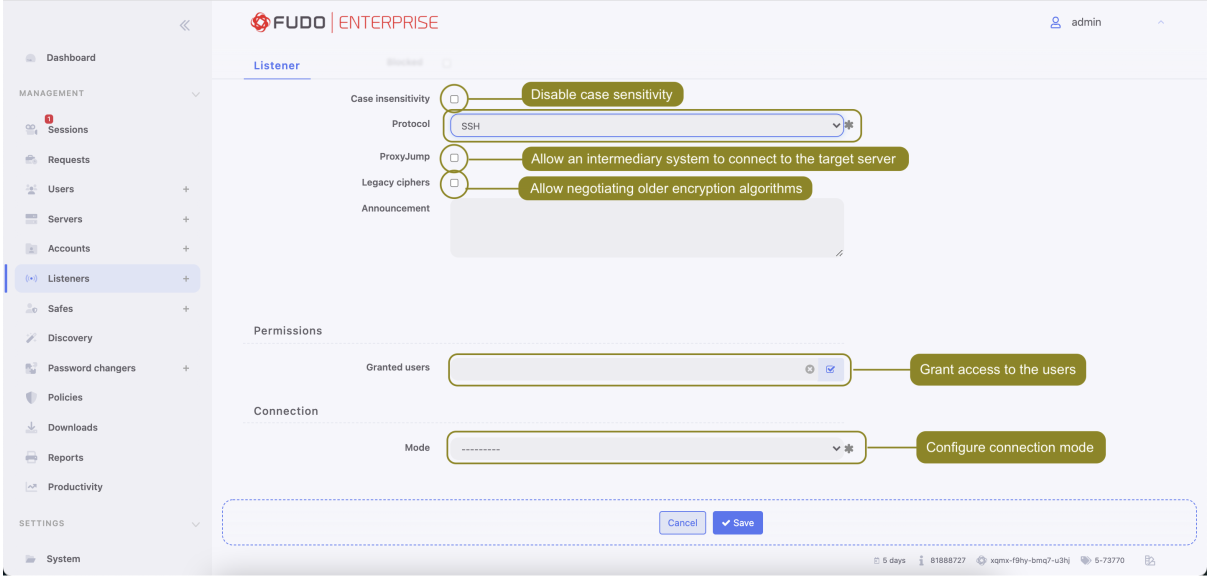
- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

11.1.5 Creating an SSH listener

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

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

2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.
4. Select the *Case insensitivity* option to disable case sensitivity in the username string when connecting over this listener.



Disable case sensitivity

Allow an intermediary system to connect to the target server

Allow negotiating older encryption algorithms

Grant access to the users

Configure connection mode

5. Select `SSH` from the *Protocol* drop-down list.
6. Select *ProxyJump* option to allow an intermediary system to connect to the target server.

7. Select *Legacy ciphers* option to allow negotiating older encryption algorithms (DSA(1024), RSA(1024)) when establishing SSH connections.
8. In the *Announcement* field, type in the announcement that will be presented to the user on the login screen.
9. In the *Permissions* section, add users allowed to manage this object.
10. 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.

gateway

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

- Select `gateway` 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 Enterprise IP address and port number which unambiguously identifies target host.

- 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.

transparent

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

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

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

Related topics:

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

- *Unblocking a listener*

11.1.6 Creating a MS SQL listener

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

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

2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.
4. Select `MS SQL (TDS)` from the *Protocol* drop-down list.
5. In the *Permissions* section, add users allowed to manage this object.
6. In the *Connection* section, select desired connection mode.

bastion

Note:

- User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
- 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 Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise 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 Enterprise IP address and port number which unambiguously identifies target host.

- 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 Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

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

7. Click *Save*.

Related topics:

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

11.1.7 Creating a Telnet listener

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

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

2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.
4. Select `Telnet` from the *Protocol* drop-down list.
5. In the *Permissions* section, add users allowed to manage this object.
6. In the *Connection* section, select desired connection mode.

bastion

Note:

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

- 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 Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise 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 Enterprise IP address and port number which unambiguously identifies target host.

- 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 Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

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

7. Click *Save*.

Related topics:

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

11.1.8 Creating a Telnet 3270 listener

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

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

2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.
4. Select `Telnet 3270` from the *Protocol* drop-down list.
5. In the *Permissions* section, add users allowed to manage this object.
6. In the *Connection* section, select desired connection mode.

bastion

Note:

- User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
- 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 Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise 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 Enterprise IP address and port number which unambiguously identifies target host.

- 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 Enterprise moderates the connection with the remote host using user's IP address. This option requires deploying Fudo Enterprise in the *bridge mode*.

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

7. Click *Save*.

Related topics:

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

11.1.9 Creating a Telnet 5250 listener

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

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

2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.
4. Select `Telnet 5250` from the *Protocol* drop-down list.
5. In the *Permissions* section, add users allowed to manage this object.
6. In the *Connection* section, select desired connection mode.

bastion

Note:

- User connects to the target host by including its name in the login string, e.g. `john_smith#mail_server`.
- 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 Enterprise moderates the connection with the remote host using own IP address. This option requires deploying Fudo Enterprise 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 Enterprise IP address and port number which unambiguously identifies target host.

- 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 Enterprise moderates the connection with the remote host using user's IP address.

This option requires deploying Fudo Enterprise in the *bridge mode*.

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

7. Click *Save*.

Related topics:

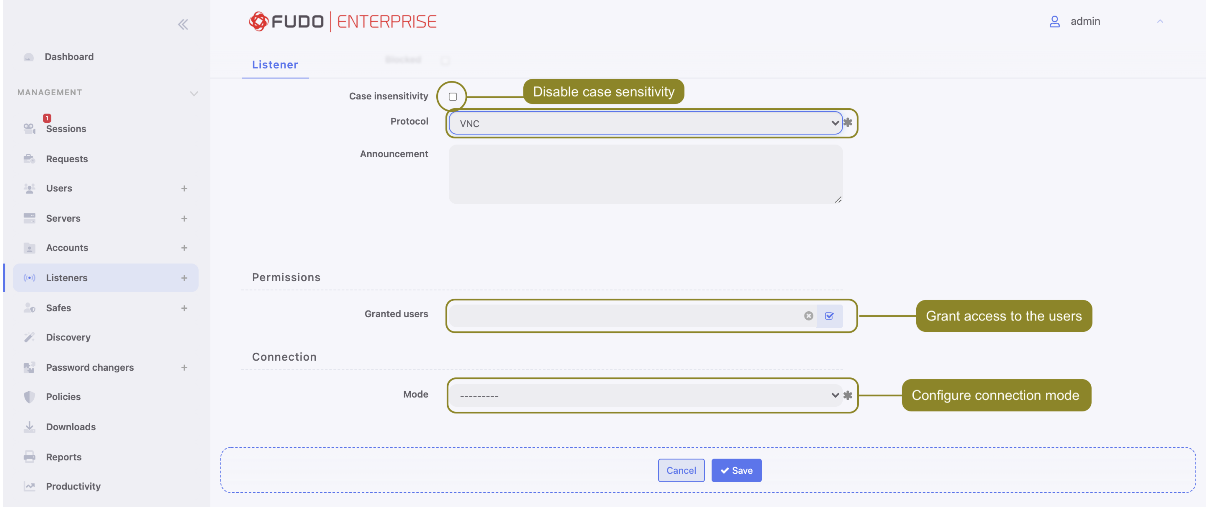
- *Data model*
- *Editing a listener*
- *Deleting a listener*
- *Blocking a listener*
- *Unblocking a listener*

11.1.10 Creating a VNC listener

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

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

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



Case insensitivity □

Protocol VNC

Announcement

Permissions

Granted users

Connection

Mode ---------

Disable case sensitivity

Grant access to the users

Configure connection mode

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

bastion

Note:

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

gateway

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

- Select `gateway` 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 Enterprise IP address and port number which unambiguously identifies target host.

- 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.

transparent

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

- Select `transparent` 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*

11.1.11 Creating a TCP listener

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

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

2. Enter listener's unique name.
3. Select *Blocked* option to disable access to servers through this listener after it's created.
4. Select `TCP` from the *Protocol* drop-down list.
5. In the *Permissions* section, add users allowed to manage this object.
6. In the *Connection* section, select desired connection mode.

gateway

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

- Select `gateway` 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 Enterprise IP address and port number which unambiguously identifies target host.

- 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.

transparent

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

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

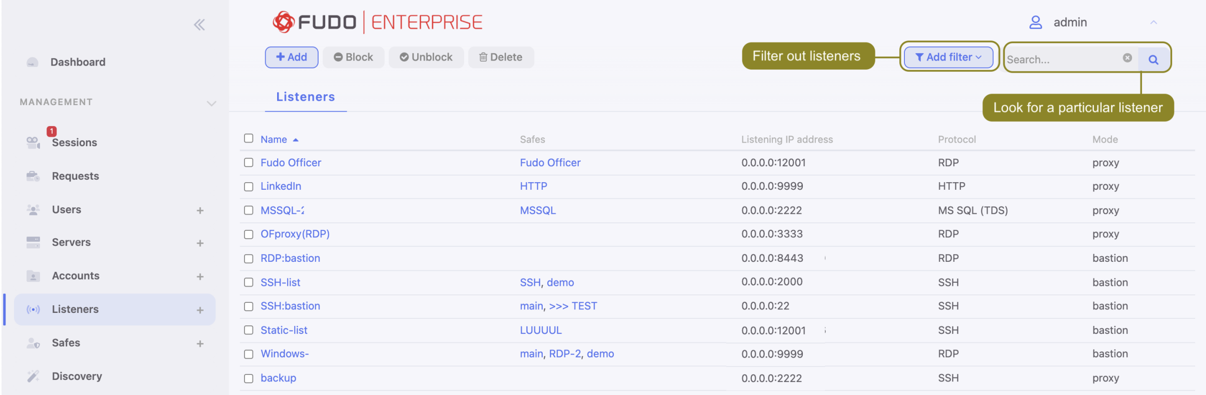
7. Click *Save*.

Related topics:

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

11.2 Editing a listener

1. Select *Management* > *Listeners*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



Filter out listeners

Look for a particular listener

Name	Safes	Listening IP address	Protocol	Mode
☐ Fudo Officer	Fudo Officer	0.0.0.0:12001	RDP	proxy
☐ LinkedIn	HTTP	0.0.0.0:9999	HTTP	proxy
☐ MSSQL-:	MSSQL	0.0.0.0:2222	MS SQL (TDS)	proxy
☐ OFproxy(RDP)		0.0.0.0:3333	RDP	proxy
☐ RDP:bastion		0.0.0.0:8443	RDP	bastion
☐ SSH-list	SSH, demo	0.0.0.0:2000	SSH	bastion
☐ SSH:bastion	main, >>> TEST	0.0.0.0:22	SSH	bastion
☐ Static-list	LUUUUL	0.0.0.0:12001	SSH	bastion
☐ Windows-	main, RDP-2, demo	0.0.0.0:9999	RDP	bastion
☐ backup		0.0.0.0:2222	SSH	proxy

3. Find and click on a name of the desired listener to access its configuration parameters.
4. Modify configuration values as needed.
5. Click *Save*.

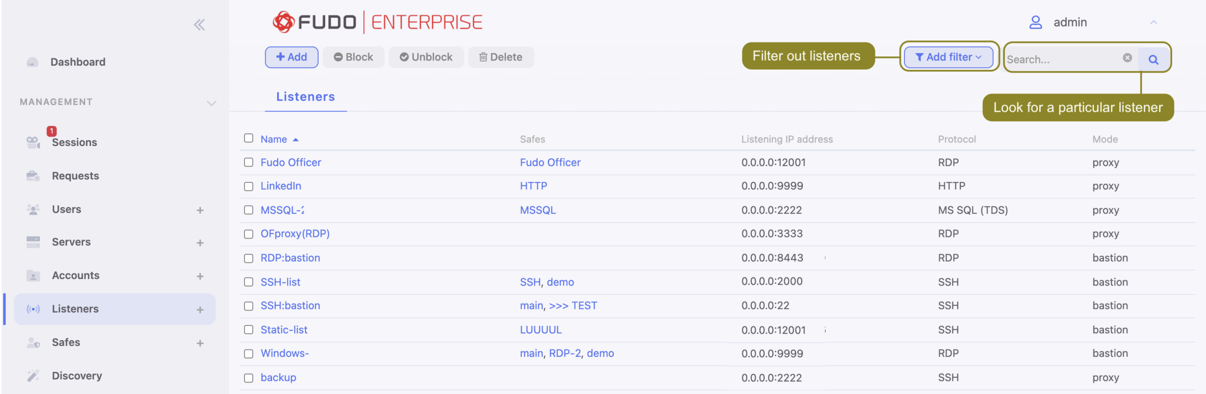
Related topics:

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

11.3 Blocking a listener

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

1. Select *Management* > *Listeners*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.

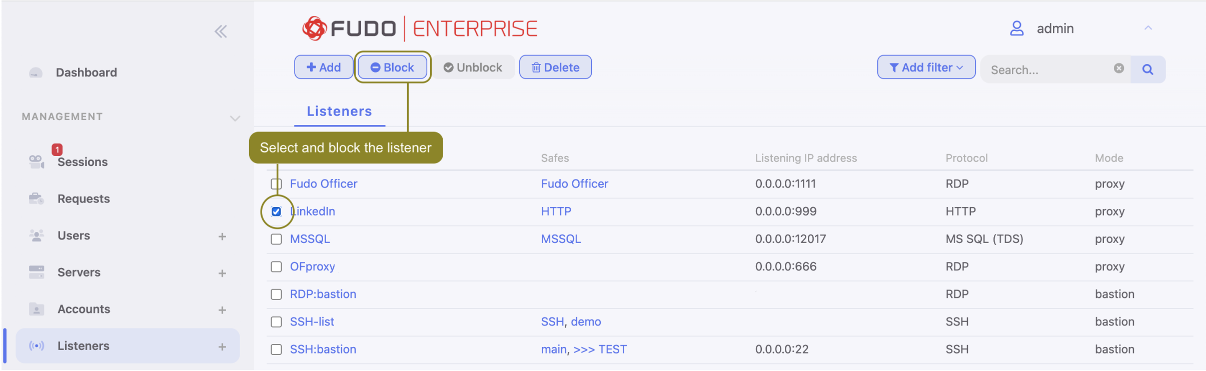


Filter out listeners

Look for a particular listener

Name	Safes	Listening IP address	Protocol	Mode
☐ Fudo Officer	Fudo Officer	0.0.0.0:12001	RDP	proxy
☐ LinkedIn	HTTP	0.0.0.0:9999	HTTP	proxy
☐ MSSQL-:	MSSQL	0.0.0.0:2222	MS SQL (TDS)	proxy
☐ OFproxy(RDP)		0.0.0.0:3333	RDP	proxy
☐ RDP:bastion		0.0.0.0:8443	RDP	bastion
☐ SSH-list	SSH, demo	0.0.0.0:2000	SSH	bastion
☐ SSH:bastion	main, >>> TEST	0.0.0.0:22	SSH	bastion
☐ Static-list	LUUUUL	0.0.0.0:12001	SSH	bastion
☐ Windows-	main, RDP-2, demo	0.0.0.0:9999	RDP	bastion
☐ backup		0.0.0.0:2222	SSH	proxy

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



Select and block the listener

	Safes	Listening IP address	Protocol	Mode
□ Fudo Officer	Fudo Officer	0.0.0.0:1111	RDP	proxy
☑ LinkedIn	HTTP	0.0.0.0:999	HTTP	proxy
□ MSSQL	MSSQL	0.0.0.0:12017	MS SQL (TDS)	proxy
□ OFproxy		0.0.0.0:666	RDP	proxy
□ RDP:bastion			RDP	bastion
□ SSH-list	SSH, demo		SSH	bastion
□ SSH:bastion	main, >>> TEST	0.0.0.0:22	SSH	bastion

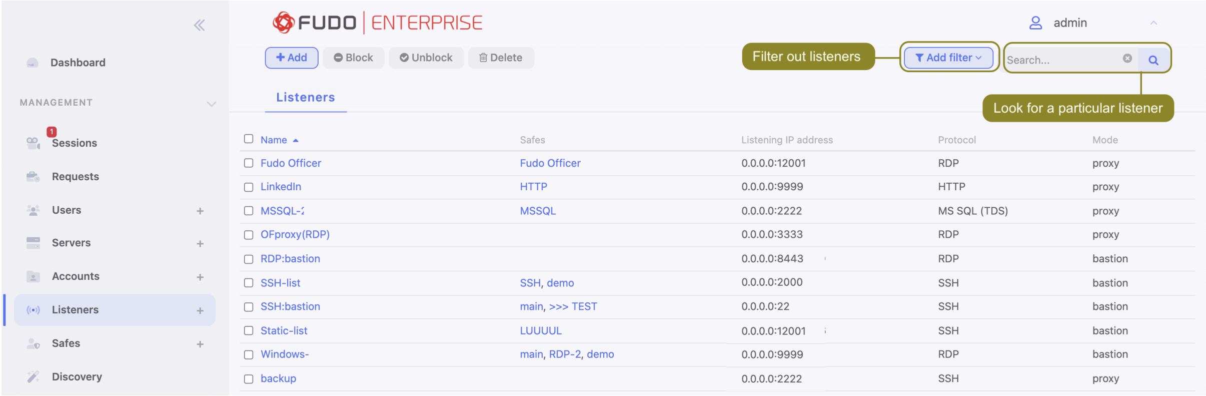
4. Optionally, provide descriptive reason for blocking given resource and click *Confirm*.

Related topics:

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

11.4 Unblocking a listener

1. Select *Management* > *Listeners*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.

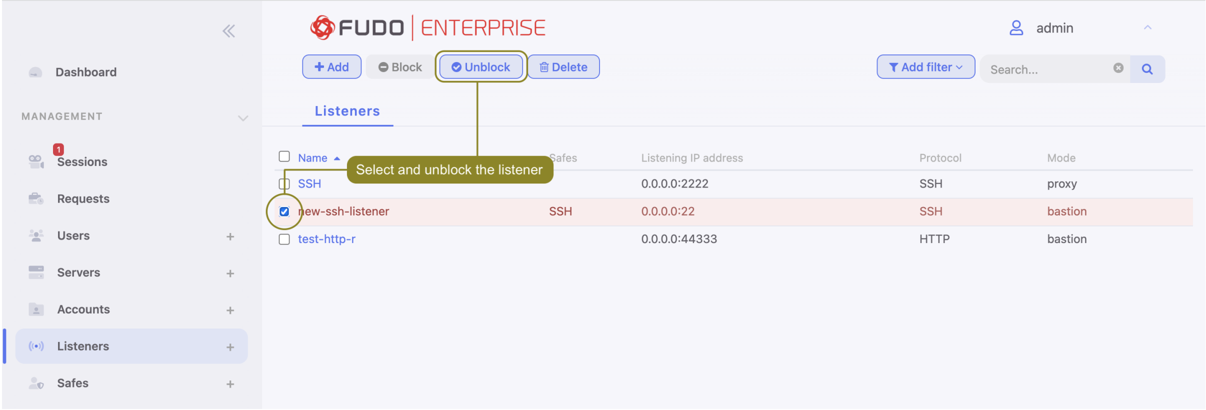


Filter out listeners

Look for a particular listener

□ Name	Safes	Listening IP address	Protocol	Mode
□ Fudo Officer	Fudo Officer	0.0.0.0:12001	RDP	proxy
□ LinkedIn	HTTP	0.0.0.0:9999	HTTP	proxy
□ MSSQL-:	MSSQL	0.0.0.0:2222	MS SQL (TDS)	proxy
□ OFproxy(RDP)		0.0.0.0:3333	RDP	proxy
□ RDP:bastion		0.0.0.0:8443	RDP	bastion
□ SSH-list	SSH, demo	0.0.0.0:2000	SSH	bastion
□ SSH:bastion	main, >>> TEST	0.0.0.0:22	SSH	bastion
□ Static-list	LUUUUL	0.0.0.0:12001	SSH	bastion
□ Windows-	main, RDP-2, demo	0.0.0.0:9999	RDP	bastion
□ backup		0.0.0.0:2222	SSH	proxy

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



Select and unblock the listener

□ Name	Safes	Listening IP address	Protocol	Mode
□ SSH		0.0.0.0:2222	SSH	proxy
☑ new-ssh-listener	SSH	0.0.0.0:22	SSH	bastion
□ test-http-r		0.0.0.0:44333	HTTP	bastion

4. Click *Confirm* to unblock selected objects.

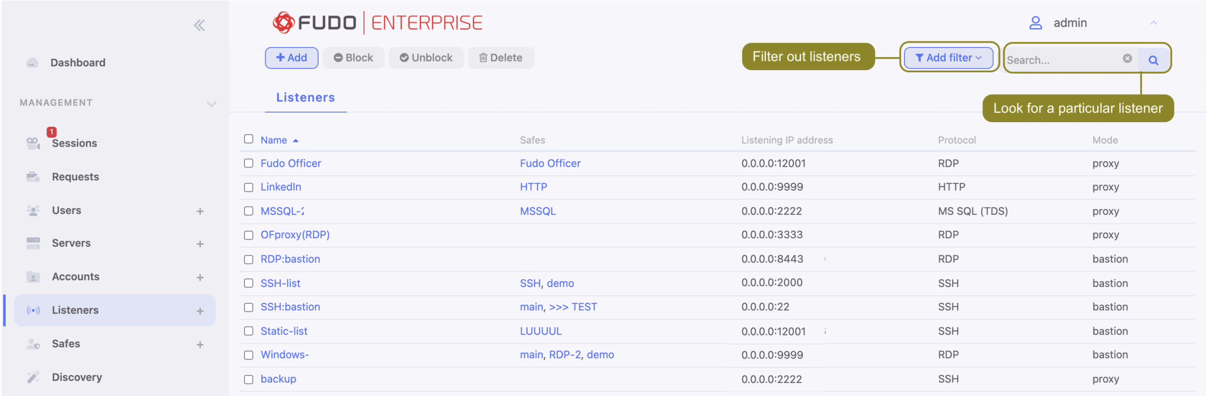
Related topics:

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

11.5 Deleting a listener

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

1. Select *Management* > *Listeners*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.

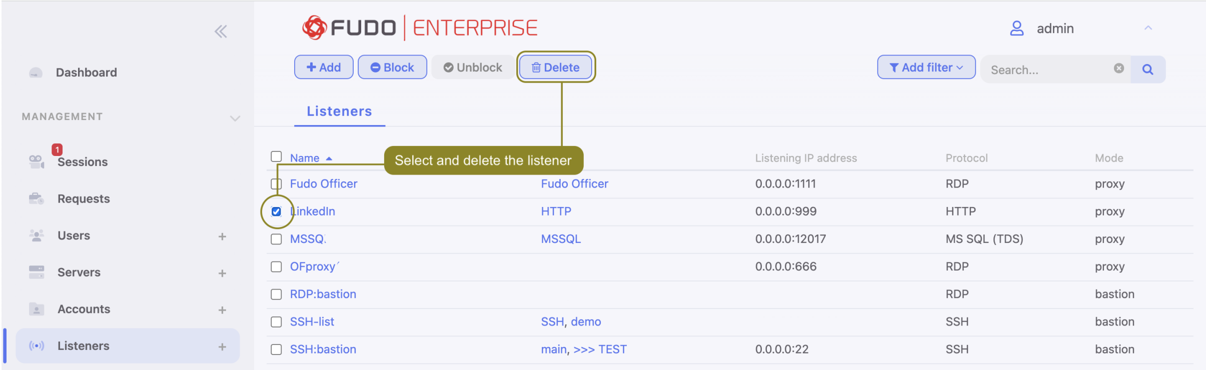


Filter out listeners

Look for a particular listener

☐ Name	Safes	Listening IP address	Protocol	Mode
☐ Fudo Officer	Fudo Officer	0.0.0.0:12001	RDP	proxy
☐ LinkedIn	HTTP	0.0.0.0:9999	HTTP	proxy
☐ MSSQL-:	MSSQL	0.0.0.0:2222	MS SQL (TDS)	proxy
☐ OFproxy(RDP)		0.0.0.0:3333	RDP	proxy
☐ RDP:bastion		0.0.0.0:8443	RDP	bastion
☐ SSH-list	SSH, demo	0.0.0.0:2000	SSH	bastion
☐ SSH:bastion	main, >>> TEST	0.0.0.0:22	SSH	bastion
☐ Static-list	LUUUUL	0.0.0.0:12001	SSH	bastion
☐ Windows-	main, RDP-2, demo	0.0.0.0:9999	RDP	bastion
☐ backup		0.0.0.0:2222	SSH	proxy

3. Click *Delete*.



Select and delete the listener

☐ Name		Listening IP address	Protocol	Mode
☐ Fudo Officer	Fudo Officer	0.0.0.0:1111	RDP	proxy
☑ LinkedIn	HTTP	0.0.0.0:999	HTTP	proxy
☐ MSSQ.	MSSQL	0.0.0.0:12017	MS SQL (TDS)	proxy
☐ OFproxy´		0.0.0.0:666	RDP	proxy
☐ RDP:bastion			RDP	bastion
☐ SSH-list	SSH, demo		SSH	bastion
☐ SSH:bastion	main, >>> TEST	0.0.0.0:22	SSH	bastion

4. Confirm deleting selected objects.

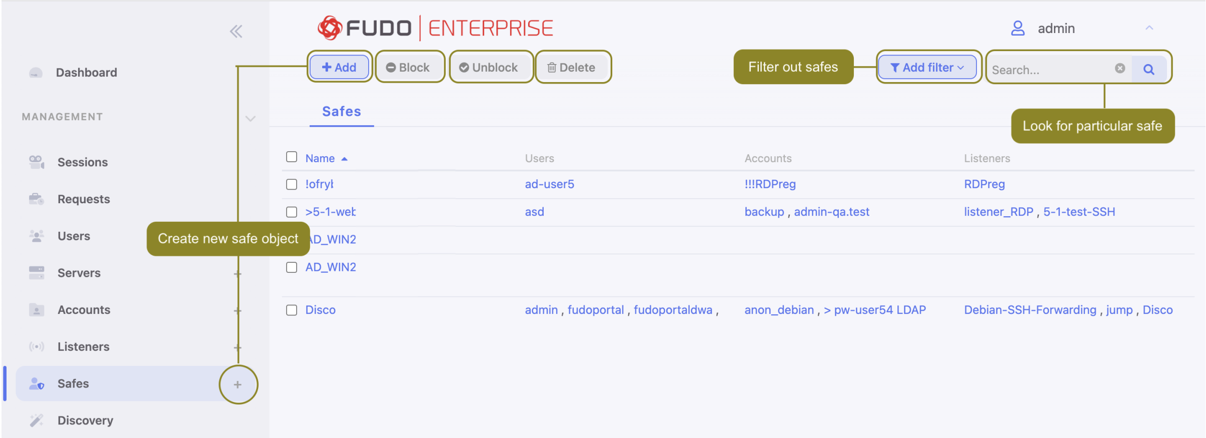
Related topics:

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

CHAPTER 12

Safes

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



Create new safe object

Filter out safes

Look for particular safe

Name	Users	Accounts	Listeners
!ofryl	ad-user5	!!!RDPreg	RDPreg
>5-1-wek	asd	backup , admin-qa.test	listener_RDP , 5-1-test-SSH
AD_WIN2			
AD_WIN2			
Disco	admin , fudoportal , fudoportaldwa ,	anon_debian , > pw-user54 LDAP	Debian-SSH-Forwarding , jump , Disco

12.1 Creating a safe

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

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

Select *Management* > *Safes* and then click + *Add*.

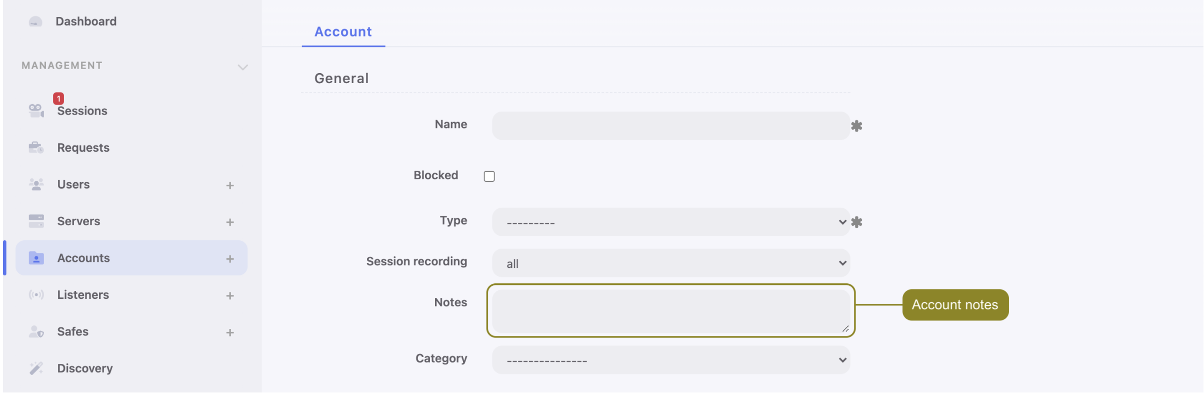
2. Enter object's name.
3. Select *Blocked* option to disable access to object after it's created.

4. 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.

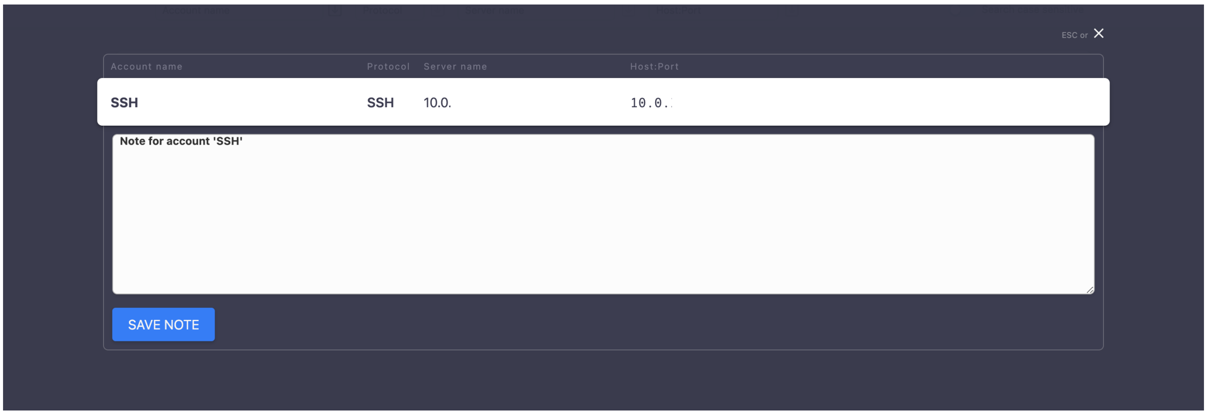
5. Select *Access request required votes* option and provide a number of the voters. This option enables a so called **Just-In-Time** feature that allows defining and scheduling the time when a user is allowed to access specific resources for a set period of time. The user sends requests via the Access Gateway and the voters accept or reject them on an the Admin Panel. Read more about the Just-In-Time feature in a *Access requests* page.
6. 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.
7. Assign *security policies* in the *Policies* field.
8. From the *Note access* drop-down list, select access rights to account related notes: `read-only access` or `write access`.

Notes can be accessed either from the account edit form



Session recording: all

or in the *Access Gateway*.



Account name	Protocol	Server name	Host:Port
SSH	SSH	10.0.	10.0.

Note for account 'SSH'

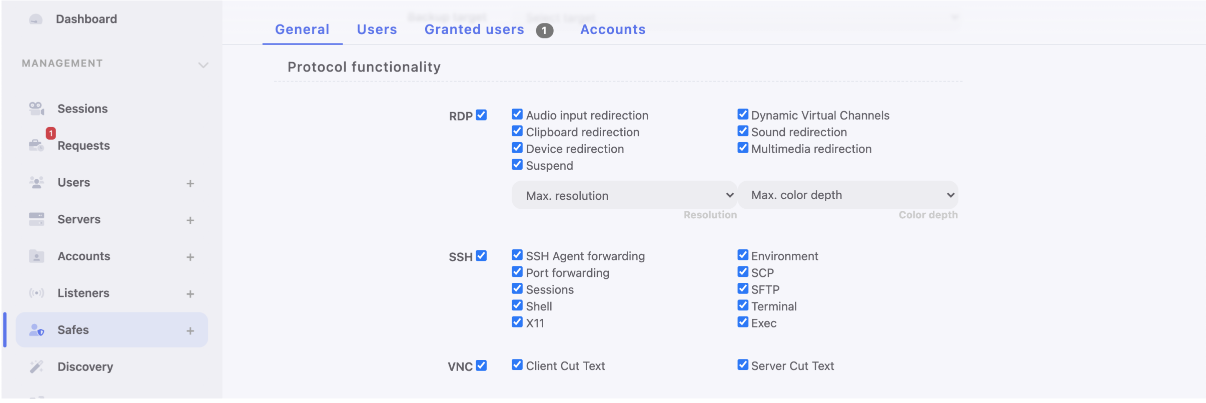
9. Select *Session time limit* option and input a minutes value.
10. Select *Session inactivity limit* option and input a minutes value.
11. The *OTP in Access Gateway* option is enabled by default and is responsible for generating OTP in the Access Gateway.

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

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

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

13. Select a *Backup target* as a destination place for storing data.
14. In the *Protocol functionality* section, select allowed protocols' features.



Protocol functionality

RDP ☑
- ☑ Audio input redirection
- ☑ Clipboard redirection
- ☑ Device redirection
- ☑ Suspend
- ☑ Dynamic Virtual Channels
- ☑ Sound redirection
- ☑ Multimedia redirection

Resolution: Max. resolution

Color depth: Max. color depth

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

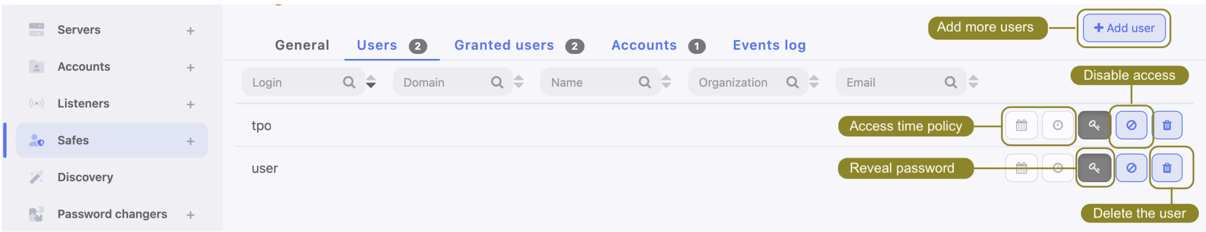
With the *Client Cut Text* option enabled for the VNC sessions, a user is allowed to paste text into the VNC server computer.

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.

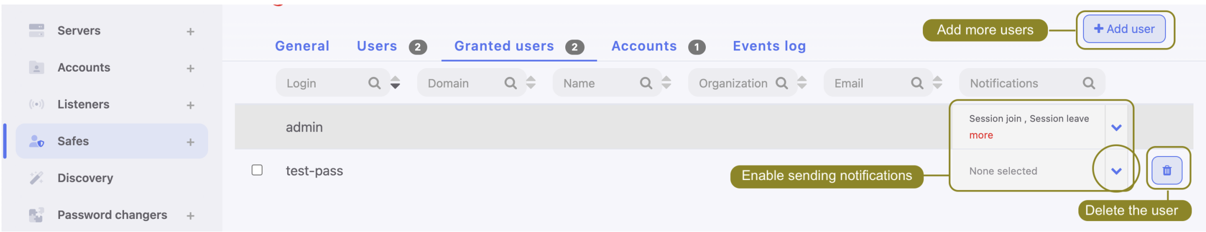
15. Select **Users** tab to assign users allowed to access accounts assigned to this safe.
    - Click *+ Add user.*
    - Click + to add users.
    - Click *ok* to close the modal window.
    - Define safe access options.
        - Click 📅 to define the timeframe when given user can access this object.
        - Click ⊙ to define daily access policy.
        - Click 🔑 to allow user to use Secret Checkout feature and view passwords in the Access Gateway.
        - Click ⊘ to disable access for selected user.

- Click 🗑 to delete selected user from the safe.

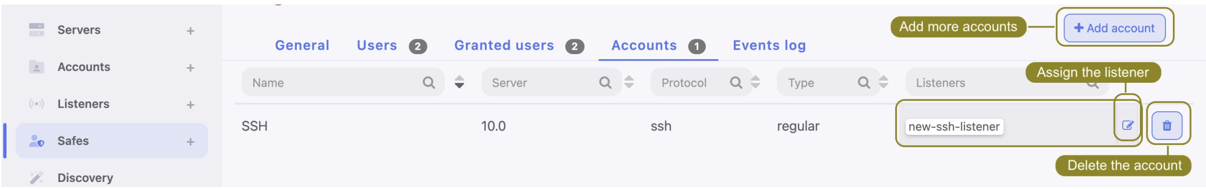
Note: Access time policy options are disabled when the *Access request required votes* option is enabled for the safe.



16. Select **Granted users** tab to assign users allowed to manage this object.
    - Click *+ Add user*.
    - Click + to add users.
    - Select notifications that will be enabled for the particular granted user. More on this subject is at the *Notifications* page.
    - Click *ok* to close the modal window.



17. Select **Accounts** tab to add *accounts* accessible through this safe.
    - Click *+ Add account*.
    - Click + to add accounts.
    - Click *ok* to close the modal window.
    - Click ✎ to assign listeners to accounts.
    - Click + to add listeners.
    - Click *ok* to close the modal window.



18. Click *Save*.

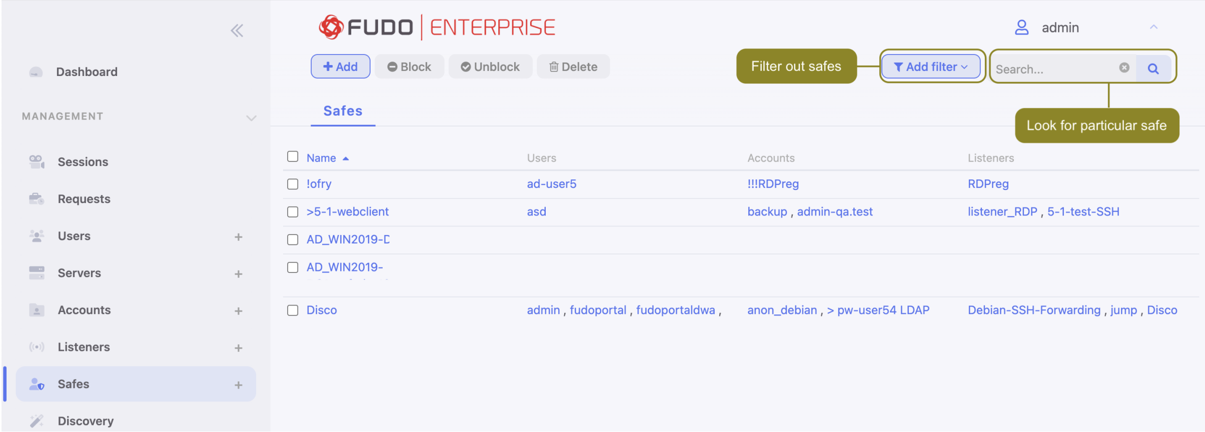
Related topics:

- *Data model*
- *Editing a safe*

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

12.2 Editing a safe

1. Select *Management > Safes*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



☐ Name	Users	Accounts	Listeners
☐ !ofry	ad-user5	!!!RDPreg	RDPreg
☐ >5-1-webclient	asd	backup , admin-qa.test	listener_RDP , 5-1-test-SSH
☐ AD_WIN2019-D			
☐ AD_WIN2019-			
☐ Disco	admin , fudoportal , fudoportaldwa ,	anon_debian , > pw-user54 LDAP	Debian-SSH-Forwarding , jump , Disco

3. Find and click desired object's name to open its configuration page.
4. Modify configuration parameters as needed.
5. Click *Save*.

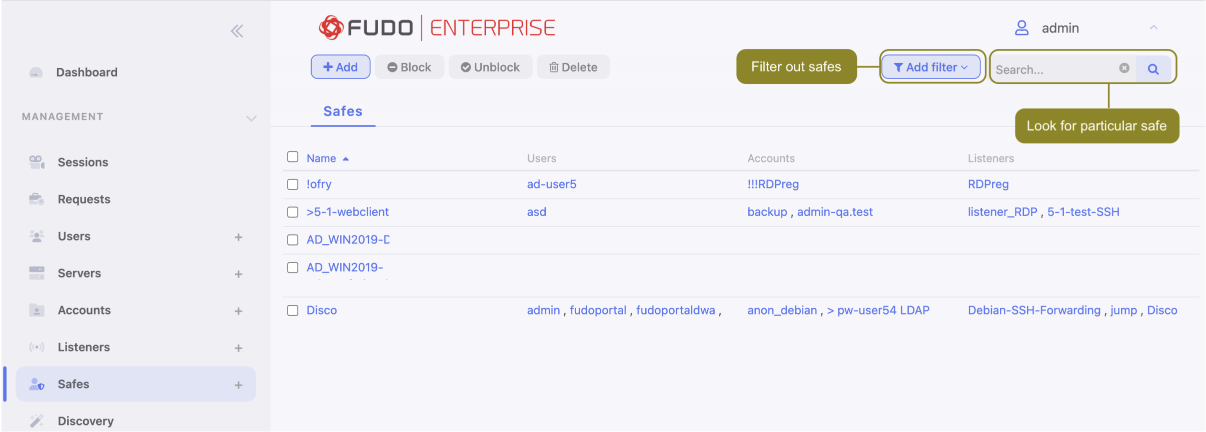
Related topics:

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

12.3 Blocking a safe

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

1. Select *Management > Safes*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.

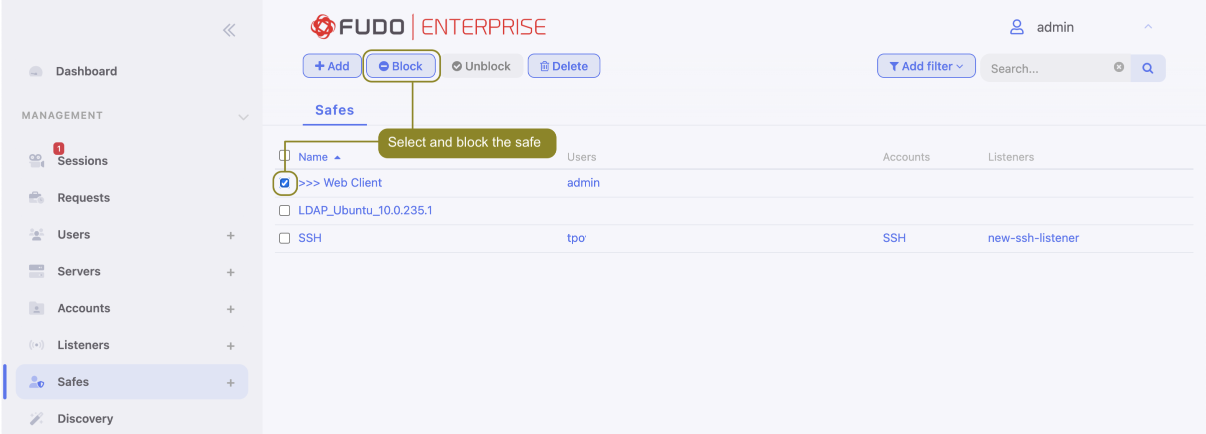


Filter out safes

Look for particular safe

☐ Name	Users	Accounts	Listeners
☐ !ofry	ad-user5	!!!RDPreg	RDPreg
☐ >5-1-webclient	asd	backup , admin-qa.test	listener_RDP , 5-1-test-SSH
☐ AD_WIN2019-D			
☐ AD_WIN2019-			
☐ Disco	admin , fudoportal , fudoportaldwa ,	anon_debian , > pw-user54 LDAP	Debian-SSH-Forwarding , jump , Disco

3. Click *Block*.



Select and block the safe

☐ Name	Users	Accounts	Listeners
☑ >>> Web Client	admin		
☐ LDAP_Ubuntu_10.0.235.1			
☐ SSH	tpo	SSH	new-ssh-listener

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

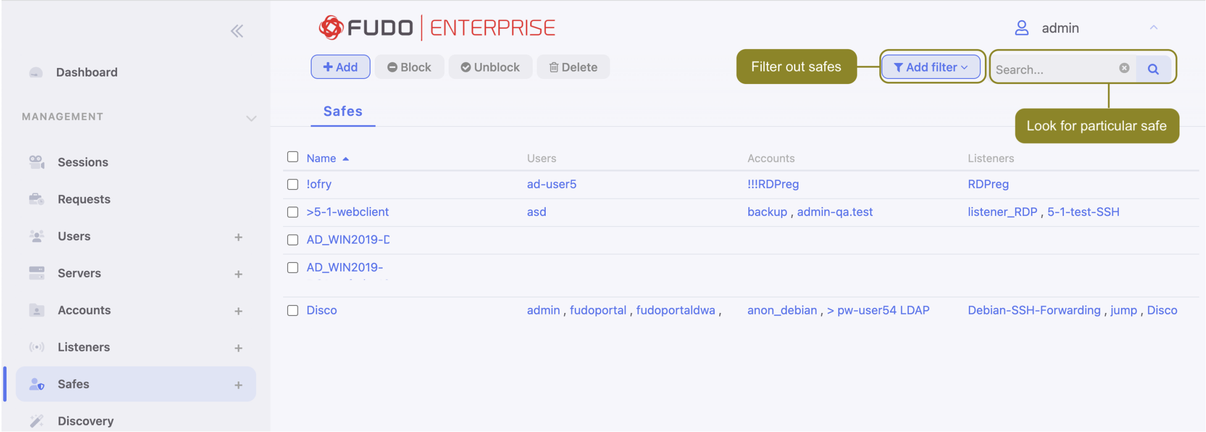
Note: To view the blocking reason, place the cursor over the 💬 icon on the safes list.

Related topics:

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

12.4 Unblocking a safe

1. Select *Management* > *Safes*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.

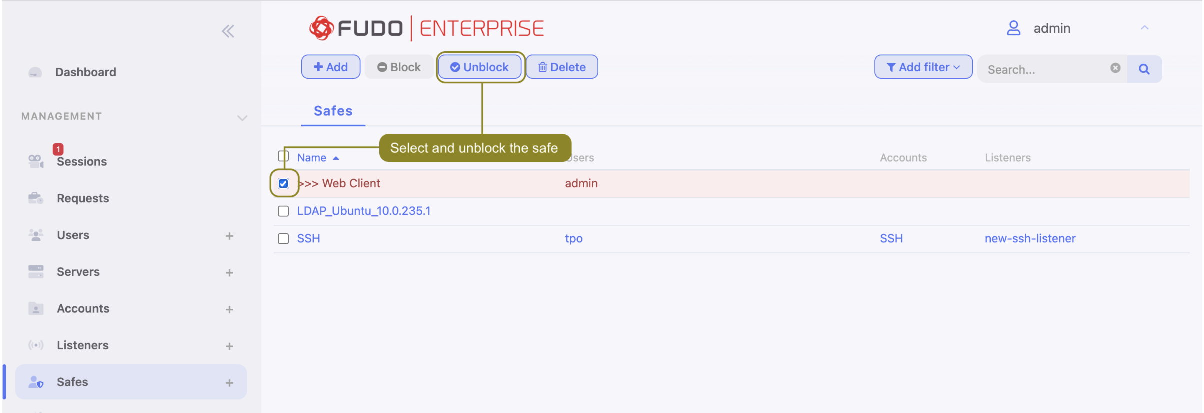


Filter out safes

Look for particular safe

☐ Name	Users	Accounts	Listeners
☐ !ofry	ad-user5	!!!RDPreg	RDPreg
☐ >5-1-webclient	asd	backup , admin-qa.test	listener_RDP , 5-1-test-SSH
☐ AD_WIN2019-D			
☐ AD_WIN2019-			
☐ Disco	admin , fudoportal , fudoportaldwa ,	anon_debian , > pw-user54 LDAP	Debian-SSH-Forwarding , jump , Disco

3. Click *Unblock*.



Select and unblock the safe

☐ Name	Users	Accounts	Listeners
☑ >>> Web Client	admin		
☐ LDAP_Ubuntu_10.0.235.1			
☐ SSH	tpo	SSH	new-ssh-listener

4. Click *Confirm* to unblock selected objects.

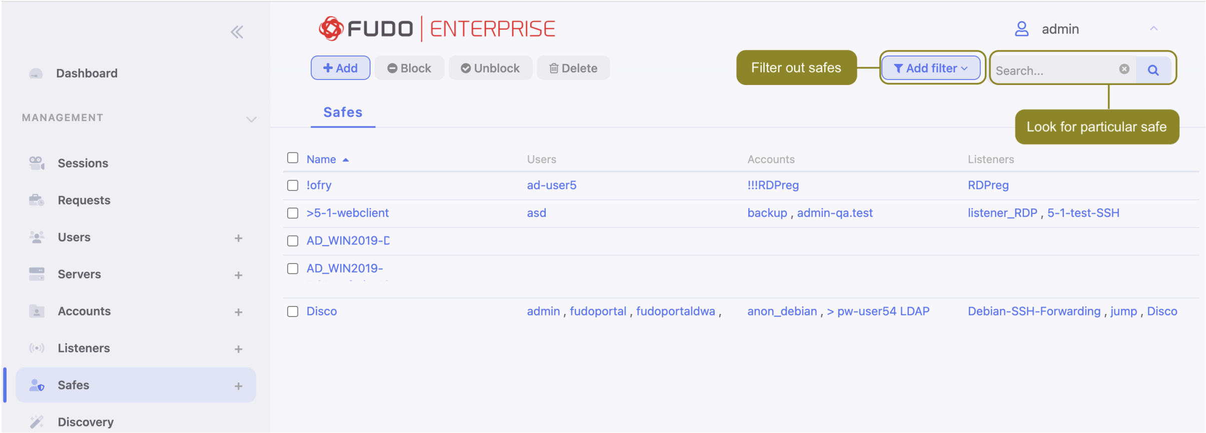
Related topics:

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

12.5 Deleting a safe

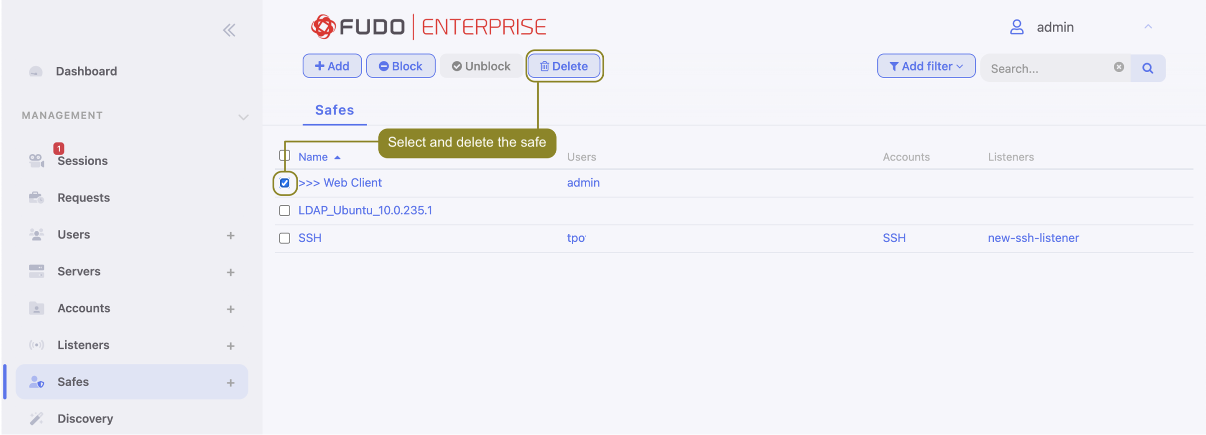
> **Warning:** Deleting a safe definition will terminate all current connections that use accounts assigned to this safe to connect to servers.

1. Select *Management > Safes*.
2. Define filters to limit the number of objects displayed on the list, or use a search bar.



□ Name	Users	Accounts	Listeners
□ !ofry	ad-user5	!!!RDPreg	RDPreg
□ >5-1-webclient	asd	backup , admin-qa.test	listener_RDP , 5-1-test-SSH
□ AD_WIN2019-C			
□ AD_WIN2019-			
□ Disco	admin , fudoportal , fudoportaldwa ,	anon_debian , > pw-user54 LDAP	Debian-SSH-Forwarding , jump , Disco

3. Click *Delete*.



□ Name	Users	Accounts	Listeners
☑ >>> Web Client	admin		
□ LDAP_Ubuntu_10.0.235.1			
□ SSH	tpo	SSH	new-ssh-listener

4. Confirm deletion of selected objects.

Related topics:

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

CHAPTER 13

Discovery

The Discovery feature is able to search domain controllers for accounts with different privilege levels and add them to the relevant safes and/or listeners. This is an *Onboarding* process, which grants the discovered accounts access to connections, is a basis of the Discovery feature. Alternatively, the feature can send the accounts to quarantine, which means blocking accounts on the target server.

Additional nomenclature that comes along with this feature within the *Discovery* and the *Accounts* tab:

Scanner - the main component that aims to discover accounts on the target server. The scanner can have a rule that defines an action that follows the discovery. The scanner can be executed manually or automatically according to the schedule.

Rule allows setting criteria for the accounts to be discovered and the actions to be performed after their discovery.

Account Category - is a privilege level of the account.

Discovered Accounts - accounts that were discovered by the scanner

Onboarded Accounts - accounts that were added to the listener and / or safe

Quarantined Accounts - accounts that were blocked on the target server.

Note: The Discovery feature executes scanning Active Directory by connecting using the LDAP protocol.

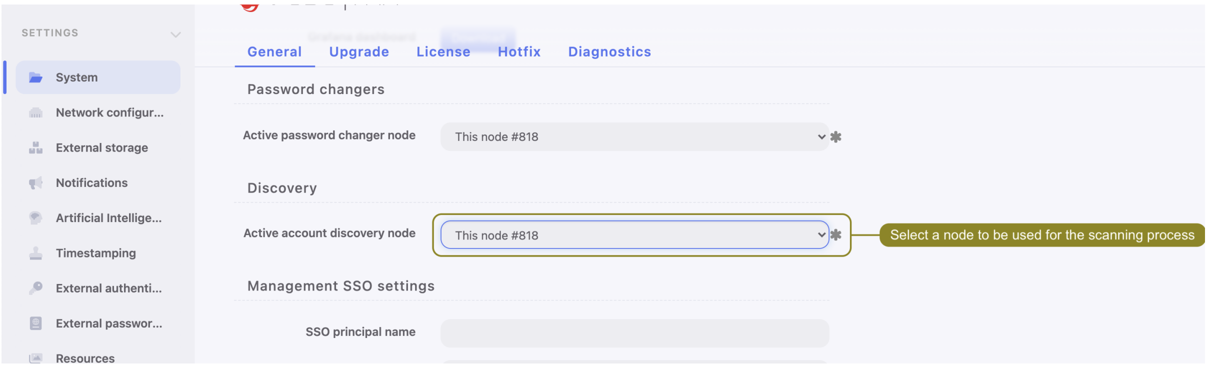
The Discovery function needs two objects to provide the most efficient results:

1. A *scanner* with configuration of the target server and an account to connect, and a schedule for running the scanner automatically.
2. A *rule* to specify what the scanner should do in terms of its discovery.

To have the Discovery function fully automatic, it is advised to start its configuration from creating a rule and next, create a scanner.

Although, if you want to onboard or send to quarantine the discovered accounts manually, you can complete *Creating a scanner* step only, as the scanner can work without the rules being added. Next, discovered accounts can be moved further with the *Manage accounts* option, available in the *Accounts* tab.

Note: Active node, which is used for the scanning process is available to check under the *Discovery* section in the *Settings > System* tab.



Password changers

Active password changer node: This node #818

Discovery

Active account discovery node: This node #818

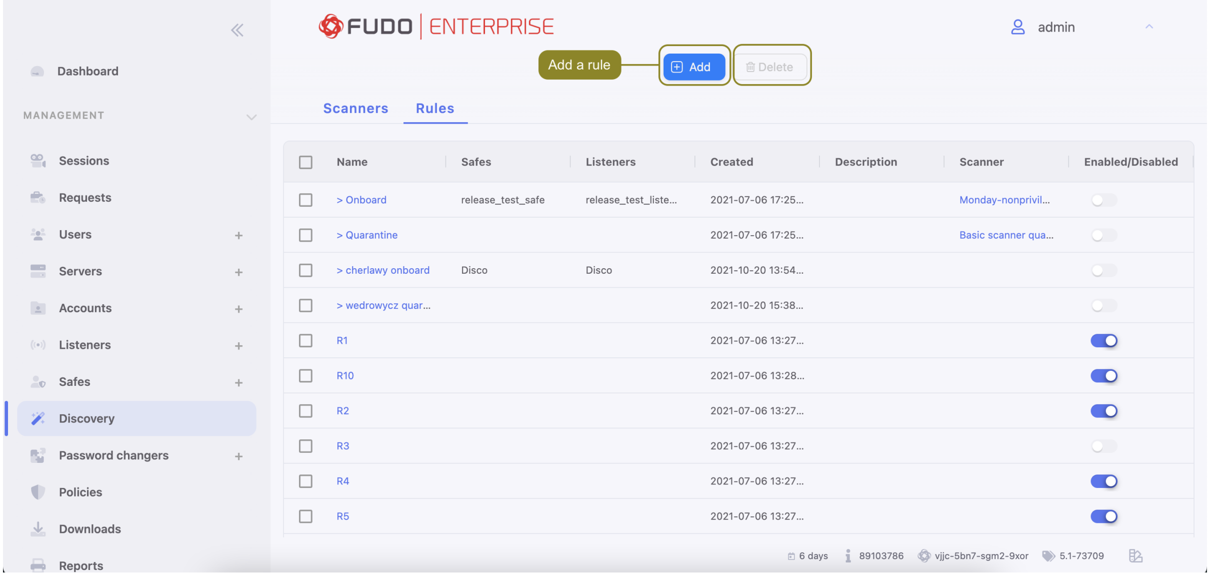
Select a node to be used for the scanning process

Management SSO settings

SSO principal name

13.1 Creating a rule

Each rule can be enabled or disabled anytime. When a rule is enabled, the system will automatically onboard or send to quarantine matching accounts according to the given rule actions. The rules apply to just discovered accounts but not to the accounts that are already onboarded or sent to quarantine by the rules. In practice, it means that after a particular rule is changed, its actions will be applied to the accounts that were discovered after the changes are saved.



Add a rule

□	Name	Safes	Listeners	Created	Description	Scanner	Enabled/Disabled
□	> Onboard	release_test_safe	release_test_liste...	2021-07-06 17:25...		Monday-nonprivil...	○
□	> Quarantine			2021-07-06 17:25...		Basic scanner qua...	○
□	> cherlawy onboard	Disco	Disco	2021-10-20 13:54...			○
□	> wedrowycz quar...			2021-10-20 15:38...			○
□	R1			2021-07-06 13:27...			●
□	R10			2021-07-06 13:28...			●
□	R2			2021-07-06 13:27...			●
□	R3			2021-07-06 13:27...			○
□	R4			2021-07-06 13:27...			●
□	R5			2021-07-06 13:27...			●

In order to create a rule, proceed as follows:

1. Select *Management > Discovery > Rules*
2. Click *+ Add*
3. Enter rule's name.

4. Optionally, enter rule's description.

5. In *Configuration* section:

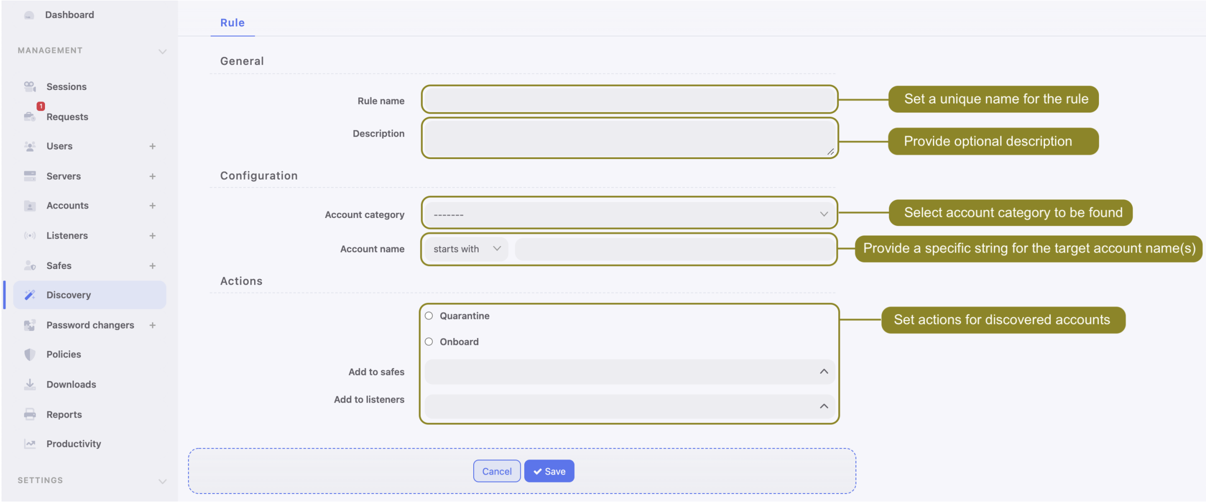
   5.1. Select *Account category* (`privileged`, `non-privileged` or `all`).

   5.2. In the *Account name* field select `consists`, `starts with` or `ends with` and provide a specific string for the target account name(s).

   5.3. Define *Actions*:

      5.3.1. **Send to quarantine** or

      5.3.2. **Onboard** by adding the discovered accounts to the Safe and/or Listener. **Please note that listeners with bastion mode are supported only.**



Set a unique name for the rule

Provide optional description

Select account category to be found

Provide a specific string for the target account name(s)

Set actions for discovered accounts

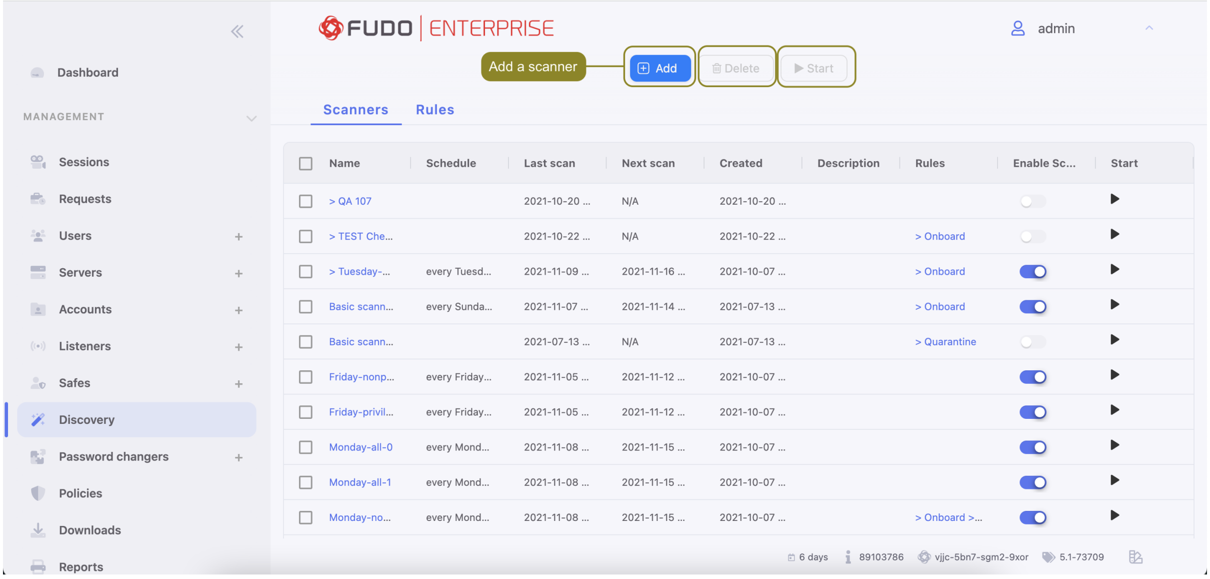
6. Click *Save*.

Related topics:

- *Creating a scanner*
- *Manage accounts*

13.2 Creating a scanner

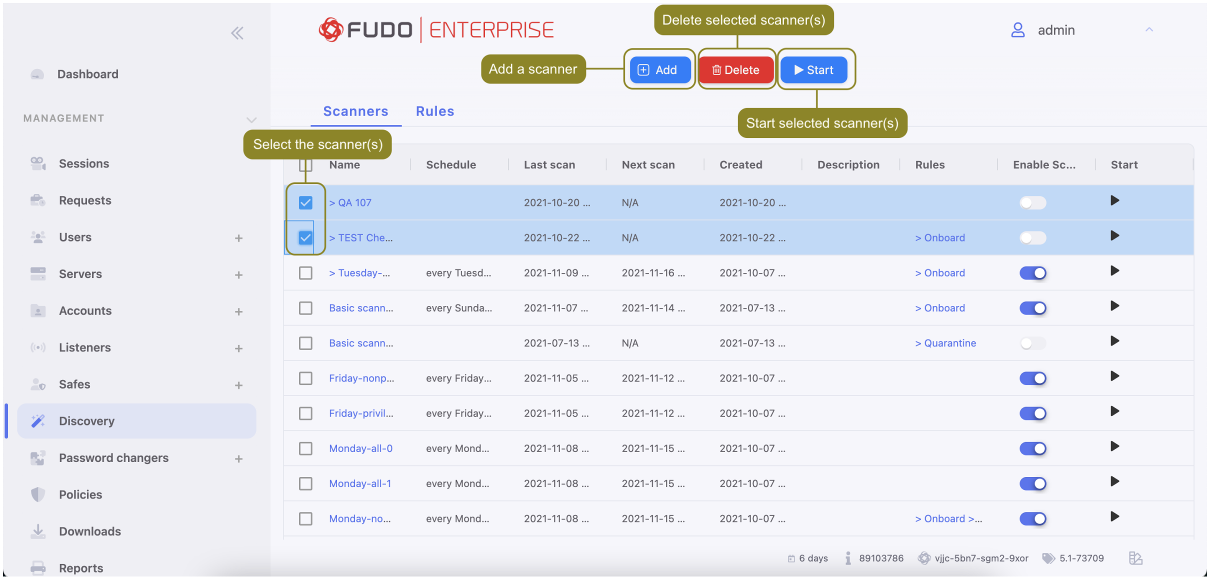
The scanners with defined schedule can have scheduling enabled or disabled anytime. When a scanner has scheduling enabled, the system will automatically execute the given scanner configuration. When a scanner's scheduling is disabled, the system will wait for the decision from superadmin to start its execution.



Add a scanner

□	Name	Schedule	Last scan	Next scan	Created	Description	Rules	Enable Sc...	Start
□	> QA 107		2021-10-20 ...	N/A	2021-10-20 ...			○	▶
□	> TEST Che...		2021-10-22 ...	N/A	2021-10-22 ...		> Onboard	○	▶
□	> Tuesday-...	every Tuesd...	2021-11-09 ...	2021-11-16 ...	2021-10-07 ...		> Onboard	●	▶
□	Basic scann...	every Sunda...	2021-11-07 ...	2021-11-14 ...	2021-07-13 ...		> Onboard	●	▶
□	Basic scann...		2021-07-13 ...	N/A	2021-07-13 ...		> Quarantine	○	▶
□	Friday-nonp...	every Friday...	2021-11-05 ...	2021-11-12 ...	2021-10-07 ...			●	▶
□	Friday-privil...	every Friday...	2021-11-05 ...	2021-11-12 ...	2021-10-07 ...			●	▶
□	Monday-all-0	every Mond...	2021-11-08 ...	2021-11-15 ...	2021-10-07 ...			●	▶
□	Monday-all-1	every Mond...	2021-11-08 ...	2021-11-15 ...	2021-10-07 ...			●	▶
□	Monday-no...	every Mond...	2021-11-08 ...	2021-11-15 ...	2021-10-07 ...		> Onboard >...	●	▶

Several scanners can be started in batch, or be deleted after being selected.



Delete selected scanner(s)

Add a scanner

Start selected scanner(s)

Select the scanner(s)

□	Name	Schedule	Last scan	Next scan	Created	Description	Rules	Enable Sc...	Start
☑	> QA 107		2021-10-20 ...	N/A	2021-10-20 ...			○	▶
☑	> TEST Che...		2021-10-22 ...	N/A	2021-10-22 ...		> Onboard	○	▶
□	> Tuesday-...	every Tuesd...	2021-11-09 ...	2021-11-16 ...	2021-10-07 ...		> Onboard	●	▶
□	Basic scann...	every Sunda...	2021-11-07 ...	2021-11-14 ...	2021-07-13 ...		> Onboard	●	▶
□	Basic scann...		2021-07-13 ...	N/A	2021-07-13 ...		> Quarantine	○	▶
□	Friday-nonp...	every Friday...	2021-11-05 ...	2021-11-12 ...	2021-10-07 ...			●	▶
□	Friday-privil...	every Friday...	2021-11-05 ...	2021-11-12 ...	2021-10-07 ...			●	▶
□	Monday-all-0	every Mond...	2021-11-08 ...	2021-11-15 ...	2021-10-07 ...			●	▶
□	Monday-all-1	every Mond...	2021-11-08 ...	2021-11-15 ...	2021-10-07 ...			●	▶
□	Monday-no...	every Mond...	2021-11-08 ...	2021-11-15 ...	2021-10-07 ...		> Onboard >...	●	▶

In order to create a scanner, proceed as follows:

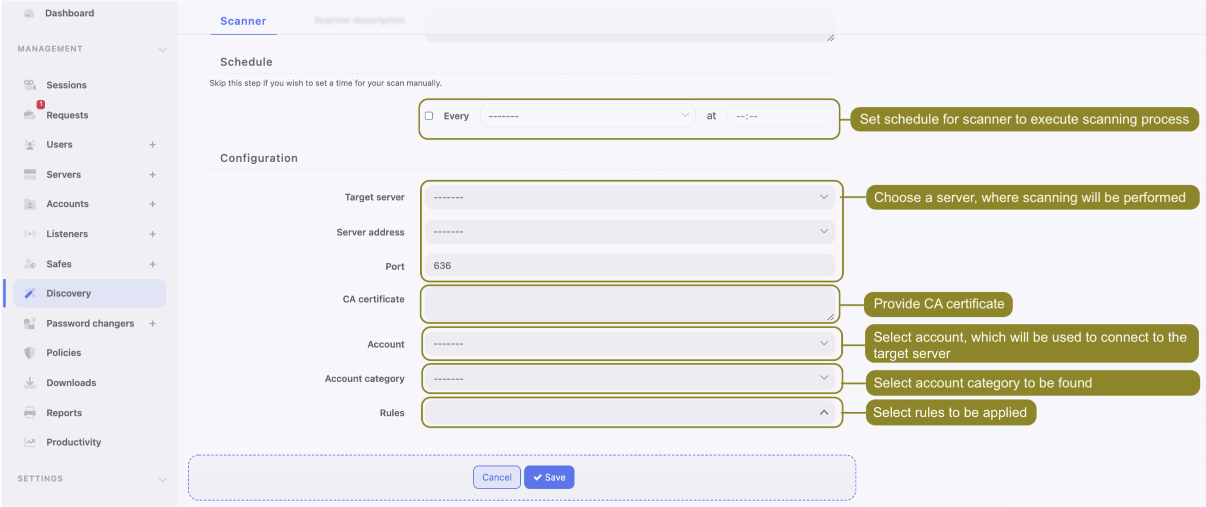
1. Select *Management* > *Discovery* > *Scanners*
2. Click + *Add*
3. Enter scanner's name.
4. The *Scanner type* field has the `Domain Controller` value by default.
5. Optionally, enter scanner's description.
6. In the *Schedule* section, choose a day and time for your scanner to start automatically on a weekly basis. This field is optional, so you can skip this step to start your scan manually anytime.
7. Fill *Configuration* section with:
   7.1. *Target server*
   7.2. *Server address* and *Port*

7.3. *CA certificate*

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

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

7.6. Choose *Rules* to set the following actions after the scan. **Please note that in case more than one rule is added and their actions overlap, the order of the rules is taken into account: the first matching rule will be applied.**



Schedule

Skip this step if you wish to set a time for your scan manually.

□ Every ------- at --:--

Set schedule for scanner to execute scanning process

Configuration

Target server -------

Server address -------

Port 636

CA certificate

Account -------

Account category -------

Rules

Choose a server, where scanning will be performed

Provide CA certificate

Select account, which will be used to connect to the target server

Select account category to be found

Select rules to be applied

8. Click Save.

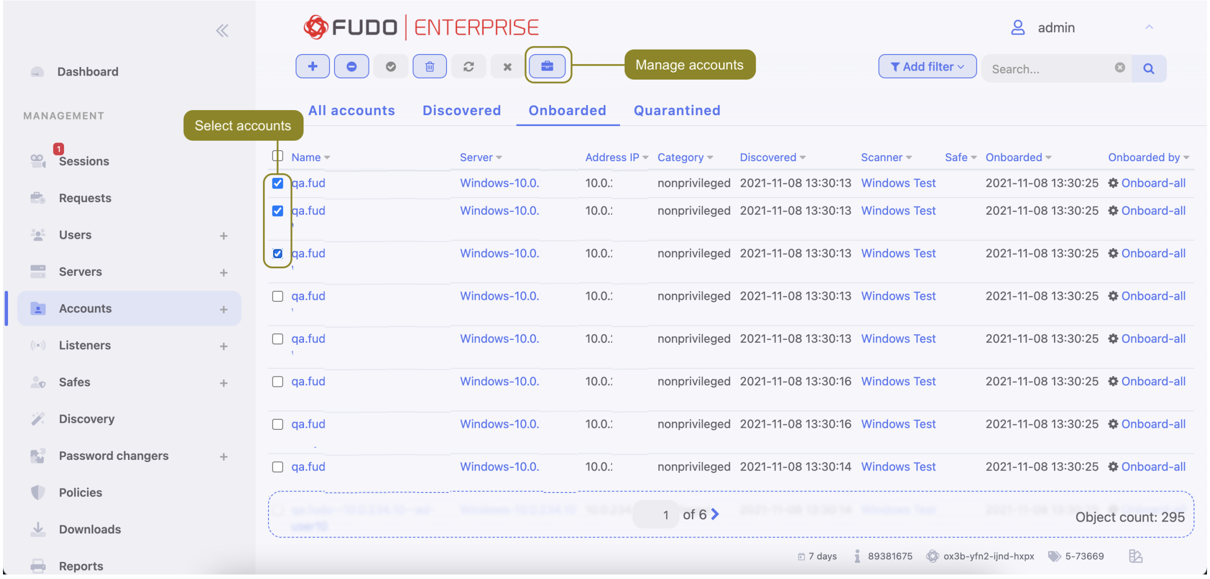
Related topics:

- *Creating a rule*
- *Manage accounts*

13.3 Manage accounts

This is a part of automatic Discovery process that scans the domain controllers in terms of unassigned accounts and onboards them automatically.

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



	Name	Server	Address IP	Category	Discovered	Scanner	Safe	Onboarded	Onboarded by
☑	qa.fud	Windows-10.0.	10.0.:	nonprivileged	2021-11-08 13:30:13	Windows Test		2021-11-08 13:30:25	Onboard-all
☑	qa.fud	Windows-10.0.	10.0.:	nonprivileged	2021-11-08 13:30:13	Windows Test		2021-11-08 13:30:25	Onboard-all
☑	qa.fud	Windows-10.0.	10.0.:	nonprivileged	2021-11-08 13:30:13	Windows Test		2021-11-08 13:30:25	Onboard-all
☐	qa.fud	Windows-10.0.	10.0.:	nonprivileged	2021-11-08 13:30:13	Windows Test		2021-11-08 13:30:25	Onboard-all
☐	qa.fud	Windows-10.0.	10.0.:	nonprivileged	2021-11-08 13:30:13	Windows Test		2021-11-08 13:30:25	Onboard-all
☐	qa.fud	Windows-10.0.	10.0.:	nonprivileged	2021-11-08 13:30:16	Windows Test		2021-11-08 13:30:25	Onboard-all
☐	qa.fud	Windows-10.0.	10.0.:	nonprivileged	2021-11-08 13:30:16	Windows Test		2021-11-08 13:30:25	Onboard-all
☐	qa.fud	Windows-10.0.	10.0.:	nonprivileged	2021-11-08 13:30:14	Windows Test		2021-11-08 13:30:25	Onboard-all

1 of 6 › Object count: 295

7 days 89381675 ox3b-yfn2-ijnd-hxpx 5-73669

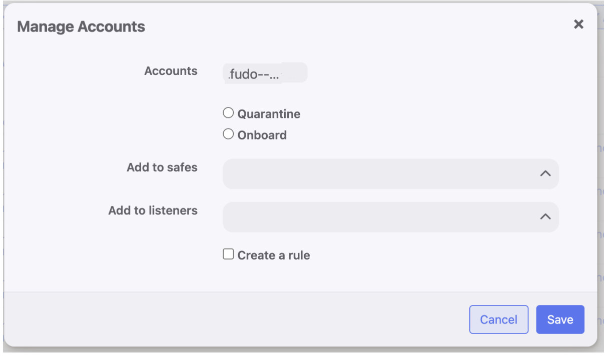
Note: Usually, *discovered* accounts are not onboarded automatically due to a lack of automatic rule in the system. Administrator can manually onboard them by choosing the Manage Accounts option.

---

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

   4.1 **Send to quarantine** (optionally, you can add a reason) or

   4.2 **Onboard** by adding the discovered accounts to the Safe and/or Listener. Warning: The listeners with bastion mode are supported only.
5. Click on a *Create a rule* checkbox if you want to set the defined actions to be executed automatically by the scanner in the future.



Accounts: fudo--...

○ Quarantine
○ Onboard

Add to safes:

Add to listeners:

☐ Create a rule

6. Click *Save*.

Related topics:

- *Creating a rule*

- *Creating a scanner*

CHAPTER 14

Password changers

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

Password changers run on a separate transport layer: SSH, LDAP, Telnet or WinRM, and you can either use one of the built-in ones or *create your own script*. You can also *write custom plugins* and *upload* them to your Fudo Enterprise.

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

14.1 Password changer policy

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

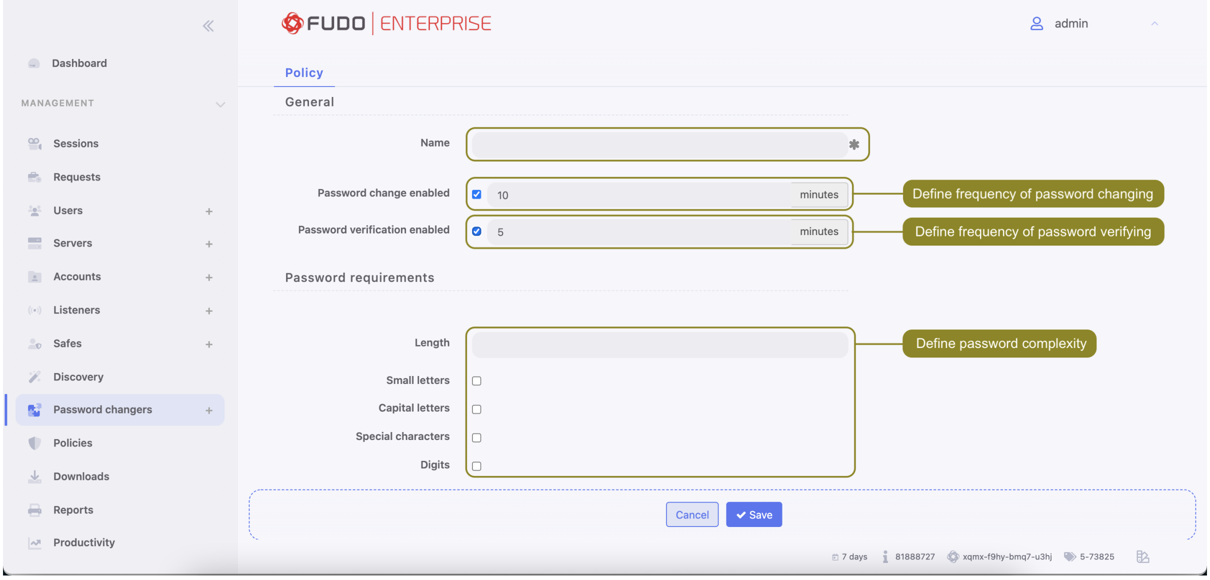
14.1.1 Defining a password changer policy

1. Select *Management* > *Password changers* > *Password policies*.
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*.



Name *

Password change enabled ☑ 10 minutes

Password verification enabled ☑ 5 minutes

Length

Small letters □

Capital letters □

Special characters □

Digits □

Define frequency of password changing

Define frequency of password verifying

Define password complexity

14.1.2 Editing a password changer policy

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

14.1.3 Deleting a password changer policy

1. Select *Management > Password changers > Password policies*.
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*

14.2 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.

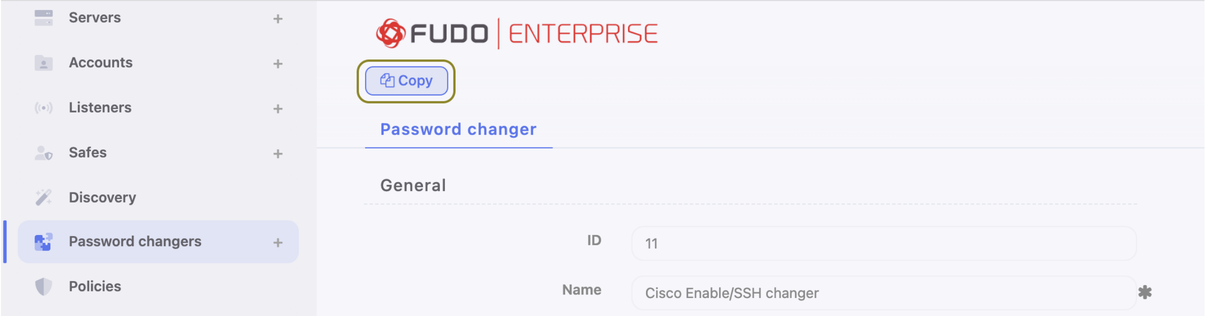
Note: In cluster configuration, the node responsible for changing passwords on monitored systems is configured in system settings. For more information refer to *Password changers - active cluster node* topic.

14.2.1 Defining a custom password changer

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

Select *Management > Password changers*. Click *+ Add* and then choose *New password changer*.

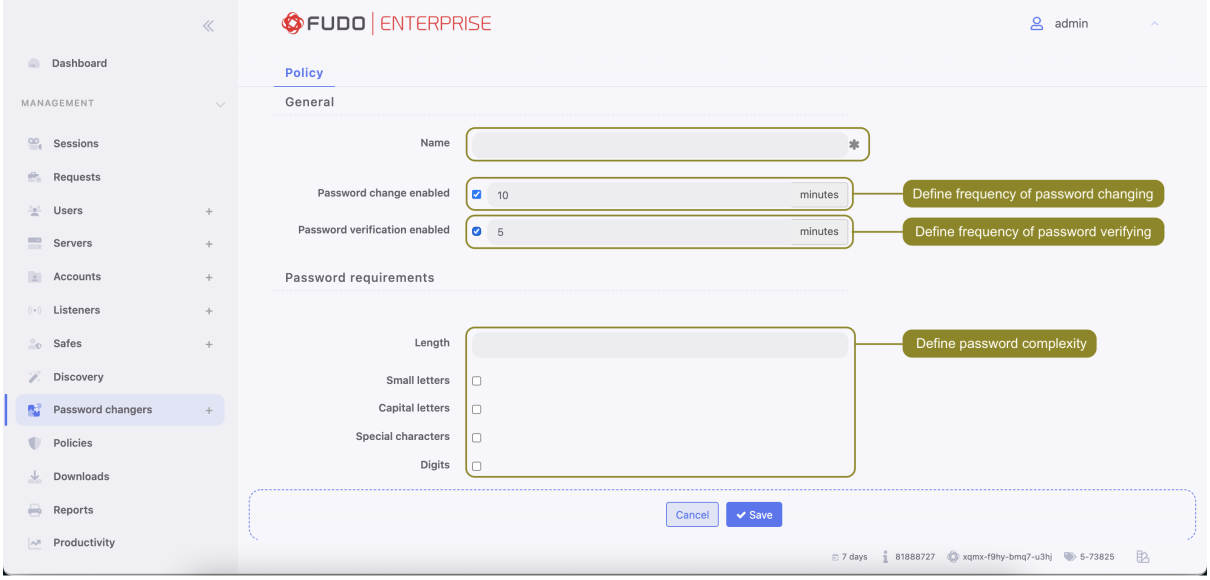
Note: Alternatively, you can find and click an existing password changer and click *Copy* to create a new password changer based on currently opened definition.



General

ID	11
Name	Cisco Enable/SSH changer

2. Define the password changer's name.
3. From the *Script type* drop-down list, select if the script is a password changer or password verifier.
4. From the *Connection mode* drop-down list, select the transport layer.
5. In the *Timeout* field, define the script's execution time limit.



General

Name	
Password change enabled	☑ 10 minutes
Password verification enabled	☑ 5 minutes

Define frequency of password changing

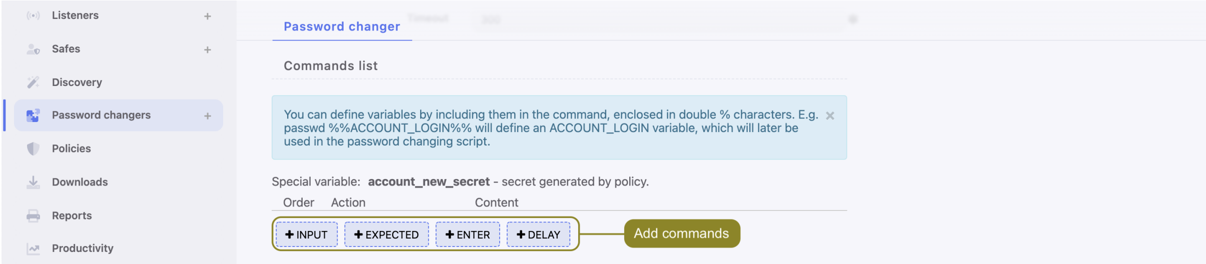
Define frequency of password verifying

Password requirements

Length	
Small letters	□
Capital letters	□
Special characters	□
Digits	□

Define password complexity

6. In the *Commands list* section, click + to add a command.



Commands list

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.

Special variable: **account_new_secret** - secret generated by policy.

Order	Action	Content

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.

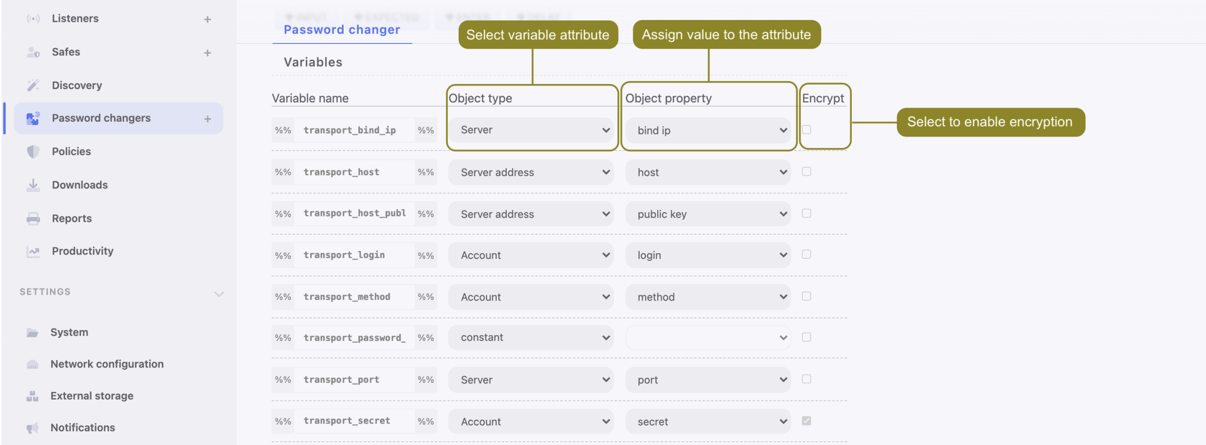
Warning: To configure **WinRM** password changers, you need to provide user credentials with the authority to change passwords (typically an admin-level account). However, it's important to avoid using this account to change its own password, as WinRM will return an error that Fudo Enterprise cannot process. **Make sure that the account_login and transport_login variables are set to different values.**

7. 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%%`).

---

8. Repeat steps 8-10 to add more commands.
9. In the *Variables* section, define variables' attributes.



Variables

Variable name	Object type	Object property	Encrypt
%% transport_bind_ip %%	Server	bind ip	☐
%% transport_host %%	Server address	host	☐
%% transport_host_publ %%	Server address	public key	☐
%% transport_login %%	Account	login	☐
%% transport_method %%	Account	method	☐
%% transport_password_ %%	constant		☐
%% transport_port %%	Server	port	☐
%% transport_secret %%	Account	secret	☑

Note: Variables can be initiated with values referenced from other objects or they can be assigned a constant value.

---

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

Note: Example

In this password changer example, the password change is triggered with the `passwd` command executed with sudo privileges on a host running FreeBSD operating system.

Commands list

	Action	Content	Comment
1	EXPECTED	`Password`	Expected terminal output with a 'Password' word in it.
2	INPUT	`%%transport_secret%%`	A value of the `transport_secret` variable is a secret for authorizing a 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	✗

14.2.2 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. Click the name of desired password changer.
3. Edit selected commands.
4. Click *X* to remove selected command.
5. Click *Save*.

14.2.3 Deleting a custom password changer

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

Related topics:

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

14.3 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.

14.3.1 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.

14.3.2 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.

14.3.3 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.

14.3.4 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

Warning: To configure WinRM password changers, you need to provide user credentials with the authority to change passwords (typically an admin-level account). However, it’s important to avoid using this account to change its own password, as WinRM will return an error that Fudo Enterprise cannot process. **Make sure that the account_login and transport_login variables are set to different values.**

Variable	Description
transport_bind_ip	Fudo IP address used to establish connection with the remote host.
transport_ca_certificate	CA certificate of the target system.
transport_encoding	Text encoding used by the target system.
transport_host	An IP address of the remote host that the password changer/verifier connects to.
transport_login	An account on the target system used to change passwords. It has to be different from the account on which the password is being changed (account_login variable).
transport_port	A port number that the password changer/verifier connects to.
transport_secret	Secret used to access the account to execute password change.
account_login	Login of the user whose password is being changed.
account_new_secret	System default variable initiated with the value automatically generated by Fudo.

Related topics:

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

- *Setting up password changing on a Unix system*

14.4 Setting up password changing on a Unix system

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

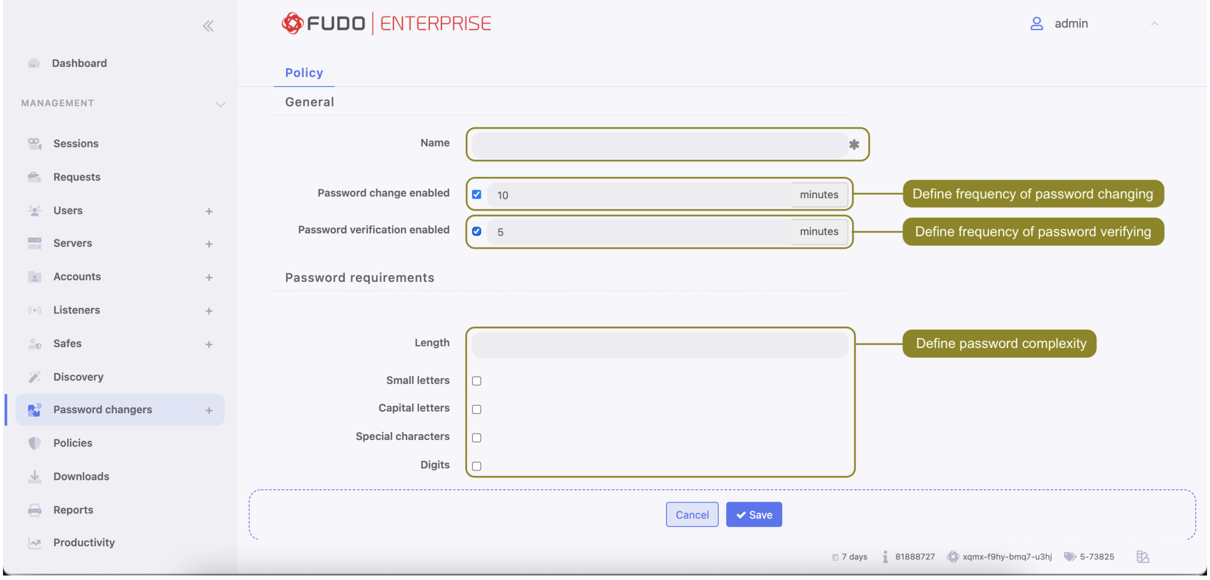
Adding a password change policy

1. Select *Management > Password changers > Password policies*.
2. Click *+ Add* to create a new password changing policy.
3. Provide password change policy name.

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

---

4. Select the *Password change enabled* option and define how frequently the password will be changed.
5. Select the *Password verification enabled* option and define how frequently the Secret Manager should verify whether the password has not been changed in any other way but the Secret Manager itself.
6. Provide the number of characters comprising the password.
7. Select desired password complexity options and provide the minimal number of characters for each.



General

Name: *

Password change enabled ☑ 10 minutes

Password verification enabled ☑ 5 minutes

Password requirements

Length:

Small letters ☐

Capital letters ☐

Special characters ☐

Digits ☐

Define frequency of password changing

Define frequency of password verifying

Define password complexity

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.

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*

14.5 Plug-ins

Plug-ins enable convenient development and deployment of complex password changers.

14.5.1 Developing plug-ins

Plug-ins enable convenient development and deployment of advanced, custom password changers.

14.5.1.1 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 Enterprise 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*

14.5.1.2 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 Enterprise 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 Enterprise 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: http, modbus, mysql, 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	Server network subnet specifier, e.g. 192.168.0.0/24
server_address	Server IP address. A single object can have unique address or network subnet 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 Enterprise.

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,
```

(continues on next page)

(continued from previous page)

```
    )
    if req.status_code != 200:
        raise RedmineChangerError(
            'HTTP status code {} from {}.'.format(req.status_code,␣
↪server_uri)
        )

    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,
    )
```

(continues on next page)

(continued from previous page)

```
        if req.status_code != 200:
                raise RedmineChangerError(
                        'HTTP status code {} from {}.'.format(req.status_code,␣
↪server_uri)
                )

        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
```

(continues on next page)

(continued from previous page)

```
                )
                return 1

        if login != transport_login:
                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)
```

(continues on next page)

(continued from previous page)

```
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*

14.5.1.3 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:

- *Custom password changers*
- *Password changer policy*
- *Setting up password changing on a Unix system*

14.5.2 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*

CHAPTER 15

Policies

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

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

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

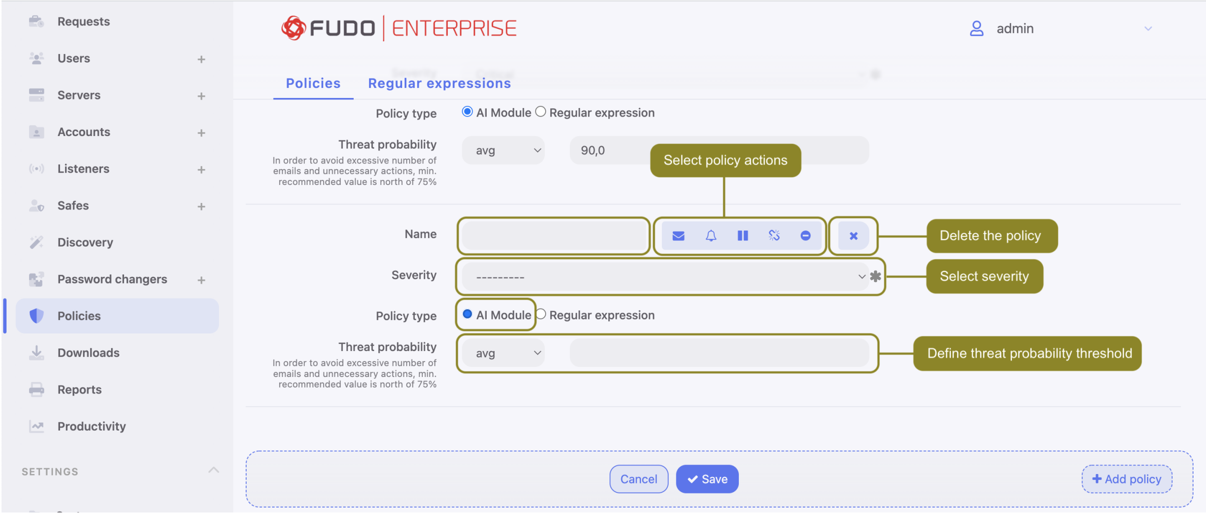
Both types of policies react by taking the following actions:

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

15.1 AI module-based policy

In order to configure an AI module-based policy, proceed as the following states:

1. Select *Management > Policies*.
2. Click *Add policy*.
3. Provide the Name for the policy.



Policy type ● AI Module ○ Regular expression

Threat probability: avg, 90,0

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

Name

Severity: ---------

Policy type ● AI Module ○ Regular expression

Threat probability: avg

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

Select policy actions

Delete the policy

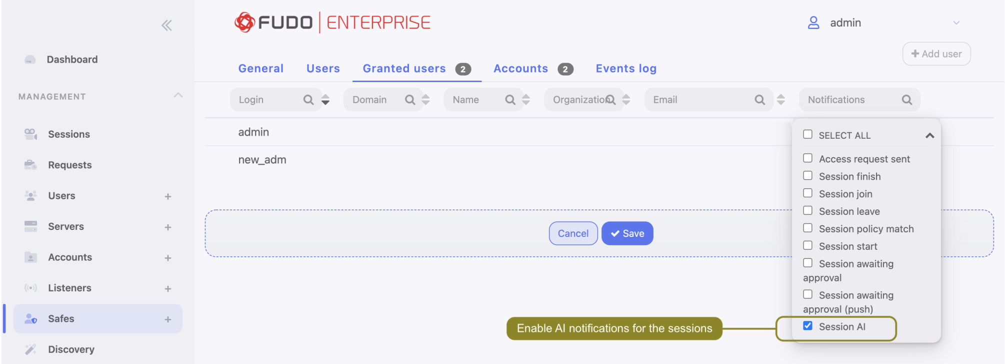
Select severity

Define threat probability threshold

4. Select the actions that will be performed when the policy is breached:

   - send email notification to system administrator,

Note: Sending email notifications requires configuring and enabling *notification service* as well as *Session AI* notification enabled in safe configuration.



□ SELECT ALL
□ Access request sent
□ Session finish
□ Session join
□ Session leave
□ Session policy match
□ Session start
□ Session awaiting approval
□ Session awaiting approval (push)
☑ Session AI

Enable AI notifications for the sessions

   - send SNMP TRAP notification to the receiver,

Note: Sending SNMP TRAP notifications requires configuring the SNMPv3 TRAP in the System tab. Check the *SNMP* page for more information.

   - pause connection,
   - terminate connection,
   - block user.

Warning: If SNMP TRAP service is not configured, all notifications on policy violation will be discarded but other options related to the session management will work.

5. Select the Severity. Severity parameter value is included in the email notification message and in the *Events log* with the `FSW0284` code.

6. Check the `AI module` in the *Policy type* field.

7. Select min, avg (default) or max option for the *Threat Probability Threshold* field and provide the value.

Note: Values for the *Threat Probability* metrics are calculated by the *AI models* for each session segment. The segment evaluations are averaged per model (e.g. Mouse Biometric, Keyboard Biometric) creating a model Threat Probability, thus the AI model delivers one Threat Probability per model for the whole session. These values are used in the policy and the policy actions can be applied to the minimum, average or maximum value of model Threat Probabilities.

In practice, if an administrator wants to decrease sensitivity of the policy so that it reacts to breaching a given threshold by **all the models**, the Threat Probability Threshold should be set to minimum. If the situation requires the policy to be more sensitive and react to the threshold breaching by **at least one model**, then the Threat Probability Threshold should be set to maximum.

Default value for the Threat Probability Threshold is average.

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

8. Click *Save*.

AI module-based policy examples

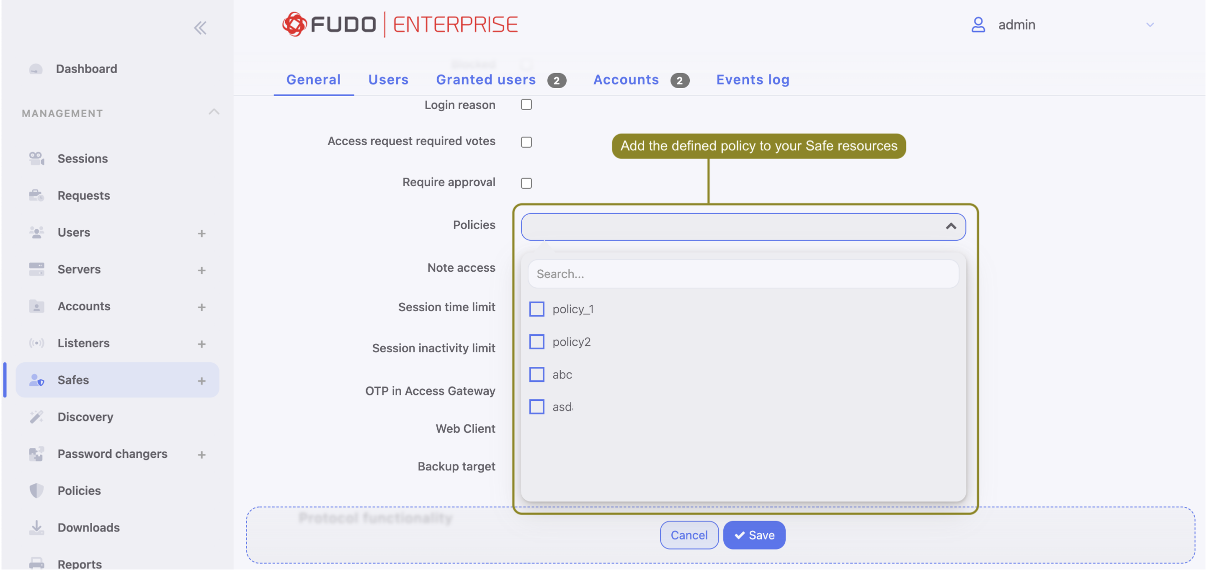
Example 1. Sending SNMP TRAP notifications about suspicious sessions.

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

1. Create a user for SNMPv3 service:
   - Select *Management* > *Users*.
   - Create a new one.
   - Enter Login.
   - Choose the service in the *Role* field.
   - Select Password in the *Authentication Type* field and provide your password.
   - In the *SNMP* section, define the settings:
     - Enable SNMP.
     - Select SHA or MD5 in the *Authentication Method* field.
     - Select *AES* or *DES* in the *Encryption* field.
   - Click *Save*.
2. Configure SNMPv3 TRAP:
   - Select *Settings* > *System*
   - Scroll down to the *Maintenance and supervision* section
   - Configure the SNMPv3 TRAP *server address* and *port*
   - Select the user with service role, created in step 1.
   - Click *Save*.

3. Create policy:
   - Select *Management > Policies*.
   - Click *Add policy*.
   - Provide the Name for the policy.
   - Select the *SNMP TRAP* option in the *Actions* field.
   - Select `AI module` in the *Policy type* field.
   - Select the option of the *Threat Probability Threshold* (e.g. `avg`) and add its value (e.g. `90%`).
   - Click *Save*.
4. Assign the policy to a *safe* that is used to establish connections to servers.

- Click *Save*.



Login reason □

Access request required votes □

Require approval □

Policies

Note access

Session time limit

Session inactivity limit

OTP in Access Gateway

Web Client

Backup target

Add the defined policy to your Safe resources

Search...

□ policy_1

□ policy2

□ abc

□ asd

Example 2. Terminating suspicious sessions when the Threat Probability Threshold is reached.

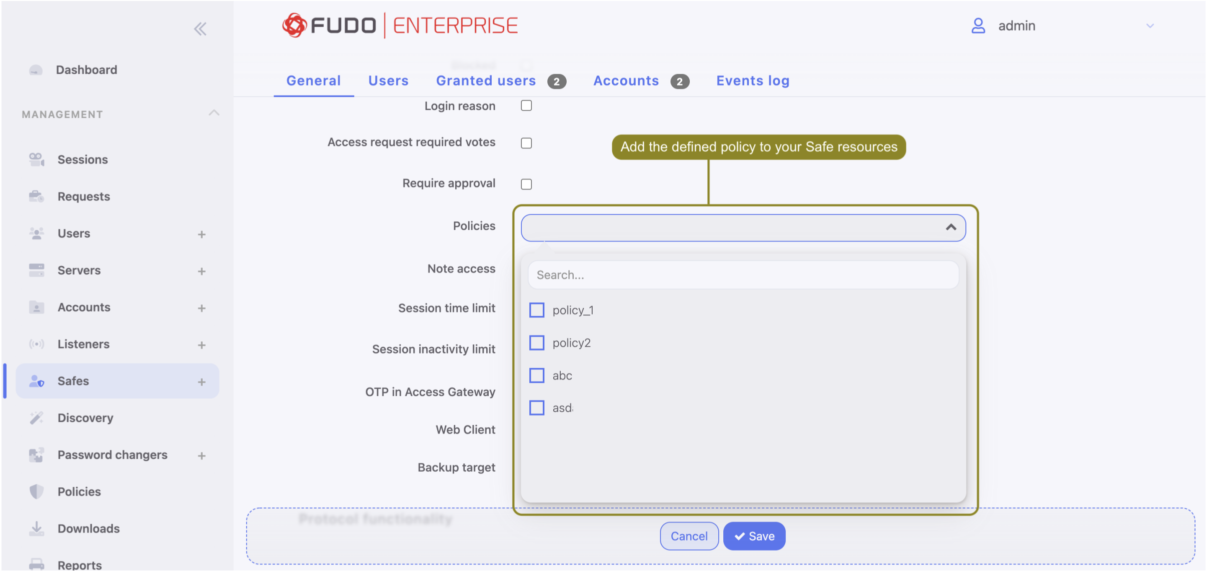
To configure the policy to terminate suspicious sessions when the Threat Probability Threshold is reached, follow the procedure:

1. Create policy:
   - Select *Management > Policies*.
   - Click *Add policy*.
   - Provide the Name for the policy.
   - Select the *Terminate session* option in the *Actions* field.
   - Select `AI module` in the *Policy type* field.
   - Select the option of the *Threat Probability Threshold* (e.g. `avg`) and add its value (e.g. `90%`).
   - Click *Save*.

Note: For harsh actions like pausing or terminating a session or blocking a user it's advised to use higher max thresholds to minimize consequences of false positives.

2. Assign the policy to a *safe* that is used to establish connections to servers.

- Click *Save*.



Add the defined policy to your Safe resources

15.2 Regular expression-based policy

Note: Fudo Enterprise supports POSIX extended regular expression.

Follow the steps to configure a regular expression-based policy:

1. Select *Management > Policies*.
2. Select *Regular expressions* tab.
3. Click *+ Add regular expression*.
4. Enter pattern name.
5. Define the pattern itself.

Note:

- Patterns can be defined as regular expressions.
- Fudo Enterprise does not recognize expressions which use backslash character, e.g. `\d`, `\D`, `\w`, `\W`.

6. Repeat steps 3-5 to define additional patterns.
7. Click *Save*.

Note: Regular expressions examples

Command `rm`

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

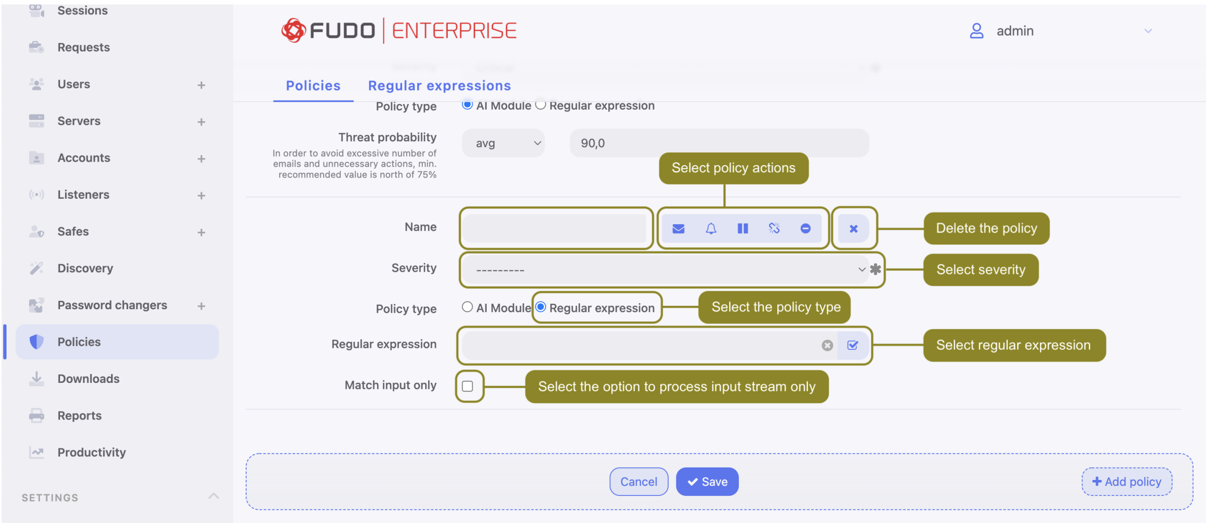
Command `rm -rf` (*also* `-fr`; `-Rf`; `-fR`)

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

Command `rm file`

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

8. Select *Management > Policies*.
9. Click *Add policy*.



Policy type ● AI Module ○ Regular expression

Threat probability
In order to avoid excessive number of emails and unnecessary actions, min. recommended value is north of 75%
avg 90,0

Name

Severity ---------

Policy type ○ AI Module ● Regular expression

Regular expression

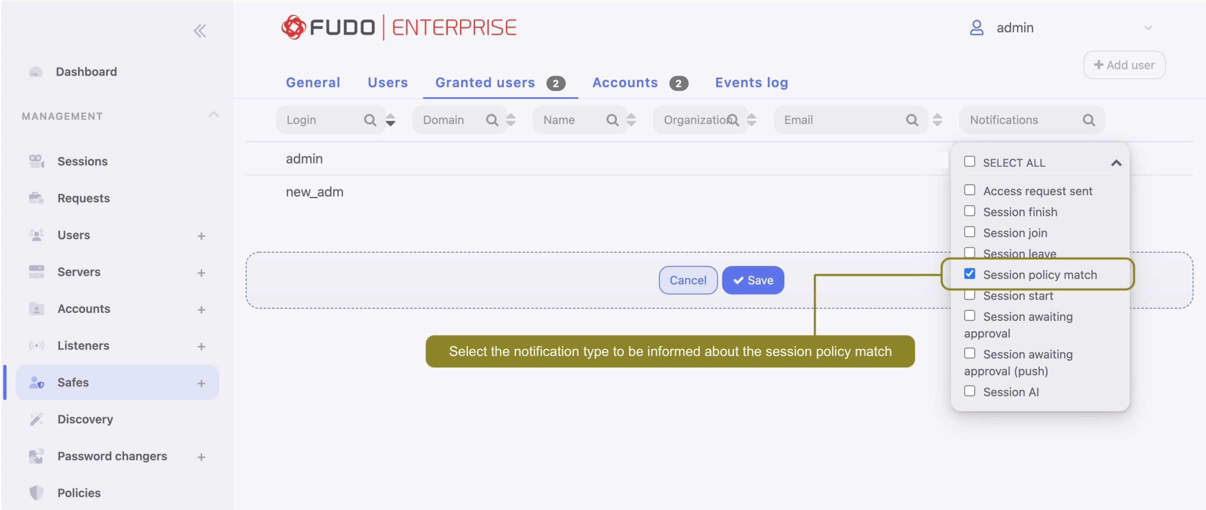
Match input only □

10. Enter policy name.
11. Select actions:

- Send email notification to system administrator,
- Send SNMP TRAP notification,
- 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*.



Select the notification type to be informed about the session policy match

- Note that blocking the user automatically terminates the connection.

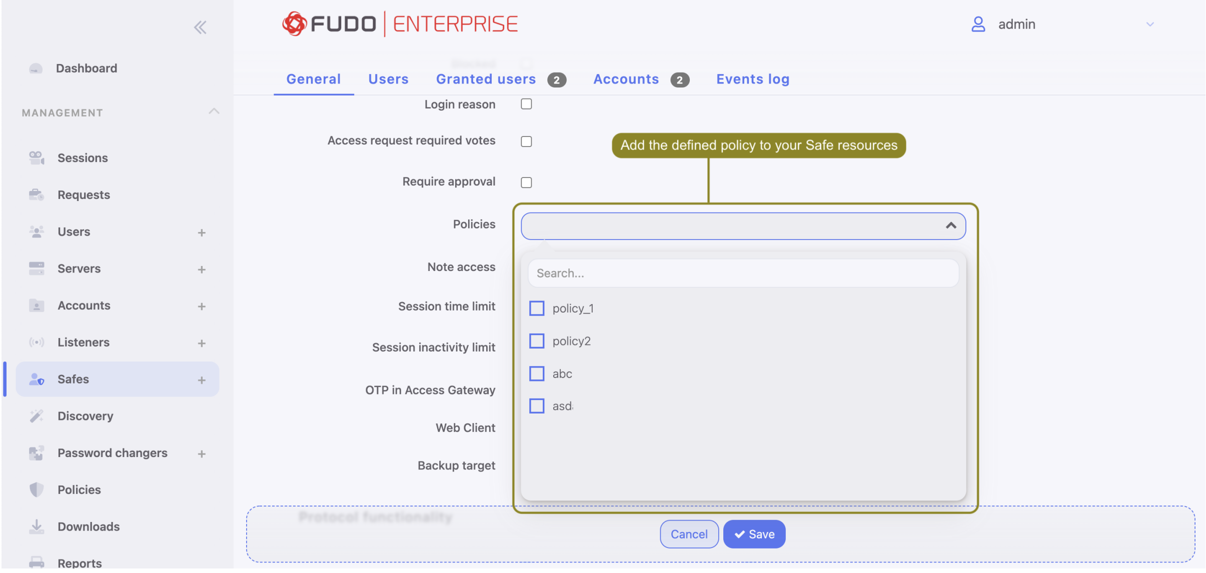
12. Select `Regular expression` in the *Policy type* field.
13. Select monitored patterns.
14. Select policy severity.

Note: Severity parameter value is included in the email notification message.

15. Select the *Match input only* option to process input stream only.

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

16. Click *Save*.
17. After defining a policy, assign it to a *safe* that is used to establish connections to servers.



Add the defined policy to your Safe resources

Related topics:

- *Artificial Intelligence*
- *AI sessions processing*
- *Safes*
- *Terminating connection*
- *Notifications*
- *Security*

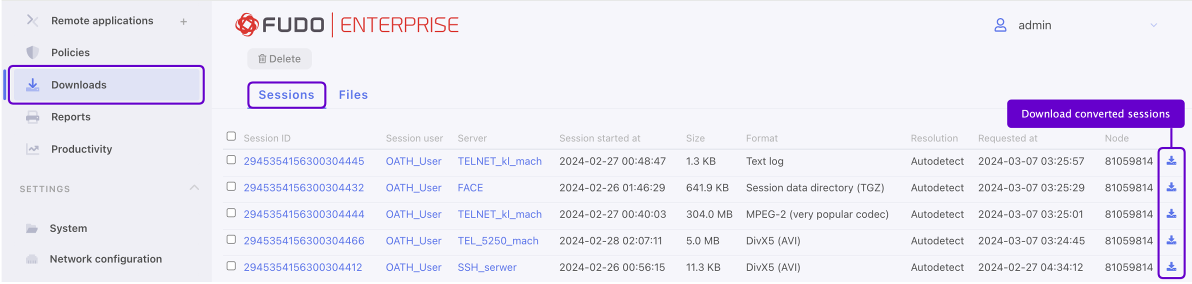
CHAPTER 16

Downloads

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

16.1 Sessions

Fudo Enterprise allows converting stored session data to one of supported formats. The **Sessions** tab is designated for managing session recordings that were previously selected for download in Management > Sessions. For detailed instructions on how to export a session, and available file formats, please refer to the *Exporting sessions* section of this manual.



☐ Session ID	Session user	Server	Session started at	Size	Format	Resolution	Requested at	Node
☐ 2945354156300304445	OATH_User	TELNET_kl_mach	2024-02-27 00:48:47	1.3 KB	Text log	Autodetect	2024-03-07 03:25:57	81059814
☐ 2945354156300304432	OATH_User	FACE	2024-02-26 01:46:29	641.9 KB	Session data directory (TGZ)	Autodetect	2024-03-07 03:25:29	81059814
☐ 2945354156300304444	OATH_User	TELNET_kl_mach	2024-02-27 00:40:03	304.0 MB	MPEG-2 (very popular codec)	Autodetect	2024-03-07 03:25:01	81059814
☐ 2945354156300304466	OATH_User	TEL_5250_mach	2024-02-28 02:07:11	5.0 MB	DivX5 (AVI)	Autodetect	2024-03-07 03:24:45	81059814
☐ 2945354156300304412	OATH_User	SSH_serwer	2024-02-26 00:56:15	11.3 KB	DivX5 (AVI)	Autodetect	2024-02-27 04:34:12	81059814

16.2 Files

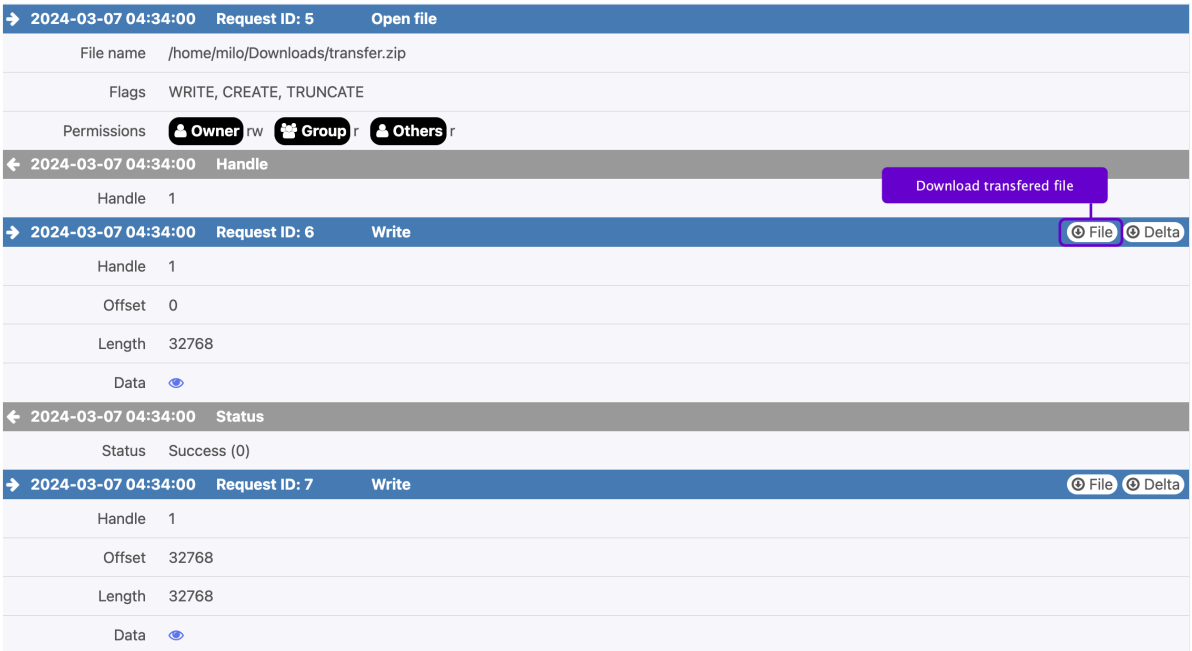
The **Files** tab is designated for managing the downloads of large files that originate from recorded sessions via the SFTP protocol. If the selected file exceeds the 50 MB threshold, it undergoes an encoding process and subsequently appears in the **Files** tab, ready for download. Files smaller than 50 MB are directly downloaded through the browser without encoding.

To download a file transfered during SFTP session, users must initiate the download from the session player interface. To view a session, proceed as follows:

1. Select *Select > Sessions*.

2. Find desired SFTP session and click the play icon next to it.
3. In the session player window, navigate through the SFTP session history to locate the desired file for download, then click the **File** button to initiate the encoding process.

Note: To ensure the download of the entire file, please use the **File** button.



2024-03-07 04:34:00 Request ID: 5 Open file

File name /home/milo/Downloads/transfer.zip

Flags WRITE, CREATE, TRUNCATE

Permissions Owner rw Group r Others r

2024-03-07 04:34:00 Handle

Handle 1

2024-03-07 04:34:00 Request ID: 6 Write

Handle 1

Offset 0

Length 32768

Data

2024-03-07 04:34:00 Status

Status Success (0)

2024-03-07 04:34:00 Request ID: 7 Write

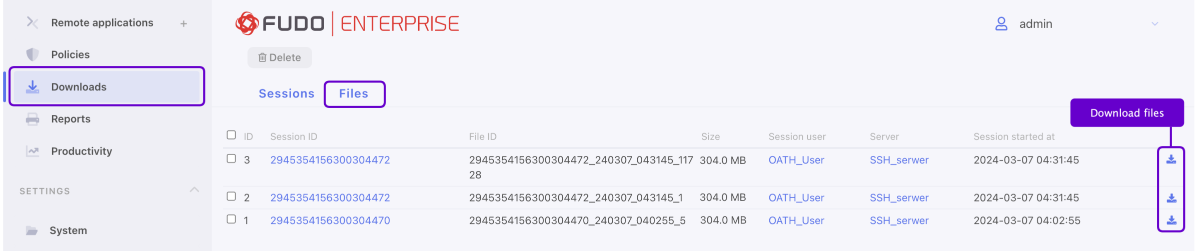
Handle 1

Offset 32768

Length 32768

Data

4. Select *Management* > *Downloads*.
5. Go to the **Files** tab.
6. Click the *Download* icon to download encoded file.



☐ ID	Session ID	File ID	Size	Session user	Server	Session started at
☐ 3	2945354156300304472	2945354156300304472_240307_043145_11728	304.0 MB	OATH_User	SSH_serwer	2024-03-07 04:31:45
☐ 2	2945354156300304472	2945354156300304472_240307_043145_1	304.0 MB	OATH_User	SSH_serwer	2024-03-07 04:31:45
☐ 1	2945354156300304470	2945354156300304470_240307_040255_5	304.0 MB	OATH_User	SSH_serwer	2024-03-07 04:02:55

Related topics:

- *Exporting sessions*
- *Sessions*

CHAPTER 17

Account activity in the Access Gateway

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

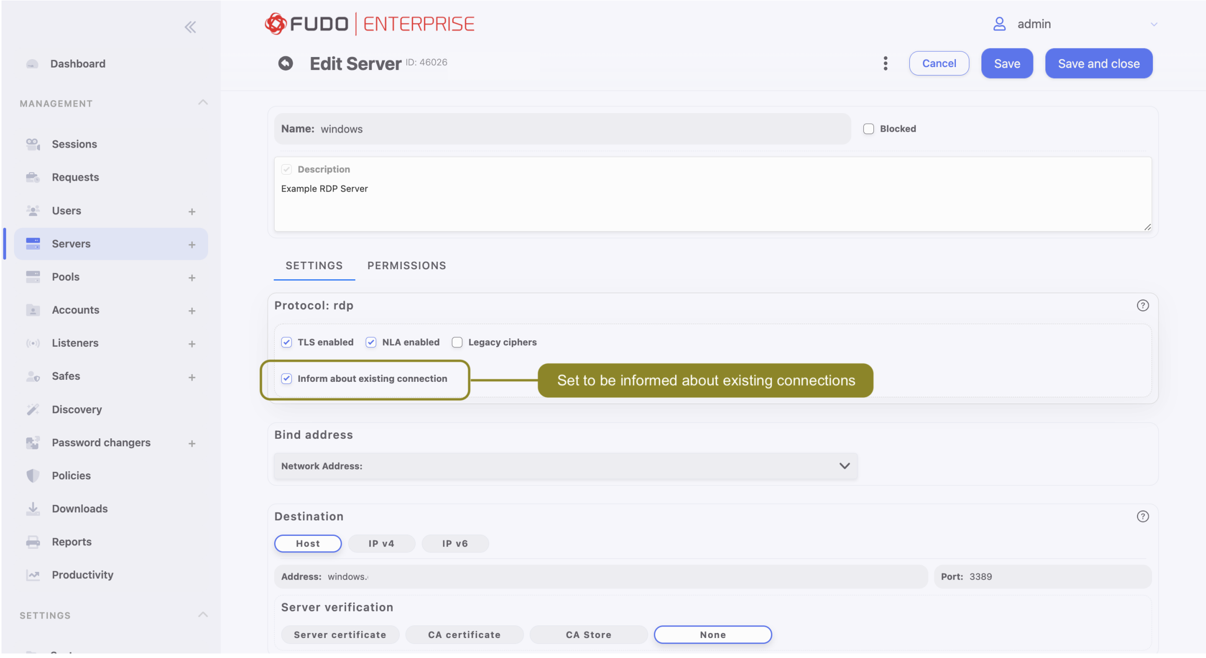
The **Resource in use** feature works while establishing connection to the target server, to which another user is already connected via the same account. If the user continues establishing connection, the session is terminated.

> **Warning:** This option is available for RDP connections only.

In order enable the *Resource in use* option for the RDP connections, follow the instruction:

1. Select *Management > Servers.*

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



Edit Server ID: 46026

Name: windows □ Blocked

Description
Example RDP Server

Protocol: rdp

☑ TLS enabled ☑ NLA enabled □ Legacy ciphers

☑ Inform about existing connection

Set to be informed about existing connections

Bind address

Network Address:

Destination

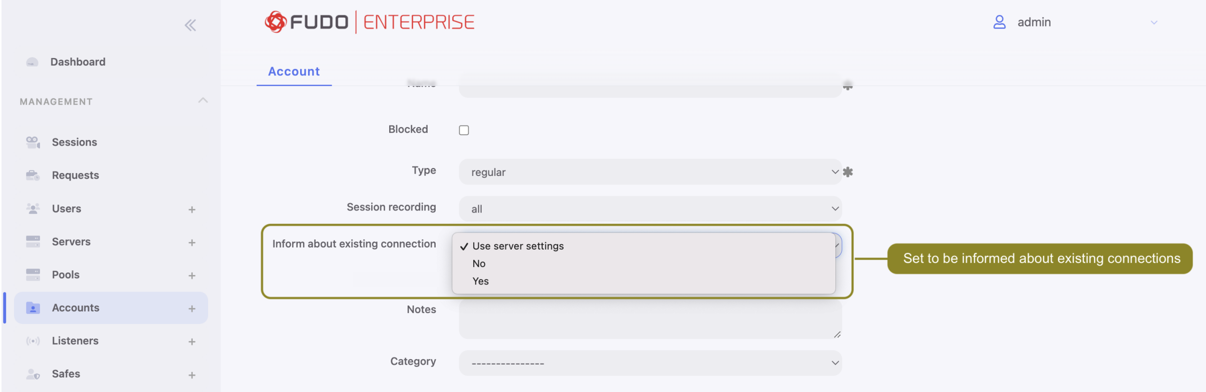
Address: windows. Port: 3389

Server verification

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

2. Select *Management* > *Accounts*.

- Define filters to limit the number of objects displayed on the list, or select an account with access to an RDP server that needs to be edited right from the list.
- In the *Inform about existing connection* field select:
  - `Use server settings` to inherit the settings of the server, which was added to the account in the *Server* section,
  - `Yes` to enable functionality (independently from the server settings),
  - `No` to disable functionality.



Blocked □

Type regular

Session recording all

Inform about existing connection ✓ Use server settings
No
Yes

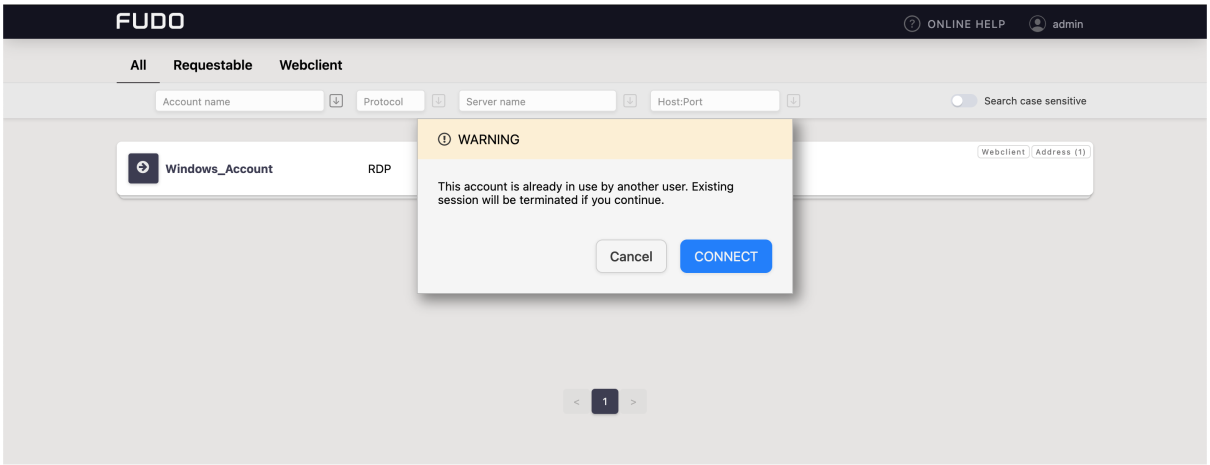
Set to be informed about existing connections

Notes

Category ---------------

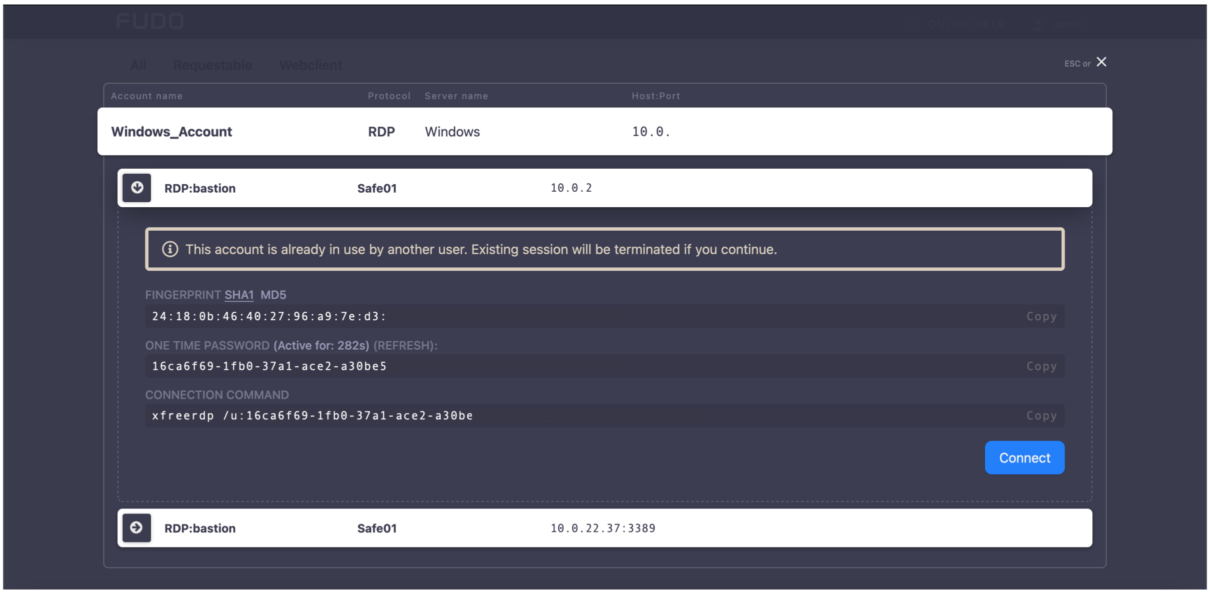
- Click *Save*.

Information about existing connection will be presented to the user in the Access Gateway. Here is the default message:



WARNING

This account is already in use by another user. Existing session will be terminated if you continue.



This account is already in use by another user. Existing session will be terminated if you continue.

FINGERPRINT SHA1 MD5

```
24:18:0b:46:40:27:96:a9:7e:d3:
```

ONE TIME PASSWORD (Active for: 282s) (REFRESH):

```
16ca6f69-1fb0-37a1-ace2-a30be5
```

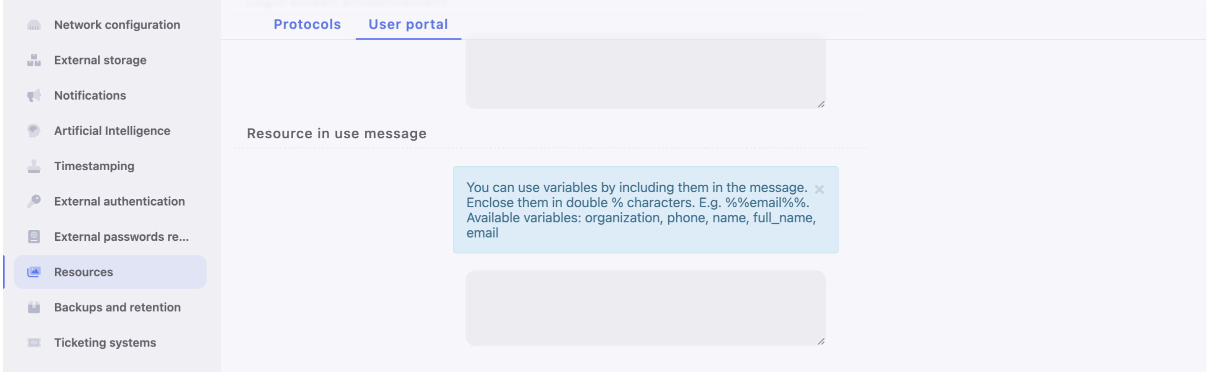
CONNECTION COMMAND

```
xfreerdp /u:16ca6f69-1fb0-37a1-ace2-a30be
```

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

In order to do that:

1. Select *Settings* > *Resources* > *User portal* tab.
2. Provide a new message in the *Resource in use message* field.
3. Click *Save*.



Resource in use message

You can use variables by including them in the message. Enclose them in double % characters. E.g. %%email%%. Available variables: organization, phone, name, full_name, email

Related Topics:

- *Creating an RDP server*
- *User portal login screen configuration*

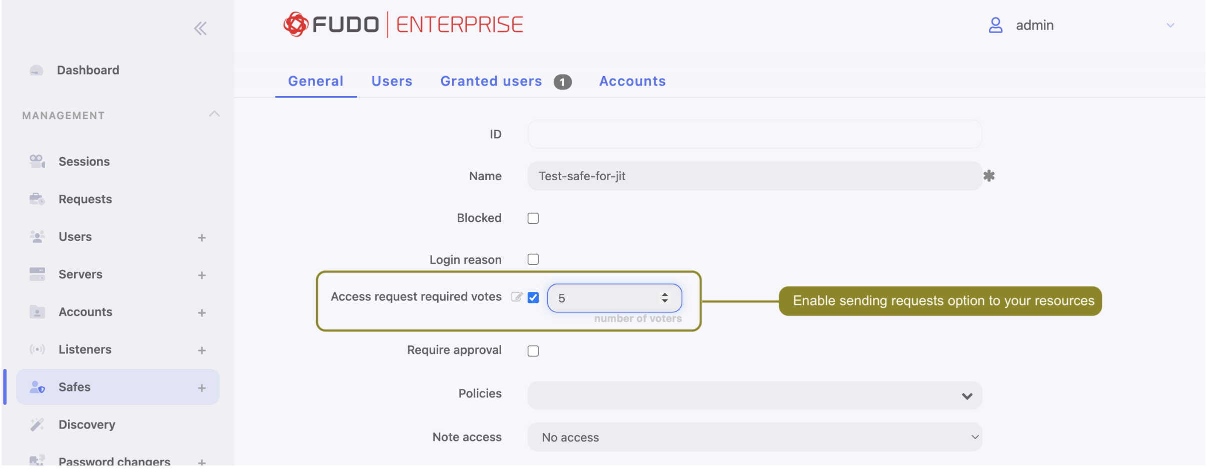
CHAPTER 18

Access requests

Granting access to the resources via the request is a basis of the Just In Time feature. A user requests for access via the Access Gateway, and authorized administrators vote for the request's approval or rejection on Admin Panel.

In order to set the voting process for access to your resources, follow the procedure:

1. Select *Management* > *Safes* tab.
2. Select the safe from the list, or create a new one.
3. Check the *Access request required votes* option. Provide a number of the voters that will be deciding about each request to the safe resources.



ID

Name: Test-safe-for-jit

Blocked □

Login reason □

Access request required votes ☑ 5 (number of voters)

Require approval □

Policies

Note access: No access

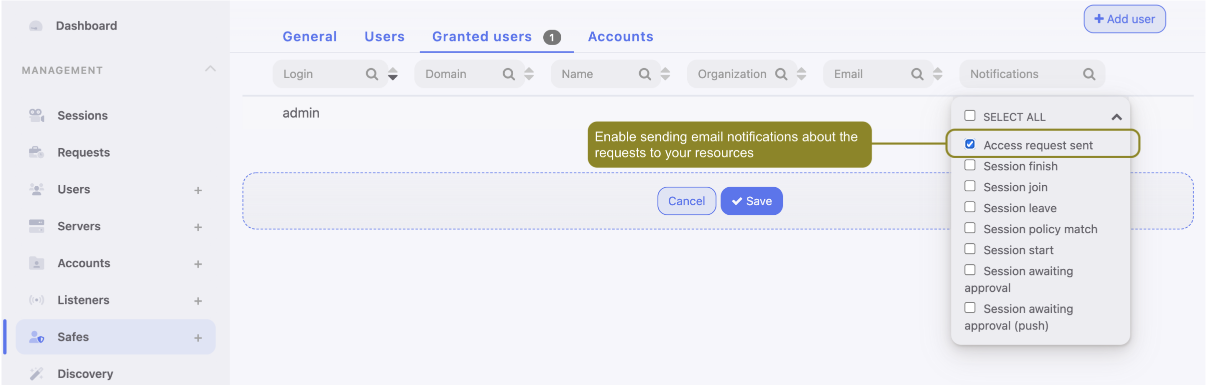
Enable sending requests option to your resources

Note:

- Users with *Admin* role and users added as the *Granted Users* to the Safe are allowed to be the voters.
- A user, who sent an access request isn't allowed to vote for access on their own request. Therefore, their own requests aren't visible for them.

- Having more than one voter sets a request to be accepted by more than 1 authorized person. If one of the voters votes for rejection, the system automatically rejects the request.

4. Go to the **Granted users** tab and for the particular user select the *Access request sent* type of notification.



Enable sending email notifications about the requests to your resources

Note: Notifications are set per node, according to the settings in the *Notifications* tab. In case of the *Access request sent* type, notifications are sent from the node, on which the request was created. More on this subject is at the *Notifications* page.

5. Click *Save*.

All the requests are available in the *Management* section on the *Requests* tab.

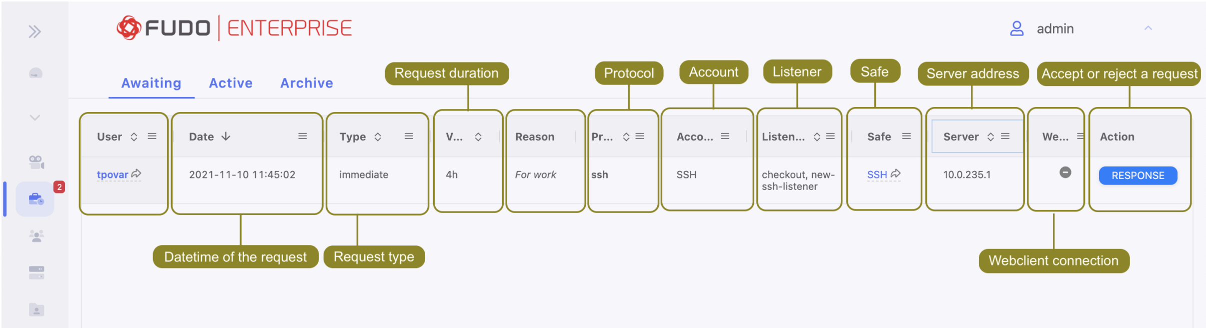
18.1 Awaiting requests

The *Awaiting* tab shows a detailed list of the requests that are waiting for a decision of the currently logged in user. Two types of requests are available for the user who sends an access request: *immediate* and *scheduled*.

Immediate requests can be set from now up to the next 24 hours.

When a user sends an immediate request, its access time starts when the request is accepted. Then, the user has 24 hours to start their session. When the user starts the session, the system counts the session time, which the user had requested, and terminates connection when the requested session time is over. If the user does not use the access and does not connect for 24 hours after access is granted, the access becomes expired.

For the *scheduled* type of requests, the user chooses a time period in the future, including exact time and date.



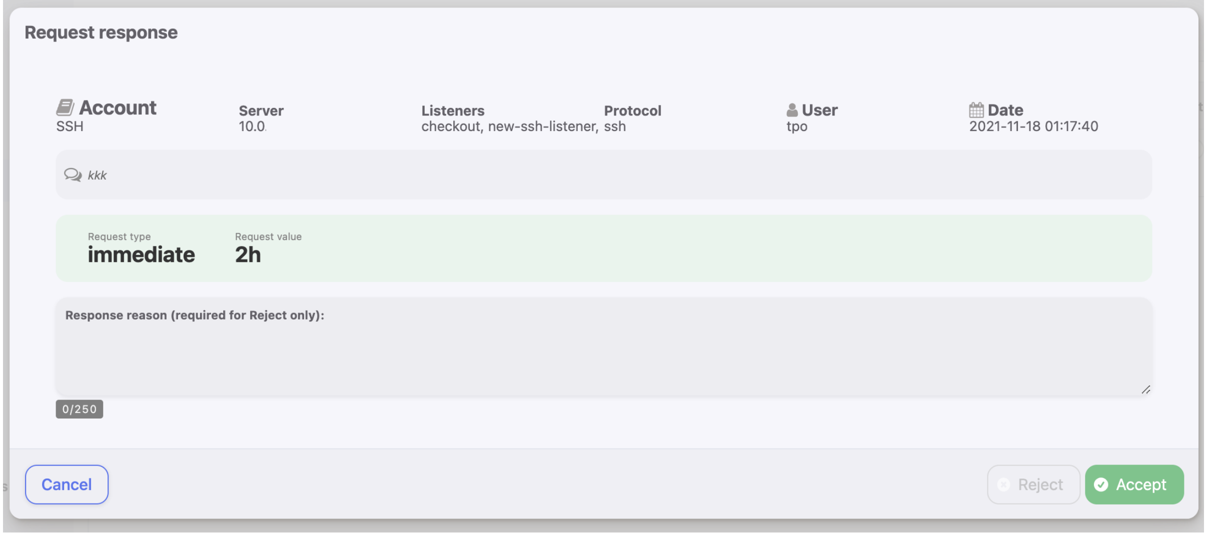
User	Date	Type	V...	Reason	Pr...	Acco...	Listen...	Safe	Server	We...	Action
tpovar	2021-11-10 11:45:02	immediate	4h	For work	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.235.1	●	RESPONSE

Sending response to the request

In order to vote for approval or rejection of the request, follow the steps:

1. Select *Management* > *Requests* tab.
2. In the *Awaiting* tab select the request to be processed and click the *Response* button .
3. In the modal click the *Accept* or the *Reject* button.

Note: The Response reason field is required to activate the rejecting option.


Request response

Account	Server	Listeners	Protocol	User	Date
SSH	10.0.	checkout, new-ssh-listener, ssh		tpo	2021-11-18 01:17:40

kkk

Request type: immediate

Request value: 2h

Response reason (required for Reject only):

0/250

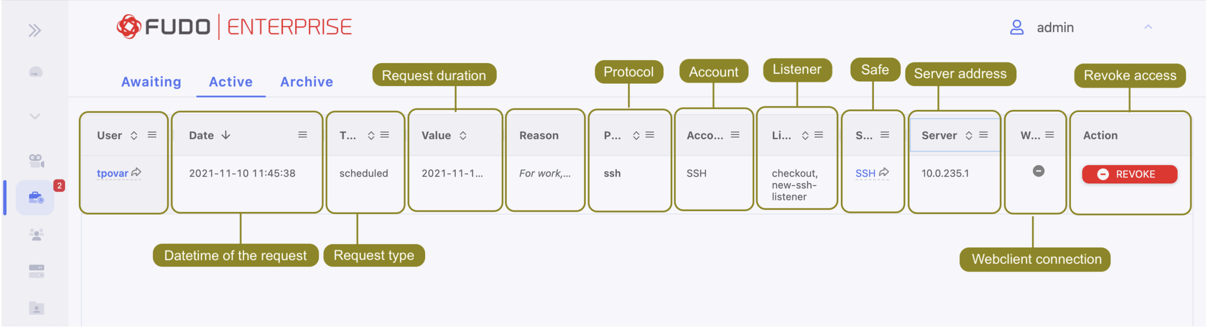
Note:

- Users who sent the request via the Access Gateway and have their e-mail address configured on the Admin Panel, receive notifications when their request was accepted or rejected.
- If a user is trying to connect to a server (for example, based on the SSH protocol) via the *native client* option, but hasn't sent an access request, a respective message about authentication error is recorded into the Event logs: `Unable to authenticate user: safe requires acceptance`.

18.2 Active requests

The Active tab shows a list of two types of the requests: 1) requests that were accepted, and their sessions are currently ongoing, and 2) requests that are waiting for the part of the voters. The Votes column of the requests list shows a number of voters that the particular request needs to be processed. Hover on its value to see the details of who had voted.

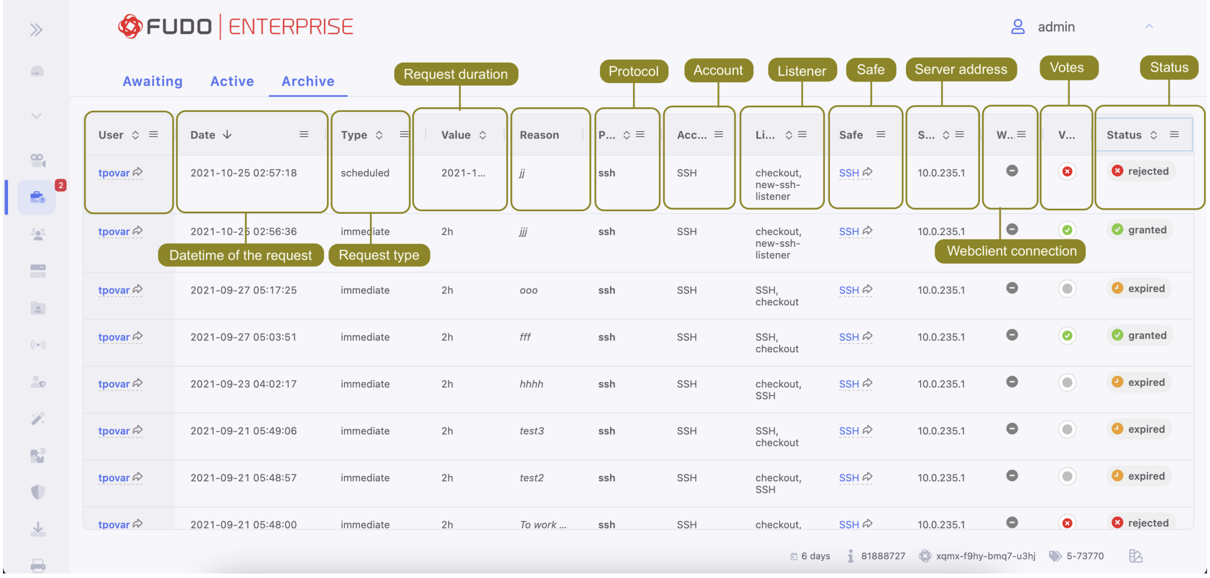
Given vote for accepted and active requests can be revoked, for example, for preventing a possible misuse. This option is useful when the user finished their work earlier than expected, but their request is still valid.



User	Date	T...	Value	Reason	P...	Acco...	Li...	S...	Server	W...	Action
tpovar	2021-11-10 11:45:38	scheduled	2021-11-1...	*For work,...*	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.235.1	⊖	REVOKE

18.3 Archived requests

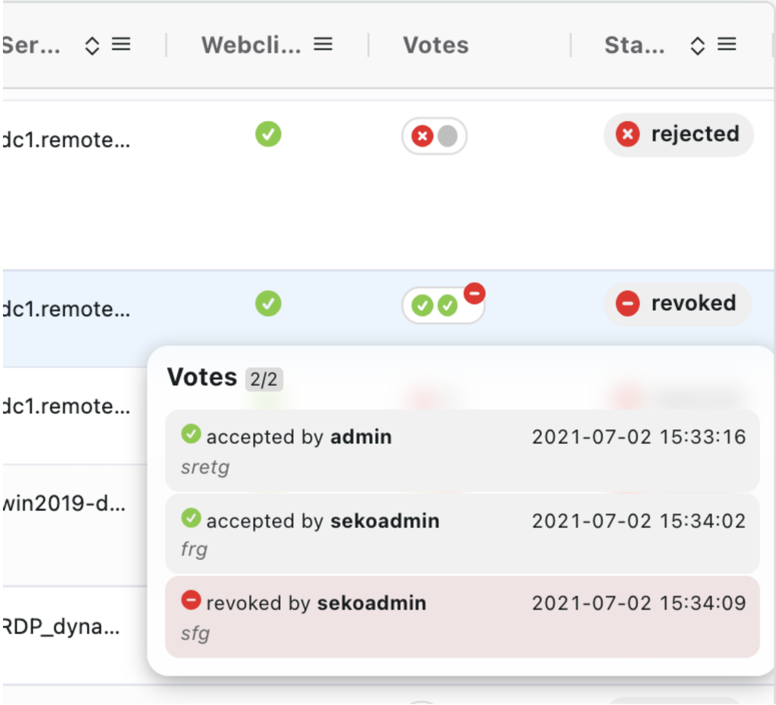
History of the processed requests is available under the *Archive* tab.



User	Date	Type	Value	Reason	P...	Acc...	Li...	Safe	S...	W...	V...	Status
tpovar	2021-10-25 02:57:18	scheduled	2021-1...	*jj*	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.235.1	⊖	✗	✗ rejected
tpovar	2021-10-25 02:56:36	immediate	2h	*jjj*	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.235.1	⊖	✓	✓ granted
tpovar	2021-09-27 05:17:25	immediate	2h	*ooo*	ssh	SSH	SSH, checkout	SSH	10.0.235.1	⊖	○	expired
tpovar	2021-09-27 05:03:51	immediate	2h	*fff*	ssh	SSH	SSH, checkout	SSH	10.0.235.1	⊖	✓	✓ granted
tpovar	2021-09-23 04:02:17	immediate	2h	*hhhh*	ssh	SSH	checkout, SSH	SSH	10.0.235.1	⊖	○	expired
tpovar	2021-09-21 05:49:06	immediate	2h	*test3*	ssh	SSH	SSH, checkout	SSH	10.0.235.1	⊖	○	expired
tpovar	2021-09-21 05:48:57	immediate	2h	*test2*	ssh	SSH	checkout, SSH	SSH	10.0.235.1	⊖	○	expired
tpovar	2021-09-21 05:48:00	immediate	2h	*To work ...*	ssh	SSH	checkout,	SSH	10.0.235.1	⊖	✗	✗ rejected

6 days 81888727 xqmx-f9hy-bmq7-u3hj 5-73770

The Votes column of the requests list shows a number of voters that the particular request needed to be processed. Hover on its value to see the details of who voted.



Ser...	Webcli...	Votes	Sta...
dc1.remote...	✓	✗ ●	✗ rejected
dc1.remote...	✓	✓ ✓ ⊖	⊖ revoked
dc1.remote...			
win2019-d...			
RDP_dyna...			

Votes 2/2

✓ accepted by **admin** 2021-07-02 15:33:16
sretg

✓ accepted by **sekoadmin** 2021-07-02 15:34:02
frg

⊖ revoked by **sekoadmin** 2021-07-02 15:34:09
sfg

The Just in Time feature also works when there are Fudo instances connected in the cluster. Votes and requests are replicated on nodes in the cluster.

Note: If the admin voted on more than one machine in the cluster and his decisions were contradictory, it will be treated as a single rejecting vote and the accepting vote will be revoked.

Related topics:

- *Creating a new safe*

CHAPTER 19

Sessions

Fudo Enterprise stores all recorded servers access sessions, allowing to playback, review, delete and export to the supported video formats.

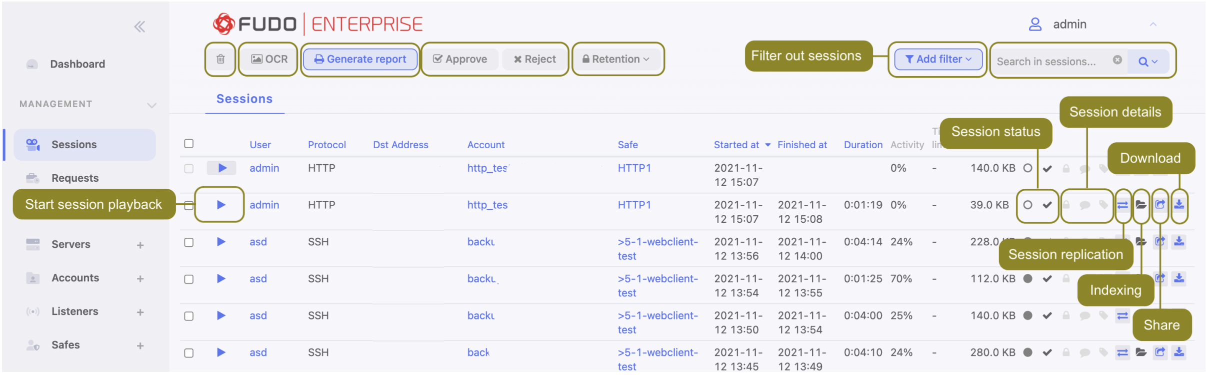
Sessions management page allows filtering stored user sessions, accessing current users connections and downloading stored sessions. It also provides status information on each session and enables access to session sharing options.

Note: Contents of the session list depend on the logged in user's access rights. Being able to access a given session requires having management privileges to: server, account, user and safe objects that were used in the given connection.

Icon	Description
▶	Start session playback (*applicable to sessions with the entire traffic recording option selected in connection properties*).
🕘	Icon indicating that session has been timestamped.
💬	Purpose why the user has connected to the server.
🏷	Session has been commented.
📂	Session has been processed for full-text search purposes.
⇄	Session replication status.
↗	Access session sharing management options.
⬇	Download session material in selected file format (*applicable to sessions with either complete or raw traffic recording option selected in connection properties*).
📶	User activity monitor (*applicable to live sessions*).
👤	Username of the user for whom approved pending session.
✔	Approve pending request.
✖	Decline pending request.
?	Pending request awaiting authorization.
+	Element aggregating connections established within the same session.
🔒	Session excluded from the retention mechanism.
⚗	Behavioral analysis status. *This is an evaluation version of the AI component.* ○ - session under analysis, initial result - no threat. ○ - session under analysis, initial result - medium threat level. ○ - session under analysis, initial result - high threat level. ○ - session awaiting analysis or being initially processed. ○ - session not analyzed due to missing a trained model. 🟢 - session processed - no risk. 🟡 - session processed - medium threat level. 🔴 - session processed - high threat level. ● - session processed - no result.

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

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



	User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Ti lin	
□ ▶	admin	HTTP		http_tes	HTTP1	2021-11-12 15:07			0%	-	140.0 KB ○ ✔
□ ▶	admin	HTTP		http_tes	HTTP1	2021-11-12 15:07	2021-11-12 15:08	0:01:19	0%	-	39.0 KB ○ ✔ ⇄ 📂 ↗ ⬇
□ ▶	asd	SSH		backu	>5-1-webclient-test	2021-11-12 13:56	2021-11-12 14:00	0:04:14	24%	-	228.0 📂 ↗ ⬇
□ ▶	asd	SSH		backu	>5-1-webclient-test	2021-11-12 13:54	2021-11-12 13:55	0:01:25	70%	-	112.0 KB ● ✔ ↗ ⬇
□ ▶	asd	SSH		backu	>5-1-webclient-test	2021-11-12 13:50	2021-11-12 13:54	0:04:00	25%	-	140.0 KB ● ✔ ⇄
□ ▶	asd	SSH		back	>5-1-webclient-test	2021-11-12 13:45	2021-11-12 13:49	0:04:10	24%	-	280.0 KB ● ✔ ⇄ 📂 ↗ ⬇

Start session playback

Filter out sessions

Session status

Session details

Download

Session replication

Indexing

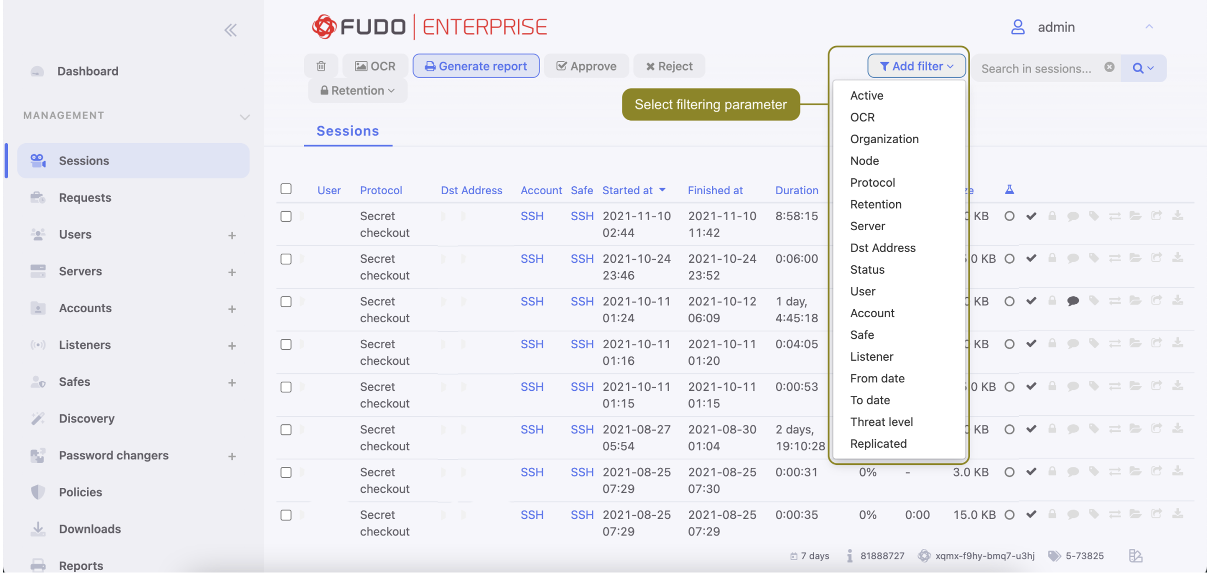
Share

19.1 Filtering sessions

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

19.1.1 Defining filters

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

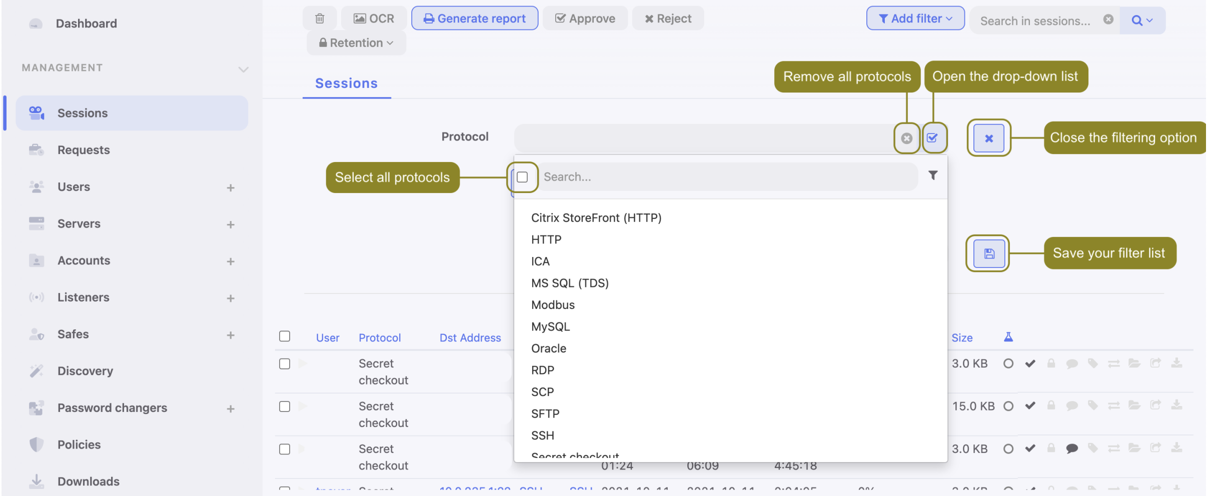


Select filtering parameter

User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration			Size
	Secret checkout		SSH	SSH	2021-11-10 02:44	2021-11-10 11:42	8:58:15			KB
	Secret checkout		SSH	SSH	2021-10-24 23:46	2021-10-24 23:52	0:06:00			0 KB
	Secret checkout		SSH	SSH	2021-10-11 01:24	2021-10-12 06:09	1 day, 4:45:18			KB
	Secret checkout		SSH	SSH	2021-10-11 01:16	2021-10-11 01:20	0:04:05			KB
	Secret checkout		SSH	SSH	2021-10-11 01:15	2021-10-11 01:15	0:00:53			0 KB
	Secret checkout		SSH	SSH	2021-08-27 05:54	2021-08-30 01:04	2 days, 19:10:28			KB
	Secret checkout		SSH	SSH	2021-08-25 07:29	2021-08-25 07:30	0:00:31	0%	-	3.0 KB
	Secret checkout		SSH	SSH	2021-08-25 07:29	2021-08-25 07:29	0:00:35	0%	0:00	15.0 KB

7 days 81888727 xqmx-f9hy-bmq7-u3hj 5-73825

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



Remove all protocols

Open the drop-down list

Close the filtering option

Select all protocols

Save your filter list

User	Protocol	Dst Address		Size
	Secret checkout			3.0 KB
	Secret checkout			15.0 KB
	Secret checkout		01:24 06:09 4:45:18	3.0 KB

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

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

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

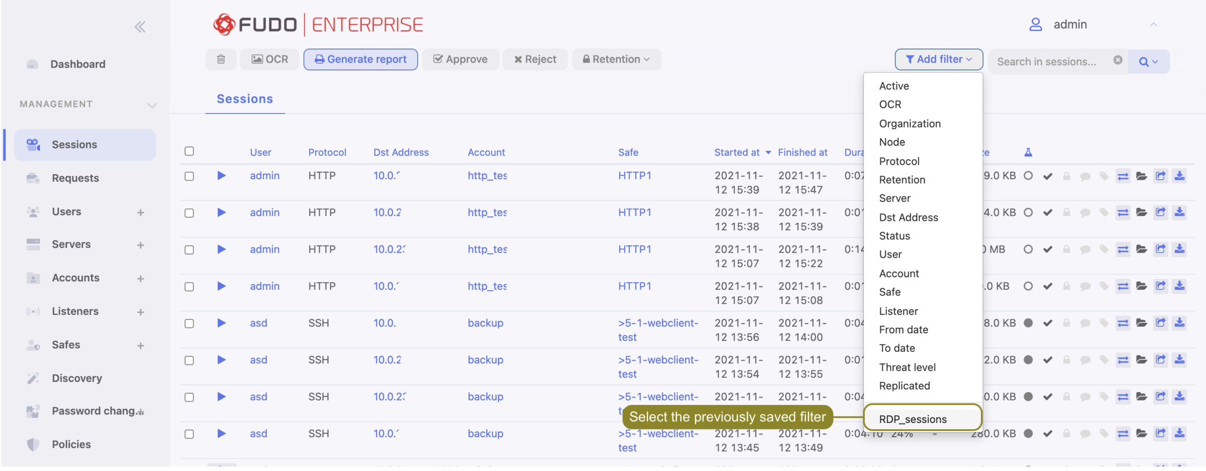
Note: Only sessions which match all defined filtering parameters will be displayed.

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

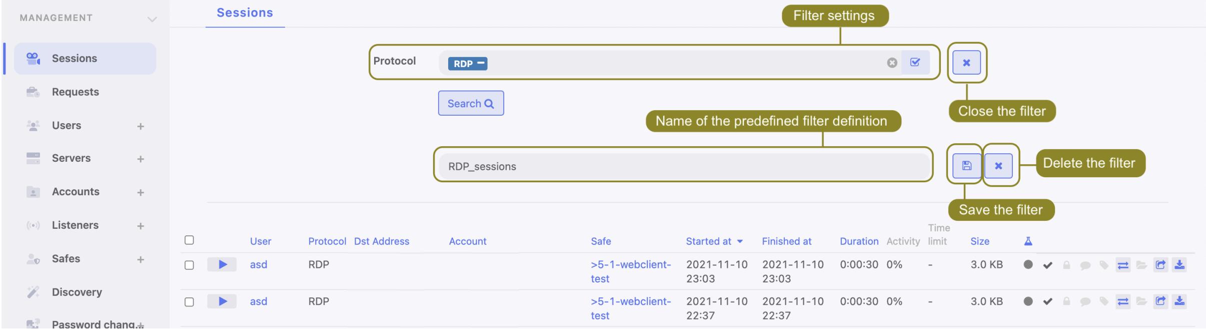
19.1.2 Managing user defined filter definitions

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

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



User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Dura	ze
admin	HTTP	10.0.‘	http_tes	HTTP1	2021-11-12 15:39	2021-11-12 15:47	0:07	9.0 KB
admin	HTTP	10.0.2	http_tes	HTTP1	2021-11-12 15:38	2021-11-12 15:39	0:01	4.0 KB
admin	HTTP	10.0.2:	http_tes	HTTP1	2021-11-12 15:07	2021-11-12 15:22	0:14	) MB
admin	HTTP	10.0.‘	http_tes	HTTP1	2021-11-12 15:07	2021-11-12 15:08	0:01	.0 KB
asd	SSH	10.0.	backup	>5-1-webclient-test	2021-11-12 13:56	2021-11-12 14:00	0:04	8.0 KB
asd	SSH	10.0.2	backup	>5-1-webclient-test	2021-11-12 13:54	2021-11-12 13:55	0:01	2.0 KB
asd	SSH	10.0.2:	backup	>5-1-webclient-t	2021-11-	2021-11-	0:04	0.0 KB
asd	SSH	10.0.‘	backup	>5-1-webclient-test	2021-11-12 13:45	2021-11-12 13:49	0:04:10 24% -	280.0 KB



User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
asd	RDP			>5-1-webclient-test	2021-11-10 23:03	2021-11-10 23:03	0:00:30	0%	-	3.0 KB
asd	RDP			>5-1-webclient-test	2021-11-10 22:37	2021-11-10 22:37	0:00:30	0%	-	3.0 KB

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

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

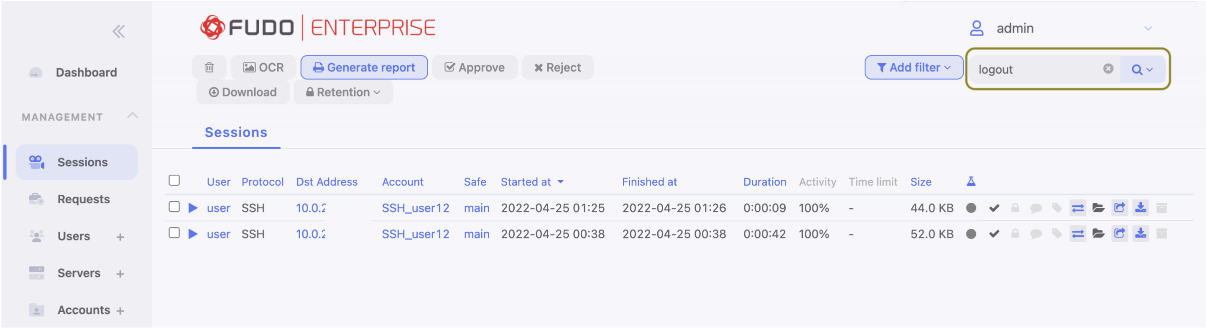
19.1.3 Full text search

Fudo Enterprise enables searching stored data to limit the number of elements on the sessions list only to those containing the specified phrase.

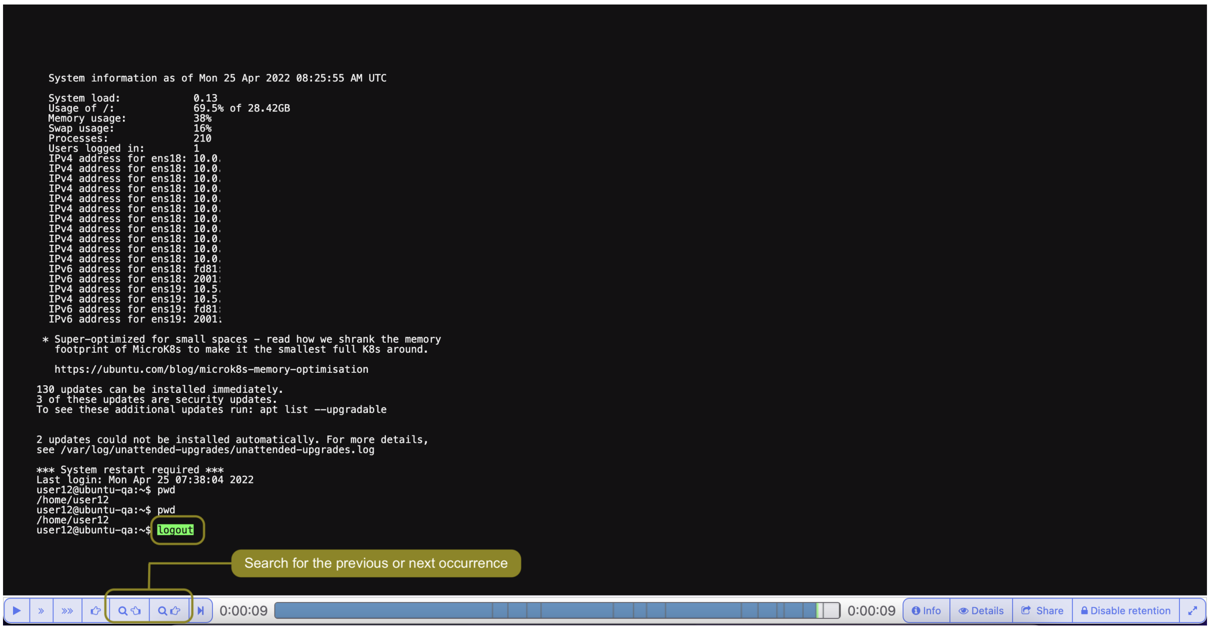
Note:

- Use the Sessions search bar to search for sessions containing specific phrases, e.g. “logout”.
- Playing a session containing the specified phrase starts from the moment of its first occurrence.

The player allows for skipping between each occurrence of the specified phrase.



☐	User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
☐	user	SSH	10.0.2	SSH_user12	main	2022-04-25 01:25	2022-04-25 01:26	0:00:09	100%	-	44.0 KB
☐	user	SSH	10.0.2	SSH_user12	main	2022-04-25 00:38	2022-04-25 00:38	0:00:42	100%	-	52.0 KB



```
  System information as of Mon 25 Apr 2022 08:25:55 AM UTC

  System load:            0.13
  Usage of /:             69.5% of 28.42GB
  Memory usage:           38%
  Swap usage:             16%
  Processes:              210
  Users logged in:        1
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv6 address for ens18: fd81:
  IPv6 address for ens18: 2001:
  IPv4 address for ens19: 10.5.
  IPv4 address for ens19: 10.5.
  IPv6 address for ens19: fd81:
  IPv6 address for ens19: 2001:

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

130 updates can be installed immediately.
3 of these updates are security updates.
To see these additional updates run: apt list --upgradable


2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Mon Apr 25 07:38:04 2022
user12@ubuntu-qa:~$ pwd
/home/user12
user12@ubuntu-qa:~$ pwd
/home/user12
user12@ubuntu-qa:~$ logout
```

Search for the previous or next occurrence

Related topics:

- *System overview*
- *Reports*

19.2 Viewing sessions

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

To view a session, proceed as follows.

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

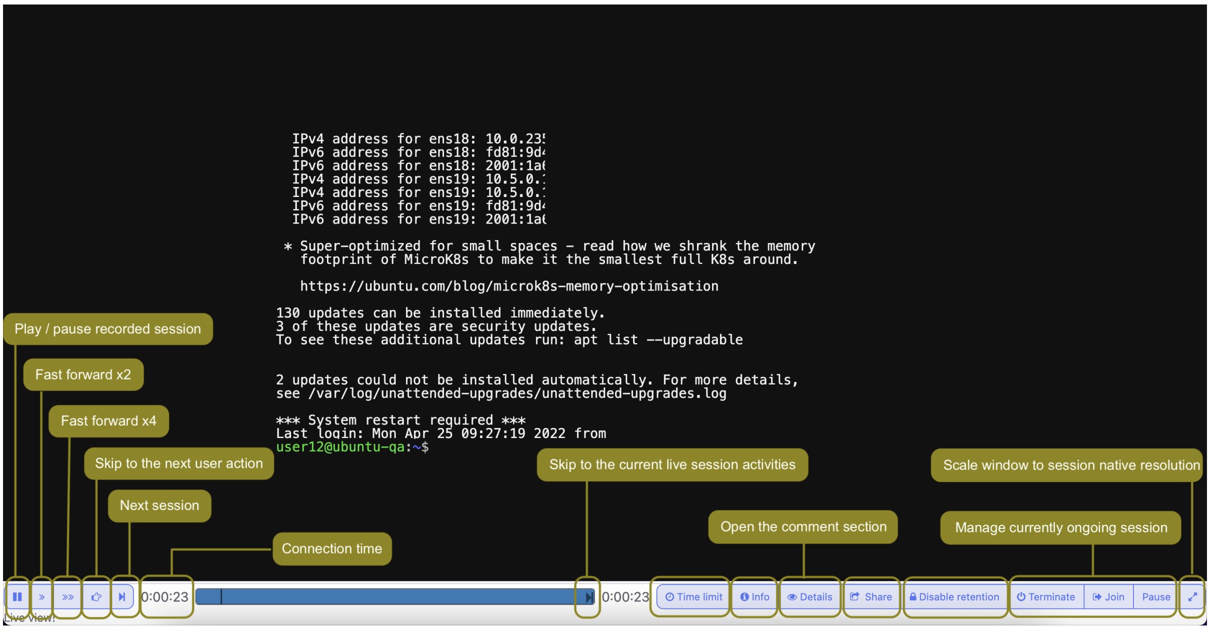
Note: Filter sessions to display only active connections:

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

Session player options

Note: Some options are available for live sessions only.

SSH, RDP, VNC, X11, Telnet

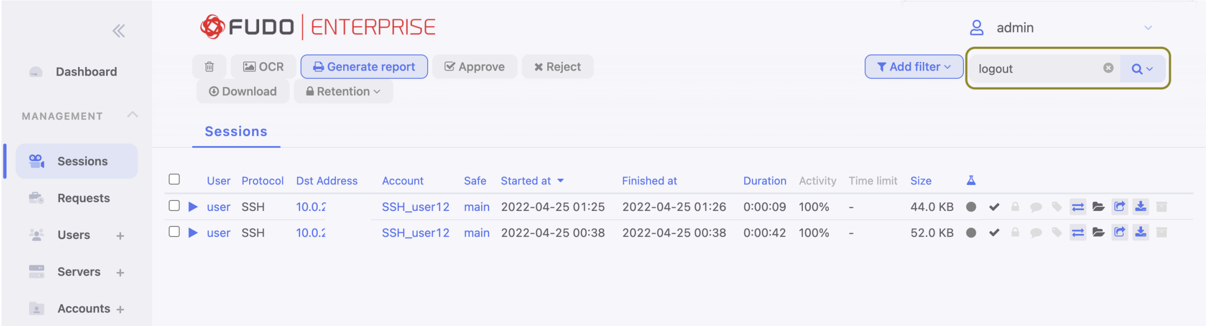


```
  IPv4 address for ens18: 10.0.23
  IPv6 address for ens18: fd81:9d
  IPv6 address for ens18: 2001:1a
  IPv4 address for ens19: 10.5.0.
  IPv4 address for ens19: 10.5.0.
  IPv6 address for ens19: fd81:9d
  IPv6 address for ens19: 2001:1a

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

130 updates can be installed immediately.
3 of these updates are security updates.
To see these additional updates run: apt list --upgradable


2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Mon Apr 25 09:27:19 2022 from
user12@ubuntu-qa:~$
```

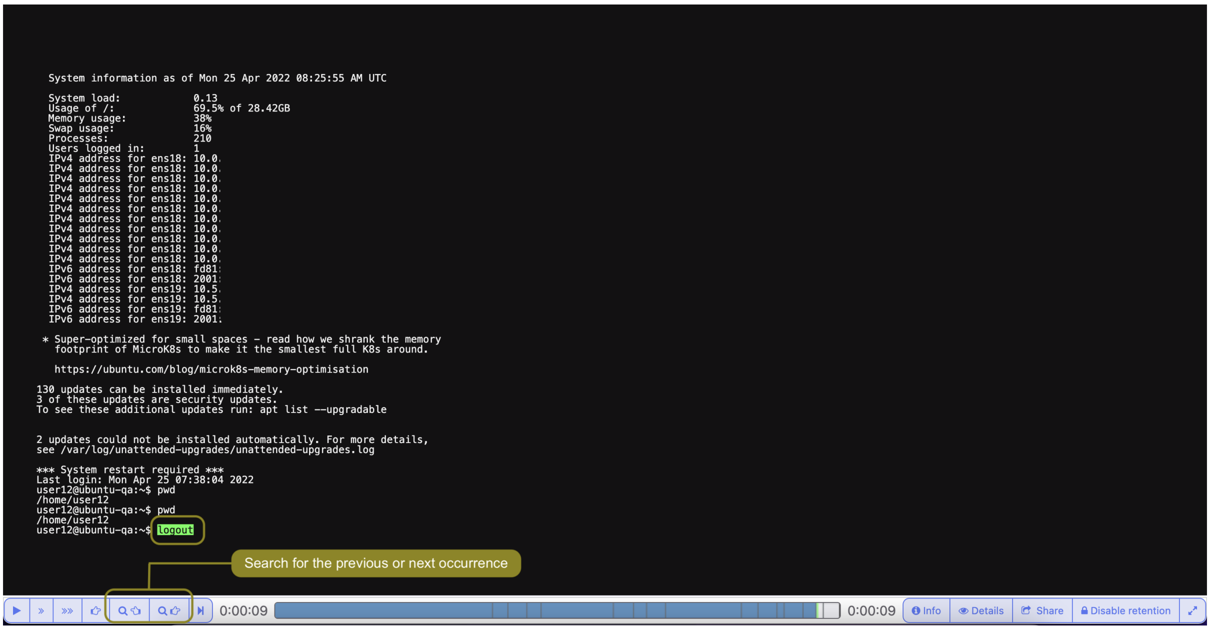
Play / pause recorded session
Fast forward x2
Fast forward x4
Skip to the next user action
Next session
Connection time
Skip to the current live session activities
Open the comment section
Scale window to session native resolution
Manage currently ongoing session
0:00:23
0:00:23
Time limit
Info
Details
Share
Disable retention
Terminate
Join
Pause
Live view!

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.



□	User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
□ ▶	user	SSH	10.0.2	SSH_user12	main	2022-04-25 01:25	2022-04-25 01:26	0:00:09	100%	-	44.0 KB
□ ▶	user	SSH	10.0.2	SSH_user12	main	2022-04-25 00:38	2022-04-25 00:38	0:00:42	100%	-	52.0 KB



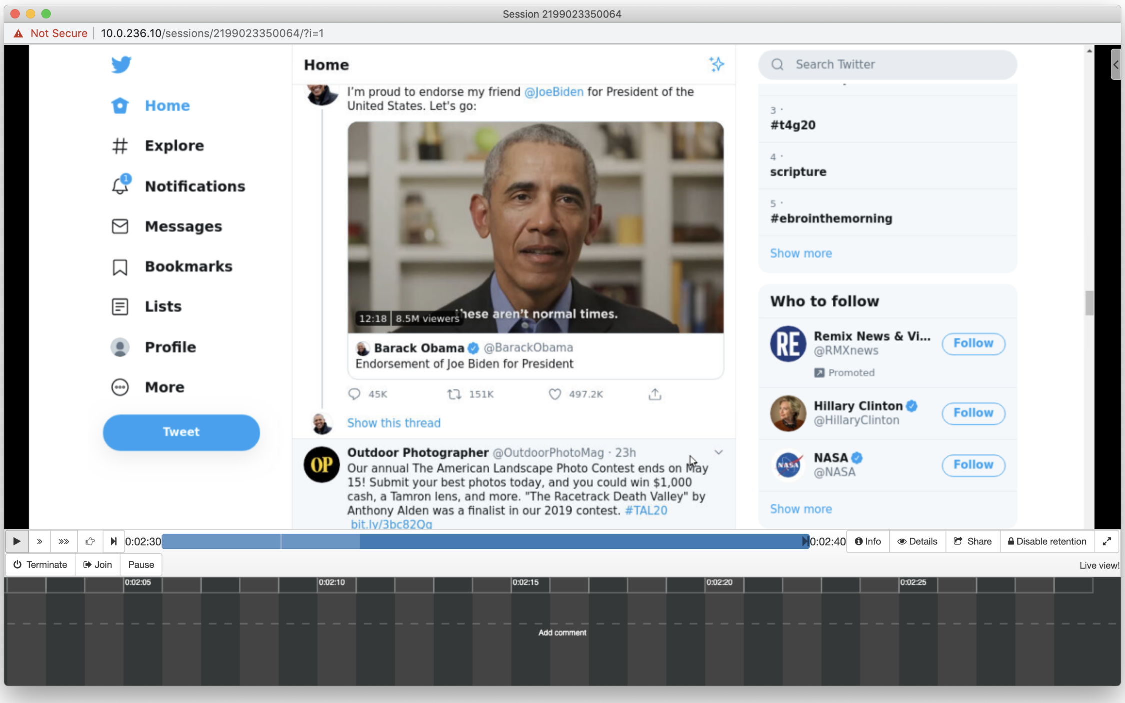
```
  System information as of Mon 25 Apr 2022 08:25:55 AM UTC

  System load:            0.13
  Usage of /:             69.5% of 28.42GB
  Memory usage:           38%
  Swap usage:             16%
  Processes:              210
  Users logged in:        1
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv4 address for ens18: 10.0.
  IPv6 address for ens18: fd81:
  IPv6 address for ens18: 2001:
  IPv4 address for ens19: 10.5.
  IPv4 address for ens19: 10.5.
  IPv6 address for ens19: fd81:
  IPv6 address for ens19: 2001:

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

130 updates can be installed immediately.
3 of these updates are security updates.
To see these additional updates run: apt list --upgradable


2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Mon Apr 25 07:38:04 2022
user12@ubuntu-qa:~$ pwd
/home/user12
user12@ubuntu-qa:~$ pwd
/home/user12
user12@ubuntu-qa:~$ logout
```

Search for the previous or next occurrence

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

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

HTTP - rendered



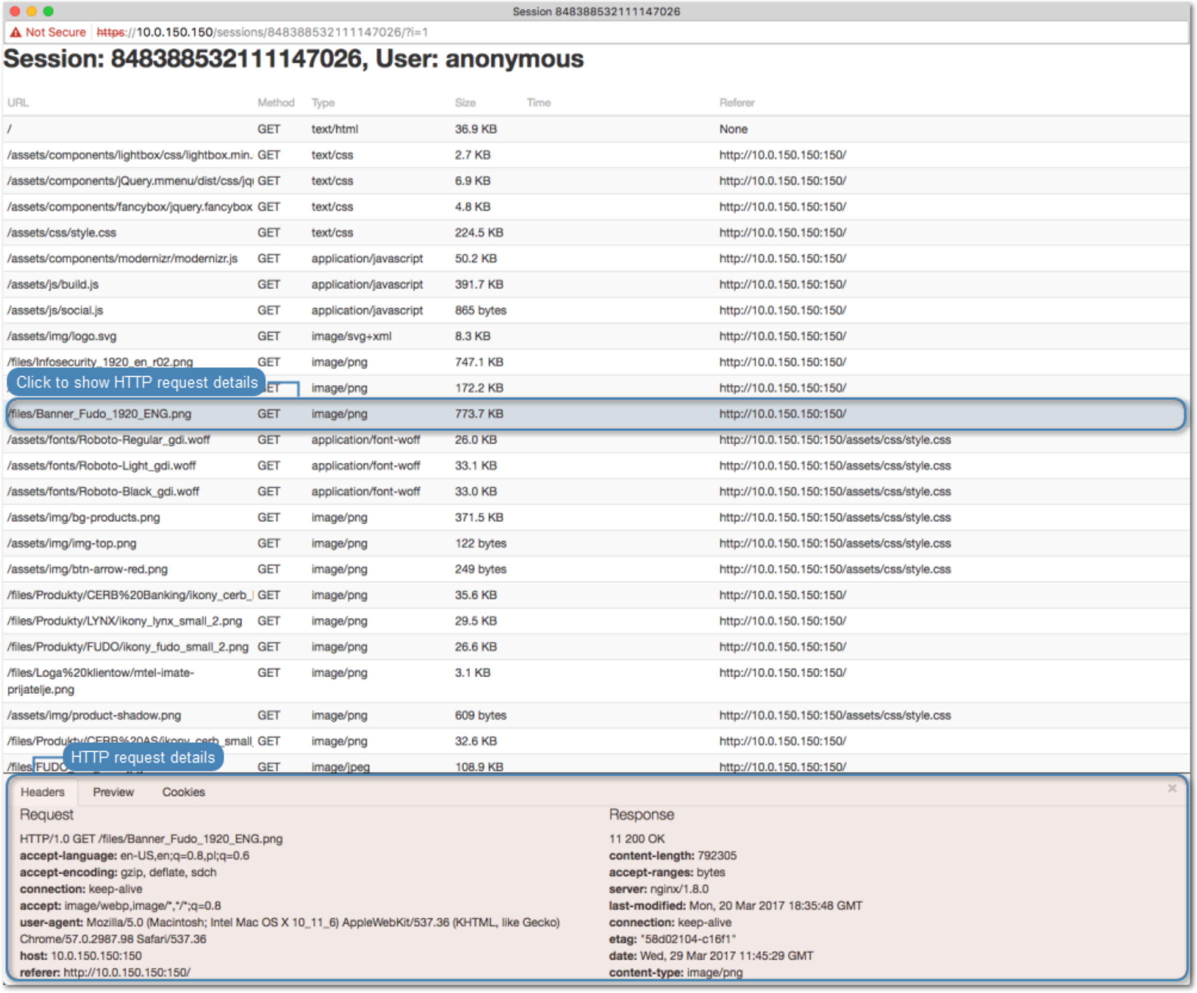
I'm proud to endorse my friend @JoeBiden for President of the United States. Let's go:

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/3bc82Oq

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

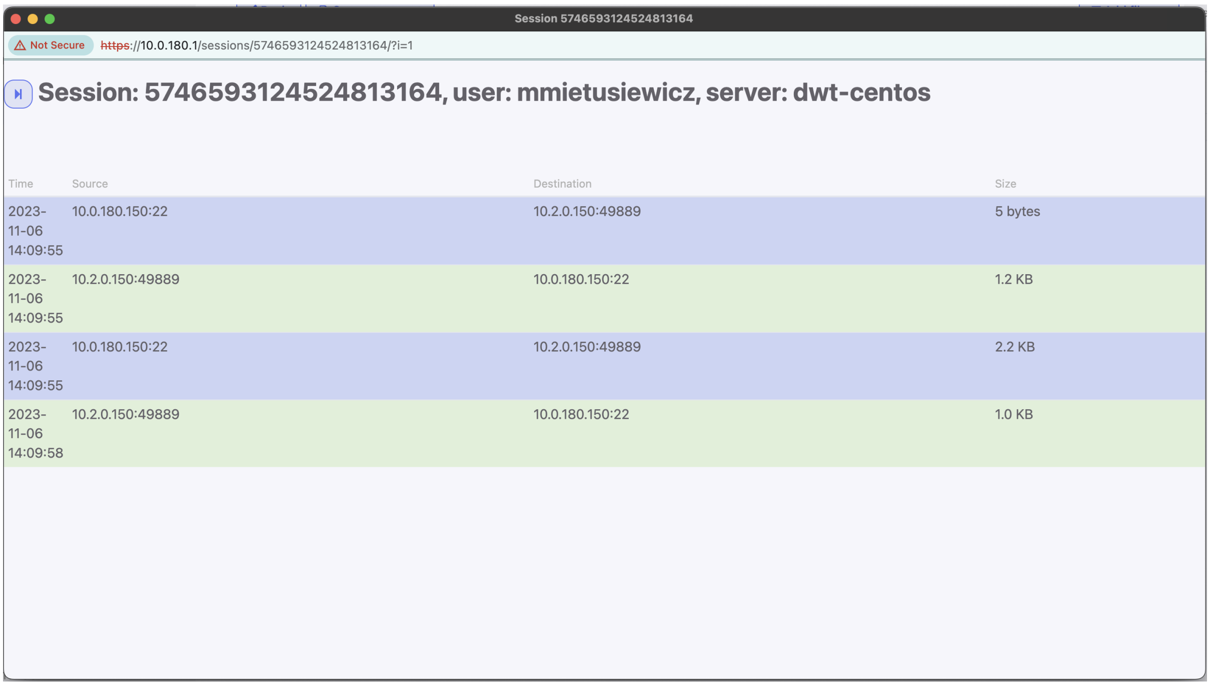
URL	Method	Type	Size	Time	Referer
/	GET	text/html	36.9 KB		None
/assets/components/lightbox/css/lightbox.min.	GET	text/css	2.7 KB		http://10.0.150.150:150/
/assets/components/jQuery.mmenu/dist/css/jq	GET	text/css	6.9 KB		http://10.0.150.150:150/
/assets/components/fancybox/jquery.fancybox	GET	text/css	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/
	ET	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/

Click to show HTTP request details

HTTP request details

Request	Response
HTTP/1.0 GET /files/Banner_Fudo_1920_ENG.png	11 200 OK
accept-language: en-US,en;q=0.8,pl;q=0.6	**content-length:** 792305
accept-encoding: gzip, deflate, sdch	**accept-ranges:** bytes
connection: keep-alive	**server:** nginx/1.8.0
accept: image/webp,image/*,*/*;q=0.8	**last-modified:** Mon, 20 Mar 2017 18:35:48 GMT
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	**connection:** keep-alive
	etag: "58d02104-c16f1"
host: 10.0.150.150:150	**date:** Wed, 29 Mar 2017 11:45:29 GMT
referer: http://10.0.150.150:150/	**content-type:** image/png

SSH



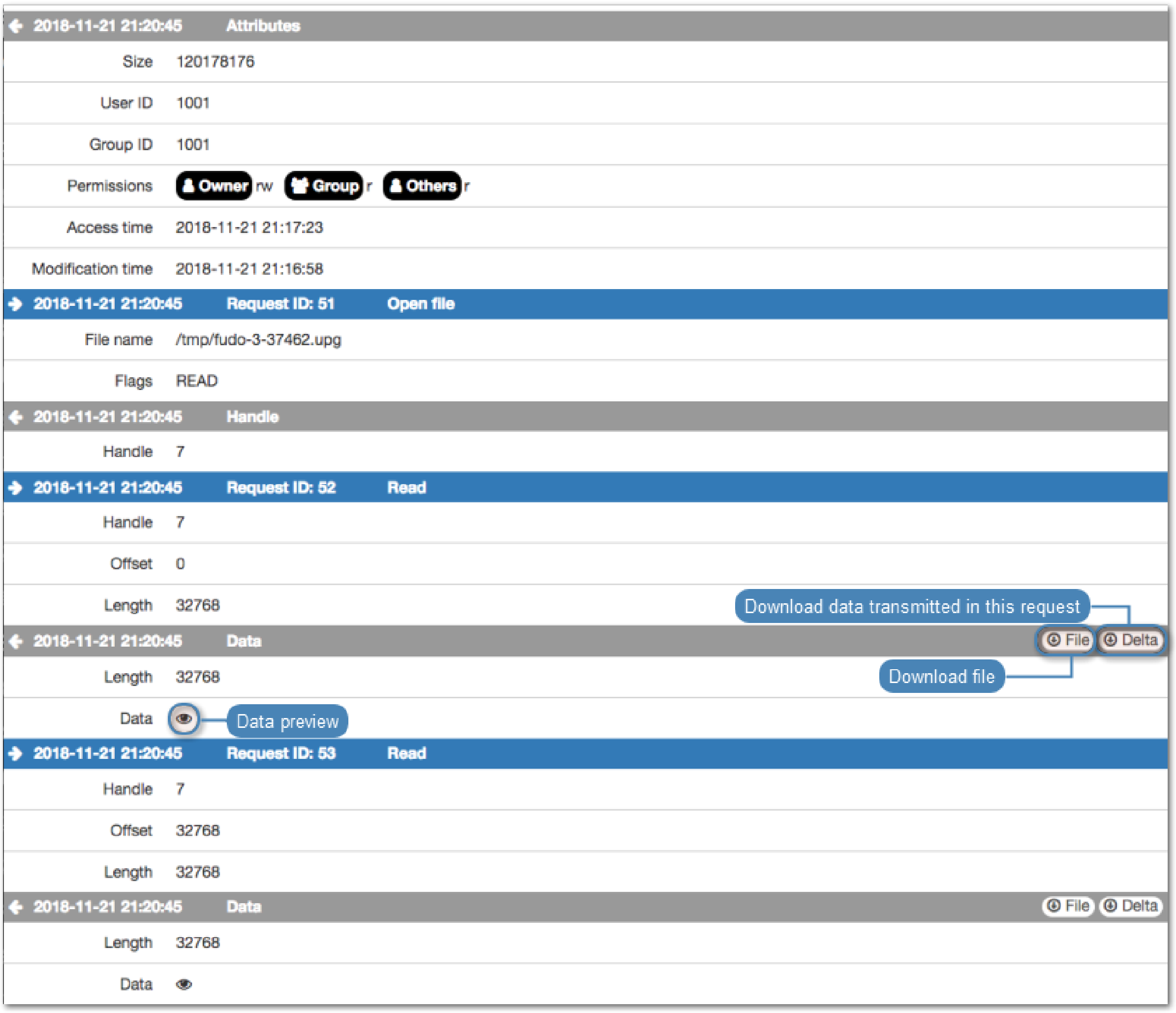
Session 5746593124524813164

⚠ Not Secure ~~https~~://10.0.180.1/sessions/5746593124524813164/?i=1

Session: 5746593124524813164, user: mmietusiewicz, server: dwt-centos

Time	Source	Destination	Size
2023-11-06 14:09:55	10.0.180.150:22	10.2.0.150:49889	5 bytes
2023-11-06 14:09:55	10.2.0.150:49889	10.0.180.150:22	1.2 KB
2023-11-06 14:09:55	10.0.180.150:22	10.2.0.150:49889	2.2 KB
2023-11-06 14:09:58	10.2.0.150:49889	10.0.180.150:22	1.0 KB

SFTP



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

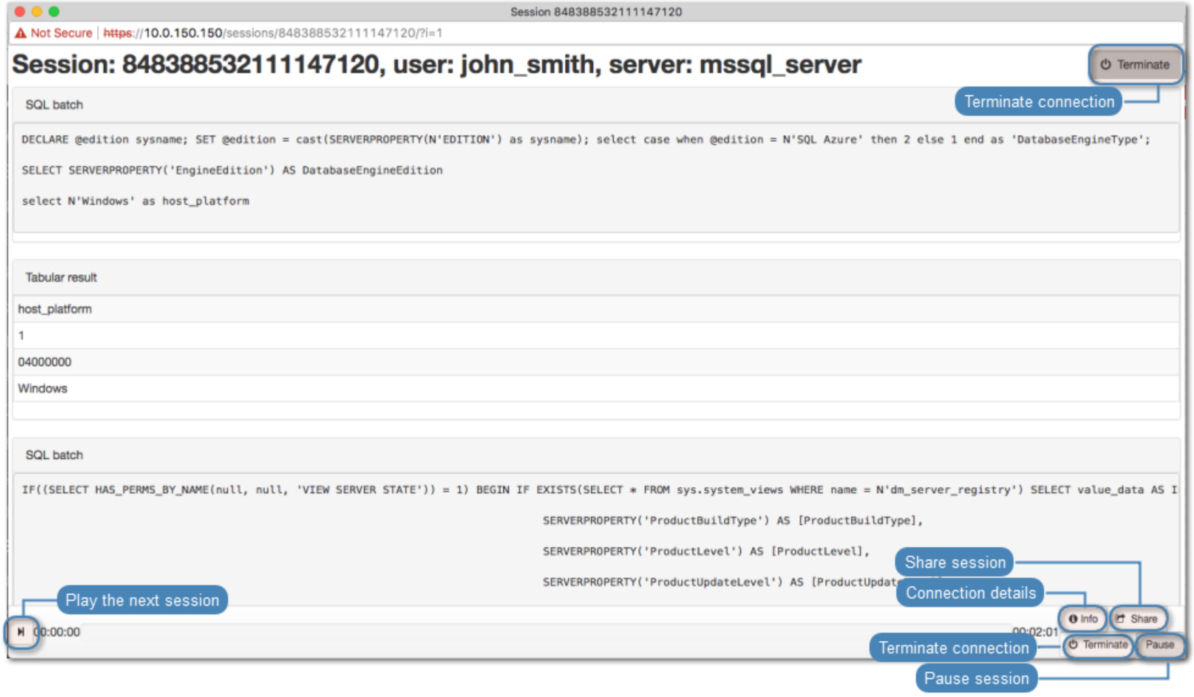
Length 32768

2018-11-21 21:20:45 Data

Length 32768

Data

MySQL, MSSQL



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

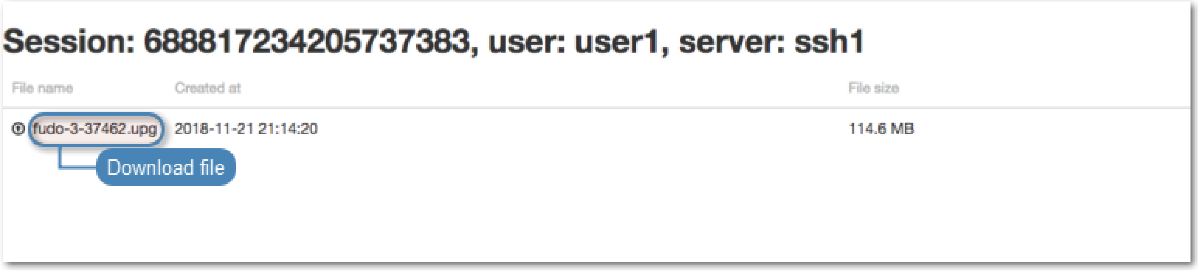
Windows

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: 6888172342057373 83, 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:

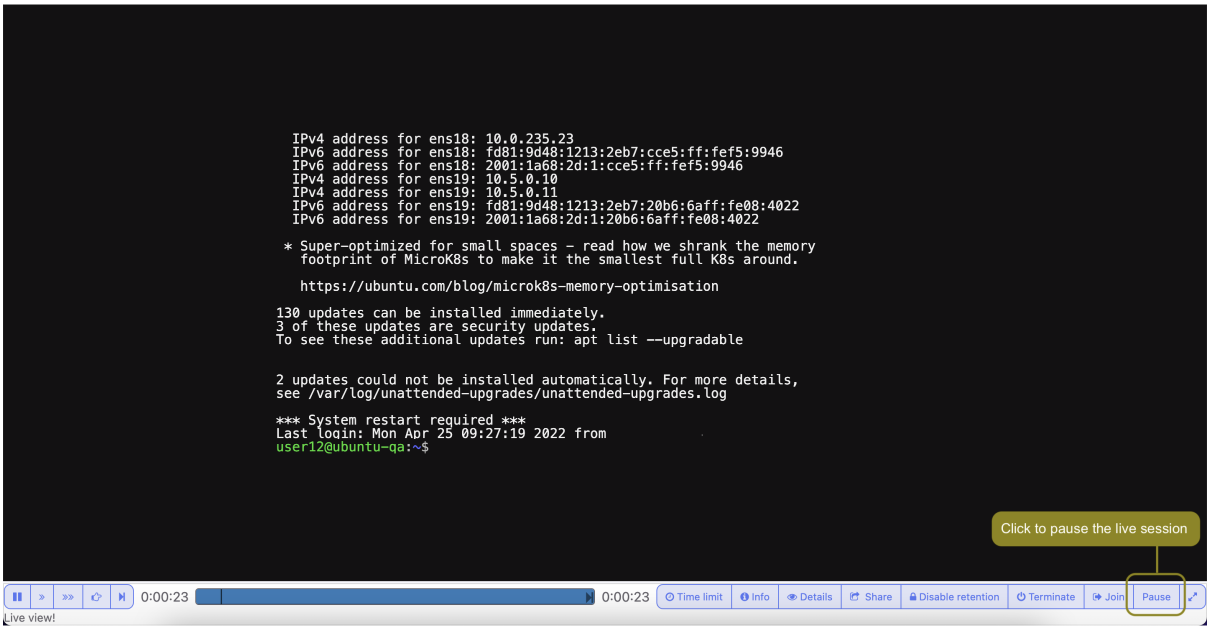
- *Sensitive features*

19.3 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*.



```
  IPv4 address for ens18: 10.0.235.23
  IPv6 address for ens18: fd81:9d48:1213:2eb7:cce5:ff:fef5:9946
  IPv6 address for ens18: 2001:1a68:2d:1:cce5:ff:fef5:9946
  IPv4 address for ens19: 10.5.0.10
  IPv4 address for ens19: 10.5.0.11
  IPv6 address for ens19: fd81:9d48:1213:2eb7:20b6:6aff:fe08:4022
  IPv6 address for ens19: 2001:1a68:2d:1:20b6:6aff:fe08:4022

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

130 updates can be installed immediately.
3 of these updates are security updates.
To see these additional updates run: apt list --upgradable


2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Mon Apr 25 09:27:19 2022 from
user12@ubuntu-qa:~$
```

Related topics:

- *Replaying session*

- *Joining session*
- *Filtering session*

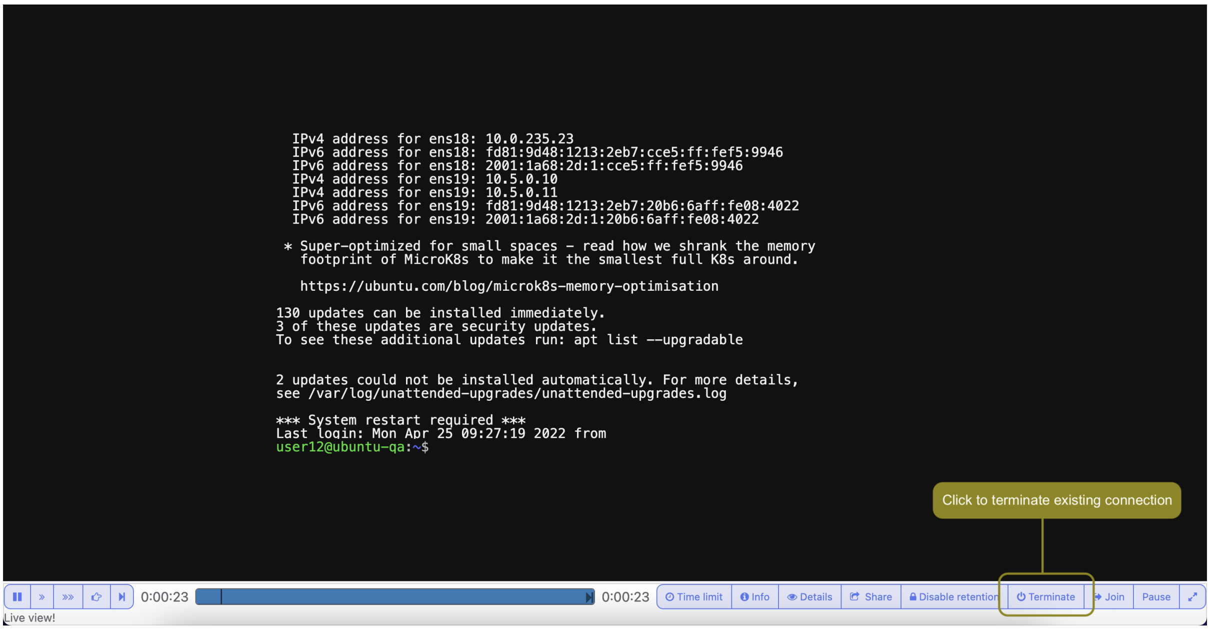
19.4 Terminating connection

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

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

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

Note: Terminating connection automatically blocks given user.



```
  IPv4 address for ens18: 10.0.235.23
  IPv6 address for ens18: fd81:9d48:1213:2eb7:cce5:ff:fef5:9946
  IPv6 address for ens18: 2001:1a68:2d:1:cce5:ff:fef5:9946
  IPv4 address for ens19: 10.5.0.10
  IPv4 address for ens19: 10.5.0.11
  IPv6 address for ens19: fd81:9d48:1213:2eb7:20b6:6aff:fe08:4022
  IPv6 address for ens19: 2001:1a68:2d:1:20b6:6aff:fe08:4022

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

130 updates can be installed immediately.
3 of these updates are security updates.
To see these additional updates run: apt list --upgradable


2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Mon Apr 25 09:27:19 2022 from
user12@ubuntu-qa:~$
```

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

Related topics:

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

- *Filtering sessions*

19.5 Joining live session

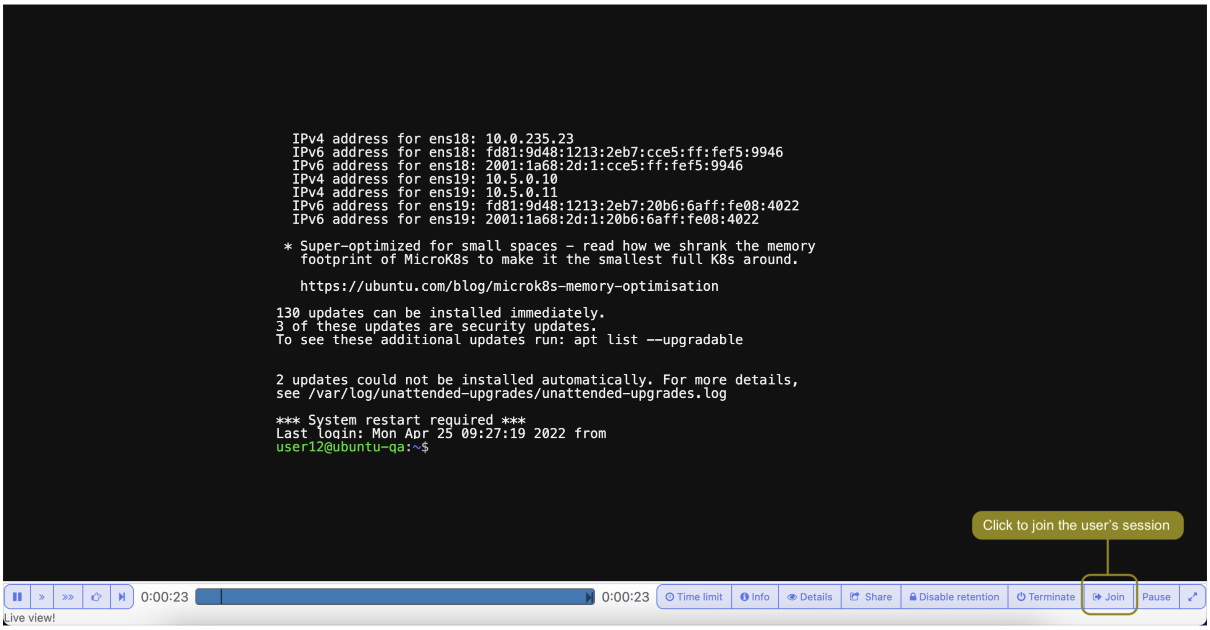
Fudo Enterprise allows joining an ongoing session to work simultaneously with the remote user.

Note:

- Session joining feature is supported in SSH, RDP, VNC and Telnet (excluding 5250 and 3270) connections.
- In case of cluster configurations, joining session is only possible after logging into the administration panel on the node that handles the given access session.

To join currently established session, proceed as follows.

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



```
  IPv4 address for ens18: 10.0.235.23
  IPv6 address for ens18: fd81:9d48:1213:2eb7:cce5:ff:fef5:9946
  IPv6 address for ens18: 2001:1a68:2d:1:cce5:ff:fef5:9946
  IPv4 address for ens19: 10.5.0.10
  IPv4 address for ens19: 10.5.0.11
  IPv6 address for ens19: fd81:9d48:1213:2eb7:20b6:6aff:fe08:4022
  IPv6 address for ens19: 2001:1a68:2d:1:20b6:6aff:fe08:4022

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

130 updates can be installed immediately.
3 of these updates are security updates.
To see these additional updates run: apt list --upgradable


2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Mon Apr 25 09:27:19 2022 from
user12@ubuntu-qa:~$
```

Related topics:

- *Replaying sessions*
- *Sharing sessions*
- *Filtering sessions*
- *Supported protocols*

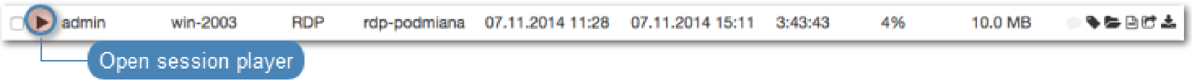
19.6 Sharing sessions

Fudo Enterprise enables sharing given session with another user.

Sharing a session

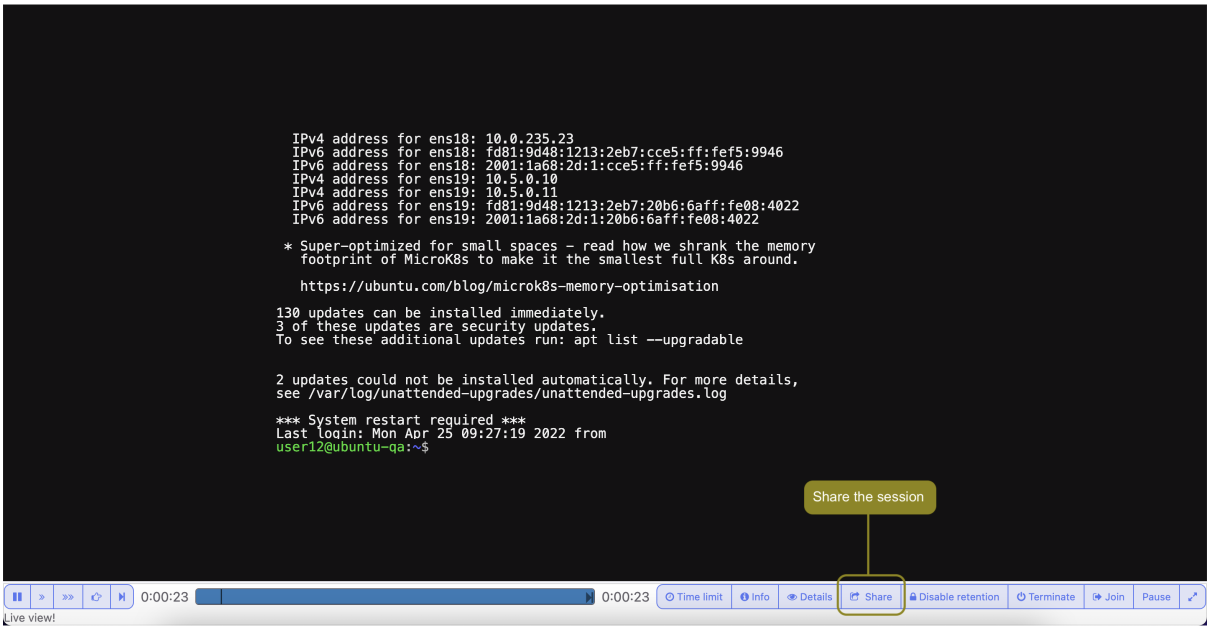
To share a session, proceed as follows.

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



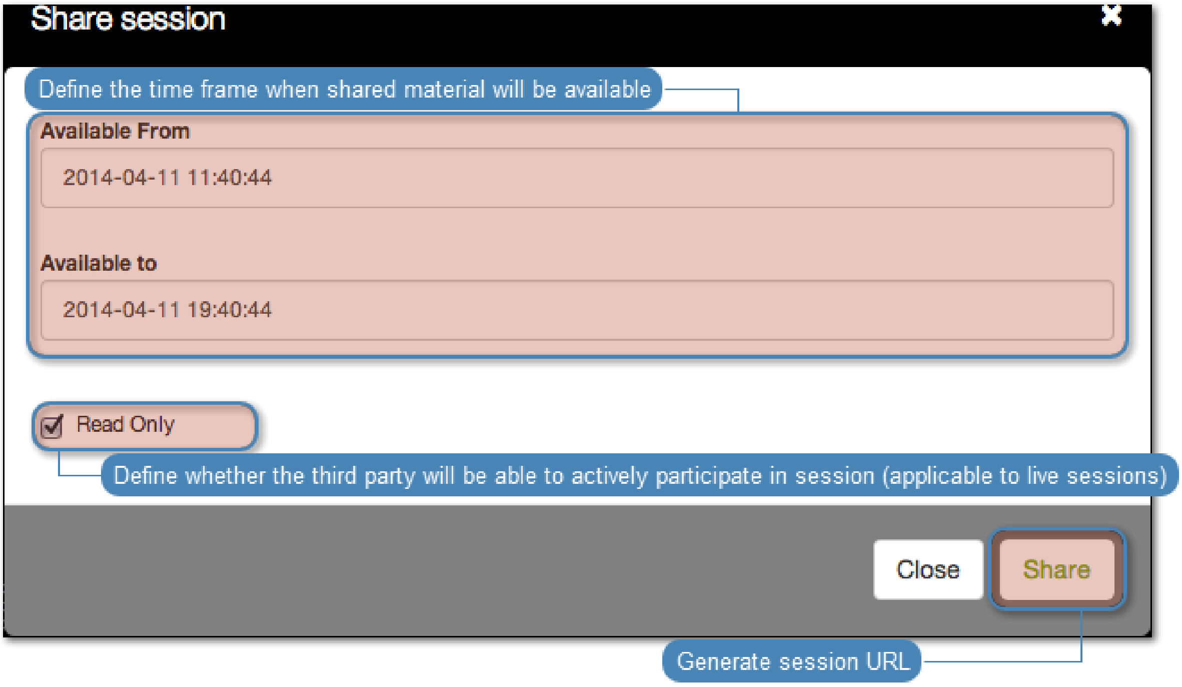
admin	win-2003	RDP	rdp-podmiana	07.11.2014 11:28	07.11.2014 15:11	3:43:43	4%	10.0 MB

3. Click *Share*.



```
  IPv4 address for ens18: 10.0.235.23
  IPv6 address for ens18: fd81:9d48:1213:2eb7:cce5:ff:fef5:9946
  IPv6 address for ens18: 2001:1a68:2d:1:cce5:ff:fef5:9946
  IPv4 address for ens19: 10.5.0.10
  IPv4 address for ens19: 10.5.0.11
  IPv6 address for ens19: fd81:9d48:1213:2eb7:20b6:6aff:fe08:4022
  IPv6 address for ens19: 2001:1a68:2d:1:20b6:6aff:fe08:4022

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

130 updates can be installed immediately.
3 of these updates are security updates.
To see these additional updates run: apt list --upgradable


2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Mon Apr 25 09:27:19 2022 from
user12@ubuntu-qa:~$
```

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)

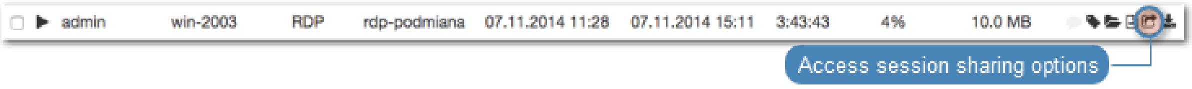
Generate session URL

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

Revoking session URL

To revoke a session URL, proceed as follows:

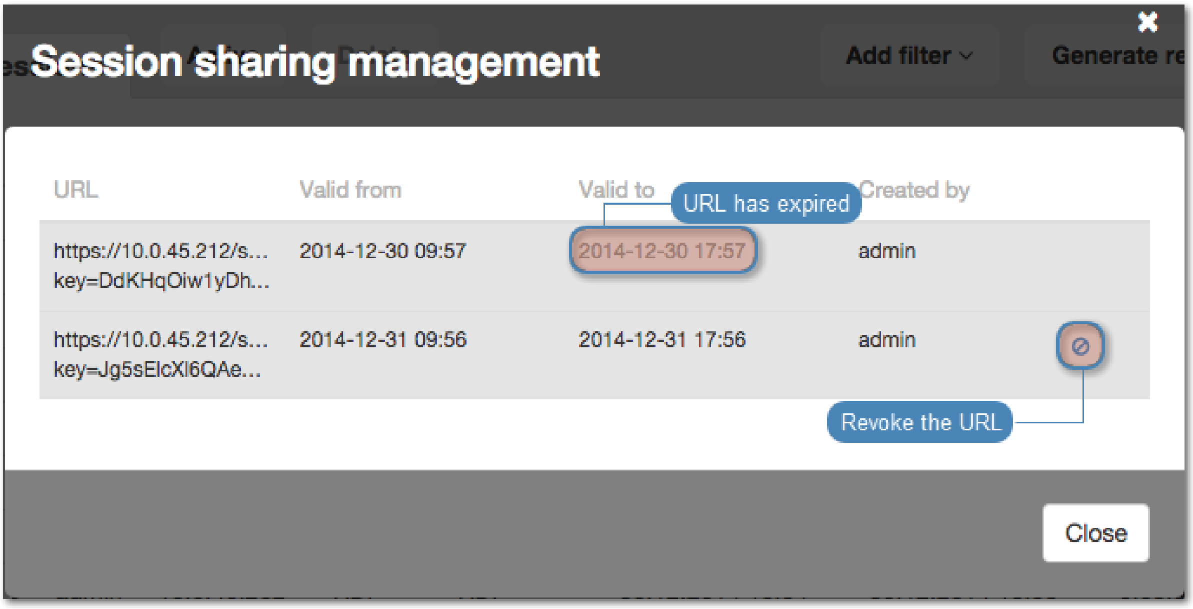
1. Select *Management* > *Sessions*.
2. Find desired session and click the *share* icon to display sessions sharing management options.



□ ▶	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=Jg5sElcXl6QAe...	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*

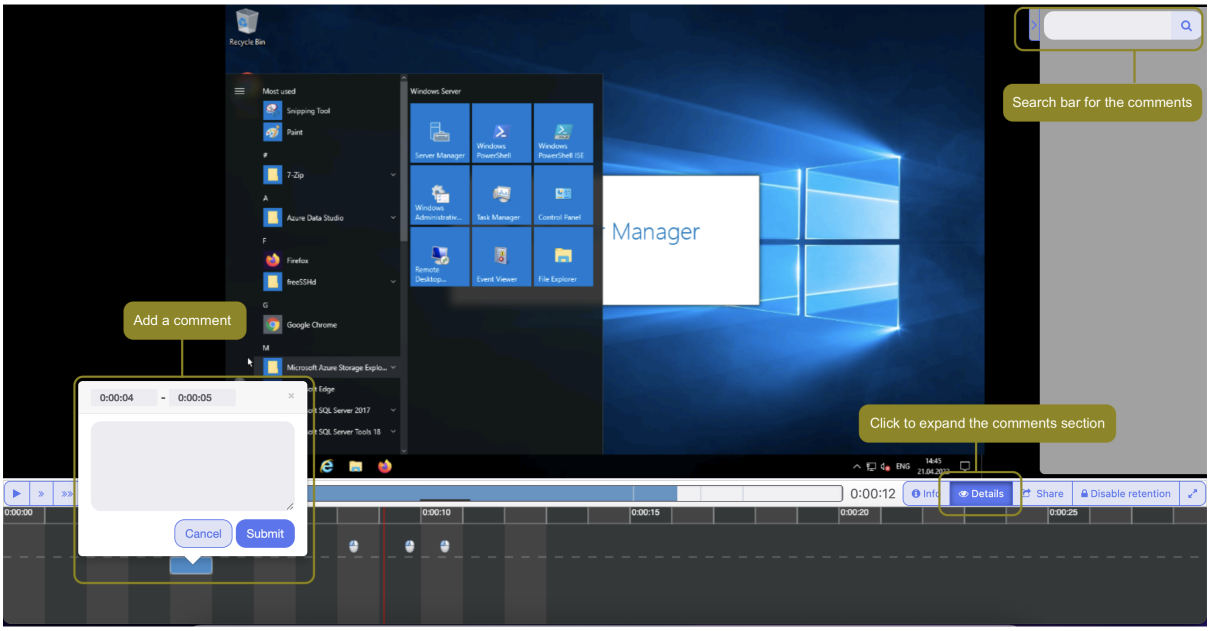
19.7 Commenting sessions

Fudo Enterprise enables adding comments and tags to recorded sessions.

Adding a comment

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

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



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

Editing a comment

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

5. Click the edit icon.

6. Change the comment and *Submit*.

Deleting a comment

1. Select *Management* > *Sessions*.

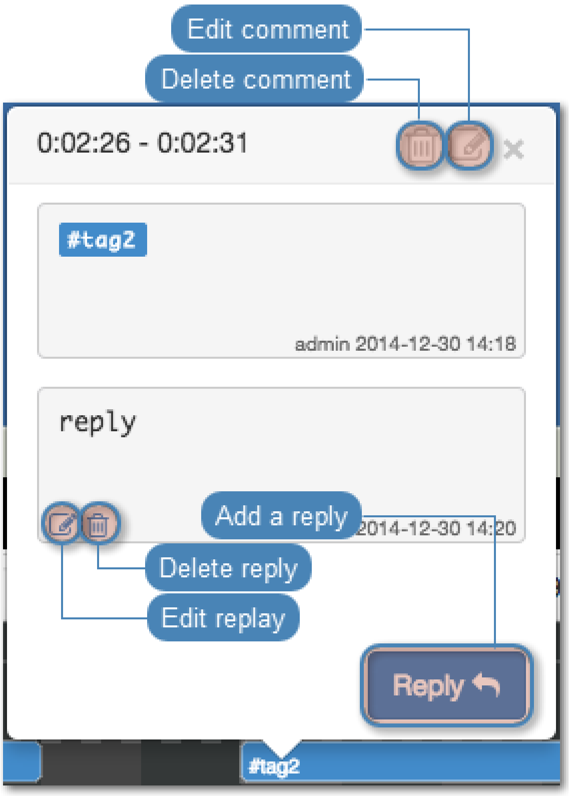
2. Find desired session and click the playback icon to start playback.

3. Click *Details*.

4. Find and click desired comment.

5. Click the trashcan icon.

6. Click *Delete* to delete the comment.



0:02:26 - 0:02:31

#tag2

admin 2014-12-30 14:18

reply

2014-12-30 14:20

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*

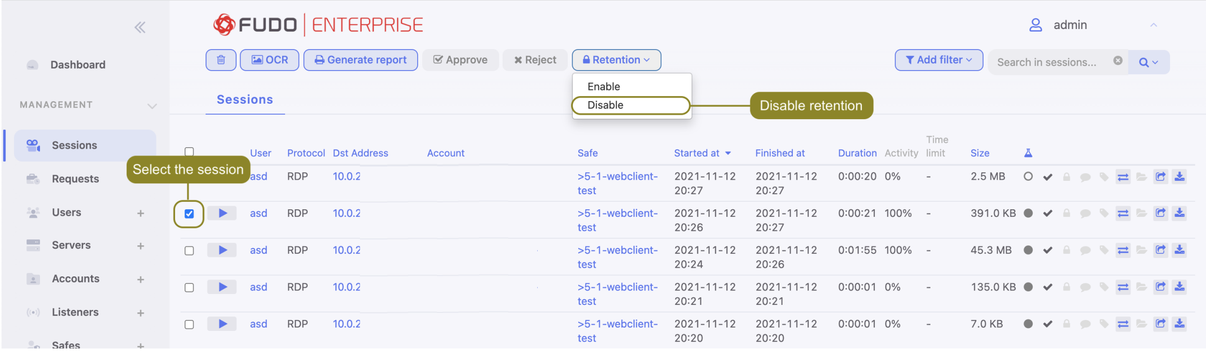
19.8 Sessions' retention lockdown

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*.



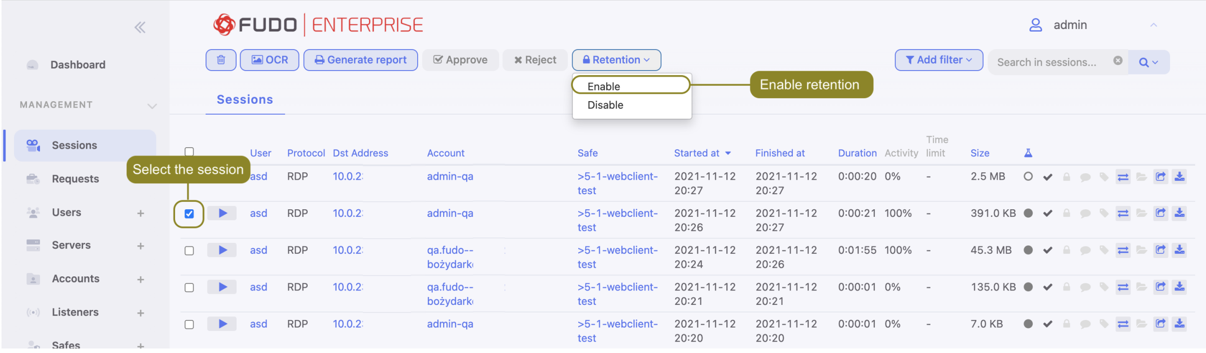
☐		User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
		asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:27	2021-11-12 20:27	0:00:20	0%	-	2.5 MB
☑	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:26	2021-11-12 20:27	0:00:21	100%	-	391.0 KB
☐	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:24	2021-11-12 20:26	0:01:55	100%	-	45.3 MB
☐	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:21	2021-11-12 20:21	0:00:01	0%	-	135.0 KB
☐	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:20	2021-11-12 20:20	0:00:01	0%	-	7.0 KB

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

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

Enabling retention

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



☐		User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
		asd	RDP	10.0.2:	admin-qa	>5-1-webclient-test	2021-11-12 20:27	2021-11-12 20:27	0:00:20	0%	-	2.5 MB
☑	▶	asd	RDP	10.0.2:	admin-qa	>5-1-webclient-test	2021-11-12 20:26	2021-11-12 20:27	0:00:21	100%	-	391.0 KB
☐	▶	asd	RDP	10.0.2:	qa.fudo--bożydark	>5-1-webclient-test	2021-11-12 20:24	2021-11-12 20:26	0:01:55	100%	-	45.3 MB
☐	▶	asd	RDP	10.0.2:	qa.fudo--bożydark	>5-1-webclient-test	2021-11-12 20:21	2021-11-12 20:21	0:00:01	0%	-	135.0 KB
☐	▶	asd	RDP	10.0.2:	admin-qa	>5-1-webclient-test	2021-11-12 20:20	2021-11-12 20:20	0:00:01	0%	-	7.0 KB

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

Related topics:

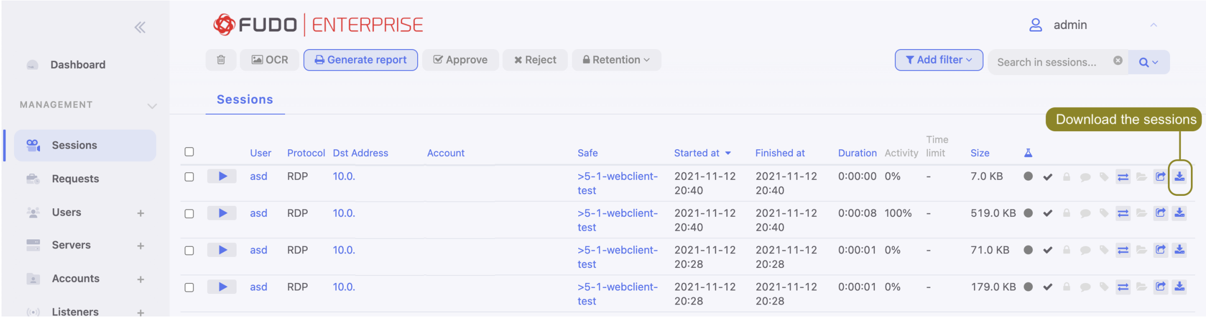
- *System backup*

19.9 Exporting sessions

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

To export a session, proceed as follows.

1. Select *Management* > *Sessions*.
2. Find desired session and click the session export icon.



☐		User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
☐	▶	asd	RDP	10.0.		>5-1-webclient-test	2021-11-12 20:40	2021-11-12 20:40	0:00:00	0%	-	7.0 KB
☐	▶	asd	RDP	10.0.		>5-1-webclient-test	2021-11-12 20:40	2021-11-12 20:40	0:00:08	100%	-	519.0 KB
☐	▶	asd	RDP	10.0.		>5-1-webclient-test	2021-11-12 20:28	2021-11-12 20:28	0:00:01	0%	-	71.0 KB
☐	▶	asd	RDP	10.0.		>5-1-webclient-test	2021-11-12 20:28	2021-11-12 20:28	0:00:01	0%	-	179.0 KB

3. Select the output file format.

Note: The output file format and the resolution determine conversion time and the size of the output file.

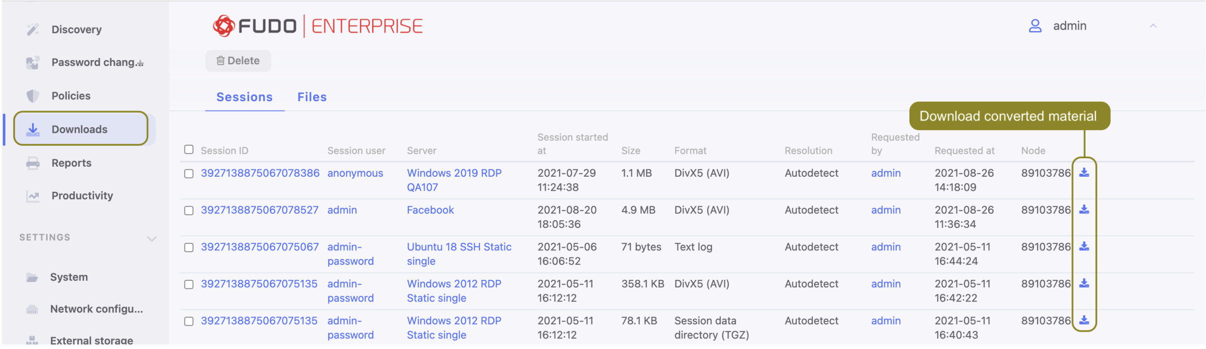
4. Select the video resolution (*not applicable to the text log file format*).

Note: *Autodetect* option will export video in the native user's screen resolution.

5. Click *Confirm* to start conversion and open the downloads page.

Note: The *Downloads* page enables monitoring conversion progress.

6. Find desired session and click the *Download* icon to download converted session material.



☐	Session ID	Session user	Server	Session started at	Size	Format	Resolution	Requested by	Requested at	Node
☐	3927138875067078386	anonymous	Windows 2019 RDP QA107	2021-07-29 11:24:38	1.1 MB	DivX5 (AVI)	Autodetect	admin	2021-08-26 14:18:09	89103786
☐	3927138875067078527	admin	Facebook	2021-08-20 18:05:36	4.9 MB	DivX5 (AVI)	Autodetect	admin	2021-08-26 11:36:34	89103786
☐	3927138875067075067	admin-password	Ubuntu 18 SSH Static single	2021-05-06 16:06:52	71 bytes	Text log	Autodetect	admin	2021-05-11 16:44:24	89103786
☐	3927138875067075135	admin-password	Windows 2012 RDP Static single	2021-05-11 16:12:12	358.1 KB	DivX5 (AVI)	Autodetect	admin	2021-05-11 16:42:22	89103786
☐	3927138875067075135	admin-password	Windows 2012 RDP Static single	2021-05-11 16:12:12	78.1 KB	Session data directory (TGZ)	Autodetect	admin	2021-05-11 16:40:43	89103786

19.9.1 Export Session File Formats

Following table provides a comparison of file formats available for session export across different protocols.

	WebM	DivX5 (AVI)	Xvid (AVI)	MPEG-2	MJPEG	Flash Video (FLV)	Text log	TGZ	PCAP * **
SSH	x	x	x	x	x	x	x	x	x
RDP	x	x	x	x	x	x		x	
VNC	x	x	x	x	x	x		x	
HTTP	x	x	x	x	x	x		x	x
MySQL								x	
TCP								x	
MS SQL (TDS)								x	
Telnet	x	x	x	x	x	x	x	x	
Telnet 3270	x	x	x	x	x	x	x	x	
Telnet 5250	x	x	x	x	x	x	x	x	
SCP								x	
SFTP								x	

Note: * PCAP files can be downloaded only for tunneled SSH sessions and non-rendered HTTP sessions.

** PCAP files can be downloaded only if the session was recorded in a RAW format. To learn more, please check the 'all' or 'raw' options in the *account configuration*.

While saving a session in one of the video file formats (AVI, MPEG-2, MJPEG, FLV), you have the option to select one of the resolutions listed below:

- 480p (852x480),
- 720p (1280x720),
- 1080p (1920x1080).

Related topics:

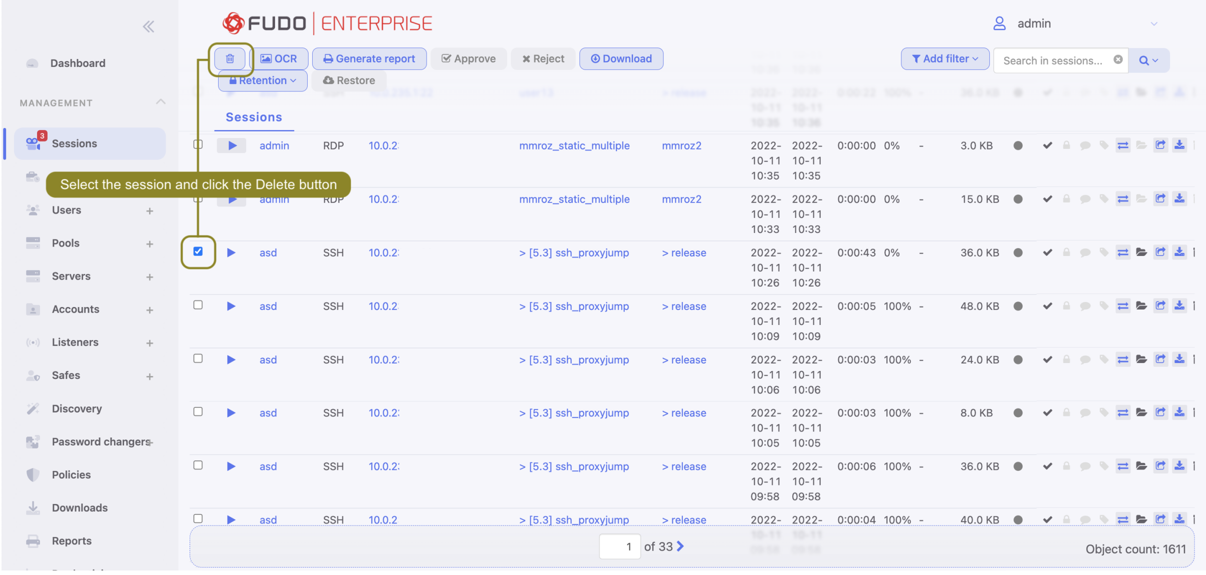
- *Filtering sessions*
- *Sharing sessions*
- *Viewing sessions*
- *Joining sessions*

19.10 Deleting sessions

Note: As the session's files and recorded videos are located in the *Management > Downloads* tab, when you remove a session, the system deletes also associated files, stored in the *Downloads > Files*. Recorded movies, stored in the *Downloads > Sessions* tab, remain and can be downloaded anytime.

To delete a recorded session, proceed as follows.

1. Select *Management > Sessions*.
2. Find and select desired session.
3. Click *Delete*.
4. Confirm deleting selected sessions.



Select the session and click the Delete button

□	admin	RDP	10.0.2:	mmroz_static_multiple	mmroz2	2022-10-11 10:35	2022-10-11 10:35	0:00:00	0%	-	3.0 KB	●
□	admin	RDP	10.0.2:	mmroz_static_multiple	mmroz2	2022-10-11 10:33	2022-10-11 10:33	0:00:00	0%	-	15.0 KB	●
☑	asd	SSH	10.0.2:	> [5.3] ssh_proxyjump	> release	2022-10-11 10:26	2022-10-11 10:26	0:00:43	0%	-	36.0 KB	●
□	asd	SSH	10.0.2:	> [5.3] ssh_proxyjump	> release	2022-10-11 10:09	2022-10-11 10:09	0:00:05	100%	-	48.0 KB	●
□	asd	SSH	10.0.2:	> [5.3] ssh_proxyjump	> release	2022-10-11 10:06	2022-10-11 10:06	0:00:03	100%	-	24.0 KB	●
□	asd	SSH	10.0.2:	> [5.3] ssh_proxyjump	> release	2022-10-11 10:05	2022-10-11 10:05	0:00:03	100%	-	8.0 KB	●
□	asd	SSH	10.0.2:	> [5.3] ssh_proxyjump	> release	2022-10-11 09:58	2022-10-11 09:58	0:00:06	100%	-	36.0 KB	●
□	asd	SSH	10.0.2	> [5.3] ssh_proxyjump	> release	2022-	2022-	0:00:04	100%	-	40.0 KB	●

1 of 33

Object count: 1611

Note: Fudo Enterprise can automatically delete sessions after certain time, specified by the retention parameter. Refer to the *Backups and retention* topic for more on data retention.

Related topics:

- *Filtering sessions*
- *Sharing sessions*
- *Viewing sessions*
- *Exporting sessions*

19.11 OCR processing sessions

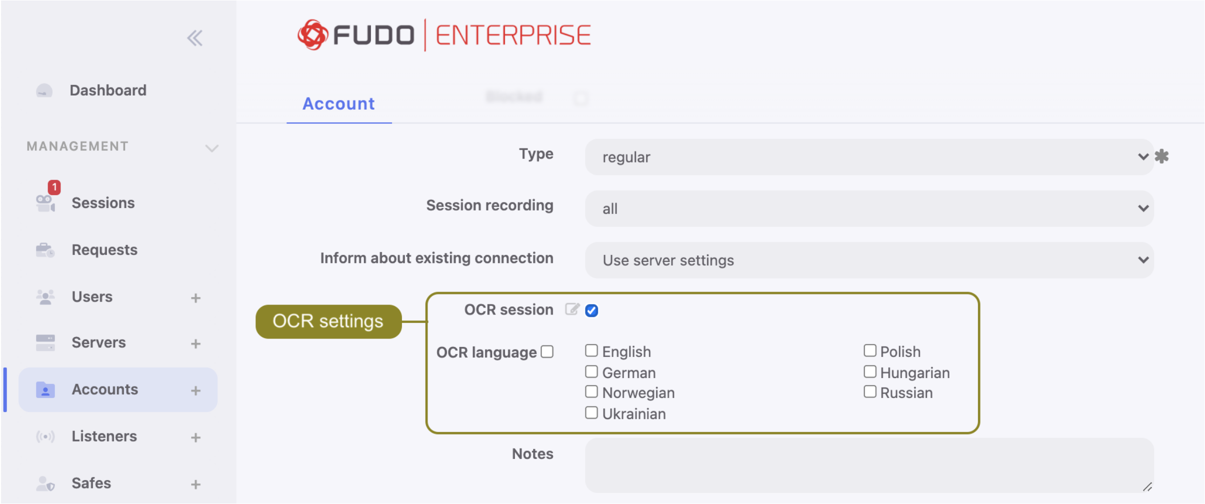
Recorded RDP, VNC and rendered HTTP sessions can be processed and indexed for full-text search purposes.

> **Warning:** OCR processing is CPU intensive and may have negative impact on system's performance. It is recommended to enable it only for those accounts, which require detailed supervision.

Automated sessions processing

To have RDP, VNC or rendered HTTP sessions automatically processed, proceed as follows.

1. Select *Management* > *Accounts*.
2. Find and click desired account.
3. Select the *OCR sessions* option.
4. Select the language of processed data.



Type: regular

Session recording: all

Inform about existing connection: Use server settings

OCR session ☑

OCR language □

□ English
□ German
□ Norwegian
□ Ukrainian
□ Polish
□ Hungarian
□ Russian

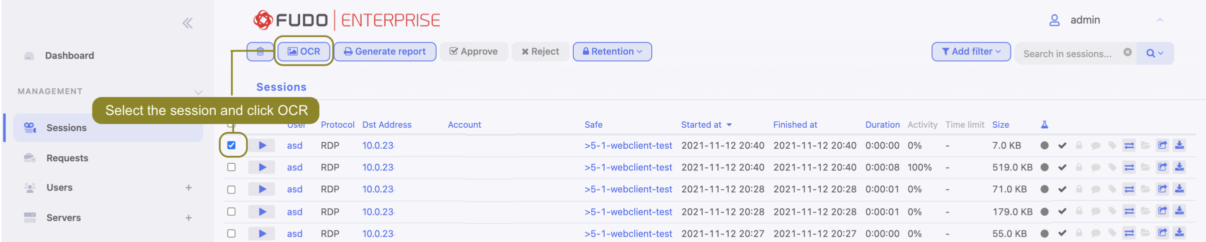
Notes

5. Click *Save*.

Processing selected sessions

To process selected sessions, proceed as follows.

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



Sessions

		User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
☑	▶	asd	RDP	10.0.23		>5-1-webclient-test	2021-11-12 20:40	2021-11-12 20:40	0:00:00	0%	-	7.0 KB
□	▶	asd	RDP	10.0.23		>5-1-webclient-test	2021-11-12 20:40	2021-11-12 20:40	0:00:08	100%	-	519.0 KB
□	▶	asd	RDP	10.0.23		>5-1-webclient-test	2021-11-12 20:28	2021-11-12 20:28	0:00:01	0%	-	71.0 KB
□	▶	asd	RDP	10.0.23		>5-1-webclient-test	2021-11-12 20:28	2021-11-12 20:28	0:00:01	0%	-	179.0 KB
□	▶	asd	RDP	10.0.23		>5-1-webclient-test	2021-11-12 20:27	2021-11-12 20:27	0:00:00	0%	-	55.0 KB

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

---

3. Confirm processing selected sessions.

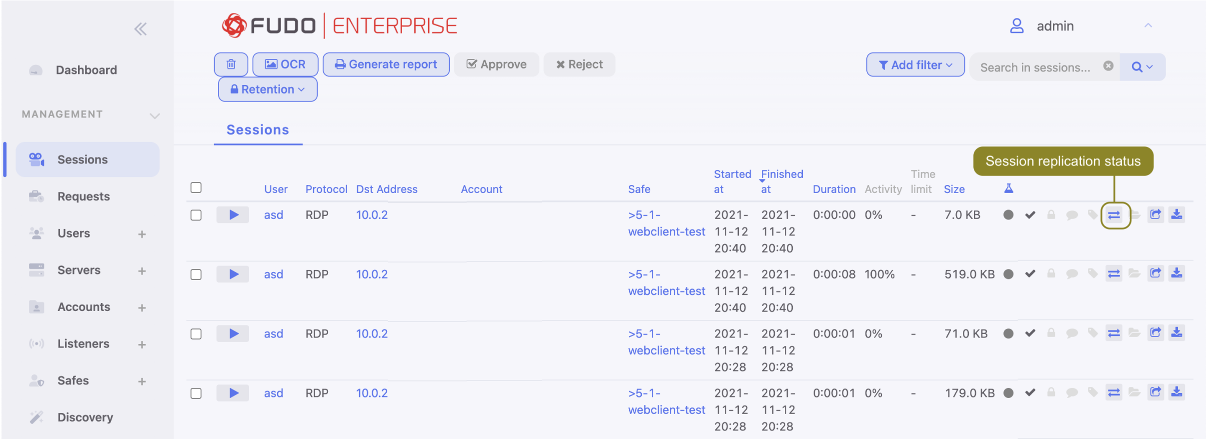
Related topics:

- *Filtering sessions*
- *Accounts*

19.12 Session data replication

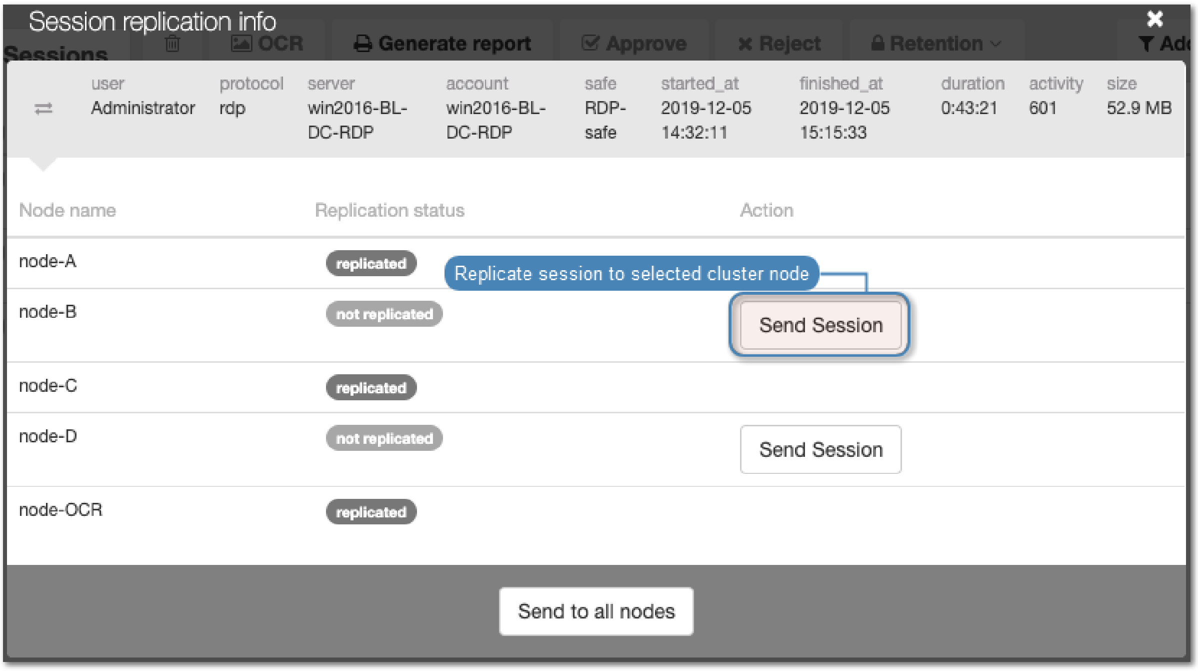
Additionally to automated session data replication, Fudo Enterprise enables on-demand replication to Fudo Enterprise instances to which the given data is not replicated automatically.

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



□		User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
□	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:40	2021-11-12 20:40	0:00:00	0%	-	7.0 KB
□	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:40	2021-11-12 20:40	0:00:08	100%	-	519.0 KB
□	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:28	2021-11-12 20:28	0:00:01	0%	-	71.0 KB
□	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:28	2021-11-12 20:28	0:00:01	0%	-	179.0 KB

3. Click *Send session* next to a specific cluster node to replicate session to selected Fudo Enterprise instance



Session replication info

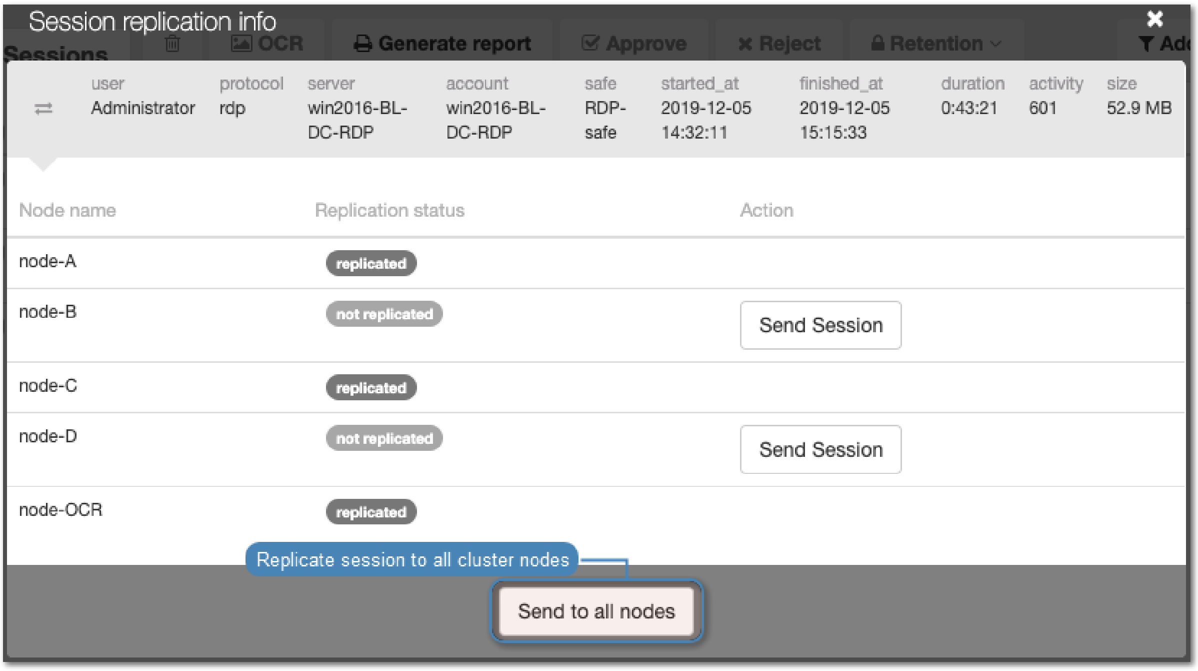
	user	protocol	server	account	safe	started_at	finished_at	duration	activity	size
⇄	Administrator	rdp	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 14:32:11	2019-12-05 15:15:33	0:43:21	601	52.9 MB

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	

Replicate session to selected cluster node

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	

Replicate session to all cluster nodes

Send to all nodes

Related topics:

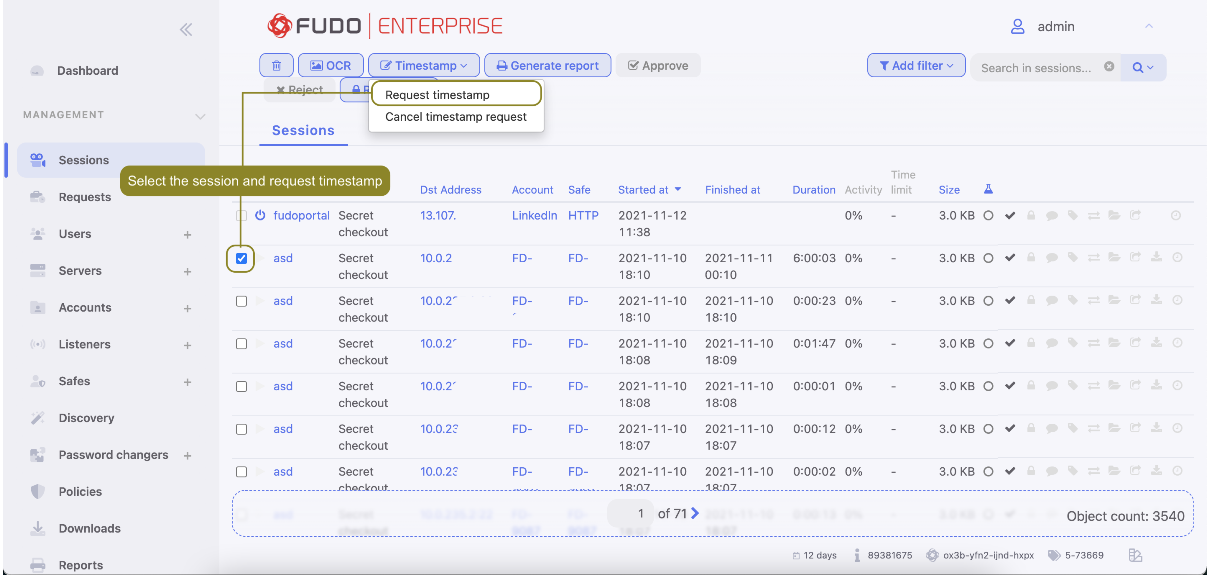
- *Cluster configuration*
- *Sessions*

19.13 Timestamping selected sessions

Note: To timestamp sessions, first you have to enable and configure the timestamping feature. Go to *Settings* > *Timestamping* and follow the instructions in the *Trusted time-stamping* section.

To timestamp selected sessions, proceed as follows.

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



Select the session and request timestamp

			Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
□	fudoportal	Secret checkout	13.107.	LinkedIn	HTTP	2021-11-12 11:38			0%	-	3.0 KB
☑	asd	Secret checkout	10.0.2	FD-	FD-	2021-11-10 18:10	2021-11-11 00:10	6:00:03	0%	-	3.0 KB
□	asd	Secret checkout	10.0.2	FD-	FD-	2021-11-10 18:10	2021-11-10 18:10	0:00:23	0%	-	3.0 KB
□	asd	Secret checkout	10.0.2	FD-	FD-	2021-11-10 18:08	2021-11-10 18:09	0:01:47	0%	-	3.0 KB
□	asd	Secret checkout	10.0.2	FD-	FD-	2021-11-10 18:08	2021-11-10 18:08	0:00:01	0%	-	3.0 KB
□	asd	Secret checkout	10.0.23	FD-	FD-	2021-11-10 18:07	2021-11-10 18:07	0:00:12	0%	-	3.0 KB
□	asd	Secret checkout	10.0.23	FD-	FD-	2021-11-10 18:07	2021-11-10 18:07	0:00:02	0%	-	3.0 KB

1 of 71

Object count: 3540

12 days 89381675 ox3b-yfn2-ijnd-hxpx 5-73669

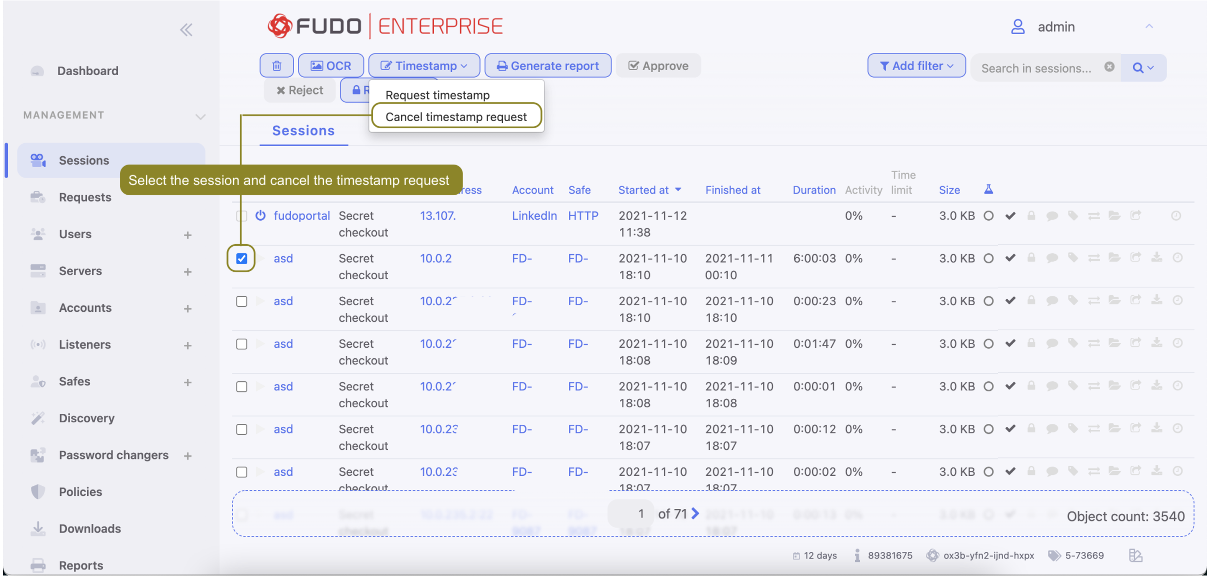
3. Click *Confirm*.

Note: Once the timestamping option is enabled, an additional column will appear on the session list. Timestamped sessions are marked with an active clock icon 🕘. By clicking on it, you can view detailed timestamp information and download the signature.

19.14 Cancelling sessions timestamping

To cancel sessions timestamping, proceed as follows.

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



			ress	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
□	fudoportal	Secret checkout	13.107.	LinkedIn	HTTP	2021-11-12 11:38			0%	-	3.0 KB
☑	asd	Secret checkout	10.0.2	FD-	FD-	2021-11-10 18:10	2021-11-11 00:10	6:00:03	0%	-	3.0 KB
□	asd	Secret checkout	10.0.2	FD-	FD-	2021-11-10 18:10	2021-11-10 18:10	0:00:23	0%	-	3.0 KB
□	asd	Secret checkout	10.0.2	FD-	FD-	2021-11-10 18:08	2021-11-10 18:09	0:01:47	0%	-	3.0 KB
□	asd	Secret checkout	10.0.2	FD-	FD-	2021-11-10 18:08	2021-11-10 18:08	0:00:01	0%	-	3.0 KB
□	asd	Secret checkout	10.0.23	FD-	FD-	2021-11-10 18:07	2021-11-10 18:07	0:00:12	0%	-	3.0 KB
□	asd	Secret checkout	10.0.23	FD-	FD-	2021-11-10 18:07	2021-11-10 18:07	0:00:02	0%	-	3.0 KB

1 of 71 › Object count: 3540

12 days 89381675 ox3b-yfn2-ijnd-hxpx 5-73669

3. Click *Confirm.*

Related topics:

- *Filtering sessions*
- *Accounts*

19.15 Require approval for access

The Require Approval option enhances security by mandating that users must request access to a server before they can connect. When this option is enabled, authorized users are given a specified timeframe to either approve or reject the access request. This mechanism ensures that access to critical systems is controlled and monitored, reducing the risk of unauthorized or inappropriate use. It also fosters accountability, as each access request is documented and reviewed by designated personnel. This feature aligns with **4-Eyes** principle by providing an additional layer of oversight and control.

Note: The **4-Eyes** principle is a security measure that enhances access management by requiring the approval or presence of two authorized individuals for critical operations. This approach ensures that no single person has complete control over sensitive actions, reducing the risk of errors, fraud, or unauthorized access.

In order to enable sending user requests, it's necessary to have the *Require approval* option checked in safe configuration. For more information, refer to the *Creating a safe* section.

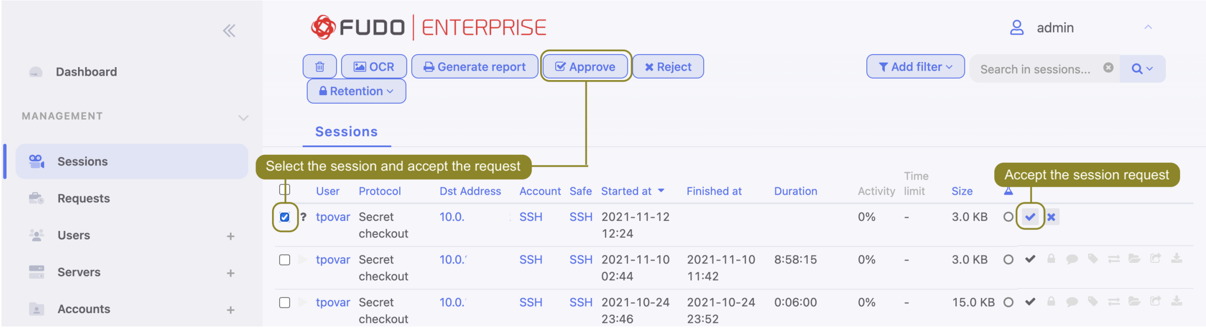
Note: To receive email notifications about pending sessions, select *Session awaiting approval* notification in safe configuration.

Approving user request is possible also via the *Fudo Officer 1.0* application. *Session awaiting approval (push)* notification should be enabled in order to see notifications about pending requests.

19.15.1 Approving pending user requests

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

or select desired pending request and click *Approve*.



Select the session and accept the request

Accept the session request

User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
☑ ? tpovar	Secret checkout	10.0.	SSH	SSH	2021-11-12 12:24			0%	-	3.0 KB
□ tpovar	Secret checkout	10.0.	SSH	SSH	2021-11-10 02:44	2021-11-10 11:42	8:58:15	0%	-	3.0 KB
□ tpovar	Secret checkout	10.0.	SSH	SSH	2021-10-24 23:46	2021-10-24 23:52	0:06:00	0%	-	15.0 KB

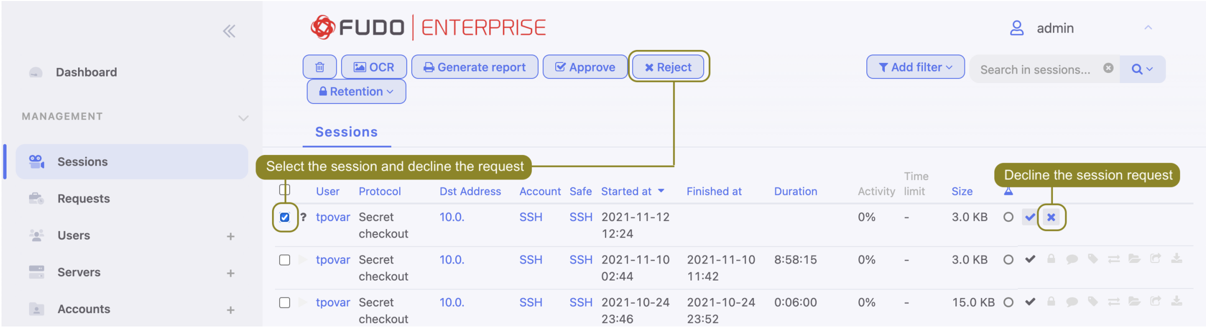
Related topics:

- *User authentication methods and modes*
- *Declining pending requests*
- *Sessions*
- *Fudo Officer 1.0*

19.15.2 Declining pending requests

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

or select pending sessions and click *Reject*.



Select the session and decline the request

Decline the session request

User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
☑ ? tpovar	Secret checkout	10.0.	SSH	SSH	2021-11-12 12:24			0%	-	3.0 KB
□ tpovar	Secret checkout	10.0.	SSH	SSH	2021-11-10 02:44	2021-11-10 11:42	8:58:15	0%	-	3.0 KB
□ tpovar	Secret checkout	10.0.	SSH	SSH	2021-10-24 23:46	2021-10-24 23:52	0:06:00	0%	-	15.0 KB

3. Optionally, enter the reason for rejecting given request.

Note: Rejection reason is displayed on the session list after positioning cursor over the 💬 icon.

4. Optionally, select the option to block the user.

Note: User blocking reason will be the same as the entered session rejection reason.

5. Click *Confirm*.

Related topics:

- *User authentication methods and modes*
- *Approving pending user requests*
- *Terminating connection*
- *Blocking a user*
- *Sessions*
- *Fudo Officer 1.0*

19.16 AI sessions processing

Fudo Enterprise is able to detect changes in user behavior and determine if user credentials have been compromised. It can also alert system administrator if there is an unusually high number of connections or a particular session is longer than expected.

19.16.1 Content models

Content models process and analyze RDP and SSH sessions in order to build behavioral user profiles. Based on these, Fudo Enterprise can detect even the slightest change in user behavior and help prevent a security breach.

RDP content model

The RDP model is based on mouse cursor movements.

The following requirements must be met in order to produce an RDP model:

Minimum:

- 5 hours of sessions recordings per predictor,
- 5 unique predictors (e.g. users).

Optimal:

- 30 hours of sessions recordings,
- 10 unique predictors.

Note: RDP model's quality depends on the consistency of how the user interacts with the monitored system. If the user has used different operating systems and input devices (e.g. different mice, a trackpad or a trackball) the resulting model will not be very effective as it will have a higher tolerance for a variety of behaviors.

SSH content model

The SSH content model is based on the keyboard input (commands).

The following requirements must be met in order to produce an SSH model:

Minimum:

- 65 sessions recorded (25 unique commands minimum),
- 5 unique predictors (e.g. users).

Optimal:

- 300 sessions recorded per predictor,
- 10 unique predictors (e.g. users).

19.16.2 Session scoring

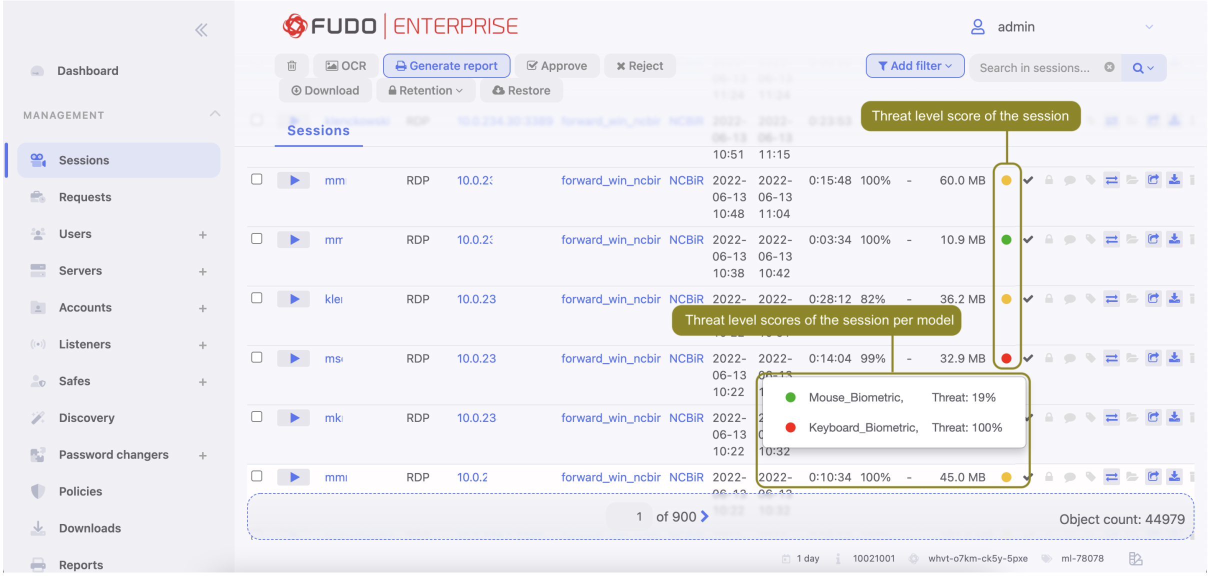
Fudo Enterprise analyzes sessions in real-time and produces threat level scores (*OK*, *LOW*, *HIGH*) depending on how the user fares against the trained model.

Note: Sessions are processed in chunks containing a specific number of events. Processing is done in real-time as long as there are workers available. When there are no workers available, ongoing sessions' parts are not analyzed.

Models are calibrated individually and session scores are presented on the *session list*.

Icon	Description
○	Session under analysis, initial result - no threat.
○	Session under analysis, initial result - medium threat level.
○	Session under analysis, initial result - high threat level.
○	Session awaiting analysis or being initially processed.
○	Session not analyzed due to missing a trained model.
🟢	Session processed - no risk.
🟡	Session processed - medium threat level.
🔴	Session processed - high threat level.
●	Session processed - no result.

Note: When it comes to building user models, data quality is essential. If users shared login credentials, the resulting model will be less likely to detect the variance in user behavior.



Threat level score of the session

Threat level scores of the session per model

□	mm	RDP	10.0.2	forward_win_ncbir	NCBiR	2022-06-13 10:48	2022-06-13 11:04	0:15:48	100%	-	60.0 MB
□	mr	RDP	10.0.2	forward_win_ncbir	NCBiR	2022-06-13 10:38	2022-06-13 10:42	0:03:34	100%	-	10.9 MB
□	kle	RDP	10.0.23	forward_win_ncbir	NCBiR	2022-	2022-	0:28:12	82%	-	36.2 MB
□	ms	RDP	10.0.23	forward_win_ncbir	NCBiR	2022-06-13 10:22	2022-	0:14:04	99%	-	32.9 MB
□	mk	RDP	10.0.23	forward_win_ncbir	NCBiR	2022-06-13 10:22	10:32				
□	mm	RDP	10.0.2	forward_win_ncbir	NCBiR	2022-	2022-	0:10:34	100%	-	45.0 MB

● Mouse_Biometric, Threat: 19%

● Keyboard_Biometric, Threat: 100%

1 of 900

Object count: 44979

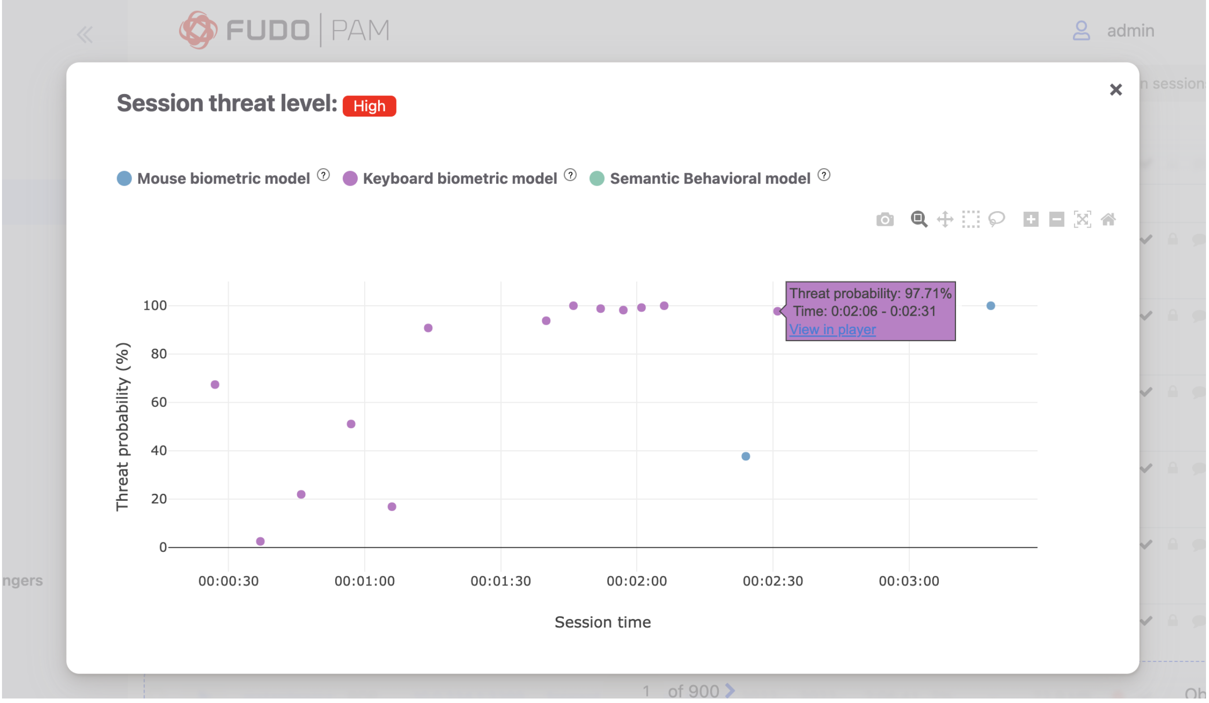
1 day 10021001 whvt-o7km-ck5y-5pxe ml-78078

Threat level popup contains information about individual **Threat Probability** for each model that assessed the session. **Threat probability** is a percentage-wise value that reflects a threat level of the session. The logic behind the different color icons is the following:

The icon is 🟢 when *Threat Probability* is below 50%.

The 🟡 icon is reflected when *Threat Probability* is above 50% but the underlying statistics of a model indicate that it could cause a *False Positive Rate* over 5%. In such case a higher, individual for each User and ML Model pair percentage threshold is derived while training to obtain most optimal results.

The icon is 🔴 when Threat Probability is above 50% and False Positive Rate would be lower than 5%. If the *False Positive Rate* requirement can't be met a higher threshold is used as described above which the red circle is eventually used.



Session threat level: High

Threat probability: 97.71%
Time: 0:02:06 - 0:02:31

The *Session threat probability* graph displays threat probability scores for specific periods of the session time (called segments), based on AI models prediction. A segment is a group of user's actions, which the AI model uses for individual prediction.

Note: A session should be long enough for running prediction algorithms. Minimum duration of the session for launching the AI model analysis is 3 segments (around 1 minute).

The graph also contains a link to the specific period of the session (segment) in the player which allows the administrator to check the session in real time and react accordingly. The administrator is also able to analyze the results, delivered by the AI training models and take actions for the future sessions by adjusting settings. For example, by adding a policy to be notified when a certain threat probability threshold is reached.

Note: The upgrading process to the Fudo Enterprise 5.3 removes session scores that were calculated for the sessions before the upgrade and introduces a new calculating algorithm. For the sessions before the upgrade detailed data is not available.

19.16.3 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*
- *Policies*

CHAPTER 20

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

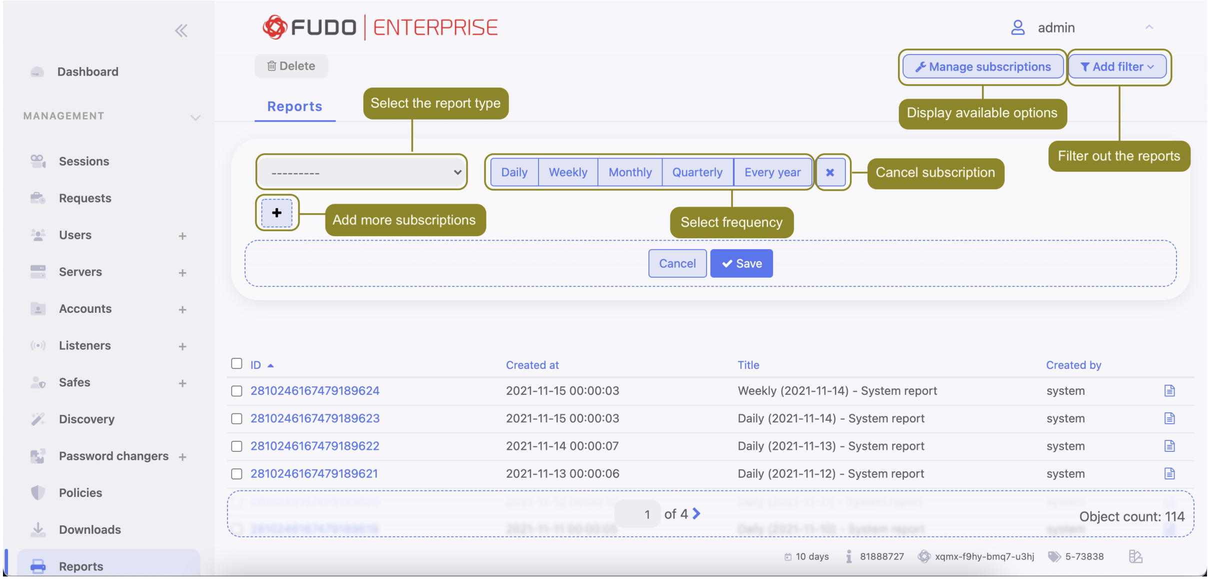
Account access report	This report contains accounts and corresponding servers and safes which have been accessed in the given time period.
Safe access report	This report contains safes and the corresponding servers accessed in the given time period.
Server access report	This report contains servers accessed 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*.



ID	Created at	Title	Created by
2810246167479189624	2021-11-15 00:00:03	Weekly (2021-11-14) - System report	system
2810246167479189623	2021-11-15 00:00:03	Daily (2021-11-14) - System report	system
2810246167479189622	2021-11-14 00:00:07	Daily (2021-11-13) - System report	system
2810246167479189621	2021-11-13 00:00:06	Daily (2021-11-12) - System report	system

1 of 4

Object count: 114

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*.

Cancelling a periodic report subscription

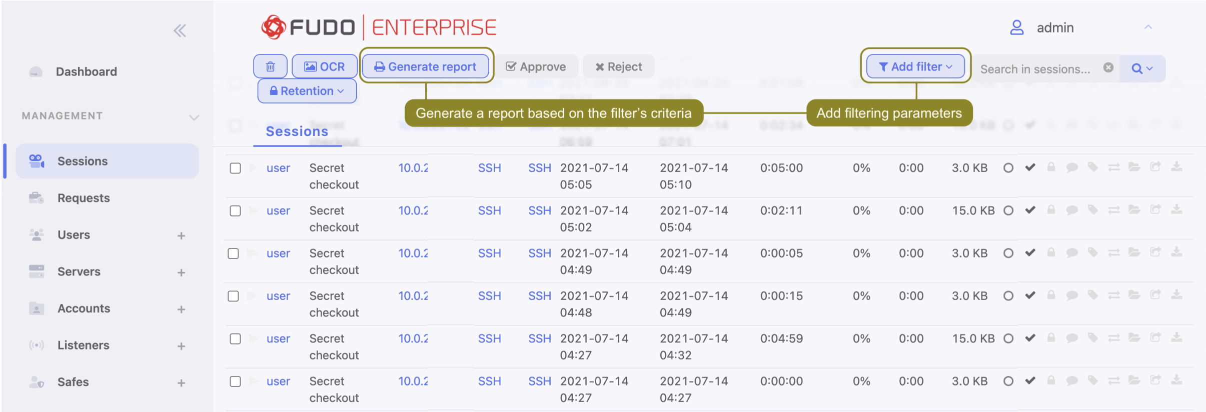
To cancel a subscription to a cyclic report, proceed as follows.

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

Generating reports on demand

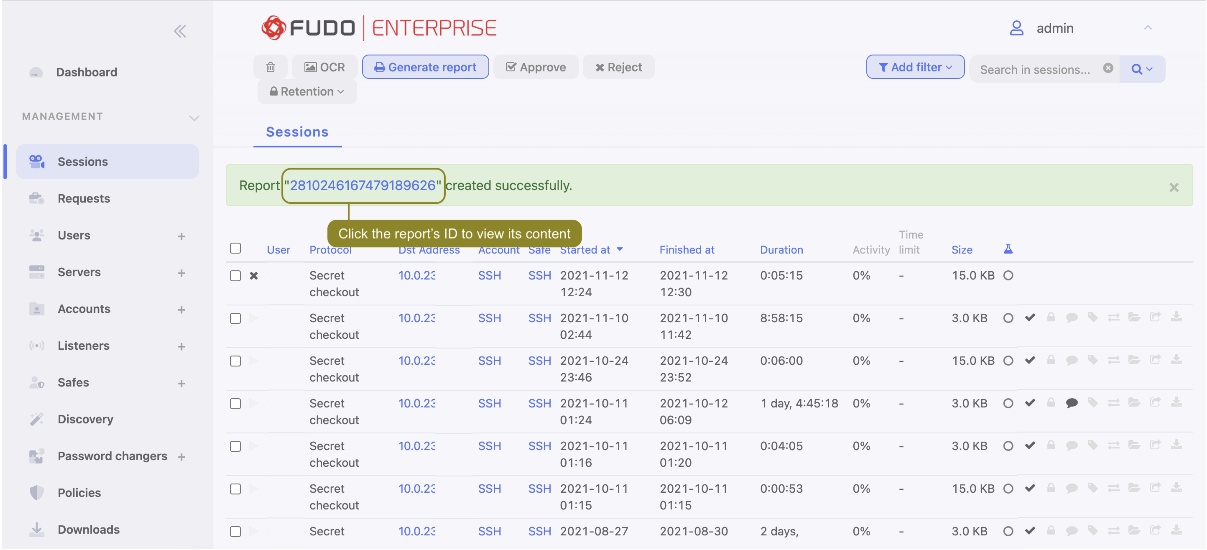
A report can be prepared for a specified subset of user sessions, determined by filtering options.

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



☐	user	Secret checkout	10.0.2	SSH	SSH	2021-07-14 05:05	2021-07-14 05:10	0:05:00	0%	0:00	3.0 KB
☐	user	Secret checkout	10.0.2	SSH	SSH	2021-07-14 05:02	2021-07-14 05:04	0:02:11	0%	0:00	15.0 KB
☐	user	Secret checkout	10.0.2	SSH	SSH	2021-07-14 04:49	2021-07-14 04:49	0:00:05	0%	0:00	3.0 KB
☐	user	Secret checkout	10.0.2	SSH	SSH	2021-07-14 04:48	2021-07-14 04:49	0:00:15	0%	0:00	3.0 KB
☐	user	Secret checkout	10.0.2	SSH	SSH	2021-07-14 04:27	2021-07-14 04:32	0:04:59	0%	0:00	15.0 KB
☐	user	Secret checkout	10.0.2	SSH	SSH	2021-07-14 04:27	2021-07-14 04:27	0:00:00	0%	0:00	3.0 KB

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



Report "2810246167479189626" created successfully.

Click the report's ID to view its content

☐		User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
☐	✖		Secret checkout	10.0.23	SSH	SSH	2021-11-12 12:24	2021-11-12 12:30	0:05:15	0%	-	15.0 KB
☐			Secret checkout	10.0.23	SSH	SSH	2021-11-10 02:44	2021-11-10 11:42	8:58:15	0%	-	3.0 KB
☐			Secret checkout	10.0.23	SSH	SSH	2021-10-24 23:46	2021-10-24 23:52	0:06:00	0%	-	15.0 KB
☐			Secret checkout	10.0.23	SSH	SSH	2021-10-11 01:24	2021-10-12 06:09	1 day, 4:45:18	0%	-	3.0 KB
☐			Secret checkout	10.0.23	SSH	SSH	2021-10-11 01:16	2021-10-11 01:20	0:04:05	0%	-	3.0 KB
☐			Secret checkout	10.0.23	SSH	SSH	2021-10-11 01:15	2021-10-11 01:15	0:00:53	0%	-	15.0 KB
☐			Secret	10.0.23	SSH	SSH	2021-08-27	2021-08-30	2 days,	0%	-	3.0 KB

5. Select *Management > Reports*.

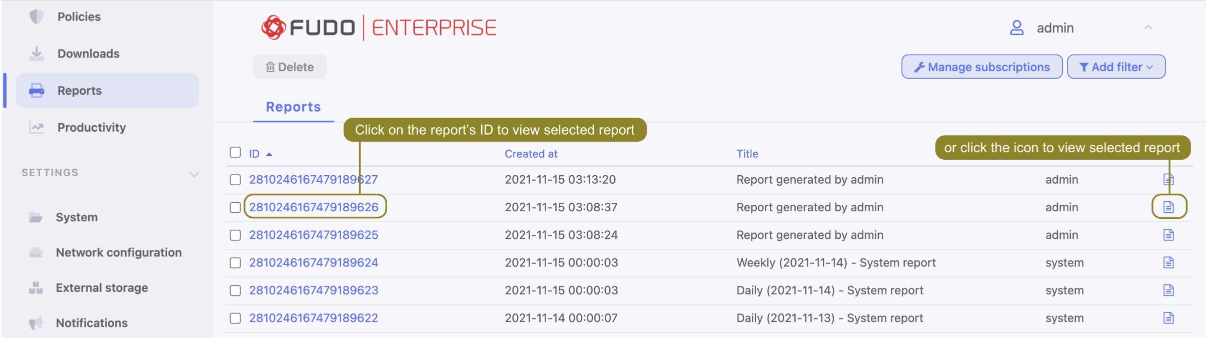
6. Find desired report and click the view icon.

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.



Click on the report's ID to view selected report

or click the icon to view selected report

☐	ID	Created at	Title		
☐	2810246167479189627	2021-11-15 03:13:20	Report generated by admin	admin	🗎
☐	2810246167479189626	2021-11-15 03:08:37	Report generated by admin	admin	🗎
☐	2810246167479189625	2021-11-15 03:08:24	Report generated by admin	admin	🗎
☐	2810246167479189624	2021-11-15 00:00:03	Weekly (2021-11-14) - System report	system	🗎
☐	2810246167479189623	2021-11-15 00:00:03	Daily (2021-11-14) - System report	system	🗎
☐	2810246167479189622	2021-11-14 00:00:07	Daily (2021-11-13) - System report	system	🗎

3. Click the corresponding button to save the report in selected format - CSV, PDF or HTML.

Deleting reports

1. Select *Management > Reports*.

2. Find, select desired reports and click *Delete*.

Related topics:

- *Notifications*
- *Filtering sessions*

CHAPTER 21

Productivity

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

21.1 Overview

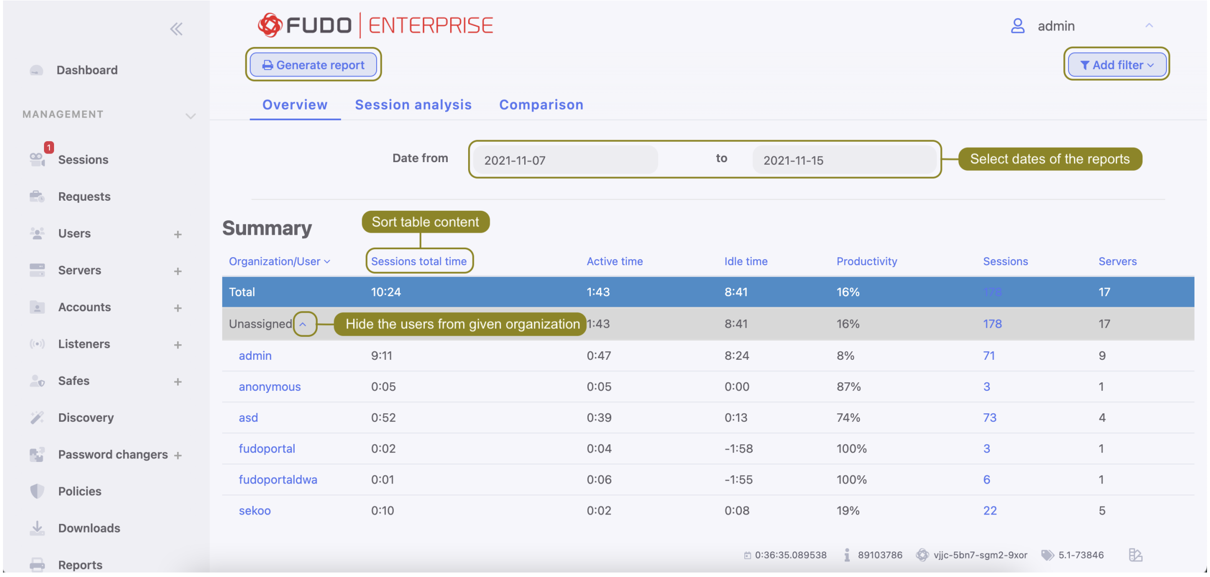
Overview displays data on users' activity in selected time interval.

Note: Activity rating is based on the user's interaction with the monitored system. Fudo Enterprise divides the time into 60 seconds long time intervals and monitors the activity within the interval. Lack of any actions in a given time period accounts such as a non-productive time.

To view the users' activity rundown, proceed as follows.

1. Select *Management* > *Productivity*.
2. Select the *Overview* tab.
3. Define the users' list filtering.
4. Click *Generate report* to generate rundown of the displayed data in HTML, CSV or PDF format.

Note: The report can be accessed in the *Reports* section.



Date from 2021-11-07 to 2021-11-15

Select dates of the reports

Summary

Sort table content

Hide the users from given organization

Organization/User	Sessions total time	Active time	Idle time	Productivity	Sessions	Servers
Total	10:24	1:43	8:41	16%	178	17
Unassigned		1:43	8:41	16%	178	17
admin	9:11	0:47	8:24	8%	71	9
anonymous	0:05	0:05	0:00	87%	3	1
asd	0:52	0:39	0:13	74%	73	4
fudoportal	0:02	0:04	-1:58	100%	3	1
fudoportaldwa	0:01	0:06	-1:55	100%	6	1
sekoo	0:10	0:02	0:08	19%	22	5

Related topics:

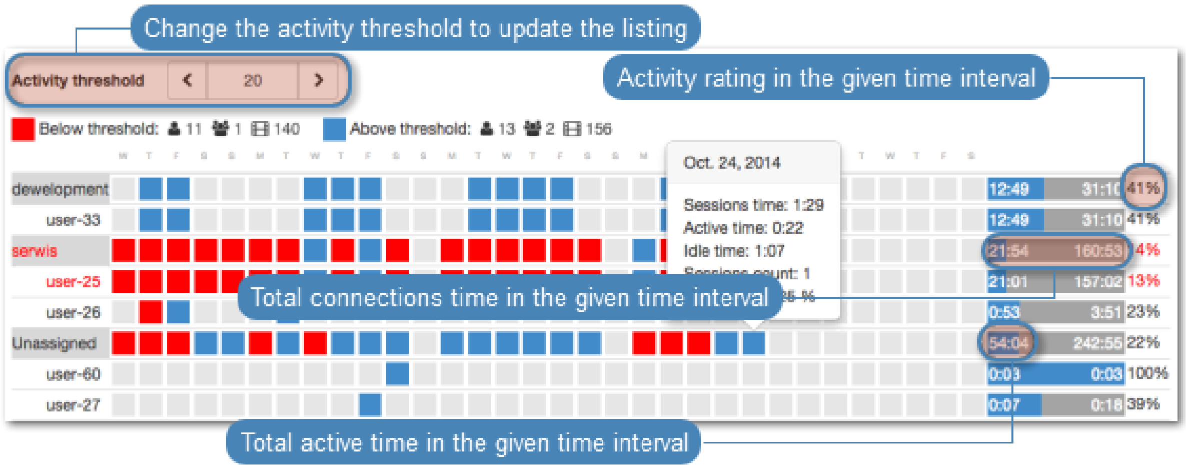
- *Productivity analysis - Sessions analysis*
- *Productivity analysis - Comparison*
- *Sessions*

21.2 Sessions analysis

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

Users activity rating allows identifying sessions which do not exceed the required user activity level. Further material analysis helps determining the reason for low activity in the given session and draw relevant conclusions.

Note: The listing does not cover time periods longer than 31 days. In case the defined time interval is longer than that, only data from the first 31 days is presented.



Change the activity threshold to update the listing

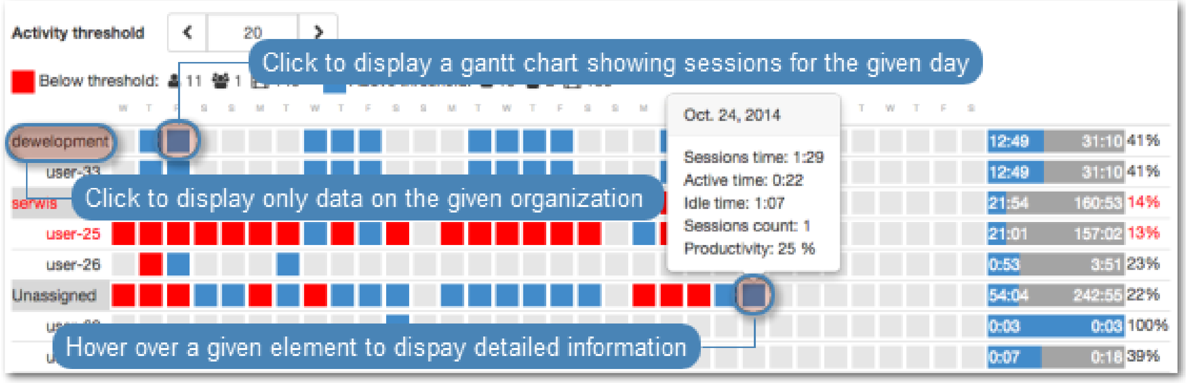
Activity rating in the given time interval

Total connections time in the given time interval

Total active time in the given time interval

Oct. 24, 2014

Sessions time: 1:29
Active time: 0:22
Idle time: 1:07
Sessions count: 1



Click to display a gantt chart showing sessions for the given day

Click to display only data on the given organization

Hover over a given element to dispay detailed information

Oct. 24, 2014

Sessions time: 1:29
Active time: 0:22
Idle time: 1:07
Sessions count: 1
Productivity: 25 %

Related topics:

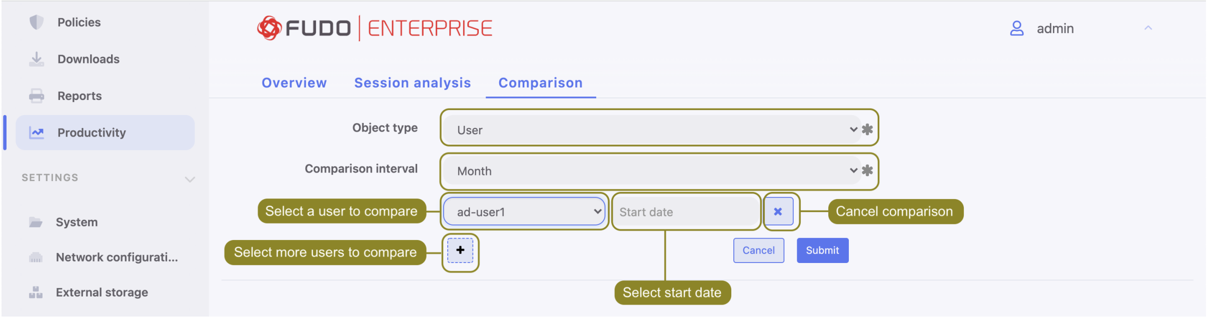
- *Productivity analysis - Overview*
- *Productivity analysis - Comparison*

21.3 Activity comparison

Productivity module enables comparing users/organizations activity in given time periods.

To compare users/organizations, proceed as follows.

1. Select *Management* > *Productivity*.
2. Select the *Comparison* tab.
3. Select object types being compared: `User` or `Organization`.
4. Select the time interval: `Month`, `Quarter`, `Half year`, or `Year`.
5. Add objects to the comparison and define starting date for each object.



Object type: User

Comparison interval: Month

Select a user to compare: ad-user1

Select start date: Start date

Cancel comparison

Select more users to compare

6. Click *Confirm* to compare selected objects.

Related topics:

- *Productivity analysis - Sessions analysis*
- *Productivity analysis - Overview*
- *Sessions*

CHAPTER 22

Administration

This section covers Fudo Enterprise administration topics.

22.1 System

22.1.1 Date and time

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

Warning:

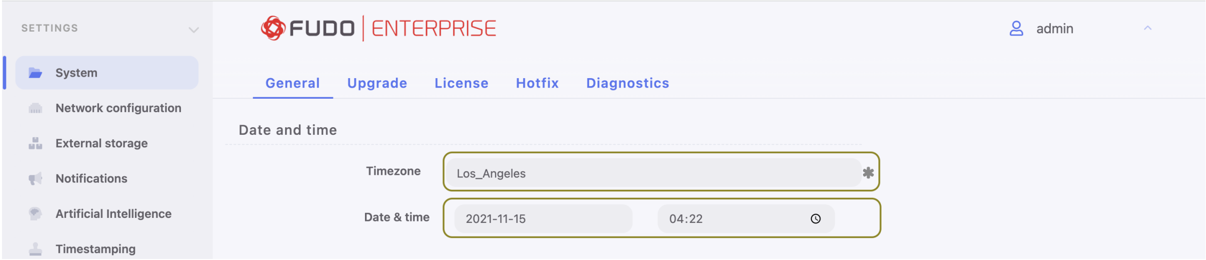
- It is strongly advised for the date and time settings to be obtained from a reliable NTP server. Changing date and time settings manually may result in system malfunction.
- Date and time synchronization with NTP server is required in *cluster configurations*.

Changing date and time settings

Note: Manual time setting is disabled if there are NTP servers configured.

To change the Fudo Enterprise's system clock settings, proceed as follows.

1. Select *Settings > System*.
2. Change date and time parameters in the *Date and time* section.



Timezone: Los_Angeles

Date & time: 2021-11-15 04:22

3. Click *Save*.

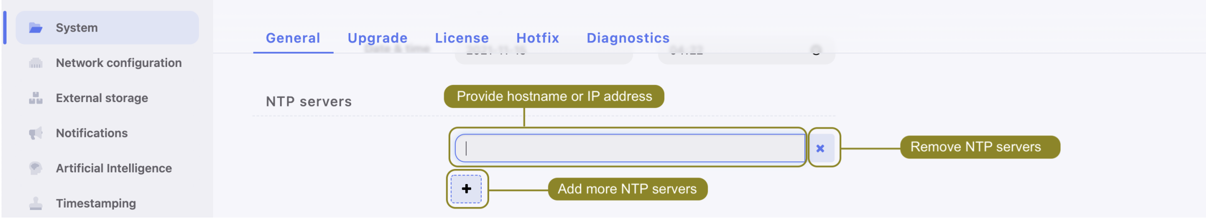
Time servers configuration

Note: NTP servers ensure that the system time on all IT infrastructure devices is synchronized. Using NTP servers guarantees that the timestamp of the recorded session matches the time settings on the monitored server.

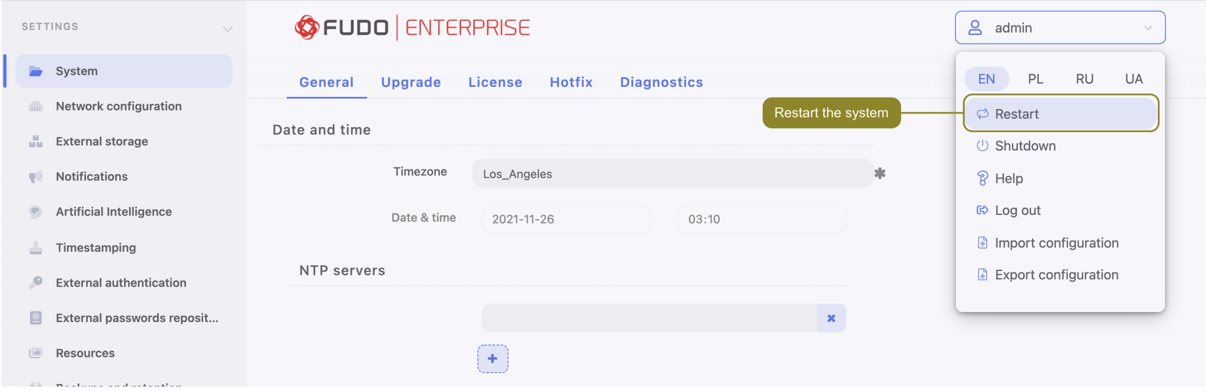
Adding an NTP server definition

To add an NTP server definition, proceed as follows.

1. Select *Settings* > *System*.
2. Click + in the *NTP servers* section to add an NTP server.
3. Enter NTP server IP address or host name.



4. Click *Save*.
5. Select *Restart* from user menu to reboot Fudo Enterprise and apply new time settings.



Timezone: Los_Angeles

Date & time: 2021-11-26 03:10

Note: After every change or removal of the NTP server definition, run *Restart* option.

Related topics:

- *Timestamping*

22.1.2 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.
4. Click *Save*.

Configuring user portal SSL certificate

1. Select *Settings > System*.
2. In the *Fudo HTTPS certificate* section, click the *Browse* button next to the *HTTPS Certificate* field in the *HTTPS certificate* section and point to the location of the SSL certificate file in PEM format.
3. Click the *Browse* button next to the *HTTPS Private Key* field and point to the location of the SSL key definition.
4. Provide *Private key passphrase*.
5. Click *Save*.

Configuring user portal CA certificates

1. In the *User portal CA certificates* section, click the *Browse* button next to the *CA certificates* field and point to the location of the CA certificates. These certificates allow users login in to the Access Gateway.
2. Click *Save*.

Related topics:

- *Security measures*
- *Servers*

22.1.3 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*

22.1.4 SSH access

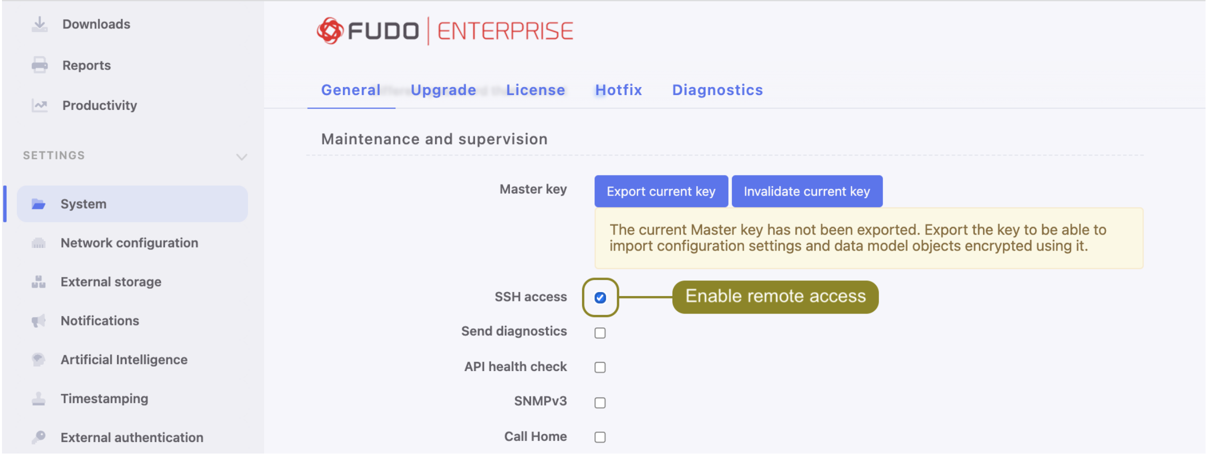
SSH access option enables remote access to Fudo Enterprise for servicing and maintenance purposes.

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

Enabling SSH access

To enable SSH access, proceed as follows.

1. Select *Settings* > *System*.
2. Select *SSH access* option in the *Maintenance and supervision* section.



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 ☑

Enable remote access

Send diagnostics □

API health check □

SNMPv3 □

Call Home □

3. Click *Save* button.

Related topics:

- *Network interfaces configuration*

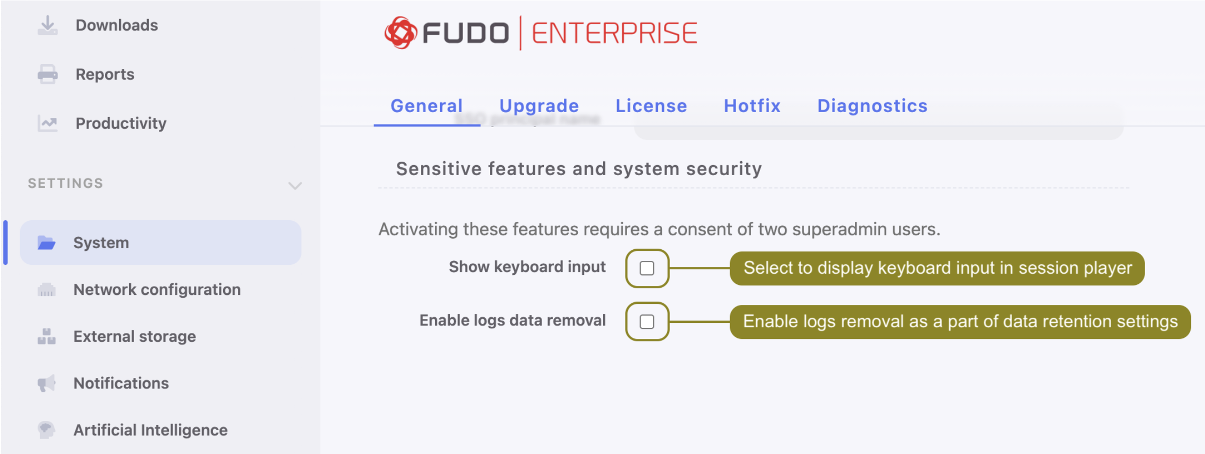
22.1.5 Sensitive features

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

Note: Keystrokes are not displayed in the session player by default. Enabling keystrokes display requires a consent from two superadmin users.

To enable sensitive features, proceed as follows.

1. Select *Settings > System*.



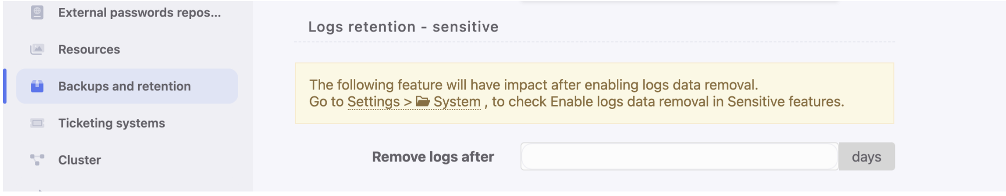
Sensitive features and system security

Activating these features requires a consent of two superadmin users.

Show keyboard input □ Select to display keyboard input in session player

Enable logs data removal □ Enable logs removal as a part of data retention settings

2. Select *Show keyboard input* in the *Sensitive features* section to initiate the feature.
3. Select *Enable logs data removal* option.
   - this option is combined with Retention settings, where you can specify when logs data should be removed.



Logs retention - sensitive

The following feature will have impact after enabling logs data removal.
Go to Settings > System , to check Enable logs data removal in Sensitive features.

Remove logs after days

4. Click *Save*.
5. Notify another system administrator that the features mentioned above have been initiated and require a confirmation.

Related topics:

- *Viewing sessions*

22.1.6 System update

Note:

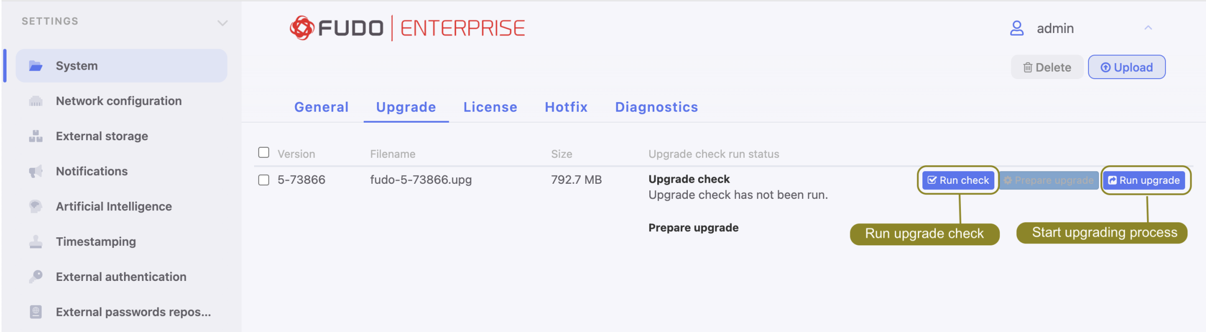
- The system update process does not influence the system configuration or the session data stored on Fudo Enterprise.
- The storage usage may temporarily increase during system update.

22.1.6.1 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 Enterprise technical support before proceeding with upgrading the system.
- During the system update, all current users' connections will be terminated. Use the *Deny new connections* option in the *User authentication and sessions* section of the system settings menu to *limit the number* of active connections before performing system upgrade.
- After running system update, Fudo Enterprise will restart automatically. Connect the USB flash drive containing the encryption key to the USB port before proceeding or have the passphrase ready in case of virtual machine instance. Note that entering incorrect passphrase will restart the machine in previous revision.
- In case of cluster configuration, upgrade slave node first and after successful upgrade, move onto upgrading the master node.
- For clients who are upgrading from 4.x Fudo Enterprise versions, a new masterkey will be generated during the upgrade. Users are encouraged to export and backup the newly generated key. Refer to the *Configuration encryption* topic to find out more about the system masterkey.

1. Select *Settings > System*.
2. Select the *Upgrade* tab.
3. Click *Upload*.
4. Browse the file system to find and upload the update image file (`.upg`).
5. Optionally, click *Run check* to verify if the current configuration and data model objects are compatible with the new system revision.



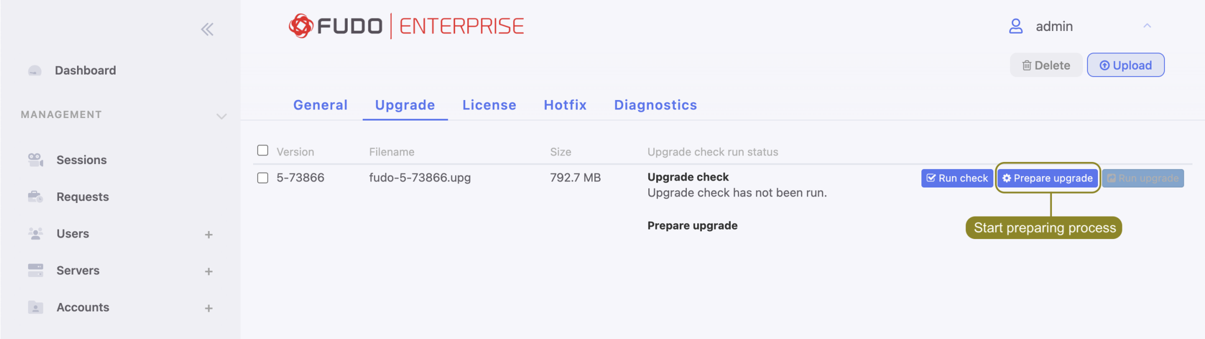
□ Version	Filename	Size	Upgrade check run status
□ 5-73866	fudo-5-73866.upg	792.7 MB	**Upgrade check** Upgrade check has not been run. **Prepare upgrade**

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
□ 5-73866	fudo-5-73866.upg	792.7 MB	**Upgrade check** Upgrade check has not been run. **Prepare upgrade**

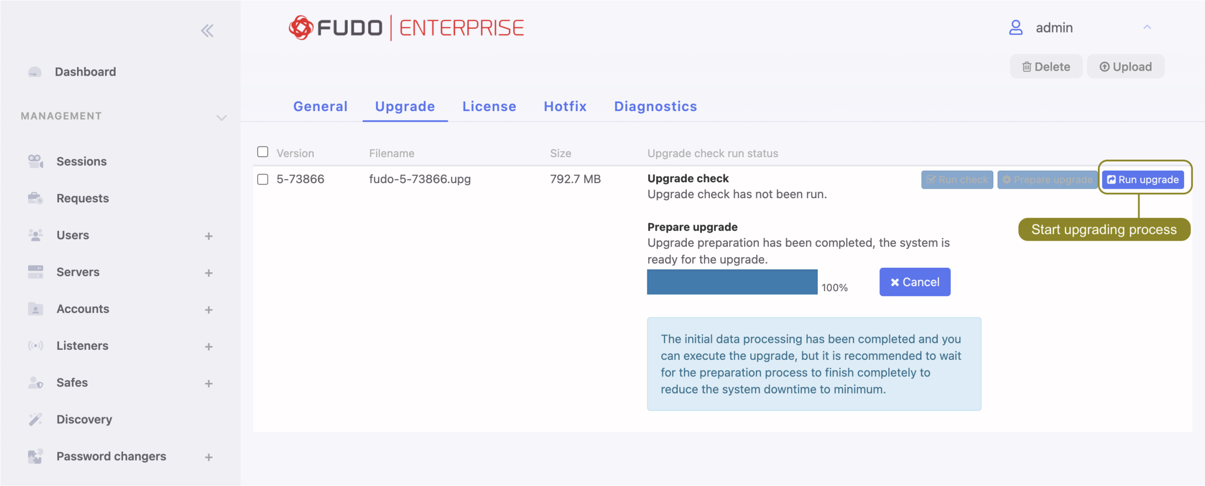
Note:

- 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.
- 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
□ 5-73866	fudo-5-73866.upg	792.7 MB	**Upgrade check** Upgrade check has not been run. **Prepare upgrade** Upgrade preparation has been completed, the system is ready for the upgrade. 100%

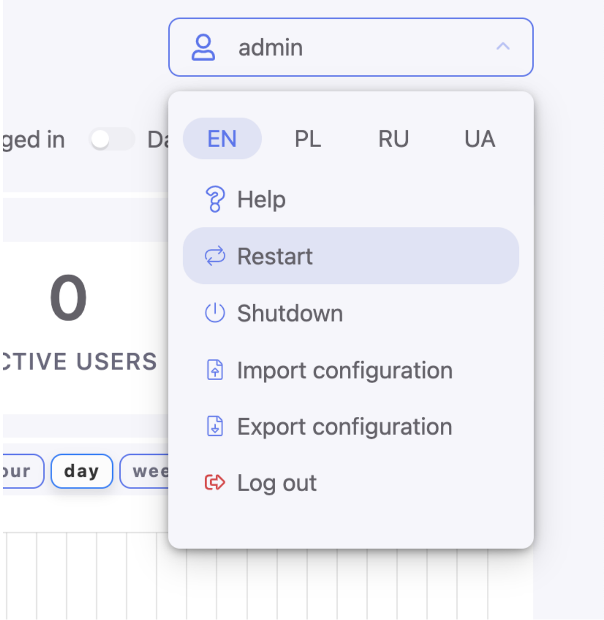
The initial data processing has been completed and you can execute the upgrade, but it is recommended to wait for the preparation process to finish completely to reduce the system downtime to minimum.

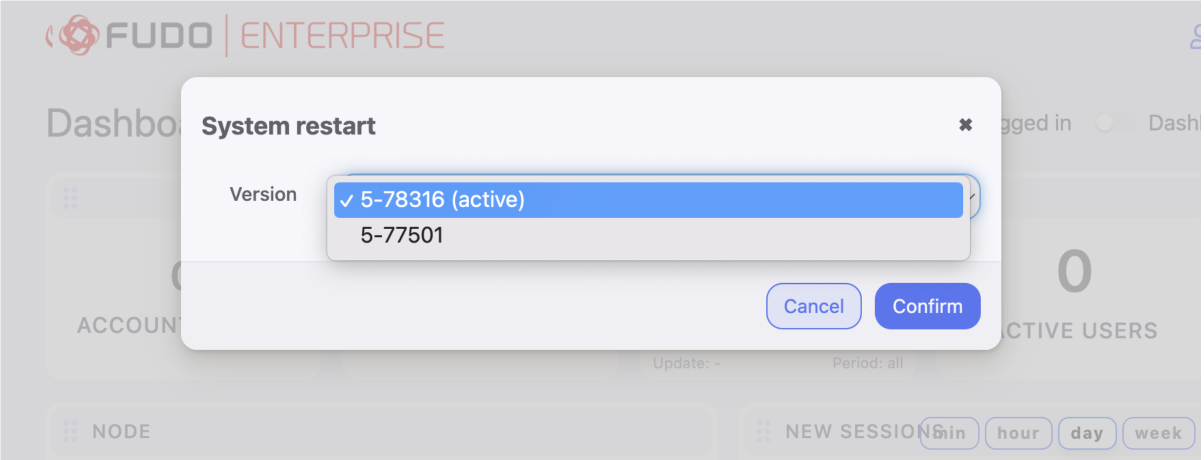
8. Click *Confirm* to proceed with system update.

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

22.1.6.2 Restoring previous system version

In addition to the current system version, Fudo Enterprise stores the previous revision, allowing for restoring the system to its previous state. In the event of an unsuccessful system update, Fudo Enterprise detects the problem during system restart and restarts itself using the previous system revision. It's also possible to bring the previous version back to the system via the *Restart* option from the options menu:





System restart

Version

✓ 5-78316 (active)

5-77501

> **Warning:** Rollback process will result in the loss of **all sessions recorded** on the new system version and **any system configuration changes**. **All the object configurations** that were created, changed or recorded between the current and the previous system versions will be deleted. This includes the **password changers** activity. If any passwords were changed during the newer version's usage, restarting Fudo will lead to lost access to corresponding systems.

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

22.1.6.3 Deleting upgrade snapshot

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

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

1. Select *Settings* > *System*.
2. Select the *Upgrade* tab.
3. Click *Remove upgrade snapshot*.
4. Confirm deleting previous system version.

Related topics:

- *System version restore*
- *Restarting system*

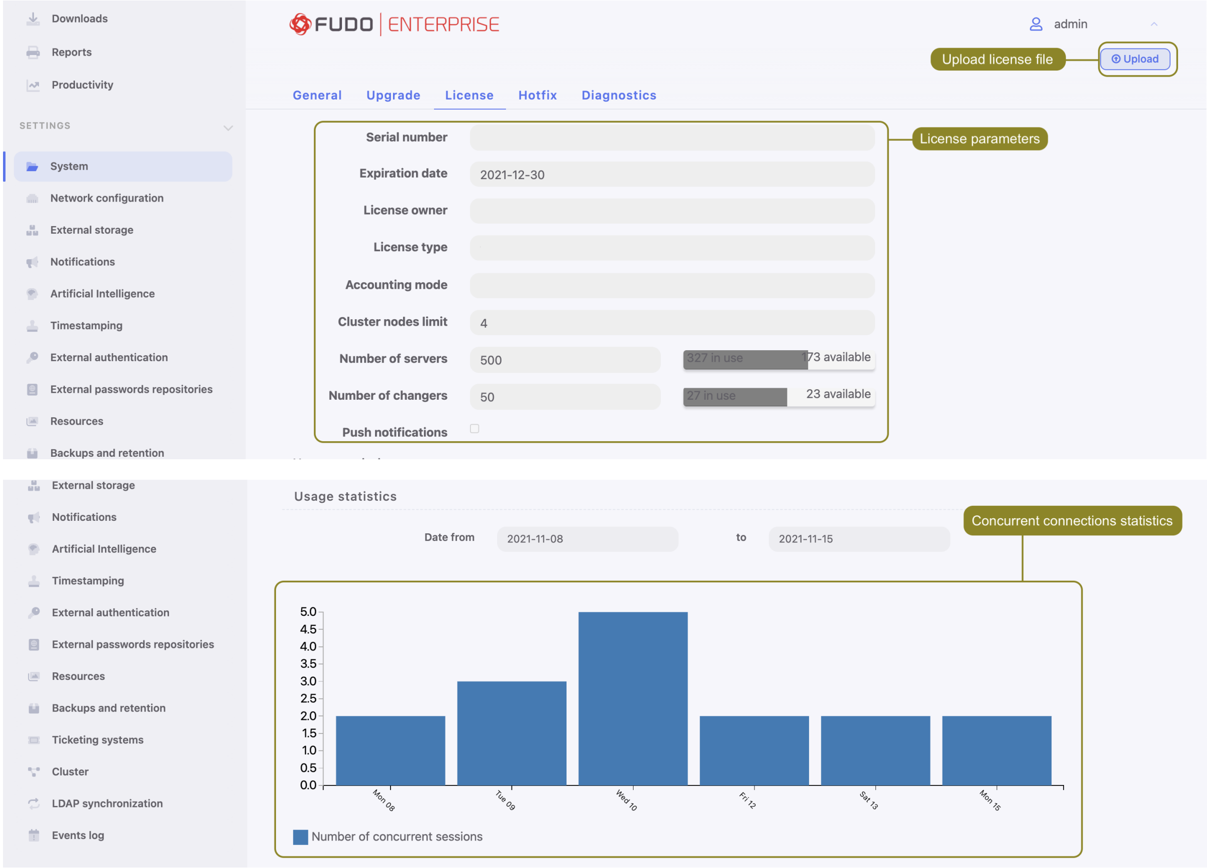
22.1.7 License

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*.



Upload license file

License parameters

Serial number:
Expiration date: 2021-12-30
License owner:
License type:
Accounting mode:
Cluster nodes limit: 4
Number of servers: 500 — 327 in use — 173 available
Number of changers: 50 — 27 in use — 23 available
Push notifications: □

Usage statistics

Date from 2021-11-08 to 2021-11-15

Concurrent connections statistics

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

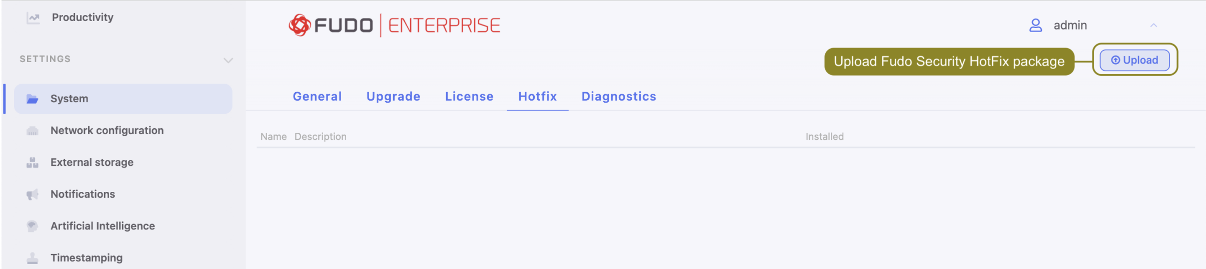
Related topics:

- *System*

22.1.8 Hotfix

The Hotfix feature allows the administrator to upload a minor fix through the Fudo Admin Panel. The fix package is delivered by the Fudo Support Team. No additional support work or machine upgrade will be required.

The Hotfix package has Fudo Security HotFix extension (`.fshf`), and can be uploaded by the administrator from the Hotfix tab:



The hotfixes cannot be removed or deinstalled as they disappear after the next upgrade.

Related topics:

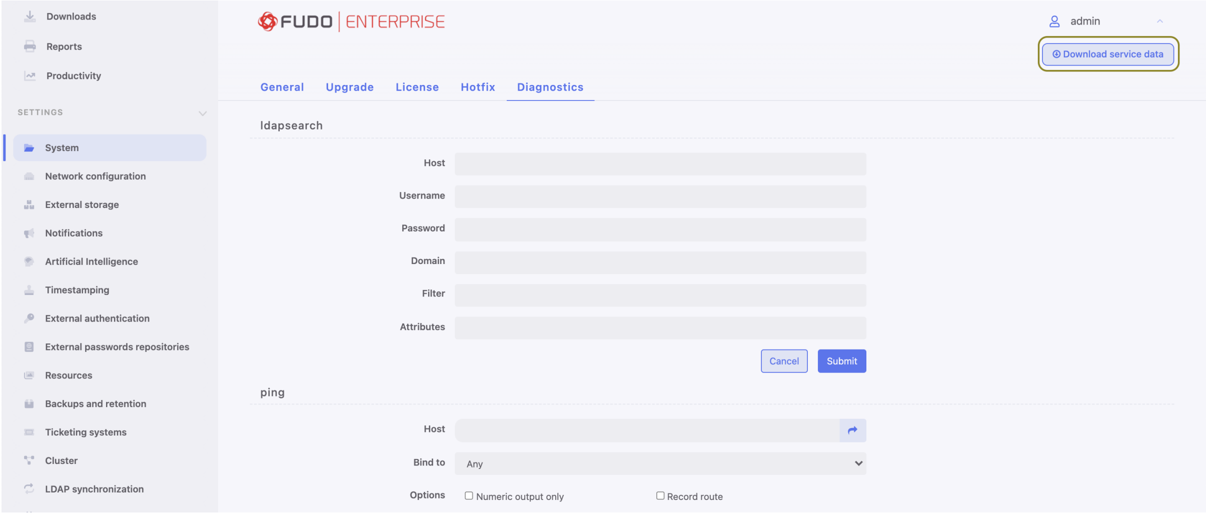
- *System update*
- *System*

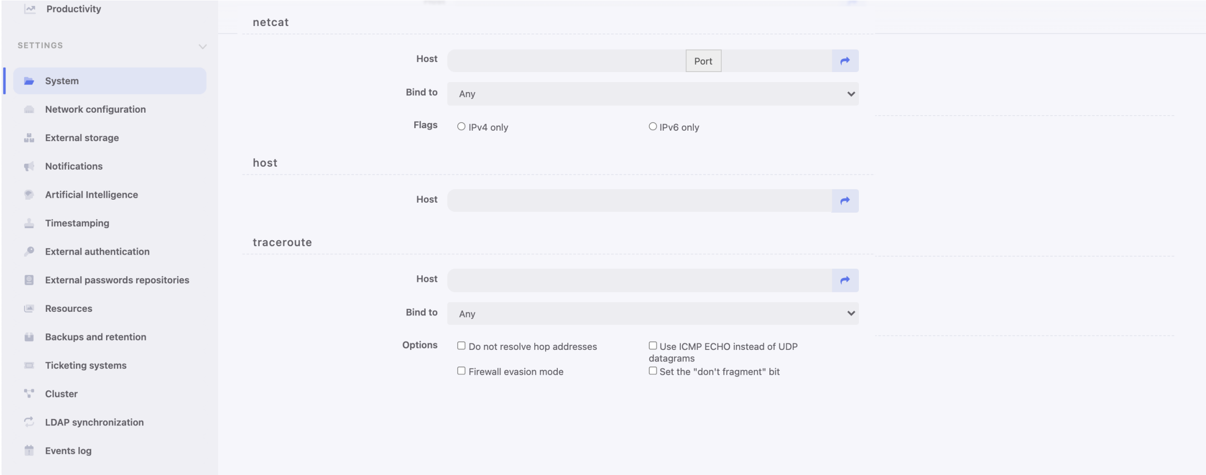
22.1.9 Diagnostics

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.





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
ldapsearch	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	`netcat` 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 Enterprise 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*

22.1.10 Configuration encryption

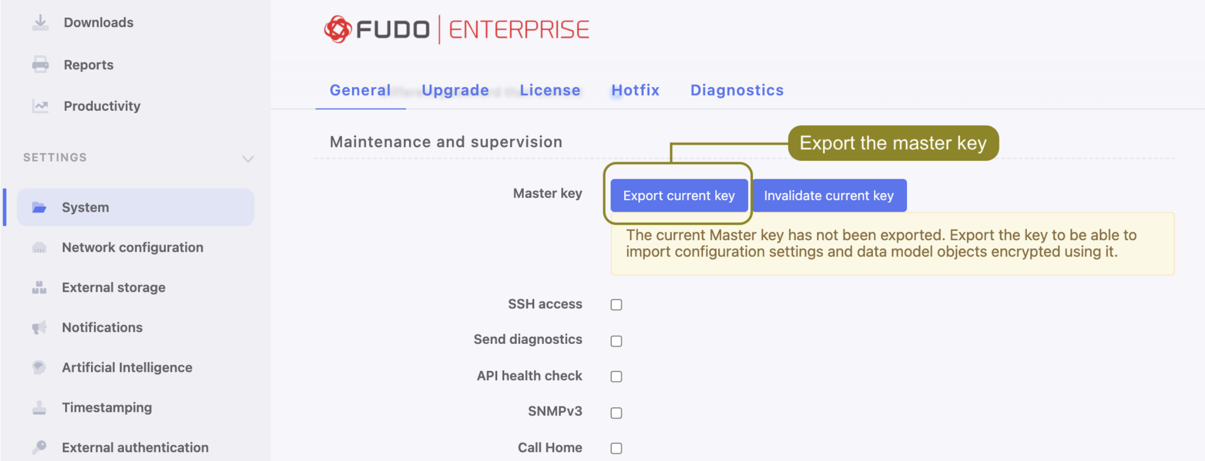
The *Master key* enables encrypting sensitive configuration parameters, system backups and external storage volumes. It also allows for recovering internal storage encryption key in case the pen drives containing encryption key are lost or damaged.

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*.



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 ☐

Send diagnostics ☐

API health check ☐

SNMPv3 ☐

Call Home ☐

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:

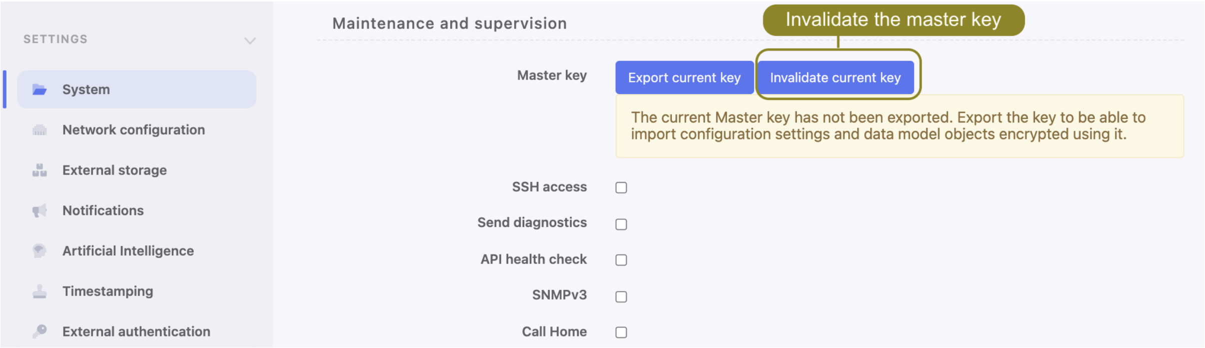
```
openssl x509 -req -in req.pem -signkey privkey.pem -out cert.pem
```

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*.



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 ☐
- Send diagnostics ☐
- API health check ☐
- SNMPv3 ☐
- Call Home ☐

3. Confirm invalidating the current key.
4. Make sure to *export the newly generated key*.

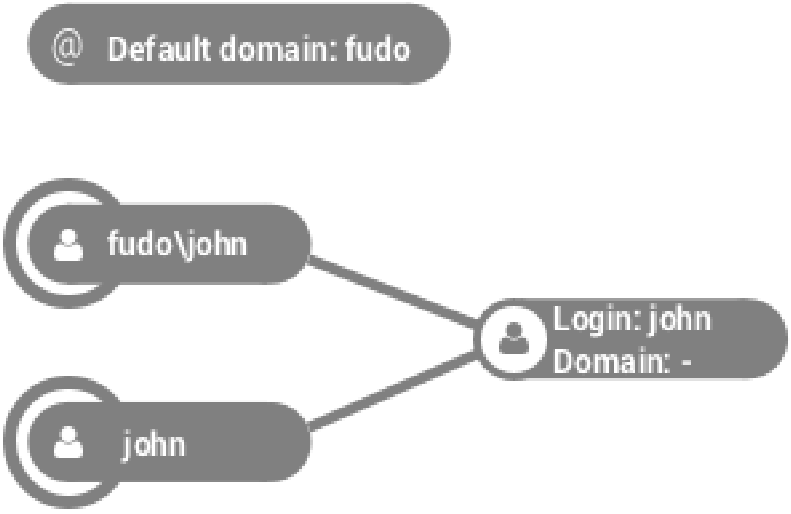
Related topics:

- *Security measures*

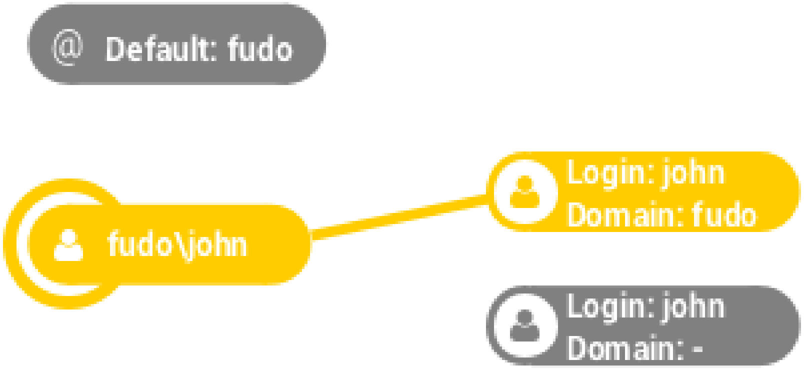
22.1.11 Default domain

Note:

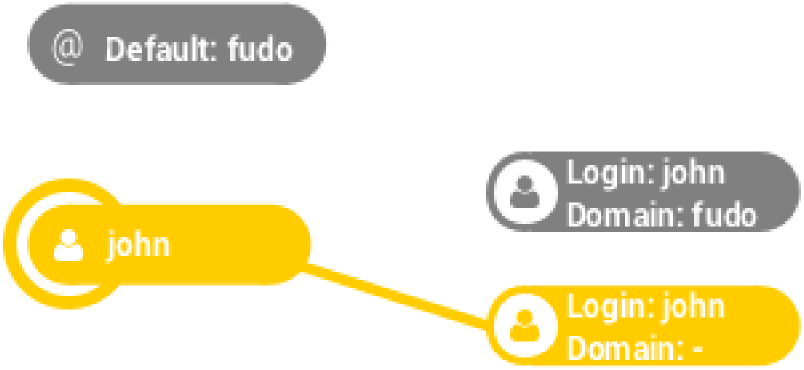
- In case the default domain is specified and the user does not have a domain defined, when logging in, the user can either include the domain (e.g. `john_smith@domain`) or leave it out (e.g. `john_smith`).



- 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 Enterprise will match the user that has the domain explicitly specified.



In case the user does not provide the domain, Fudo Enterprise 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:

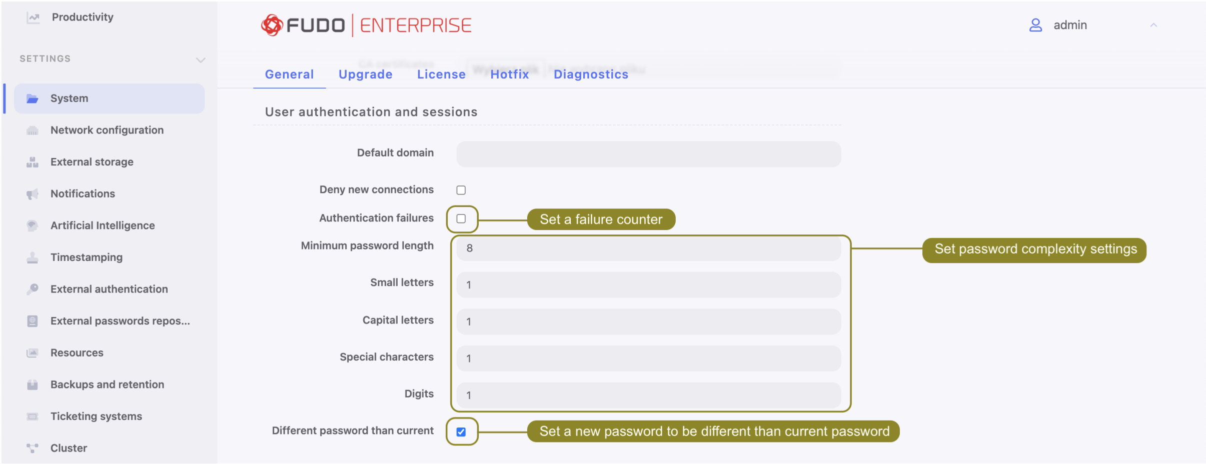
- *Creating a user*
- *Users synchronization*

22.1.12 Password complexity

Fudo Enterprise 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 *Authentication failures* to set a counter of the login failures.
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.



User authentication and sessions

Default domain

Deny new connections □

Authentication failures □

Minimum password length 8

Small letters 1

Capital letters 1

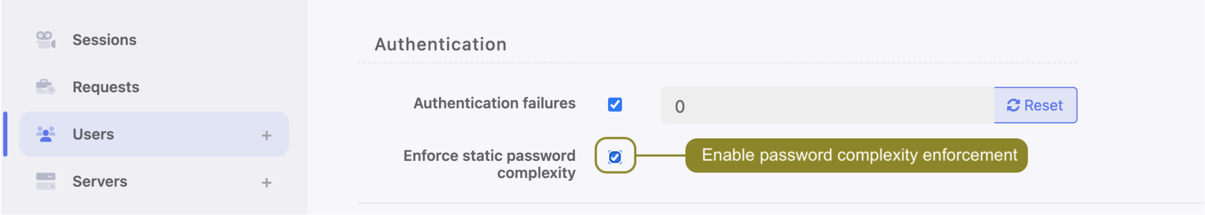
Special characters 1

Digits 1

Different password than current ☑

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

Enforce static password complexity ☑

Enabling password complexity will trigger password change for users with the *Enforce static password complexity* option enabled whose passwords do not comply with the complexity settings. The password will have to be changed upon logging into the *Access Gateway*.

Related topics:

- *Creating a user*
- *Users synchronization*

22.1.13 Single Sign On

Single Sign On allows to automatically authenticate the user when logging into the system. Fudo Enterprise allows to set the Single Sign On functionality for both Admin Panel and User Portal (Access Gateway).

22.1.13.1 Setting up Fudo Enterprise for SSO

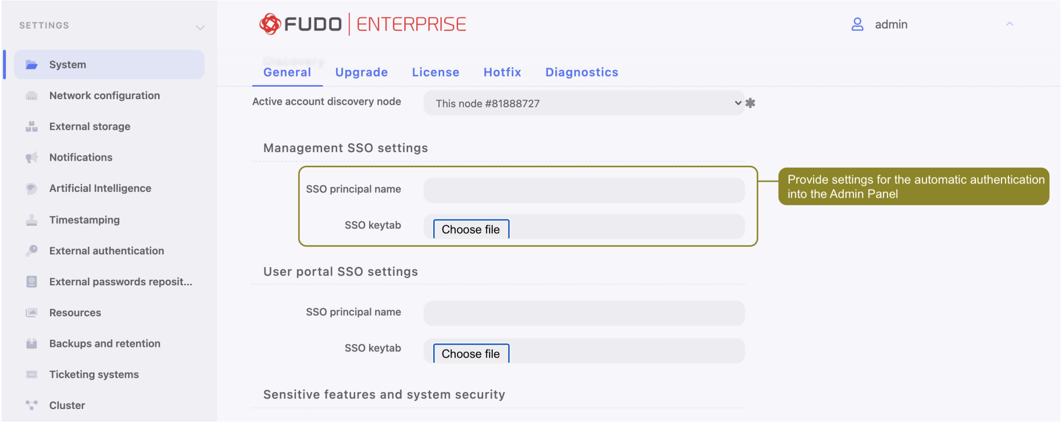
1. Set Fudo Enterprise hostname to `hostname.yourdomain.local`.
    - Select *Settings > Network configuration*.
    - Switch to the *Name & DNS* tab.
    - Enter `hostname.yourdomain.local` in the *Hostname* field.
2. Configure DNS server to point to a DNS server in the *yourdomain.local* domain.
    - Click *Add new* to define new DNS server.
    - Enter DNS server IP address.
    - Click *Save*.
3. Add user, that has an AD domain account.
    - *Set up LDAP users synchronization* or
    - *add user account manually*, with Active Directory eternal authentication method.

22.1.13.2 Single Sign On in Admin Panel

> **Warning: Single Sign On in Admin Panel** is available to set for a user with `superadmin` role only, and can be used by the users with `operator`, `admin` and `superadmin` roles.

In order to define SSO service parameters in system settings, follow the steps:

- Select *Settings > System*.
- In the *Management SSO settings* section, provide service identifier that will match the user account with the service instance.
- Upload the keytab file containing admin's ID and encryption keys for encrypting and decrypting Kerberos tickets.



Active account discovery node: This node #81888727

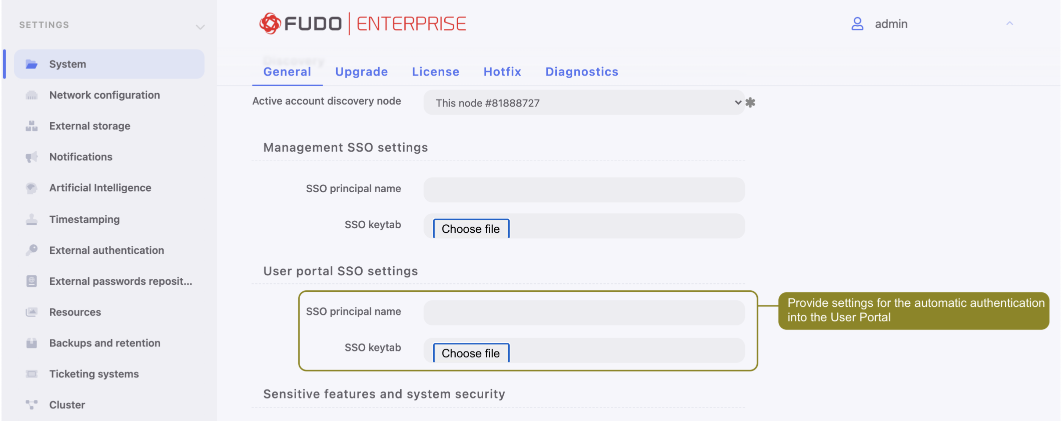
Provide settings for the automatic authentication into the Admin Panel

- Click *Save*.

22.1.13.3 Single Sign On in User Portal

In order to define SSO service parameters in system settings, follow the steps:

- 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.



Active account discovery node: This node #81888727

Provide settings for the automatic authentication into the User Portal

- Click *Save*.

22.1.13.4 Setting up domain controller

1. Add user account, which will be used by the *User Portal* or *Admin Panel* to communicate with the *yourdomain.local* domain.

Note: When adding the account, enable the *Password does not expire* option.

2. On the DNS server add forward and reverse DNS entries for *hostname.yourdomain.local.*
3. Create a Kerberos ticket for Fudo Enterprise running the following command in the Powershell or CMD console:

```
ktpass -princ HTTP/hostname.yourdomain.local@yourdomain.local -mapuser
sso\username -pass password. - ptype KRB5_NT_PRINCIPAL -out hostname.yourdomain.
local.keytab
```

22.1.13.5 Setting up user workstations

1. Log in using credential of a user that will be connecting to servers.
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 address `hostname.yourdomain.local`.
8. Close settings window.

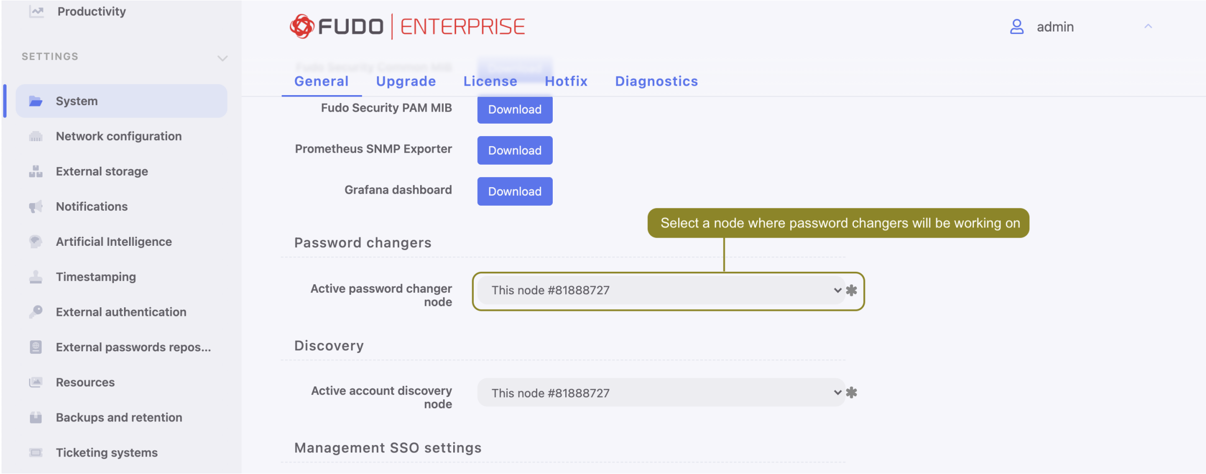
Related topics:

- *Creating a user*
- *Users synchronization*

22.1.14 Password changers - active cluster node

Active cluster node option determines the Fudo Enterprise 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.



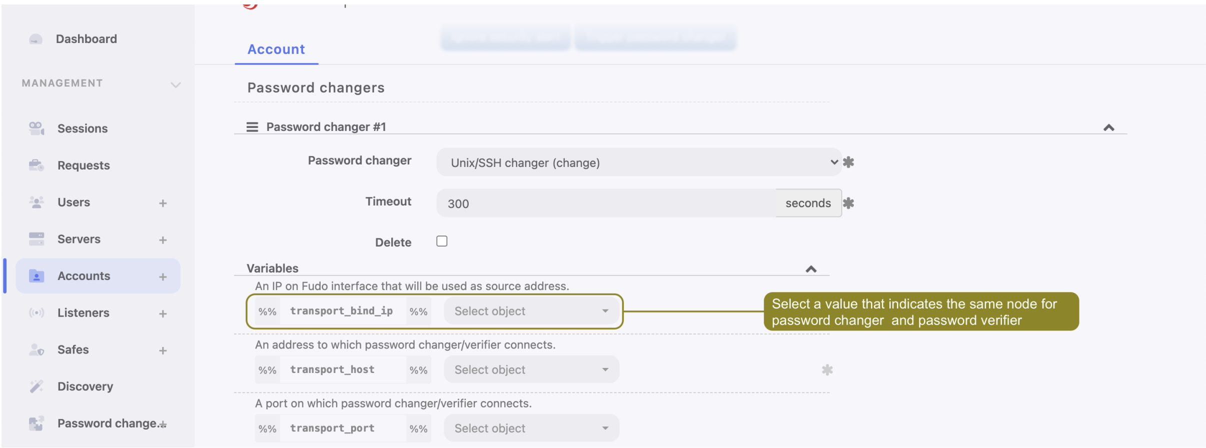
3. Click *Save*.

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

22.1.14.1 Cluster Password Changers

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

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



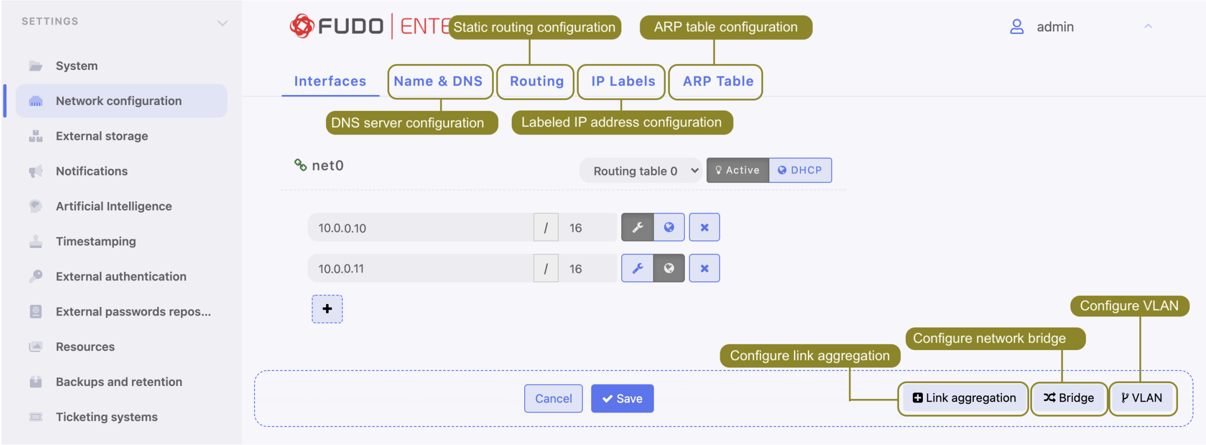
If the `transport_bind_ip` variable values indicate different cluster nodes, the configured password changer/verifier will be running on a node that set as an *Active cluster node for Password changers*.

Related topics:

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

22.2 Network settings

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



22.2.1 Network interfaces configuration

22.2.1.1 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.

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

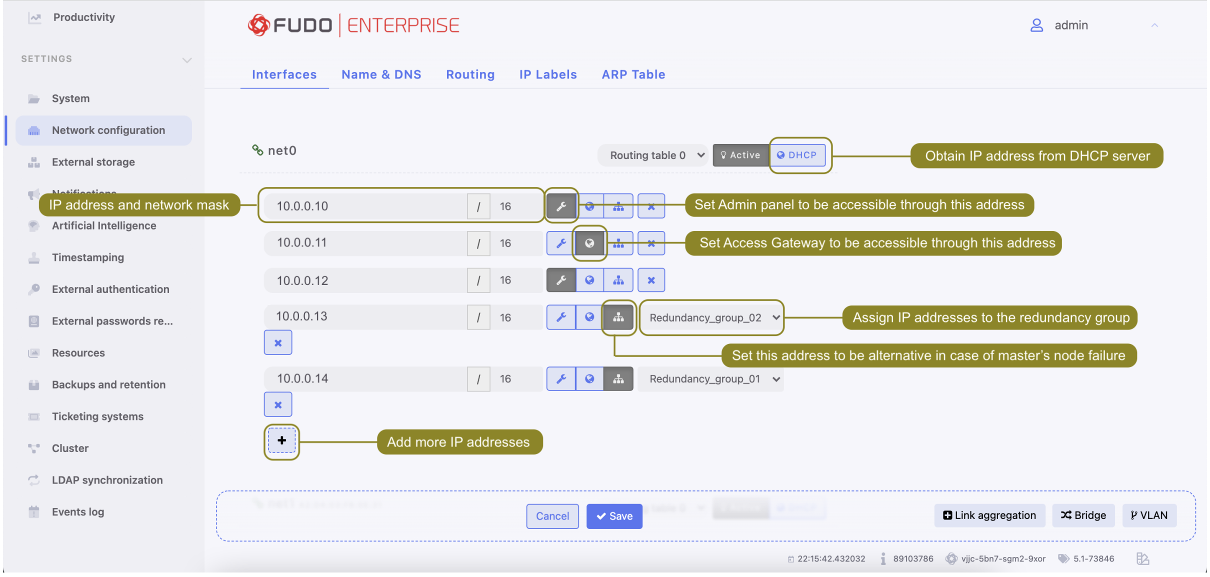
Note: Cluster IP address must be added manually on every cluster node, with the 品 option enabled.

● 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*.



10.0.0.10 / 16
10.0.0.11 / 16
10.0.0.12 / 16
10.0.0.13 / 16 Redundancy_group_02
10.0.0.14 / 16 Redundancy_group_01

Obtain IP address from DHCP server

IP address and network mask

Set Admin panel to be accessible through this address

Set Access Gateway to be accessible through this address

Assign IP addresses to the redundancy group

Set this address to be alternative in case of master's node failure

Add more IP addresses

22:15:42.432032 89103786 vjjc-5bn7-sgm2-9xor 5.1-73846

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

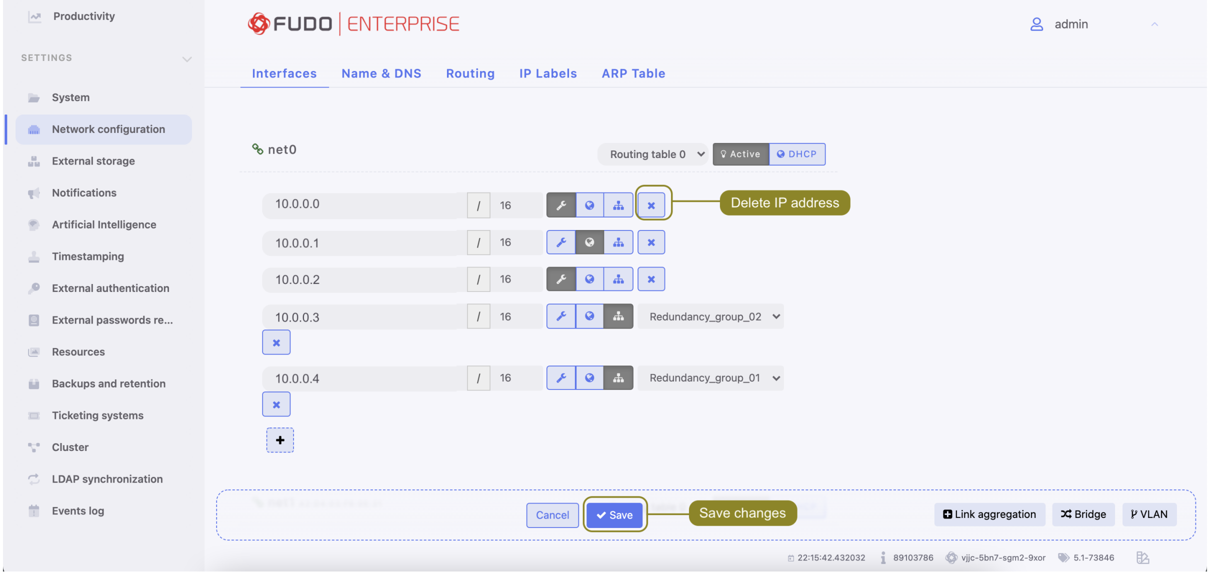
🔗	Interface active and connected.
⛓	Interface active but disconnected.
✖	Interface disabled.

Removing defined IP addresses

> **Warning:** Deleting an IP address will disable access to servers which had this IP configured in the *Local address* of the proxy server.

To delete an IP address assigned to a given network interface, proceed as follows.

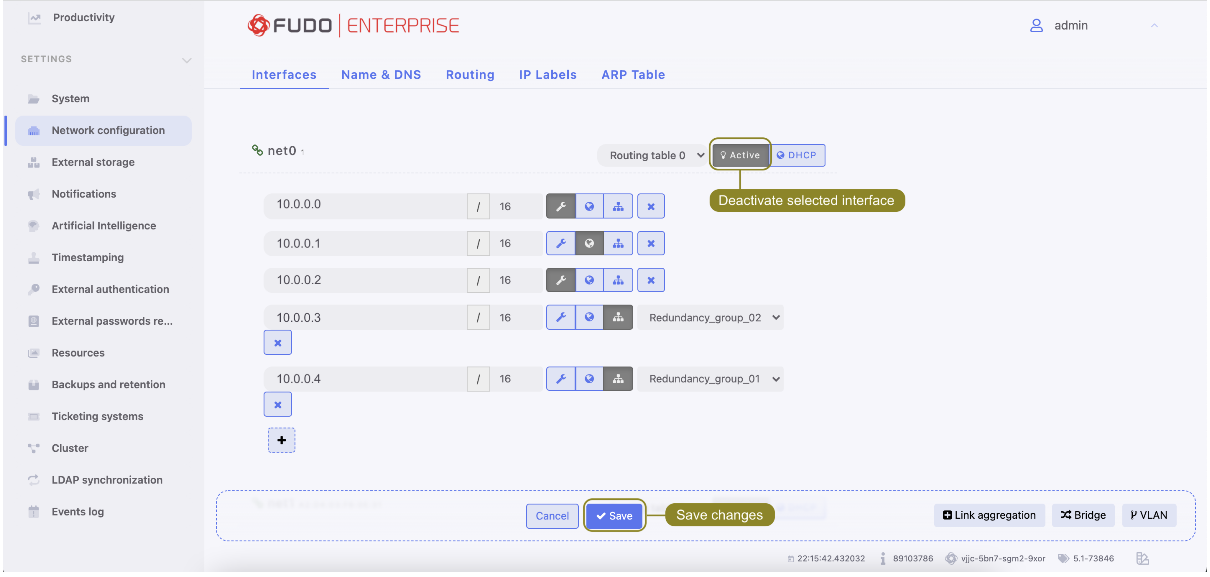
1. Select *Settings* > *Network configuration*.
2. Select desired IP address assigned to given network interface and click *x*.
3. Click *Save*.



Disabling network interface

To disable a network interface, proceed as follows.

1. Select *Settings* > *Network configuration*
2. Click the *Active* icon next to given interface to deactivate it.



10.0.0.0 / 16
10.0.0.1 / 16
10.0.0.2 / 16
10.0.0.3 / 16 Redundancy_group_02
10.0.0.4 / 16 Redundancy_group_01

Deactivate selected interface

Save changes

22:15:42.432032 89103786 vjjc-5bn7-sgm2-9xor 5.1-73846

3. Click *Save*.

22.2.1.2 Defining IP address using system console

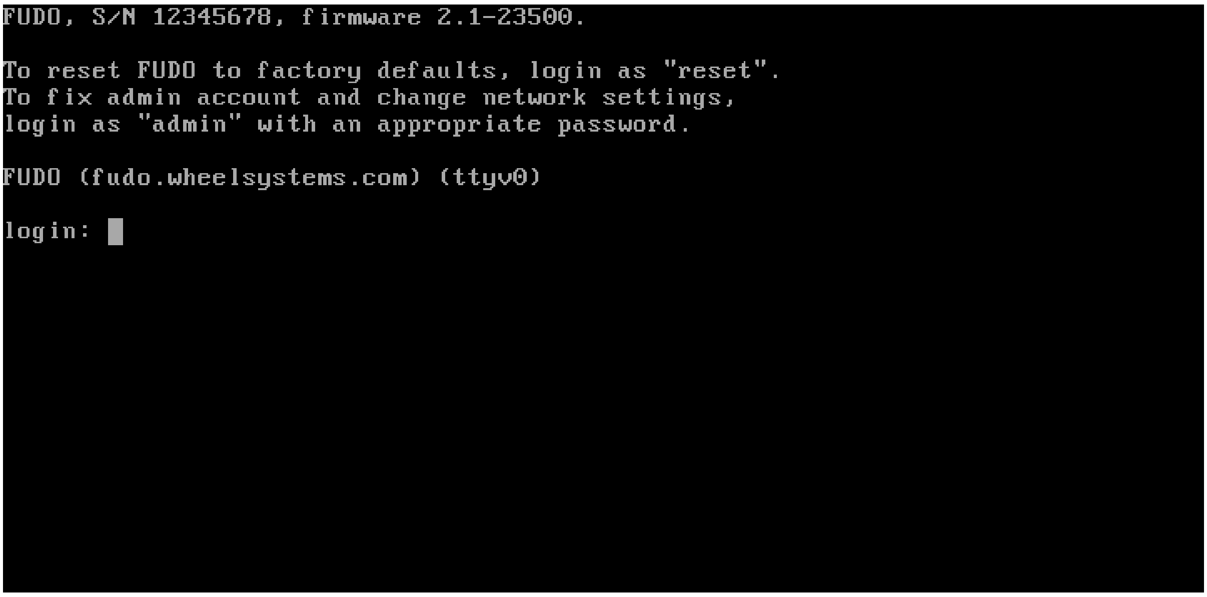
In case the web administration interface cannot be accessed, IP address can be defined using console connection.

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

Note: Default login credentials:

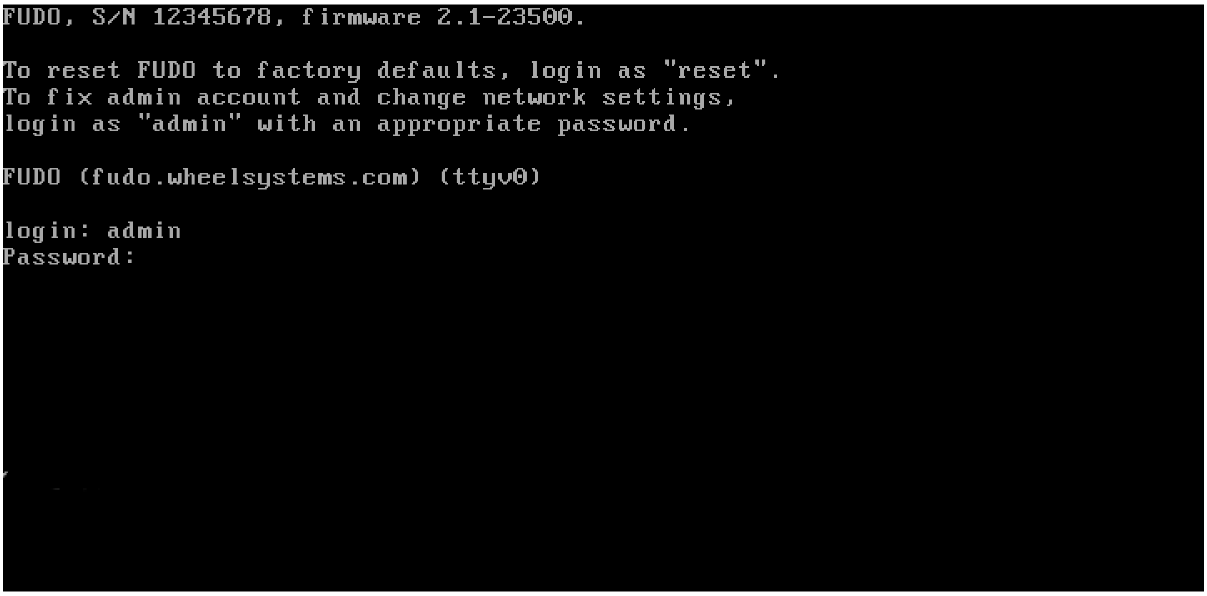
login: admin
password: proxycrypto

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



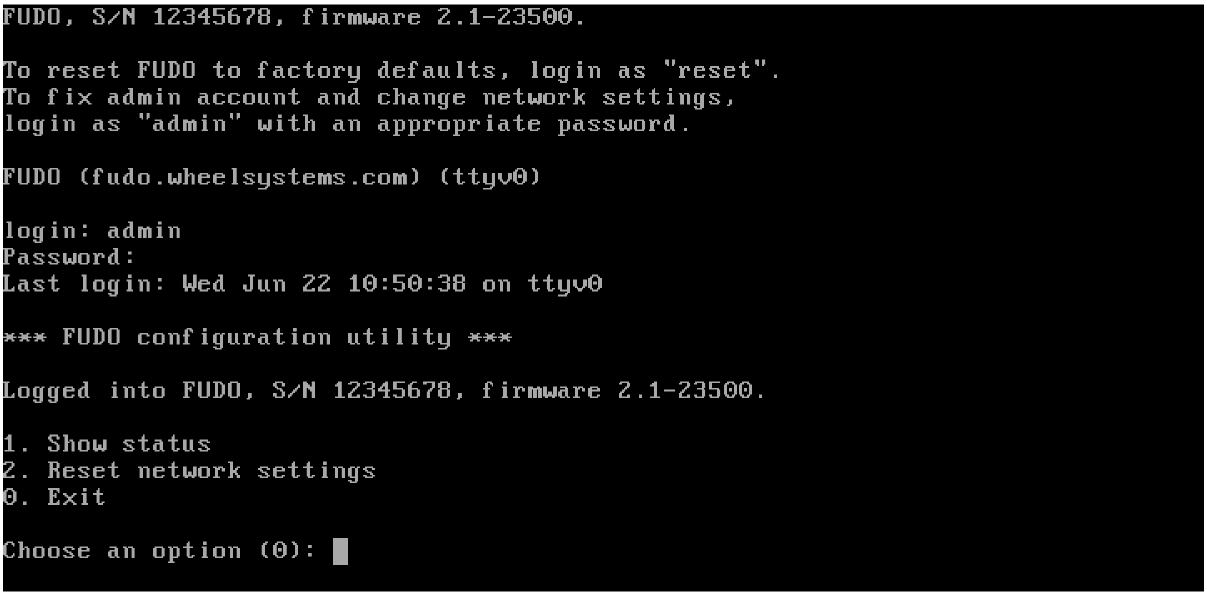
```
FUDO, S/N 12345678, firmware 2.1-23500.

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*.



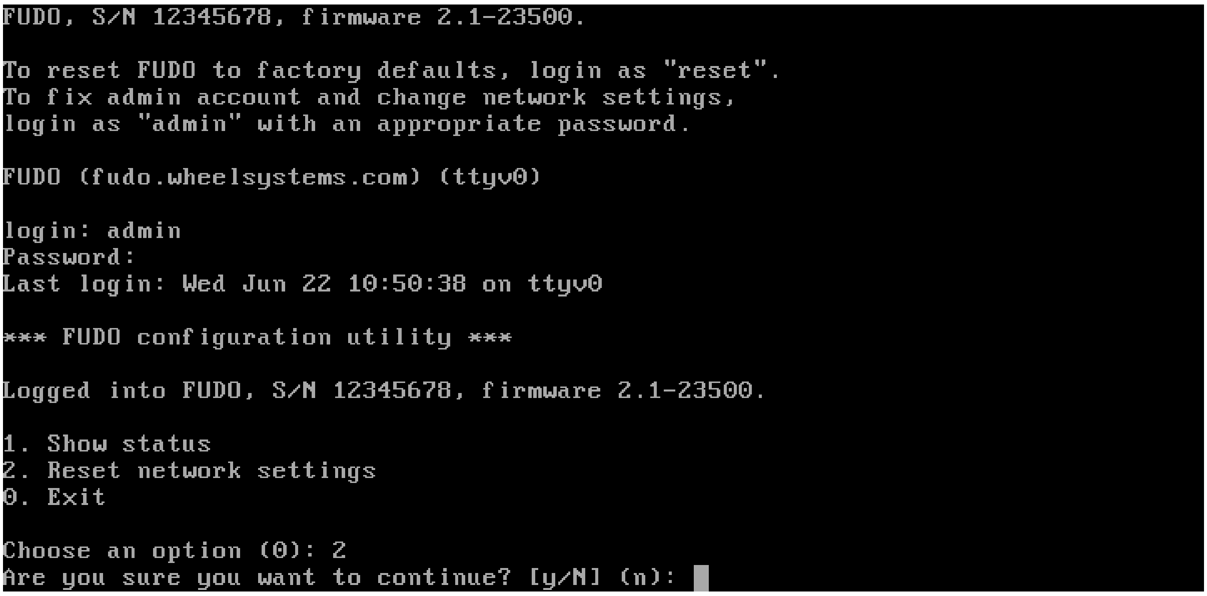
```
FUDO, S/N 12345678, firmware 2.1-23500.

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.



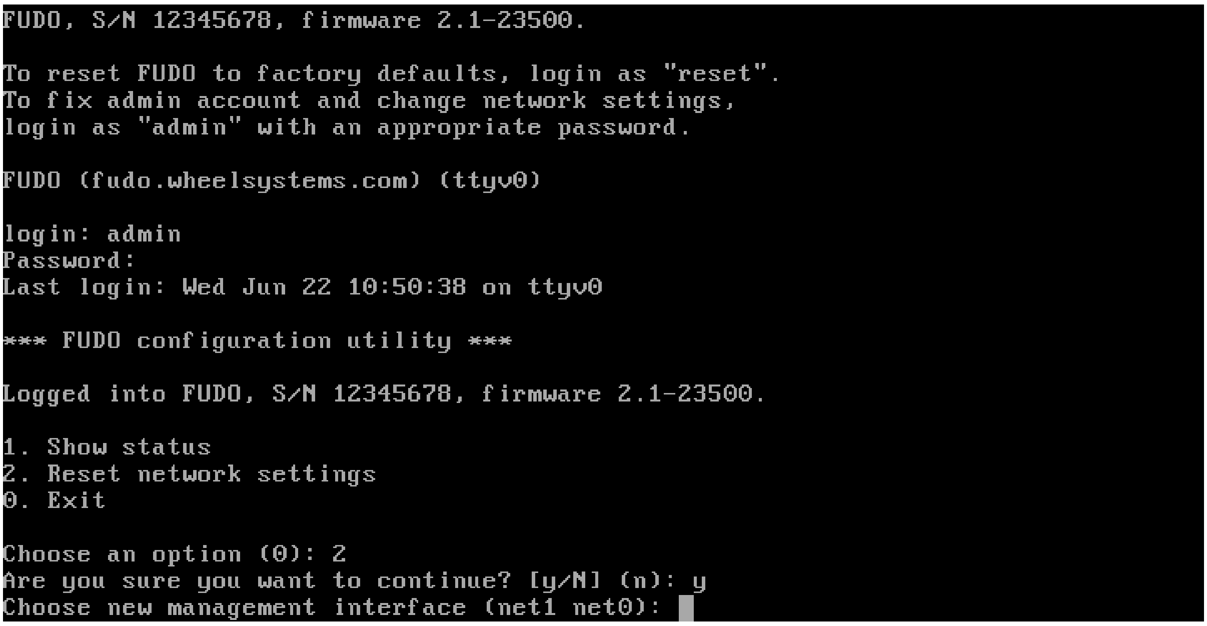
```
FUDO, S/N 12345678, firmware 2.1-23500.

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.



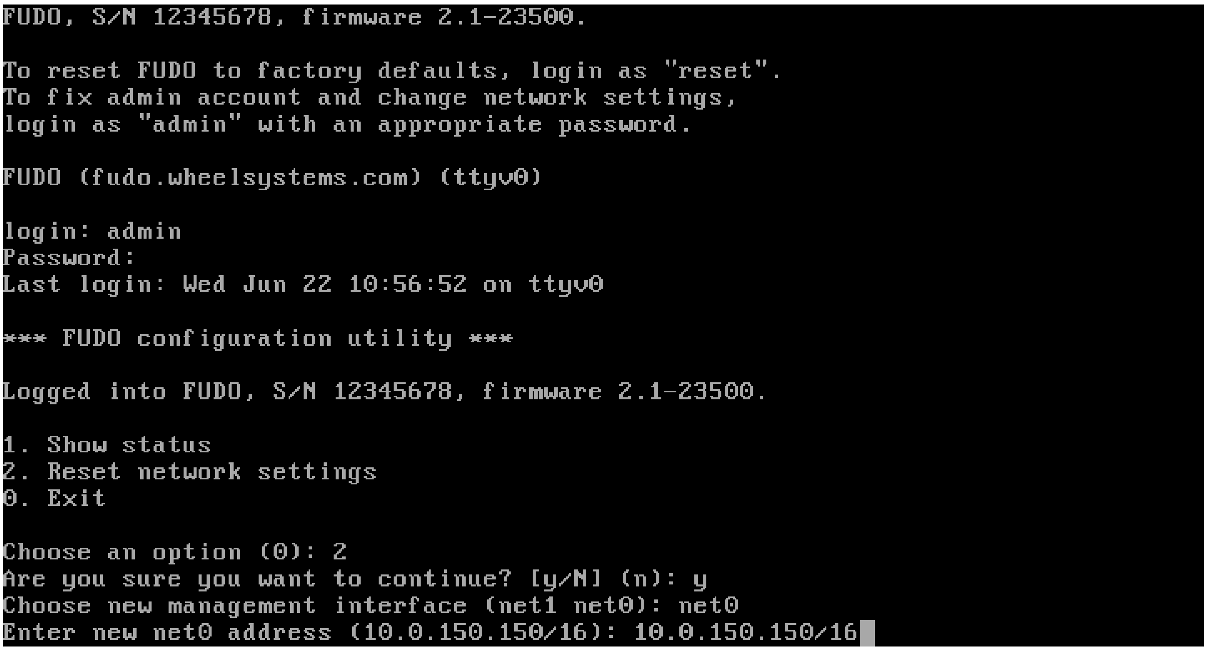
```
FUDO, S/N 12345678, firmware 2.1-23500.

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 Enterprise web interface is accessible through the management interface).



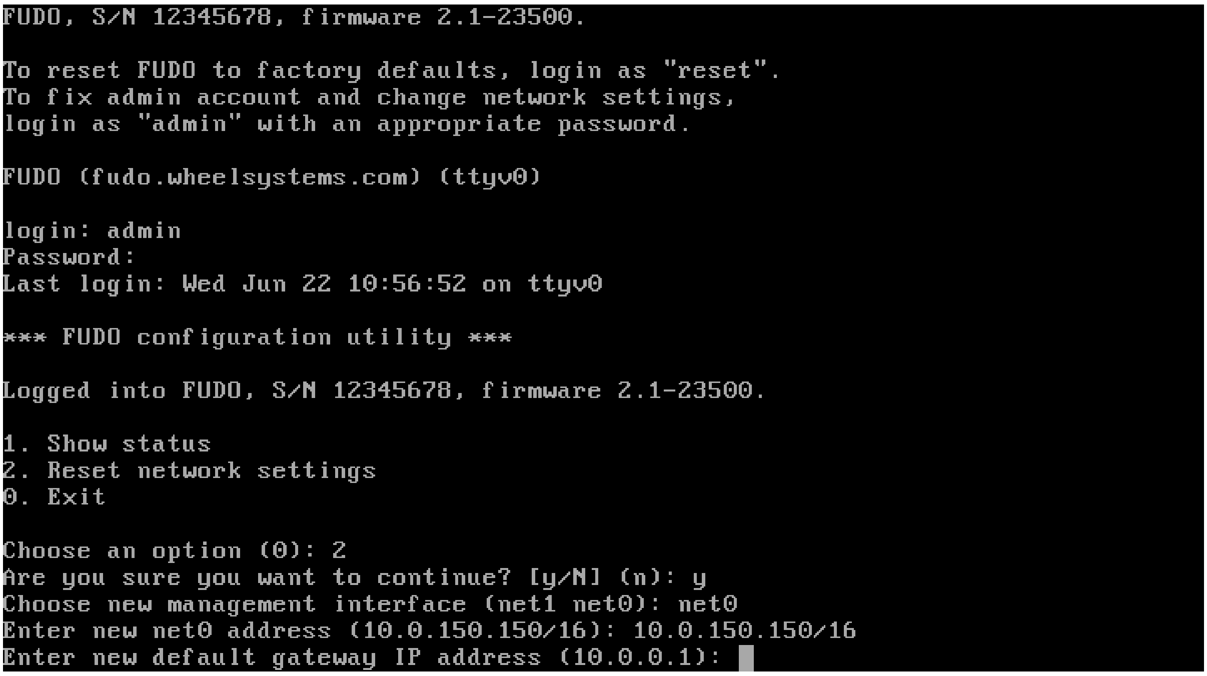
```
FUDO, S/N 12345678, firmware 2.1-23500.

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0):
```

7. Enter IP address along with the network subnet mask separated with / (e.g. `10.0.0.8/24`) and press *Enter*.



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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

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

8. Enter network gate and press *Enter*.



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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

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

22.2.1.3 Setting up a network bridge

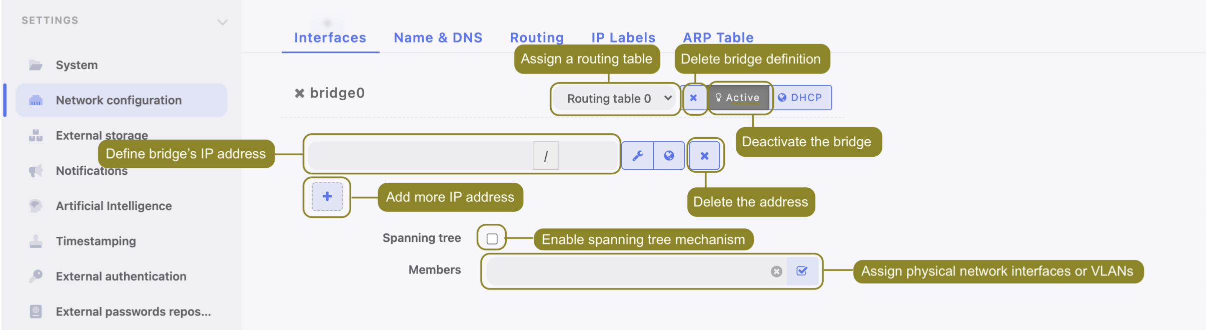
Bridge deployment scenario requires setting up a network bridge.

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*.



22.2.1.4 Setting up virtual networks (VLANs)

VLAN networks allow separating broadcast domains.

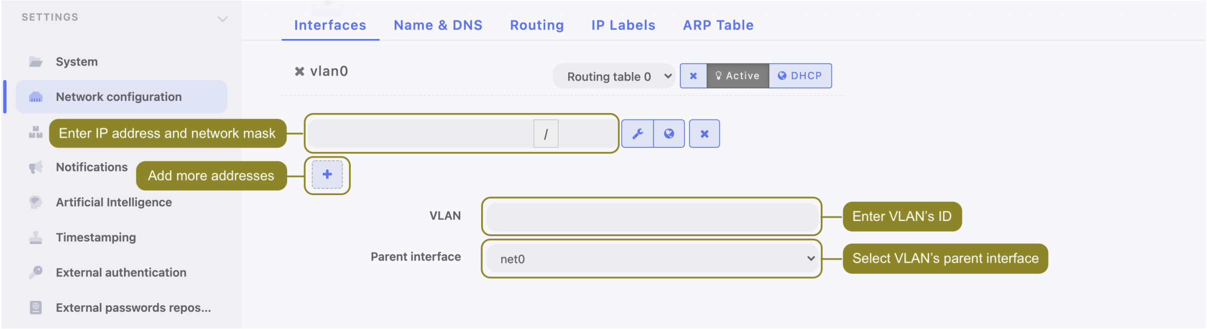
To configure a VLAN on , proceed as follows.

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*.

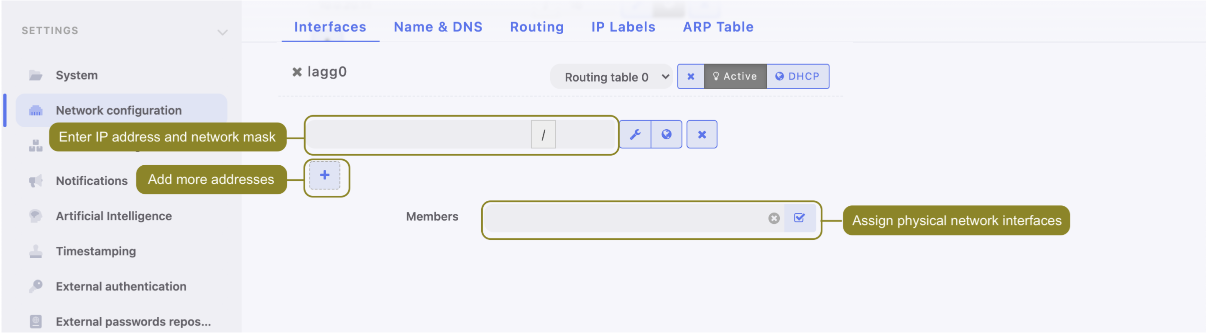


22.2.1.5 Setting up LACP link aggregation

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.
品	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*

22.2.2 Labeled IP addresses

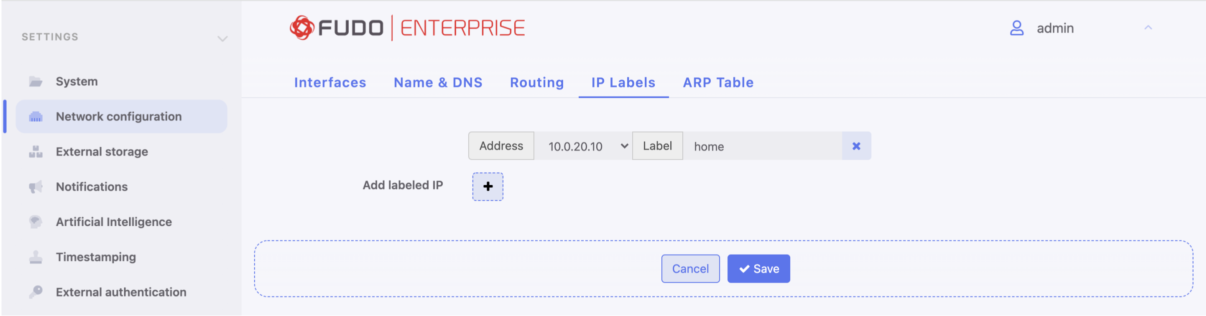
IP address labels are global configuration parameters. They are replicated throughout cluster's nodes, but their assignment is strictly local, applicable to each node separately. Labels enable ensuring constant access to LDAP authentication services in case of a node failure and allow for implementing 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.


Address 10.0.20.10 Label home

Add labeled IP +

Related topics:

- *Network interfaces configuration*
- *Authentication*
- *Servers*
- *Listeners*

22.2.3 Routing configuration

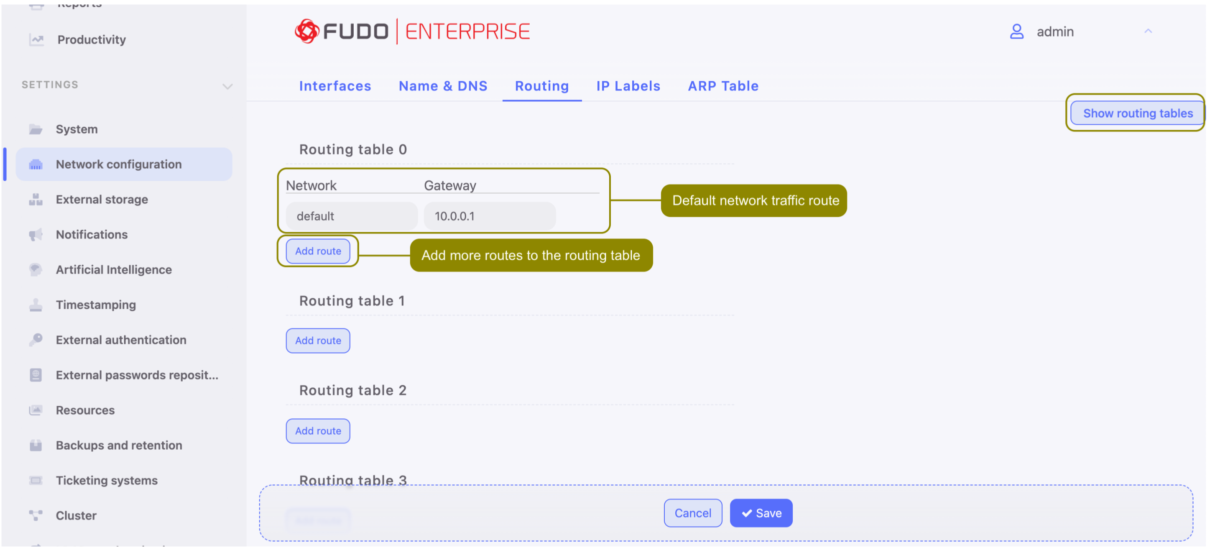
In default configuration, Fudo Enterprise directs all incoming traffic to defined gate. Static routing enables defining routes for packets coming from selected networks.

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

Adding a route

To add a route, proceed as follows. There are 7 routing tables available for configuration, with multiple routes.

1. Select *Settings* > *Network configuration*.
2. Select *Routing* tab.
3. Click *Add route* to define a new route.
4. Enter network address along with the network mask (e.g. `10.0.1.1/32`) and gateway address.
5. Click *Save*.



Network	Gateway
default	10.0.0.1

Default network traffic route

Add more routes to the routing table

Editing a route

To edit a route, proceed as follows.

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

Deleting a route

To delete a route, proceed as follows.

1. Select *Settings* > *Network configuration*.
2. Select *Routing* tab.

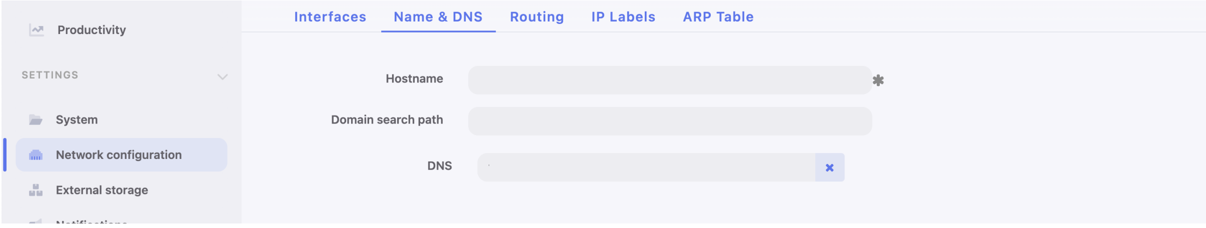
3. Find desired route entry and click the delete icon.
4. Click *Save*.

Related topics:

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

22.2.4 DNS configuration

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



Defining domain search path

Domain search path enables convenient hosts identification based on short names. For example, defining `tech.whl` as the domain search path, enables defining target host as `ftp` instead of `ftp.tech.whl`.

To define a domain search path, proceed as follows.

1. Select *Settings > Network configuration*.
2. Switch to the *Name & DNS* tab.
3. Enter the domain search path.

Note:

- To define more than one value, enter desired values separated by space character. E.g. `tech.whl wheel.com`
- Protocol implementation enables defining up to six domain search paths.

4. Click *Save*.

Adding a DNS server definition

To add a DNS server definition, proceed as follows.

1. Select *Settings > Network configuration*.
2. Switch to the *Name & DNS* tab.
3. Click *Add 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*

22.2.5 ARP table configuration

Note: Adding an entry to ARP table can resolve network communication issues.

Adding an ARP entry

To add an ARP entry, proceed as follows.

1. Select *Settings > Network configuration*.
2. Switch to the *ARP table* tab.
3. Click *+ Add* to define new ARP table entry.
4. Enter IP address and corresponding MAC address.
5. Click *Save*.

Editing an ARP table entry

To edit an ARP table entry, proceed as follows.

1. Select *Settings > Network configuration*.
2. Switch to the *ARP table* tab.
3. Find and edit desired ARP table entry.
4. Click *Save*.

Deleting an ARP table entry

Note: Deleting an ARP table entry may cause system malfunction due to network communication issues.

To delete an ARP entry, proceed as follows.

1. Select *Settings > Network configuration*.
2. Switch to the *ARP table* tab.
3. Find desired ARP entry and click the ✖ icon.
4. Click *Save* .

Related topics:

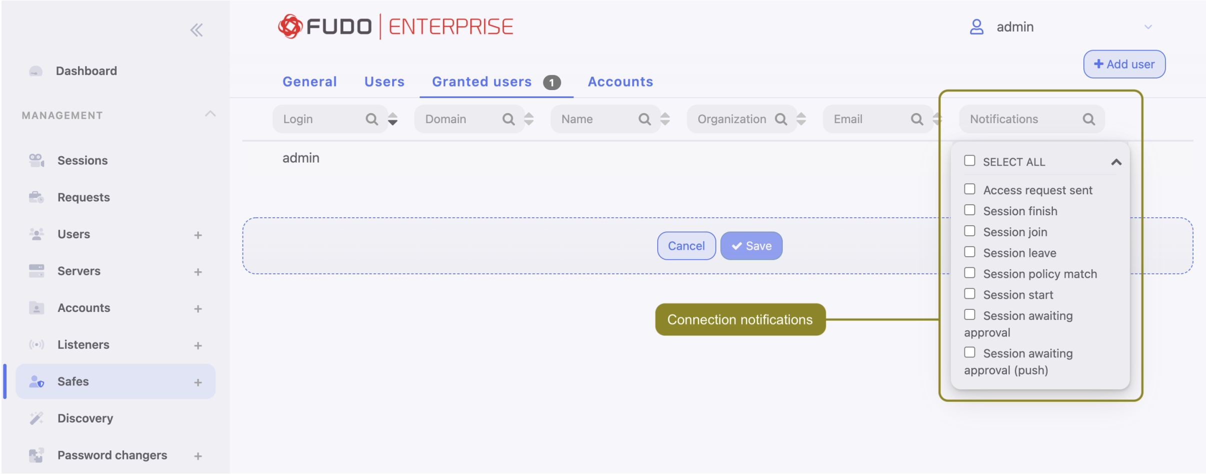
- *Network interfaces configuration*
- *Time servers configuration*

22.3 Notifications

Fudo Enterprise can send email notifications concerning defined connections:

- access request sent,
- session awaiting approval,
- session awaiting approval(push),
- session start,
- session join,
- session leave,
- session policy match,
- session finish.

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 Enterprise administration panel and select desired notifications in the Safe's configuration within *Granted users* tab. You need to do this with each *granted* user that should receive the notification.

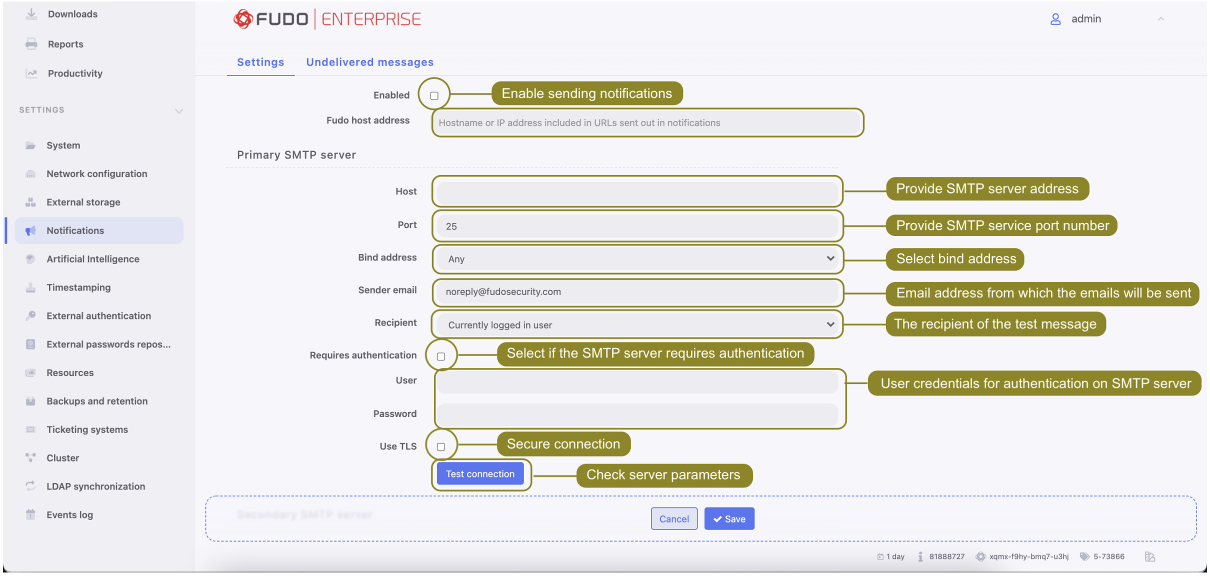
Email notifications service requires configuring SMTP server.

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.



Enabled □

Fudo host address: Hostname or IP address included in URLs sent out in notifications

Primary SMTP server

Host:

Port: 25

Bind address: Any

Sender email: noreply@fudosecurity.com

Recipient: Currently logged in user

Requires authentication □

User:

Password:

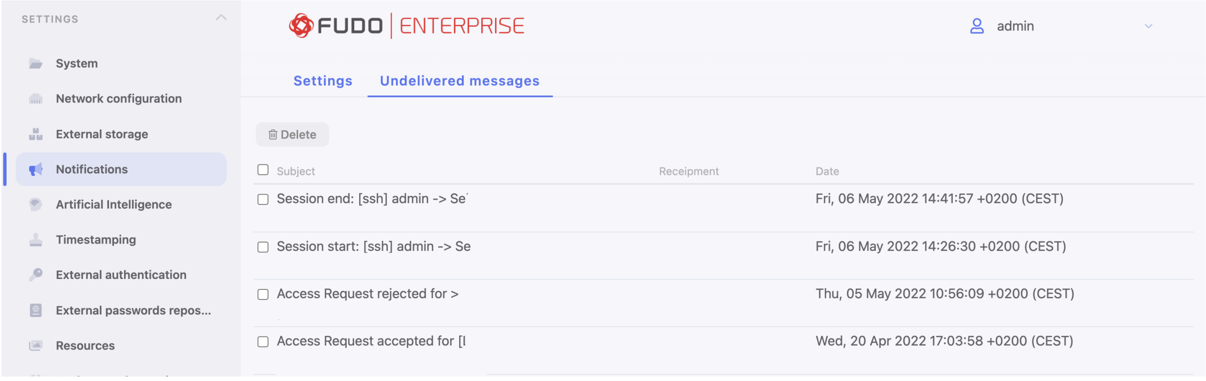
Use TLS □

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*.

The **Undelivered messages** sub-tab shows a list of the notifications that weren't delivered to the receiver. This helps the users to diagnose the issue and fix it for the future events. The messages here can be deleted.



□ Subject	Receipment	Date
□ Session end: [ssh] admin -> Se		Fri, 06 May 2022 14:41:57 +0200 (CEST)
□ Session start: [ssh] admin -> Se		Fri, 06 May 2022 14:26:30 +0200 (CEST)
□ Access Request rejected for >		Thu, 05 May 2022 10:56:09 +0200 (CEST)
□ Access Request accepted for [I		Wed, 20 Apr 2022 17:03:58 +0200 (CEST)

Related Topics:

- *Accounts*

22.4 Artificial Intelligence

Fudo Enterprise allows configuring model trainers and behavioral analysis models with custom settings so that it precisely analyses your users' behavior, detects unusual actions and marks sessions as suspicious so that you can quickly react.

Fudo Enterprise's AI module is a multicomponent system that needs to be set first to properly work and deliver the best results. There are 3 things to do to use AI module as effective as possible:

1. Configure model trainers, as described in the following section.
2. Enable *AI models* so that they run the behavioral analysis based on selected protocols (SSH and/or RDP), and deliver individual statistics per model.
3. Set session *Policies* so that AI module can detect specific user's behavior during a session, react automatically, and send messages and SNMP TRAP notifications about the current situation.

When those steps are done, you can observe:

- amount of suspicious sessions for the given period of time on the Dashboard within the Suspicious sessions widget. The widget also provides an URL to the filtered Sessions list with *Threat level: High* criteria set.
- threat levels and *Threat Probability* of the ongoing *sessions* within a graph that can redirect to the suspicious session segment in the player.

22.4.1 Configuring models trainers

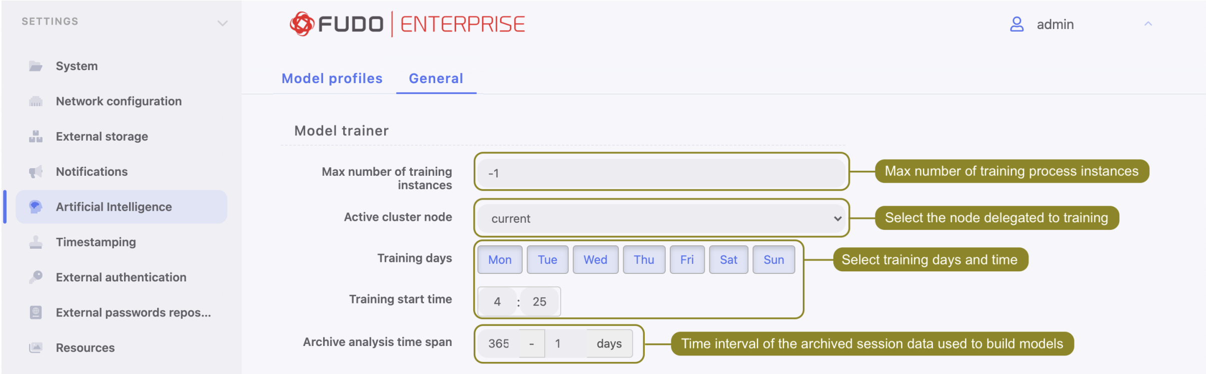
Training models requires processing power. Proper system configuration enables optimal processing of archived sessions while preserving overall system responsiveness in handling current user requests.

To change models trainers configuration, proceed as follows.

1. Select *Settings > Artificial Intelligence > General.*
2. In the *Model trainer* section, in the *Max number of training instances* field, define the number of processes delegated to constructing user profiles.

Note: Default value is the optimal value based on available hardware resources. The actual number of processes cannot be higher than the number of available CPU cores.

3. From the *Active cluster node* dropdown list, select the node responsible for training models.
4. Select weekdays when the training will take place.
5. Set the training start time.
6. Define the timespan of the data which will be processed to create models.



Model trainer

Max number of training instances: -1 — Max number of training process instances

Active cluster node: current — Select the node delegated to training

Training days: Mon Tue Wed Thu Fri Sat Sun — Select training days and time

Training start time: 4 : 25

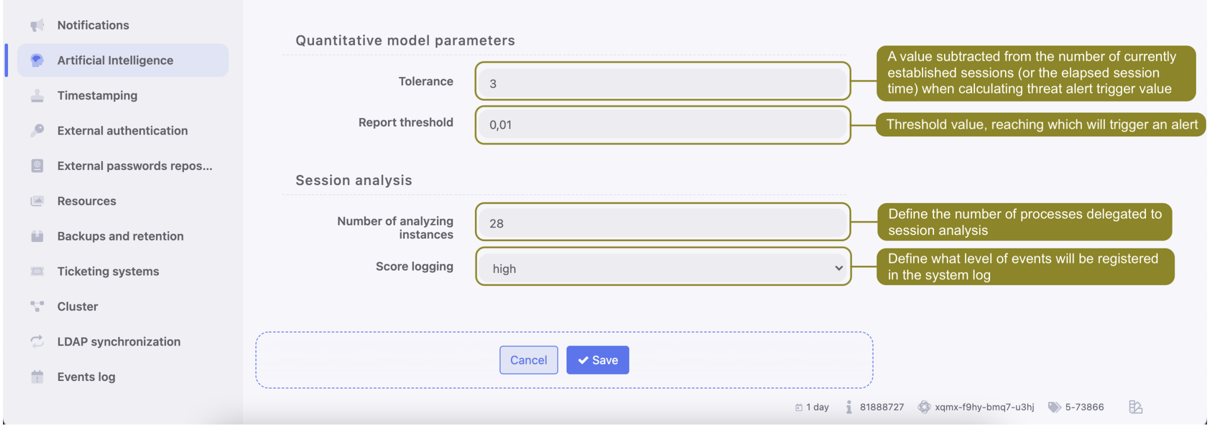
Archive analysis time span: 365 - 1 days — Time interval of the archived session data used to build models

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

Note: This parameter is used to calculate the threat risk which triggers the alert. Tolerance value is deducted from the current connections number or the number of minutes of elapsed session time. E.g. if the expected number of connections is 100, the current connection number is 109 and the tolerance value is set to 10, alarm will not be triggered as the calculated value (99) is less than the expected value.

8. In the *Report threshold* field, define the allowed deviation from the expected results.

Note: Report threshold is defined in % and it determines the threshold value when the alert gets triggered on the account of too many sessions or a single connection lasting longer than expected. E.g. with the report threshold set to 1%, the alert will be triggered if the current number of connections has been observed before in 1% of cases.



Quantitative model parameters

Tolerance: 3 — A value subtracted from the number of currently established sessions (or the elapsed session time) when calculating threat alert trigger value

Report threshold: 0,01 — Threshold value, reaching which will trigger an alert

Session analysis

Number of analyzing instances: 28 — Define the number of processes delegated to session analysis

Score logging: high — Define what level of events will be registered in the system log

9. In the *Session analysis* section, in the *Number of analyzing instances*, define the number of processes delegated to session analysis.
10. Select the threat level from the *Score logging* drop-down list to define what type of events will be registered within the system log.

Note: In case the pool of available data processing processes has been exhausted, online analysis is suspended. After the session is finished the data is picked up by the session analysis processes.

10. Click *Save*.

22.4.2 Behavioral analysis models

Configuration parameters enable fine tuning behavioral models to match the specifics of your IT environment.

Note: Fudo Enterprise 5.3 release contains the modified AI module.

Warning:

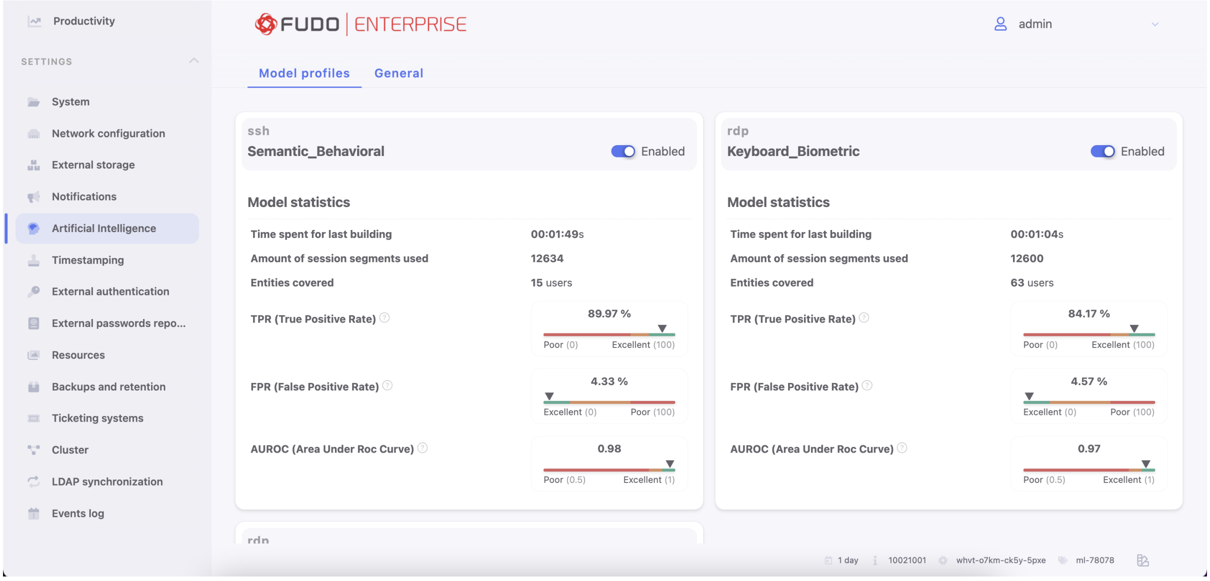
- The upgrading script to the Fudo Enterprise 5.3 version disables all *AI models* and adds new models during the upgrading process. When the process is finished, all AI models need to be manually enabled in the *Settings > Artificial Intelligence* tab.
- If you have cluster configuration, it is required to update the active models on the master node first.

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

Mouse biometric Model (RDP) - AI prediction model based on mouse movements and clicks. It works by deriving a set of over 700 distinct features associated with the way a user operates a pointing device. Those features are used to train the model which is individually calibrated for each user to obtain the best possible predictive value whilst minimizing the *False Positive Rate*.

Keyboard biometric Model (RDP) - AI prediction model based on keyboard typing dynamics. It works by deriving a set of over a 100 unique features associated with the way a user types on the keyboard. Those features are used to train the model which is individually calibrated for each user to obtain the best possible predictive value whilst minimizing the *False Positive Rate*.

Semantic Behavioral Model (SSH) model is based on the keyboard input (commands). It works by identifying individual preferences of people to achieve the same results in different ways. For example one person prefers to use `wget` over `curl` and `vim` over `emacs`, another person might use a `reset` command to clear the terminal while someone else might have a preference for using `CTRL+L` combination. Those features are not static but learned from the training data. Additionally a set of over 600 features for different groups of characters is derived. Those features are combined with preferences and used to train the model which is individually calibrated for each user to obtain the best possible predictive value whilst minimizing the *False Positive Rate*.



ssh
Semantic_Behavioral
Enabled

Model statistics

Time spent for last building	00:01:49s
Amount of session segments used	12634
Entities covered	15 users
TPR (True Positive Rate)	89.97 % Poor (0) Excellent (100)
FPR (False Positive Rate)	4.33 % Excellent (0) Poor (100)
AUROC (Area Under Roc Curve)	0.98 Poor (0.5) Excellent (1)

rdp
Keyboard_Biometric
Enabled

Model statistics

Time spent for last building	00:01:04s
Amount of session segments used	12600
Entities covered	63 users
TPR (True Positive Rate)	84.17 % Poor (0) Excellent (100)
FPR (False Positive Rate)	4.57 % Excellent (0) Poor (100)
AUROC (Area Under Roc Curve)	0.97 Poor (0.5) Excellent (1)

rdp

For each AI model Fudo Enterprise shows training statistics, such as:

Time spent for the last building - duration of the last building.

Amount of session segments used - number of the session segments that were used for the last building.

Entities covered - how many users were participating in the last training session.

True Positive Rate (TPR), sometimes called Recall - is a percentage of malicious sessions properly flagged by the model as suspicious (the higher the better).

False Positive Rate (FPR) is the percentage of legitimate sessions inappropriately identified as malicious (the lower the better).

Area Under ROC curve (AUROC) is a single metric representing model quality (the higher the better).

Statistics of the TPR, FPR and AUROC values are visualized in the colored bar.

Note: Model statistics appear after the model's first training and are updated after each of the performed training.

Related topics:

- *Sessions*
- *AI sessions processing*
- *Policies*

22.5 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 Enterprise must be able to reach the `http://www.ts.kir.com.pl/HttpTspServer` web address in case of the KIR time-stamping service.
- Fudo Enterprise must be able to reach the `193.178.164.5` IP address in case of the PWPW time-stamping service.

Data Transmitted to Timestamp Provider

When timestamping sessions in Fudo Enterprise, a hash is generated and sent to the timestamp provider. This hash is composed of session data from the `fudo_session` table, and content from the session's RAW dump. It is a one-way hash, ensuring that no session details can be extracted from it.

Note: To ensure the generation of a RAW dump, set the *Session recording* option in Account settings to `all` or `raw` (refer to the *Creating a regular account* section to see the example).

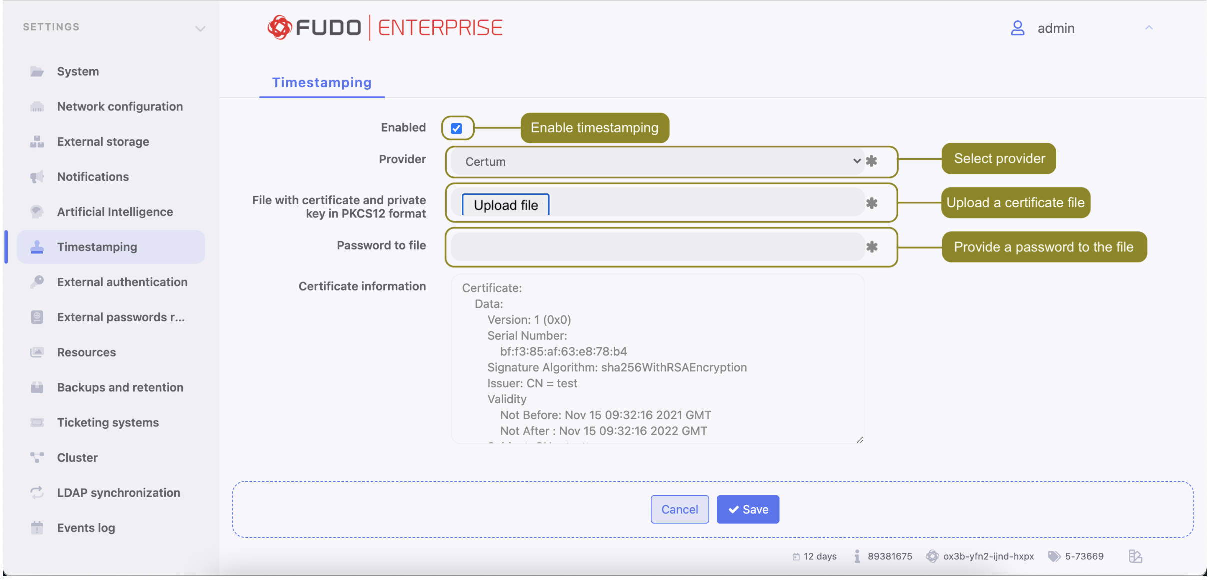
Enabling and configuring trusted time-stamping

Note: Fudo Enterprise 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.*



Enabled ☑ — Enable timestamping

Provider: Certum — Select provider

File with certificate and private key in PKCS12 format: Upload file — Upload a certificate file

Password to file — Provide a password to the file

Certificate information

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            bf:f3:85:af:63:e8:78:b4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = test
        Validity
            Not Before: Nov 15 09:32:16 2021 GMT
            Not After : Nov 15 09:32:16 2022 GMT
```

Related topics:

- *Security measures*

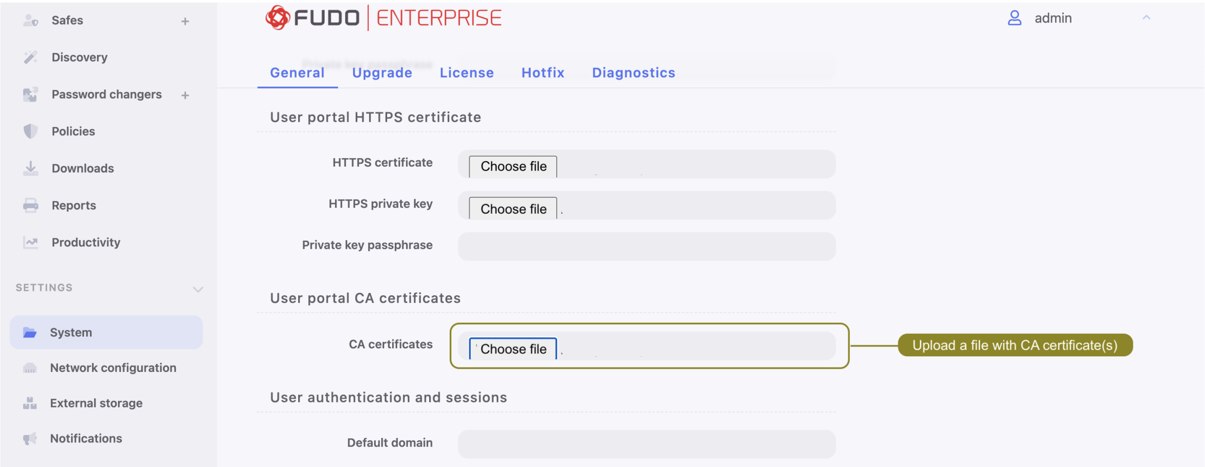
22.6 Certificate-based authentication scheme

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

In order to configure authentication method `certificate`, proceed as follows:

1. Select *Settings* > *System*
2. In the *User portal CA certificates* section upload a file with CA certificate(s) in PEM format.

Note: Fudo Enterprise supports a multiple-domain configuration. For such configuration, the administrator has to upload a PEM file that consists of root/intermediate certificates from all the CAs. The *Subject* field should be unique for each user.



User portal HTTPS certificate

HTTPS certificate: Choose file

HTTPS private key: Choose file

Private key passphrase

User portal CA certificates

CA certificates: Choose file — Upload a file with CA certificate(s)

User authentication and sessions

Default domain

3. Click *Save*.

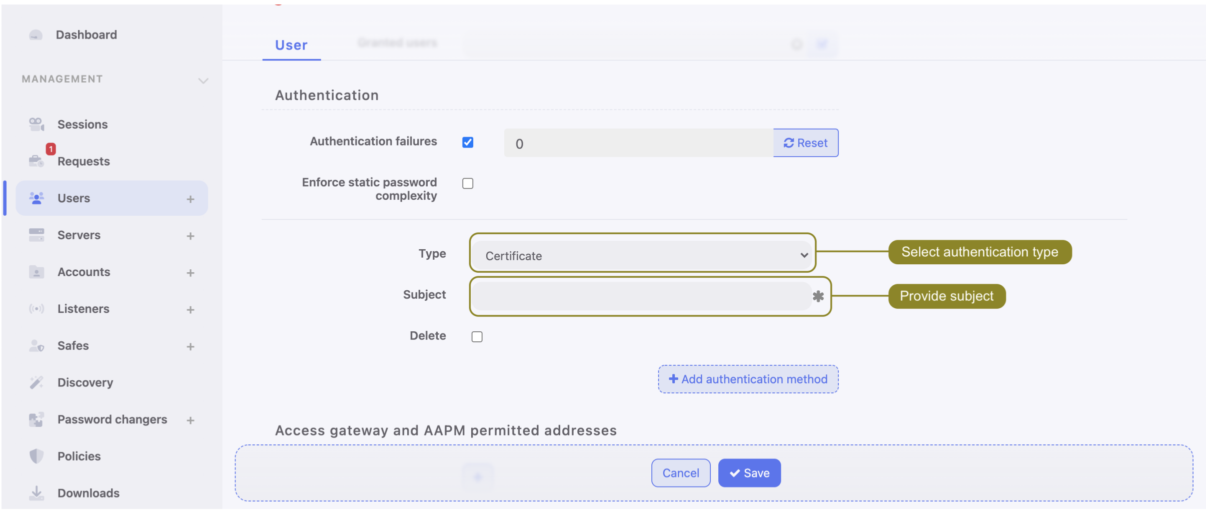
4. Go to *Management > Users* and select the user, for whom you want to set authentication method `certificate`, or

Create a new user by clicking + icon in the main menu next to the *Users* tab, or selecting *Management > Users* and then clicking *+ Add*.

5. In the *Authentication* section select Type: `certificate`.

6. Provide *Subject*.

Note: The subject must comply with the RFC 2253 or RFC 4514 requirements.



Authentication failures ☑ 0

Enforce static password complexity □

Type: Certificate

Subject:

Select authentication type

Provide subject

7. Click *Save*.

Related Topics:

- *Creating a user*

22.7 Authentication

Fudo Enterprise has a broad spectrum of authentication methods for user's authentication against the target server. Those are:

- External authentication:
  - *CERB*,
  - *RADIUS*,
  - *LDAP*,
  - *Active Directory*,
- *OATH*,
- *SMS*,
- *DUO*,
- *OpenID Connect*.

Mentioned authentication methods require defining connections to the external authentication servers.

22.7.1 External authentication server definition

To add an external CERB, Radius, Active Directory or LDAP authentication server, proceed as follows.

1. Select *Settings > Authentication*.
2. Click *+ Add an external authentication source*.
3. Select authentication service type: `CERB`, `Radius`, `Active Directory` or `LDAP`.
4. Provide configuration parameters depending on selected external authentication system type.
5. Click *Save*.

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.
Service	CERB service used for authenticating Fudo Enterprise users.
Secret	Secret used to establish server connection.
Second factor	Additional verification step with authentication methods `OATH`, `SMS` or `DUO`.
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.
NAS ID	RADIUS server NAS-Identifier parameter.
Secret	Secret used to establish server connection.
Repeat secret	Repeat secret used to establish server connection.
Second factor	Additional verification step with authentication methods `OATH`, `SMS` or `DUO`.
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.
Bind DN	Template containing a path which will be used to create queries to LDAP server.
Encrypted connection	This option is required to be checked for the domain users who change their passwords in the Access Gateway.
Server certificate	LDAP server certificate.
Second factor	Additional verification step with authentication methods `OATH`, `SMS` or `DUO`.
Active Directory	
Host	Server's IP address.
Port	Port used to establish connections with given server.

Continued on next page

Table 1 – continued from previous page

Parameter	Description
Bind address	IP address used for sending requests to given host.
Active Directory domain	Domain which will be used for authenticating users in Active Directory.
Encrypted connection	This option is required to be checked for the domain users who change their passwords in the Access Gateway.
Server certificate	Active Directory server certificate.
Login	The privileged account's login name to modify a user password on the Active Directory server.
Secret	Secret used to establish server connection to modify a user password on the Active Directory server.
Repeat secret	Secret used to establish server connection to modify a user password on the Active Directory server.
Second factor	Additional verification step with authentication methods `OATH`, `SMS` or `DUO`.

Warning: When additional authentication method (`OATH`, `SMS` or `DUO`) is selected as a *Second factor* for synchronization with *External authentication server* (AD / LDAP / CERB / RADIUS), it won't be enough to just select one of the *External authentication server source* within the User definition. The additionally selected authentication method should be configured within the User definition as a primary authentication method. Then users' authentication methods will be automatically synchronized according to *External authentication server* settings.

Note: Labeled IP addresses

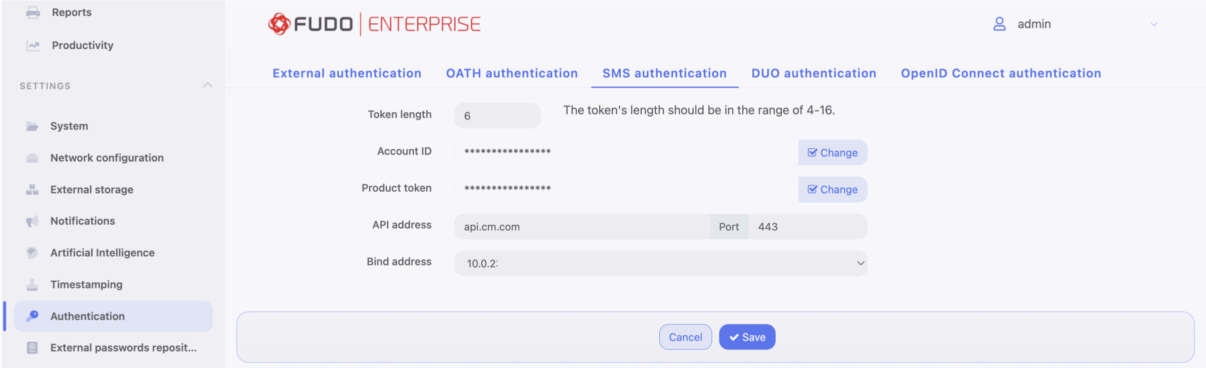
In case of cluster configuration, select a labeled IP address from the *Bind address* drop-down list and make sure that other nodes have IP addresses assigned to this label. For more information refer to the *Labeled IP addresses* topic.

22.7.2 OATH authentication definition

Refer to the *Two-factor OATH authentication with Google Authenticator* page.

22.7.3 SMS authentication definition

1. Select *Settings > Authentication.*
2. Choose **SMS Authentication** tab.



Token length: 6 — The token's length should be in the range of 4-16.

Account ID: ****************

Product token: ****************

API address: api.cm.com Port 443

Bind address: 10.0.2:

- Input *Token length*.

Note: The token's length should be in the range of 4-16.

- Input *Account ID*.
- Input *Product token*.
- 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.

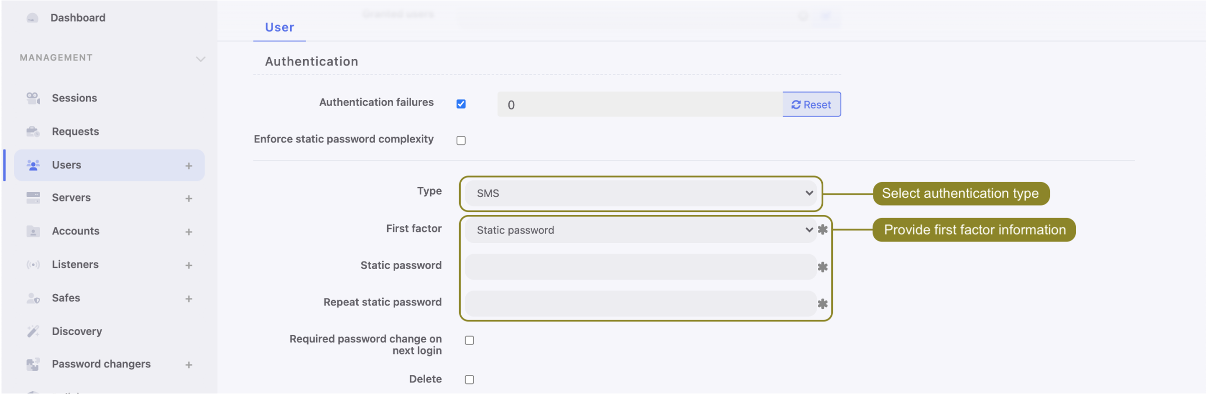
- Select the *Bind address*.

3. Click *Save*.

Configure SMS authentication method for the User:

4. Go to *Management > Users*.
5. Find and select the user for whom you want to enable SMS authentication.

- Input a phone number in the **Phone** input field.
- Under the *Authentication* section choose Type: `SMS`.
- From a **First factor** drop-down list choose `Static password` or `External authentication` (AD or LDAP).



Authentication failures ☑ 0

Enforce static password complexity □

Type: SMS

First factor: Static password

Static password

Repeat static password

Required password change on next login □

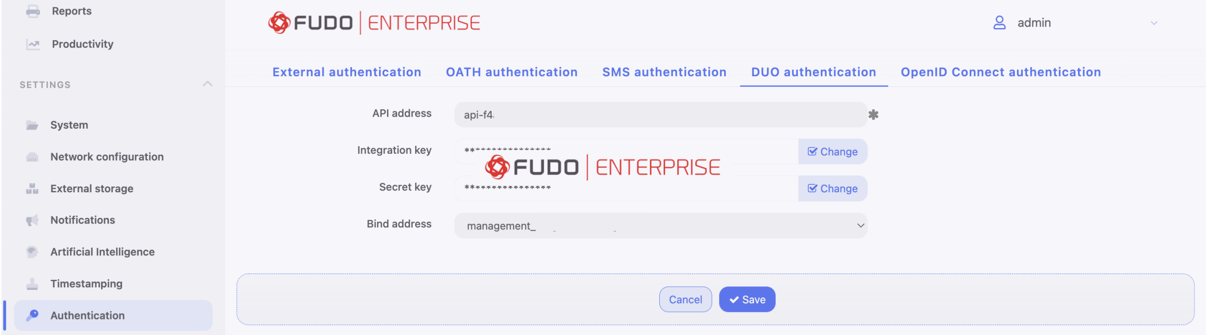
Delete □

6. Click *Save*.

7. Log in to the Access Gateway with SMS code.

22.7.4 DUO authentication definition

1. Download and install Duo Mobile phone application.
2. Sign up for a personal account on Duo Security.
3. Select *Settings > Authentication*.
4. Choose **DUO Authentication** tab.



API address: api-f4

Integration key: ****************

Secret key: ****************

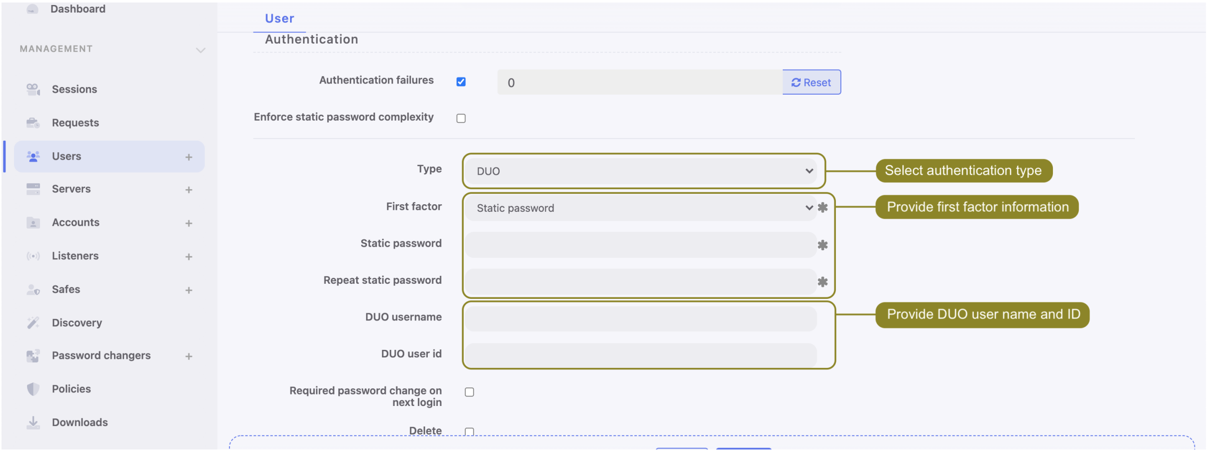
Bind address: management_

5. Input from the personal Duo Security profile: *API address*, *Integration key* and *Secret key*.
6. Select the *Bind address*.
7. Click *Save*.

Configure DUO authentication method for the User:

8. Go to *Management > Users*.
9. Find and select the user for whom you want to enable DUO authentication.

- Under **Authentication** section choose Type: `DUO`.
- From a **First factor** drop-down list choose `Static password` or `External authentication` (AD or LDAP).
- Input *DUO username*.
- Input *DUO user id*.



Authentication failures ☑ 0

Enforce static password complexity □

Type: DUO

First factor: Static password

Static password

Repeat static password

DUO username

DUO user id

Required password change on next login □

Delete □

Select authentication type

Provide first factor information

Provide DUO user name and ID

10. Click *Save*.
11. Log in to the Access Gateway by tapping *Accept* on push notification from Duo Mobile application.

22.7.5 OpenID Connect authentication definition

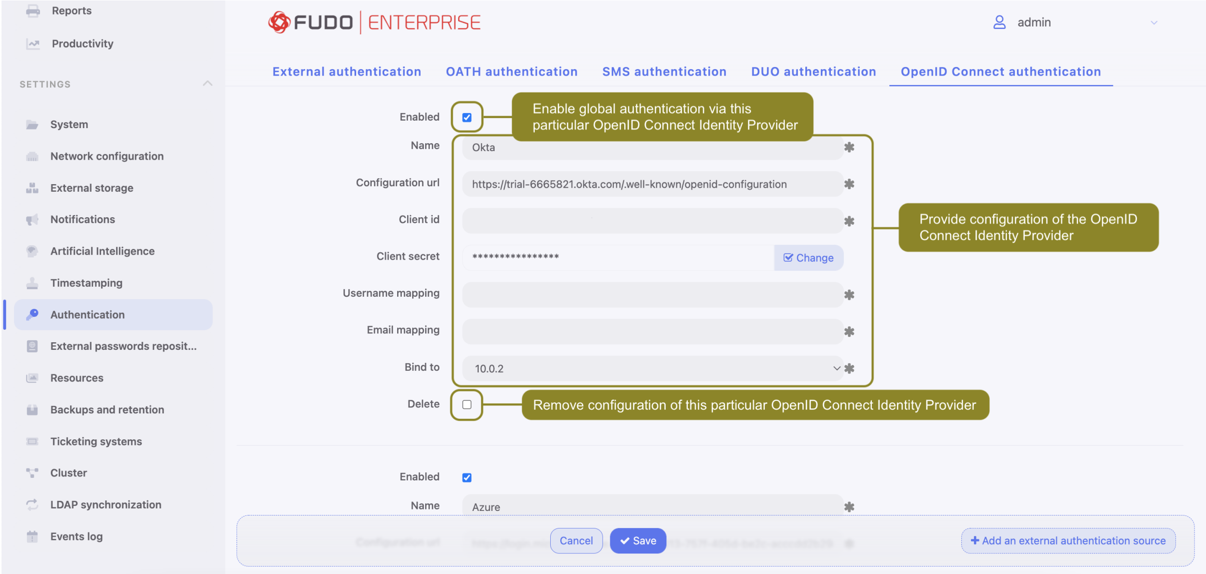
This authentication method is configured globally and is not tied to any particular user. Thus even if a user has no authentication methods configured, they can authenticate using OpenID Connect in Access Gateway and Admin Panel.

Follow the steps to configure the OpenID Connect authentication method:

1. Select *Settings* > *Authentication*.
2. Choose **OpenID Connect authentication** tab.
3. Click *Add an external authentication source*.
4. Check the *Enabled* option to globally enable OpenID Connect authentication.
5. Provide Name (`Azure`, `Okta` or any other Identity Provider).
6. Input *Configuration URL*.

Note: This URL is specific for every Identity Provider and allows identifying one for correct configuration. Example of *Configuration URL* for Google: `https://accounts.google.com/.well-known/openid-configuration`.

7. Provide *Client ID*, *Client secret*. Those values are available after the registration on selected provider.
8. Add *Username mapping* and *Email mapping*. Those fields are useful when user's name has different naming convention.
9. Provide *Bind address*.



Enabled ☑

Name: Okta

Configuration url: https://trial-6665821.okta.com/.well-known/openid-configuration

Client id:

Client secret: ****************

Username mapping:

Email mapping:

Bind to: 10.0.2

Delete □

Enable global authentication via this particular OpenID Connect Identity Provider

Provide configuration of the OpenID Connect Identity Provider

Remove configuration of this particular OpenID Connect Identity Provider

Enabled ☑

Name: Azure

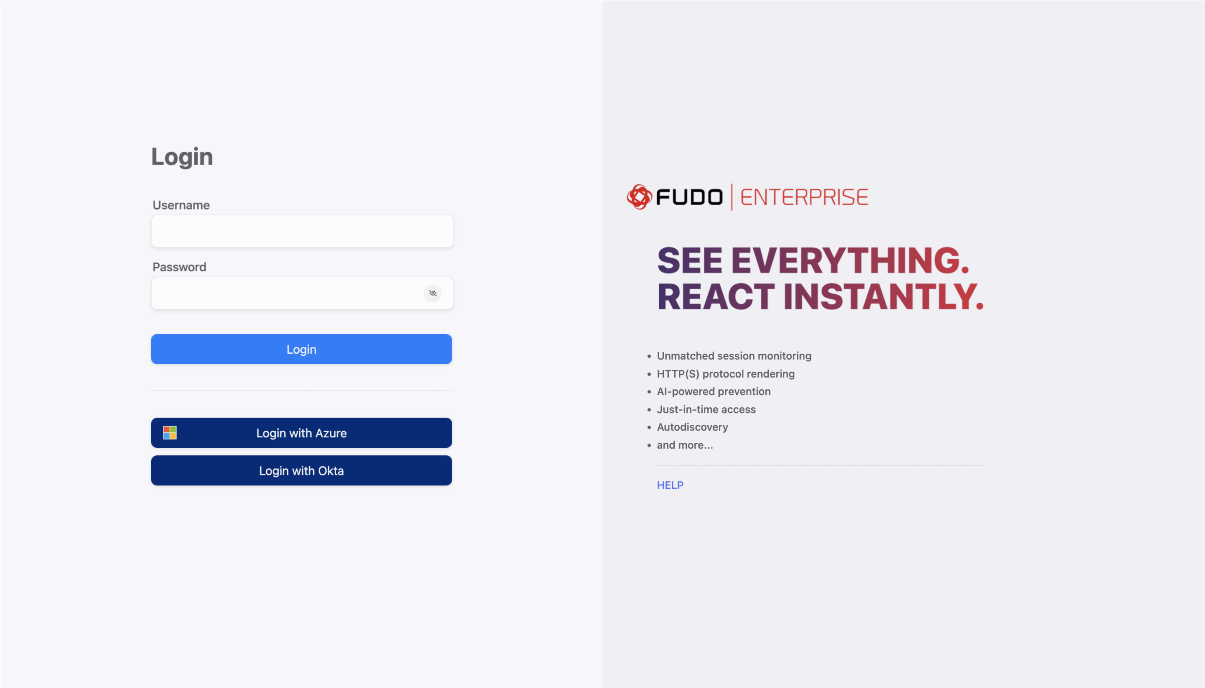
10. Click *Save*.

Note: The **algorithm to determine the user's identity** is following:

1. If *Username mapping* is defined, we try to find field in the data with that name. If JSON data contains this field, we will try to find user by this name.
2. If *Username mapping* is not defined, the field is not found in the data or the user is not found by name, we check if *Email mapping* is defined. If it is defined and exists in JSON data, we try to find user by this email.
3. When neither *Username mapping* nor *Email mapping* is defined we try to find the user by his name or his email by looking for those fields in the data in the following order: email, upn, unique_name.

Furthermore, if the `email_verification` field is present in the data, it must be set to `true`.

Log in using the defined authentication method:



Login

Username

Password

Login

Login with Azure

Login with Okta

FUDO | ENTERPRISE

SEE EVERYTHING.
REACT INSTANTLY.

- Unmatched session monitoring
- HTTP(S) protocol rendering
- AI-powered prevention
- Just-in-time access
- Autodiscovery
- and more...

HELP

Related topics:

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

22.8 External passwords repositories

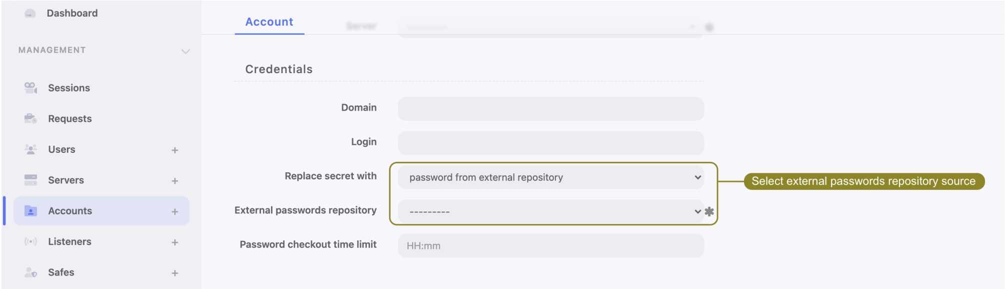
Fudo Enterprise supports external passwords repositories for managing passwords to monitored servers.

22.8.1 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: ---------

Password checkout time limit: HH:mm

Select external passwords repository source

- 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*

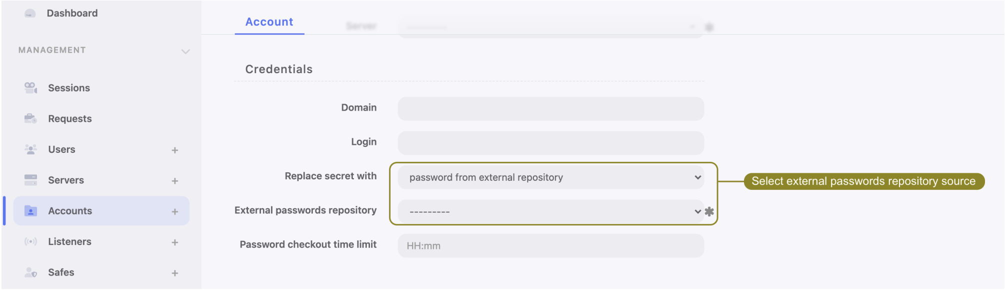
22.8.2 Thycotic Secret Server

Adding a new passwords repository

1. Select *Settings > External passwords repositories.*
2. Click *+ Add server.*
3. Select `Thycotic Secret Server` from the *Type* drop-down list.
4. Enter object's name.
5. Provide the URL to the passwords server's API.

Note: Specify HTTPS protocol within the URL so that communication with the server is encrypted.

6. Enter user login allowed to access passwords repository.
7. Provide user password in the *Password* and *Repeat password* fields.
8. Define secret string format used for identifying objects on Thycotic Secret Server.
9. Click *Save*.
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: ---------

Password checkout time limit: HH:mm

Select external passwords repository source

    - 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*.

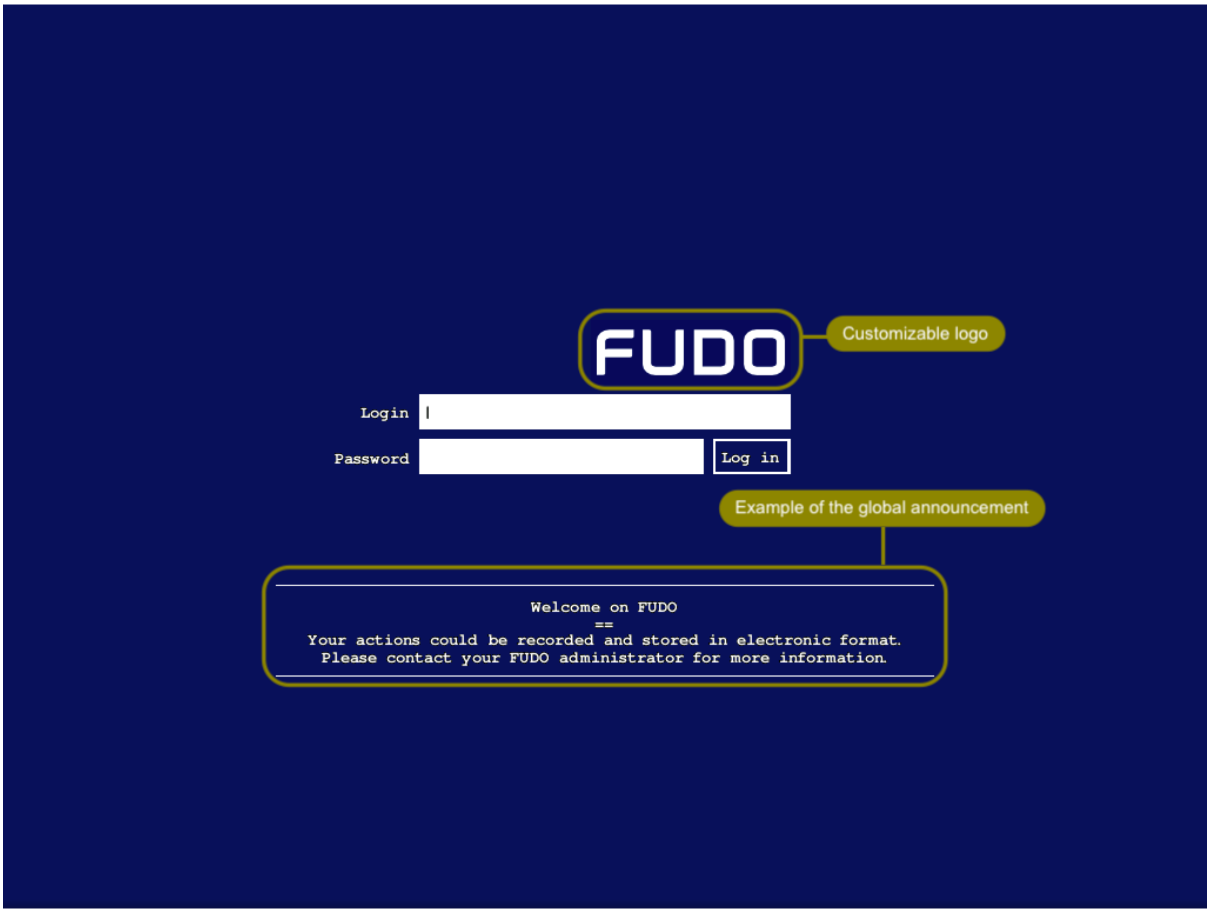
Related topics:

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

22.9 Resources

22.9.1 RDP/VNC login screen configuration

Fudo Enterprise enables customizing RDP, SSH 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.

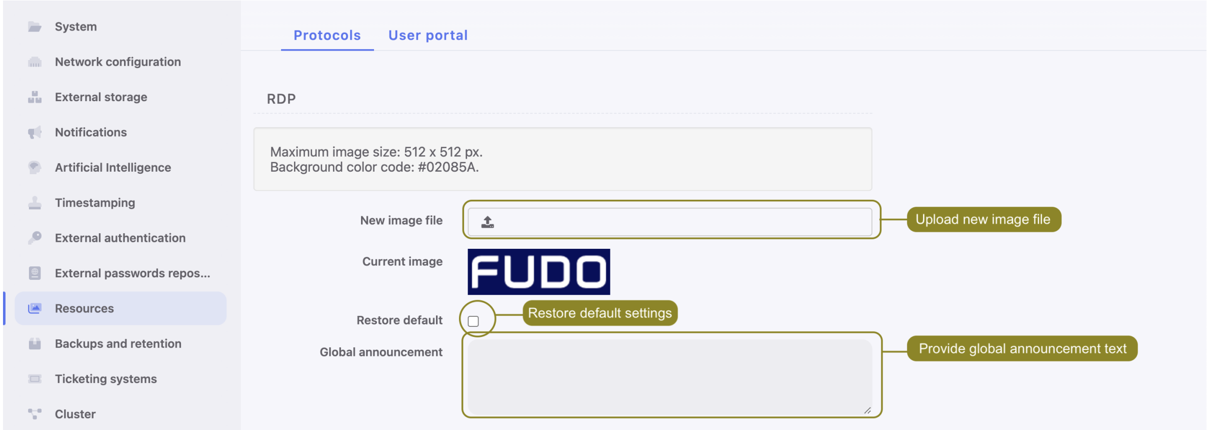
RDP login screen customization

1. Select *Settings* > *Resources*.
2. Select the *Protocols* tab.
3. In the *RDP* section, click *Choose File* button and select desired image.

Note: Maximum image size is 512 x 512 px.

4. Input *Global announcement* text as a message to be appeared on login screen.

Note: Login screen announcement can be four lines, up to 120 characters.



RDP

Maximum image size: 512 x 512 px.
Background color code: #02085A.

New image file

Current image

Restore default □

Global announcement

5. Click *Save*.

SSH login screen customization

1. Select *Settings* > *Resources*.
2. Select the *Protocols* tab.
3. In the *SSH* section, input *Global announcement* text as a message to be appeared on login screen.

Note: Login screen announcement can be four lines, up to 120 characters.

4. Click *Save*.

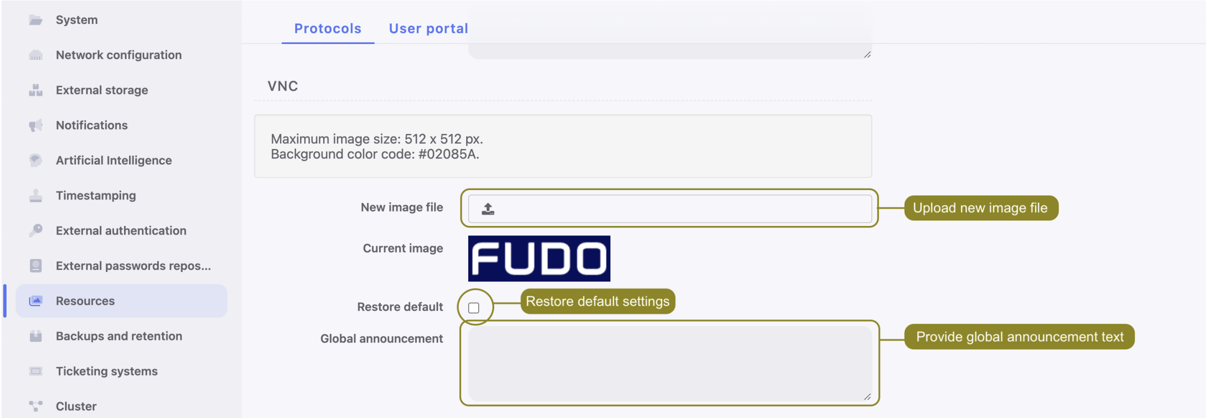
VNC login screen customization

1. Select *Settings* > *Resources*.
2. Select the *Protocols* tab.
3. In the *VNC* section, click *Choose File* button and select desired image.

Note: Maximum image size is 512 x 512 px.

4. Input *Global announcement* text as a message to be appeared on login screen.

Note: Login screen announcement can be four lines, up to 120 characters.



Maximum image size: 512 x 512 px.
Background color code: #02085A.

New image file

Current image

Restore default □

Global announcement

Upload new image file

Restore default settings

Provide global announcement text

5. Click *Save*.

Related topics:

- *Quickstart - RDP*

22.9.2 *User portal* login screen configuration

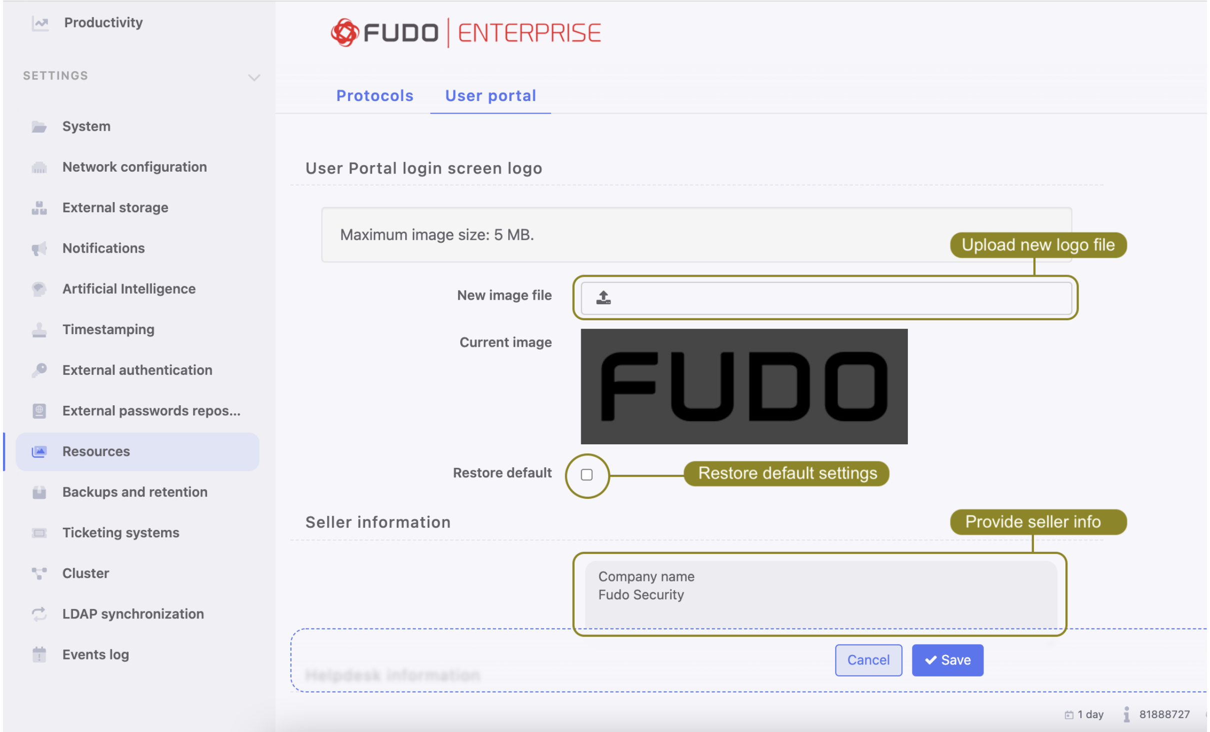
Fudo Enterprise enables customizing information displayed on the *User portal* login screen.

1. Select *Settings* > *Resources*.
2. Select the *User portal* tab.
3. 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 5 MB.

4. Provide company information.

Note: Company information can be five lines, up to 70 characters.



User Portal login screen logo

Maximum image size: 5 MB.

Upload new logo file

New image file

Current image

Restore default □

Restore default settings

Seller information

Provide seller info

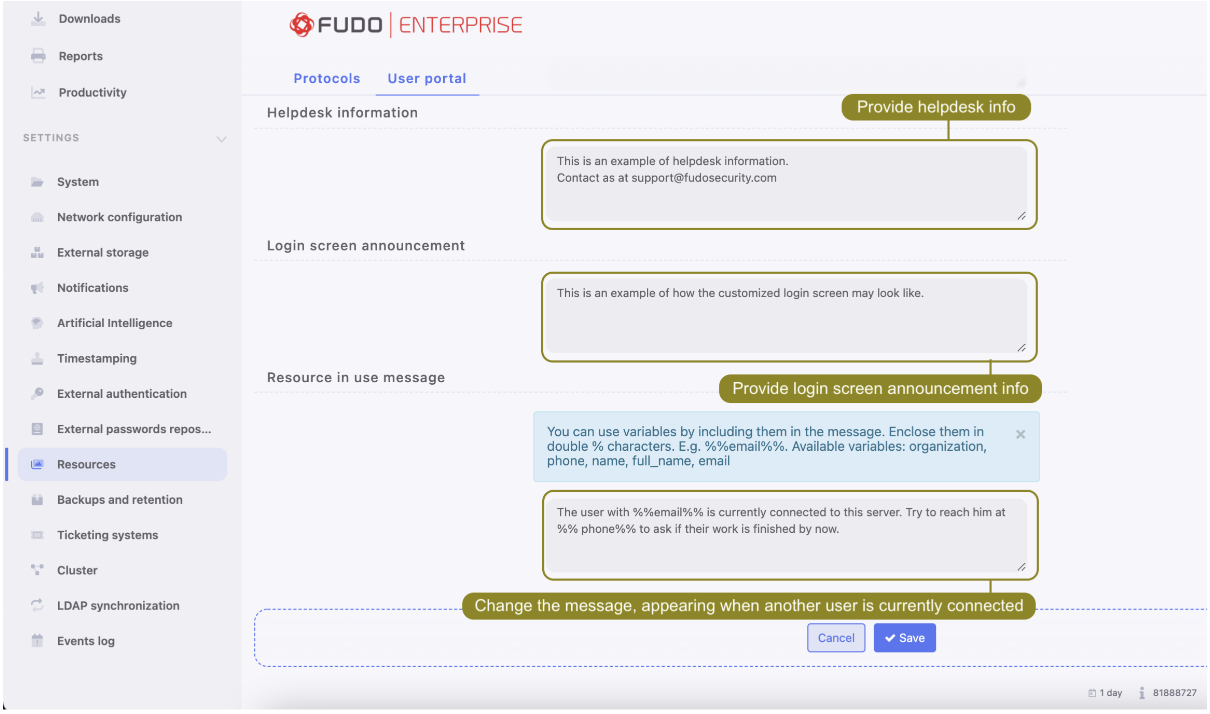
Company name
Fudo Security

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.



Helpdesk information

Provide helpdesk info

This is an example of helpdesk information.
Contact as at support@fudosecurity.com

Login screen announcement

This is an example of how the customized login screen may look like.

Provide login screen announcement info

Resource in use message

You can use variables by including them in the message. Enclose them in double % characters. E.g. %%email%%. Available variables: organization, phone, name, full_name, email

The user with %%email%% is currently connected to this server. Try to reach him at %% phone%% to ask if their work is finished by now.

Change the message, appearing when another user is currently connected

7. Provide information in the *Resource in use message* field. This information will be displayed to the user in the User Portal (Access Gateway) when trying to connect to the target server, another user will be already connected to that server via the same account.

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

> **Warning:** **Resource in use** feature is available for RDP connections only and can be configured while *Creating an RDP server* by checking the *Inform about existing connection* option.

8. Click *Save*.

Related topics:

- *User Portal (Access Gateway)*

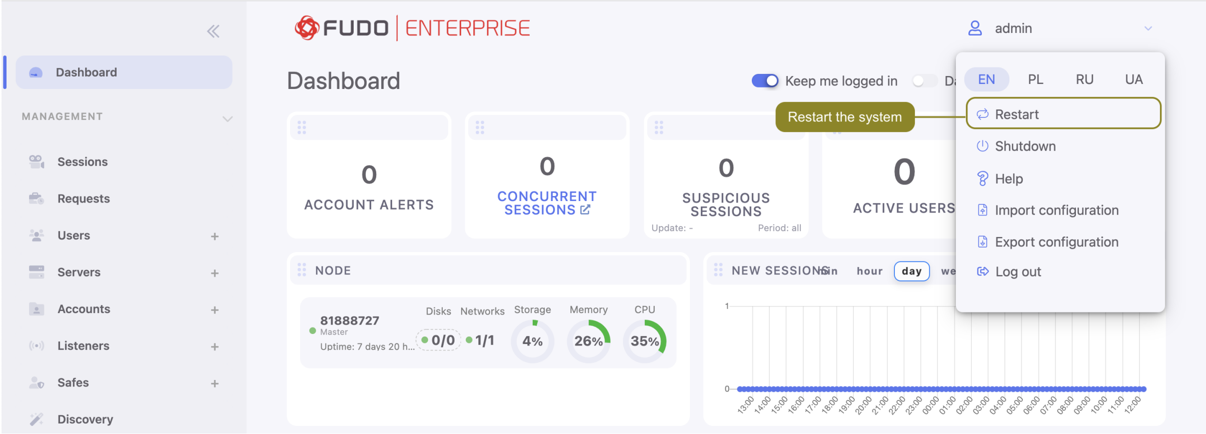
22.10 System version restore

In the case there is a problem with the current system revision, it is possible to restore the system to its previous version.

> **Warning:** Restoring the system to the previous version will bring back the system's state prior the update. **Session data** and **configuration changes** in the current system revision will be lost. This includes the **password changers** activity. If any passwords were changed during the newer version's usage, restarting Fudo will lead to lost access to corresponding systems.

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:

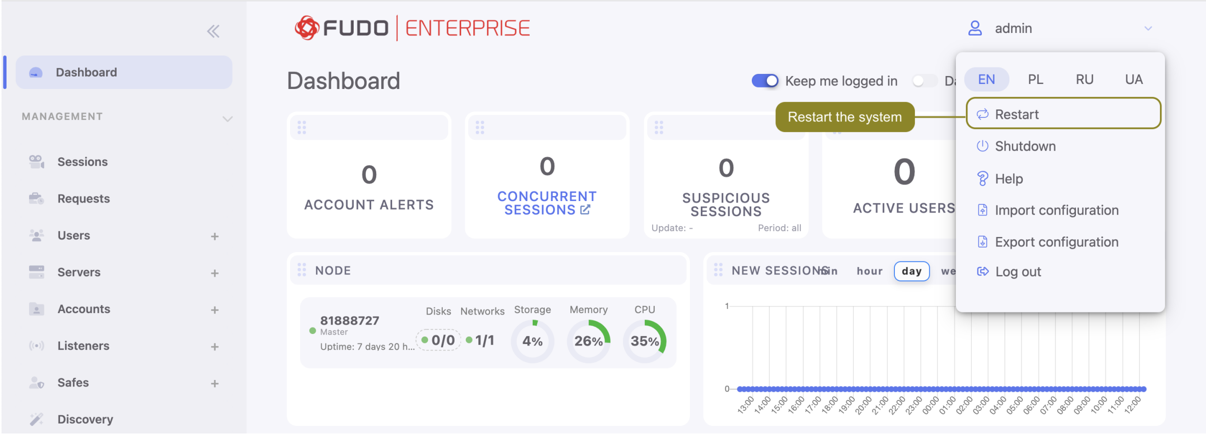
- *System initiation*
- *System update*

22.11 System restart

Note:

- System restart requires USB flash drive with the encryption key connected to the device.
- Restarting the system will terminate all current users' connections.
- Use the *Deny new connections* option in the *Sessions* section in the system settings menu.

1. Connect one of the USB flash drives containing the encryption key.
2. Select *Restart* from user options menu.



3. Select the previous system revision to be loaded after restarting the system.

Note: Current system version is selected by default.

Warning: Restoring the system to the previous version will bring back the system's state prior the update. **Session data** and **configuration changes** in the current system revision will be lost. This includes the **password changers** activity. If any passwords were changed during the newer version's usage, restarting Fudo will lead to lost access to corresponding systems.

4. Click *Confirm* to proceed with restarting the system to the selected revision.

Related topics:

- *System initiation*
- *System version restore*

22.12 SNMP

Fudo Enterprise's status can be monitored over SNMPv3 protocol.

22.12.1 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*.

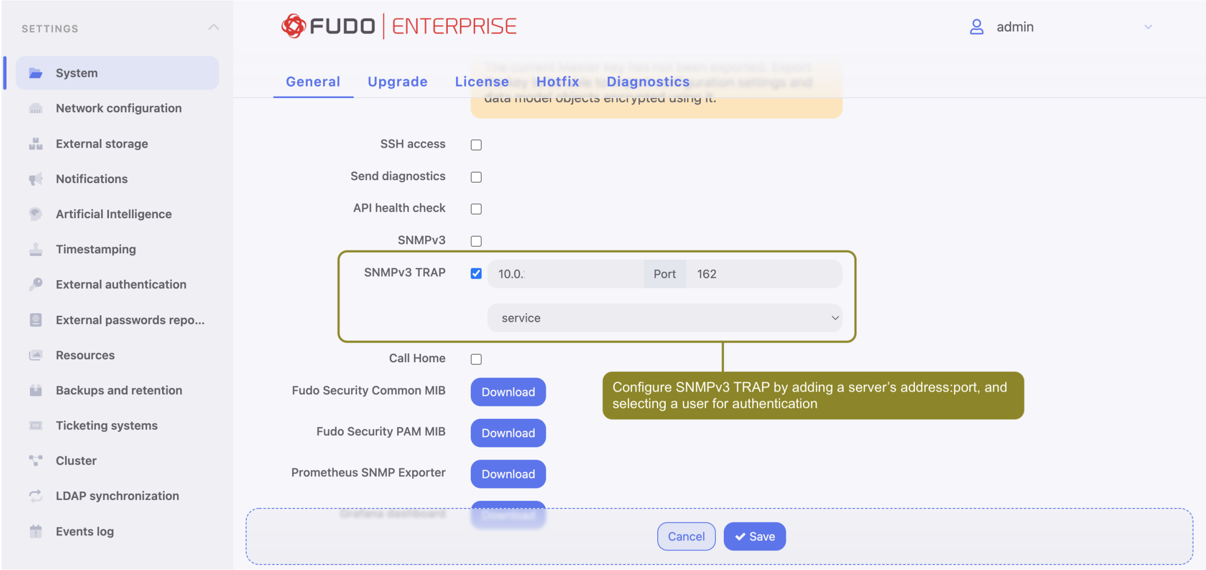
22.12.2 Configuring SNMPv3 TRAP

On *Policies* violation, Fudo is able to send a SNMPv3 TRAP, `fudoPolicyViolationNotification` with information containing during which session which user violated which policy. For more details check Fudo's MIB definition in the following section.

To configure SNMP TRAPs the administrator has to configure the service in the System settings and enable them for particular policy.

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

1. Create a user for SNMPv3 service:
   - Select *Management > Users*.
   - Create a new one.
   - Enter Login.
   - Choose the `service` in the *Role* field.
   - Select `Password` in the *Authentication Type* field and provide your password.
   - In the *SNMP* section, define the settings:
     - Enable SNMP.
     - Select `SHA` or `MD5` in the *Authentication Method* field.
     - Select *AES* or *DES* in the *Encryption* field.
   - Click *Save*.
2. Configure SNMPv3 TRAP:
   - Select *Settings > System*
   - Scroll down to the *Maintenance and supervision* section
   - Configure the SNMPv3 TRAP *server address* and *port*
   - Select the user with `service` role, created in step 1.
   - Click *Save*.



SSH access □

Send diagnostics □

API health check □

SNMPv3 □

SNMPv3 TRAP ☑ 10.0. Port 162

service

Call Home □

Fudo Security Common MIB

Fudo Security PAM MIB

Prometheus SNMP Exporter

Configure SNMPv3 TRAP by adding a server's address:port, and selecting a user for authentication

As Fudo Enterprise uses SNMPv3 for sending TRAPs, the manager software (such as snmptrapd from Net-SNMP) has to know the user's name and password.

Note: The `fudoPolicyViolationNotification` TRAP contains Fudo object identifiers: `sessionId`, `userId` and `policyId`. As all identifiers in Fudo Enterprise are 64-bit integers and SNMP doesn't support 64-bit integers natively, those ids are encoded as big-endian 8-byte arrays.

22.12.3 SNMP MIBs

Fudo Enterprise supports following MIBs:

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790) - partly supported
- UCD-SNMP-MIB

22.12.4 Getting SNMP readings using `snmpwalk`

Note: Getting SNMP readings requires installing *Net-SNMP 5.7.3*.

Fetching all SNMP information

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}" -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1
```

Fetching specific SNMP information

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}" -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1.3.6.1.4.1.24410
```

Data specifier	Description
.1.3.6.1.4.1.24410.1.1.1	Disk status (ZFS status)
.1.3.6.1.4.1.24410.1.1.2	Power supply status **Note:** This feature is not supported on all Fudo Enterprise units. Contact technical support for more information.
.1.3.6.1.4.1.24410.1.1.3	CPU temperatures
.1.3.6.1.4.1.24410.1.1.4	S.M.A.R.T status

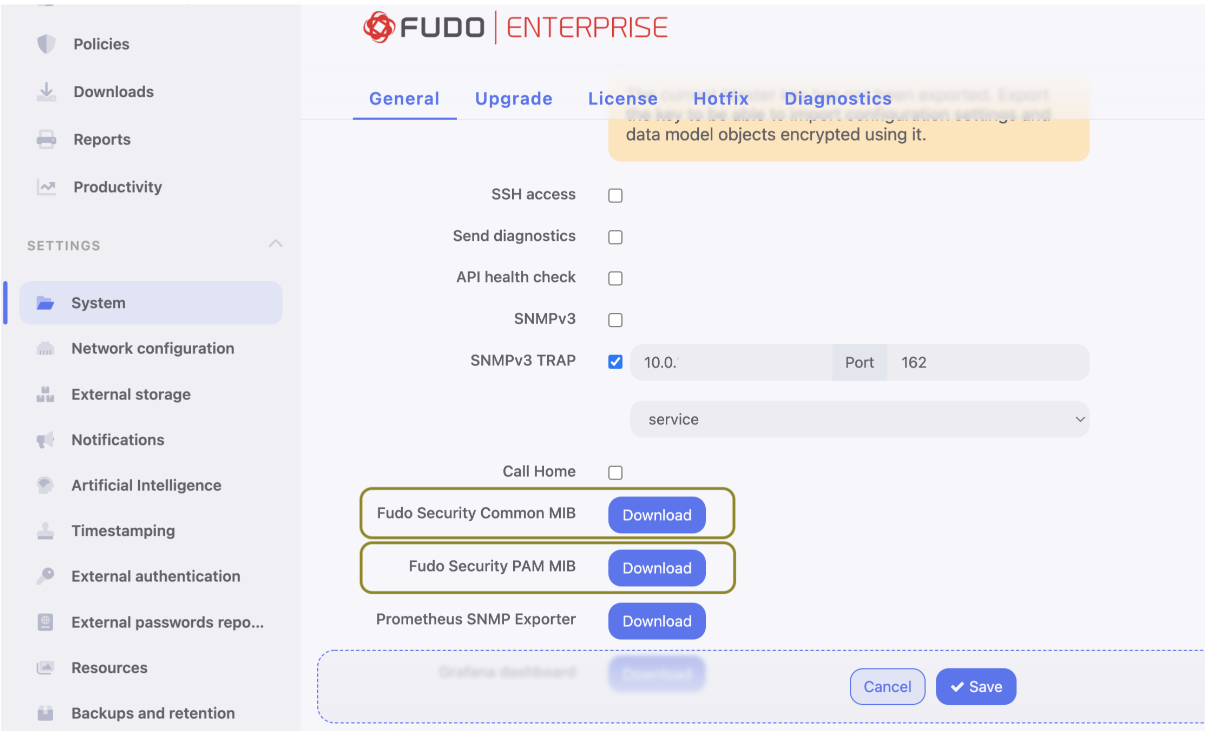
22.12.5 Fudo Enterprise specific SNMP extensions

Overview

Extensions enable monitoring the number of active sessions, ZFS status, PSU status (if available), CPU temperature on all cores, S.M.A.R.T status such as temperature, health or reallocated sectors.

MIB specification file

MIB specification files (Fudo Security Common MIB and Fudo Security PAM MIB) are available for downloading at the Settings > System in the *Maintenance and supervision* section:



data model objects encrypted using it.

SSH access ☐

Send diagnostics ☐

API health check ☐

SNMPv3 ☐

SNMPv3 TRAP ☑ 10.0. Port 162

service

Call Home ☐

Fudo Security Common MIB Download
Fudo Security PAM MIB Download
Prometheus SNMP Exporter Download
Grafana dashboard Download
Cancel
Save

Related topics:

- *Security measures*
- *Troubleshooting*
- *Policies*

22.13 Backups and retention

22.13.1 System backup

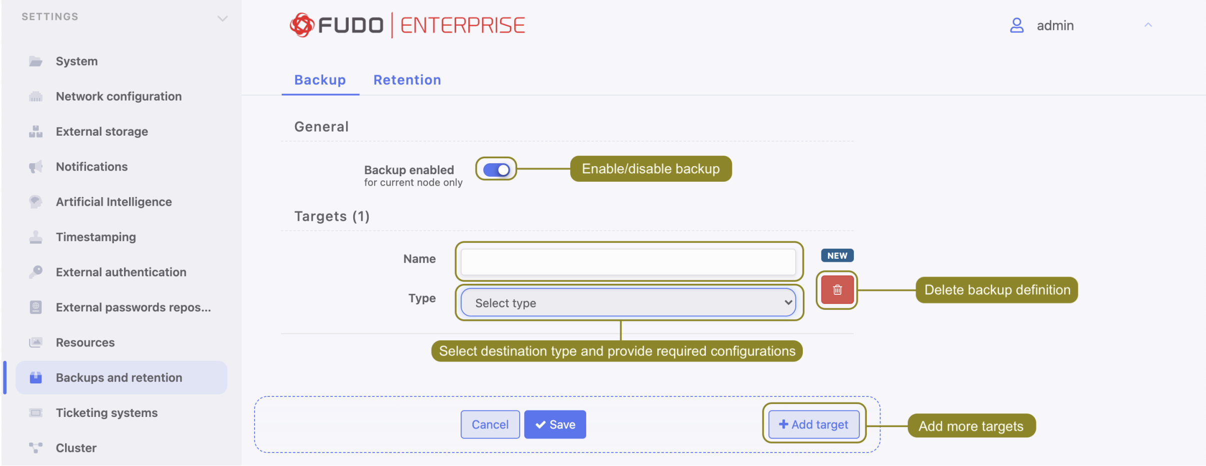
Warning: Data backup contains confidential information.

Fudo allows configuring multiple backup target destinations, where data can be stored. Each backup target can have S3, Backblaze, FTP, or SFTP as a destination place.

To enable automated backups service, proceed as follows.

1. Select *Settings* > *Backups and retention*.
2. Select *Backup enabled* option. Please note that in case of the configured cluster, this option enables backup for the current node only.
3. Click *+Add target* in order to add your future backup target place.
4. Set a name for your backup target.
5. Select a type: S3, Backblaze, FTP or SFTP.
6. Provide additional data depending on the selected connection type:

- With **S3** type chosen, provide additionally: *Bucket*, *Directory*, *Access key*, *Secret Access key*, *Region* and *Endpoint*.
- Configuring a **Backblaze** backup target, provide: *Bucket*, *Directory* and credentials, such as *Account* and *Key*.
- For **FTP** type backup target provide: *Directory*, *Server address* and credentials, such as *Username* and *Password*.
- For **SFTP** type backup target provide: *Directory*, *Server address*, *Username*, *User private key*, *Server public key* and *Port* number.



Enable/disable backup

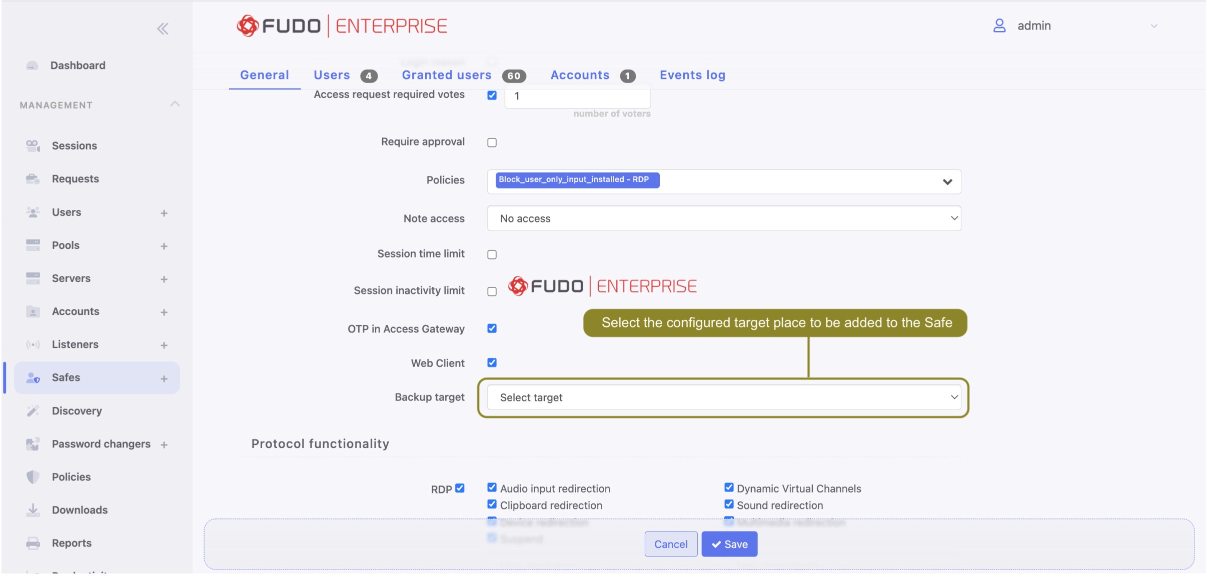
Delete backup definition

Select destination type and provide required configurations

Add more targets

7. Click *Save*.

Now, the configured *Backup target* can be added to the Safe settings to enable automatic storing the sessions and safe data in the defined target place.



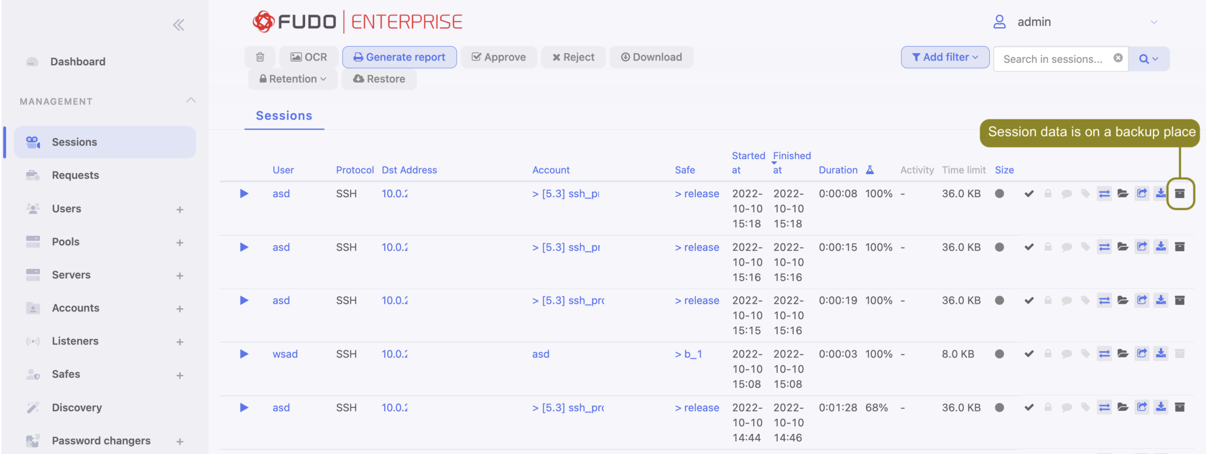
Access request required votes	☑ 1 (number of voters)
Require approval	□
Policies	Block_user_only_input_installed - RDP
Note access	No access
Session time limit	□
Session inactivity limit	□
OTP in Access Gateway	☑
Web Client	☑
Backup target	Select target

Protocol functionality

RDP ☑ ☑ Audio input redirection ☑ Clipboard redirection ☑ Dynamic Virtual Channels ☑ Sound redirection

Select the configured target place to be added to the Safe

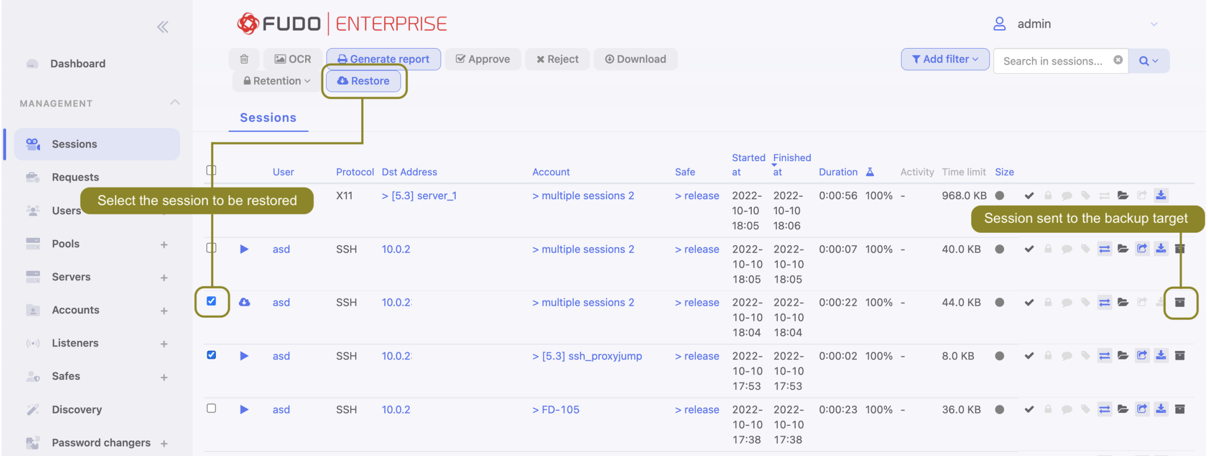
Sessions data that was sent to the backup target place is assigned with the respective icon on the Sessions list.



Session data is on a backup place

User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
asd	SSH	10.0.:	> [5.3] ssh_p	> release	2022-10-10 15:18	2022-10-10 15:18	0:00:08	100%	-	36.0 KB
asd	SSH	10.0.:	> [5.3] ssh_p	> release	2022-10-10 15:16	2022-10-10 15:16	0:00:15	100%	-	36.0 KB
asd	SSH	10.0.:	> [5.3] ssh_prc	> release	2022-10-10 15:15	2022-10-10 15:16	0:00:19	100%	-	36.0 KB
wsad	SSH	10.0.:	asd	> b_1	2022-10-10 15:08	2022-10-10 15:08	0:00:03	100%	-	8.0 KB
asd	SSH	10.0.:	> [5.3] ssh_prc	> release	2022-10-10 14:44	2022-10-10 14:46	0:01:28	68%	-	36.0 KB

If the session has its backup version stored outside of Fudo Enterprise, it can be downloaded from the backup place to the Fudo Enterprise local instance with the *Restore* option.



Select the session to be restored

Session sent to the backup target

	User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
		X11	> [5.3] server_1	> multiple sessions 2	> release	2022-10-10 18:05	2022-10-10 18:06	0:00:56	100%	-	968.0 KB
□	asd	SSH	10.0.2	> multiple sessions 2	> release	2022-10-10 18:05	2022-10-10 18:05	0:00:07	100%	-	40.0 KB
☑	asd	SSH	10.0.2	> multiple sessions 2	> release	2022-10-10 18:04	2022-10-10 18:04	0:00:22	100%	-	44.0 KB
☑	asd	SSH	10.0.2	> [5.3] ssh_proxyjump	> release	2022-10-10 17:53	2022-10-10 17:53	0:00:02	100%	-	8.0 KB
□	asd	SSH	10.0.2	> FD-105	> release	2022-10-10 17:38	2022-10-10 17:38	0:00:23	100%	-	36.0 KB

Restoring system from backup

System restore service is provided by the technical support department on terms agreed in the SLA.

Related topics:

- *Exporting/importing system configuration*
- *Security measures*
- *Creating a new safe*

22.13.2 Data retention

Fudo Enterprise supports two data retention scenarios depending on the availability of external storage:

- **Two-steps retention:** Initially, data is transferred from the internal storage to external storage connected via a fiber channel interface. After defined time period session data is automatically deleted.
- **One-step retention:** If external storage is not used, sessions will be immediately deleted from Fudo Enterprise.

For more information on configuring the external storage, see the *External storage* chapter.

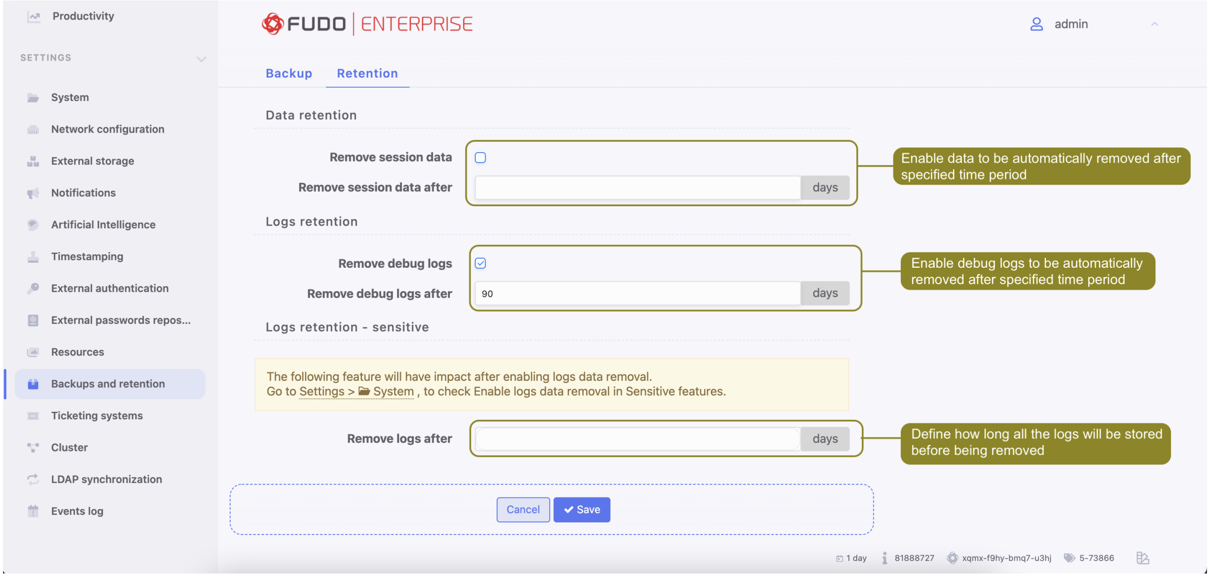
Note: Sessions which have been exported and the content is still available for download, will not be deleted automatically. These sessions must be either *deleted manually* or you must delete the exported material in the *Downloads* section for the retention mechanism to delete those session.

Enabling data retention

To enable data retention service, proceed as follows.

1. Select *Settings > Backups and retention > Retention.*
2. Select *Remove session data* option in the *Data retention* section to have the data automatically removed after specified time period.
3. Define how long data will be stored before being removed.
4. Select *Remove debug logs* option in the *Logs retention* section to have the debug logs automatically removed after specified time period.
5. Define how long debug logs will be stored before being removed. Default value is 90 days.
6. In the *Logs retention - sensitive* section define how long all the logs will be stored before being removed.

Warning: The following feature will have impact after enabling logs data removal. Go to *Settings > System* to check *Enable logs data removal* option in the *Sensitive features and system security* section.



Data retention

Remove session data □

Remove session data after days

Enable data to be automatically removed after specified time period

Logs retention

Remove debug logs ☑

Remove debug logs after 90 days

Enable debug logs to be automatically removed after specified time period

Logs retention - sensitive

The following feature will have impact after enabling logs data removal.
Go to Settings > System , to check Enable logs data removal in Sensitive features.

Remove logs after days

Define how long all the logs will be stored before being removed

7. Click *Save*.

Overwriting the global value of the data retention for accounts

It is possible to overwrite the value of the data retention parameter for the selected account. To specify the value of the data retention parameter in the account settings, proceed as follows.

1. Select *Management* > *Accounts*.
2. Find and click desired object's name to open its configuration page.
3. In the *Data retention* section, define automatic data removal settings.
   - Select *Override global retention settings* option to set other than global retention values for connections established using this account.
   - Check the *Delete session data* option to exclude sessions from retention mechanism.
   - Next to the *Delete session data* field, define the number of days after which the session data will moved to external storage device. Default value when the option is checked, is 30 days.
4. Click *Save*.

Note:

- Defining the retention parameter value in the account settings will not activate data retention itself. Data retention has to be enabled globally (from the menu *Settings* > *Backups and retention* > *Retention*).
- Global retention parameter values have lower priority than the values set in the *accounts*.
- Global retention settings are replicated within the *cluster configuration*. Please note that *Remove session data after* variable is not replicated within the cluster but is set per node.

Sessions' retention lockdown

Fudo Enterprise allows for excluding selected sessions from the retention mechanism. Session exclusion procedure is described in chapter *Sessions' retention lockdown*.

Related topics:

- *Security measures*
- *Exporting/importing system configuration*
- *Creating a new safe*

22.14 External storage

Fudo Enterprise 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.

22.14.1 Configuring external storage

1. Select *Settings > External storage*.

Note: Fiber channel cards status is depicted by the icons.

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

2. Select fiber channel cards operating mode.
   - Failover - data is transmitted using one fiber channel interface. If the card fails, the other one takes over ensuring continuous availability of the external storage device.
   - Load balancing - both fiber channel interfaces are used to transfer data between Fudo Enterprise and the external storage device.
3. In the *External storage devices* section, select desired *WWN* object and click the 🔗 icon.

Note: Click the 🔄 icon to refresh the list of available storage devices.

4. Click *Save* and proceed with enabling *session data retention*.

22.14.2 Expanding external storage device

After resizing the WWN object, it must be expanded in Fudo Enterprise in order to take advantage of the additional storage space.

> **Warning:** The storage device cannot be down-sized after it has been expanded.

1. Select *Settings > External storage*.
2. In the section describing the *WWN* object click *Expand*.
3. Confirm expanding external storage.
4. Click *Save*.

Related topics:

- *System backup*

22.15 Exporting/importing system configuration

Fudo Enterprise enables exporting current system state, defined objects and configuration settings, which later can be used to initiate the system.

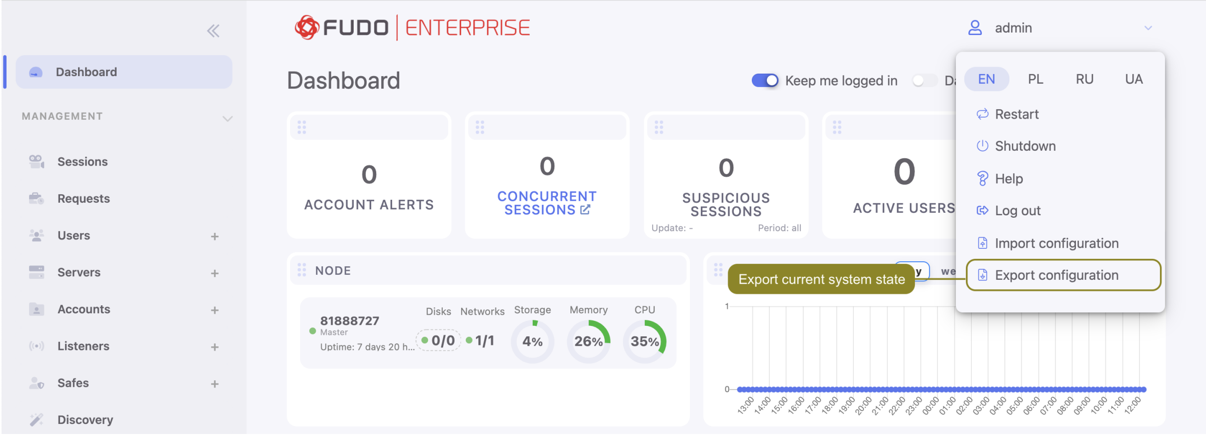
> **Warning:** Exported configuration data contains confidential information.

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

22.15.1 Exporting system configuration

To export system configuration, proceed as follows.

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



22.15.2 Importing system configuration

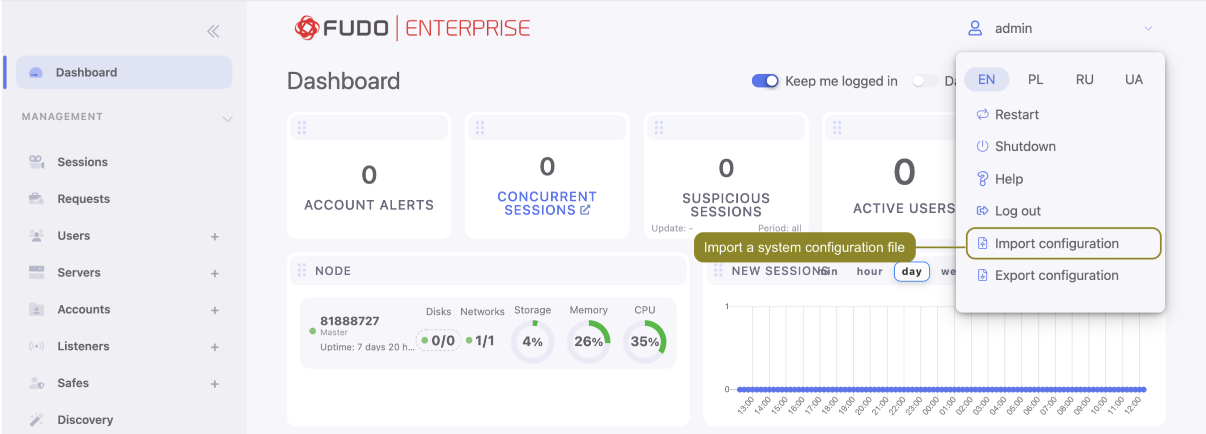
Warning: Importing a configuration file and initiating system with imported data will delete all existing session data.

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*
- *System backup*
- *System initiation*
- *System update*

22.16 Cluster configuration

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

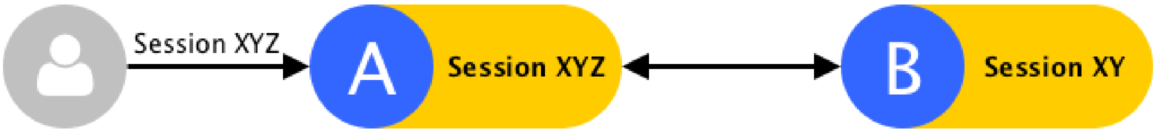
Warning:

- Cluster configuration does not facilitate data backup. If session data is deleted on one of the cluster nodes, it is also deleted from other nodes.
- Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances must not be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

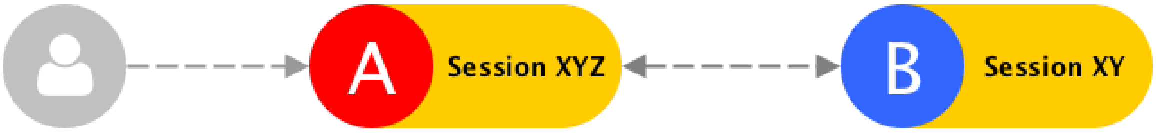
Data replication between cluster nodes is highly customizable. The administrator can choose the node that the data will be replicated to as well as which data (data model objects/session data) is replicated.

In case of a node failure, user access requests will be picked up by another cluster node, determined by the *redundancy group priority*.

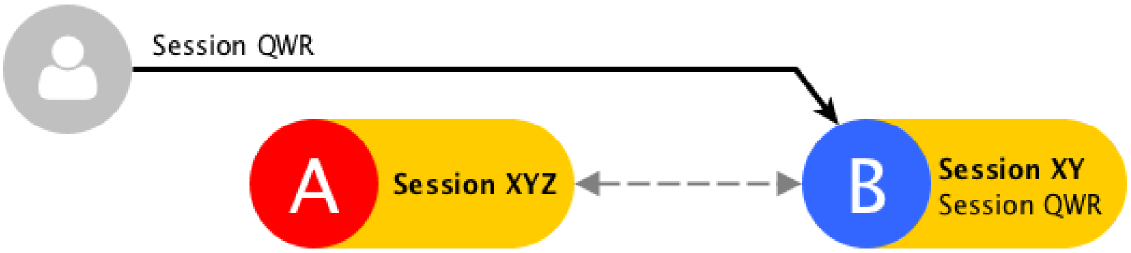
Current session data is replicated to other nodes while the connection is still ongoing.



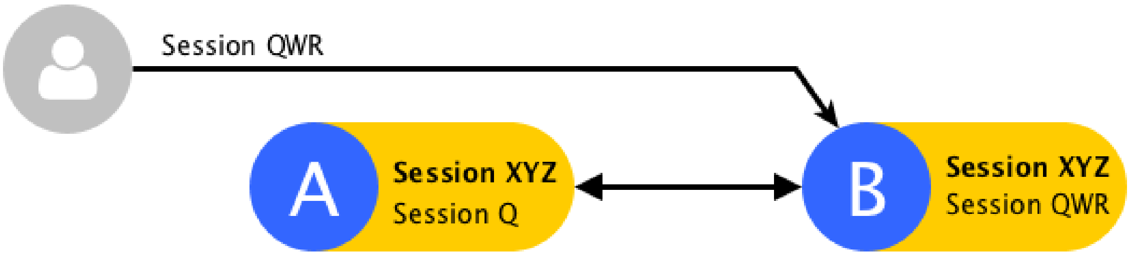
If the node that fails was recording sessions, those sessions will be terminated. . .



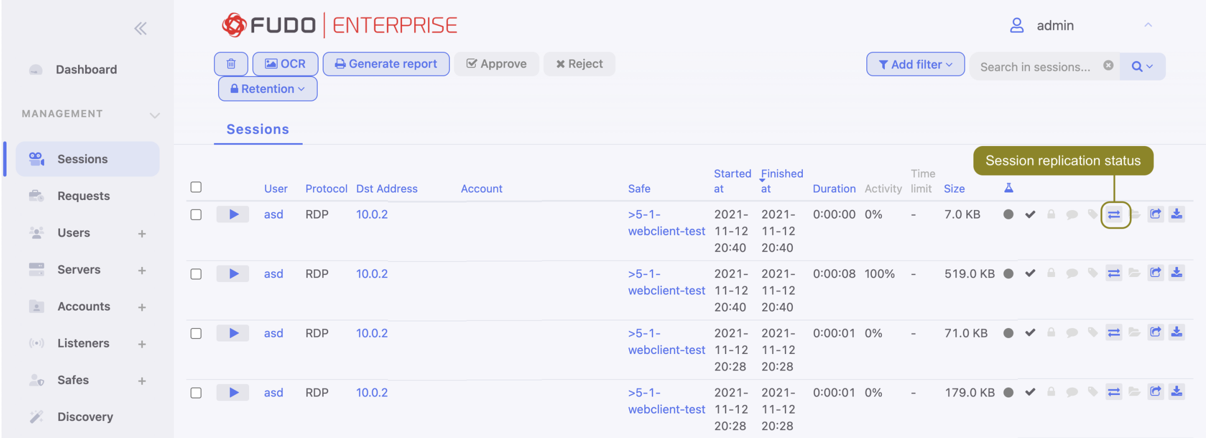
. . . and users will have to reconnect.



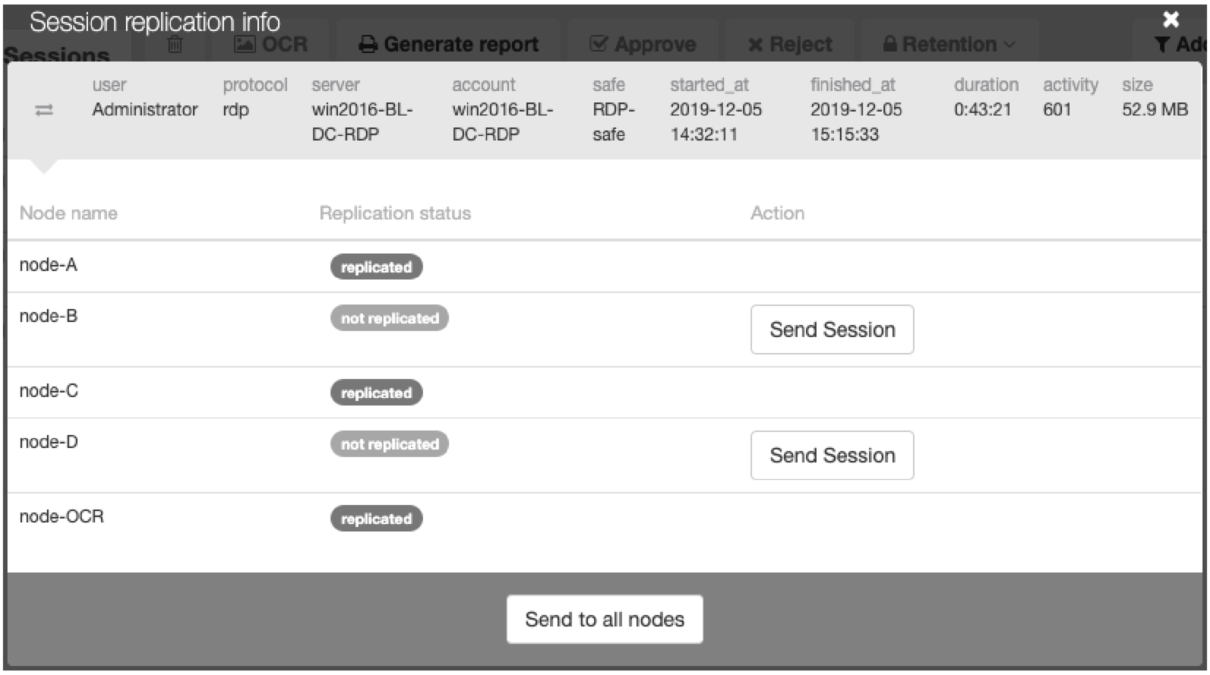
A part of the session data from the node that malfunctioned, which has synchronized, can be accessed on the other nodes, but the session will be fully accessible once the node becomes operational and session data is synchronized between cluster nodes.



Session replication status can be verified by clicking the ⇄ icon on the sessions list.



☐		User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
☐	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:40	2021-11-12 20:40	0:00:00	0%	-	7.0 KB
☐	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:40	2021-11-12 20:40	0:00:08	100%	-	519.0 KB
☐	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:28	2021-11-12 20:28	0:00:01	0%	-	71.0 KB
☐	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:28	2021-11-12 20:28	0:00:01	0%	-	179.0 KB



	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

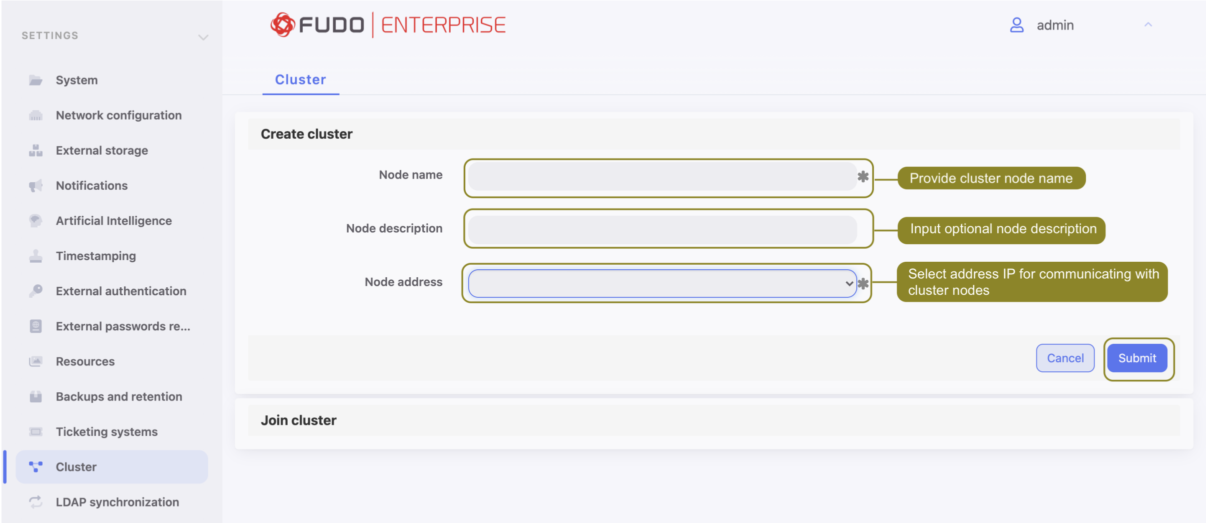
Node name	Replication status	Action
node-A	replicated	
node-B	not replicated	Send Session
node-C	replicated	
node-D	not replicated	Send Session
node-OCR	replicated	

22.16.1 Initiating cluster

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

To initiate Fudo Enterprise cluster, proceed as follows.

1. Select *Settings > Cluster*.
2. Click *Create cluster*, to display cluster definition options.
3. Provide node name and description helping identify given object.
4. From the *Address* drop-down list, select IP address for communicating with other cluster nodes.



Provide cluster node name

Input optional node description

Select address IP for communicating with cluster nodes

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*

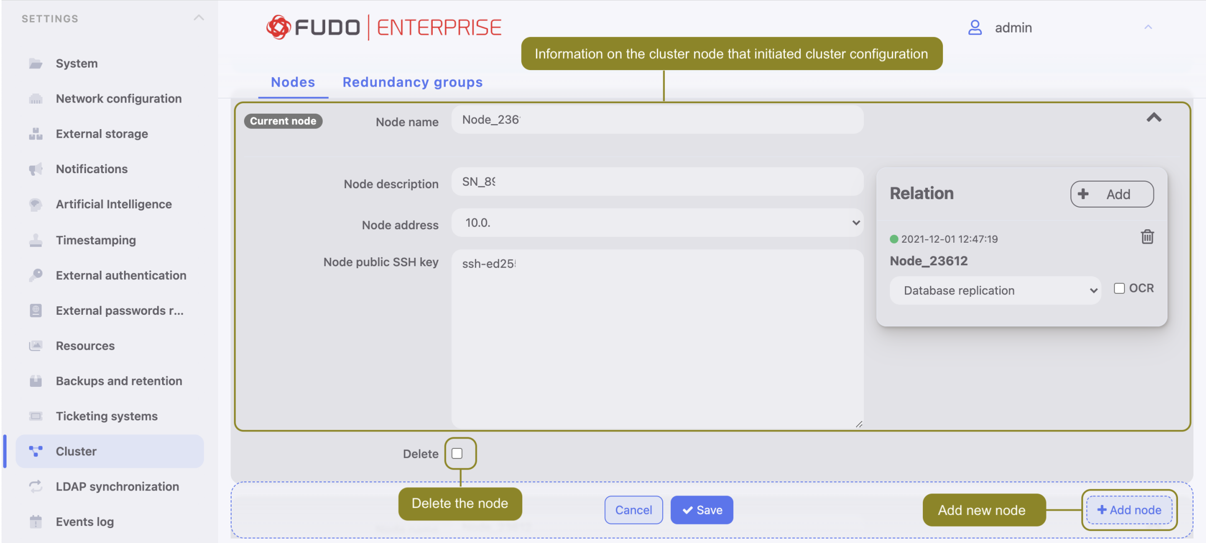
22.16.2 Adding cluster nodes

Warning:

- Session and configuration data (*servers*, *users*, *safes*, *accounts*, *listeners*, *external authentication servers*) of the joining node are deleted and initiated with data replicated from the cluster.
- Data model objects: *safes*, *users*, *servers*, *accounts* and *listeners* are replicated within the cluster and object instances must not be added on each node. In case the replication mechanism fails to copy objects to other nodes, contact technical support department.

To add a node to Fudo Enterprise cluster, proceed as follows.

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



Information on the cluster node that initiated cluster configuration

Node name: Node_236

Node description: SN_8§

Node address: 10.0.

Node public SSH key: ssh-ed25

● 2021-12-01 12:47:19

Node_23612

Database replication □ OCR

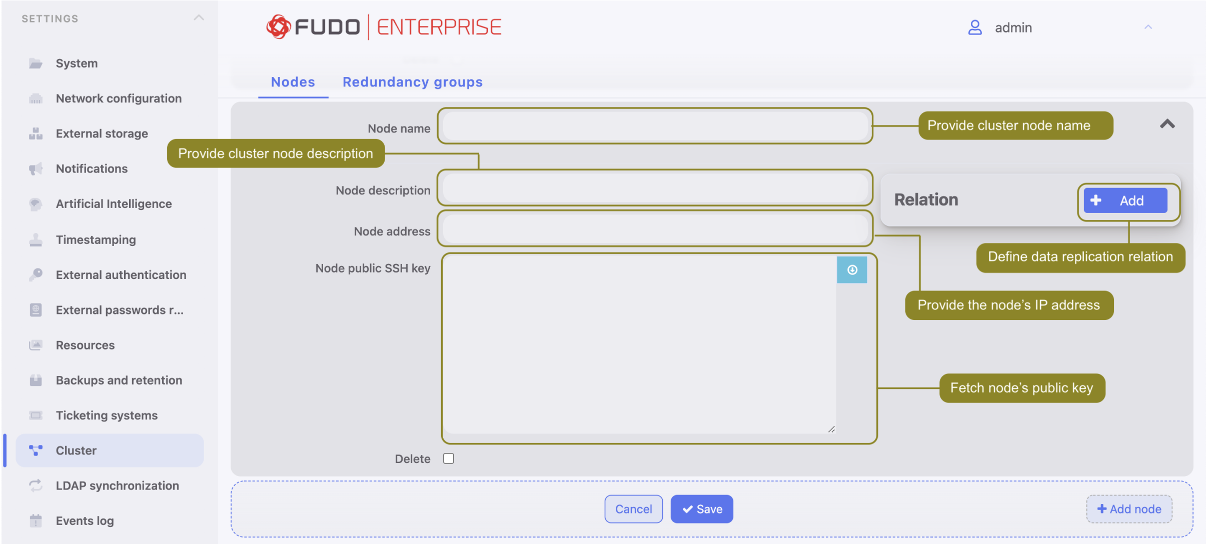
Delete □

Delete the node

Add new node

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.



Provide cluster node name

Provide cluster node description

Define data replication relation

Provide the node's IP address

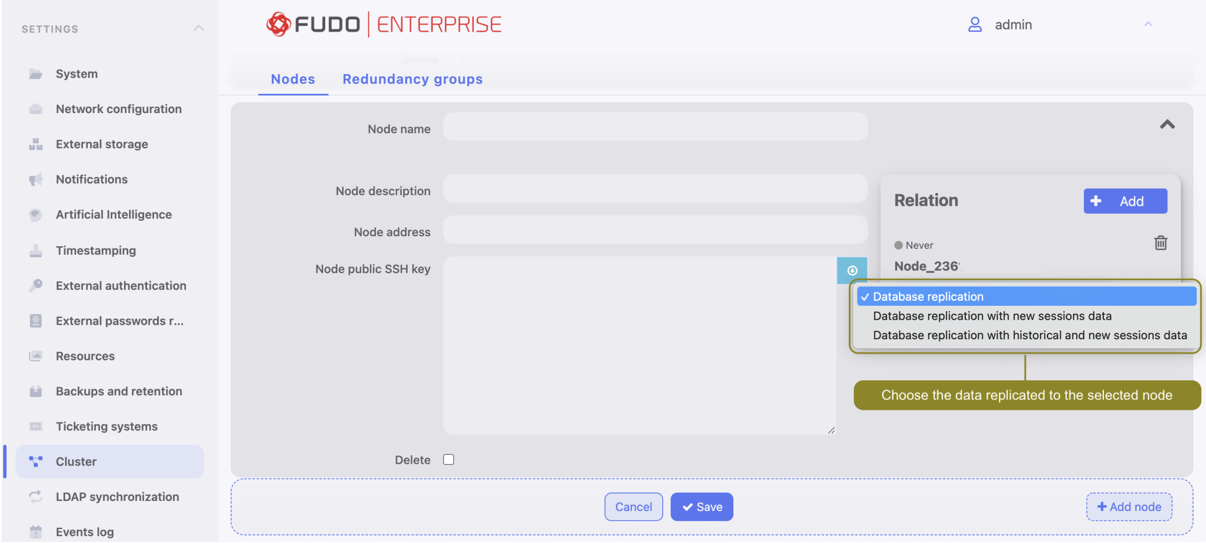
Fetch node's public key

6. Click ⊙ to download node's public SSH key.

7. In the *Relations* section, click + *Add*.

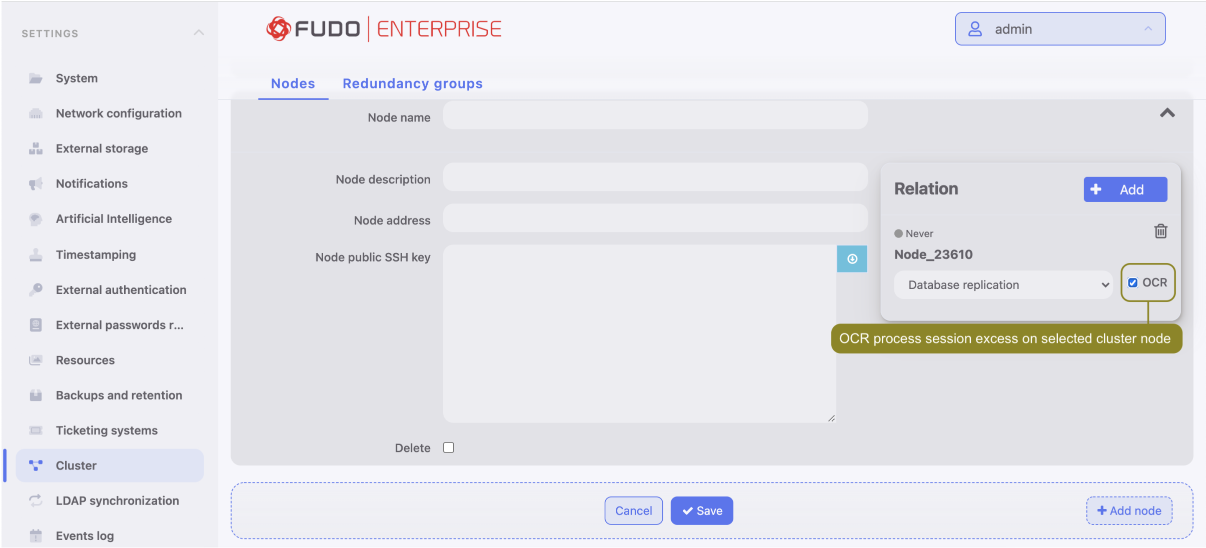
8. Select the cluster node to which the data from the given node will be replicated.

9. Select which data will be replicated.



Choose the data replicated to the selected node

10. Select *OCR* option to delegate OCR processing in case they cannot be processed locally.



● Never

Node_23610

Database replication

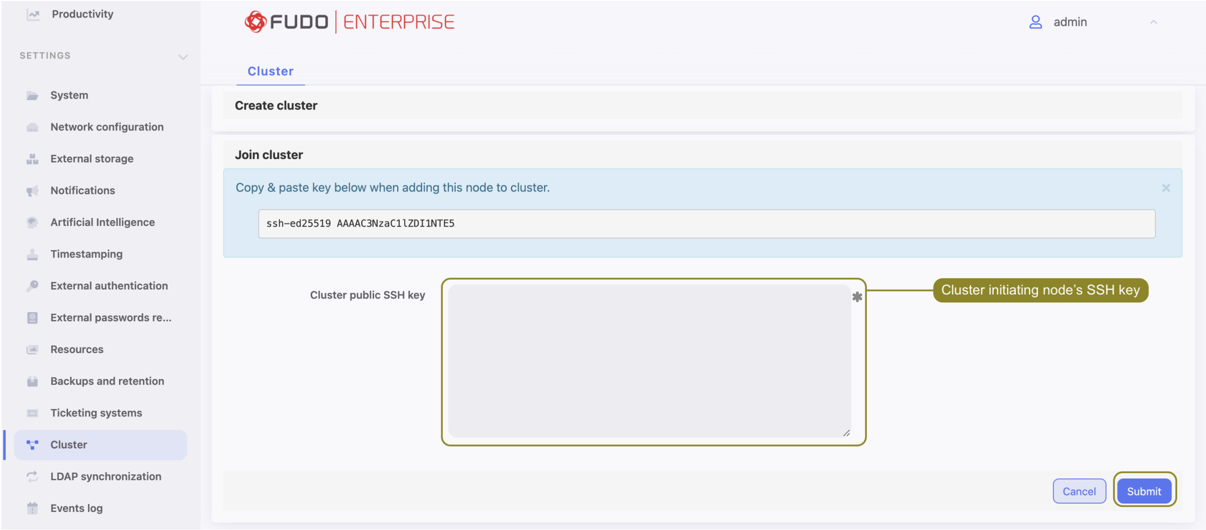
☑ OCR

OCR process session excess on selected cluster node

Note: Each Fudo Enterprise instance has a defined number of resources dedicated to OCR processing. If the *OCR* option is selected, excess of sessions that cannot processed locally at the moment, is forwarded for processing to selected node.

---

11. In the *Relations* section of the primary node, click + *Add*.
12. Select the cluster node to which the data from the given node will be replicated.
13. Select which data will be replicated.
14. Click *Save*, to add node definition.
15. Copy cluster key to clipboard.
16. Log in to administration panel of the joining node.
17. Select *Settings* > *Cluster*.
18. Click *Join cluster*.
19. Paste cluster public SSH key and click *Submit*.



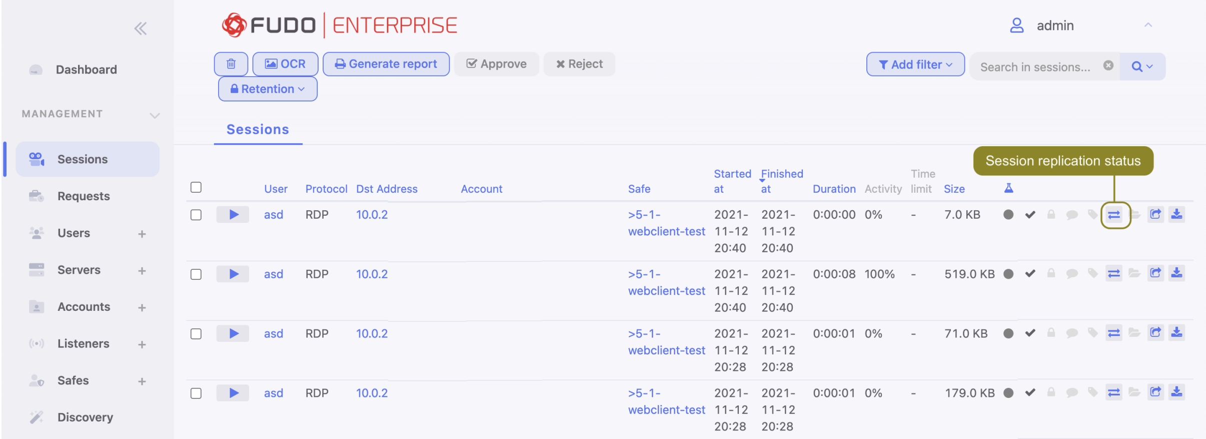
Copy & paste key below when adding this node to cluster.

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5
```

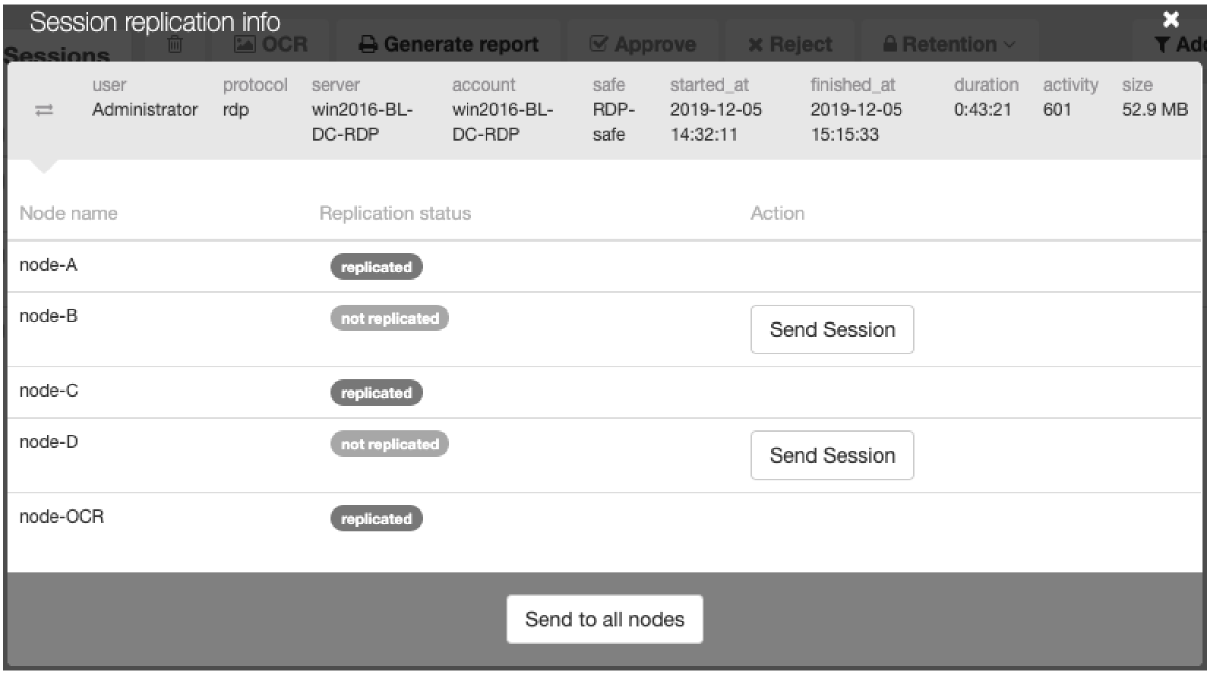
Cluster initiating node's SSH key

20. Click *I understand the consequences, proceed.*

Note: To view session replication status, go to sessions list and click the ⇄ icon.



□		User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Duration	Activity	Time limit	Size
□	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:40	2021-11-12 20:40	0:00:00	0%	-	7.0 KB
□	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:40	2021-11-12 20:40	0:00:08	100%	-	519.0 KB
□	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:28	2021-11-12 20:28	0:00:01	0%	-	71.0 KB
□	▶	asd	RDP	10.0.2		>5-1-webclient-test	2021-11-12 20:28	2021-11-12 20:28	0:00:01	0%	-	179.0 KB



	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*

22.16.3 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*

22.16.4 Deleting cluster nodes

Warning:

- Removing a node and re-adding it to a cluster may result in data loss.
- After removing a node, you will no longer be able to delete session data recorded by this node and replicated to other nodes.

To remove a cluster node, proceed as follows.

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

Related topics:

- *Adding cluster nodes*
- *Editing cluster nodes*
- *Security: Cluster configuration*

22.16.5 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.

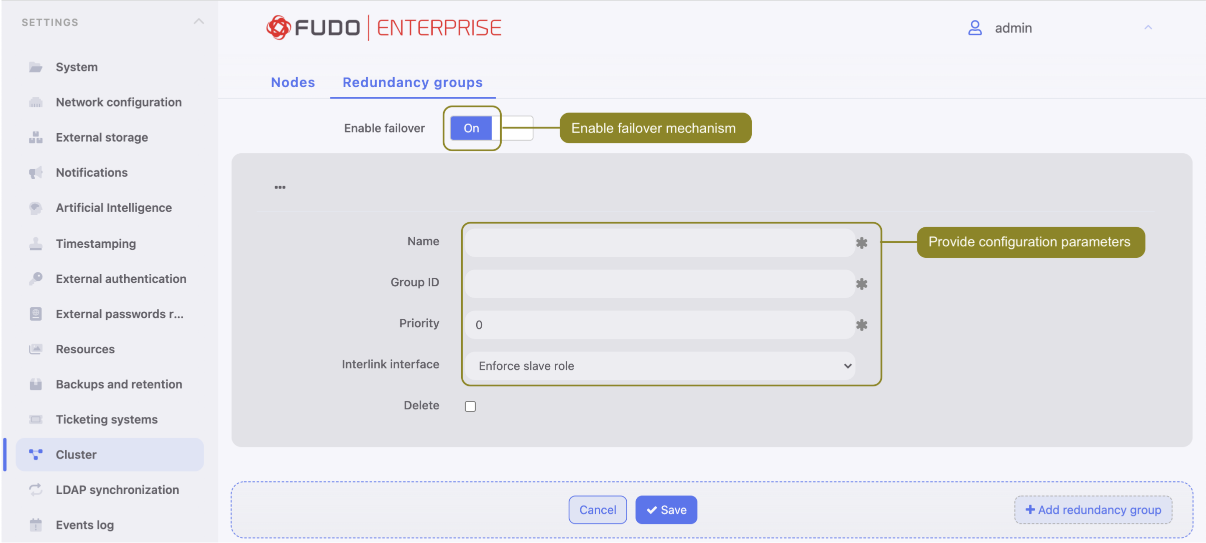
Adding redundancy groups

To add a redundancy group, proceed as follows.

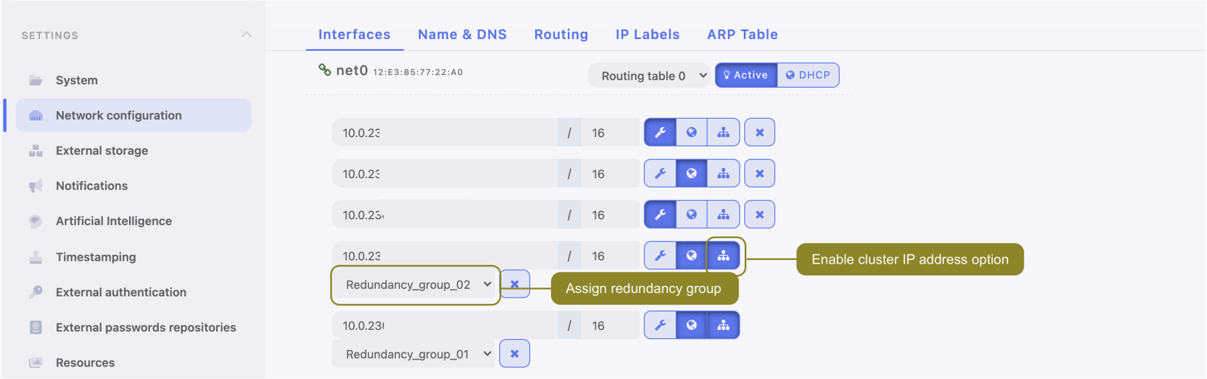
1. Select *Settings* > *Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Click + *Add redundancy group*.
4. Define group properties.

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.



5. Click *Save*.
6. Select *Settings* > *Network configuration*.
7. Click + to add new IP address.
8. Enter IP address and click the 品 icon to mark the entry as a cluster IP address.
9. Assign previously added redundancy group.
10. Click *Save*.



net0 12:E3:85:77:22:A0

Routing table 0

10.0.23 / 16

10.0.23 / 16

10.0.25 / 16

10.0.23 / 16

Redundancy_group_02

10.0.23 / 16

Redundancy_group_01

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*.

Deleting a redundancy group

To delete a redundancy group, proceed as follows.

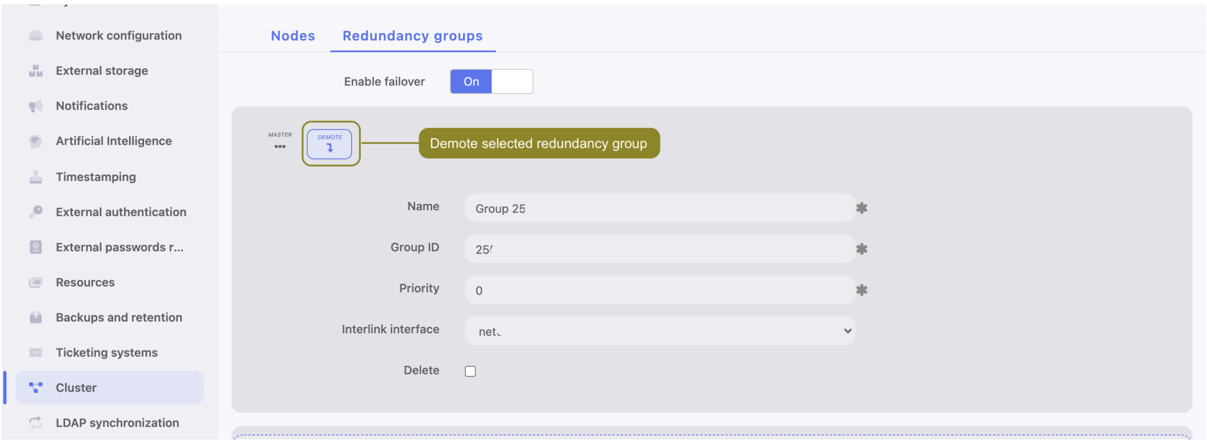
1. Select *Settings* > *Cluster*.
2. Switch to the *Redundancy groups* tab.
3. Select *Delete* next to the desired redundancy group.
4. Click *Save*.

Demoting a redundancy group

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

To demote a redundancy group, proceed as follows.

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



Enable failover: On

Name: Group 25

Group ID: 25

Priority: 0

Interlink interface: net

Delete: □

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*.

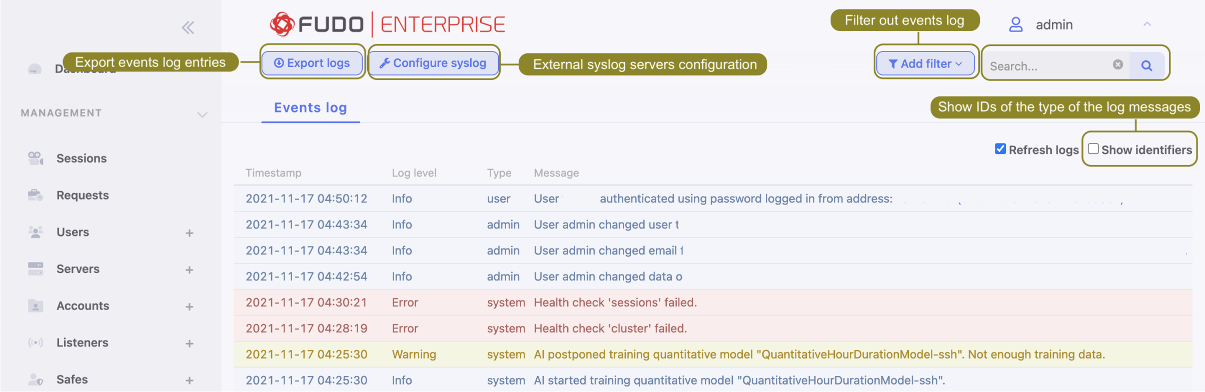
Related topics:

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

22.17 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.



Export events log entries

External syslog servers configuration

Filter out events log

Show IDs of the type of the log messages

Timestamp	Log level	Type	Message
2021-11-17 04:50:12	Info	user	User authenticated using password logged in from address:
2021-11-17 04:43:34	Info	admin	User admin changed user t
2021-11-17 04:43:34	Info	admin	User admin changed email t
2021-11-17 04:42:54	Info	admin	User admin changed data o
2021-11-17 04:30:21	Error	system	Health check 'sessions' failed.
2021-11-17 04:28:19	Error	system	Health check 'cluster' failed.
2021-11-17 04:25:30	Warning	system	AI postponed training quantitative model "QuantitativeHourDurationModel-ssh". Not enough training data.
2021-11-17 04:25:30	Info	system	AI started training quantitative model "QuantitativeHourDurationModel-ssh".

22.17.1 External syslog servers

Note:

- Fudo Enterprise 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:  8483885321111147015) (fudo_session:
8483885321111147219)          (fudo_user:  8483885321111147012) (fudo_connection:
8483885321111147014)    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*.

22.17.2 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.

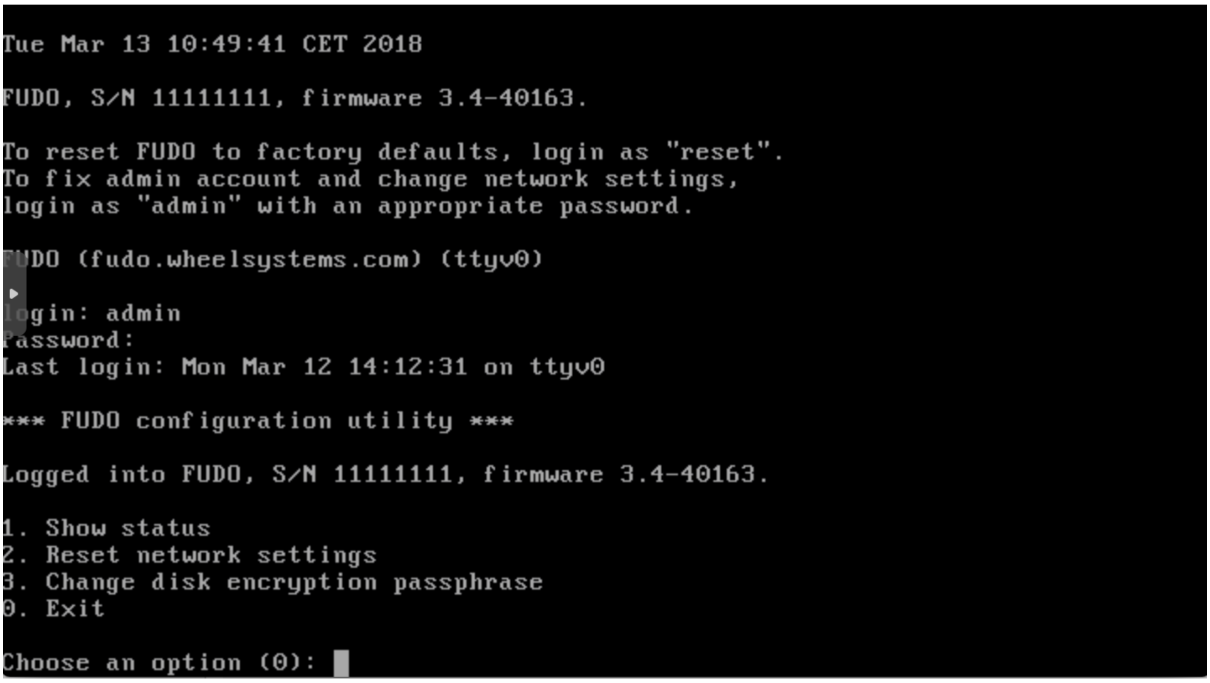
Related topics:

- *Log messages*
- *Security*
- *Managing servers*

22.18 Changing encryption passphrase

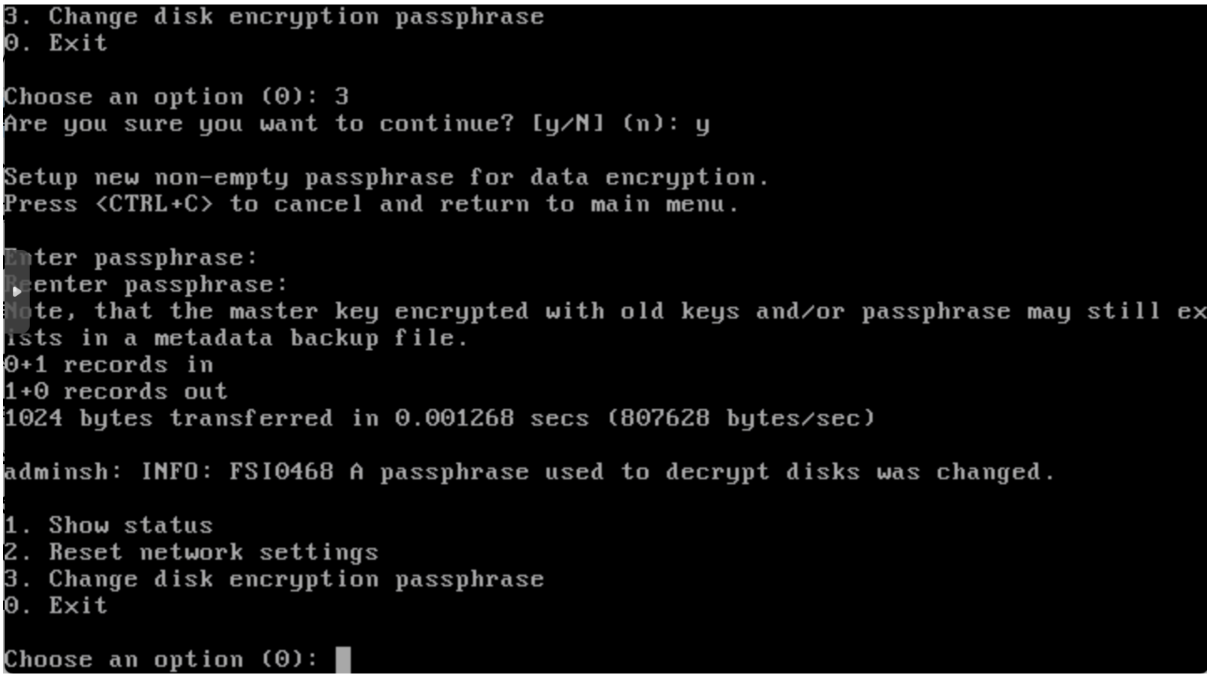
In case of Fudo Enterprise deployed in a virtual environment, data is encrypted using a passphrase. To change current passphrase, proceed as follow.

1. Log in to system console on an account with *superadmin* privileges.
2. Type in 3 and confirm by pressing the *Enter* key.



```
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*
- *System backup*

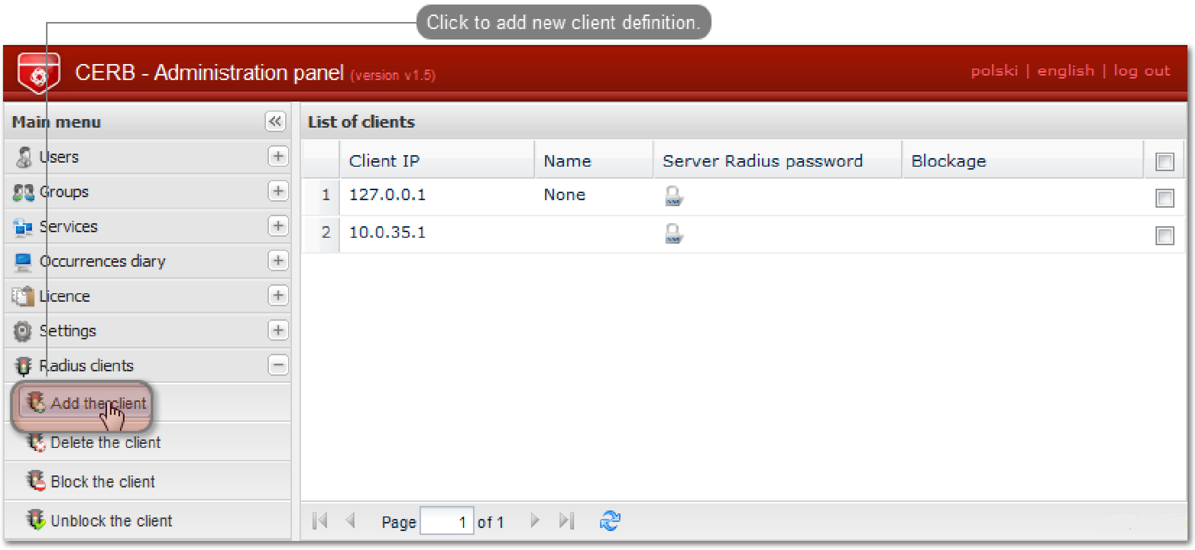
22.19 Integration with CERB server

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

CERB server configuration

1. Adding RADIUS client.

- Select *RADIUS clients > Add client* to add Fudo Enterprise as a RADIUS client.

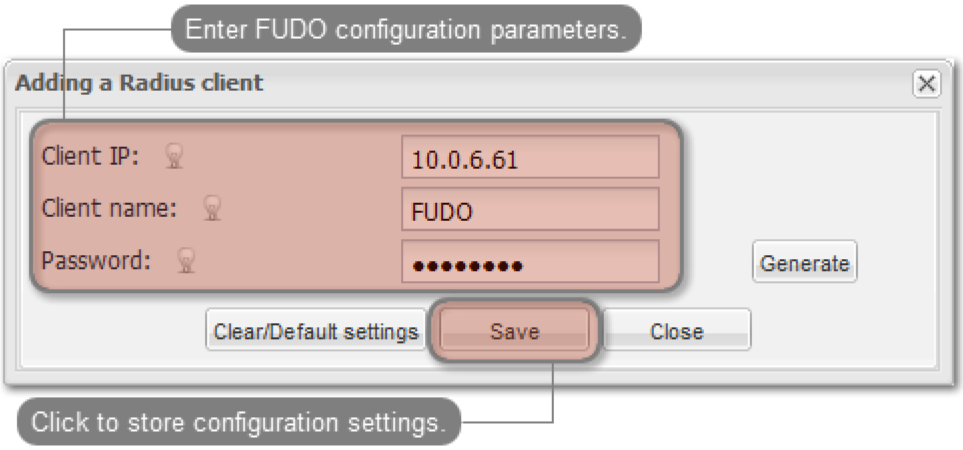


Click to add new client definition.

List of clients

	Client IP	Name	Server Radius password	Blockage	□
1	127.0.0.1	None			□
2	10.0.35.1				□

- Provide Fudo Enterprise 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: •••••••••

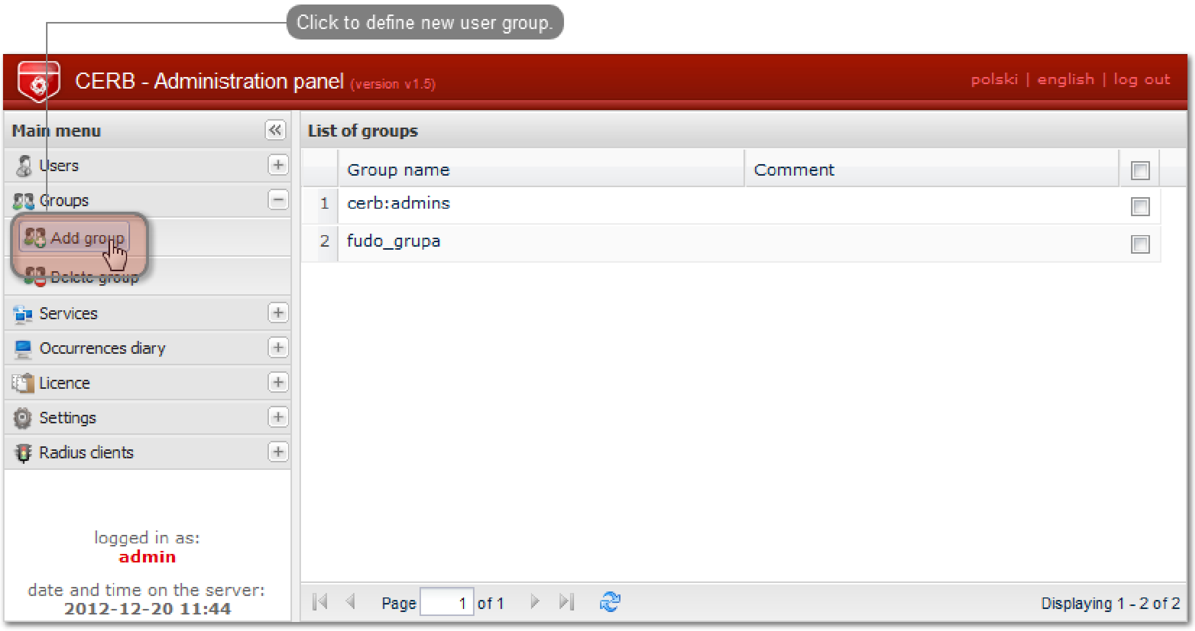
Click to store configuration settings.

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

2. Adding user group.

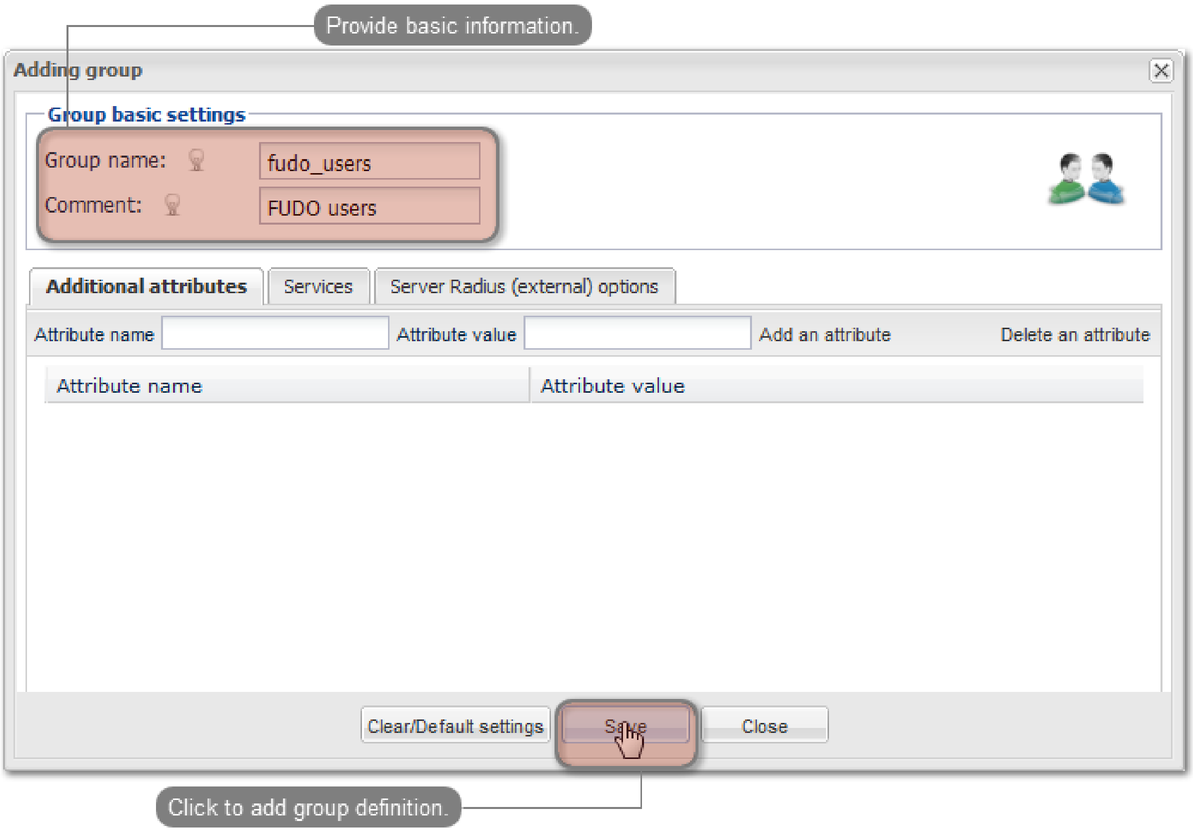
- Select *Groups* > *Add group* to define Fudo Enterprise users who will be authorized by the CERB server.

Click to define new user group.



	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

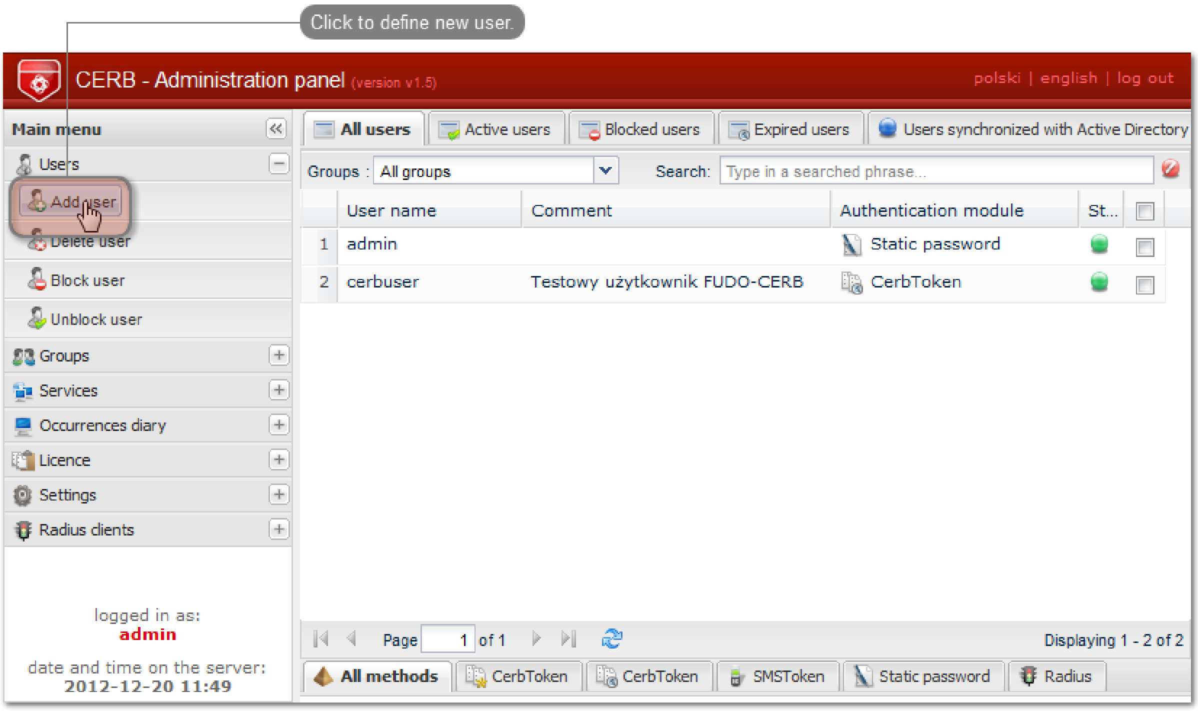
Attribute name	Attribute value

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)

Groups : All groups

Search: Type in a searched phrase...

	User name	Comment	Authentication module	St...	□
1	admin		Static password	●	□
2	cerbuser	Testowy użytkownik FUDO-CERB	CerbToken	●	□

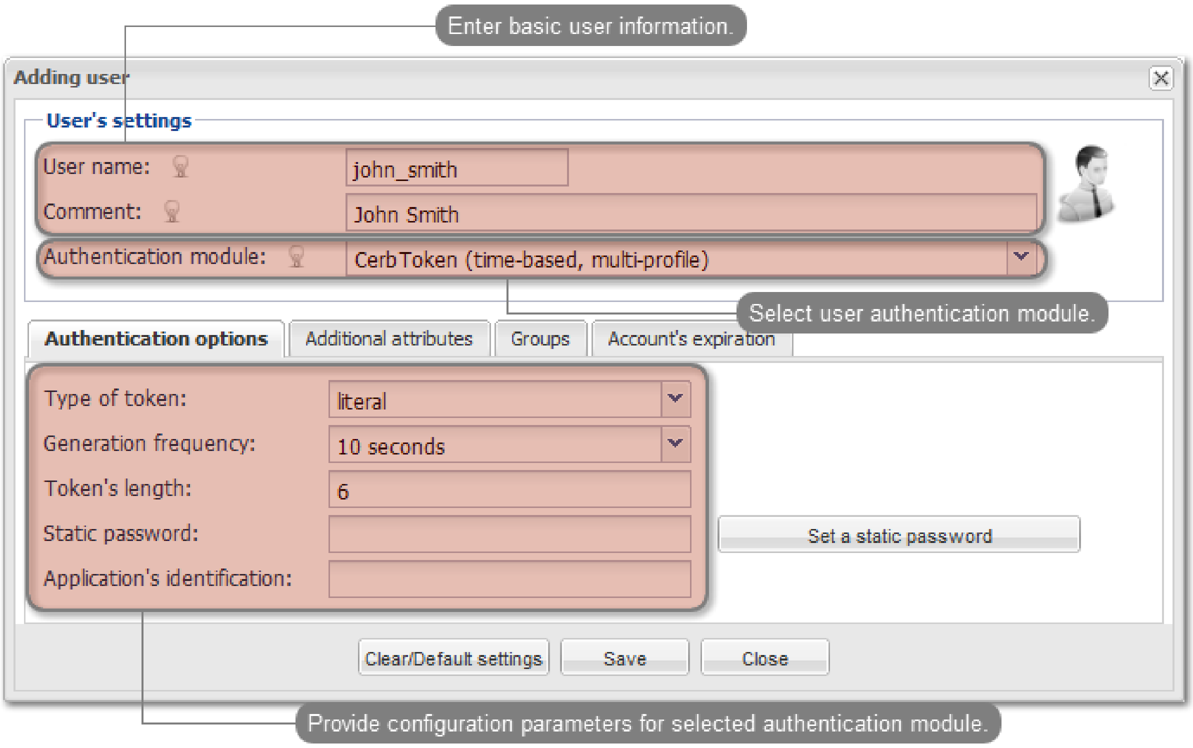
Page 1 of 1

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

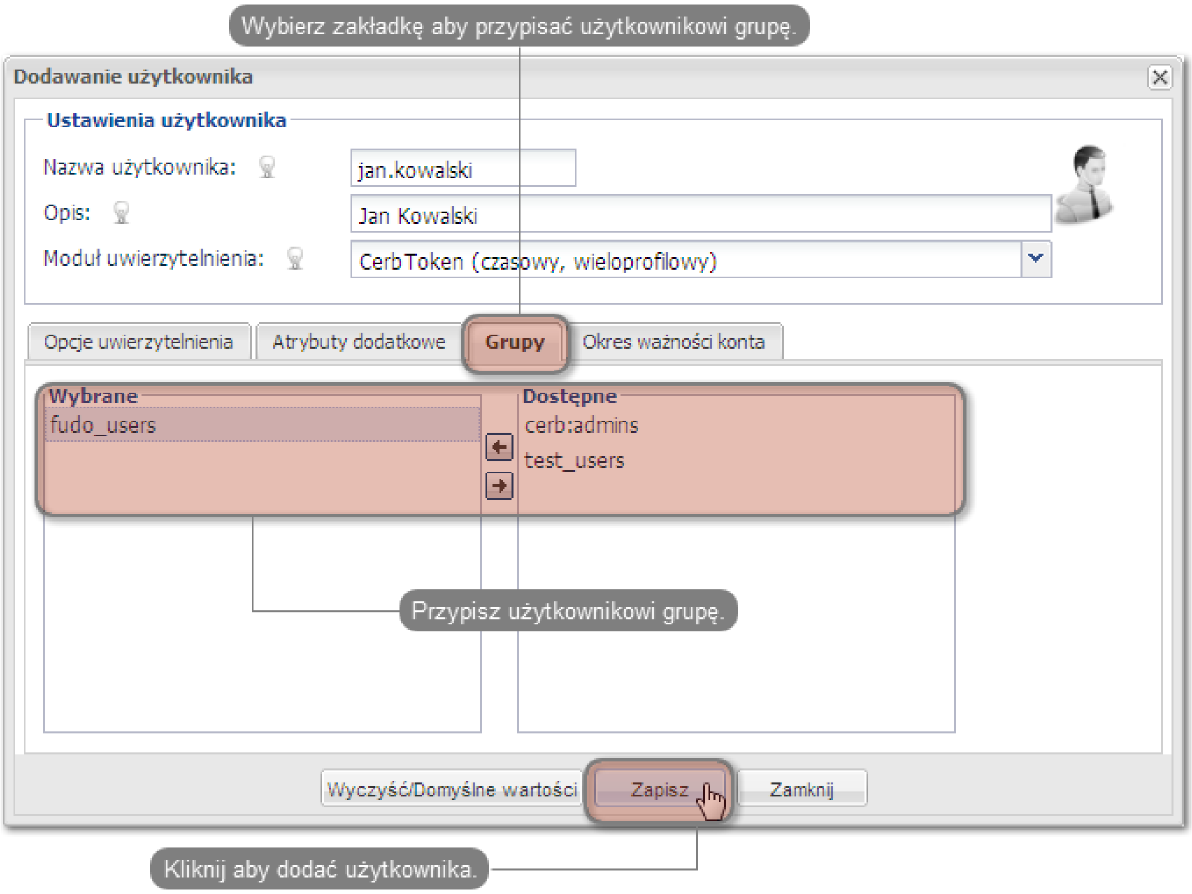
Static password:

Application's identification:

Provide configuration parameters for selected authentication module.

Note: Username is used to authenticate users on Fudo Enterprise.

- 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

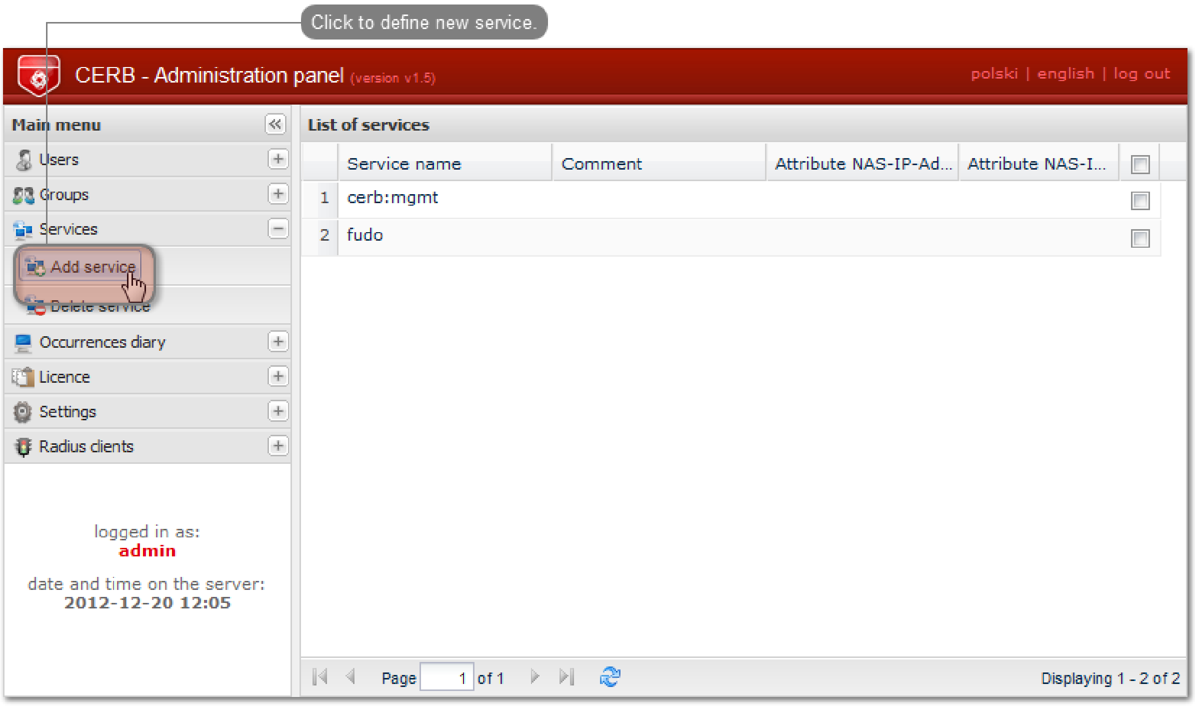
Dostępne: cerb:admins, test_users

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.

List of services

	Service name	Comment	Attribute NAS-IP-Ad...	Attribute NAS-I...
1	cerb:mgmt			
2	fudo			

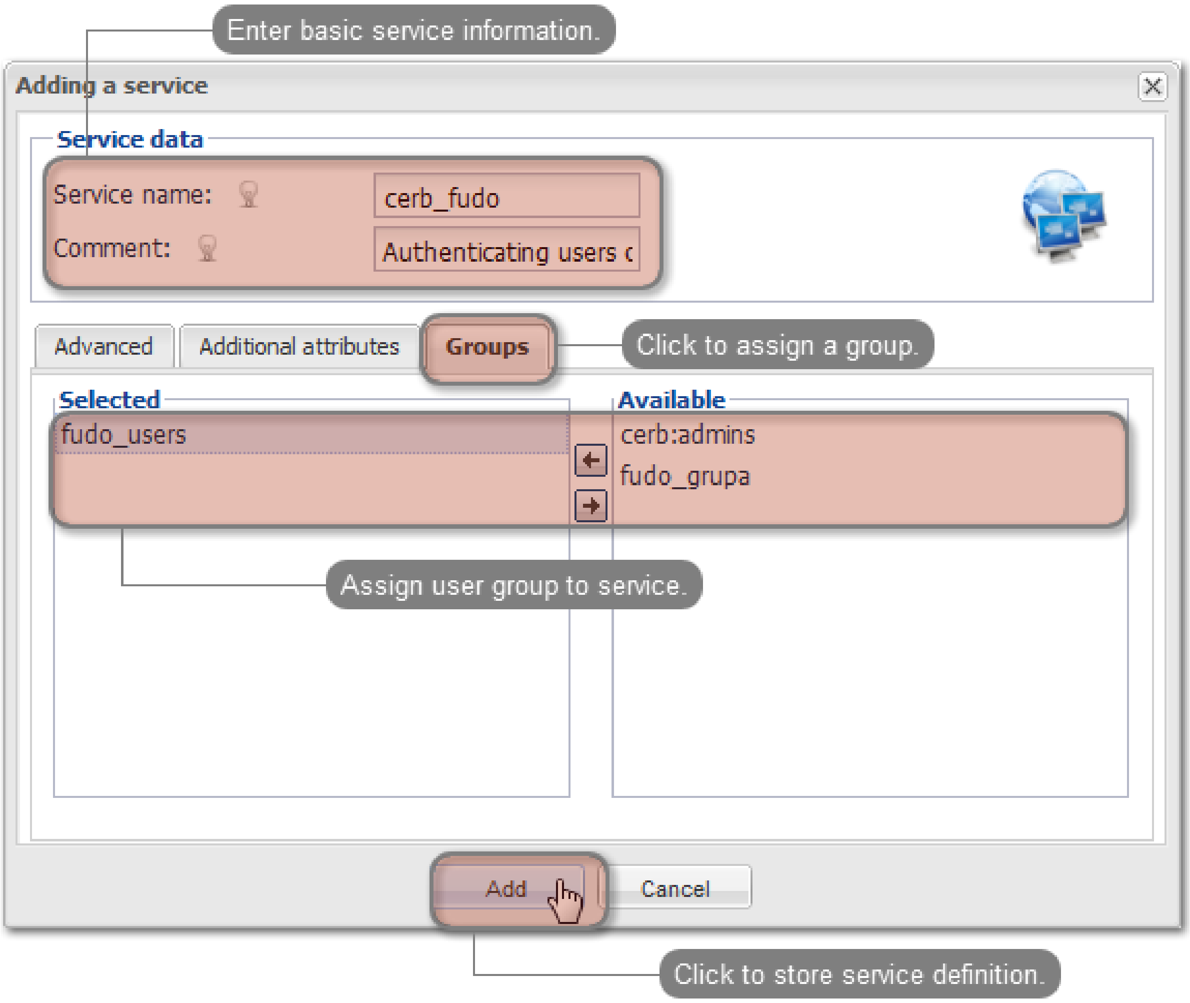
logged in as: admin

date and time on the server: 2012-12-20 12:05

Page 1 of 1 Displaying 1 - 2 of 2

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

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

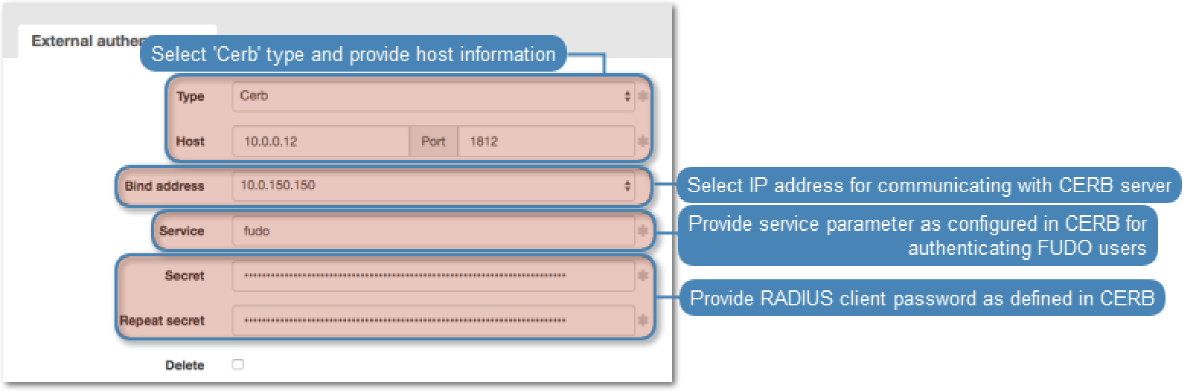


Fudo Enterprise server configuration

1. Adding CERB external authorization server.

- Select *Settings > External authentication*.
- Click *Add external authentication source* to add CERB server definition.
- Provide CERB server IP address, *secret* and service name identifying authorization service.

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



External authen

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: ••

Delete □

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

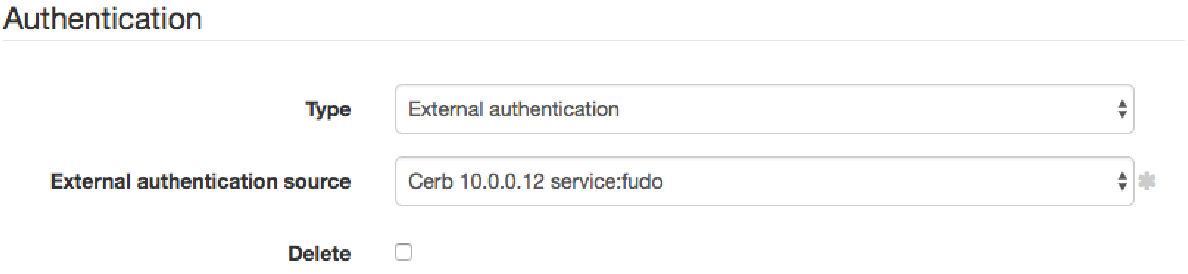
- Click *Save*.

2. Adding user.

- Select *Management* > *Users*.
- Click *Add*.
- Provide basic user information.

Note: Username must match the user name defined on CERB server.

- Add safes that the user will be able to access.
- In the *Authentication* section, select *External authentication* from the *Type* drop-down list and select previously created Cerb server from the *External authentication source* drop-down list.



Authentication

Type: External authentication

External authentication source: Cerb 10.0.0.12 service:fudo

Delete □

- Click *Save*.

Related topics:

- *Users*
- *Authentication*
- *User authentication methods and modes*

22.20 System maintenance

The following section contains descriptions of maintenance procedures.

Fudo Enterprise allows resizing internal system storage by applying the Virtual Hardware storage settings. Once respective VM changes are made, restart your Fudo instance, as described at the *Restart* page so that the current VM settings are taken by Fudo Enterprise.

22.20.1 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

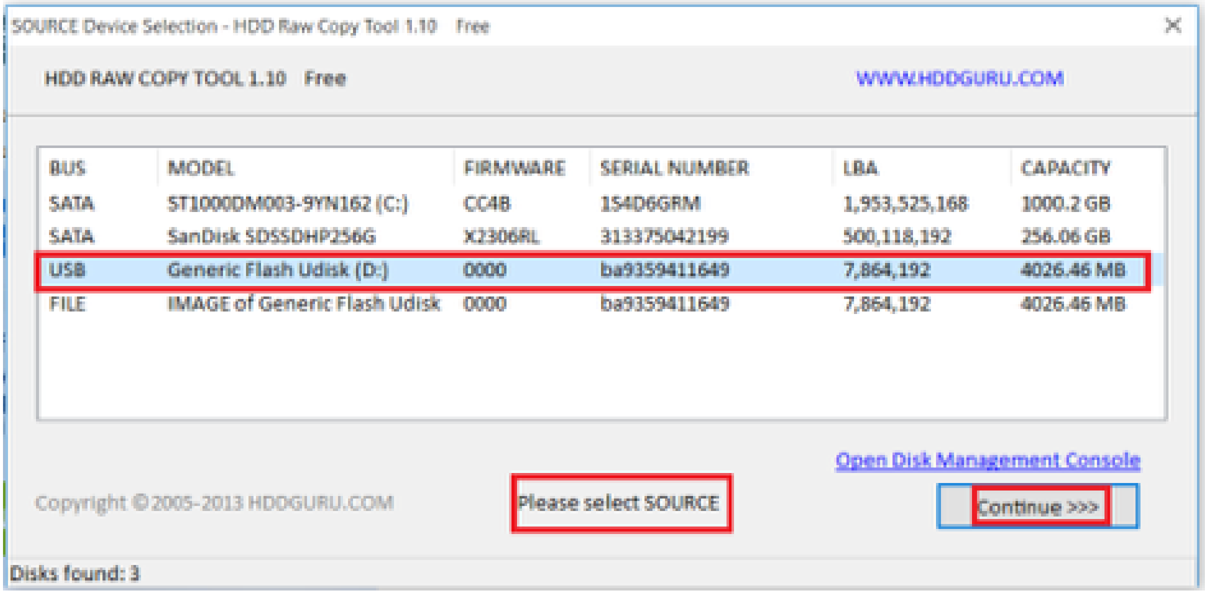
> **Warning:** After connecting the flash drive to your computer, do not initiate or format it. Ignore the system message about it not being able to read data and proceed with the backup procedure.

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

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

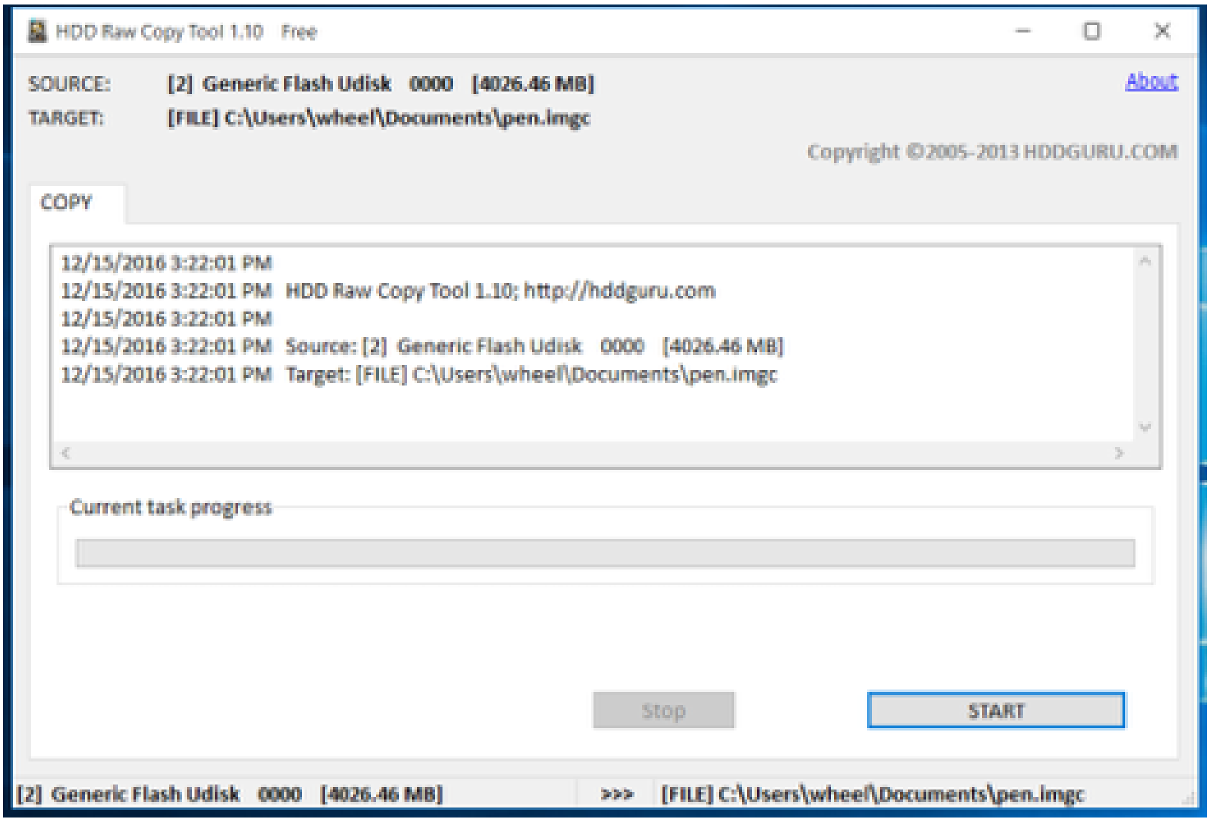
Copyright © 2005-2013 HDDGURU.COM

Please select SOURCE

Disks found: 3

4. Click *FILE* twice, select the target image file and click *Continue*.

5. Click *START* to proceed with copying data.



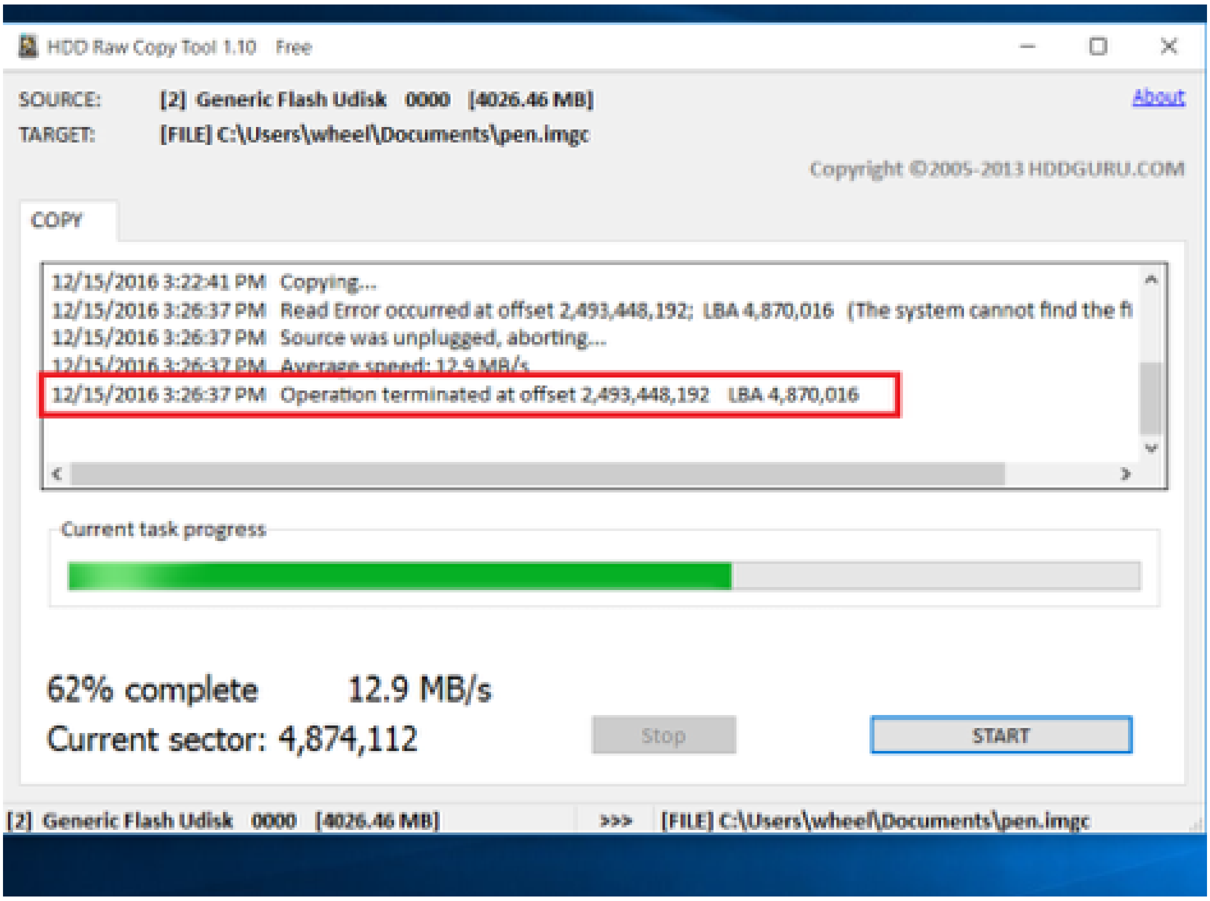
SOURCE: [2] Generic Flash Udisk 0000 [4026.46 MB]
TARGET: [FILE] C:\Users\wheel\Documents\pen.imgc

```
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.



HDD Raw Copy Tool 1.10 Free

SOURCE: [2] Generic Flash Udisk 0000 [4026.46 MB]

TARGET: [FILE] C:\Users\wheel\Documents\pen.imgc

Copyright ©2005-2013 HDDGURU.COM

```
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
```

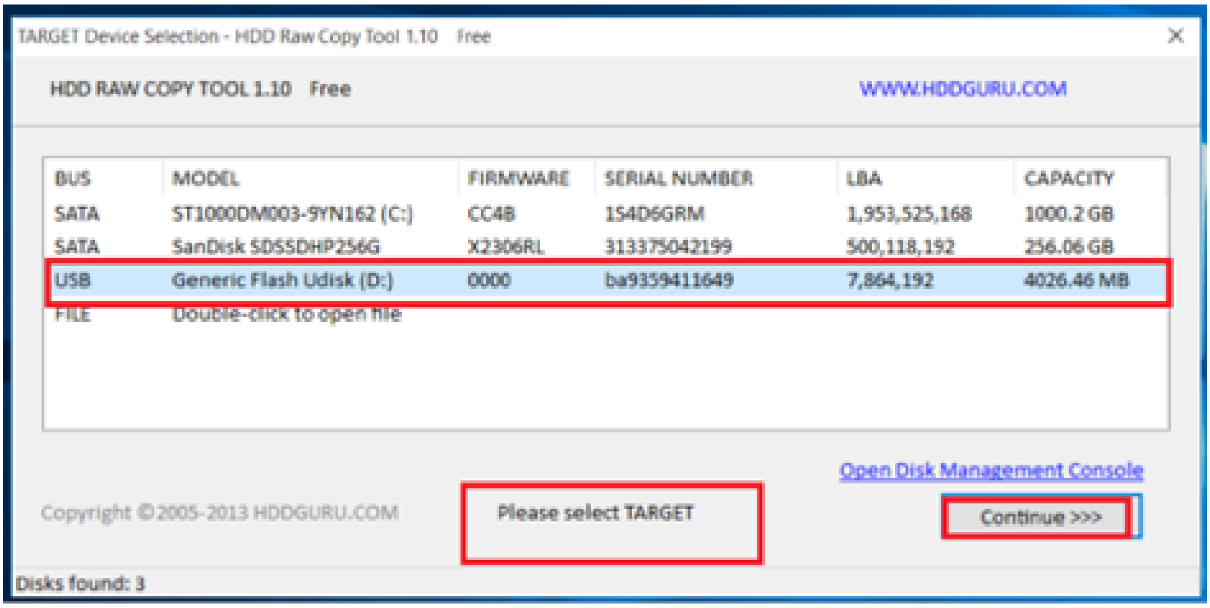
Current task progress

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				

Copyright ©2005-2013 HDDGURU.COM

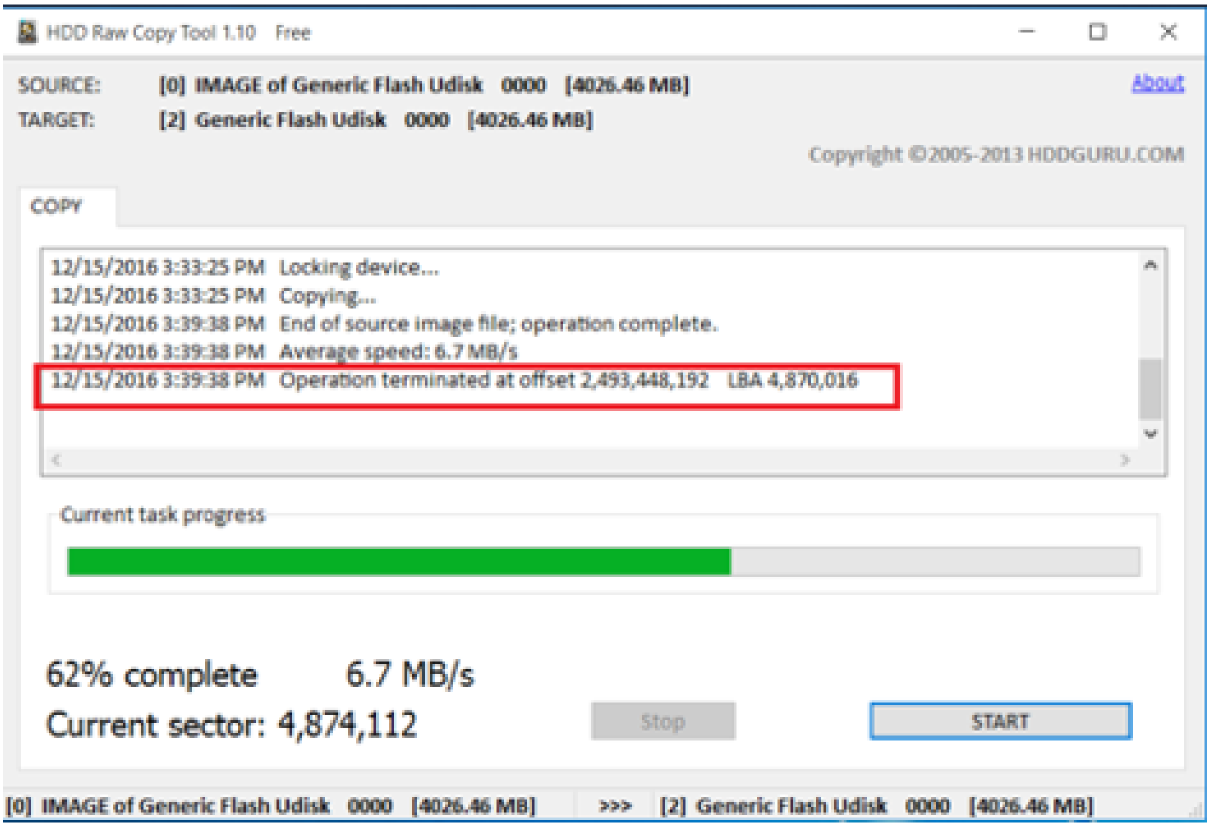
Please select TARGET

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]

Copyright ©2005-2013 HDDGURU.COM

```
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*

22.20.2 Monitoring system condition

Monitoring system condition allows preventing system failures and overloads, ensuring Fudo Enterprise Fudo Enterprise remains operational.

Monitoring active sessions

1. Login to Fudo Enterprise administration panel.
2. Select *Management > Dashboard*.
3. Check the number of currently running user sessions.

Note: Fudo Enterprise supports up to 300 RDP connections.

Monitoring network bandwidth

1. Login to Fudo Enterprise administration panel.
2. Select *Management > Dashboard*.
3. Check current network transfer rate.

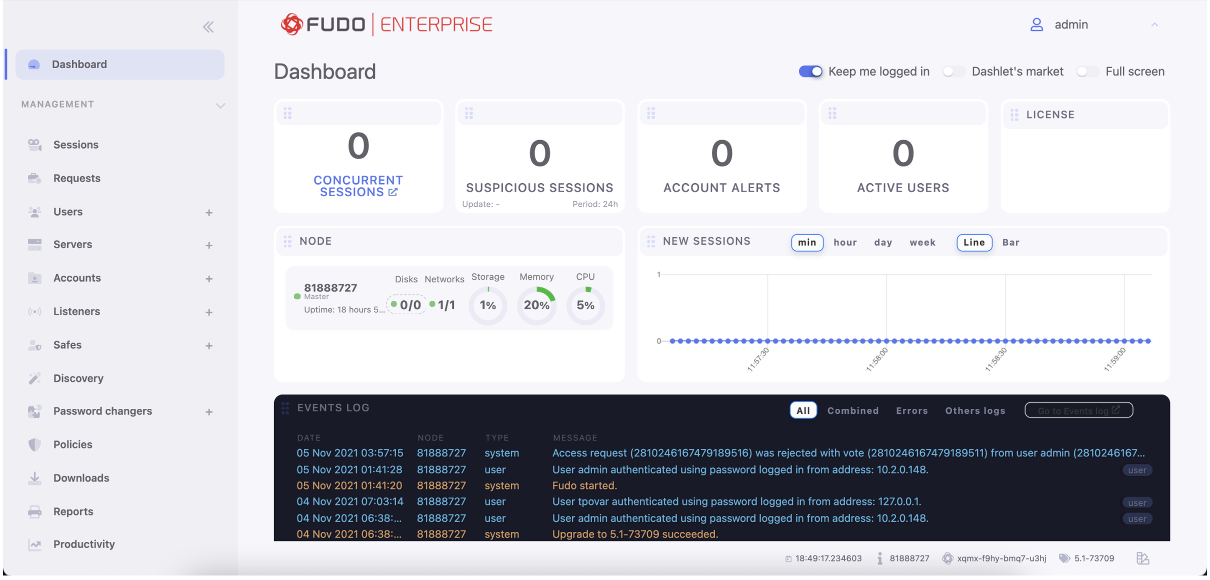
Note: Fudo Enterprise features 1Gbps network interface cards. In case the current network bandwidth usage exceeds 500Mbps, users may notice a decrease in system communication performance.

Monitoring storage

Warning: Fudo Enterprise will not allow new connections when storage usage reaches 90%.

1. Login to Fudo Enterprise administration panel.
2. Select *Management > Dashboard*.

3. Check the storage usage percentage, review and delete archived sessions to free up space if need be.



```
DATE                  NODE      TYPE    MESSAGE
05 Nov 2021 03:57:15  81888727  system  Access request (2810246167479189516) was rejected with vote (2810246167479189511) from user admin (2810246167...
05 Nov 2021 01:41:28  81888727  user    User admin authenticated using password logged in from address: 10.2.0.148.   user
05 Nov 2021 01:41:20  81888727  system  Fudo started.
04 Nov 2021 07:03:14  81888727  user    User tpovar authenticated using password logged in from address: 127.0.0.1.   user
04 Nov 2021 06:38:...  81888727  user    User admin authenticated using password logged in from address: 10.2.0.148.   user
04 Nov 2021 06:38:...  81888727  system  Upgrade to 5.1-73709 succeeded.
```

Related topics:

- *System log*
- *Frequently asked questions*

22.20.3 Health Check

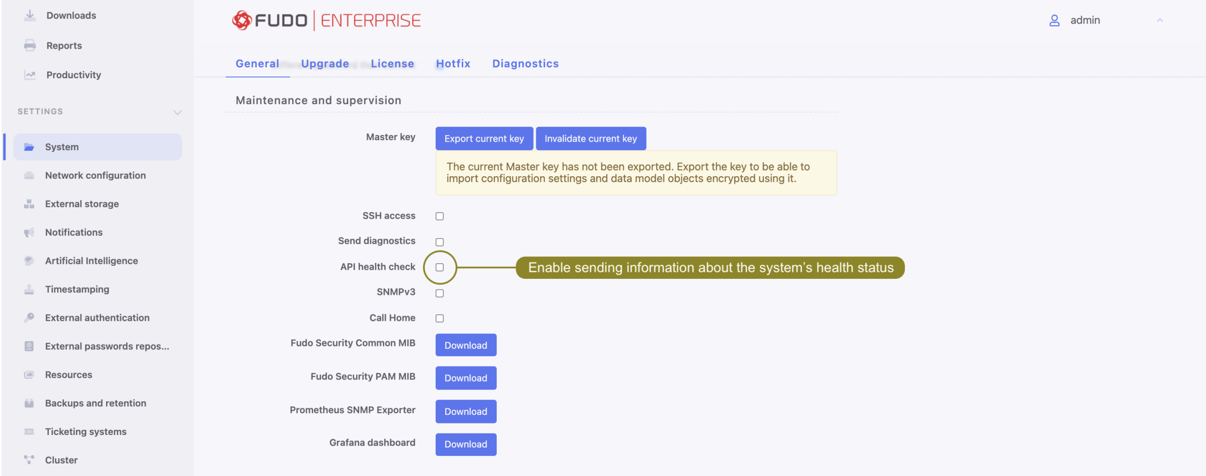
Fudo Enterprise regularly checks its "health" status. There are multiple tests that check the status of both hardware and software components. These tests are called "health checks".

The results of the health checks can be accessed by an administrator in two ways:

1. Using *SNMP*, which provides all *health check* results.
2. Using the *API health check* endpoint, which provides a summary of all *health checks*.

22.20.3.1 API Health Check

The *Health Check API* option is available under the *Maintenance and supervision* section of the Settings > System tab.



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 ☐

Send diagnostics ☐

API health check ☐

Enable sending information about the system's health status

SNMPv3 ☐

Call Home ☐

Fudo Security Common MIB

Fudo Security PAM MIB

Prometheus SNMP Exporter

Grafana dashboard

Enabled the API endpoint providing quick information about Fudo Enterprise's health status. It may be used by external devices to periodically check Fudo Enterprise's health status.

The information is available as a JSON object:

```
{
"status": "${value}"
}
```

The `${value}` may be set to:

- `ok`: if Fudo Enterprise works properly
- `error`: if Fudo Enterprise doesn't work properly and some of it functions may not be available.

Note: The health check status is designed to be simple and easy to interpret, therefore it doesn't contain detailed information about the problems that caused the error status. The detailed information about health check results can be obtained using *SNMP*.

After enabling, the endpoint will be available at a URL path:

```
api/healthcheck
```

Warning: The API endpoint is accessible without authentication. It means that anyone having TCP access to Fudo Enterprise will be able to get information about its health status.

22.20.4 Call Home

Call Home service is a valuable tool designed to collect statistics on feature usage, offering insights into how often specific functions are utilized and identifying areas for improvement. This service also helps to enhance customer support by allowing certain tasks to be performed remotely and automatically. It simplifies the process of product maintenance and diagnostics, enabling the Fudo Support Team to gather essential data without direct user intervention.

Note: *Call Home* is intended solely for collecting diagnostic data and monitoring system status. For remote support, a separate function—*SSH access*—must be enabled through the system settings to ensure secure and direct assistance when needed.

22.20.4.1 Data Collected by Call Home Service

The *Call Home* service automatically collects essential diagnostic data to ensure the Fudo Enterprise system remains optimized and secure. The following metrics are monitored:

- **Disk Status:** Keeps track of disk health to prevent failures.
- **Storage Utilization:** Monitors how storage resources are being used.
- **Sensor Temperatures:** Checks the temperature of various system sensors to avoid overheating.
- **Session Data Replication Status:** Monitors the replication status to ensure data integrity.
- **Critical Errors:** Logs any critical errors that could impact system performance.
- **System Crashes:** Records crashes to help identify and resolve issues quickly.
- **Version Deployment:** Gathers data on Fudo Enterprise version usage, including hours in operation and reported issues.

The *Call Home* service is designed with strict security measures in mind:

- Fudo Security **cannot make any changes** to the Fudo Enterprise system.
- Fudo Security **does not collect any data related to the client's configuration.**
- Fudo Security **does not collect or process any personal data** stored in Fudo Enterprise.

22.20.4.2 The Benefits of Using Call Home

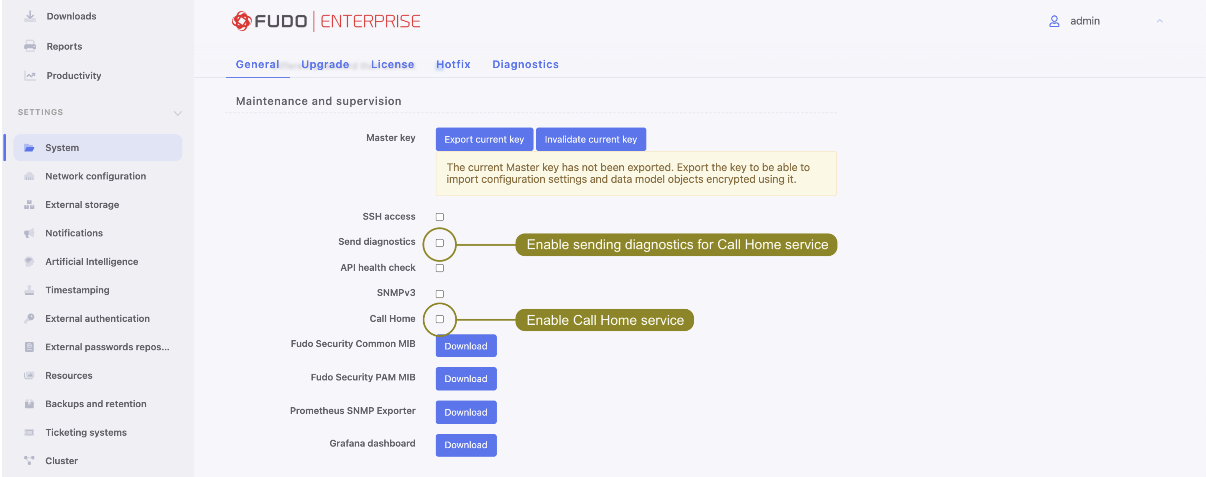
- **Insight into Feature Usage:** Fudo Security gains visibility into which features are actively utilized by clients, enabling the prioritization and enhancement of the most valuable functionalities based on actual user preferences.
- **Priority Client Engagement:** Proactive users play a pivotal role in the development process. Their usage data directly informs future enhancements of Fudo Security products.
- **Version Tracking:** Provides immediate insight into which clients have upgraded and their current version, ensuring all users are operating on the most secure and efficient release.

- **Faster Issue Resolution:** Enables swifter problem resolution by reducing the need for extensive communication. Immediate access to diagnostics allows for quicker interventions.
- **Remote Management:** License updates, upgrades, and hotfixes can be deployed remotely, minimizing the need for client involvement.
- **Rapid Security Response:** In the event of a vulnerability, Fudo Security can implement hotfixes immediately, reducing exposure to threats and bypassing time-consuming communications.

22.20.4.3 Enable/Disable Call Home

In order to configure the Call Home service, proceed as follows:

1. Go to *Settings* > *System*, and then to the *Maintenance and supervision* section.
2. Check the *Call Home* option.
3. Choose the IP address of your Fudo Enterprise instance or `Any` address.
4. Additionally, check the *Send diagnostics* option to share diagnostic results with Fudo Support Team.



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 □

Send diagnostics □

API health check □

SNMPv3 □

Call Home □

Fudo Security Common MIB

Fudo Security PAM MIB

Prometheus SNMP Exporter

Grafana dashboard

Enable sending diagnostics for Call Home service

Enable Call Home service

Note: Starting from version 5.4.5, enabling the *Call Home* feature now automatically activates the sending of diagnostics, and the **Send diagnostics** checkbox has been removed.

Note:

- The Call Home functionality requires an account created on Fudo Security servers. To create an account, contact your partner and provide your machine Fudo Unique Identifier (FUID). Check at the *Footer Information* page where you can see your FUID.
- The Fudo appliance initiate an outbound SSH connection to `home.fudosecurity.com` (IP:`178.33.6.1`, Port: `22`).

Related topics:

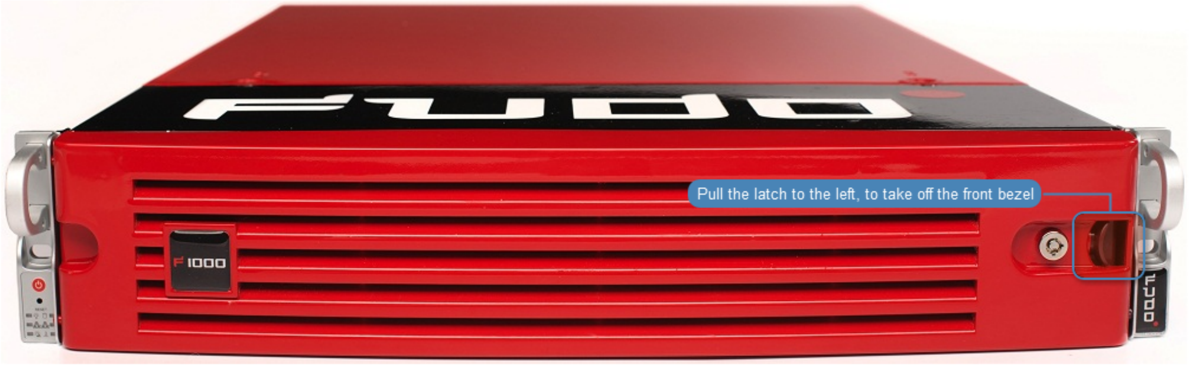
- *SSH access*

22.20.5 Hard drive replacement

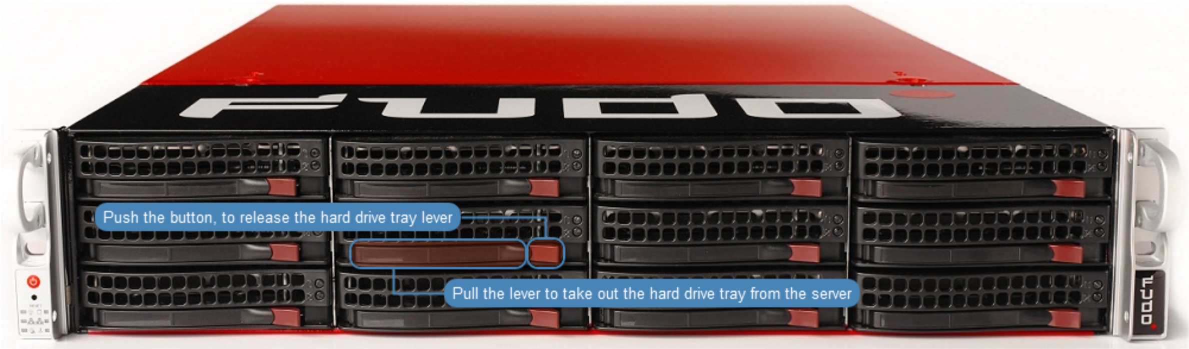
In default configuration, Fudo Enterprise's storage array comprises 12 hard drives in RAIDZ2 configuration running ZFS file system allowing the system to remain fully operational in case of a failure of two hard drives.

Replacing a hard drive

1. Move the front bezel release latch to the left and take the front bezel off.



2. Push the hard drive tray lever release button and pull the lever to take out the tray from the chassis.


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 Enterprise will automatically detect the change in the storage array state and will start rebuilding the data structure. The duration of the array rebuilding process depends on the volume of data stored on the server.

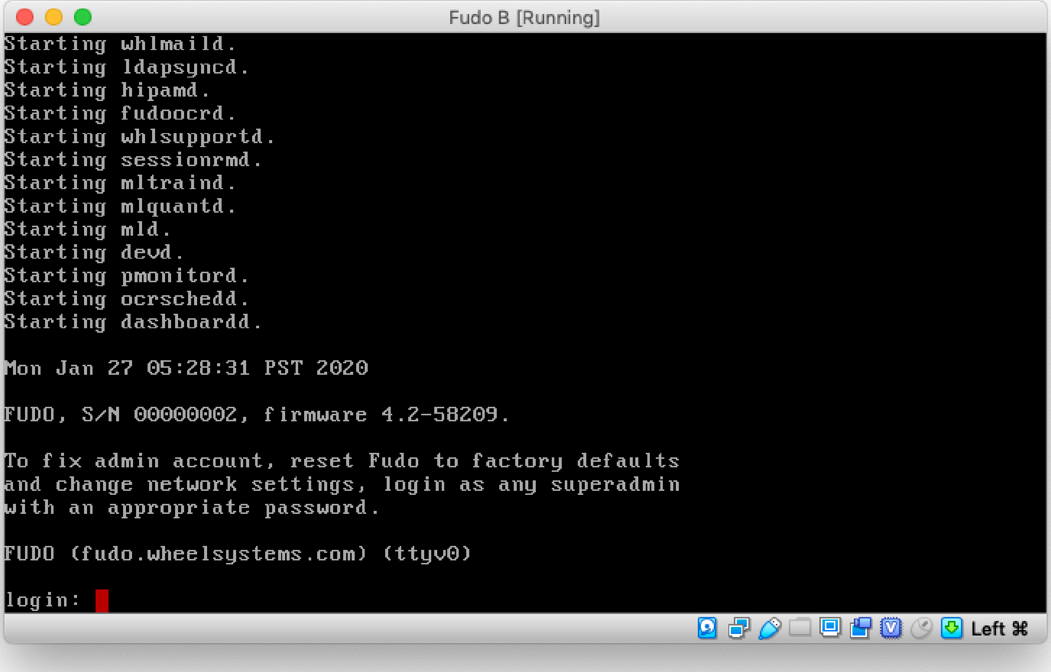
Related topics:

- *Hardware overview*
- *Frequently asked questions*

22.20.6 Resetting configuration to default settings

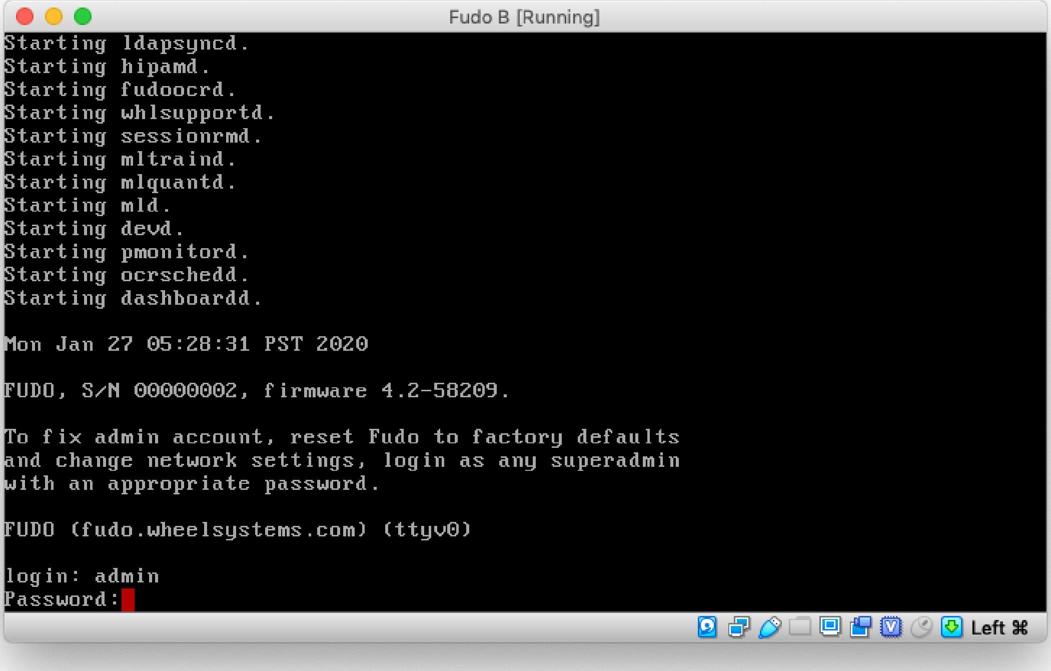
> **Warning:** Configuration reset procedure is irreversible and it results in deleting all recorded sessions, system settings and defined objects. The device needs 2 pendrives plugged in to be properly executed.

1. Access system terminal.
2. Enter administrator account login and press *Enter*.



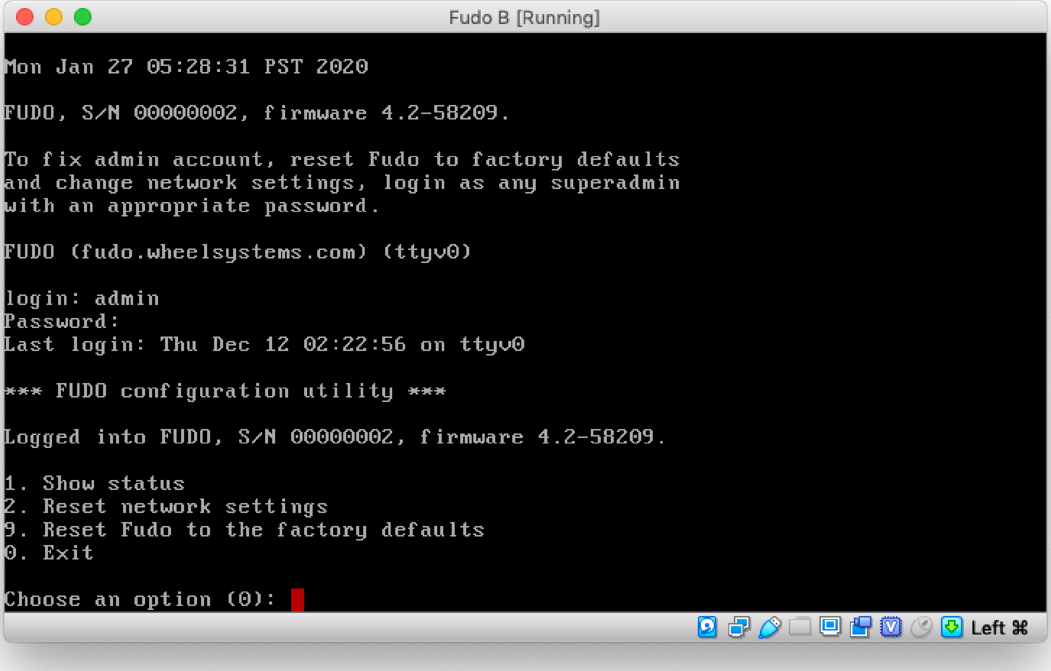
```
Starting whlmaild.
Starting ldapsyncd.
Starting hipamd.
Starting fudoocrd.
Starting whlsupportd.
Starting sessionrmd.
Starting mltraind.
Starting mlquantd.
Starting mld.
Starting devd.
Starting pmonitord.
Starting ocrschedd.
Starting dashboardd.

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*.



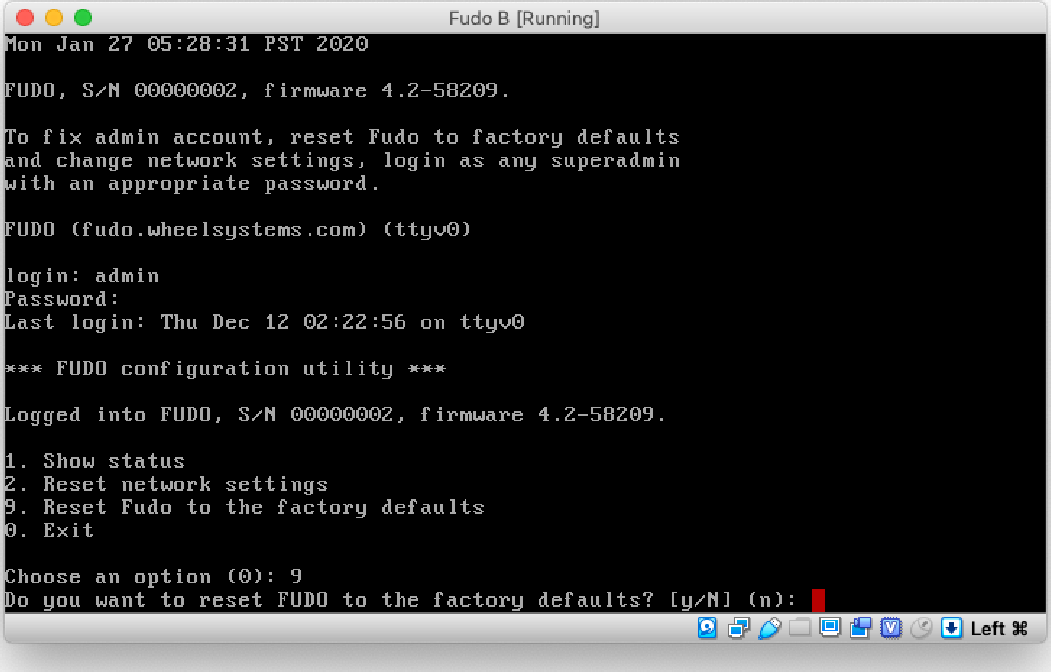
```
Starting ldapsyncd.
Starting hipamd.
Starting fudoocrd.
Starting whlsupportd.
Starting sessionrmd.
Starting mltraind.
Starting mlquantd.
Starting mld.
Starting devd.
Starting pmonitord.
Starting ocrschedd.
Starting dashboardd.

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*.



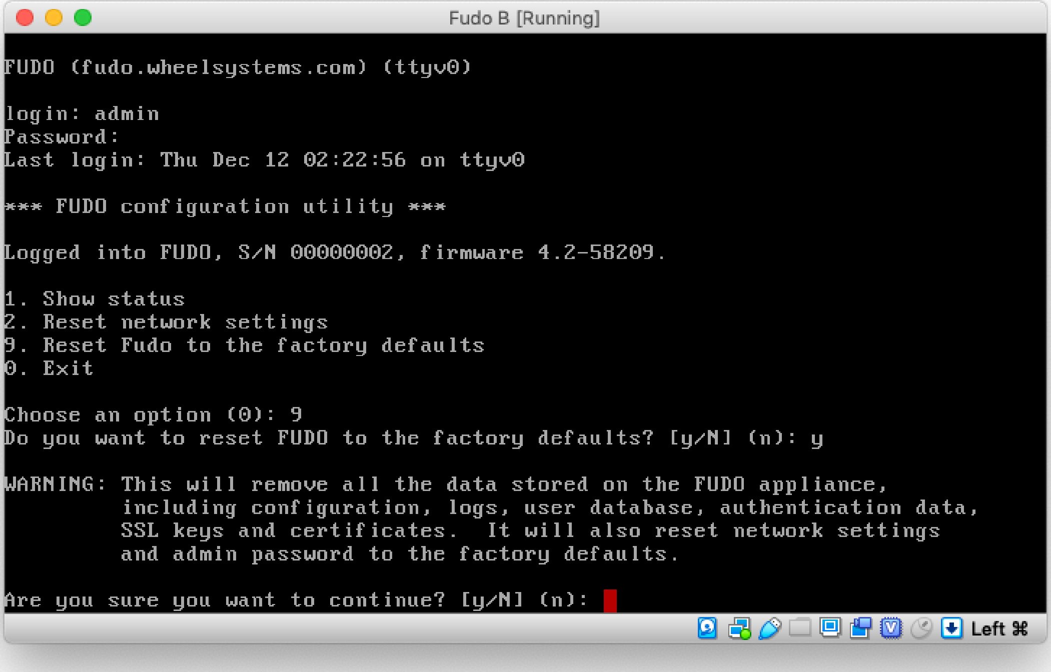
```
Mon Jan 27 05:28:31 PST 2020

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*

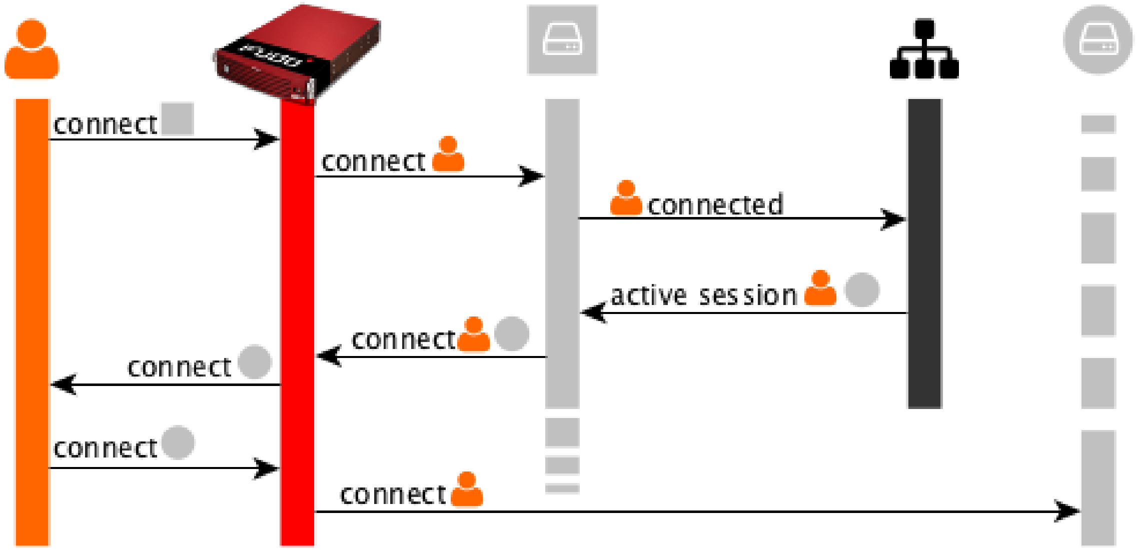
CHAPTER 23

Reference information

23.1 RDP connections broker

Connections broker enables users to reconnect to their existing sessions on a specific server within a pool of load-balanced resources.

If the broker identifies an existing user session on another server, the connection will be redirected to it and the user will be prompted to login again.



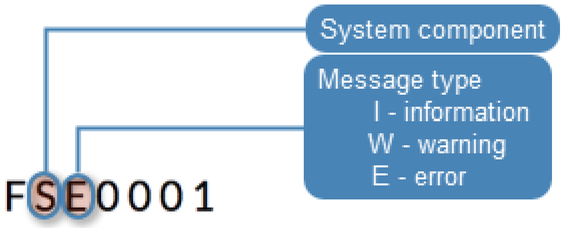
Note: To successfuly redirect a connection, the server identified by the broker must be defined on Fudo Enterprise, it must listen on default RDP port (3389) and user must be allowed to connect to given server.

Related topics:

- *Data model*
- *RDP*
- *Servers*
- *Accounts*

23.2 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

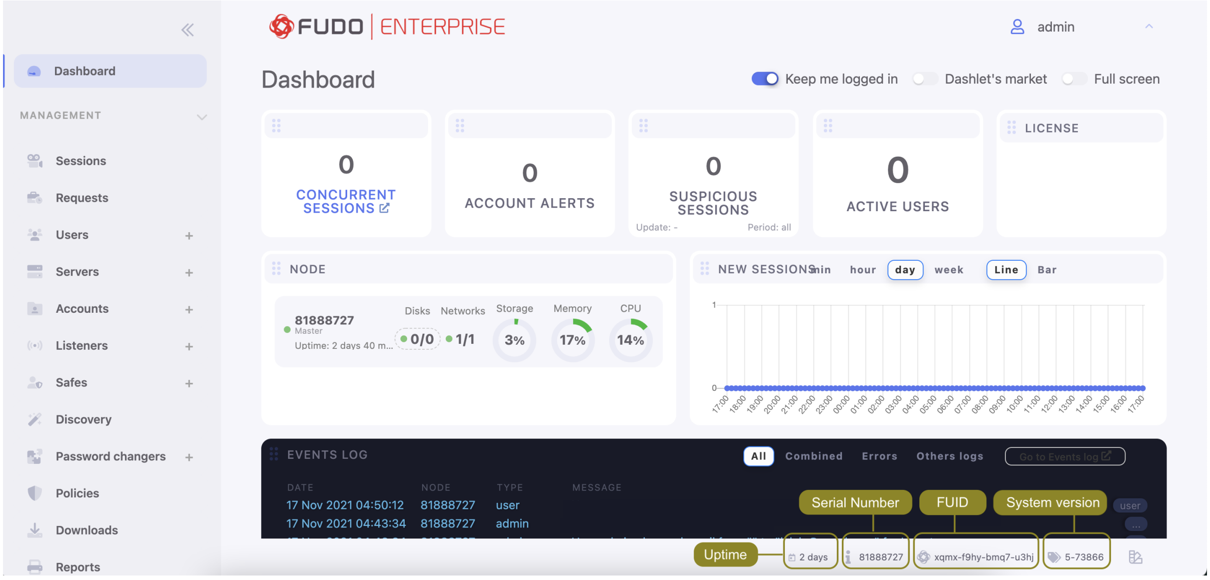
Table 1 – continued from previous page

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.
FSI0578	User %s (%s) was removed. Reason: user's external server dosen't exists any more.
FSE0580	Cluster %s has an invalid token: %s.
FAI0581	User %s changed domain search path from %s to %s.
FSW0582	Disk $cdev was removed.

23.3 Footer Information

The footer on the left menu displays 4 elements describing current Fudo Enterprise instance:

1. **Uptime** - when the system was activated last time.
2. **Serial Number** - ID of the cluster node. It's unique for a single cluster.
3. **FUID (Fudo Unique Identifier)** - Unique ID of the current Fudo Enterprise instance.
4. **System Version** - Current software version.



```
DATE                  NODE      TYPE   MESSAGE
17 Nov 2021 04:50:12  81888727  user
17 Nov 2021 04:43:34  81888727  admin
```

CHAPTER 24

Fudo Officer 1.0

Fudo Officer 1.0 is a mobile app that allows Fudo Enterprise administrators to manage the users' requests to the target servers. The requests are accepted or rejected by the administrators via the Fudo Officer app, or on Admin Panel in the *Management > Sessions* tab.

Note: Refer to the *Approving pending user requests* and *Declining pending requests* topics for more information about maintaining the users' requests on the Admin Panel.

English, Polish, Russian, and Ukrainian languages are available as an application language. Application language is set according to the phone settings.

Warning: Fudo Officer app requires enabling the *Call Home* service at the *Maintenance and supervision* section of the *Settings > System* tab.

Additionally, there must be selected the *Require approval* option within the Safe and enabled an option for push notifications *Session awaiting approval (push)* for the user. An associated device can be configured for the currently logged user only.

24.1 Configuration

Warning: An associated device can be configured for the currently logged user only.

In order to configure the Fudo Officer app, follow the instruction:

1. Allow the application sending notifications.
2. Set a PIN (a 4-6 digits number). This PIN is independent from the PIN you use to unblock your phone.

3. Create your first profile.

3.1. Open Fudo Enterprise Admin panel. Go to *Management > Users*. Choose a user to create a profile for.

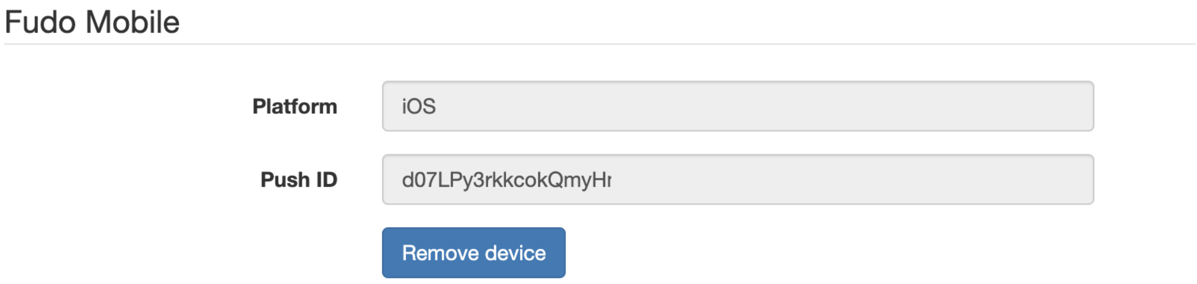
3.2. Scroll down to the *Fudo Mobile* section and click the *Add device* button. The showed QR code has to be scanned with the app.

3.3. Go back to the app and click the *Add your profile* button. Next, click the *Scan QR code* button.

3.4. Scan showed QR code with your phone.

3.5. Set a profile name and click the *Create profile* button. The profile name is editable.

3.6. Go back to the Fudo Enterprise Admin panel and click *OK* in the QR code window. The *Fudo Mobile* section now has the *Platform* field filled with the binding device name and the *Push ID* with the respective string.



Fudo Mobile

Platform: iOS

Push ID: d07LPy3rkkcokQmyHr

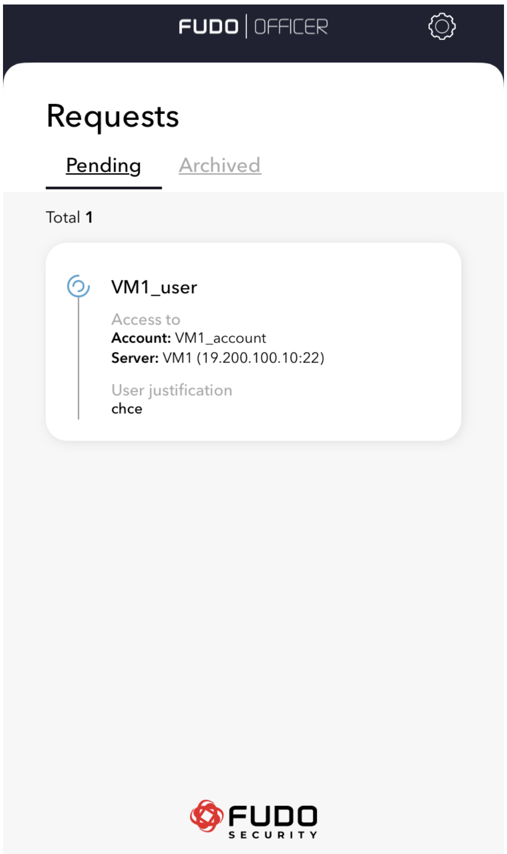
3.7. Click the *Save* button.

Now, you can manage the users' requests via the created profile.

Note: A profile is unique for one user within one Fudo Enterprise instance.

24.2 Managing session requests

The requests which are waiting for the response, are located under the `Pending` tab. Click on a request item to accept or reject the request.



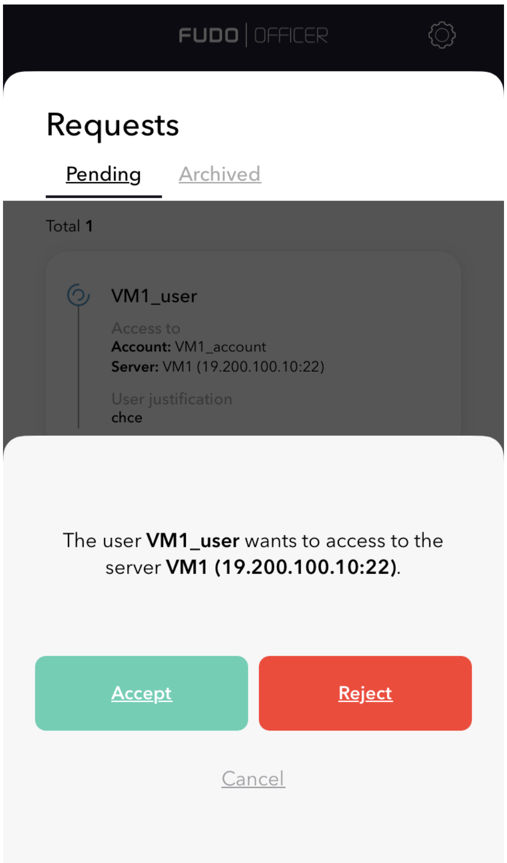
Requests

Total 1

VM1_user

Access to
Account: VM1_account
Server: VM1 (19.200.100.10:22)

User justification
chce



Requests

Total 1

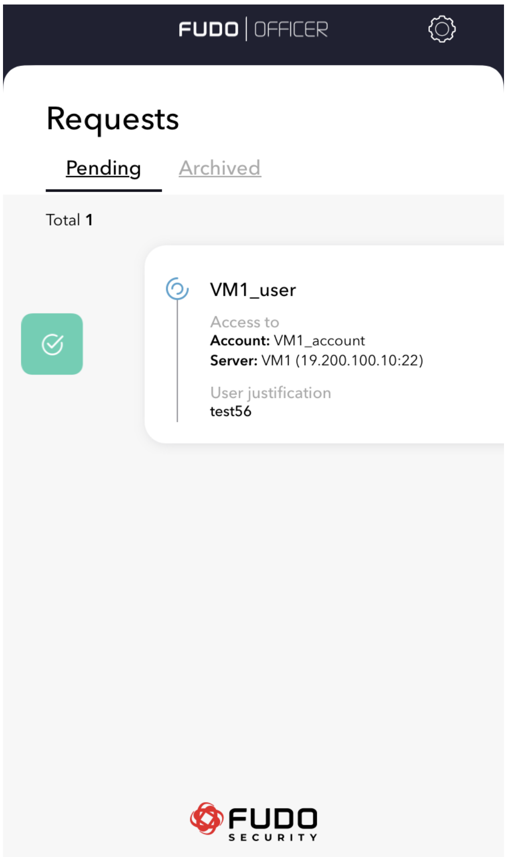
VM1_user

Access to
Account: VM1_account
Server: VM1 (19.200.100.10:22)

User justification
chce

The user **VM1_user** wants to access to the server **VM1 (19.200.100.10:22)**.

Alternatively, swipe `right` on a request item to accept the request or swipe `left` to reject the request.



FUDO | OFFICER

Requests

Pending Archived

Total 1

VM1_user

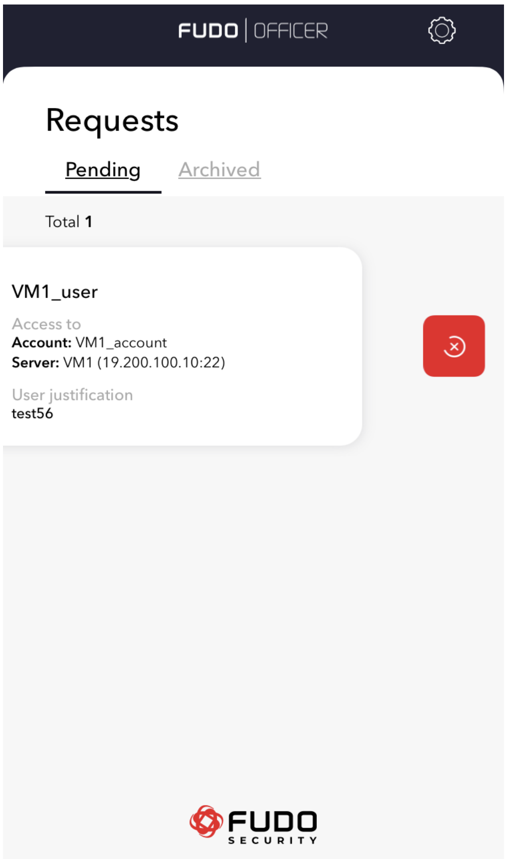
Access to

Account: VM1_account

Server: VM1 (19.200.100.10:22)

User justification

test56



FUDO | OFFICER

Requests

Pending Archived

Total 1

VM1_user

Access to

Account: VM1_account

Server: VM1 (19.200.100.10:22)

User justification

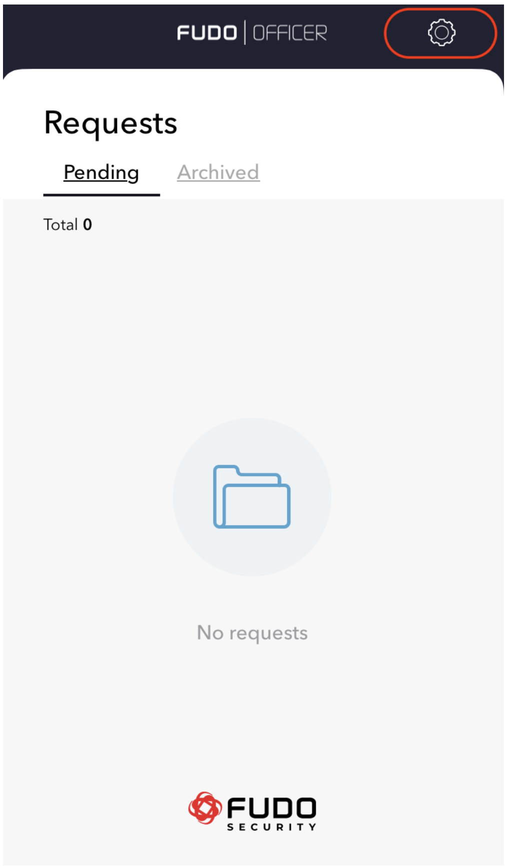
test56

The processed requests (accepted and rejected) can be found under the `Archived` tab. These requests can be sorted by `Date`, `Server name` or `User`.

24.3 Settings

Edit profile

1. Choose a cog icon in the upper right corner.



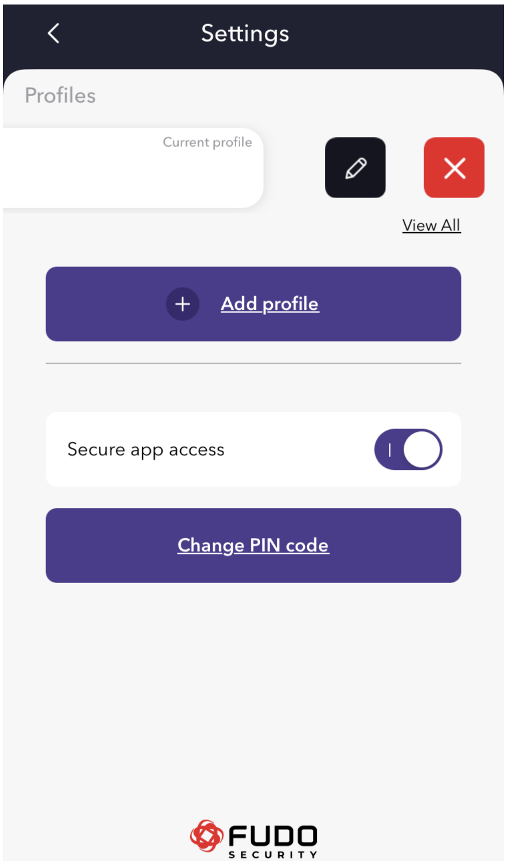
FUDO | OFFICER

Requests

Total 0

No requests

2. Swipe `left` on the profile item.



3. Click on the pencil icon to edit the profile name, or Click the red button if you want to delete the profile.

Add profile

1. Open Fudo Enterprise Admin panel. Go to Management > Users. Choose a user to create a profile for.

2. Scroll down to the *Fudo Mobile* section and click the *Add device* button. The showed QR code has to be scanned with the app.

3. Go back to the app and click the *Add your profile* button. Next, click the *Scan QR code* button.

4. Scan showed QR code with your phone. Set a profile name and click the *Create profile* button. The profile name is editable.

5. Go back to the Fudo Enterprise Admin panel and click *OK* in the QR code window. The *Fudo Mobile* section now has the *Platform* field filled with the binding device name and the *Push ID* with the respective string.

6. Click the *Save* button.

Change PIN code

1. Choose a cog icon in the upper right corner.

2. Click *Change PIN code*.

3. Enter your current PIN code. You will have 5 attempts.

4. Create a new 4-6 digits PIN code.

5. Confirm the entered PIN code.

The *Secure app success* toggle is enabled by default - it's allowing an authentication method for logging in to the application.

CHAPTER 25

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 Enterprise Secret Manager module to retrieve passwords.

The AAPM module supports Microsoft Windows, Linux and BSD family operating systems.

25.1 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.

25.1.1 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.

25.1.2 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.

25.1.3 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.

25.1.4 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*

25.2 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*

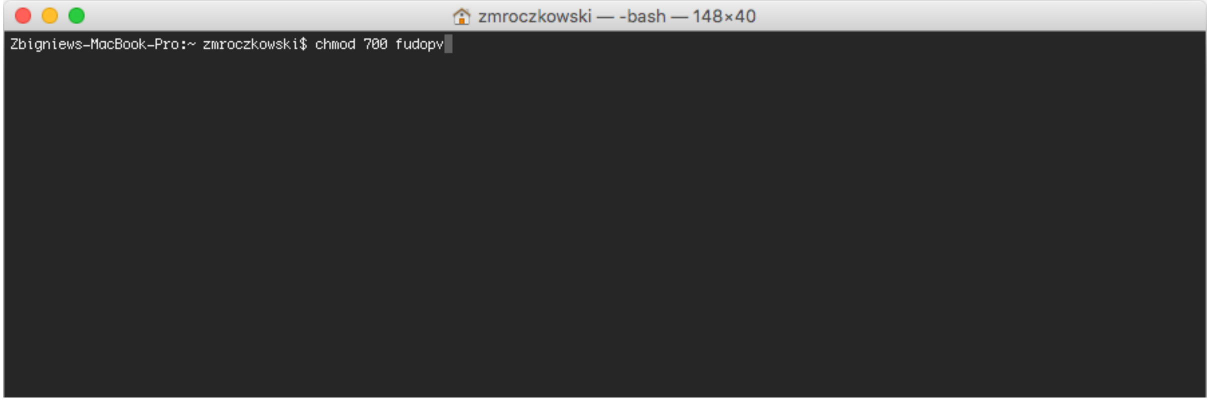
25.3 Using *fudopv*

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
```

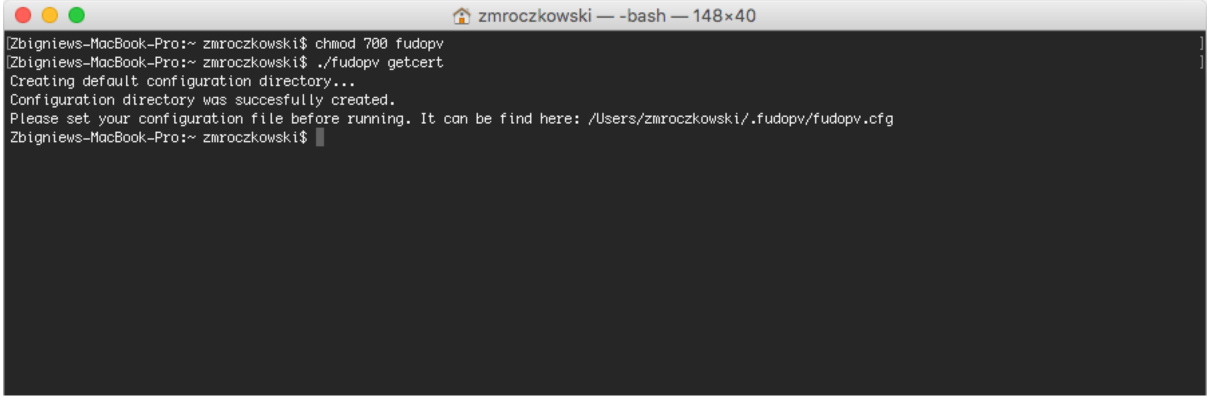
2. Log in to the Fudo Enterprise administration panel.
3. Create a user object with `user` role, static or one-time password authentication and server's IP address defined in the *API* section.

Note:

- Select *Management > Users*.
- Click *+Add*.
- Enter user's name.
- Define account's validity period.
- Select `user` from the *Role* drop-down list.

- Assign safe and click the object to open its properties.
- Select the *Reveal password* option.
- In the *Authentication* section, select `Password` or `One time password` from the *Type* drop-down list.
- In case of static password authentication, type in the password in *Password* and *Repeat password* fields.
- In the *API* section, click the + icon and enter the IP address of the server, which will be requesting passwords using `fudopv` script.
- Click *Save*.

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

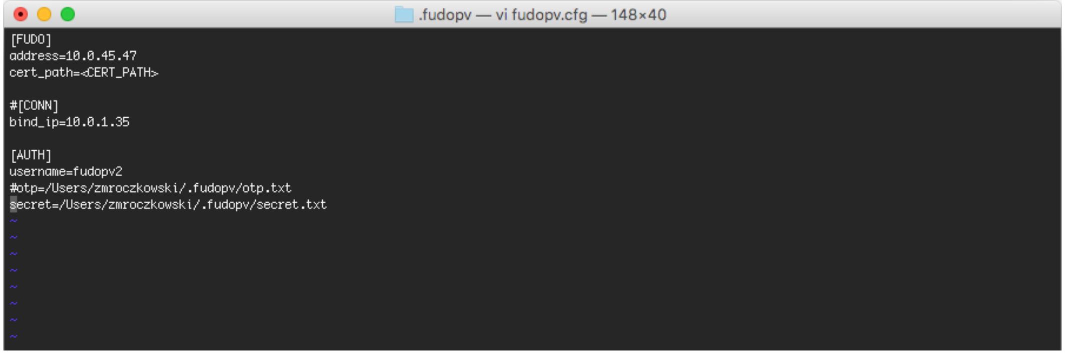


```
[Zbigniews-MacBook-Pro:~ zmroczkowski$ chmod 700 fudopv
[Zbigniews-MacBook-Pro:~ zmroczkowski$ ./fudopv getcert
 Creating default configuration directory...
 Configuration directory was succesfully created.
 Please set your configuration file before running. It can be find here: /Users/zmroczkowski/.fudopv/fudopv.cfg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

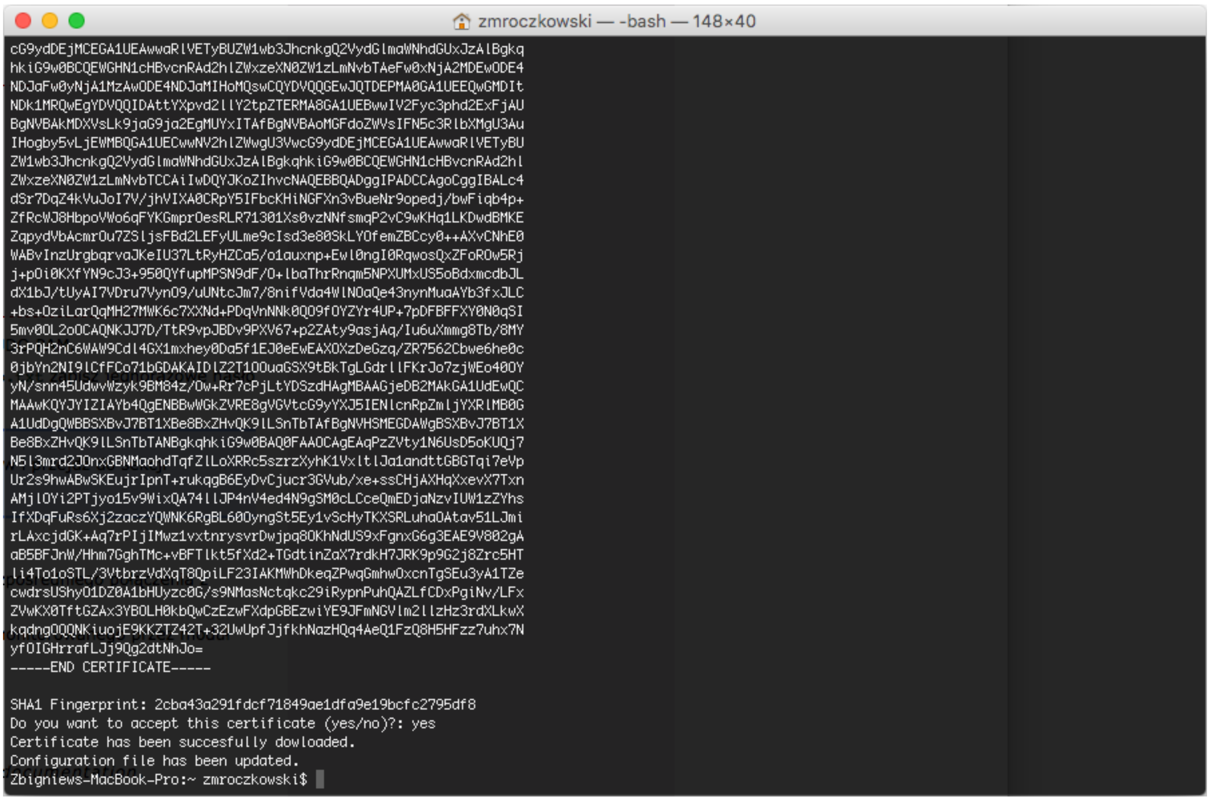
Note:

- 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 Enterprise 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:

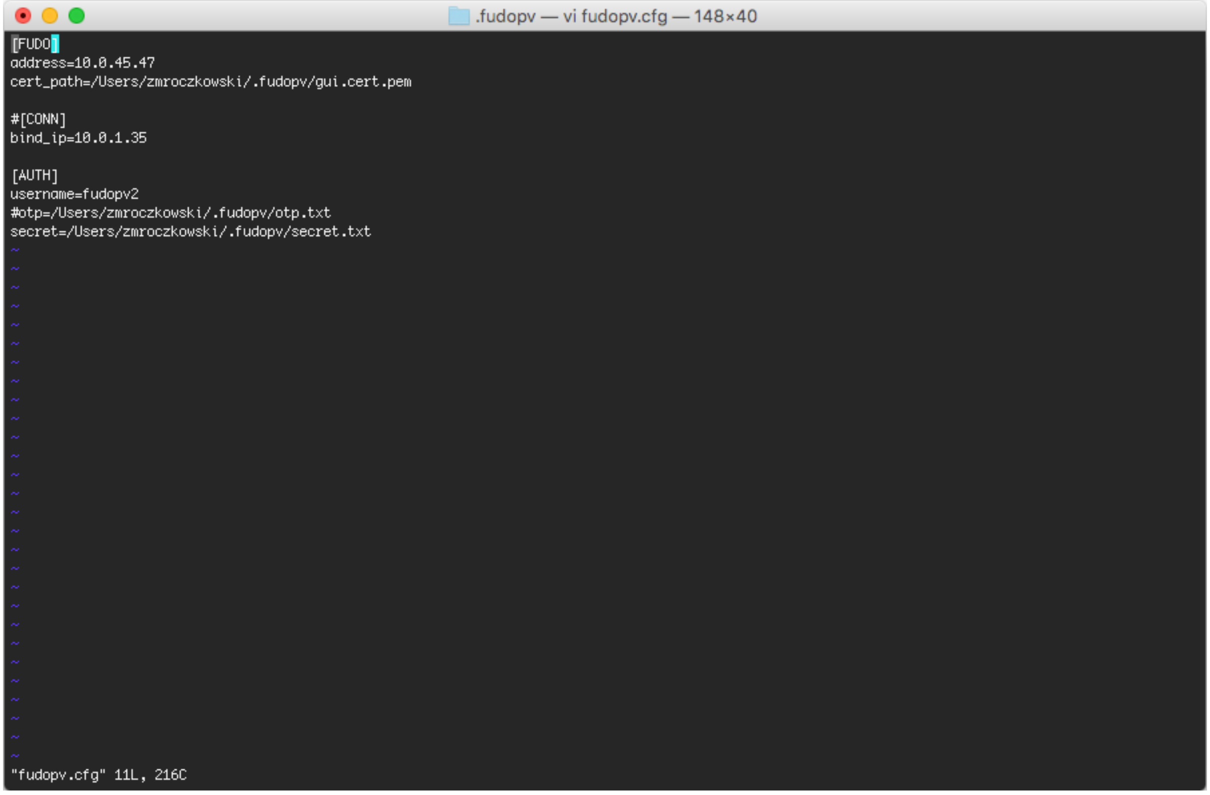
```
[FUDO]
address=10.0.0.8.61
cert_path=<CERT_PATH>

#[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.

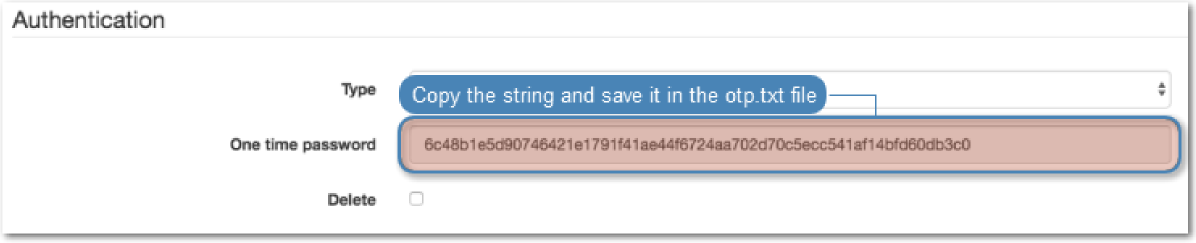


```
[FUDO]
address=10.0.45.47
cert_path=/Users/zmroczkowski/.fudopv/gui.cert.pem

#[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

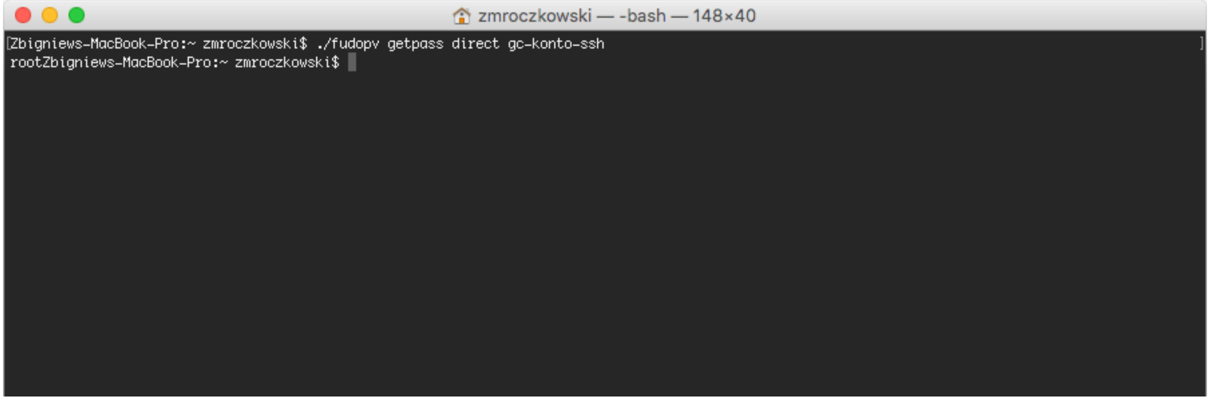
One time password: 6c48b1e5d90746421e1791f41ae44f6724aa702d70c5ecc541af14bfd60db3c0

Delete ☐

- The `otp.txt` file will be automatically updated each time the `fudopv getpass` command is run.

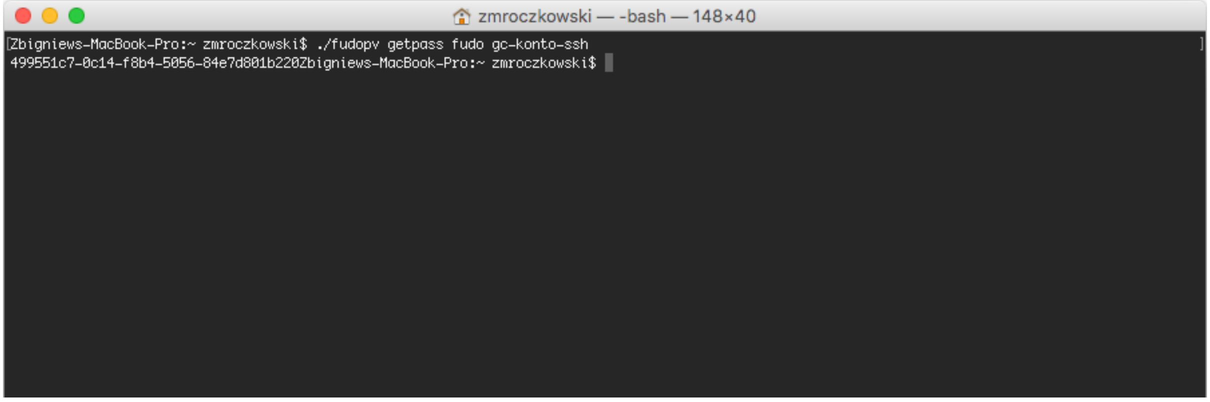
8. Run command:

- `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.

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*

25.4 API interface

AAPM's API interface is described in detail in the *Fudo Enterprise - 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*

25.5 Authentication methods

Conventions and symbols:

- **url**: `fudo` connection address,
- **->**: `fudopv` request,
- **<-**: response from Fudo Enterprise,
- **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.

25.5.1 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.*

25.5.2 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 26

Ticketing systems

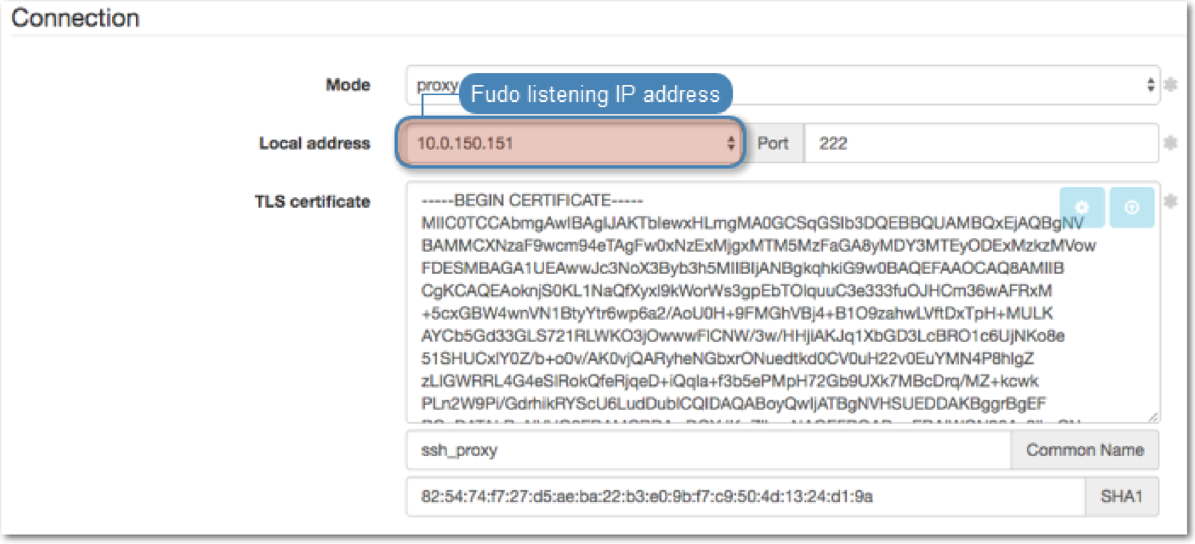
The *Ticketing system* tab is responsible for the **Service Now** functionality, which is deprecated now.

CHAPTER 27

Client applications

27.1 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

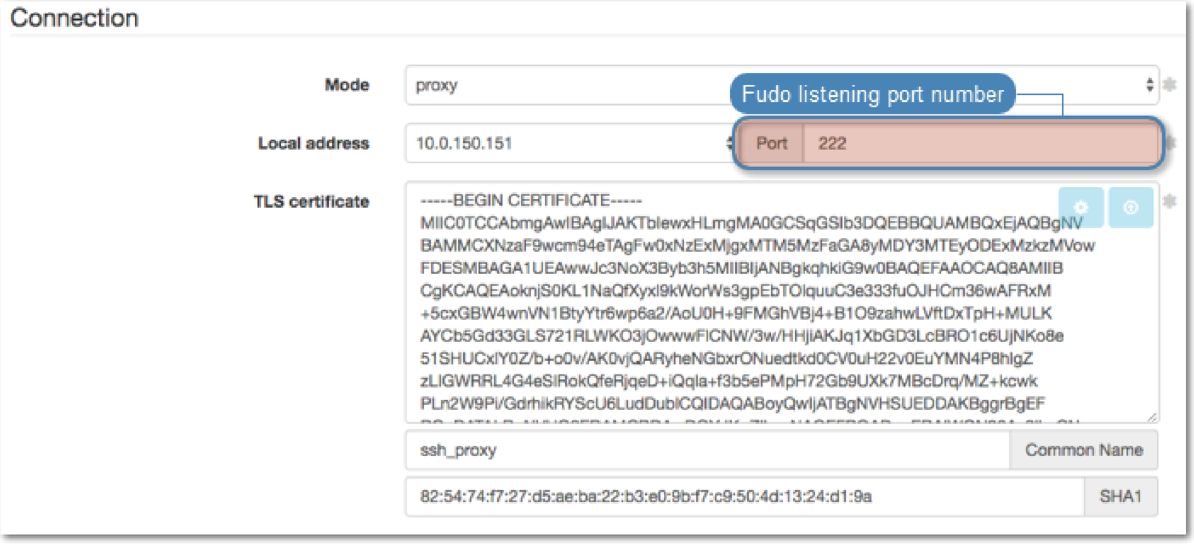
TLS certificate:

```
-----BEGIN CERTIFICATE-----
MIIC0TCCAbmgAwIBAgIJAKTblewxHLmgMA0GCSqGSIb3DQEBBQUAMBQxEjAQBgNV
BAMMCXNzaF9wcm94eTAgFw0xNzExMjgxMTM5MzFaGA8yMDY3MTEyODExMzkzMVow
FDESMBAGA1UEAwwJc3NoX3Byb3h5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAoknjS0KL1NaQfXyxl9kWorWs3gpEbTOlquuC3e333fuOJHCm36wAFRxM
+5cxGBW4wnVN1BtyYtr6wp6a2/AoU0H+9FMGhVBj4+B1O9zahwLVftDxTpH+MULK
AYCb5Gd33GLS721RLWKO3jOwwwFlCNW/3w/HHjiAKJq1XbGD3LcBRO1c6UjNKo8e
51SHUCxlY0Z/b+o0v/AK0vjQARyheNGbxrONuedtkd0CV0uH22v0EuYMN4P8hlgZ
zLIGWRRL4G4eSIRokQfeRjqeD+iQqla+f3b5ePMpH72Gb9UXk7MBcDrq/MZ+kcwk
PLn2W9Pi/GdrhikRYScU6LudDublCQIDAQABoyQwIjATBgNVHSUEDDAKBggrBgEF
```

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

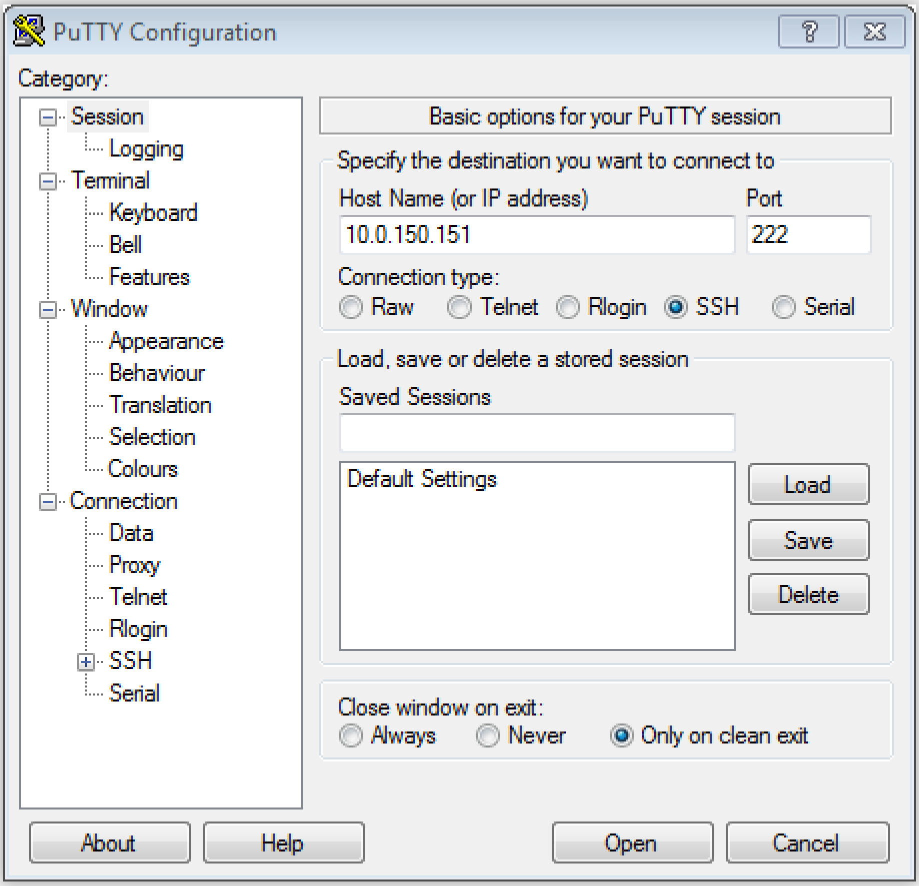
TLS certificate:

```
-----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
```

Common Name: ssh_proxy

SHA1: 82:54:74:f7:27:d5:ae:ba:22:b3:e0:9b:f7:c9:50:4d:13:24:d1:9a

4. Select the SSH connection type.



Specify the destination you want to connect to

Host Name (or IP address): 10.0.150.151

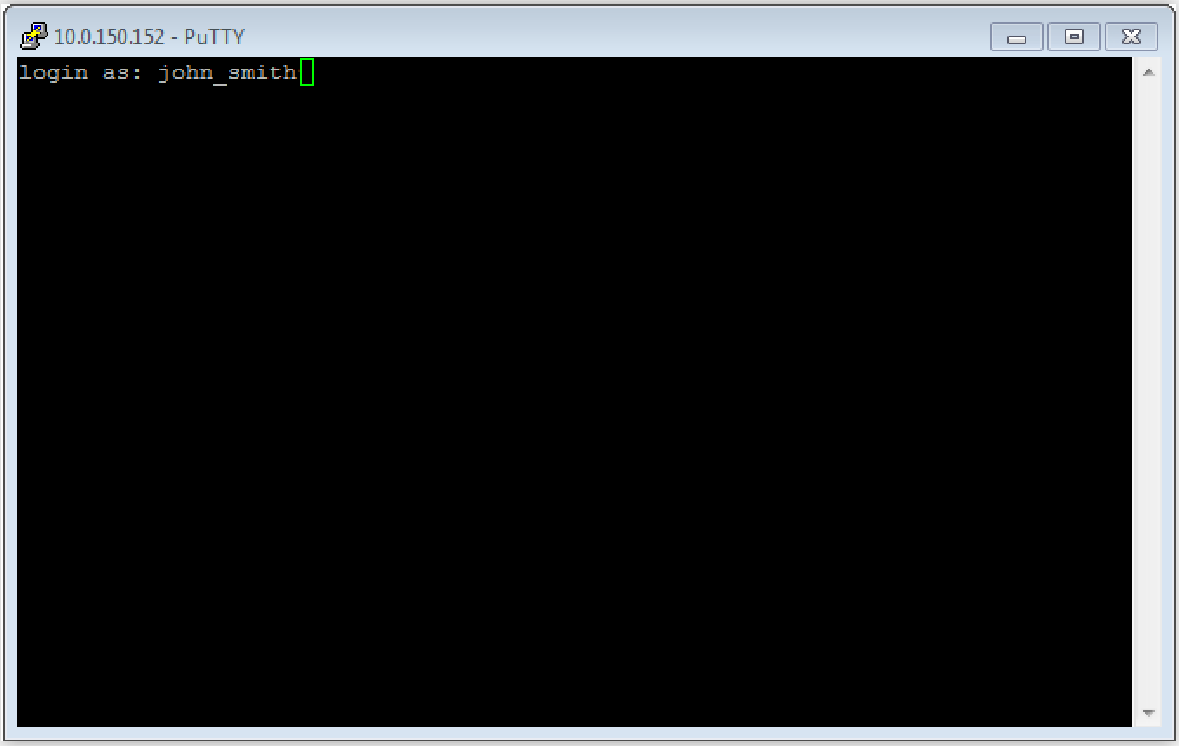
Port: 222

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
```

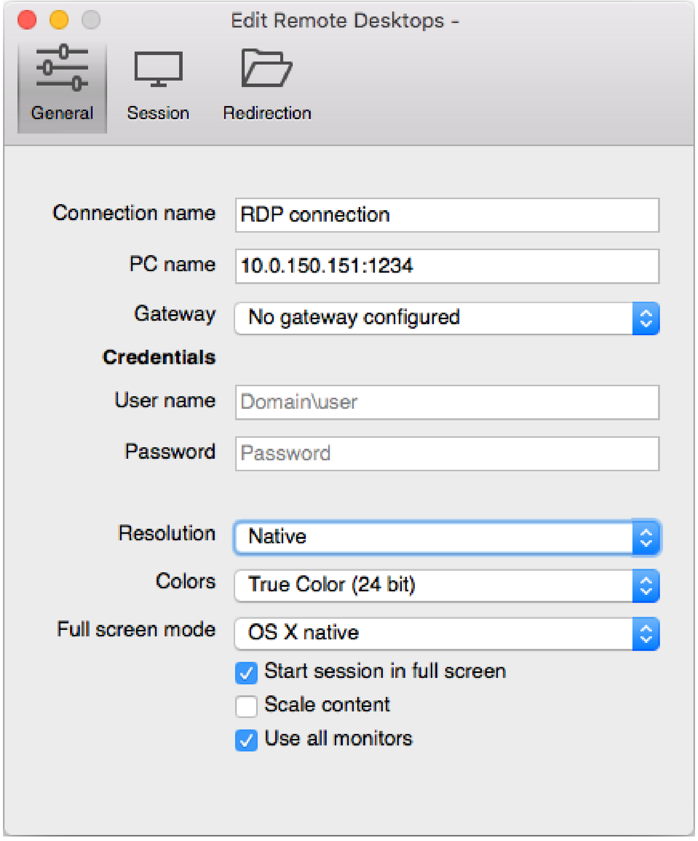
7. Enter password.

Related topics:

- *SSH*
- *Creating an SSH server*
- *Creating an SSH listener*

27.2 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)

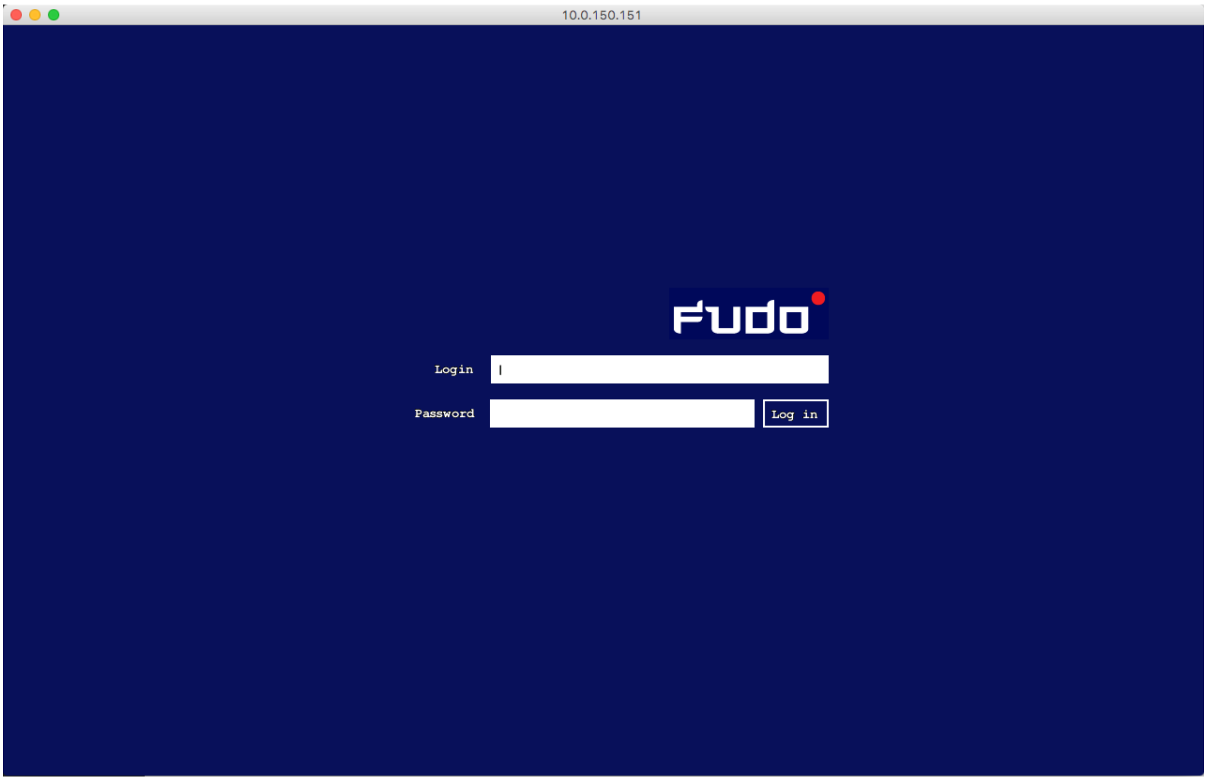
Full screen mode: OS X native

☑ Start session in full screen

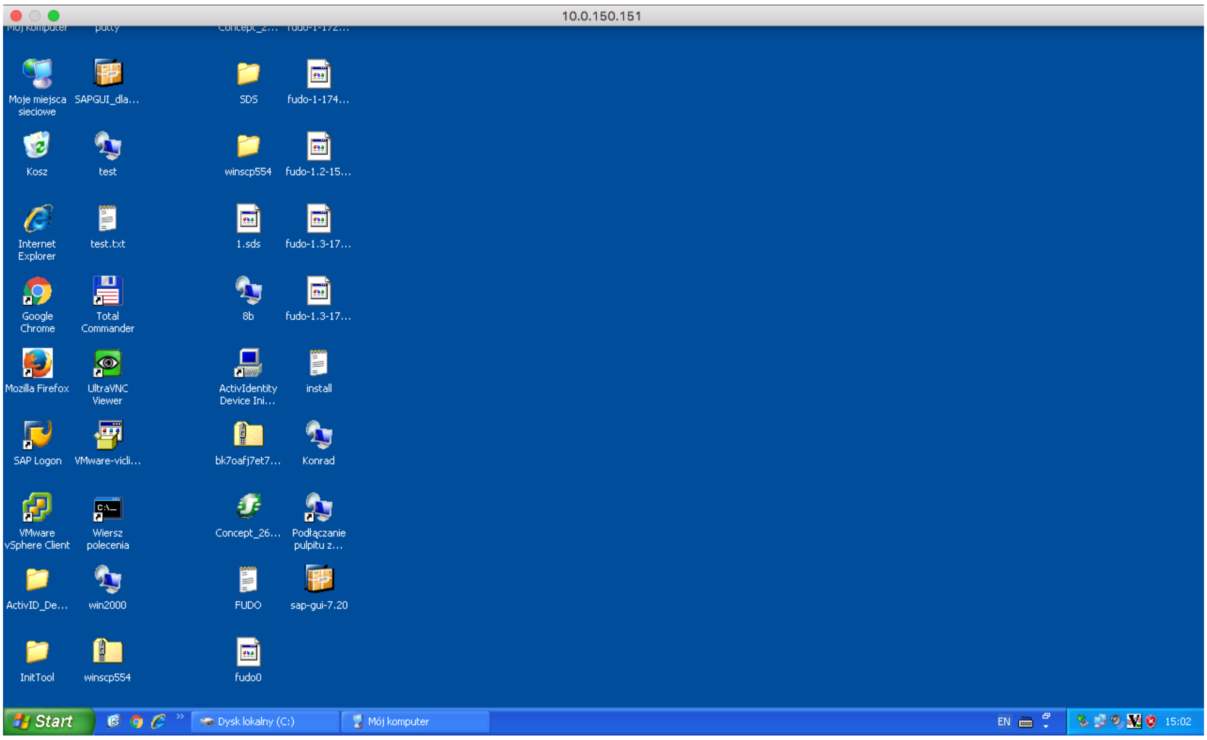
□ Scale content

☑ Use all monitors

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



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

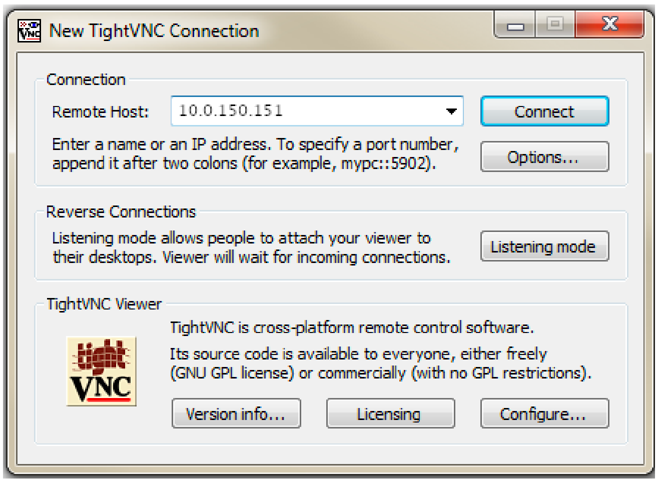


Related topics:

- *RDP*
- *Creating an RDP server*
- *Creating an RDP listener*

27.3 TightVNC Viewer

1. Launch *TightVNC Viewer*.
2. Enter IP address in the server address field as defined in the created VNC listener object (for more information refer to the *Quick start - VNC* topic).



New TightVNC Connection

Connection

Remote Host: 10.0.150.151

Enter a name or an IP address. To specify a port number, append it after two colons (for example, mypc::5902).

Reverse Connections

Listening mode allows people to attach your viewer to their desktops. Viewer will wait for incoming connections.

TightVNC Viewer

TightVNC is cross-platform remote control software.

Its source code is available to everyone, either freely (GNU GPL license) or commercially (with no GPL restrictions).

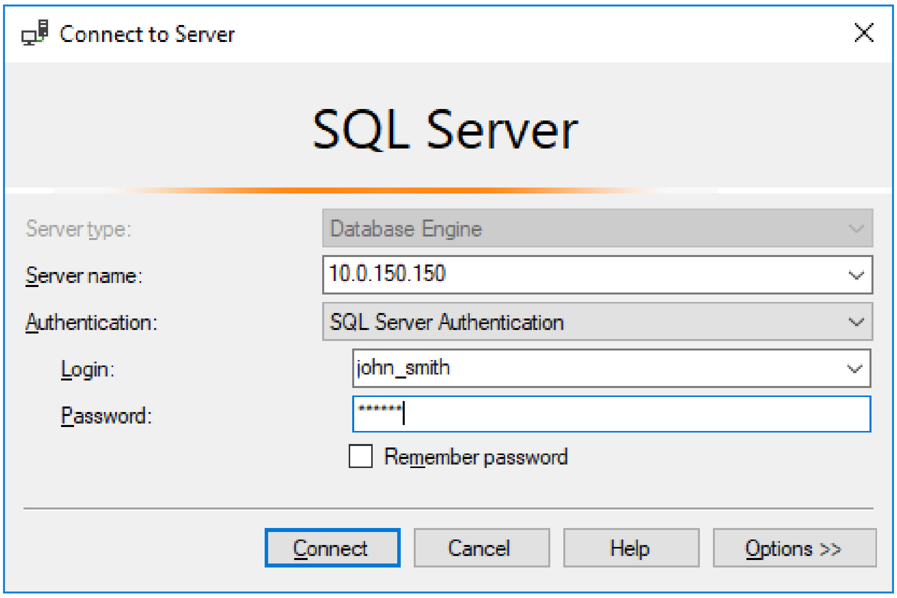
3. Enter username and password and press the enter key.

Related topics:

- *VNC*
- *Creating a VNC server*
- *Creating a VNC listener*

27.4 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

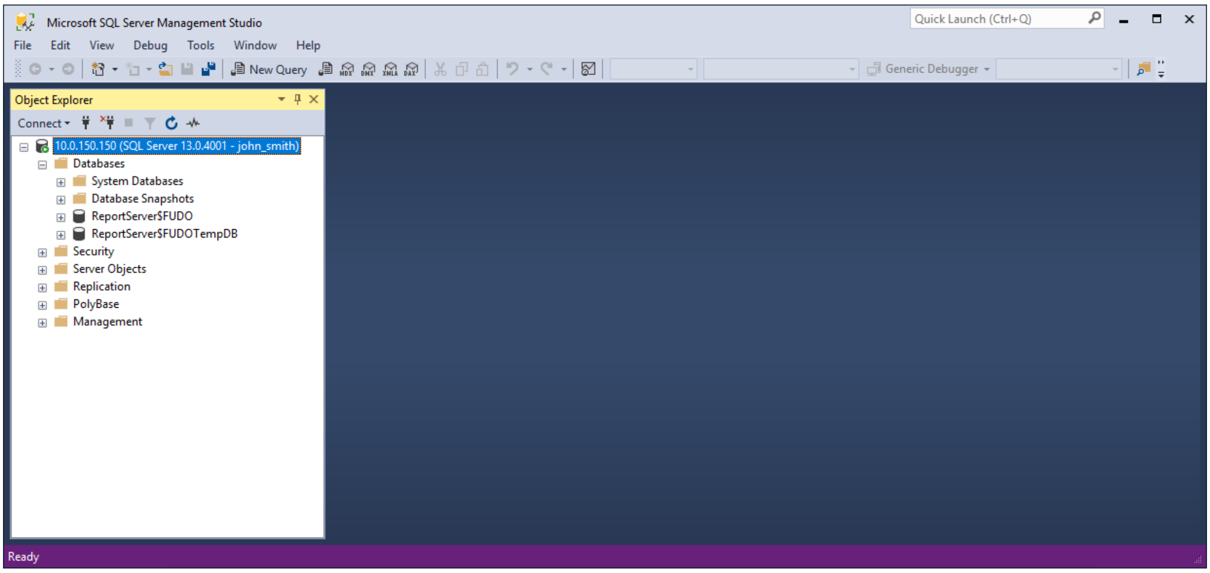
Server name: 10.0.150.150

Authentication: SQL Server Authentication

Login: john_smith

Password: ******

□ Remember password



10.0.150.150 (SQL Server 13.0.4001 - john_smith)
- Databases
  - System Databases
  - Database Snapshots
  - ReportServer$FUDO
  - ReportServer$FUDOTempDB
- Security
- Server Objects
- Replication
- PolyBase
- Management

Related topics:

- *MS SQL*
- *Creating a MS SQL server*
- *Creating a MS SQL listener*

CHAPTER 28

Troubleshooting

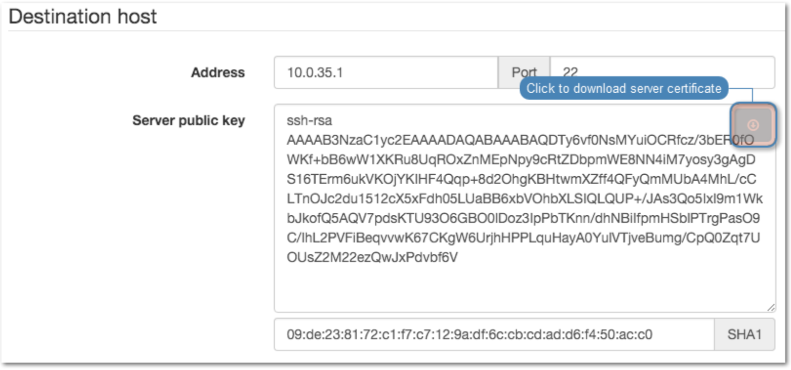
28.1 Booting up

Problem	Symptoms and solution
Fudo Enterprise does not boot up	• Make sure that both power supplies are connected to power outlets. Not connecting both power supplies will result in sound alarm. • Make sure that encryption key is properly connected. • In case the problem is a result of unsuccessful system update, wait a few minutes. During that time, Fudo Enterprise will detect the problem and will restore previous system revision.

28.2 Connecting to servers

Problem	Symptoms and solution
Cannot connect to server	**Symptoms:** • User cannot log in. • Events log entry: *Authentication failed: Invalid username kowalski or password.*
	Solution: • Verify that user definition exists in Fudo Enterprise database. • Make the login credentials are correct. • Make sure that the client software does not have outdated credentials stored. • Check if the user has a domain defined and make sure it is provided when attempting to log in. • If there are two users with the same login, one of which has the domain configured the same as the *default domain*, and the other does not have the domain defined, Fudo Enterprise will report authentication problem as it cannot determine which user is trying to connect.
	Symptoms: events log entry: *Unable to establish connection to server zbigniew (10.0.35.53:3399).*
	Cause: incorrect server configuration.
	Solution: • Verify that the server in question is properly configured (IP address, port number). • Check if the server is reachable from Fudo Enterprise: 1. Log in to Fudo Enterprise administration panel. 2. Select *Settings* > *System*, *Diagnostics* tab. 3. Enter server address in the *Ping* section and execute command and test host's availability. • Check if the server is reachable on given port number: 1. Log in to Fudo Enterprise administration panel. 2. Select *Settings* > *System*, *Diagnostics* tab. 3. Enter server address along with the port number in the *Netcat* section and execute command.
	Symptoms: Message in client software: *Cannot establish new connection because the capacity of the filesystem has been reached.*
	Cause: Storage usage has reached 90%.
	Solution: *Delete sessions* to free up storage space.

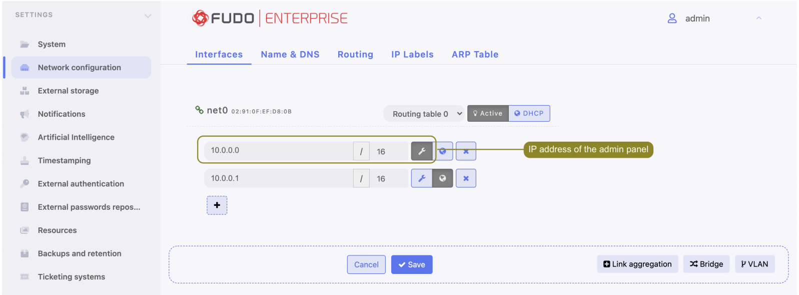
Problem	Symptoms and solution
When logging in not all of the users see the Fudo Enterprise logon screen.	**Cause:** • Credentials stored in RDP client result in users being automatically logged in to remote host. • Credentials stored in RDP client, user is successfully authenticated against credentials stored so the Fudo Enterprise logon screen is not displayed. Next, Fudo Enterprise forwards user credentials to target server but they are no longer valid which results in Windows gina being displayed.
	Symptoms: • Client software message: *Connection closed by remote host.* • Events log entry: *Failed to authenticate against the server as user root using password.*
	Cause: incorrect login credentials.
	Solution: provide correct login credentials in server configuration.
	Symptoms: • RDP client message: *Connection refused.* • SSH client message: *ssh: connect to host 10.0.1.111 port 10011: Connection refused*
	Cause: server has been blocked.
	Solution: log in to Fudo Enterprise administration panel and unblock the server.

Problem	Symptoms and solution
Connection is terminated	**Symptoms:** • User tries to log in to server monitored by Fudo Enterprise, after entering username and password session is immediately terminated. • Events log entry: *TLS certificate verification failed.*
	Solution:
	Download new target host certificate in the *Target host* section.
	 Destination host Address: 10.0.35.1 Port: 22 Click to download server certificate Server public key: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDTy6vf0NsMYuiOCRfcz/3bER0fOWKf+bB6wW1XKRu8UqROxZnMEpNpy9cRtZDbpmWE8NN4iM7yosy3gAgDS16TErm6ukVKOjYKIHF4Qqp+8d2OhgKBHtwmXZff4QFyQmMUbA4MhL/cCLTnOJc2du1512cX5xFdh05LUaBB6xbVOhbXLSIQLQUP+/JAs3Qo5Ixl9m1WkbJkofQ5AQV7pdsKTU93O6GBO0lDoz3IpPbTKnn/dhNBiIfpmHSbIPTrgPasO9C/IhL2PVFiBeqvvwK67CKgW6UrjhHPPLquHayA0YulVTjveBumg/CpQ0Zqt7UOUsZ2M22ezQwJxPdvbf6V 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 Enterprise administration panel and unblock the user in question.
User has to provide login credentials twice	**Symptoms:** user connecting over RDP protocol enters login credentials and immediately afterwards is asked again for the same login information.
	Cause: server is a part of an infrastructure managed by connections broker which has detected an active user's session on another server.
	Symptoms: user connecting over SSH protocol enters login credentials and immediately afterwards is asked again for login information.
	Cause: in *connection* object options for login and password substitution are enabled but the input fields are left blank which results in two fold authentication - first time against Fudo Enterprise and second time against the target host.
Cannot connect to server over RDP protocol	**Symptoms:** • User connecting over RDP is disconnected a moment after establishing connection. • Events log entry: *RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.*
	Cause: connection is redirected to a host which does not listen on port number 3389.
	Solution: configure server in question so it accepts user connections on port number 3389.
	Symptoms: • Events log entry: *User user0 has no access to host 192.168.0.1:3389*
	Cause: connections broker determines an existing user session on another server and redirects user to that host but it is not configured on Fudo Enterprise or the user does not have sufficient access rights to connect to given server.
	Solution: • Make sure that the server object exists. • Add user to proper *safe* object.

Problem	Symptoms and solution
Cannot connect to Telnet5250 server using PC5250 client revision 20091005 S/20111019 S	**Symptoms:** cannot establish connection to target host.
	Cause: in case of aforementioned client applications, Fudo Enterprise requires setting up additional objects to enable TCP traffic on ports number 449, 8470 and 8476.
	Soluiton: - Add Telnet TN5250 server with default port number. - Add three server objects with `TCP` protocol and following port numbers 449, 8470 and 8476. - Add `TN5250` listener, in `Proxy` mode with default port number. - Add three `TCP` listener objects, in `Proxy` mode, with port numbers 449, 8470 and 8476. - Add `regular` account, define authentication parameters and assign it to the main TN5250 server definition. - Add three `anonymous` accounts and assign each to one of supporting servers. - Add safe and assign account with corresponding listeners.

28.3 Logging to administration panel

Problem	Symptoms and solution
Cannot log in to administration panel	- Make sure that Fudo Enterprise IP address is correct. - Set Fudo Enterprise IP address from the console as described in the *Fudo Enterprise System documentation* in the *Network interfaces configuration* topic. - Make sure that the IP address in question has the management access option enabled.  net0 02:91:0F:EF:D8:0B 10.0.0.0 / 16 10.0.0.1 / 16 IP address of the admin panel SETTINGS System Network configuration External storage Notifications Artificial Intelligence Timestamping External authentication External passwords repos... Resources Backups and retention Ticketing systems FUDO ENTERPRISE admin Interfaces Name & DNS Routing IP Labels ARP Table Routing table 0 Active DHCP + Cancel Save Link aggregation Bridge VLAN

28.4 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.

28.5 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.

28.6 Trusted timestamping

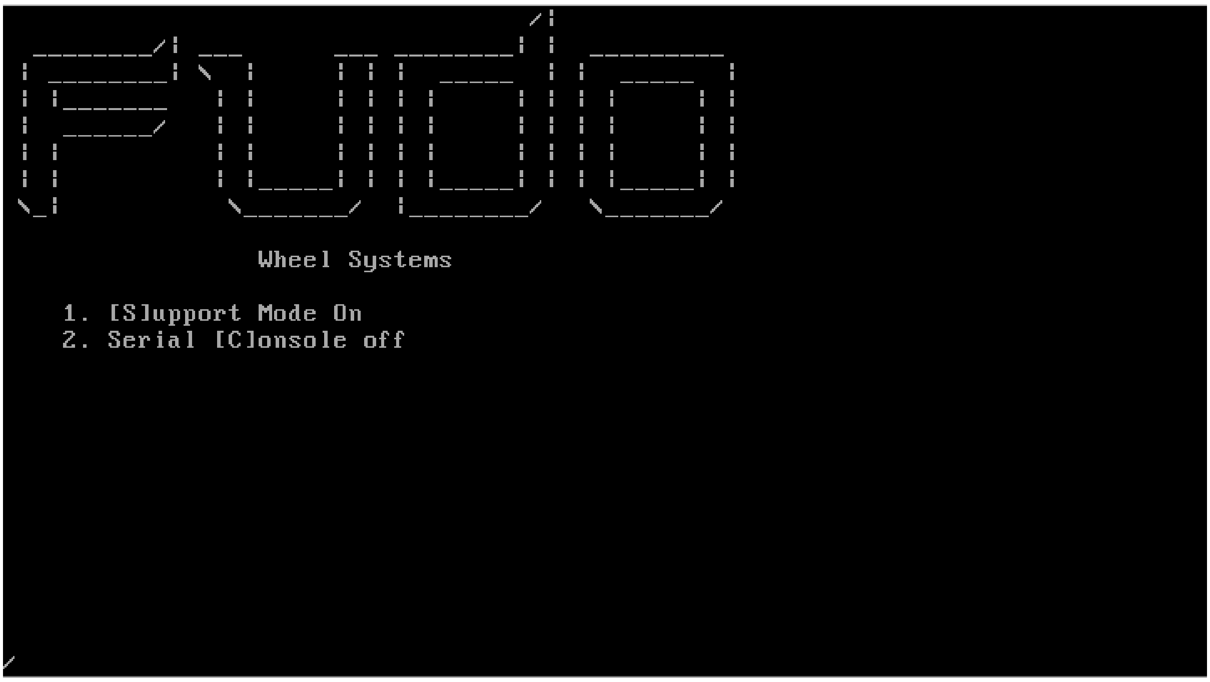
Problem	Symptoms and solution
Session are not timestamped	**Symptoms:** • System log entry: *Timestamping service communication error.*
	Reason: Time-stamping host is not reachable by Fudo.
	Solution: Make sure that firewall settings allow traffic to the time-stamping service server. • PWPW time-stamping 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*.

28.7 Support mode

Support mode enables remote access to Fudo Enterprise in case it cannot boot up properly.

Enabling support mode

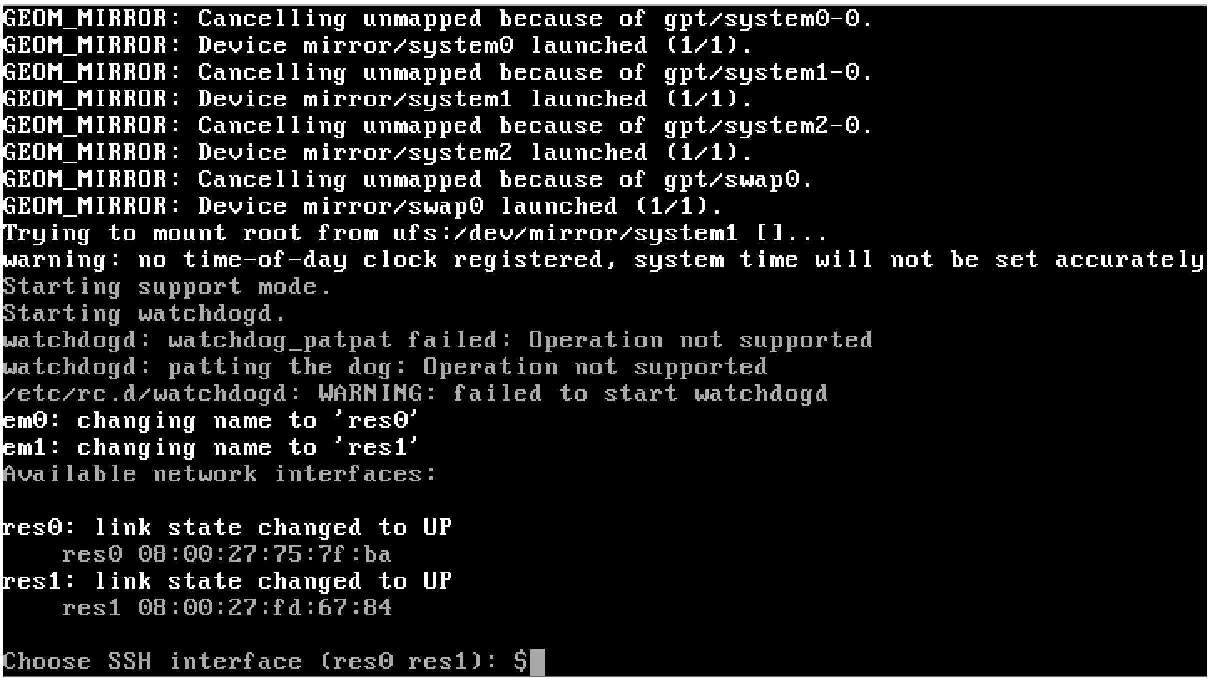
1. Access the system terminal.
2. During the boot up, enter `1` and press the *Enter* key to confirm.



```
                 Wheel Systems

    1. [S]upport Mode On
    2. Serial [C]onsole off
```

3. Select network interface.

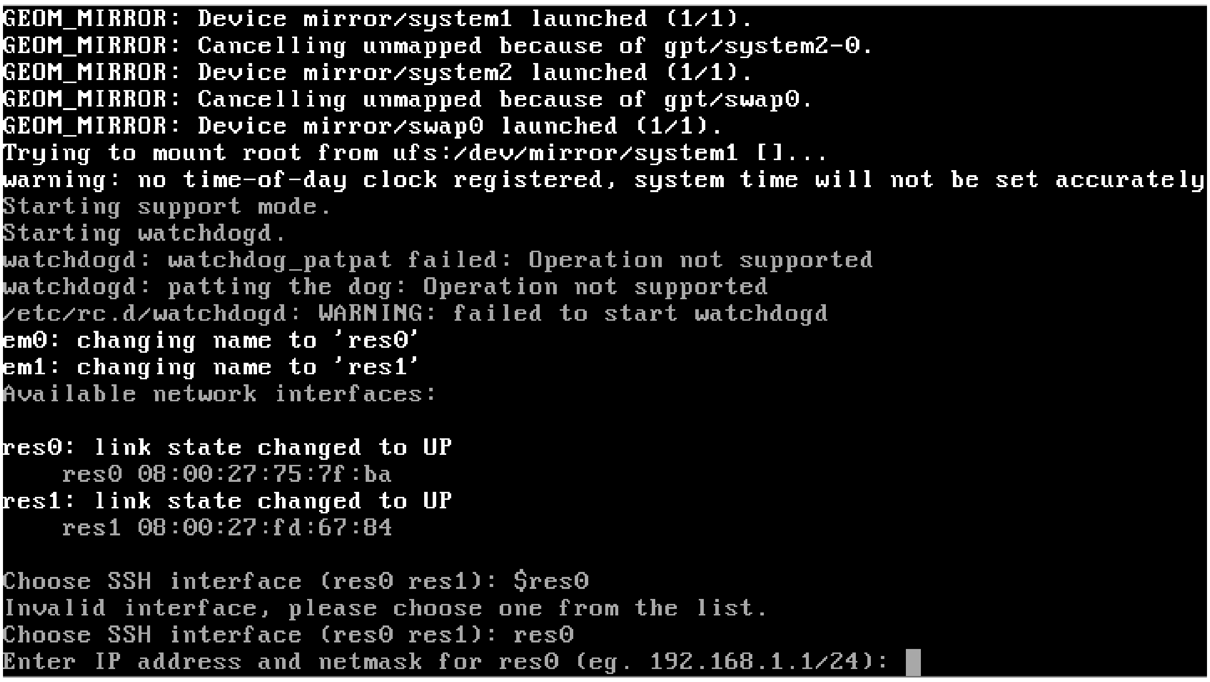
Note: In support mode, network interfaces are named `res*` instead of `net*`.



```
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): $
```

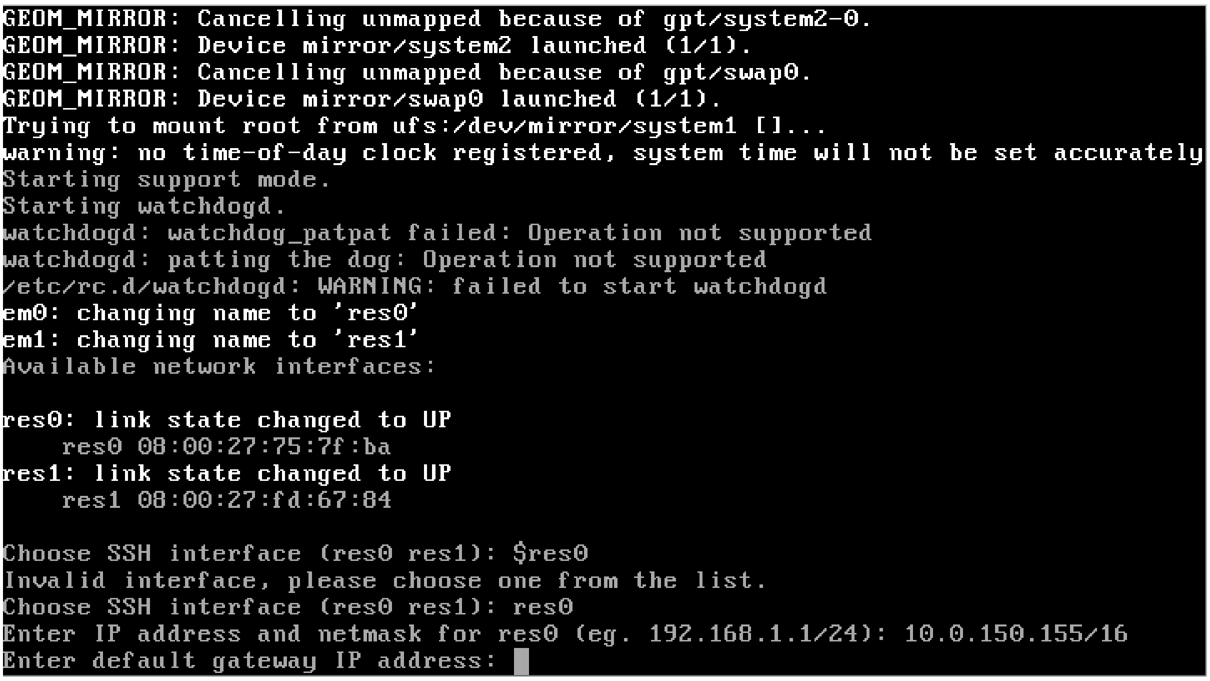
4. Enter the IP address along with network mask, eg. `10.0.0.8/16`.

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):
```

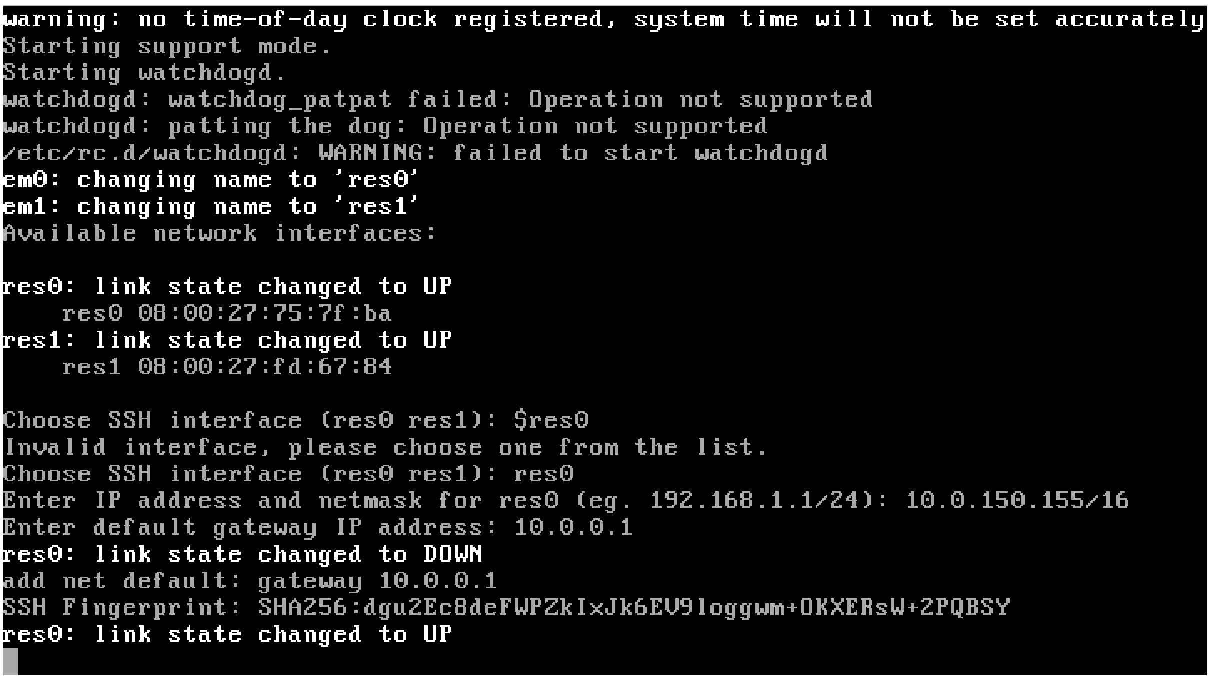
5. Enter the gateway's IP address and press enter to enable connection to your Fudo Enterprise.



```
GEOM_MIRROR: Cancelling unmapped because of gpt/system2-0.
GEOM_MIRROR: Device mirror/system2 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/swap0.
GEOM_MIRROR: Device mirror/swap0 launched (1/1).
Trying to mount root from ufs:/dev/mirror/system1 []...
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24): 10.0.150.155/16
Enter default gateway IP address:
```

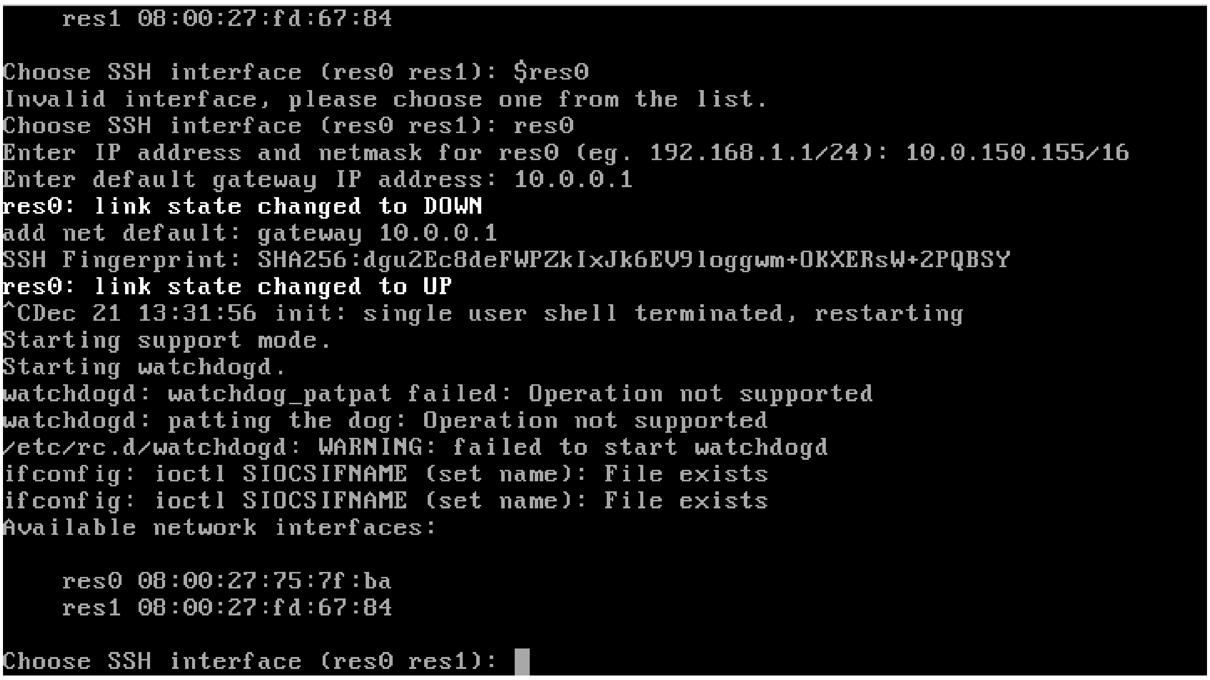
Note:

- Fingerprint allows for verifying that the connection has been established with the correct remote host.



```
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24): 10.0.150.155/16
Enter default gateway IP address: 10.0.0.1
res0: link state changed to DOWN
add net default: gateway 10.0.0.1
SSH Fingerprint: SHA256:dgu2Ec8deFWPZkIxJk6EV9loggwm+0KXERsW+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+0KXERsW+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 29

Frequently asked questions

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

2. How Fudo Enterprise supports sessions archiving?

3. How to calculate storage space required for archiving sessions?

4. How users can hide their activities on servers which they access through Fudo Enterprise?

5. How to determine unauthorized access attempts to supervised servers?

6. Is it possible to hide the login screen when connecting over the RDP protocol?

7. Why the users list in the connection's properties is incomplete?

8. Why is a user removed from the LDAP/AD server still present on the users list?

9. How frequently are users' definitions synchronized with an LDAP/AD server?

*10. I see * instead of the keystrokes in the session player. Is it possible to see the actual keyboard input?*

11. Can I deactivate a session URL?

12. What should I do before returning a demonstration unit after testing?

AI session processing

13. How long does it take for the model to learn? How many sessions do I have to record to see results?

14. We have 20 accounts and 20 users in our company - how long will it take to see differences?

15. If I connect to different servers, does Fudo create a separate model for each of them?

16. If I give my login credentials to another person, will the AI detect that someone else has logged in and terminate the session?

17. Session status icon is yellow all the time - what does it mean?

18. Five users use the same account to establish connections - will the system be able to determine who and when has logged in onto the server?

19. How will the system determine that it wasn't me if we all use the same commands?

20. Sessions are not analyzed, why is that?

1. How many user sessions can be stored at once?

Fudo Enterprise F1000 series is delivered with 24 TB of RAW hard drive space (15.9 TB usable) while the F3000 series appliances come with 96 TB of RAW storage space (59.9 TB usable) dedicated for storing users sessions.

Size of the stored session is determined by user's activity. An hour of recorded connection takes on average:

RDP	218 MB active user session (no activity generates almost no data). Definite session size depends on the screen resolution, color depth and actual user activity.
SSH	41.5 MB active session.

Given that assumptions, internal storage space enables recording of:

	RDP	SSH
F1000	28.6 years	150.2 years
F3000	112.8 years	592.5 years

Note:

- Disk usage figures include space taken up by the filesystem's redundancy mechanism. The filesystem reserves a portion of available storage, which results in some of the storage space being reported as used on a newly initiated system.
- Fudo Enterprise allows specifying how long sessions data should be stored, and will automatically delete session data after a certain time, determined by *retention parameter*, elapses.

2. How Fudo Enterprise supports sessions archiving?

All sessions are stored on Fudo Enterprise internal storage space. In addition to that, Fudo Enterprise allows exporting sessions in native format or a video record.

3. How to calculate storage space required for archiving sessions?

File size of sessions in native format are the same as in question 1. In case of video record, file size depends on the codec and resolution settings.

4. How users can hide their activities on servers which they access through the Fudo Enterprise?

In case of the SSH protocol, Fudo Enterprise supports SCP channel and monitors all transferred files, including scripts. This allows auditing given session searching for malicious code embedded in software sent to the server.

Protection of other communication channels (e.g. web browser or other applications) are task for different kind of solutions. There is no solution similar to Fudo Enterprise which are able to monitor such channels, thus it is important to create proper server configuration by the system administrator.

5. How to determine unauthorized access attempts to supervised servers?

Unauthorized access and DoS attacks attempts, can be determined by analyzing event log entries. Each ERROR or WARNING severity entries should be closely examined. Cases of login timeout errors can be potential DoS attack attempts.

6. Is it possible to hide the login screen when connecting over the RDP protocol?

Hiding the Fudo Enterprise login screen requires using the `Enhanced RDP Security (TLS) + NLA` security mode.

7. Why the users list in the connection's properties is incomplete?

The users list in the connection's properties does not contain users synchronized with the LDAP service. To assign a connection to an LDAP synchronized user, define a group mapping in the *LDAP synchronization properties* or disable the synchronization option for the given user.

8. Why is a user removed from the LDAP/AD server still present on users list?

Deleting a user object from an AD or an LDAP server requires performing the full synchronization to reflect those changes on Fudo Enterprise. The full synchronization process is triggered automatically once a day at 00:00, or can be triggered manually in the *LDAP synchronization* settings view.

9. How frequently are users' definitions synchronized with an LDAP/AD server?

New users definitions and changes in existing objects are imported from the directory service periodically every 5 minutes. The full synchronization process is triggered automatically once a day at 00:00.

10. I see * instead of the keystrokes in the session player. Is it possible to see the actual keyboard input?

Presenting keyboard input qualifies as a sensitive feature and it is disabled by default. Enabling displaying keystrokes in the session player requires a consent from two `superadmin` users. Refer to the *Sensitive features* topic for the details on enabling this functionality.

11. Can I deactivate a session URL?

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

12. What should I do before returning a demonstration unit after testing?

After testing Fudo, you should delete all session and configuration data by *resetting configuration to default settings* and erase the flash drive with the encryption key.

13. How long does it take for the model to learn? How many sessions do I have to record to see results?

Models are trained as scheduled in the *AI system settings*.

- For the SSH model the minimum are 65 sessions (with at least 25 different commands) and 5 unique predictors (e.g. users). Optimal results require 300 sessions per predictor (e.g. user) and 10 unique predictors (e.g. users).
- For the RDP model, the minimum are 5 hours of session recordings per predictor (e.g. user). Optimal results require 30 hors of session recordings and 10 unique predictors (e.g. users).

14. We have 20 accounts and 20 users in our company - how long will it take to see differences?

This solely depends on the availability of session data. If there is enough session information available to build models, you can expect model to be trained the next day after first predictor session is recorded.

- For SSH model the minimum are 65 sessions (with at least 25 different commands) and 5 unique predictors (e.g. users). Optimal results require 300 sessions per predictor (e.g. user) and 10 unique predictors (e.g. users).
- For RDP model, the minimum are 5 hours of session recordings per predictor (e.g. user). Optimal results require 30 hours of session recordings and 10 unique predictors (e.g. users).

15. If I connect to different servers, does Fudo create a separate model for each of them?

Fudo creates and maintains one RDP and one SSH model for a single user.

16. If I give my login credentials to another person, will the AI detect that someone else has logged in and terminate the session?

Fudo Enterprise will detect that someone else has logged in and will set the session risk status to high, 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 Enterprise so it can correctly determine if an account security has been breached.

19. How will the system determine that it wasn't me if we all use the same commands?

Every user runs the same commands differently. E.g. one user will execute `ls -la` and another will run `ls -al`. Combination of such subtle differences allows for determining a if the currently logged in user matches the profile.

20. Sessions are not analyzed, why is that?

In order for a session to be analyzed, there must be a matching model available. Also, session has to meet volumetric requirements - it must be long enough and carry enough information. Refer to *AI sessions processing* for more information.

CHAPTER 30

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.

Azure Microsoft Azure is a cloud computing service operated by Microsoft for application management via Microsoft-managed data centers.

anonymous safe An anonymous safe has at least one anonymous account assigned to it and it can only have that type of accounts assigned. You cannot assign users to anonymous safes.

AUROC Area Under ROC curve (AUROC) is a single metric representing model quality (the higher the better).

ARP Address Resolution Protocol - protocol used for mapping Internet layer addresses (IP addresses) to the physical - link layer addresses (MAC addresses).

CERB Complete user authentication and authorization solution, supporting different authentication methods i.e., mobile token (mobile phone application), static password, SMS onetime passwords, etc.

CIDR Short notation of network addressing, in which the IP address is written according to the IPv4 standard, and the subnet mask is provided as a number of *1* in the subnet mask in binary system (192.168.1.1 - 255.255.255.0; 192.168.1.1/24).

data retention Data retention mechanism automatically deletes session data after define time period transpires.

DHCP Mechanism for dynamic IP addressing management i LAN networks.

DNS Domain Name Server - name server service which maps IP addresses to hosts names which are easier to remember.

DUO is a mobile application that works with Duo Security's two-factor authentication service. The application generates passcodes for login and can receive push notifications for authentication.

Efficiency Analyzer/Productivity Analyzer Efficiency Analyzer/Productivity Analyzer module delivers statistical information on users' activity.

external authentication server Server storing user data used for verification of user login credentials when connecting to Fudo Enterprise or the monitored server.

False Positive Rate False Positive Rate (FPR) is the percentage of legitimate sessions inappropriately identified as malicious (the lower the better).

Fingerprint Characters string being a result of a hash function on input data, allowing to determine if the input data has been altered.

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.

Okta Okta provides cloud software to manage and secure user authentication into applications.

OpenID Connect OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol.

password changer Tool which enables facilitating automated password changing on a server.

passwords repository Passwords repository manages password to privileged accounts on monitored hosts.

policy Mechanism which enables defining patterns which in case of being detected will trigger defined actions.

PSM (Privileged Session Management) PSM module is used for recording remote access sessions.

PSM PSM (Privileged Session Monitoring) module enables monitoring and recording remote access sessions.

Public key Authentication method which uses a pair of keys - private (held only by the user) and public (publicly available) to determine user's identity.

RADIUS Remote Authentication Dial In User Service - networking protocol used to control access to different services within IT infrastructure.

RDP Remote Desktop Protocol - remote access protocol to computer systems running Microsoft operating system.

RDP connections broker Remote sessions management mechanism for server farms.

redundancy group Defined group of IP addresses, which in case of a system failure, will be seamlessly carried over to another cluster node to maintain the availability of the services.

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

server

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

shared session User session which was joined by another user.

SMS is a text messaging service component of most telephone, and mobile device systems.

SSH Secure Shell - networking protocol for secure communication with remote systems.

SSH access Service access to Fudo Enterprise over SSH protocol.

Static password Basic user authorization method which uses login and password combination to determine users's identity.

Syslog Events logging standard in computer systems. Syslog server collects and stores log data from networked devices, which can be later used for analysis and reporting.

Threat Probability Threat probability is a percentage-wise value that reflects a threat level of the session.

time policy Time policy mechanism enables defining time periods during which users are allowed to connect to monitored hosts.

timestamp Session data hash value, which enables verifying that the data has not been modified.

True Positive Rate True Positive Rate (TPR), sometimes called Recall - is a percentage of malicious sessions properly flagged by the model as suspicious (the higher the better).

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

VLAN Virtual networks mechanism, enabling separation of broadcast domains.

VNC Remote access protocol to graphical user interfaces.

WWN World Wide Name - unique object identifier in external storage solutions.

Index