# FUDD

# Wheel Fudo PAM 3.3 - System Documentation

Release is not supported

Wheel Systems

September 09, 2021

## Contents

1	<b>Gene</b> 1.1	eral information About documentation	<b>1</b> 1		
<b>2</b>	em overview	3			
	2.1	PSM	3		
		2.1.1 Citrix StoreFront (HTTP)	3		
		2.1.2 HTTP	4		
		2.1.3 ICA	4		
		2.1.4 Modbus	4		
		2.1.5 MS SQL (TDS) $\ldots$	5		
		$2.1.6 \qquad MySQL \qquad \dots \qquad $	5		
		2.1.7 Oracle	5		
		2.1.8 RDP	6		
		2.1.9 SSH	6		
		2.1.10 Telnet 3270	7		
		2.1.11 Telnet 5250	7		
		2.1.12 Telnet	7		
		2.1.13 VNC	8		
		2.1.14 X11	8		
	2.2	AAPM (Application to Application Password Manager)	9		
	2.3	Secret manager	9		
	2.4Efficiency Analyzer2.5User portal				
	2.6	Data model	10		
	2.7	Deployment scenarios	12		
	2.8	Connection modes	13		
	2.9	User authentication methods and modes	15		
	2.10	Security measures	16		
		2.10.1 Data encryption	16		
		2.10.2 Backups	17		
		2.10.3 Permissions	17		
		2.10.4 Sandboxing	17		
		2.10.5 Reliability	17		
		2.10.6 Cluster configuration	18		

## 3 System deployment

	3.1	Requirements
	3.2	Hardware overview
	3.3	System initiation
4	Quic	ck start 27
	4.1	SSH
	4.2	RDP
	4.3	Telnet
	4.4	Telnet $5250 \ldots 48$
	4.5	$MySQL \dots \dots$
	4.6	HTTP
	4.7	Citrix
		4.7.1 ICA
		$4.7.1.1  \text{Prerequisites}  \dots  \dots  \dots  \dots  \dots  \dots  \dots  \dots  \dots  $
		$4.7.1.2  \text{Configuration}  \dots  \dots  \dots  \dots  \dots  \dots  \dots  \dots  \dots  $
		4.7.1.3 Creating .ica file with connection parameters
		4.7.1.4 Connecting to remote resource $\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots $
		4.7.1.5 Viewing user session $\ldots$ 76
		4.7.2 ICA via Citrix StoreFront
		$4.7.2.1$ Prerequisites $\ldots$ $77$
		4.7.2.2 Configuration
		4.7.2.3 Connecting to remote resource
		4.7.2.4 Viewing user session
	4.8	Setting up password changing on a Unix system
<b>5</b>	User	rs 91
	5.1	Creating a user
	5.2	Editing a user
	5.3	Blocking a user
	5.4	Unblooking a user
	5.5	Deleting a user
	5.6	Roles
	5.7	Users synchronization
~	C	
6	Serv	107 107
	6.1	Creating a server
		$6.1.1  \text{Creating a Citrix server}  \dots  \dots  \dots  \dots  \dots  \dots  \dots  \dots  \dots  $
		$6.1.2  \text{Creating an HTTP server}  \dots  \dots  \dots  \dots  \dots  \dots  \dots  \dots  \dots  $
		$6.1.3  \text{Creating an ICA server} \dots \dots$
		6.1.4 Creating a Modbus server
		6.1.5 Creating a MS SQL server
		6.1.6 Creating a MySQL server
		6.1.7 Creating an Oracle server
		6.1.8 Creating an RDP server 121
		6.1.9 Creating an SSH server $\ldots \ldots \ldots$
		6.1.10 Creating a Telnet server $\ldots \ldots \ldots$
		6.1.11 Creating a Telnet 3270 server
		6.1.12 Telnet 5250 server
		6.1.13 Creating a VNC server
	6.2	Editing a server
	6.3	Blocking a server

	6.5	Deleting a server					
7 Accounts							
	7.1	Creating an account					
		7.1.1 Creating an <i>anonymous</i> account					
		7.1.2 Creating a <i>forward</i> account					
		713 Creating a <i>regular</i> account 1111 1111 1111 1111 1111 1111 1111 1					
	7 9	Editing an account					
	1.2	Editing an account					
	1.3	Blocking an account					
	7.4	Unblocking an account					
	7.5	Deleting an account					
8	Safe	149					
	8.1	Creating a safe					
	82	Editing a safe 151					
	83	Blocking a safe					
	0.0 Q 1	Unblocking a safe 152					
	0.4						
	8.5	Deleting a safe					
9	Liste	eners 157					
	9.1	Creating a listener					
		9.1.1 Creating a Citrix listener					
		0.1.2 Creating a HTTP listener 150					
		0.1.2 Creating an ICA ligtoner 161					
		9.1.5 Creating all ICA listener 101					
		9.1.4 Creating a Modulus Insteher					
		9.1.5 Creating a MySQL listener					
		9.1.6 Creating an Oracle listener					
		9.1.7 Creating an RDP listener					
		9.1.8 Creating an SSH listener					
		9.1.9 Creating a MS SQL listener					
		9.1.10 Creating a Telnet listener					
		9.1.11 Creating a Telnet 3270 listener					
		9.1.12 Creating a VNC listener 173					
	0.2	Editing a ligtonor					
	9.2						
	9.3						
	9.4	Unblocking a listener					
	9.5	Deleting a listener					
10	Pass	word changers 179					
	10.1	Password changer policy					
	10.2	Custom password changers					
11	Polie	ties 185					
12	Sessi	ons 191					
	12.1	Filtering sessions 192					
		12.1.1 Defining filters 102					
		12.1.1 Doming moto					
		12.1.2 Full text search $1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.$					
	10.0	12.1.5 Managing user defined filter definitions					
	12.2	Viewing sessions					
	12.3	Viewing live sessions					
	12.4	Pausing connection					

1: 1: 1: 1: 1: 1: 1: 1: 1: 1:	2.5 2.6 2.7 2.8 2.9 2.10 2.11 2.12	Terminating connection20Joining live session20Sharing sessions20Commenting sessions20Exporting sessions20Deleting sessions20OCR processing sessions20Timestamping selected sessions2021	10 12 12 15 17 19 19 19
13 R	lepo	21	3
14 E	ffic	ency analyzer 21	7
14	4.1	Overview	.7
14	4.2	Sessions analysis	.8
14	4.3	Activity comparison	0
15 A	dm	inistration 22	1
1!	5.1	System	1
		15.1.1 Date and time	21
		15.1.2 SSL certificate	3
		15.1.3 Deny new connections	:4
		15.1.4 SSH access	:5
		15.1.5 Reset account	6
		15.1.6 Sensitive features	1
		15.1.7 System update	6, 0
		15.1.7.1 Opdating system	.9 20
		15.1.7.2 Rulling upgrade snapshot	.9 20
		15.1.8 License 23	20
		15.1.0 Diagnostics 23	31
1!	5.2	Network settings	12
1		15.2.1 Network interfaces configuration	3
		15.2.1.1 Managing physical interfaces	3
		15.2.1.2 Defining IP address using system console	6
		15.2.1.3 Setting up a network bridge	0
		15.2.1.4 Setting up virtual networks (VLANs)	0
		15.2.2 Bypasses configuration	1
		15.2.3 Routing configuration	2
		15.2.4 DNS servers configuration $\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots 24$	3
1!	5.3	Notifications	.5
1!	5.4	Trusted timestamping	7
1	5.5	External authentication	8
1	5.6	External passwords repositories	:9
		15.6.1 CyberArk Enterprise Password Vault	0
		15.6.2 Hitachi ID Privileged Access Manager	0
		15.6.4 Theoretic Counter Count	1
11		15.0.4 Inycotic Secret Server	2
11	0.1 5 0	Resources     25       System version restore     25	з Л
1	9.0 5.0	System restart 25	4
1 i	5.9 5.10	SNMP 25	7
<b>T</b> (	0	15.10.1 Configuring SNMP	7

	15.10.2 SNMP MIBs
	15.10.3 Wheel Fudo PAM specific SNMP extensions
15.11	Backups and retention
15.12	External storage
	15.12.1 Configuring external storage
	15.12.2 Expanding external storage device
15.13	Exporting/importing system configuration
	15.13.1 Exporting system configuration
	15.13.2 Importing system configuration
15.14	Cluster configuration
-	15.14.1 Initiating cluster
	15.14.2 Adding cluster nodes
	15.14.3 Editing cluster nodes
	15.14.4 Deleting cluster nodes
	15.14.5 Forcing full data synchronization 269
	15 14 6 Redundancy groups
15.15	Events log
15.16	Integration with CERB server 276
15.10	System maintenance
10.17	15 17 1 Backing up encryption keys
	15.17.2 Monitoring system condition
	15.17.3 Hard drive replacement
16 Refe	rence information 293
16.1	RDP connections broker
16.2	Error codes
16.3	Fudo 2.2 to Fudo 3.0 parameters mapping
	16.3.1 Connection
	16.3.2 Server
16.4	Data model migration from Wheel Fudo PAM version 2.2 to 3.0
	16.4.1 Server
	16.4.2 Safe (previously <i>connection</i> )
	16.4.3 Account (previously <i>login credentials</i> )
	16.4.4 Listener (previously <i>bastion</i> or part of a server)
	$16.4.5$ Sessions $\ldots \ldots 302$
16.5	Supported protocols
	16.5.1 Citrix StoreFront (HTTP)
	16.5.2 HTTP
	16.5.3 ICA
	16.5.4 Modbus
	16.5.5 MS SQL (TDS)
	16.5.6 MvSQL
	16.5.7 Oracle
	16.5.8 RDP
	16.5.9 SSH
	16.5.10 Telnet
	16.5.11 Telnet 3270 306
	16.5.12 Telnet 5250 306
	16.5.13 VNC 306
	16 5 14 X11 307
16.6	ICA configuration file
10.0	Outering and

	16.6.1 Plik ICA do połączeń bez TLS	307
	16.6.2 Plik ICA do połączeń bez TLS	307
17 AAF	PM (Application to Application Password Manager) 3	609
17.1	Overview	309
17.2	fudopv	309
17.3	API interface	317
18 Trou	ibleshooting 3	<b>319</b>
18.1	Booting up	319
18.2	Connecting to servers	320
18.3	Logging to administration panel	324
18.4	Session playback	324
18.5	Cluster configuration	325
19 Freq	uently asked questions 3	27
20 Glos	asary 3	31
Index	3	35

# CHAPTER 1

## General information

## 1.1 About documentation

#### **Documentation Structure**

1. General information

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

2. Configuration

This chapter covers detailed configuration procedures.

3. Sessions

This chapter contains information on stored access sessions.

4. Productivity analysis

This chapter describes the productivity analysis module.

 $5. \ Administration$ 

This chapter contains administration procedures.

6. Reference information

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

7. Troubleshooting

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

8. Frequently asked questions

This chapter contains frequently requested information about Wheel Fudo PAM.

9. Glossary

This chapter contains list of terms used throughout this documentation.

#### Conventions and symbols

This section covers conventions used throughout this documentation.

italic

Uster interface elements.

#### example

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

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

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

#### Disclaimer

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

## CHAPTER 2

System overview

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

## 2.1 PSM

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



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

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

Supported protocols and systems

#### 2.1.1 Citrix StoreFront (HTTP)

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Notes:

- Session player displays raw text without graphical rendering.
- Lack of bastion mode support results from protocol's limitations. Citrix StoreFront itself provides access to a bastion of hosts. When logging to Citrix StoreFront, user can select desired host to connect to over ICA protocol.
- Initiating connections with ICA servers over Citrix StoreFront interface requires *anony-mous* or *forward* accounts assigned to those servers.

#### 2.1.2 HTTP

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Notes:

- Session player displays raw text without graphical rendering.
- Bastion mode is not supported due to limitations of the protocol.
- Access to external resources is not monitored.
- Following redirections is not supported.

#### 2.1.3 ICA

Supported connection modes:

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

Supported client applications:

• Citrix Receiver.

#### 2.1.4 Modbus

Supported connection modes:

- Gateway,
- Proxy,

#### • Transparent.

Notes:

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

#### 2.1.5 MS SQL (TDS)

Supported connection modes:

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

Supported client applications:

- SQL Server Management Studio,
- sqsh.

#### 2.1.6 MySQL

Supported connection modes:

- *Gateway*,
- Proxy,
- Transparent.

Supported client applications:

- Official MySQL client,
- PyMySQL libraries for Python.

Notes:

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

#### 2.1.7 Oracle

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

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Supported client applications:

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

#### Notes:

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

#### 2.1.8 RDP

Supported connection modes:

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

Supported client applications:

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

Notes:

- When authenticating Fudo users against AD (or other external source) the TLS+NLA (Network Level Authentication) is not supported; TLS mode is used instead. NLA mode on server side is supported.
- RemoteApp support is in development.

#### 2.1.9 SSH

Supported connection modes:

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

Supported features:

- Connections multiplexing,
- SCP,
- Ports redirection.

#### Notes:

• SFTP sessions playback is not supported,

• SSH keys forwarding is not supported.

#### 2.1.10 Telnet 3270

Supported connection modes:

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

Notes:

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

Supported client applications:

- IBM Personal Communications,
- c3270.

#### 2.1.11 Telnet 5250

Supported connection modes:

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

Notes:

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

Supported client applications:

- IBM Personal Communications,
- tn5250.

#### 2.1.12 Telnet

Supported connection modes:

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

Notes:

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

#### 2.1.13 VNC

Supported connection modes:

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

Supported client applications:

- TightVNC,
- RealVNC.

#### 2.1.14 X11

X11 protocol is supported within the SSH protocol.

Supported servers:

- Xorg,
- Xming,
- XQuartz.

The PSM module supports following system configurations:

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

#### **Related topics:**

- Requirements
- Data model
- Security measures

## 2.2 AAPM (Application to Application Password Manager)

AAPM module enables secure passwords exchange between applications.

#### **Related topics:**

- Requirements
- Data model
- Security measures

## 2.3 Secret manager

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

Secret manager module supports password changing on following systems:

- Unix
- $\bullet~{\rm MySQL}$
- Cisco
- Cisco Enable Password
- MS Windows

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

Related topics:

- Requirements
- Data model
- Security measures

## 2.4 Efficiency Analyzer

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

#### **Related topics:**

- Requirements
- Data model
- Security measures

## 2.5 User portal

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

Fudo							(
ACCOUNTS	_						User men
- AUTHENTICATION		ST OF	ACCOU	NTS			
		NAME	TYPE	SERVER NAME	LISTENER	HOST	PROTOCOL
		RDP	regular	RDP		10.0.40.203:3389	
	0	Show a	iccount pa	assword	RDP	10.0.8.61:2222	rdp
		SSH	regular	SSH		127.0.0.1:22	
	0	- Sho Cor	w passwo inect to s	ords history erver usina se	<mark>ssн</mark> elected listener	10.0.8.61:24	ssh

#### **Related topics:**

- Requirements
- $\bullet \ Data \ model$
- Security measures

## 2.6 Data model

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

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

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

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

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

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

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



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

#### **Objects** relations chart



#### Related topics:

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

## 2.7 Deployment scenarios

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

#### Bridge

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



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

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

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

#### Forced routing

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



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

#### **Related topics:**

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

## 2.8 Connection modes

#### Transparent

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



#### Gateway

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





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



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

#### Bastion

In bastion mode, the account on the target host is specified within the string identifying the user, e.g. ssh john\_smith#admin@10.0.0.8. This enables facilitating access to a group of monitored servers through the same IP address and port number combination.



#### Note:

- The *bastion* mode is supported when connecting over SSH, RDP, VNC, Telnet or Telnet 3270 protocols.
- In case the specified account is not found, Wheel Fudo PAM will try to match the name with a server object.

#### **Related topics:**

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

• Initial boot up

## 2.9 User authentication methods and modes

#### User authentication methods

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

- Static password,
- Public key,
- CERB,
- RADIUS,
- LDAP,
- Active Directory.

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

#### Authentication modes

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

#### Authentication with original login and password

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



#### Authentication with login and password substitution

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

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



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

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

#### Two-fold authentication

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

#### **Related topics:**

- System overview
- External authentication servers configuration
- Security measures

## 2.10 Security measures

#### 2.10.1 Data encryption

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

#### Appliance

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

After encryption keys have been initiated and Wheel Fudo PAM has booted up, both USB flash drives can be removed and placed somewhere safe. During daily operation, encryption key is required only for system boot up. If safety procedures allow, one USB flash drive can stay

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

#### Virtual machine distribution

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

#### 2.10.2 Backups

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

#### 2.10.3 Permissions

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

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

#### 2.10.4 Sandboxing

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

#### 2.10.5 Reliability

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

## 2.10.6 Cluster configuration

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

**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

# chapter 3

System deployment

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

## 3.1 Requirements

#### Administration panel

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

#### Network requirements

Correct operation requires:

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

Hardware requirements (not applicable to virtual appliance distributions)

Wheel Fudo PAM is a complete solution combining both hardware and software. Installing system requires 2U space in 19" rack cabinet and connection to network infrastructure.

VNC software client requirements

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

## 3.2 Hardware overview

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

Front panel view



#### Hard drive bays

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

A hard drive in a hot-swap tray	
Image: state	
Hard drive's state L A hot-swap tray release lever	ED ligths

#### **Related topics:**

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

## 3.3 System initiation

#### Appliance

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

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

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

3. Connect network cable to one of the RJ-45 ports.

4. Connect both of the USB flash drives delivered with Wheel Fudo PAM.

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

5. Press the power button on the front panel.



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

#### Warning:

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

#### Note:

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

#### Setting IP address using system console

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

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
```

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

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

To reset FUDO to factory defaults, login as "reset".

To fix admin account and change network settings,

login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin

Password:

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

*** FUDO configuration utility ***

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

1. Show status

2. Reset network settings

0. Exit

Choose an option (0): 2

Are you sure you want to continue? [y/N] (n):
```

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

FUDO, S/N 12345678, firmware 2.1-23500. To reset FUDO to factory defaults, login as "reset". To fix admin account and change network settings, login as "admin" with an appropriate password. FUDO (fudo.wheelsystems.com) (ttyv0) login: admin Password: Last login: Wed Jun 22 10:50:38 on ttyv0 \*\*\* FUDO configuration utility \*\*\* Logged into FUDO, S/N 12345678, firmware 2.1-23500. 1. Show status 2. Reset network settings 0. Exit Choose an option (0): 2 Are you sure you want to continue? [y/N] (n): y Choose new management interface (net1 net0): 📕

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

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

```
To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.
FUDO (fudo.wheelsystems.com) (ttyv0)
login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0
*** FUDO configuration utility ***
Logged into FUDO, S/N 12345678, firmware 2.1-23500.
1. Show status
2. Reset network settings
0. Exit
Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
```

8. Enter network gate and press *Enter*.

FUDO, S/N 12345678, firmware 2.1-23500. To reset FUDO to factory defaults, login as "reset". To fix admin account and change network settings, login as "admin" with an appropriate password. FUDO (fudo.wheelsystems.com) (ttyv0) login: admin Password: Last login: Wed Jun 22 10:56:52 on ttyv0 \*\*\* FUDO configuration utility \*\*\* Logged into FUDO, S/N 12345678, firmware 2.1-23500. 1. Show status 2. Reset network settings 0. Exit Choose an option (0): 2 Are you sure you want to continue? [y/N] (n): y Choose new management interface (net1 net0): net0 Enter new net0 address (10.0.150.150/16): 10.0.150.150/16 Enter new default gateway IP address (10.0.0.1):

#### Related topics:

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

## CHAPTER 4

Quick start

## 4.1 SSH

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



#### Prerequisites

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

#### Configuration



#### $Adding \ a \ server$

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

1. Select *Management* > *Servers*.

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

Parameter	Value
General	
Name	ssh_server
Blocked	×
Protocol	SSH
Description	×
Permissions	
Granted users	×
Destination host	
Address	10.0.150.150
Port	22

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

Destination host						
Address	10.0.150.150	Port	22	1		
Bind address	Any \$					
Server public key	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC6pbHklb/uemFNLcbQ49s Qss/gWM to 2 cond Marker Jacks Vanage Mearer Dawy 102/104/SVR BX/RDQ Download server's public SSH key Aveze WEH/UVast coAx1j21wasdenksyonmiczcDodyropocz11rcdWsxN//FG MQSHlxOkq6TSkmE8WGLISosk8tWwE898DwcAk6aD+5BThsTmrGq11 BGt0e/Q2M0zQFhkZGOgH55r7CEHWZDWI4YpAv+bU0UrbsqqID6dRLs KENtv2sb6Ppkm3700hxjH+p59K880Y9rNmh3lyJv4vCTPx4gF Destination server's fingerprint c9:b9:e8:14:b5:5e:d0:8f:c6:b5:02:96:e7:72:1c:6d:f0:cc:64:36 SHA1					

5. Click Save.

Adding a user

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

- 1. Select Management > Users.
- 2. Click + Add.
- 3. Provide essential user information:
| Parameter          | Value            |
|--------------------|------------------|
| General            |                  |
| Login              | john_smith       |
| Blocked            | X                |
| Account validity   | Indefinite       |
| Role               | user             |
| Preferred language | English          |
| Safes              | default settings |
| Full name          | John Smith       |
| Email              | john@smith.com   |
| Organization       | X                |
| Phone              | X                |
| AD Domain          | ×                |
| LDAP Base          | X                |
|                    |                  |
| Permissions        |                  |
| Granted users      | X                |
|                    |                  |
| Authentication     |                  |
| Туре               | Password         |
| Password           | john             |
| Repeat password    | john             |

#### Adding a listener

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

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

Parameter	Value
General	
Name	ssh_listener
Blocked	×
Protocol	SSH
Permissions	
Granted users	×
Connection	
Mode	proxy
Local address	10.0.150.151
Port	1022

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

Connection	
Mode	proxy \$
Fudo public key	Generate FUDO's private SSH key
	WI+d4nY Upload FUDO's private SSH key HWnmM gUF/Cb9 Upload FUDO's private SSH key MwsHOh 9SSh0ED9BGcwtowQg+Uo44X5t/1zPAAAFQDa1dZXglBamfYL6okb5 2Mckz]ReQAAAIEAgCTQH9PydSERsLwn0jxkwNro+jVcHJtvKsaj89Fjvrl
	FOWINMODY7NGQqGDDwoC/67L/MruL+0783ADnYSKgvaQlfdDdT5UN AACAIGGYskAACMHEetWsSNDYITaSKAxl H5Lm+B3086p9RJ+5BrkRLgbEhBHceD52
	8b:be:11:c4:e5:dc:96:96:a0:c4:c2:1f:a0:bf:aa:bf:9b:1e:cd:15 SHA1

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

5. Click Save.

#### Adding an account

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

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

Parameter	Value
General	
Name	admin_ssh_server
Account type	regular
Session recording	complete
OCR sessions	X
Delete session data after	61 days
Permissions	
Granted users	X
Server	
Server	ssh_server
Credentials	
Domain	X
login	root
Replace secret with	with password
Password	password
Repeat password	password
Password change policy	Static, without restrictions
Replace secret	4
Password changer	
Password changer	None
Privileged user	X
Privileged user password	X

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:

	N/ 1
Parameter	Value
General	
Name	ssh_safe
Notifications	×
Ask for login reason	×
Policies	×
Protocol functionality	
RDP	×
SSH	$\checkmark$
VNC	×
Objects relations	
Users	john_smith
Accounts	admin_ssh_server
Listeners	ssh_listener

# Establishing connection

At this point john\_smith can connect to the target host over the SSH protocol.

Example:

```
    Control Contro Control Control Control Control Control Control Control Control
```

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

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

#### Viewing user session

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

Management <	Fudo								🔺 ad	min ~ 🥐
Dashboard	Casalana	Active	⊜ Delete	OCR		▼ Add filter ~	Generate report	Search	0	Q.v
Sessions	Sessions									
📽 Users	User User	Protocol	Server	Account	Safe	Started at +	Finished at Dura	ation Activity St	20	
Servers	🗆 🕨 john_sn	nith SSH	ssh_server	admin_ssh_server	ssh_safe	2016-10-17 13:45		10	.0 KB 🔊 📎 I	<b>⊳</b> I)
R Accounts	John's ac	tive conne	ction wit	h test_server	ssh_safe	2016-10-17 13:18	2016-10-17 13:32 0:13	3:56 7% 10	.0 KB	2 2

#### **Related topics:**

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

# 4.2 RDP

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



# Prerequisites

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

# Configuration



# $Adding\ a\ server$

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

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

Parameter	Value
Name	rdp_server
Blocked	X
Protocol	RDP
Description	×
Permissions	
Granted users	X
Destination host	
Address	10.0.35.54
Port	3389
Bind address	10.0.150.151

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

Destination host	
Address	10.0.35.54 Port 3389
Bind address	Provide server's IP address and port number
Server certificate	BEGIN PUBLIC KEY MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANApps8+1WF1sEEE7v Var/CNulwboAtX f5ZW328Rab7CpVKI Fetch server's certificate VFUCAwEAAQ== END PUBLIC KEY
	c0:4c:1b:4c:a6:2a:c5:f3:31:6d:12:4e:14:ba:0a:0a:0d:58:38:00 SHA1

5. Click Save.

#### $Adding \ a \ user$

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

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

Parameter	Value
Login	john_smith
Blocked	X
Account validity	Indefinite
Role	user
Preferred language	English
Safes	default settings
Full name	John Smith
Email	john@smith.com
Organization	X
Phone	X
AD Domain	×
LDAP Base	×
Permissions	
Granted users	×
Authentication	
Type	Password
Password	john
Repeat password	john

#### 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	X
Permissions	
Granted users	×
Connection	
Mode	proxy
Local address	10.0.150.151
Port	3389

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

Connection		_
Mode	proxy \$	;
Local address	10.0.150.151 ¢ Port 3389	
Server public key	Generate Fudo's private key MFwitch rotocontected and swawsaddar AWt26rXtk by BKA dA16XJeT1fng fL2W2COJSDHEX Upload Fudo's private key CAWEAAQ== END PUBLIC KEY	*
	FUDO's fingerprint d5:d2:b3:d3:9f:57:59:14:24:20:f4:07:43:29:0a:e4:68:33:ab:e6 SHA1	

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

5. Click Save.

# $Adding \ an \ account$

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

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

Parameter	Value
General	
Name	admin_rdp_server
Blocked	×
Type	regular
Session recording	all
OCR sessions	4
OCR Language	English
Delete session data after	61 days
Permissions	
Granted users	X
Server	
Server	rdp_server
Credentials	
Domain	×
Login	administrator
Replace secret with	with password
Password	password
Repeat password	password
Password change policy	Static, without restrictions
Password changer	
Password changer	None
Privileged user	X
Privileged user password	X

# $Defining \ a \ safe$

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

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

Parameter	Value
General	
Name	rdp_safe
Blocked	×
Login reason	×
Notifications	×
Policies	×
Protocol functionality	
RDP	$\checkmark$
SSH	×
VNC	×
Objects relations	
Users	john_smith
Accounts	admin_rdp_server
Listeners	rdp_listener

# 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 Rei	mote Desktops - 10.0.150.151
General Session F	ledirection
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.

	10.0.150.151
Login Password	Log in

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



# Viewing user session

1. Open a web browser and go to the 10.0.150.151 web address.

- 2. Enter the login and password to login to the Wheel Fudo PAM administration panel.
- 3. Select Management > Sessions.
- 4. Click Active.
- 5. Find John Smith's session and click the playback icon.

Management <		Fudo										<b>≜</b> ad	min ~ 🤶 ?
		Gassiana	al Active	≙ Delete	I OCR		▼ Add fil	ter v 🔒 Generate	report	Search		0	Q.V
Sessions	Ľ	Sessions											
		User	Protocol	Server	Account	Safe	Started at *	Finished at	Duration	Activity	Size		
		🗆 🕨 john_sm	ith RDP	rdp_server	admin_rdp_server	rdp_safe	2016-10-17 14:30				1.1 MB		ः ः न्व
E Accounte		John's act	ive connect	ion with t	est server	ssh_safe	2016-10-17 13:45				10.0 KB		
	•				server	ssh_safe	2016-10-17 13:18	2016-10-17 13:32	0:13:56	7%	10.0 KB	10.0	5 U A
Safes													

#### **Related topics:**

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

# 4.3 Telnet

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

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



# Prerequisites

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

#### Configuration



#### Adding a server

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

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

Parameter	Value
General	
Name	telnet_server
Blocked	×
Protocol	Telnet
Enable SSLv2 support	X
Enable SSLv3 support	×
Description	×
Permissions	
Granted users	×
Destination host	
Address	10.0.35.137
Port	23

4. Click Save.

#### Adding a user

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

1. Select Management > Users.

2. Click + Add.

3. Provide essential user information:

Parameter	Value
Login	john_smith
Blocked	×
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	X
Phone	<u>×</u>
AD Domain	X
LDAP Base	X
Permissions	
Granted users	×
Connections	
Connections	×
Authentication	
Туре	Password
Password	john
Repeat password	john

#### Adding a listener

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

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

Parameter	Value
General	
Name	telnet_listener
Blocked	×
Protocol	Telnet
Enable SSLv2 support	×
Enable SSLv3 support	×
Permissions	
Granted users	×
Connection	
Mode	proxy
Local address	10.0.150.151
Port	23

# Adding an account

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

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

Parameter	Value
General	
Name	admin_telnet_server
Blocked	×
Type	forward
Session recording	all
OCR sessions	×
Delete session data after	61 days
Permissions	
Granted users	X
Server	
Server	telnet_server
Credentials	
Replace secret with	with password
Password	X
Repeat password	×

#### 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	X
Login reason	×
Notifications	X
Policies	×
Protocol functionality	
RDP	×
SSH	×
VNC	×
Permissions	
Granted users	×
Objects relations	
Users	john_smith
Accounts	admin_telnet_server
Listeners	telnet_listener

#### Establishing a telnet connection with the remote host

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

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

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

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

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

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

Note: Telnet connections do not support user credentials substitution.

#### Viewing user's session

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

Management <	Fudo							📥 adn	nin ~ 🤶
🖬 Dashboard	Consigna	Active 🔒 Delete	I OCR		T Add filter ∨	Generate report	Search	0	a.~
Sessions	Sessions								-
쑬 Users	User	Protocol Server	Account	Safe	Started at +	Finished at Duration	n Activity Size		_
Servers	john_smiti	h Teinet teinet_server	admin_telnet_server	telnet_safe	e 2016-10-18 00:	47	10.0 KB		· · · )
Accounts	John's activ	ve connection							

#### **Related topics:**

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

# 4.4 Telnet 5250

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

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



#### Prerequisites

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

#### Configuration

8	1   server	•	2   account		3   safe	4	4   user	۳	5   listener
---	------------	---	-------------	--	----------	---	----------	---	--------------

#### Adding a server

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

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

Parameter	Value
General	
Name	telnet_server
Blocked	×
Protocol	Telnet 5250
Enable SSLv2 support	X
Enable SSLv3 support	×
Description	X
Permissions	
Granted users	×
Destination host	
Address	10.0.35.137
Port	23

4. Click Save.

#### Adding a user

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

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

Parameter	Value
Login	john_smith
Blocked	×
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	X
Phone	<u>×</u>
AD Domain	X
LDAP Base	X
Permissions	
Granted users	×
Connections	
Connections	×
Authentication	
Туре	Password
Password	john
Repeat password	john

#### Adding a listener

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

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

Parameter	Value
General	
Name	telnet_listener
Blocked	×
Protocol	Telnet
Enable SSLv2 support	×
Enable SSLv3 support	×
Permissions	
Granted users	×
Connection	
Mode	proxy
Local address	10.0.150.151
Port	23

#### Adding an account

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

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

Parameter	Value
General	
Name	admin_telnet_server
Blocked	×
Type	forward
Session recording	all
OCR sessions	×
Delete session data after	61 days
Permissions	
Granted users	X
Server	
Server	telnet_server
Credentials	
Replace secret with	with password
Password	X
Repeat password	×

#### 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	X
Login reason	×
Notifications	X
Policies	×
Protocol functionality	
RDP	×
SSH	×
VNC	×
Permissions	
Granted users	×
Objects relations	
Users	john_smith
Accounts	admin_telnet_server
Listeners	telnet_listener

#### Establishing a telnet connection with the remote host

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

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

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

<b>9</b> ]	Session A - [24 x 80]
File Edit View Communication Actions Window	Help
🖻 🖻 📾 🛤 🖬 🖬 🔤 💩	
FUDO Authentication.	
Vsername:	
rassword.	
M <u>A</u> A	

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



Note: Telnet connections do not support user credentials substitution.

D         Session A - [24 x 80]
File Edit View Communication Actions Window Help
MAIN IBM i Main Menu Sustem:
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 1 Access tasks
90. Sign off
Selection or command
===>
F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Information Assis
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2015.
M <sup>A</sup>

# Viewing user's session

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

					IBM :	i Main Menu			
							System: POB40	10	
			Se == F3 F2 (0	<pre>1. User tasks 2. Office tasks 3. General syst 4. Files, librs 5. Programming 6. Communication 7. Define or ch 8. Problem hand 9. Display a me 10. Information 11. IBM i Access 90. Sign off lection or command =&gt; =Exit F4=Prompt 3=Set initial menu ) COPYRIGHT IBM CC</pre>	s tem tasks aries, and folde: ons hange the system dling enu Assistant option s tasks d F9=Retrieve DRP. 1980, 2015.	rs ns F12=Cancel			
Ш	» »»	127 M	0:00:22					0:00:22	<ul><li>Info</li></ul>
U Te	rminate	🕞 Join	Pause						

#### **Related topics:**

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

# 4.5 MySQL

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

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



#### Prerequisites

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

#### Configuration



#### Adding a server

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

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

Parameter	Value
General	
Name	mysql_server
Blocked	×
Protocol	MySQL
Description	X
Permissions	
Granted users	×
Destination host	
Address	10.0.1.35
Port	3306
Bind address	Any

4. Click Save.

#### Adding a user

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

1. Select Management > Users.

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

Parameter	Value
Login	john_smith
Blocked	×
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	×
Phone	×
AD Domain	×
LDAP Base	×
Permissions	
Granted users	×
Connections	
Connections	×
Authentication	
Туре	Password
Password	john
Repeat password	john

#### 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	X
Connection	
Mode	proxy
Local address	10.0.150.151
Port	3306

#### 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	X
Туре	regular
Session recording	all
OCR sessions	×
Delete session data after	61 days
Permissions	
Granted users	X
Server	
Server	mysql_server
Credentials	
Domain	×
Login	root
Replace secret with	with password
Password	password
Repeat password	password
Password change policy	Static, without restrictions
Password changer	
Password changer	None
Privileged user	X
Privileged user password	X

# Defining a safe

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

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

Parameter	Value
General	
Name	mysql_safe
Blocked	×
Login reason	×
Notifications	×
Policies	×
Protocol functionality	
RDP	×
SSH	X
VNC	×
Objects relations	
Users	john_smith
Accounts	admin_mysql_server
Listeners	mysql_listener

#### Establishing connection with a MySQL database

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



4. Continue browsing the database contents using SQL queries.

#### Viewing user session

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

Management	<	۴ı	Jao.									
Dashboard		Sec	sions	I Active		G OCR		▼ Add filter ~	Generate repo	ort i	Search	
Sessions		565	sions									
볼 Users			User	Protocol	Server	Account	Safe	Started at *	Finished at	Duration	Activity	Size
🖴 Servers			john_smith	MySQL	mysql_server	admin_mysql_server	mysql_safe	2016-10-18 10:5	6			2.0
Accounts		Joh	n's active	e conne	ction							
					Coo	-ion 04020052041	11117060					
A https://10.0.150.151/	sessions/8	848388	3532111	147069/	ses: i=1&qi=on8?	sion 84838853211 &qc=on&live=2016	6-10-18+1	0%3A58%3A2	6&qo=on			

# Session: 848388532111147069, user: john\_smith, server: mysql\_serve

INIT	2016-10-1
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_CONNEC CLIENT_MULTI_RESULTS, CLIENT_CONNECT_ATTRS, CLIENT_NO_SCHEMA, CLIENT_TRANSACTIONS, CLIENT_IGNORE_SIGPIPE, CLIE CLIENT_CONNECT_WITH_DB, CLIENT_FOUND_ROWS, CLIENT_PLUGIN_AUTH_LENENC_CLIENT_DATA, CLIENT_LOCAL_FILES, CLIENT CLIENT_MULTI_STATEMENTS, CLIENT_LONG_PASSWORD, CLIENT_ODBC, CLIENT_PS_MULTI_RESULTS, CLIENT_PROTOCOL_41	TION, NT_LONG_ _COMPRE
ок	2016-10-1
Affected rows: 0 Last inserted_id rows: 0 Status: 2 Warnings: 0 Info:	
COM_QUERY	2016-10-1
Query:	

select @@version\_comment limit 1

00:04:02

#### **Related topics:**

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

00:00:00

- Quick start HTTP connection configuration
- Quick start Telnet connection configuration
- Requirements
- Data model
- Configuration

# 4.6 HTTP

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



#### Prerequisites

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

#### Configuration



#### $Adding \ a \ server$

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

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

	N / 1
Parameter	Value
Genera	
Name	http_server
Blocked	×
Protocol	HTTP
HTTP timeout	900
Enable SSLv2 support	×
Enable SSLv3 support	×
Description	X
Permissions	
Granted users	X
Destination host	
Address	www.wheelsystems.com
Port	80
HTTP host	×

# Adding a user

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

- 1. Select Management > Users.
- 2. Click + Add.
- 3. Provide essential user information:
| Parameter          | Value          |
|--------------------|----------------|
| Login              | john_smith     |
| Blocked            | X              |
| Account validity   | Indefinite     |
| Role               | user           |
| Preferred language | English        |
| Full name          | John Smith     |
| Email              | john@smith.com |
| Organization       | X              |
| Phone              | ×              |
| AD Domain          | X              |
| LDAP Base          | ×              |
| Permissions        |                |
| Granted users      | ×              |
| Connections        |                |
| Connections        | ×              |
| Authentication     |                |
| Туре               | Password       |
| Password           | john           |
| Repeat password    | john           |

#### Adding a listener

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

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

Parameter	Value
General	
Name	http_listener
Blocked	×
Protocol	HTTP
Enable SSLv2 support	×
Enable SSLv3 support	×
Permissions	
Granted users	X
Connection	
Mode	proxy
Local address	10.0.150.151
Port	8080
Use TLS	X

## Adding an account

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

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

Parameter	Value
General	
Name	admin_http_server
Blocked	×
Type	forward
Session recording	all
OCR sessions	×
Delete session data after	61 days
Permissions	
Granted users	×
Server	
Server	http_server
Credentials	
Replace secret with	with password
Password	X
Repeat password	×

#### Defining a safe

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

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

Parameter	Value
General	
Name	http_safe
Blocked	X
Login reason	×
Notifications	×
Policies	×
Protocol functionality	
RDP	×
SSH	×
VNC	×
Objects relations	
Users	john_smith
Accounts	admin_http_server
Listeners	http_listener

#### Connecting to remote resource

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

۴ı	JCC
	Authentication
Lo	sgin
Pa	assword
	Login

4. Continue browsing the website.

Viewing user session

- 1. Open a web browser and go to the Wheel Fudo PAM administration page.
- 2. Enter user login and password to log in to Wheel Fudo PAM administration panel.
- 3. Select Management > Sessions.
- 4. Click Active.

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

Management	<	Fudo							🕹 adm	in ~  ?
🖬 Dashboard		Sessions *	d Active	🖹 Delete	OCR	▼ Add filter ~	🔒 Generate report	Search	0	q.~
Sessions										
曾 Users		User User	Server	Protocol	Connection	Started at - Finis	hed at Duration Activ	rity Size		_
		□ ► john_smith	http_www	HTTP	http-test	2015-07-03 08:14	0%	118.2 KB		-al
		John's active	connecti	ion —						
Policies										
				Consist	402005204	11147070				

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

## Session: 848388532111147070, User: john\_smith

V=4050			11.10.04.122011	
/webman/resources/images/icon_dsm_48.png? GET v=4398	image/png	1.6 KB	2016-10-18 11:18:54.158837	http://10.0.150.151:8080/
/webman/resources/images/icon_dsm_64.png? GET v=4398	image/png	1.7 KB	2016-10-18 11:18:54.204921	http://10.0.150.151:8080/
/webman/resources/images/icon_dsm_96.png? GET v=4398	image/png	2.1 KB	2016-10-18 11:18:54.240588	http://10.0.150.151:8080/
/scripts/ext- GET 3/ux/images/default/1x/Components/checkbox v=0846062016020243	image/png	2.1 KB	2016-10-18 11:18:55.159765	http://10.0.150.151:8080/scripts/ext-3/ux/ux-all.css? v=1470092212
/webman/resources/images/default/1x/login/ch GET v=5934	image/png	1.9 KB	2016-10-18 11:18:55.174328	http://10.0.150.151:8080/webman/resources/css/desktop.css? v=1471385610
/webman/resources/images/default/1x/login/sp GET sd716acf281.png	image/png	1.8 KB	2016-10-18 11:18:55.472084	http://10.0.150.151:8080/webman/resources/css/desktop.css? v=1471385610
/webman/3rdparty/VideoStation/font/Roboto- GET Bold.ttf	application/octet-stream	132.6 KB	2016-10-18 11:18:55.481876	http://10.0.150.151:8080/webman/3rdparty/VideoStation/style.css? v=1468242934
/webman/3rdparty/VideoStation/font/Roboto- GET Regular.ttf	application/octet-stream	141.9 KB	2016-10-18 11:18:55.491117	http://10.0.150.151:8080/webman/3rdparty/VideoStation/style.css? v=1468242934
/webman/resources/images/default/1x/login/log GET v=08560520161740167	image/png	4.4 KB	2016-10-18 11:18:55.540508	http://10.0.150.151:8080/webman/resources/css/desktop.css? v=1471385610
/webman/resources/images/default/1x/login/log GET v=08560520161740167	image/png	2.0 KB	2016-10-18 11:18:55.557389	http://10.0.150.151:8080/webman/resources/css/desktop.css? v=1471385610
/webman/resources/images/default/1x/login/log GET v=08560520161740167	image/png	1.4 KB	2016-10-18 11:18:55.677498	http://10.0.150.151:8080/webman/resources/css/desktop.css? v=1471385610
/webman/resources/images/default/1x/login/log GET v=08560520161740167	image/png	1.3 KB	2016-10-18 11:18:55.691060	http://10.0.150.151:8080/webman/resources/css/desktop.css? v=1471385610
/webman/resources/images/default/1x/default_ GET v=1476386269	image/jpeg	295.5 KB	2016-10-18 11:18:55.870018	http://10.0.150.151:8080/

### **Related topics:**

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

ර Terminate

# 4.7 Citrix

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

# 4.7.1 ICA

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



## 4.7.1.1 Prerequisites

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

### 4.7.1.2 Configuration

<mark>-</mark> 1	server		2   account	•	3   safe	-	4   user	۳	5   listener
------------------	--------	--	-------------	---	----------	---	----------	---	--------------

#### Adding a server

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

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

Devenue la c	
Parameter	value
General	
Name	ica_server
Blocked	X
Protocol	ICA
Description	×
Permissions	
Granted users	×
Destination host	
Address	10.0.21
Port	1494
Use TLS	×

# Adding a listener

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

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

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

# Adding an account

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

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

Parameter	Value
General	
Name	admin_ica_server
Blocked	×
Type	regular
Session recording	all
OCR sessions	×
Delete session data after	61 days
Permissions	
Granted users	X
Server	
Server	ica_server
Credentials	<u> </u>
Domain	X
Login	citrixuser
Replace secret with	password
Password	password
Repeat password	password
Password change policy	Static, without restrictions
Password changer	
Password changer	none
Privileged user	X
Privileged user password	X

# Adding a user

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

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

Parameter	Value
Login	john_smith
Blocked	×
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	X
Phone	X
AD Domain	X
LDAP Base	X
Permissions	
Granted users	×
Connections	
Connections	×
Authentication	
Туре	Password
Password	john
Repeat password	john

# Defining a safe

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

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

Parameter	Value
General	
Name	ica_safe
Blocked	×
Login reason	×
Notifications	X
Policies	×
Protocol functionality	
RDP	×
SSH	X
VNC	×
Objects relations	
Users	john_smith
Accounts	admin_ica_server
Listeners	ica_listener

#### 4.7.1.3 Creating .ica file with connection parameters

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

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

1. Create configuration file containing the following:

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

2. Save the file with .ica extension.

#### 4.7.1.4 Connecting to remote resource

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

#### 4.7.1.5 Viewing user session

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

#### **Related topics:**

- Data model
- Creating an ICA server
- Creating an ICA listener
- $\bullet \ ICA$

# 4.7.2 ICA via Citrix StoreFront

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



## 4.7.2.1 Prerequisites

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

# 4.7.2.2 Configuration

	-		-					
🔒 1   server		2   account	•	3   safe	4	4   user	۳	5   listener

#### Adding an ICA server

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

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

#### 3. Provide essential configuration parameters:

Parameter	Value
General	
Name	ica_server
Blocked	×
Protocol	ICA
Description	X
Permissions	
Granted users	×
Destination host	
Address	10.0.21
Port	1494
Use TLS	X

4. Click Save.

#### Adding an ICA listener

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

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

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

4. Click Save.

#### Adding an account for the ICA server

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

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

Parameter	Value
General	
Name	ICA_forward
Blocked	×
Type	forward
Session recording	all
OCR sessions	×
Delete session data after	61 days
Permissions	
Granted users	X
Server	
Server	ica_server
Credentials	
Replace secret with	X
Forward domain	×

# Adding a Citrix StoreFront server

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

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

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

# Adding a Citrix StoreFront listener

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

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

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

# Adding an account for the Citrix StoreFront server

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

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

Parameter	Value
General	
Name	citrixuser_at_SF
Blocked	X
Туре	regular
Session recording	all
OCR sessions	×
Delete session data after	61 days
Permissions	
Granted users	×
Server	
Server	citrix_storefront
Credentials	
Domain	tech.whl
Login	citrixuser
Replace secret with	password
Password	password
Repeat password	password
Password change policy	Static, without restrictions
Password changer	
Password changer	none
Privileged user	X
Privileged user password	X

# Adding a user

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

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

Parameter	Value
Login	john_smith
Blocked	X
Account validity	Indefinite
Role	user
Preferred language	English
Full name	John Smith
Email	john@smith.com
Organization	X
Phone	×
AD Domain	X
LDAP Base	×
Permissions	
Granted users	×
Connections	
Connections	×
Authentication	
Туре	Password
Password	john
Repeat password	john

# Defining a safe

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

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

Parameter	Value
General	
Name	ica_safe
Blocked	×
Login reason	×
Notifications	×
Policies	×
Protocol functionality	
RDP	×
SSH	×
VNC	×
Objects relations	
Users	john_smith
Accounts	citrixuser_at_SF, ICA_forward
Listeners	ica_listener, citrix_storefront_listener

## 4.7.2.3 Connecting to remote resource

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

F٦			
	A Login Password	uthentication	
		Login	

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



#### 4.7.2.4 Viewing user session

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

M	anagement		F	udo"									
Gul	Dashboard												
			Se	ssions	Delete	CCR	C Timestamp	Generate report			T A	dd filter ~	Searc
	Sessions												
-			0	User	Protocol		Server	Account	Safe	Started at +	Finished at	Duratio	n Activity
A	Servers		●►	► admin	Citrix StoreF	Front (HTTP)	SF	citrixuser at SF	Citrix	2017-02-16 15:12			0%
		1	Lake				ICA	forward@ICA	Citrix	2017-02-16 14:56	2017-02-16 14	1:57 0:00:32	2 0%
		1	Jon	n's active	connect	ion	ICA	forward@ICA	Citrix	2017-02-16 14:54	2017-02-16 14	:55 0:00:42	2 0%
2			⊳►	<ul> <li>admin</li> </ul>	ICA		ICA	citrixuserICA	Citrix-BASTION	2017-02-16 14:49	2017-02-16 14	4:49 0:00:11	100%
	Safes		⊳►	<ul> <li>admin</li> </ul>	ICA		ICA	citrixuserICA	Citrix-BASTION	2017-02-16 14:49	2017-02-16 14	49 0:00:14	100%
				admin	ICA		ICA	forward@ICA	Citrix	2017-02-16 14:48	2017-02-16 14	48 0:00:26	5 100%

# **Related topics:**

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

# 4.8 Setting up password changing on a Unix system

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

#### Configuration

Adding a password change policy

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

Ma	anagement		Ful Define new p	bassword change		
M	Dashboard		Password policies	Custom changers	+ Add 🔒 Delete	Search
₿		г.	r asserter a poneteo	oustonn ondingero		
쓭	Users		Name +		Change frequency	
8			20 minut		20	
_			<ul> <li>Custom password policy</li> </ul>	y	1	
	Accounts		Static, without restriction	ns	None	
•						
2	Listen Manage password	chan	gers			
•	Password changers					

3. Provide password change policy name.

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

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

Management <	Fudo	
I Dashboard	Policy	
E Sessions	1 only	
별 Users	General	Provide descriptive name
⊖ Servers	Name	10 minutes, 20 chars, iowercase, digits
Accounts	Enable password change	1
Cofee	Password change enabled	0 10
Jaios	Password verification enabled	Concerning the password will be changed
か Listeners		Enable password verification

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

+ Password changers	Password requirements
Policies	Define password length
🛓 Downloads	Length 20
⊖ Reports	Small letters 15
Productivity	Enable enforcing selected requirement Provide the minimum number of characters
Settings	Special characters
😂 System	Digits 🛛 5
Ø <sup>e</sup> Network configuration	

8. Click Save to store password changer policy.

Assigning password changer to the privileged account

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

м	lanagement <	Fudo									
	i Dashboard	Accounts	+ Add	© Bloc	k © Unbloci	c 🕆 Delete			<b>T</b> Add filter ∨	Searc	h
E	Sessions										
1	Users	🗆 Name +			Server +	Recording *	Туре	Password change polic	сy		Password
0	Serve Manage accounts	<ul> <li>http-account</li> </ul>			10.0.235.254	all	regular	Static, without restric	tions		None
G		http-anonym	ous		10.0.235.254	all	anonymous	None			None
C	Accounts	linux1-nginx-	account		inux1-nginx	all	forward	None			None
	Safes	Iinux1-ssh-us	ser1	1	inux1-ssh	all	regular	Static, without restric	tions		None
	Listeners	Iinux1-ssh-us	ser2	1	inux1-ssh	all	regular	Static, without restric	tions		Unix Acc
		linux1-telnet-	-user1	1	inux1-telnet	all	regular	Static, without restric	tions		None
- ń-	Password changers	<ul> <li>mysql-root</li> </ul>			mysql	all	regular	Static, without restric	tions		None
U	Policies	rdp-forward	Edit acc	ount	win2008r2	all	forward	None			None
1. Deverteeste		root-BSD			BSD	all	regular	10 minutes, 20 chars	, lowercase, digits		Unix Acc
-	Downloads	<ul> <li>terminalserve</li> </ul>	er-anonymous	1	terminalserver	all	anonymous	None			None

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

a, External authentication	Credentials	
III External passwords repositories	Domain	
Resources		Provide privileged account login
Backups and retention	Select password substitution	user
🖧 Cluster	Replace secret with	with password
LDAP synchronization	Provide password Password	[
≡ Events log	Repeat password	(
	Password change policy	10 minutes, 20 chars, lowercase, digits
© 0:10:09.5568404 12945678 ♥ pam-29484Not configured		Select password change policy

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

Password changer	Select password changer specific to the target operating
Provide superuser account login Privileged user	Unix Account over SSH root
Privileged user password	Provide superuser account password

Note: Superuser account enables resetting the password in case the Secret manager detects

that it has been changed by someone else.

9. Click Save.

# Related topics:

- Requirements
- Data model
- Configuration

# CHAPTER 5

Users

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

Allow selected users	s to access servers	)	_			
Block selected users				Delete selec	cted users	
Management Define new	user do			Filter users	list	
In Dashboard	Hann + Add	Block	Unblock	Delete	T Add	filter Search
E Sessions	Users O					
볼 Users	🗇 Login 🔺	Role	Organization	Email	Full name	Authentication method
⊖ Servers	admin	superadmin				Password
	admin1	admin				Password
Accounts	o an <mark>onyme</mark> Editusen	definition				
Safes	api-robot-operator1	operator				Password
3 Listeners	api-robot-operator2	operator				Password
A LISICITOS	api-robot-superadmin1	superadmin				
<ul> <li>Password changers</li> </ul>	api-robot-user1	user				
V Policies	api-robot-user2	user				Blocked u
	( jdoe	user			Joe Doe	External authentication
Downloads	<ul> <li>kwitaszczyk</li> </ul>	user			Konrad Wite Reaso	on the user has bee
🖶 Reports	<ul> <li>mborysiak</li> </ul>	user			Michal Boryslax	External authentication
■ Productivity	<ul> <li>mzaborski</li> </ul>	superadmin	Wheel Systems	m.zaborski@wheelsystems.com	Mariusz Zaborski	External authentication
	pdawidek	user	Wheel Systems	p.dawidek@wheelsystems.com	Paweł Jakub Dawidek	External authentication

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

# 5.1 Creating a user

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

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

M	anagement	Create new	user 🗖							
	Dashboard		Users +	Add O Block	O Unblock	≘ Delete		T Ad	d filter ~	Search
₿			Users C							
쓭	Users		🗋 Login 🔺	Role	Organization	Email	Full name	Authentication	n method	Last
	Servers		admin	superadmin	WHL_LAB		lmię Nazwisko	Password		12 r
			admin0	admin		email@email.	.aa	Password		3 m
		0	administrator	admin				Password		new
•	Safes		andrzej	user				Password		2 ye

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

Management <	Fudo	were been down a last ad a birst	🛓 admin 🗸 🤗
Jashboard	User Copy user	user based on selected object	
E Sessions			
📽 Users	General		
🕀 Servers	ID	848388532111147009	
Accounts	Synchronize with LDAP	0	
Safes	Login	admin	*
ふ Listeners			
+ Password changers	Account validity	Indefinite	•

3. Enter a unique user login.

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

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

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

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

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

- 8. Grant access to safes.
- 9. Define time access policy.

• Click desired safe object.

Preferred language	English	ŧ	*
	Click to define access time policy to the safe		
Safes	RDP SSH portal O	Q	
Full name			
Email			

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

Access time policy	×
Enable time policy	Click to enable time policy for the given safe
00:00	Allow user to see passwords 23:59
Monday	
Tuesday	
Wednesday	
Thursday	Click to define access time interval
Friday	Cherk to denne access time interval
Saturday	
Sunday	
	Cancel

- Click OK.
- 10. Enter user's full name.
- 11. Enter user's email address.
- 12. Enter user's organizational unit.
- 13. Enter user's phone number.
- 14. Provide user's Active Directory domain.
- 15. Enter *LDAP* service *BaseDN* parameter.

# Note:

• LDAP base is necessary for authenticating the user using the Active Directory service.

- E.g. for example.com domain, the LDAP base parameter value should be dc=example, dc=com.
- 16. In the *Permissions* section, select users allowed to manage this user object.
- 17. In the Authentication section, select authentication type.

## External authentication

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

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

## Password

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

#### $SSH \ key$

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

One-time password

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

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

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

19. Click Save.



# **Related topics:**

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

# 5.2 Editing a user

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

Manageme	nt <	Fuda	<b>.</b>							
Dashboa		Hears	+ Add	Block	O Unblock	Delete			▼ Add filter ~	Search
E Session		Users								
😁 Users		🗌 Login 🔺	Role	0	Organization	Email	Full name	Auth	entication method	Last
A Servers		admin	super	radmin V	VHL_LAB		lmię Nazwisko	Pas	sword	12 п
		admin0	admir	n		email@em	ail.aa	Pas	sword	3 m
Account		<ul> <li>adminis</li> </ul>	Edit user	definiti	on			Pas	sword	neve
Safes		<ul> <li>andrzej</li> </ul>	user					Pas	sword	2 ye

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

3. Modify configuration values as needed.

#### Note:

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

Ma	anagement <	Fudo		💄 admin ~	?
.11	Dashboard	Lleor Copy user			
⊞	Sessions	User			
썉	Users	General			
a	Servers	ID	848388532111147082	1	
Ø	Accounts				
	Safes	Synchronize with LDAP			
٣	Listeners	Login	john_smith	*	

• Unsaved changes are marked with an icon.

General	Unsaved	changes
Login	john_smith	
Blocked		
Account validity	Indefinite	\$
Role	operator	\$

4. Click Save.

#### **Related topics:**

• Users synchronization

- Data model
- System initiation
- Servers
- Accounts

# 5.3 Blocking a user

Warning: Blocking a user will terminate its current connections.

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

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

3. Click *Block*.

Management <	Fudo			🛔 admin ~	?
	+ Add O Block © Unblock @ Delete		T Add filter ∼	Search O	Q
	Users				_
😁 Users	Logh Select objects Organization Email	Full name	Authentication method	Last login	
	admin Block selected objects email@er	Imię Nazwisko nail.aa	Password Password	12 minutes ago 3 months ago	
	administrator admin		Password	never	
	andrzej user		Password	2 years, 5 months ago	

4. Optionally, provide blocking reason and click Confirm.

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



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

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

#### **Related topics:**

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

# 5.4 Unblcoking a user

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

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

#### 3. Click Unblock.

Management	< Fudo		🛓 admin 🐇 🤶 🤶
	Liesre + Add   Block  Unblock  Delete	▼ Add filter ~	Search O Q
	Users		
😁 Users	Login Solact objects Organization Email Full name	Authentication method	Last login
	admin Select objects WHL LAB Imię Nazwisko	Password	11 minutes ago
	admin0 adm Activate selected objects agemail.aa	Password	3 months ago 🛛 🗭
	administrator admin	Password	never
	andrzej user	Password	2 years, 5 months ago
	anonymous user		2 years, 2 months ago

#### 4. Click *Confirm* to unblock selected objects.



#### **Related topics:**

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

# 5.5 Deleting a user

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

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

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

3. Click Delete.

Management	¢	Fudo <sup>*</sup>			
Dashboard		+ Add O Block O Unblock	☐ Delete	T Add filter ~ Sea	irch
E Sessions		Users			
🖶 Users		C Login Select objects	Email Full name	Authentication method L	.ast
⊖ Servers		eadmin Delete selected objects	Imię Nazwisko email@email.aa	Password 1 Password 3	2 n
Accounts		administrator admin		Password n	iew
Safes		andrzej user		Password 2	ye

4. Confirm deleting selected objects.

Delete objects	×
Are you sure you want to delete 1 object?	
	Cancel Confirm
Confirm deleting selected objects	

### **Related topics:**

- Users synchronization
- Data model
- System initiation
- Servers
- Accounts
# 5.6 Roles

Role	Access rights
user	<ul> <li>Connecting to servers through assigned safes.</li> <li>Loggin to the User Portal (requires adding the user to the portal safe)</li> <li>Fetching servers' passwords (requires additional access right).</li> </ul>

service	Accessing SNMP information.
operator	<ul> <li>Logging in to the administration panel.</li> <li>Browsing objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions.</li> <li>Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions.</li> <li>Generating reports on demand and subscribing to periodic reports.</li> <li>Activating/deactivating email notifications.</li> <li>Viewing live and archived sessions involving objects (user, safe, account, listener, server), to which the user has been assigned sufficient access permissions.</li> <li>Converting sessions and downloading converted content involving objects (user, safe, account, listener, server), to which the user has been assigned sufficient access permissions.</li> </ul>
admin	<ul> <li>Logging in to the administration panel.</li> <li>Managing objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions.</li> <li>Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions.</li> <li>Generating reports on demand and subscribing to periodic reports.</li> <li>Activating/deactivating email notifications.</li> <li>Viewing live and archived sessions involving objects (user, safe, account, listener, server), to which the user has been assigned management privileges.</li> <li>Converting sessions and downloading converted content involving objects (user, safe, account, listener, server), to which the user has been assigned sufficient access permissions.</li> <li>Managing policies.</li> </ul>
superadmin	<ul><li>Full access rights to objects management.</li><li>Full access rights to system configuration options.</li></ul>

### Related topics:

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

# 5.7 Users synchronization

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

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

**Note:** Users imported from the catalog service cannot be edited. To edit a user definition imported from an LDAP or an AD server, disable the Synchronize with LDAP option for the given user.

Management <	FUDD <sup>®</sup> Administration panel
M Dashboard	Harr
Sessions	User
볼 Users	General Disable synchronization to edit user information
+ Connections	Synchronize with LDAP
⊖ Servers	Login def
V Policies	Blocked 🖂
🛓 Downloads	Account validity Indefinite +
🕀 Reports	
Settings	Role User \$

#### Configuring users synchronization service

To enable users synchronization feature, proceed as follows.

- 1. Select Settings > LDAP synchronization.
- 2. Select Enabled.
- 3. Select the data source type from the *Server type* drop-down list.
- 4. Provide the user authentication information to access user data on given server.
- 5. Enter domain name, to which imported users definition belong to.

6. Provide base DN for directory tree (eg. DC=devel,DC=whl).

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

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

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

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

HTTPS certificate	Fields mapping	^
Resources	rious mapping	
† Linarada	Login	sAMAccountName
Backuns and retention	Email	mail
Luster	Group assignment	memberof
	Phone	telephoneNumber
	Organization	company
() 1-19-41.816281 i 12245678	Full name	displayName
♦ 1-15988	Distinguished name	distinguishedName
	GUID	objectGUID
	External authenticat	ion Define user information mapping for nonstandard attributes names
	External authentication source	Active Directory 10.0.40.100:389 domain:tech.whl
	Group mappings	
		+
		C Reset Save

- 13. Select external authentication services which will be automatically assigned to user definitions imported from the directory service.
- 14. Assign safes to user groups.
- 15. Assign external authentication sources to user groups.

**Note:** External authentication sources are assigned to users in the exact sequence they are defined in groups mapping. Thus if the same user is present in more than one group, Wheel

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

For example:

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

### Group mappings

Mapping 🕝	Group B	∢	Connectior	RDP	\$	Q* ~	×
				CE	RB		
				🗹 Rad	dius		
				□ AD			
Mapping 🕜	Group A	⇒	Connection	SSH	<b>‡</b>	a, ~	×
	+				RB		
	•				dius		
				🖸 AD			

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

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

16. 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.

Management <	Fudo <sup>*</sup>		🕹 admin 🗸 💡
M Dashboard	I DAP synchronization		
E Sessions	EDAF Synonionization		
쓸 Users	Enabled	0	
⊖ Servers	Directory service		
Accounts	Server type	Active Directory	•
Safes	Username	administrator	
ラ Listeners	Password		
n Password changers	D-main management		
Policies	Domain name	tech.whi	
📩 Downloads	Base	dc=tech,dc=whl	
🔒 Reports	User filter	(&(objectclass=user))	*
■ Productivity	Group filter	(&(objectclass=group))	*
Settings	Servers		
😂 System	Address	10.0.40.100 Port 389	
Ø <sup>e</sup> Network configuration	Page   DAP results		
Notifications	Encrypted connection		
C Timestamping	Delete		
a. External authentication	Contra Co	Č.	
III External passwords repositories		Add another directory and in any a	
Resources	Attributes mapping	Add another directory service server	$\bigcirc$
Backups and retention	Group mappings		Display LDAP fields mapping options
♣ Cluster			
LDAP synchronization	Mapping	CN=wheel,DC=fech,DC=whi + adusers + a, ~ ×	
≡ Events log	Define group to saf	es assignment	
	Assign selected au	thentication methods to imported users	Force full synchronization

- Data model
- Users management
- Servers management
- Accounts

# chapter 6

# Servers

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

			Block	access to select	ed servers
			Activa	te access to sele	cted servers
Management Add s	server definition		Delete	e selected servers	
M Dashboard	Servers + Add	© Block	@ Delete		T Add filter ~ Search
E Sessions				Filtor convorc	list
쓭 Users	O Name +	Protocol	Host	Port	Last login
⊖ Servers	CentOS	SSH	10.0.7.11	22	1 month, 1 week ago
_	FreeBSD10	SSH	10.0.45.4	22	1 week, 6 days ago
Accounts	FreeBSD2	SSH	10.0.35.52	22	1 month, 1 week ago
Safes	Windows2012	RDP	10.0.40.101	3389	1 month, 1 week ago
> Listenere	Windows Edit serve	r definition	10.0.8.106	3389	1 month ann
W Listeners	asd	SSH	localhost	22 Blo	cked resource
A- Password changers	0 vnc	VNC	10.0.0.7	59102	1 month, 1 week ago
Policies				Rea	ason the resource has bee

# 6.1 Creating a server

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

### 6.1.1 Creating a Citrix server

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

Ma	anagement Create	new safe			
M	Dashboard	Segure + Add © Block © Unblock @ Delete		▼ Add filter ~	Search
₿		Servers			
쓭		Name A Protocol	Host	Port	Last login
_	Sanuara	□ 10.0.35.1 SSH	10.0.35.1	22	4 months
-		MSSQL-10.0.35.1 MS SQL (TDS)	s) 10.0.35.1	1433	never
-	Accounts	MYSQL-0-10.0.35.52 MySQL	10.0.35.52	3306	2 years, 5
		MYSQL-10.0.35.1 MySQL	10.0.35.1	3306	never
2	Listeners	ORACLE-10.0.40.149 Oracle	10.0.40.149	1521	2 years, 5
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN RDP	10.0.35.54	3389	1 year ag
n-	Password changers	DP-10.0.8.103- RDP	10.0.8.103	3389	1 year ag

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

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

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

Mana	agement <	Fudo	
Jan Da		Remon	
🖽 Se		Server	
상 나		General	Unique object name
⊟ <b>S</b> e	ervers	Name	
🔊 Ad			
🔳 Sa		Blocked	Disable access after object is created
≫ Li:		Protocol	Citrix StoreFront (HTTP) + Select connectio
ni- Pa			
U Po		HTTP timeout	etter HTIP conn
± 00		Description	Add optional des
🖨 Re		Permissions	
⊖ Re ≣ Pr		Permissions	
⊕ Re ≣ Pr Settin	reports roductivity n <b>gs</b>	Permissions Granted users	(
B Re E Pr Settin	reports roductivity n <b>gs</b> ystem	Permissions Granted users Destination host	Users allowed to manage this object
B Re B Pr Settin B Sy O <sup>©</sup> Ne	reports roductivity ngs ystem letwork configuration	Permissions Granted users Destination host	Users allowed to manage this object Server's IP address
Rettin     Settin     So	reports roductivity ngs ystem letwork configuration lotifications	Permissions Granted users Destination host Address	Users allowed to manage this object Port 80
Rettin     Settin     Solution     No     No     No     Theorem	reports roductivity ngs ystem letwork configuration lotifications imestamping	Permissions Granted users Destination host Address Bind address	Users allowed to manage this object Port 60 Any Source IP address
Pr     Settin     So     No     C     The     Q     C	reports roductivity ngs ystem letwork configuration lotifications imestamping xternal authentication	Permissions Granted users Destination host Address Bind address URL	Users allowed to manage this object Server's IP address Port 80 Any Cource IP address Specify StoreFrom
Ret     Ret     Ret     Ret     Ret     Settin	reports roductivity ngs ystem letwork configuration lotifications imestamping xternal authentication xternal passwords repositories	Permissions Granted users Destination host Address Bind address URL	Users allowed to manage this object Port 80 Any Cource IP address Server's IP address Server's IP address Server's IP address
Ret     Ret     Ret     Settin     Sett	eports roductivity ngs ystem letwork configuration lotifications imestamping xternal authentication xternal passwords repositories lesources	Permissions Granted users Destination host Address Bind address URL	Users allowed to manage this object Very Bo Any Server's IP address Server's IP address Server's IP address Server's IP address Server's IP address Server's IP address

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

### 6.1.2 Creating an HTTP server

#### Note:

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- 1. Select *Management* > *Servers*.
- 2. Click + Add.

Ma	anagement Create	e new safe					
M	Dashboard	Senuere + Add © Block ©	Unblock 🕆 Delete			T Add filter ~	Search
₿		Servers					
굩		Name +	P	Protocol	Host	Port	Last login
	Sanara	□ 10.0.35.1	s	SSH	10.0.35.1	22	4 months
	Gervers	MSSQL-10.0.35.1	N	VIS SQL (TDS)	10.0.35.1	1433	never
₽		MYSQL-0-10.0.35.52	N	MySQL	10.0.35.52	3306	2 years, 5
•		MYSQL-10.0.35.1	Ν	MySQL	10.0.35.1	3306	never
2	Listeners	ORACLE-10.0.40.149	C	Dracle	10.0.40.149	1521	2 years, 5
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN	. F	RDP	10.0.35.54	3389	1 year ag
- 10-	Password changers	RDP-10.0.8.103-	F	RDP	10.0.8.103	3389	1 year ag

- 3. Enter server's unique name.
- 4. Select *Blocked* option to disable access to server after it's created.
- 5. Select HTTP from the *Protocol* drop-down list.
- 6. Enter value of the *HTTP timeout* parameter, determining the time period of inactivity (expressed in seconds), after which the user will have to authenticate again.
- 7. Select the Enable SSLv2 support to support SSL v2 encrypted connections.
- 8. Select the Enable SSLv3 support to support SSL v3 encrypted connections.
- 9. Enter optional description, which will help identifying this server object.
- 10. In the *Permissions* section, add users allowed to manage this object.
- 11. In the Destination host section, enter server's IP address and port number.
- 12. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

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

Management <	Fudo <sup>*</sup>	
Jashboard	Conver	
E Sessions	Server	
쑬 Users	General	Unique object name
🖨 Servers	Name	
Accounts		
Safes	Blocked	Disable access after object is created
ሕ Listeners	Protocol	с (нтр) Select connection pro
n- Password changers	HTTP timeout	900 Enter HTTP connectio
C Policies	Enable SSLv2 support	Select to enable SSL v2 encrypted connections
📩 Downloads	Enable SSLv3 support	Select to enable SSL v3 encrypted connections
🖨 Reports	Description	Add optional descripti
E Productivity	Pormissions	
Settings	Permissions	
👺 System	Granted users	<u> </u>
¢ <sup>e</sup> Network configuration	Destination host	Users allowed to manage this object
☑ Notifications		Server's IP address and
@ Timestamping	Address	
At External authentication	Bind address	Any 9 Source IP address
## External passwords repositories	HTTP host	Specify monitored res
🖾 Resources		Upse TLS
Backups and retention	Server certificate	Connect to server over TLS
n Cluster		Click to download server's certificate
		Click to upload server's certificate
≡ Events log		
0 21:13:56.9466396 12245578		
%-3-30375 JL Net configured		SHA1
		C Reset Save Save object's definition



- Data model
- System initiation
- Users
- Listeners
- Safes
- $\bullet \ Accounts$

### 6.1.3 Creating an ICA server

1. Select Management > Servers.

2. Click + Add.

Ma	anagement Crea	te new safe				
	Dashboard	Servers + Add   Block   Unblock	🗑 Delete		T Add filter ~	Search
₿		Servers				
쓭		Name +	Protocol	Host	Port	Last login
_	Servers	10.0.35.1	SSH	10.0.35.1	22	4 months
	Cervers	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	never
		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 years, 5
•		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	never
	Listeners	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 years, 5
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN	RDP	10.0.35.54	3389	1 year ag
n-	Password changers	DP-10.0.8.103-	RDP	10.0.8.103	3389	1 year ag

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

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

- 10. Select the Use TLS options to connect to monitored server over TLS.
- 11. Select the Enable SSLv2 support to support SSL v2 encrypted connections.
- 12. Select the Enable SSLv3 support to support SSL v3 encrypted connections.
- 13. Click the certificate download icon to fetch server's certificate, or the certificate upload icon to upload a certificate.
- 14. Click Save.

Management <	Fudo	
Jashboard		
E Sessions	Server	
쑐 Users	General	Unique object name
🖴 Servers	Name	
Accounts		
Safes	Blocked	Disable access after object is created
ふ Listeners	Protocol	CA Select connecti
<ul> <li>Password changers</li> </ul>		
0 Policies	Description	Add optional de
🕹 Downloads	Permissions	Users allowed to manage this object
🖨 Reports	Granted users	
■ Productivity	chanted users	
Settings	Destination host	Server's IP address and port number
🖕 System	Address	Port 1494
Op Network configuration		
Notifications	Bind address	s) - Source IP addr
@ Timestamping		Connect to server over TLS
a, External authentication	Enable SSLv2 support	Select to enable SSL v2 encrypted connections
III External passwords repositories	Enable SSLv3 support	Select to enable SSL v3 encrypted connections
Resources	Server certificate	
Backups and retention	CI	ick to download server's certificate
🚓 Cluster	CI	ick to upload server's certificate
LDAP synchronization		
≡ Events log		
		SHA1
32 days ii 12345678 ● 3-31753		
		Save object's definition

- $\bullet \ Data \ model$
- $\bullet \ ICA$
- Creating an ICA listener
- ICA configuration file
- ICA

### 6.1.4 Creating a Modbus server

#### Note:

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- 1. Select Management > Servers.
- 2. Click + Add.

Ma	anagement Create r	ew safe			
	Dashboard	Sequer + Add © Block © Unblock @ Delete		T Add filter ∨	Search
₿	Sessions				
*	Users	Name + Protoco	ool Host	Port	Last login
_	Servere	□ 10.0.35.1 SSH	10.0.35.1	22	4 months
	Servers	MSSQL-10.0.35.1 MS SQL	QL (TDS) 10.0.35.1	1433	never
	Accounts	MYSQL-0-10.0.35.52 MySQ	AL 10.0.35.52	3306	2 years, 5
	Safes	MYSQL-10.0.35.1 MySQL	AL 10.0.35.1	3306	never
	Listeners	ORACLE-10.0.40.149 Oracle	e 10.0.40.149	1521	2 years, 5
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN	10.0.35.54	3389	1 year ag
19-	Password changers	□ RDP-10.0.8.103- RDP	10.0.8.103	3389	1 year ag

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

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

10. Click Save.

Management <	≓udo <sup>•</sup>	
I Dashboard	Server	
E Sessions	301401	
촬 Users	General	Unique object name
⊖ Servers	Name	
Accounts		
Safes	Blocked	Disable access after object is created
Դ Listeners	Protocol	Modbus
n- Password changers	Description	Add optional descripti
<b>V</b> Policies	Permissions	
🛓 Downloads		
🕀 Reports	Granted users	् २
E Productivity	Destination host	Users allowed to manage this object
Sattinge		Server's IP address and
Gettings	Address	Port 502
System	Bind address	Any +- Source IP address
© Network configuration		
Notifications		
C Timestamping		Save object's definition

- Data model
- System initiation
- Users
- Listeners
- Safes
- $\bullet \ Accounts$

### 6.1.5 Creating a MS SQL server

### Note:

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- 1. Select Management > Servers.
- 2. Click + Add.

Ma	anagement Create	e new safe					
M	Dashboard	Senuere + Add © Block ©	Unblock 🕆 Delete			T Add filter ~	Search
₿		Servers					
굩		Name +	P	Protocol	Host	Port	Last login
	Sanara	□ 10.0.35.1	s	SSH	10.0.35.1	22	4 months
	Gervers	MSSQL-10.0.35.1	Ν	VIS SQL (TDS)	10.0.35.1	1433	never
₽		MYSQL-0-10.0.35.52	N	MySQL	10.0.35.52	3306	2 years, 5
•		MYSQL-10.0.35.1	Ν	MySQL	10.0.35.1	3306	never
2	Listeners	ORACLE-10.0.40.149	C	Dracle	10.0.40.149	1521	2 years, 5
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN	. F	RDP	10.0.35.54	3389	1 year ag
- 10-	Password changers	RDP-10.0.8.103-	F	RDP	10.0.8.103	3389	1 year ag

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

10. Click Save.

Management <	Fudo	
Jashboard	Comme	
E Sessions	Server	
쯀 Users	General	Unique object name
⊖ Servers	Name	
Accounts	Biocheck	
Safes	Biocked	Disable access after object is created
Դ Listeners	Protocol	Celect connection pro
n- Password changers	Description	Add optional descripti
C Policies	Permissions	
📩 Downloads	Created warra	
🖨 Reports	Granted users	
E Productivity	Destination host	Users allowed to manage this object
Settings	Address	Port 1433
🖨 System		
Ø <sup>e</sup> Network configuration	Bind address	Any Source IP address
☑ Notifications		
C Timestamping		Save object's definition

- Data model
- System initiation
- Users
- Listeners
- $\bullet$  Safes
- Accounts

### 6.1.6 Creating a MySQL server

### Note:

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- 1. Select Management > Servers.
- 2. Click + Add.

Ma	anagement Create	e new safe					
M	Dashboard	Senuere + Add © Block ©	Unblock 🕆 Delete			T Add filter ~	Search
₿		Servers					
굩		Name +	P	Protocol	Host	Port	Last login
	Sanara	□ 10.0.35.1	s	SSH	10.0.35.1	22	4 months
	Gervers	MSSQL-10.0.35.1	Ν	VIS SQL (TDS)	10.0.35.1	1433	never
₽		MYSQL-0-10.0.35.52	N	MySQL	10.0.35.52	3306	2 years, 5
•		MYSQL-10.0.35.1	Ν	MySQL	10.0.35.1	3306	never
2	Listeners	ORACLE-10.0.40.149	C	Dracle	10.0.40.149	1521	2 years, 5
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN	. F	RDP	10.0.35.54	3389	1 year ag
- 10-	Password changers	RDP-10.0.8.103-	F	RDP	10.0.8.103	3389	1 year ag

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

10. Click Save.

Management <	Fudo	
🖬 Dashboard		
E Sessions	Server	
쓭 Users	General	Unique object name
⊖ Servers	Name	
Accounts	Biocheck	
Safes	DIOCKED	Usable access after object is created
ሕ Listeners	Protocol	C MysaL Select connection pro
n- Password changers	Description	Add optional descripti
C Policies	Permissions	
📩 Downloads		
🖨 Reports	Granted users	• a
E Productivity	Destination host	Users allowed to manage this object
Settings	Artiraco	Server's IP address and
🗁 System	Address	Polt 0000
¢ Network configuration	Bind address	Any Source IP address
☑ Notifications		
C Timestamping		Save object's definition

- Data model
- System initiation
- Users
- Listeners
- Safes
- $\bullet \ Accounts$

### 6.1.7 Creating an Oracle server

### Note:

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- 1. Select Management > Servers.
- 2. Click + Add.

Ma	anagement Create	new safe					
M	Dashboard	+ Add O Block O Unbid	ck 🔒 Delete			T Add filter ~	Search
₿		Servers				1 - 100 - 11101 -	Council
~		🗆 Name 🔺		Protocol	Host	Port	Last login
	Sanara	0 10.0.35.1		SSH	10.0.35.1	22	4 months
	Gervers	MSSQL-10.0.35.1		MS SQL (TDS)	10.0.35.1	1433	never
₽		MYSQL-0-10.0.35.52		MySQL	10.0.35.52	3306	2 years, 5
•		MYSQL-10.0.35.1		MySQL	10.0.35.1	3306	never
	Listeners	ORACLE-10.0.40.149		Oracle	10.0.40.149	1521	2 years, 5
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN		RDP	10.0.35.54	3389	1 year ag
- H-	Password changers	D RDP-10.0.8.103-		RDP	10.0.8.103	3389	1 year ag

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

10. Click Save.

Management <	Fudo	
I Dashboard		
E Sessions	Server	
쑬 Users	General	Unique object name
🖴 Servers	Name	
Accounts	Biocheck	
Safes	Biocked	Disable access after object is created
ふ Listeners	Protocol	Coracle Select connection pro
n- Password changers	Description	Add optional descripti
C Policies	Permissions	
🛓 Downloads	Graated users	
🕀 Reports	Granted users	
■ Productivity	Destination host	Users allowed to manage this object
Settings	Address	Port 1521
🖨 System		
Ø <sup>e</sup> Network configuration	Bind address	Any Source IP address
☑ Notifications		
C Timestamping		Save object's definition

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

### 6.1.8 Creating an RDP server

### Note:

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- 1. Select Management > Servers.
- 2. Click + Add.

Ma	anagement Create	e new safe					
M	Dashboard	Senuere + Add © Block ©	Unblock 🕆 Delete			T Add filter ~	Search
₿		Servers					
굩		Name +	P	Protocol	Host	Port	Last login
	Sanara	□ 10.0.35.1	s	SSH	10.0.35.1	22	4 months
	Gervers	MSSQL-10.0.35.1	Ν	VIS SQL (TDS)	10.0.35.1	1433	never
₽		MYSQL-0-10.0.35.52	N	MySQL	10.0.35.52	3306	2 years, 5
•		MYSQL-10.0.35.1	Ν	MySQL	10.0.35.1	3306	never
2	Listeners	ORACLE-10.0.40.149	C	Dracle	10.0.40.149	1521	2 years, 5
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN	. F	RDP	10.0.35.54	3389	1 year ag
- 10-	Password changers	RDP-10.0.8.103-	F	RDP	10.0.8.103	3389	1 year ag

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

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

11. Click Save.

Management <	≓udo <sup>•</sup>	
Dashboard	Samer	
E Sessions	361761	
쯀 Users	General	Unique object name
🖴 Servers	Name	
Accounts	Biocheck	Disable appage offer object is greated
Safes	Blocked	Disable access alter object is created
Դ Listeners	Protocol	RDP Select connection
n- Password changers	Security	Enhanced RDP Security (TLS) + NLA - Select RDP securi
Policies	Description	Add optional desc
📥 Downloads	Permissions	
🖨 Reports	Permissions	
E Productivity	Granted users	<u>्</u>
Settings	Destination host	Users allowed to manage this object
system 😂		Server's IP address a
Ø <sup>o</sup> Network configuration	Address	Port 3389
Notifications	Bind address	Any Source IP addres
@ Timestamping	Server certificate	
e External authentication		Click to download server's certificate
III External passwords repositories		
Resources		
Backups and retention		
🚓 Cluster		SHA1
LDAP synchronization		
≡ Events log		C Reset Save Save object's definition

- $\bullet \ Data \ model$
- System initiation
- $\bullet \ Users$
- Listeners
- $\bullet$  Safes
- $\bullet \ Accounts$

### 6.1.9 Creating an SSH server

#### Note:

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- 1. Select Management > Servers.
- 2. Click + Add.

Ma	anagement Create	new safe				
M	Dashboard	Sequera + Add © Block © Unblock @ Delete			T Add filter ∨	Search
₿						
*		Name +	Protocol	Host	Port	Last login
_	Sanuara	0 10.0.35.1	SSH	10.0.35.1	22	4 months
-		MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	never
-		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 years, 5
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	never
2	Listeners	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 years, 5
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN	RDP	10.0.35.54	3389	1 year ag
- 10-	Password changers	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 year ag

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

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

- 10. Click the fetch key icon to download server's public key.
- 11. Click Save.

Management <	Fudo	
M Dashboard	Convor	
E Sessions	Server	
嶜 Users	General	Unique object name
⊖ Servers	Name	
Accounts	Plantad	Disable assess after object is greated
Safes	Biocked	Disable access alter object is created
Դ Listeners	Protocol	Select connection
<ul> <li>Password changers</li> </ul>	Description	Add optional desc
C Policies	Permissions	
🛓 Downloads	1011113310113	
🔒 Reports	Granted users	<u>्</u>
■ Productivity	Destination host	Users allowed to manage this object
Settings	Addmin	Server's IP address a
👺 System	Address	
¢ <sup>e</sup> Network configuration	Bind address	Any Source IP addres
Notifications	Server public key	
C Timestamping		Click to download server's public key
a External authentication		
III External passwords repositories		
Resources		
Backups and retention		SHA1
🖧 Cluster		
LDAP synchronization		Save object's definition

- Data model
- System initiation
- Users
- Listeners
- $\bullet \ Safes$
- $\bullet \ Accounts$

## 6.1.10 Creating a Telnet server

#### Note:

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

- A server object can be linked to only one *forward* account.
- In case of Telnet connections over *forward* and *regular* accounts, users are asked to provide their login credentials twice. First time to authenticate against Wheel Fudo PAM and then to connect to the target host.
- 1. Select Management > Servers.
- 2. Click + Add.

_											
м	anagement	Create new	/ safe 上								
	Dashboard		Servers + Add © Block © Unblock @ Delete			т	Add filter ~	Search			
B											
			Name +				Protocol	Host		Port	Last login
	Servers	0	10.0.35.1				SSH	10.0.35.1		22	4 months
	Servers		MSSQL-10.0.35.1				MS SQL (TDS)	10.0.35.1		1433	never
-		0	MYSQL-0-10.0.35.	i2			MySQL	10.0.35.52		3306	2 years, 5
			MYSQL-10.0.35.1				MySQL	10.0.35.1		3306	never
	Listeners	0	ORACLE-10.0.40.1	49			Oracle	10.0.40.149		1521	2 years, \$
			RDP-0-10.0.35.54,	RDP-0-10.0.35.5	i4-AN		RDP	10.0.35.54		3389	1 year ag
- 19-	Password changers		RDP-10.0.8.103-				RDP	10.0.8.103		3389	1 year ag

- 3. Enter server's unique name.
- 4. Select *Blocked* option to disable access to server after it's created.
- 5. Select Telnet from the *Protocol* drop-down list.
- 6. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
- 7. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
- 8. Enter optional description, which will help identifying this server object.
- 9. In the *Permissions* section, add users allowed to manage this object.
- 10. In the *Destination host* section, enter server's IP address and port number.
- 11. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

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

Management <	Fudo <sup>•</sup>	
Jail Dashboard	Conjor	
E Sessions	Server	
쑬 Users	General	Unique object name
🖴 Servers	Name	
Accounts		
Safes	Blocked	Disable access after object is created
ふ Listeners	Protocol	Celect connection pro
n- Password changers	Enable SSLv2 support	Select to enable SSL v2 encrypted connections
Policies	Enable SSLv3 support	Select to enable SSL v3 encrypted connections
🛓 Downloads	Description	Add optional descript
🕀 Reports	Permissions	
■ Productivity		
Settings	Granted users	
🖨 System	Destination host	Users allowed to manage this object
¢ <sup>e</sup> <sub>6</sub> Network configuration	Address	Port 23
☑ Notifications	Rived a data	
C Timestamping	Bind address	Source IP address
a, External authentication		Use TLS
III External passwords repositories	Server certificate	Connect to server over TLS
Resources		Click to download server's certificate
Backups and retention		Click to upload server's certificate
4 Cluster		
LDAP synchronization		
		SHA1
© 3:10:58.8005986 12345678 ● 3:33429 Al Not comfigured		C Reset Save Save Object's definition

- Data model
- System initiation
- Users
- Listeners
- $\bullet Safes$
- Accounts

### 6.1.11 Creating a Telnet 3270 server

### Note:

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

- A server object can be linked to only one *forward* account.
- In case of Telnet connections over *forward* and *regular* accounts, users are asked to provide their login credentials twice. First time to authenticate against Wheel Fudo PAM and then to connect to the target host.
- 1. Select Management > Servers.
- 2. Click + Add.

M	anagement	Create ne	w safe 上	_							
	Dashboard		Samore	+ Add	O Block	O Unblock	🕆 Delete			T Add filter ∽	Search
₿		- 11	Servera								
~			🗆 Name 🔺					Protocol	Host	Port	Last login
_	Convom		0 10.0.35.1					SSH	10.0.35.1	22	4 months
	Servers		MSSQL-10	.0.35.1				MS SQL (TDS)	10.0.35.1	1433	never
₽			MYSQL-0-1	10.0.35.52				MySQL	10.0.35.52	3306	2 years, 5
			MYSQL-10.	.0.35.1				MySQL	10.0.35.1	3306	never
2	Listeners		ORACLE-10	0.0.40.149				Oracle	10.0.40.149	1521	2 years, s
			RDP-0-10.0	).35.54, RDP-	0-10.0.35.54	-AN		RDP	10.0.35.54	3389	1 year ag
n-	Password changers		RDP-10.0.8	.103-				RDP	10.0.8.103	3389	1 year ag
_								1.01	10.0.0.100	0000	- your ag

- 3. Enter server's unique name.
- 4. Select *Blocked* option to disable access to server after it's created.
- 5. Select Telnet 3270 from the Protocol drop-down list.
- 6. Select the *Enable SSLv2 support* to support SSL v2 encrypted connections.
- 7. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
- 8. Enter optional description, which will help identifying this server object.
- 9. In the *Permissions* section, add users allowed to manage this object.
- 10. In the *Destination host* section, enter server's IP address and port number.
- 11. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

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

Management <	Fudo	
Jashboard	Conver	
E Sessions	Server	
쌸 Users	General	Unique object name
🕀 Servers	Name	
Accounts		
Safes	Blocked	Disable access after object is created
ふ Listeners	Protocol	Ceinet 3270 Select connection pro
n- Password changers	Enable SSLv2 support	Select to enable SSL v2 encrypted connections
Policies	Enable SSLv3 support	Select to enable SSL v3 encrypted connections
🛓 Downloads	Description	Add optional descripti
🖨 Reports	Permissions	
E Productivity		
Settings	Granted users	<u>े व</u>
🖨 System	Destination host	Users allowed to manage this object
¢ <sup>0</sup> <sub>6</sub> Network configuration	Address	Port 3270
Notifications		
C Timestamping	Bind address	Any Source IP address
e External authentication		U Jue TLS
III External passwords repositories	Server certificate	Connect to server over TLS
Resources		Click to download server's certificate
Backups and retention		Click to upload server's certificate
ሔ Cluster		
LDAP synchronization		A
≡ Events log		SHA1
© 3:10:58.8995986 12345678 ♥ 3:33429 44, Net configured		CReset Save Save Object's definition

- Data model
- System initiation
- Users
- Listeners
- $\bullet Safes$
- Accounts

### 6.1.12 Telnet 5250 server

Adding an Telent 5250 server

### Note:

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- In case of Telnet connections over *forward* and *regular* accounts, users are asked to provide their login credentials twice. First time to authenticate against Wheel Fudo PAM and then to connect to the target host.
- 1. Select Management > Servers.
- 2. Click + Add.

Ma	anagement Creat	new safe				
M	Dashboard	Sequere + Add © Block © Unblock @ Del	ete		T Add filter ∽	Search
₿		Servera				
쓭		Name +	Protocol	Host	Port	Last login
_	Sanuara	10.0.35.1	SSH	10.0.35.1	22	4 months
	Celvela	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	never
₽		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 years, 5
•		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	never
2	Listeners	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 years, \$
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN	RDP	10.0.35.54	3389	1 year ag
÷-	Password changers	DP-10.0.8.103-	RDP	10.0.8.103	3389	1 year ag

3. Enter server's unique name.

- 4. Select *Blocked* option to disable access to server after it's created.
- 5. Select Telnet 5250 from the Protocol drop-down list.
- 6. Select the Enable SSLv2 support to support SSL v2 encrypted connections.
- 7. Select the *Enable SSLv3 support* to support SSL v3 encrypted connections.
- 8. Enter optional description, which will help identifying this server object.
- 9. In the *Permissions* section, add users allowed to manage this object.
- 10. In the *Destination host* section, enter server's IP address and port number.
- 11. From the *Bind address* drop-down list, select Wheel Fudo PAM IP address used for communicating with this server.

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

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

#### **Related topics:**

• Data model

- System initiation
- Users
- Listeners
- Safes
- Accounts

#### 6.1.13 Creating a VNC server

#### Note:

- A server object can be linked to only one *anonymous* account.
- A server object can be linked to only one *forward* account.
- 1. Select Management > Servers.
- 2. Click + Add.

Ma	anagement 🛛	Create new safe		
M	Dashboard	Servers + Add © Block © Unblock @ Delete	▼ Add filter ~	Search
₿				
쓭		Name + Protocol Host	Port	Last login
_	Servers	□ 10.0.35.1 SSH 10.0.35.1	22	4 months
-	Gervera	MSSQL-10.0.35.1 MS SQL (TDS) 10.0.35.1	1433	never
-		MYSQL-0-10.0.35.52 MySQL 10.0.35.52	3306	2 years, 5
		□ MYSQL-10.0.35.1 MySQL 10.0.35.1	3306	never
2	Listeners	ORACLE-10.0.40.149 Oracle 10.0.40.149	1521	2 years, 5
		□ RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN RDP 10.0.35.54	3389	1 year ag
- H-	Password changers	□ RDP-10.0.8.103- RDP 10.0.8.103	3389	1 year ag

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

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

10. Click Save.

Management <	Fudo <sup>•</sup>	
M Dashboard	Server	
E Sessions	361761	
쯓 Users	General	Unique object name
🖴 Servers	Name	
Accounts		
Safes	Biocked	Disable access after object is cleated
ふ Listeners	Protocol	C VNC Select connection pro
n- Password changers	Description	Add optional descripti
<b>V</b> Policies	Permissions	
📩 Downloads		
🖨 Reports	Granted users	ं ब
■ Productivity	Destination host	Users allowed to manage this object
Settings		Server's IP address and
🗁 System	Address	Port Sevu
¢ Network configuration	Bind address	Any Source IP address
Notifications		
C Timestamping		
ae External authentication		
III External passwords repositories		C Reset Save Save object's definition

- Data model
- System initiation
- Users
- Listeners
- Safes
- $\bullet \ Accounts$

# 6.2 Editing a server

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

Ma	anagement	۲.	Fudo'									
	Dashboard		Soniore	+ Add	O Block	O Unblock	🕆 Delete			T Ad	d filter ~	Search
₿			Servera									
*			🗆 Name +	Name +					Host		Port	Last login
_	Sanuara		0 10.0.35.1	10.0.35.1 \$					10.0.35.1		22	4 months
	Servers		MSSQL-10	.0.35.1				MS SQL (TDS)	10.0.35.1		1433	never
			MISQL-0	MISQL-9 Edit object definition				MySQL	10.0.35.52		3306	2 years, 5
			MYSQL-10	0.0.35.1				MySQL	10.0.35.1		3306	never
	Listeners		ORACLE-1	0.0.40.149				Oracle	10.0.40.149		1521	2 years, 5
			RDP-0-10.	0.35.54, RDF	-0-10.0.35.54	-AN		RDP	10.0.35.54		3389	1 year ag
n-	Password changers		□ RDP-10.0.8.103-				RDP	10.0.8.103		3389	1 year ag	

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

3. Modify configuration parameters as needed.

Note:	Unsaved	changes	are	marked	with	the	🕼 icon
-------	---------	---------	-----	--------	------	-----	--------

General	Unsaved	changes
Login	john_smith	
Blocked		
Account validity	Indefinite	\$
Role	operator	\$

4. Click Save.

#### **Related topics:**

- Data model
- System initiation
- $\bullet \ Users$
- Listeners
- Safes
- Accounts

# 6.3 Blocking a server

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

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

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

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

3. Click Block.

Manage	ement <	Fudo <sup>*</sup>				📥 admin 🕤	÷	?
		Servers + Add Block © Unblock @ Delet	8		▼ Add filter ~	Search	0	٩
	sions	Select object						
	rs	Name	Protocol	Host	Port	Last login		
G Serv	are .	10.0.35.1 Deactivate selected objects	SSH	10.0.35.1	22	4 months, 1 week ago		
		MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	never		
	ounts	MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 years, 5 months ago		
	95	MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	never		
	eners	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 years, 5 months ago		
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN	RDP	10.0.35.54	3389	1 year ago		
n- Pass	sword changers	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 year ago		

4. Optionally, provide blocking reason and click Confirm.

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

Block objects	×
Reason	
Provide blocking reason	Cancel Confirm
Block selected	objects

### **Related topics:**

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

# 6.4 Unblocking a server

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

1. Select Management > Servers.

2. Find and select desired objects.

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

3. Click Unblock.

Manag	jement <	Fudo <sup>*</sup>				📥 admin 🗸	?
		Sequere + Add @ Block OUnbloct: @ Dele	te		T Add filter	- Search (	Q
		Select object					
		Name Select Object	Protocol	Host	Port	Last login	
A Sen	Vars	O 10.0.35.1 Activate selected objects	SSH	10.0.35.1	22	4 months, 1 week ago	
		MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	never	
		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 years, 5 months ago	
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	never	
		ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 years, 5 months ago	
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-AN	RDP	10.0.35.54	3389	1 year ago	
	ssword changers	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 year ago	

4. Click *Confirm* to unblock selected objects.

Unblock objects
Are you sure you want to unblock 1 object?
Cancel
Confirm unblocking selected objects

#### **Related topics:**

- Data model
- System initiation
- Users
- Listeners
- $\bullet \ Safes$
- Accounts

## 6.5 Deleting a server

#### Deleting a server definition

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

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

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

3. Click *Delete*.

Ma	anagement <	Fudo <sup>•</sup>					
M	Dashboard	+ Add	O Block O Unblock	A Delete		T Add filter ∨	Search
₿		Servers	hingt	4			
~		Name Select 0	bject	Protocol	Host	Port	Last login
	Samaro	10.0.35.1 Delete	e selected objects	SSH	10.0.35.1	22	4 months
		MSSQL-10.0.35.1		MS SQL	TDS) 10.0.35.1	1433	never
₽	Accounts	MYSQL-0-10.0.35.52		MySQL	10.0.35.52	3306	2 years, 5
		MYSQL-10.0.35.1		MySQL	10.0.35.1	3306	never
	Listeners	ORACLE-10.0.40.149	)	Oracle	10.0.40.149	1521	2 years, 5
		RDP-0-10.0.35.54, R	DP-0-10.0.35.54-AN	RDP	10.0.35.54	3389	1 year ag
· **	Password changers	RDP-10.0.8.103-		RDP	10.0.8.103	3389	1 year ag

4. Confirm deletion of selected objects.

Delete objects	×
Are you sure you want to delete 1 object?	
	Cancel Confirm
Confirm deleting selected	l objects

### Related topics:

- Data model
- System initiation
- Users
- Listeners
- Safes
- Accounts
# chapter 7

# Accounts

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

**Note:** In case of Telnet connections, user has to go through authentication process twice. First time to authenticate against Wheel Fudo PAM and then to connect to the target host.

Activate	selected accou	unts					
Deactivate	selected accou	unts	_		Dele	te selected accounts	
Management	Create new ad	count				Defi	ne objects li
Jashboard		+ Add	Block	ck 🛱 Delete		T Add filter	Search
E Sessions	Ad	counts (1990)					oonon
쯀 Users	0	Name +	Server *	Recording *	Туре	Password change policy	Password cha
A Servers		acc	CentOS	all	regular	Static, without restrictions	None
		admin@win2012	Windows2012	all	regular	Static, without restrictions	None
Accounts		admin@windows7)	Windows7	all	regular	Static, without restrictions	None
Safes		<sup>anonyme</sup> Edit accoun	t definition	all	anonymous	None	None
Listeners	0	asd	CentOS	all	regular	Static, without restrictions	None
in Later of a		joe@FreeBSD10	FreeBSD10	all	regular	Random, 8 length, change 1 hour	Unix Account
h Password changers		root@CentOS	CentOS	all	regular	Static, without restrictions	None
Policies	0	root@freebsd10	FreeBSD10	all	regular	static, v Blocked account	None
A Brown br		vnc	vnc	all	regular	Static, without restrictions	None
Z Downloads						Ho	ver to view tl
🕀 Reports							
■ Productivity							

# 7.1 Creating an account

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

# 7.1.1 Creating an anonymous account

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

Ma	nagement	Create nev	v account										
			Accounts	+ Add	© Block	O Unblock	Belete	C Timestamp				▼ Add filter ~	Se
₿			Accounts										
쓭			🗆 Name +			Serve	/*			Recording *	Туре	Password change policy	Pass
_			account_4			10.0.3	35.1			all	regular	Static, without restrictions	Non
-			admin@serw	er3		serwe	er3			all	regular	Static, without restrictions	Non
-	Accounts		administrator	rat RDP-0-10.	0.35.54, RD	RDP-	0-10.0.35.54, R	DP-0-10.0.35.54-A	NONYMOUS	all	regular	Static, without restrictions	None
			administrator	r@serwer1		serwe	er1			all	regular	Static, without restrictions	Non
			administrator	r@serwer2		serwe	# <b>2</b>			all	regular	Static, without restrictions	None
			anonymous			SSH-	0-10.0.35.52			all	anonymous	None	Non

- 3. Define object's name.
- 4. Select *Blocked* option to disable account after it's created.
- 5. Select anonymous from the *Type* drop-down list.
- 6. Select desired session recording option.
- all Wheel Fudo PAM records network traffic allowing for future session playback, using the built in session player, as well as converting session material to a selection of video file formats.
- raw Wheel Fudo PAM keeps records of the data exchanged between the user and the monitored server. The raw data can be downloaded later on but the session cannot be played back using the built in session player.
- none Wheel Fudo PAM only takes note of the fact that the give session took place but does not record the data exchanged between the user and the server.
- 7. Select the OCR sessions option to fully index RDP and VNC sessions contents.
- 8. Select language used for processing recorded sessions.
- 9. In the *Delete session data after* field, define the number of days after which the session data will be deleted.
- 10. In the *Permissions* section, add users allowed to manage this object.
- 11. In the *Server* section, assign account to a specific server by selecting it from the *Server* drop-down list.
- 12. Click Save.

м	anagement <	Fudo'	
1	Dashboard		
₿		Account	
*		General	Unique object name
8		Name	
	Accounts		
•		Blocked	Disable access after creating object
2	Listeners	Type	anonymous System events not
ė.		.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
U		Session recording	Security policies
*	Downloads	OCR sessions	O Ask for login reason
Ð		Delete session data after	days Session data reter
≡		Permissions	
Se	attings		Users allowed to manage this object
		Granted users	<b>०</b> २
¢ŝ		Server	
Ø		Server	Assign account to
a,			
	External passwords repositories		Reset Save Save object's definition

### **Related topics:**

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

### 7.1.2 Creating a forward account

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

Management	Create new a	account									
M Dashboard		+ Add	O Block	O Unblock	Delete	C Timestamp				T Add filter	- Se
E Sessions	· · · · · · · · · · · · · · · · · · ·										
쓸 Users		Name +		Server	~			Recording +	Туре	Password change policy	Pass
		account_4		10.0.3	5.1			all	regular	Static, without restrictions	None
		admin@serwer3		serwe	3			all	regular	Static, without restrictions	Non
Accounts	0	administrator at RDP-0-10.	0.35.54, RD	RDP-0	-10.0.35.54, RI	DP-0-10.0.35.54-AM	NONYMOUS	all	regular	Static, without restrictions	Non
Safes		administrator@serwer1		serwe	1			all	regular	Static, without restrictions	None
Listeners		administrator@serwer2		serwe	2			all	regular	Static, without restrictions	None
		anonymous		SSH-0	-10.0.35.52			all	anonymous	None	Non

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

- 5. Select forward from the *Type* drop-down list.
- 6. Select desired session recording option.
- all Wheel Fudo PAM records network traffic allowing for future session playback, using the built in session player, as well as converting session material to a selection of video file formats.
- raw Wheel Fudo PAM keeps records of the data exchanged between the user and the monitored server. The raw data can be downloaded later on but the session cannot be played back using the built in session player.
- none Wheel Fudo PAM only takes note of the fact that the give session took place but does not record the data exchanged between the user and the server.
- 7. Select the OCR sessions option to fully index RDP and VNC sessions contents.
- 8. Select language used for processing recorded sessions.
- 9. In the *Delete session data after* field, define the number of days after which the session data will be deleted.
- 10. In the *Permissions* section, add users allowed to manage this object.
- 11. In the *Server* section, assign the account to a server by selecting it from the *Server* dropdown list.

### Note: Two-fold authentication

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

To enable two-fold authentication, proceed as follows.

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

12. Click Save.

M	anagement <	Fudo	
	Dashboard		
₿		Account	
쓭		General	Unique object name
8		Name	
	Accounts		
•		Blocked	Disable access after creating object
٣	Listeners	Type	r forward System events not
ń-			
U		Session recording	Security policies
*	Downloads	OCR sessions	O Ask for login reason
₽		Delete session data after	days Session data reter
≡		Permissions	
Se	ettings		Users allowed to manage this object
		Granted users	् २
¢ŝ		Server	
Ø		Server	Assign account to
a,			
	External passwords repositories		Save object's definition

#### **Related topics:**

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

# 7.1.3 Creating a regular account

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

Management	Create new account					
M Dashboard	Accounts + Add • Block @	Unblock 🖹 Delete 🕼 Timestamp			▼ Add filter ~	Se
E Sessions	Accounts					
🗑 Users	Name +	Server *	Recording *	Туре	Password change policy	Pass
	account_4	10.0.35.1	all	regular	Static, without restrictions	None
	admin@serwer3	serwer3	all	regular	Static, without restrictions	None
Accounts	administrator at RDP-0-10.0.35.54, RD	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None
Safes	administrator@serwer1	serwer1	all	regular	Static, without restrictions	None
Listeners	administrator@serwer2	serwer2	all	regular	Static, without restrictions	None
	anonymous	SSH-0-10.0.35.52	all	anonymous	None	None

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

- 5. Select **regular** from the *Type* drop-down list.
- 6. Select desired session recording option.
- all Wheel Fudo PAM records network traffic allowing for future session playback, using the built in session player, as well as converting session material to a selection of video file formats.
- raw Wheel Fudo PAM keeps records of the data exchanged between the user and the monitored server. The raw data can be downloaded later on but the session cannot be played back using the built in session player.
- none Wheel Fudo PAM only takes note of the fact that the give session took place but does not record the data exchanged between the user and the server.
- 7. Select the OCR sessions option to fully index RDP and VNC sessions contents.
- 8. Select language used for processing recorded sessions.
- 9. In the *Delete session data after* field, define the number of days after which the session data will be deleted.
- 10. In the *Permissions* section, add users allowed to manage this object.
- 11. In the *Server* section, assign account to a specific server by selecting it from the *Server* drop-down list.
- 12. In the *Credentials* section, enter privileged account domain.
- 13. Type in login to the privileged account.
- 14. From the *Replace secret with* drop down list, select desired option.

#### with passwords

- Provide account password.
- Repeat account password.

#### with key

- Click the key type selection icon and select the key type.
- Click the upload icon 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.
- 15. Select the defined password changing policy from the *Password change policy* drop-down list.
- 16. In the *Password changer* section, from the *Password changer* drop-down list select password changer specific for given account.

# Unix Account over SSH

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

# Windows Account over WMI

• Enter privileged user name.

• Enter privileged user password.

# MySQL User Account on Unix Server over SSH

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

# Cisco Account over Telnet

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

# Cisco Enable Password over Telnet

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

### Cisco Account over SSH

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

# Cisco Enable Password poprzez SSH

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

# LDAP

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

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

17. Click Save.

Management <	Fudo	
M Dashboard		
E Sessions	Account	
曫 Users	General	Unique object name
🖴 Servers	Name	
Accounts		
Safes	Blocked	Disable access after creating object
ふ Listeners	Туре	regular System events no
<ul> <li>Password changers</li> </ul>	0	Convituation
Policies	Session recording	Security policies
🕹 Downloads	OCR sessions	O Ask for login reason
🔒 Reports	Delete session data after	days Session data reto
■ Productivity	Permissions	
Settings		Users allowed to manage this object
🖕 System	Granted users	० ९
¢ Network configuration	Server	
Notifications		
Imestamping	Server	Assign account to
at External authentication	Credentials	
III External passwords repositories	Domain	Account domain o
🖾 Resources	Domain	Account domain a
Backups and retention	Login	Account user logi
🚓 Cluster	Replace secret with	with password Account login cre
LDAP synchronization	Password	
≡ Events log	Repeat password	
	Beenverd shares college	Carelia without anticipiese
1:47:05.162754 i 12345678 \$ 3-30631 _B Not configured	Password change policy	Calanci, Mundot restrictions
	Password changer	
	Password changer	None Dassword change
	Privileged user	Privileged account
	Privileged user password	
		CReset Save Save Object's definition

# Related topics:

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

# 7.2 Editing an account

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

м	anagement <	Fudo'											
	Dashboard		+ Add	O Block	© Unb	lock i	≘ Delete	@ Timestamp				T Add fil	ter v Se
₿	Sessions	Accounts											
-	Users	🗆 Name +				Server *				Recording *	Туре	Password change policy	/ Pass
	Servers	account_4				10.0.35.1				all	regular	Static, without restrict	ions Non
_	Contors	admin@serw	ver3			serwer3				all	regular	Static, without restrict	ions Non
-	Accounts	administr E	Edit acco	unt defini	tion	RDP-0-10	0.0.35.54, R	DP-0-10.0.35.54-/	ANONYMOUS	all	regular	Static, without restrict	ions Non
	Safes	<ul> <li>administrator</li> </ul>	r@serwer1			serwer1				all	regular	Static, without restrict	ions Non
2	Listeners	administrator	r@serwer2			serwer2				all	regular	Static, without restrict	ions Non
		<ul> <li>anonymous</li> </ul>				SSH-0-10	0.0.35.52			all	anonymous	None	Non
n-	Password changers	anonymous f	for RDP-0-10.	0.35.54, RDP-	0	RDP-0-10	0.0.35.54, R	DP-0-10.0.35.54-/	ANONYMOUS	all	anonymous	None	Non
U	Policies	anonymous f	for RDP-0-TLS	S-10.0.40.100		serwer1				all	anonymous	None	Non
	Doubloade	anonymous f	for RDP-0-TLS	S-NLA-10.0.40	).1	serwer2				all	anonymous	None	Non

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

3. Modify configuration parameters as needed.

**Note:** Unsaved changes are marked with the  $\square$  icon.

General	Unsaved changes
Login	john_smith
Blocked	
Account validity	Indefinite \$
Role	operator ÷

4. Click Save.

#### **Related topics:**

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

# 7.3 Blocking an account

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

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

Mana	agement	Deactivate selected	l object						🛔 admir	n~ 1	?
		Accounts	+ Add Block	© Unblock	C Timestamp			▼ Add filter ~	Search	0	a
		Accounts									-
		🗆 Name 🔺		Server +		Recording *	Туре	Password change policy	Password changer		
		account_4		10.0.35.1		all	regular	Static, without restrictions	None		
		admin@serwe	ar3	serwer3		all	regular	Static, without restrictions	None		
<i>a</i> A	ccounts	administrator	at RDP-0-10.0.35.54, RD	RDP-0-10.0.35.54, F	DP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None		
		administrator	Øserwer1	serwer1		all	regular	Static, without restrictions	None		_
		administratori	@serwer2	serwer2		all	regular	Static, without restrictions	None		_
		anonymous		SSH-0-10.0.35.52		all	anonymous	None	None		_

4. Optionally, provide blocking reason and click Confirm.

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



# **Related topics:**

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

# 7.4 Unblocking an account

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

Ma	anagement <	Activate selected objects					
M		Accounte + Add © Block OU	nblock 🕆 Delete 🧭 Timestamp			T Add filter ∽	Se
₿		Accounts					
쓭		Name A	Server *	Recording *	Туре	Password change policy	Passw
_		@account_4	10.0.35.1	all	regular	Static, without restrictions	None
		adr Edit account definition	serwer3	all	regular	Static, without restrictions	None
8	Accounts	administrator at RDP-0-10.0.35.54, RD	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None
		administrator@serwer1	serwer1	all	regular	Static, without restrictions	None
	Listeners	administrator@serwer2	serwer2	all	regular	Static, without restrictions	None
		anonymous	SSH-0-10.0.35.52	all	anonymous	None	None
÷-	Password changers	anonymous for RDP-0-10.0.35.54, RDP-0	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	anonymous	None	None
U	Policies	anonymous for RDP-0-TLS-10.0.40.100,	serwer1	all	anonymous	None	None

4. Confirm unblocking selected objects.

Unblock objects	6
Are you sure you want to unblock 1 object?	
Cancel Confirm	)
Confirm unblocking selected objects	

#### **Related topics:**

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

# 7.5 Deleting an account

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

- 1. Select Management > Accounts.
- 2. Find and select desired objects.
- 3. Click Delete.

Ma	anagement <	Fudo					
M	Dashboard	Annour Colored Line Vock ØU	nblock			T Add filter ∽	Se
₿	Sessions	Accour Select objects					
*	Users	Delete selected elements	S Server *	Recording *	Туре	Password change policy	Passw
	Sarvare	@account_4	10.0.35.1	all	regular	Static, without restrictions	None
	Gerrera	admin@serwer3	serwer3	all	regular	Static, without restrictions	None
8	Accounts	administrator at RDP-0-10.0.35.54, RD	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Static, without restrictions	None
•	Safes	administrator@serwer1	serwer1	all	regular	Static, without restrictions	None
2	Listeners	administrator@serwer2	serwer2	all	regular	Static, without restrictions	None
		anonymous	SSH-0-10.0.35.52	all	anonymous	None	None
њ-	Password changers	anonymous for RDP-0-10.0.35.54, RDP-0	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	anonymous	None	None
U	Policies	anonymous for RDP-0-TLS-10.0.40.100,	serwer1	all	anonymous	None	None

4. Confirm deletion of selected objects.

Delete objects	×
Are you sure you want to delete 1 object?	
Cancel	
Confirm deleting selected objects	

# **Related topics:**

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

# chapter 8

Safes

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

Activate s	elected safes			
Deactivate s	elected safes		Delete selected safes	
Management Cr	eate new safe 🛄			Define objects li
I Dashboard	Safas + Add	Block OUnblock		T Add filter - Search
E Sessions	Sales			
쓭 Users	□ Name +	Users	Accounts	
⊖ Servers	adusers	jdoe, kwitaszczyk, mborysiak, mzaborski, tdwornicki		
Accounts	api-robot-safe1			
E Plotoina	api-robot-safe2	1		
Safes	pdrtal Edit s	afe definition st-fudo		
S Listeners	safe - anonymous	anonymous	anonymous@FreeBSD2	
in Libbining	<ul> <li>support</li> </ul>	pdawidek	joe@FreeBSD10 Blocke	ed safe
n- Password changers	testsafe			
C Policies	<ul> <li>whisys</li> </ul>	admin1, pdawidek	admin@windows7, vnc, root@Cent0	DS, root@freebs Hover to view t
📩 Downloads				

Note:

- The system safe can only contain system account.
- The portal safe can only contain the portal account.
- Operator, admin and superadmin users always have access to the system safe.
- User type users cannot have access to the system safe.

# 8.1 Creating a safe

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

- 1. Select Management > Safes.
- 2. Click + Add.

Management Create new	w safe 🗖				
Jashboard	Safas + Add	O Block O Unblock @ Delete		▼ Add filter ~	Search
E Sessions	Sales				
쓭 Users	<ul> <li>Name *</li> </ul>	Users	Accounts		L
🖴 Servers	<ul> <li>adusers</li> </ul>	jdoe, kwitaszczyk, mborysiak, mzaborski, tdwornicki			F
C. Assessed	<ul> <li>api-robot-safe1</li> </ul>				
E Accounts	api-robot-safe2				
Safes	portal	admin1, pdawidek, test-fudo			
> Listener	<ul> <li>safe - anonymous</li> </ul>	anonymous	anonymous@FreeBSD2		5
M Listemers	<ul> <li>support</li> </ul>	pdawidek	joe@FreeBSD10		
- Password changers	<ul> <li>testsafe</li> </ul>				
♥ Policies	<ul> <li>whisys</li> </ul>	admin1, pdawidek	admin@windows7, vnc, root@CentOS	6, root@freebsd10, a	idmin@win2012 \$
🕹 Downloads					

- 3. Enter object's name.
- 4. Select *Blocked* option to disable access to object after it's created.
- 5. Select *Login reason* option, to display prompt upon logging in, asking user to enter login reason.
- 6. Select *Notifications* option and choose notifications sent out to Wheel Fudo PAM administrator.
- 7. Assign security policies in the Policies field.
- 8. In the *Protocol functionality* section, select allowed protocols' features.
- 9. In the *Permissions* section, add users allowed to manage this object.
- 10. In the *Object relations* section, add users allowed to connect to servers using accounts assigned to this safe.
- 11. In the Accounts field, add privileged accounts used to connect to monitored servers.
- 12. In the Listeners field, add listeners used to initiate connections with monitored hosts.
- 13. Click Save.

Management <	Fudo'		
Jashboard	8.6		
E Sessions	Sate		
쓸 Users	General	Unique object name	
⊖ Servers	Name		
Accounts			
Safes	Blocked	Disable access after creating object	
ふ Listeners	Login reason	Ask for login reason	
n- Password changers	Notifications	Session start Session finish	
Policies		Session join Session leave S	/stem events notifi
📥 Downloads	Policies	0 0	
🔒 Reports		Security policies	
■ Productivity	Protocol functionality		
Settings	RDP 💋	Clipboard redirection	
system		Device redirection     Dynamic Virtual Channels     Audio input redirection     Multimedia redirection	
Ø <sup>e</sup> Network configuration		Max. resolution	bwed protocol feat
Notifications	CCU	Seecine     Part forwarding	
C Timestamping	55H <u>6</u>	Terminal     Zenvironment     X11     ZSSL Agent forwarding	
4 External authentication		Shell SCP	
III External passwords repositories	100	Clean Cut Taxt	
Resources	VNC G		
Backups and retention	Permissions	Users allowed to manage this object	
# Cluster	Granted users	0 Q	
≡ Events log	Object relations		
	Users	0 QR	elations with other
3 days i 12345678	Accounts	0 0	
	Listeners	ं ९	
		C Reset Save Save Save object's	definition

# **Related topics:**

- $\bullet \ Data \ model$
- Editing a safe
- Blocking a safe
- Deleting a safe

# 8.2 Editing a safe

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

Management <	Fudo			
Jashboard	Series + Add	O Block O Unblock 🗎 Delete		T Add filter ~ Search
E Sessions	38168			
쓭 Users	○ Name ▲	Users	Accounts	
🖴 Servers	<ul> <li>adusers</li> </ul>	jdoe, kwitaszczyk, mborysiak, mzaborski, tdwornicki	i	
🖉 Accounts	api-robot-safe1			
Safes	portal Edit	safe definition <sup>pst-fudo</sup>		
Lietanare	<ul> <li>safe - anonymous</li> </ul>	a anonymous	anonymous@FreeBSD2	
A Listemera	<ul> <li>support</li> </ul>	pdawidek	joe@FreeBSD10	
n- Password changers	<ul> <li>testsafe</li> </ul>			
<b>V</b> Policies	<ul> <li>whisys</li> </ul>	admin1, pdawidek	admin@windows7, vnc, root@Cent0	S, root@freebsd10, admin@win2012
🛓 Downloads				

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

3. Modify configuration parameters as needed.

**Note:** Unsaved changes are marked with the  $\square$  icon.

General	Unsaved change	es
Login	john_smith	
Blocked		
Account validity	Indefinite	\$
Role	operator	\$

4. Click Save.

#### **Related topics:**

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

# 8.3 Blocking a safe

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

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

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

3. Click Block.

Management <	fudo <sup>*</sup>	🛓 admin 🗸 🤰
	Safee + Add Block © Unblock @ Delete	T Add filter - Search O Q
	Calastabiast	
	Name Select Object Users	Accounts Listeners
	anonymou Block selected elements	anonymous for RDP-0-10.0.35.54, RDP-0- RDP-0-10.0.35.54-ANONYMOUS 10.0.35.54-ANONYMOUS
	anonymous > RDP-0-TLS- 10.0.40.100-ANO	anonymous for RDP-0-TLS-10.0.40.100, RDP-0-TLS-10.0.40.100- RDP-0-TLS-10.0.40.100-ANONYMOUS ANONYMOUS
Safes	anonymous > RDP-0-TLS-NLA- anonymous	anonymous for RDP-0-TLS-NLA- RDP-0-TLS-NLA-10.0.40.101-
	10.0.40.101	10.0.40.101, RDP-0-TLS-NLA- ANONYMOUS 10.0.40.101-ANONYMOUS
n- Password changers	anonymous > RDP-10.0.8.103-	anonymous for RDP-10.0.8.103- RDP-10.0.8.103-

4. Optionally, provide blocking reason and click Confirm.

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

Block of	ojects	×
Reason		
	Provide blocking reason	Cancel Confirm
	Block selected	objects

#### **Related topics:**

- Unblocking a safe
- $\bullet \ Data \ model$
- Creating a safe
- Blocking a safe

# 8.4 Unblocking a safe

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

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

3. Click Unblock.

м	anagement <	Fudo			
-	Dashboard				-
		Safes + Add   Block  Unblock  Delete		▼ Add filter ~	Search
		Name Select object	Accounts	L	steners
8		Activate selected elements	anonymous for RDP-0-10.0.3 0-10.0.35.54-ANONYMOUS	5.54, RDP- R	DP-0-10.0.3
8		anonymous > RDP-0-TLS- anonymous 10.0.40.100-ANO	anonymous for RDP-0-TLS-1 RDP-0-TLS-10.0.40.100-ANC	0.0.40.100, R DNYMOUS A	DP-0-TLS-1 NONYMOU
	Safes	anonymous > RDP-0-TLS-NLA- anonymous	anonymous for RDP-0-TLS-N	ILA- R	DP-0-TLS-N
2	Listeners	10.0.40.101	10.0.40.101, RDP-0-TLS-NLA 10.0.40.101-ANONYMOUS	λ- Α	NONYMOU
ń-	Password changers	anonymous > RDP-10.0.8.103-	anonymous for RDP-10.0.8.1	03- R	DP-10.0.8.1

4. Click *Confirm* to unblock selected objects.

Unblock objects X
Are you sure you want to unblock 1 object?
Cancel
Confirm unblocking selected objects

### **Related topics:**

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

# 8.5 Deleting a safe

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

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

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

3. Click Delete.

М	anagement <	Fudo		
ш	Dashboard	Add O Block O Unblock	▼ Add filter	- Searcl
₿		Salact abject		
*		Name A Users	Accounts	Listeners
8		ANONYMOUS	anonymous for RDP-0-10.0.35.54, RDP-0- 10.0.35.54-ANONYMOUS	RDP-0-10.
8		anonymous > RDP-0-TLS- anonymous 10.0.40.100-ANO	anonymous for RDP-0-TLS-10.0.40.100, RDP-0-TLS-10.0.40.100-ANONYMOUS	RDP-0-TLS ANONYMO
	Safes	anonymous > RDP-0-TLS-NLA- anonymous	anonymous for RDP-0-TLS-NLA-	RDP-0-TLS
2	Listeners	10.0.40.101	10.0.40.101, RDP-0-TLS-NLA- 10.0.40.101-ANONYMOUS	ANONYMO
ń-	Password changers	anonymous > RDP-10.0.8.103-	anonymous for RDP-10.0.8.103-	RDP-10.0.

4. Confirm deletion of selected objects.

Delete objects	×
Are you sure you want to delete 1 object?	
	Cancel Confirm
Confirm deleting selected objects	

### **Related topics:**

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

# CHAPTER 9

# Listeners

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

Activa	te selected listeners		1		
Deactiva	te selected listeners		Delete s	elected listeners	
Management	Create new listener			Def	ine objects li
Jashboard	Listerer	+Add O Block O Unk	block R Delete	T Add filter ~	Search
E Sessions	Listeners				
曫 Users	🗆 Namo 🔺	Safe	s Listen	address Prof	tocol Mc
🖴 Servers		adus	sers, whisys 10.0.8	.60:3389 RDF	P ba
	□ SSH	whis	ys 10.0.8	.160:22 SSI	H ba
Accounts	SSH - And	nymous safe	- anonymous 10.0.8	.60:222 SSI	H pr
Safes		Edit safe definition while	ys 10.0.8	.60:9999 RDI	P ba
N Listerer	<ul> <li>ssh-listen</li> </ul>	br	10.0.8	Blocked listener ssi	H pr
1 Listeners	🕞 vnc	whis	ys 10.0.8	.60:59102 VN	C pri
+ Password changers				Н	over to view t
V Policies					

#### Note:

- A *proxy* type listener can link to only one account to a server with the same protocol through different safes.
- A *bastion* type listener cannot link to an anonymous account on a server with the same protocol as the listener's protocol.
- A listener cannot link to an *anonymous* and a *regular* or *forward* account to the same server with the same protocol as the listener's protocol.
- A listener cannot link to two *regular* or *forward* type accounts to the same server with the same protocol as the listener's protocol, to which a single user has access.

• For a given linked RDP listener and RDP server, both have to use either *Standard RDP Security* or *TLS* or *NLA*.

# 9.1 Creating a listener

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

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

# 9.1.1 Creating a Citrix listener

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

Management Cre	eate new listener				
I Dashboard	Listeners +Add o	Block O Unblock 🔒 Delete	τ/	dd filter - Search	
E Sessions					
쓸 Users	Name +	Safes	Listen address	Protocol	Mc
🔒 Servers	RDP	adusers, whisys	10.0.8.60:3389	RDP	ba
	□ SSH	whisys	10.0.8.160:22	SSH	ba
Accounts	<ul> <li>SSH - Anonymous</li> </ul>	safe - anonymous	10.0.8.60:222	SSH	pro
Safes	rdp2	whisys	10.0.8.60:9999	RDP	ba
S. Listanare	<ul> <li>ssh-listener</li> </ul>		10.0.8.60:666	SSH	pro
	vnc	whisys	10.0.8.60:59102	VNC	pro
Beneficial Angles Password changers					
U Policies					

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

#### gateway

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

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

### proxy

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

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

#### transparent

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

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

#### Related topics:

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

#### 9.1.2 Creating a HTTP listener

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

Management	Create new listener	1			
I Dashboard	Listanar	Add © Block © Unblock @ Dele	te	T Add filter ~ Search	
E Sessions	Listeners				
🔮 Users	🗆 Name 🔺	Safes	Listen address	Protocol	Ma
🔒 Servers	RDP	adusers, whisys	10.0.8.60:3389	RDP	ba
	□ SSH	whisys	10.0.8.160:22	SSH	ba
Accounts	SSH - Anonymo	us safe - anonymous	10.0.8.60:222	SSH	pn
Safes	rdp2	whisys	10.0.8.60:9999	RDP	ba
S. Listeners	ssh-listener		10.0.8.60:666	SSH	pn
7 Listeners	🗆 vnc	whisys	10.0.8.60:59102	VNC	pn
+ Password changers					
<b>V</b> Policies					

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

#### gateway

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

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

#### proxy

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

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

#### transparent

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

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

### 10. Click Save.

#### **Related topics:**

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

# 9.1.3 Creating an ICA listener

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

Management	Create new listener	<b></b>				
Jashboard	Listanor	+Add © Block	O Unblock 🕆 Delete		T Add filter v Search	
E Sessions	Listerier					
쓸 Users	🗆 Name 🔺		Safes	Listen address	Protocol	Mo
A Servers			adusers, whisys	10.0.8.60:3389	RDP	ba
	□ SSH		whisys	10.0.8.160:22	SSH	ba
Accounts	SSH - A	nonymous	safe - anonymous	10.0.8.60:222	SSH	pro
Safes	□ rdp2		whisys	10.0.8.60:9999	RDP	ba
S. Listenare	<ul> <li>ssh-liste</li> </ul>	ner		10.0.8.60:666	SSH	pro
	🗆 vnc		whisys	10.0.8.60:59102	VNC	pro
+ Password changers						
Policies						

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

bastion

**Note:** User connects to the target host by including its name in the login string, e.g. john\_smith#mail\_server.

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

gateway

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

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

proxy

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

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

#### transparent

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

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

#### **Related topics:**

- Data model
- ICA via Citrix StoreFront
- $\bullet$  ICA
- Creating an ICA server
- ICA configuration file

# 9.1.4 Creating a Modbus listener

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

Management	Create new listener				
M Dashboard	Listener +	Add © Block © Unblock @ Del	ete	T Add filter ~ Search	
E Sessions	Listeners				
촬 Users	🗆 Name 🔺	Safes	Listen address	Protocol	Mc
Servers	C RDP	adusers, whisys	10.0.8.60:3389	RDP	ba
	□ SSH	whisys	10.0.8.160:22	SSH	ba
Accounts	SSH - Anonymou	s safe - anonymous	10.0.8.60:222	SSH	pro
Safes	rdp2	whisys	10.0.8.60:9999	RDP	ba
S. Listanore	<ul> <li>ssh-listener</li> </ul>		10.0.8.60:666	SSH	pro
	🗆 vnc	whisys	10.0.8.60:59102	VNC	pro
+ Password changers					
♥ Policies					

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

### gateway

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

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

#### proxy

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

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

#### transparent

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

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

#### **Related topics:**

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

# 9.1.5 Creating a MySQL listener

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

Management	Create new listener				
Jashboard	Listeners + Add	Block     OUnblock     Gelete		Add filter ~ Search	
E Sessions					
촬 Users	□ Name +	Safes	Listen address	Protocol	Mc
Servers		adusers, whisys	10.0.8.60:3389	RDP	ba
	C SSH	whisys	10.0.8.160:22	SSH	ba
Accounts	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	pro
Safes	□ rdp2	whisys	10.0.8.60:9999	RDP	ba
S Listanare	ssh-listener		10.0.8.60:666	SSH	pro
	🗆 vnc	whisys	10.0.8.60:59102	VNC	pro
H- Password changers					
<b>V</b> Policies					

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

#### gateway

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

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

#### proxy

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

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

#### transparent

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

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

#### Related topics:

• Data model

- Editing a listener
- Deleting a listener
- Blocking a listener
- Unblocking a listener

# 9.1.6 Creating an Oracle listener

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

Management C	reate new listener				
I Dashboard	Listeners +Add	Block O Unblock 🔒 Delete	TA	dd filter - Search	
E Sessions					
쓸 Users	<ul> <li>Name +</li> </ul>	Safes	Listen address	Protocol	Mo
🕀 Servers	RDP	adusers, whisys	10.0.8.60:3389	RDP	ba
	SSH	whisys	10.0.8.160:22	SSH	ba
Accounts	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	pro
Safes	rdp2	whisys	10.0.8.60:9999	RDP	ba
> Listeners	<ul> <li>ssh-listener</li> </ul>		10.0.8.60:666	SSH	pro
	vnc	whisys	10.0.8.60:59102	VNC	pro
H- Password changers					
C Policies					

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

### gateway

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

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

#### proxy

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

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

transparent

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

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

### **Related topics:**

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

# 9.1.7 Creating an RDP listener

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

Μ	lanagement	Create ne	w listener						
đ	) Dashboard		Listeners +Add	© Block	O Unblock 🔒 Delete		T Add filter	Search	
€									
-			<ul> <li>Name +</li> </ul>		Safes	Listen address		Protocol	М
e	Servers		RDP		adusers, whisys	10.0.8.60:3389		RDP	ba
			SSH SSH		whisys	10.0.8.160:22		SSH	ba
8	Accounts		<ul> <li>SSH - Anonymous</li> </ul>		safe - anonymous	10.0.8.60:222		SSH	pr
			rdp2		whisys	10.0.8.60:9999		RDP	ba
	Lietonare		<ul> <li>ssh-listener</li> </ul>			10.0.8.60:666		SSH	pr
			o vnc		whisys	10.0.8.60:59102		VNC	pr
*									
U									

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

#### bastion

**Note:** User connects to the target host by including its name in the login string, e.g. john\_smith#mail\_server.

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

#### gateway

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

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

#### proxy

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

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

#### transparent

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

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

### **Related topics:**

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

### 9.1.8 Creating an SSH listener

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

Management	Create new listener					
M Dashboard	Listeners	+ Add O Block	O Unblock 🔋 Delete		T Add filter ~ Search	
E Sessions	Listeners					
쓸 Users	🗆 Name 🔺		Safes	Listen address	Protocol	Mc
Servers	RDP		adusers, whisys	10.0.8.60:3389	RDP	ba
	□ SSH		whisys	10.0.8.160:22	SSH	ba
Accounts	SSH - Anony	mous	safe - anonymous	10.0.8.60:222	SSH	pro
Safes	rdp2		whisys	10.0.8.60:9999	RDP	ba
S Listanare	<ul> <li>ssh-listener</li> </ul>			10.0.8.60:666	SSH	pro
	🗆 vnc		whisys	10.0.8.60:59102	VNC	pro
h- Password changers						
Policies						

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

bastion

**Note:** User connects to the target host by including its name in the login string, e.g. john\_smith#mail\_server.

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

gateway

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

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

proxy

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

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

#### transparent

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

- Select transparent from the *Mode* drop-down list.
- Select the network interface used for handling connections over this listener.
- 6. In the *Fudo public key* field, click the generate certificate icon to generate certificate, or the certificate upload icon to upload a certificate.
- 7. Click Save.

### **Related topics:**

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

# 9.1.9 Creating a MS SQL listener

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

Management	Create new listener					
Jashboard	Listeners	+Add O Block	9 Unblock 🔋 Delete		T Add filter - Search	
E Sessions	Listeners					
쓸 Users	🗆 Name 🔺		Safes	Listen address	Protocol	Mo
Servers	RDP		adusers, whisys	10.0.8.60:3389	RDP	ba
-	SSH		whisys	10.0.8.160:22	SSH	ba
Accounts	SSH - Anon	ymous	safe - anonymous	10.0.8.60:222	SSH	pro
Safes	rdp2		whisys	10.0.8.60:9999	RDP	ba
S Listanare	<ul> <li>ssh-listener</li> </ul>			10.0.8.60:666	SSH	pro
	🗆 vnc		whisys	10.0.8.60:59102	VNC	pro
A-Password changers						
0 Policies						

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

#### gateway

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

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

proxy

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

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

#### transparent

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

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

#### Related topics:

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

# 9.1.10 Creating a Telnet listener

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

Management Create ne	w listener			
Jashboard	Listeners +Add   Block	O Unblock 😑 Delete	▼ Add fil	ter ~ Search
E Sessions				
쓸 Users	□ Name +	Safes	Listen address	Protocol M
🖴 Servers	RDP	adusers, whisys	10.0.8.60:3389	RDP ba
	□ SSH	whisys	10.0.8.160:22	SSH ba
Accounts	<ul> <li>SSH - Anonymous</li> </ul>	safe - anonymous	10.0.8.60:222	SSH pr
Safes	□ rdp2	whisys	10.0.8.60:9999	RDP be
S Listeners	ssh-listener		10.0.8.60:666	SSH pr
	vnc	whisys	10.0.8.60:59102	VNC pr
Password changers				
V Policies				

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

#### gateway

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

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

#### proxy

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

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

#### transparent

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

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

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

### **Related topics:**

- $\bullet \ Data \ model$
- Editing a listener
- Deleting a listener
- Blocking a listener
- Unblocking a listener

# 9.1.11 Creating a Telnet 3270 listener

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

Management	Create new listener					
Jashboard	Listeners	+ Add O Block	O Unblock 🔒 Delete		T Add filter ~ Search	
E Sessions	Listeners					
쑡 Users	🗆 Name 🔺		Safes	Listen address	Protocol	Mc
Servers			adusers, whisys	10.0.8.60:3389	RDP	ba
	□ SSH		whisys	10.0.8.160:22	SSH	ba
Accounts	SSH - Anon	ymous	safe - anonymous	10.0.8.60:222	SSH	pro
Safes	□ rdp2		whisys	10.0.8.60:9999	RDP	ba
ন Listeners	<ul> <li>ssh-listener</li> </ul>			10.0.8.60:666	SSH	pro
	O vnc		whisys	10.0.8.60:59102	VNC	pro
- Password changers						
<b>V</b> Policies						

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

#### gateway

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

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

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

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

#### transparent

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

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

#### **Related topics:**

- $\bullet \ Data \ model$
- Editing a listener
- Deleting a listener
- Blocking a listener
- Unblocking a listener

## 9.1.12 Creating a VNC listener

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

Management	Create new listener				
Jashboard	Listeners +Add	Block O Unblock  Delete	TA	dd filter - Search	
E Sessions					
쓸 Users	Name +	Safes	Listen address	Protocol	Mc
🔒 Servers	RDP	adusers, whisys	10.0.8.60:3389	RDP	ba
	C SSH	whisys	10.0.8.160:22	SSH	ba
Accounts	<ul> <li>SSH - Anonymous</li> </ul>	safe - anonymous	10.0.8.60:222	SSH	pro
Safes	rdp2	whisys	10.0.8.60:9999	RDP	ba
S Listeners	ssh-listener		10.0.8.60:666	SSH	pro
	🗆 vnc	whisys	10.0.8.60:59102	VNC	pro
- Password changers					
Policies					

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

#### bastion

**Note:** User connects to the target host by including its name in the login string, e.g. john\_smith#mail\_server.

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

#### gateway

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

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

#### proxy

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

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

transparent

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

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

## **Related topics:**

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

## 9.2 Editing a listener

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

Management	Fudo							
I Dashboard	Listeners	+ Add	© Block	O Unblock	🕆 Delete		T Add filter ∨	Search
E Sessions	Listeners							
쓸 Users	🗆 Name +			Safes		Listen address	Prot	tocol M
🖴 Servers	RDP			adusers, wh	nisys	10.0.8.60:3389	RDF	P ba
	SSH			whisys		10.0.8.160:22	SSF	H ba
Accounts	SSH - Anony	mous		safe - anon	ymous	10.0.8.60:222	SS	l pr
Safes	rdp2	dit obje	ct	whisys		10.0.8.60:9999	RDF	p ba
> Listenare	ssh-listener					10.0.8.60:666	SSF	H pr
A Listeners	vnc			whisys		10.0.8.60:59102	VNC	C pr
+ Password changers								
10 Policies								

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

3. Modify configuration values as needed.

Note: Unsaved changes are marked with an icon.

General	Unsaved changes
Login	john_smith
Blocked	
Account validity	Indefinite \$
Role	operator

4. Click Save.

## **Related topics:**

- Data model
- System initiation
- Servers

## 9.3 Blocking a listener

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

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

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

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

м	anagement <	Fudo		
	Dashboard	Listeners + Add Block	O Unblock B Delete	T Add filter ~ Search
₿		Select objects		
*			Safes	Listen addres
	Servers	2 10.0.40.50:90 Block selected o	bjects 2	10.0.40.50:9
		10.0.40.50:9999	http	10.0.40.50:9
₽	Accounts	Listner-10.0.40.50:8000	test-safe-1	10.0.40.50:8
		MYSQL-0-10.0.35.52	db-0 > MYSQL-0-10.0.35.52	10.0.40.50:3
2	Listeners	ORACLE-10.0.40.149	db-0 > ORACLE-10.0.40.149	10.0.40.50:1
		RDP-0-10.0.35.54	rdp-podmiana-0 > RDP-0-10.0.35.54	10.0.40.50:1
- 19-	Password changers	RDP-0-10.0.35.54-ANONYMOUS	anonymous > RDP-0-10.0.35.54-ANONYMOUS	10.0.40.50:2

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

#### **Related topics:**

- Data model
- System initiation

• Servers

## 9.4 Unblocking a listener

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

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

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

м	anagement <	Fudo		
	Dashboard	Listeners + Add OBlock	O Unblock 🔒 Delete	T Add filter ~ Search
₿		Select objects		
*	Users	Name Name Black selected o	Safes	Listen addres
8		0 10.0.40.50:90 DIOCK Selected 0	bjects 2	10.0.40.50:9
		0 10.0.40.50(9999	http	10.0.40.50:9
-	Accounts	<ul> <li>Listner-10.0.40.50:8000</li> </ul>	test-safe-1	10.0.40.50:8
		MYSQL-0-10.0.35.52	db-0 > MYSQL-0-10.0.35.52	10.0.40.50:3
	Listeners	<ul> <li>ORACLE-10.0.40.149</li> </ul>	db-0 > ORACLE-10.0.40.149	10.0.40.50:1
	Decement	RDP-0-10.0.35.54	rdp-podmiana-0 > RDP-0-10.0.35.54	10.0.40.50:1
- 10-	Password changers	RDP-0-10.0.35.54-ANONYMOUS	anonymous > RDP-0-10.0.35.54-ANONYMOUS	10.0.40.50:2

4. Click *Confirm* to unblock selected objects.

Unblock objects	×
Are you sure you want to unblock 1 object?	
	Cancel Confirm
Confirm unblocking selected o	objects

## **Related topics:**

- Data model
- System initiation
- $\bullet \ Servers$

## 9.5 Deleting a listener

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

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

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

3. Click Delete.

м	anagement <	Fudo	
	Dashboard	Listenars + Add • Block © Unblock	T Add filter ~ Search
₿		Calest abiasta	
*		Name Select Objects Safes	Listen addres
	Servers	Opto.o. Delete selected objects st-safe-2	10.0.40.50:9
		10.0.40.50:9999 http	10.0.40.50:9
8	Accounts	Listner-10.0.40.50:8000 test-safe-1	10.0.40.50:8
		□ MYSQL-0-10.0.35.52 db-0 > MYSQL-0-10.0.35.52	10.0.40.50:3
	Listeners	ORACLE-10.0.40.149 db-0 > ORACLE-10.0.40.149	10.0.40.50:1
		RDP-0-10.0.35.54 rdp-podmiana-0 > RDP-0-10.0.35.54	10.0.40.50:1
÷.	Password changers	RDP-0-10.0.35.54-ANONYMOUS anonymous > RDP-0-10.0.35.54-ANONYMOUS	10.0.40.50:2

4. Confirm deleting selected objects.

Delete objects	×
Are you sure you want to delete 1 object?	
Са	ncel Confirm
Confirm deleting selected objects	

## Related topics:

- Data model
- System initiation
- Servers

# chapter 10

Password changers

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

- Unix over SSH
- $\bullet\,$  MySQL over SSH
- Cisco over SSH and Telnet
- Cisco Enable Password over SSH and Telnet
- MS Windows over WMI

# 10.1 Password changer policy

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

## Defining a password changer policy

- 1. Select Management > Password changers.
- 2. Click + Add.
- 3. Enter object name.

- 4. Select the *Password change enabled* option and specify the time interval between each password change.
- 5. Select the *Password verification enabled* option and specify the time interval between each password verification.
- 6. Define password complexity.

Parameter	Description				
Length	Provide the number of characters comprising the password.				
Small letters	Select to include lowercase characters, define their minimal				
	number.				
Capital letters	Select to include uppercase characters, define their minimal				
	number.				
Special characters	Select to include special characters, define their minimal num-				
	ber.				
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.

Management <	Fudo <sup>*</sup>
Jul Dashboard	Dallay
E Sessions	Policy
볼 Users	General Unique object name
🖴 Servers	Name
Accounts	
Safes	Password change enabled 2 10 minutes Define now freque
ħ Listeners	Password verification enabled 2 2 5 minutes
A- Password changers	Defin
Policies	Password requirements the password
🛓 Downloads	Define passwords complexity
🔒 Reports	Length Z 20
■ Productivity	Small letters 2 2 5
Settings	Capital letters 2 5 5
🖕 System	Special characters 2 2 6
O Network configuration	
Notifications	bigns ( 4
@ Timestamping	
Re External authentication	C Reset Save Object

#### Editing a password changer policy

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

Note: Unsaved changes are marked with an icon.

General	Unsaved	changes	
Login	john_smith		
Blocked			
Account validity	Indefinite		\$
Role	operator		\$

4. Click Save.

## Deleting a password changer policy

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

# 10.2 Custom password changers

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

## Defining a custom password changer

- 1. Select Management > Password changers.
- 2. Select *Custom changers* tab.

- 3. Click + Add.
- 4. Define the password changer's name.
- 5. Click + to add a command.
- 6. Enter command.

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

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

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

10. Click Save.

## Editing a custom password changer

- 1. Select Management > Password changers.
- 2. Select *Custom changers* tab.
- 3. Click the name of desired password changer.
- 4. Edit selected commands.
- 5. Click X to remove selected command.
- 6. Click Save.

## Deleting a custom password changer

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

## Related topics:

- Data model
- System initiation
- Servers

# CHAPTER 11

Policies

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

## **Defining patterns**

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

Management <	Fudo		👗 admin 🗸 🤶
M Dashboard	Policies Regular expr	essions - Select patterns settings tab	
E Sessions			
쑵 Users	Name	delete all	
⊖ Servers	Regular expression	rm -Rf	
•# Bastions	Delete		
open policies configurat	ion page Name	assasinate all	
V Policies	Regular expression	kilal	
La Downloads	Delete	0	
🖨 Reports			
■ Productivity			
Settings			
😂 System			
Q <sup>o</sup> Network configuration			
Notifications		A	dd pattern definition
C Timestamping		C Reset Save	+ Add regular expression

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

Note: Patterns can be defined as regular expressions.

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

- 6. Repeat steps 3-5 to define additional patterns.
- 7. Click Save.

Management <	≓udo'	🛔 admin 🐇 💡
M Dashboard	Policies Popular everencions	
E Sessions	Policies negular expressions	
쓭 Users	Name delete all	
⊖ Servers	Regular expression rm -Rf	
•# Bastions	Delete 🗆	
+ Connections	Name assasinate all	
V Policies	Regular expression killali	
🕹 Downloads	Delete  Enter name of the pattern	
🔒 Reports	Name	
■ Productivity	Regular expression	
Settings		
🖨 System	Delete	
¢ <sup>e</sup> Network configuration		
☑ Notifications	Save changes	
C Timestamping	C Reset Save + Add regular e	xpression

## Note: Regular expressions examples

 $Command \ {\tt rm}$ 

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

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

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

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

## **Defining policies**

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

Management <	Fudo								🛓 admin 🗸 🤶
M Dashboard	Policies	Regular evo	ressions						
E Sessions	Folicies	negulai expi	Costona						
쓸 Users		Name	polityka		п	13	۰	×	]
🖴 Servers	Regu	lar expression	delete all assasinate all				0	Q	]
•@ Bastions									
+ Come Open policies configu	ration page								
1 Policies									
🕹 Downloads									
🔒 Reports									
E Productivity									
Settings									
🖕 System									
Ø <sup>e</sup> Network configuration									
☑ Notifications									Create new policy
C Timestamping			CR	eset 🗸 🤄	Save				+ Add policy

- 3. Enter policy name.
- 4. Select actions.

$\sim$	Send email notification to system administrator.
	Pause connection.
55	Terminate connection.
•	Block user.

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

- 5. Select monitored patterns.
- 6. Click Save.

Management <	Fudo	🛔 admin 🐇 🤶 📍
I Dashboard	Policies Begular expressions	
E Sessions		
쓭 Users	Name polityka 🛛 🖬 🖏 🗢 🗙	
⊖ Servers	Regular exp Define policy name	
📲 Bastions	Name Z II S O ×	
+‡+ Connections	Regular expression 0 Q	
Policies	Select patterns to be monitored by given policy	
📥 Downloads		
🖨 Reports		
■ Productivity		
Settings		
😂 System		
¢ <sup>e</sup> Network configuration		
Notifications	Save changes	
C Timestamping	2 Reset Save	Add policy

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

## Deleting patterns

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

Management <	Fudo'	👗 admin 🕤 📍
M Dashboard	Delleien Begular everansiene	
E Sessions	Policies regular expressions	
쓭 Users	Name delete all	
⊖ Servers	Regular expression rm -Rf	
•# Bastions	Delete 🗆	
+ Connections	Name assasinate all	
0 Policies	Regular expression killall	
📥 Downloads	Delete	
🕀 Reports	Select to delete given pattern	
E Productivity		
Settings		
🖨 System		
¢° Network configuration		
☑ Notifications	Save changes	
C Timestamping	C Reset Save + Add regular	expression

## **Deleting policies**

To delete policy definition, proceed as follows.

- 1. Select Management > Policies.
- 2. Find desired policy definition and select corresponding Delete option.
- 3. Click Save.

Management <	Fudo										📥 adm	in 🕤 ?
💷 Dashboard	Delicies	Degular ave										
E Sessions	Policies	Regular exp	Select option t	o delete	give	n po	olicy	)—	1			
알 Users		Name	polityka			ш	5	• (	×			
🖴 Servers	Regu	lar expression	delete all assasinate a	al I				0	Q			
• Bastions												
🕂 con Open policies configura	ation page											
0 Policies												
🕹 Downloads												
🖨 Reports												
E Productivity												
Settings												
😂 System												
Ø Network configuration												
☑ Notifications	Save changes											
C Timestamping	C Reset Save + Add policy											

## Related topics:

- Terminating connection
- Notifications
- Accounts
- Security

# CHAPTER 12

Sessions

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

Sessions management page allows filtering stored user sessions, accessing current users connections and downloading stored sessions. It also provides status information on each session and enables access to session sharing options.

lcon	Description
	Start session playback (applicable to sessions with the entire traffic
	recording option selected in connection properties).
Ø	Icon indicating that session has been timestamped.
•	Purpose why the user has connected to the server.
•	Session has been commented.
5	Session has been processed for full-text search purposes.
C	Access session sharing management options.
*	Download session material i selected file format (applicable to ses-
	sions with either complete or raw traffic recording option selected in
	connection properties).
	User activity monitor (applicable to live sessions).

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

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

OCR selec	ted sessions												
Management Show current	connections -								Define	filtering o	ptions	?	
M Dashboard		Delete BOCB	Timestamp		report		6	Add filter		arch		0.~	
E Sessions	Sessions			C achierate			C		<b>)</b> "		Ű	~	-
₩ Users	Timestamp sel	ected sessions	Server	Account	Safe	Started at *	Finished at	Duration	Activity	Size			
	Generate sessi	ons report	citrix	ica-anon	citrix-anon	2017-02-16 16:51	2017-02-17 07:52	15:00:42	0%	131.0 KB		104	Ł
La Servers	□ ► anonymous	ICA	citrix	ica-anon	citrix-anon	2017-02-16 16:49	2017-02-16 16:51	0:02:24	42%	792.0 KB		- 11 A	Ł
Accounts	Danonymous	ICA	citrix	ica-anon	citrix-anon	2017-02-16 16:46	2017-02-16 16:46	0:00:04	0%	83.0 KB	- 95	- C 4	£.
A Listeners	De anor Start	session playback	citrix	ica-anon	citrix-anon	2017-02-16 16:45	2017-02-16 16:46	0:00:05	0%	123.0 KB		004	9
Safes	anonymous	ICA	citrix	ica-anon	citrix-anon	2017-02-16 16:43	2017-02-16 16:45	0:02: S	ession	status io	ons –	4	Ł.
+ Decovered abarran	Iser1	ICA	citrix	ica-reg	citrix2	2017-02-16 16:37	2017-02-16 16:37	0:00:03	0%	5.0 ND	2.0	- 11 đ	£.
n- Password changers	Iser1	ICA	citrix	ica-reg	citrix2	2017-02-16 15:16	2017-02-16 15:16	0:00:12	0%	31.0 KB		- C 4	£.
Policies	Anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:13	2017-02-16 15:14	0:00:29	0%	1.0 KB		4	£.
📥 Downloads	Anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:05	2017-02-16 15:05	0:00:11	0%	44.0 KB		4	£.
A Reports	Image:	ICA	citrix	ica-anon	citrix2	2017-02-16 15:04	2017-02-16 15:04	0:00:19	100%	250.0 KB		4	ŝ.
	anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:03	2017-02-16 15:03	0:00:11	0%	31.0 KB		- C 4	£.
E Productivity	Anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:02	2017-02-16 15:02	0:00:11	0%	67.0 KB		4	<u>t</u>
Settings	anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 14:58	2017-02-16 14:58	0:00:12	0%	29.0 KB		- C 4	Ł.
😂 System	anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 14:58	2017-02-16 14:58	0:00:12	0%	62.0 KB		- C 4	Ł
6°. Network configuration	anonymous	Citrix StoreFront (HTTP)	storefront	sf-anon	citrix2	2017-02-16 14:20	2017-02-16 14:39	0:18:29	0%	144.0 KB		5 J	Ł
	anonymous	Citrix StoreFront (HTTP)	storefront	sf-anon	citrix2	2017-02-16 14:20	2017-02-16 14:20	0:00:01	0%	22.0 KB		5 . 7	Ł
☑ Notifications	Anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:31	2017-02-16 12:31	0:00:00	0%	1.0 KB		- C 4	Ł
C Timestamping	anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:30	2017-02-16 12:30	0:00:00	0%	1.0 KB		5 C 4	<u>k</u>
A External authentication	Anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:30	2017-02-16 12:30	0:00:00	0%	1.0 KB		- C 4	Ł
III Externel pessuorde modeltaries	anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:28	2017-02-16 12:28	0:00:00	0%	1.0 KB		4	<u>.</u>
External passwords repositories	anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:24	2017-02-16 12:24	0:00:00	0%	1.0 KB		- C 4	<u>-</u>
Resources	anonymous	Citrix StoreFront (HTTP)	storefront	sf-anon	citrix2	2017-02-16 12:21	2017-02-16 12:48	0:26:47	0%	17.0 KB		5 2	5
Backups and retention	■ ► ad-user10	Citrix StoreFront (HTTP)	storefront	sf-forward	citrix	2017-02-16 12:02	2017-02-16 12:15	0:12:51	0%	20.0 KB		5 3	<u>-</u>
击 Cluster	Administrator	RDP	rdp1.endpoint	Forward	Hdp	2017-02-14 14:23	2017-02-14 14:24	0:00:02	0%	226.0 KB	0	4	5
	■ ► ad-user10	RDP	rdp1.endpoint	Forward	Нар	2017-02-14 14:20	2017-02-14 14:20	0:00:05	0%	164.0 KB			
LUAP synchronization	ad-user10	RDP	rdp1.endpoint	Forward	Rdp	2017-02-14 14:17	2017-02-14 14:18	0:00:56	100%	242.0 KB		9 4	5
6:31:04.052877 i 10023610 % 3-33526 .‰ Not configured													

# 12.1 Filtering sessions

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

## 12.1.1 Defining filters

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

Management		F۱	udo"										📥 adr	nin 🕤 📍
M Dashboard		Se	Select des	ired fi	ltering	paramet	er	¥ Add filter ∨	🔒 Gener	ate report	Sea	rch	0	Q.~
E Sessions	E.							By protocol						
쓭 Users			User	Server	Protocol	Connection	St	By user	d at	Duration	Activity	Size		
⊖ Servers		⋼▶	Mickey Mouse	fudo4	SSH	ssh	20	By server	7-16 08:01	0:00:00	0%	16.0 KB		> :: ±
-C Rastions		⊳►	Mickey Mouse	fudo4	SSH	ssh	20	By organization	7-16 08:01	0:00:00	0%	15.0 KB		r :: ₹
•g basuons			<ul> <li>Mickey Mouse</li> </ul>	fudo4	SSH	ssh	20	From date	7-16 08:01	0:00:00	0%	15.0 KB		⊧∷ ±
++ Connections								OCR						
Policies														

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

< Fudo"	🛓 admin 🗸 🤶 📍
	T Add filter → ⊖ Generate report Search ◎ Q →
Enter a string of characters to limit the number of objects	s on the list
Select all objects By user	Remove all objects
Mickey Mouse Spiderman	
User Server Protoc Winnie the Pooh	n Activity Size
D ► Mickey Mouse fudo4 SSH anonymous jan_kowalski	) 0% 16.0 KB 🗩 🛸
Mickey Mouse fudo4 SSH     Mickey Mouse fudo4 SSH     SH     Sh     Choo	be objects for the selected filtering parameter
	Fudo <sup>•</sup> Enter a string of characters to limit the number of objects Select all objects By user Mickey Mouse Spiderman Winnie the Pooh anonymous anonymous anonymous anonymous anonymous anonymous b Mickey Mouse fudo4 SSH

**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.

Management	<	Fudo								📤 ad	min ~ '	?
Jashboard		Casalana			G OCR		T Add filter ~	Generate repor	t Search	0	Qv	
E Sessions		Sessions										٦
출 Users			в	y user 🚺	Alickey Mouse	Enter	a user nam	e, a role or an	organizatior	n unit		
🖴 Servers					user			T	8			
📲 Bastions	Select	a previously	added ob	iect to	Mickey Mouse) Spide†man							-
++ Connections	remove	e it from the f	iltering list		Winnie the Pooh				vity Size			

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

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

Management <	Fudo	🔺 admin 🗸 🧳						
Dashboard	Sessions ul Active 🖹 Delete 🖾 OCR 🕇 Add	d filter ~ 🔒 Generate report Search O Q ~						
E Sessions		A A						
챨 Users	By user Mickey Mouse Spideman Wine the Pool Q X							
⊖ Servers	By server MySQL with SSH O Q X							
•# Bastions	Filter nam The filtering mechanism allows for adding multiple							
+ Connections	objects t	to the selected filtering parameter						

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

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

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

Management	<	Fudo								🏝 admi	in ~ ?
Jashboard		Consigns	d Active	🕆 Del	iete 🗔	OCR	▼ Add filter ~	Generate report	Search	0	۹v
E Sessions		Sessions				(	✓ By protocol		-		-
랼 Users			By pro	otocol			By user	ଁ ପ୍	×		
🖴 Servers					Filter na	ıme	By serve Click to	remove the give	n filtering pa	aramter	
•# Bastions							By organization From date				
+ Connections		User	Server Pro	iocol Ca	onnection	Started at 🛩	To date	Duration Ac	tivity Size		
			Audat CO		-	0015 07 0	OCR	0.00.0E 1/	2010		

## 12.1.2 Full text search

Wheel Fudo PAM enables searching stored data to limit the number of elements on the sessions list only to those containing the specified phrase.

Management <	F	udo'								👗 admi	n~ ?
	Se	essions	.al A	ctive	Delete	OCR	▼ Add filter ~	Generate report	Search		Q.~)
E Sessions						Find sessions	containing s	pecified string	of characters		
쓭 Users		User	Server	Protocol	Connection	Started at *	Finished at	Define s	earch options =		
		▶ a	fudo	SSH	ssh	2015-07-21 13:32	2015-07-21 13:3	12 0.00.00			± .
		▶ a	fudo	SSH	ssh	2015-07-21 13:30	2015-07-21 13:3	2 0:01:47 5	6% 34.0 KB	<b>-</b>	- ±
		▶ a	fudo	SSH	ssh	2015-07-21 13:30	2015-07-21 13:3	0 0:00:05 1	00% 14.0 KB	<b>-</b> -	±
+ Connections		▶ a	fudo	SSH	ssh	2015-07-21 13:28	2015-07-21 13:2	9 0:00:07 1	00% 14.0 KB	<b>- -</b>	4

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

The player allows for skipping between each occurrence of the specified phrase.

000	Session 848388532111147062		H <sub>N</sub>
& https://10.0.40.50/sessions/8483885321111470	62/?q=11		
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994 The Regents of the University of California.	ta reserved.		
FreeDSD 8.3-RELEASE (GENERIC) #0: Mon Apr 9 21:23:18 UTC 2012			
Welcome to FreeBGDI			
Before seeking technical support, please use the foreving res	OLECES :		
<ul> <li>Security advisories and updated errats information for all at http://www.freeMSD.org/releases/ - always consult the EM for your release first as it's updated frequently.</li> </ul>	releases are SATA section		
<ul> <li>The Handbook and FAQ documents are at http://www.FreeBSD.or along with the mailing lists, can be searched by going to http://www.FreeBSD.org/search/. If the doc distribution ha been installed, they're also available formatted in /usr/ah</li> </ul>	g/ and, a are/doc.		
if yow still have a question or problem, plasse take the outpop 'uname -a', along with any relevant error messages, and email as a question to the questionsfromStorey mailing list. If y unfamiliar with freeMSU's directory layout, plasse refer to the manual page. If you are not familiar with manual pages, type	t of it ou are e hier(7) man man .		
Too may also use syminate (3) to re-enter the installation an configuration untility. Edit /etc/motd to change this login an fbed83-cert 1	d mousement.		
The search phrase is	highlighted		
Skip to the p	previous occurrence		
Skip to the r	next occurrence		
► > >> & Q Q Q C 00:00:10		00:00:25 0 Info @ Details	년 Share 🖌
00:00:00	00:00:10	00:00:15	
	1 (mbus)	1 Instant	
	- Level	, hannit	

## 12.1.3 Managing user defined filter definitions

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

## Storing a user defined filter definition

- 1. Define filtering options as described in the *Filtering sessions* section.
- 2. Provide the name for the filter definition.
- 3. Click the save icon to store the filter definition.

Management <	Fudo							🕹 adn	nin ~ 🤉
	Sessions	l Active	🕆 Delete	C OCR	▼ Add filter ~	Generate report	Search	0	۹×
E Sessions	000010110								_
🖀 Users		By prot	locol	SH	Provide the name	for the filtering d	efinition		
			my	/_very_own_filt	er		×		
					Store the filte	ering definition –			

## Editing a user defined filter definition

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

Management	<	Fudo										📥 adr	nin ~	?
Jul Dashboard		Sessions	.al Activ	ve 🗄	Delete	G OCR	¥ Add filter ∽	a g	enerate repo	ort	Search	0	Q	~
E Sessions		000010110					By protocol							
Users		User	Server I	Protocol	Connectio	on Started at -	By user By connection		Duration	Activi	ty Size			
🖴 Servers		🗆 🕨 admin	fudo4 8	SSH	ssh	2015-07-2	By server	)6:52	0:00:05	100%	7.0 KB		e li v	÷
		🗆 🕨 admin	fudo4	SSH	ssh	2015-07-1	By organization	08:01	0:00:00	0%	16.0 KB		8 U 7	*
• Bastions		🗆 🕨 admin	fudo4 3	SSH	ssh	2015-07-1	From date	38:01	0:00:00	0%	15.0 KB		e the	±
+ Connections		🗆 🕨 admin	fudo4 3	SSH	ssh	2015-07-1	To date	38:01	0:00:00	0%	15.0 KB		e the	±
E Delining		🗆 🕨 admin	fudo4	SSH	ssh	2015-07-1	OCR	38:01	0:00:00	0%	18.0 KB		e tra	±
V Policies		🗆 🕨 admin	fudo4 s	SSH	ssh	2015-07-1	my_very_own_filter	08:01	0:00:00	0%	15.0 KB		e ti a	±
🛓 Downloads		□ ► admin	fudo4 S	Select o	desired	l filterina de	finition 2015-07-16	08:01	0:00:00	0%	15.0 KB		e Dia	±

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

## Deleting a user defined filter definition

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

Management <	Fudo									📥 adr	nin 🕤 📍
Je Dashboard	Secolone	I Active		G OCR	¥ Add filter ∨	⊖ Ge	nerate repo	rt s	earch	0	Q.~
E Sessions	365510115				By protocol	-					
曫 Users	User User	Server Protoc	ol Connecti	ion Started at -	By user		Duration	Activity	Size		
🖴 Servers	🗆 🕨 admin	fudo4 SSH	ssh	2015-07-2	By server	)6:52	0:00:05	100%	7.0 KB		4 11 ±
	🗆 🕨 admin	fudo4 SSH	ssh	2015-07-1	By organization	)8:01	0:00:00	0%	16.0 KB		> ∷ ±
+∉ Bastions	admin	fudo4 SSH	ssh	2015-07-1	From date	38:01	0:00:00	0%	15.0 KB		4 H A
++ Connections	🗆 🕨 admin	fudo4 SSH	ssh	2015-07-1	To date	38:01	0:00:00	0%	15.0 KB		e 🗆 🛎
R Delision	admin	fudo4 SSH	ssh	2015-07-1	OCR	38:01	0:00:00	0%	18.0 KB		きじ 出
U Policies	🗆 🕨 admin	fudo4 SSH	ssh	2015-07-1	my_very_own_filter	38:01	0:00:00	0%	15.0 KB		e li A
🛓 Downloads	admin	<sup>fudo4</sup> Selec	t desired	l filterina de	finition 2015-07-16	08:01	0:00:00	0%	15.0 KB		4 日本

2. Click the delete icon to remove the filtering definition.

Management <	Fudo							🛔 admin <  ?
Jashboard	Gassions	l Active		G OCR	▼ Add filter ~	Generate report	Search	0 Q~
E Sessions	Sessions							
🔮 Users		By protoc	col	SH		© @	×	
⊖ Servers			m	y_very_own_filter				
					Delet	e filterina definitio	on	

3. Confirm deleting the selected filtering definition.

## **Related topics:**

- System overview
- Reports

# 12.2 Viewing sessions

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

To view a session, proceed as follows.

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

## Session player options

Note: Some options are available for live sessions only.

000	See	<b>ココ 周</b>
R https://10.0.8.64/soc	Session 68/194/604880/088	23 <u>M</u>
<b>X</b> mups.//10.0.8.04/ses	510115/06/194/004880/08825/	
Last login: Tue Oc root@marcin-fudo:~	t 7 08:38:17 2014 from 10.0.1.1 # Play recorded session Fast forward x2	3 Skip to the current live session activities
	Fast forward x4	Display information on current session
	Skip to next user action	Display detailed timeline with user's activities
U Terminate Pause (+ Jo	zin	D1:16:27 Info Details IP Share C Scale window to session native resolution re view!
	Pause session Terminate session Torminate session	01:16:25

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

The player enables skipping between each occurrence of the specified phrase.



**Note:** Click the displayed elapsed time to switch between the connections's actual and relative time.



## **Related topics:**

• Sensitive features

## 12.3 Viewing live sessions

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

- 1. Select Management > Sessions.
- 2. Click Add filter and select Active.
- 3. Select Yes from the drop-down list.
- 4. Find desired session and click the play icon to start playback.

## **Related topics:**

- Viewing sessions
- Terminating connection

# 12.4 Pausing connection

In case a current user action requires analysis, the connection to the server can be paused.

**Note:** Pausing connection temporarily suspends data transmission. After resuming connection, buffered user's actions are forwarded to the server.

- 1. Select *Management* > *Sessions*.
- 2. Click Add filter and select Active.
- 3. Select Yes from the drop-down list.
- 4. Find desired session and and click the play icon to start playback.
- 5. Click Pause.



## **Related topics:**

- Replaying session
- Joining session
- Filtering session

# 12.5 Terminating connection

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

**Note:** Wheel Fudo PAM can automatically block user account upon detecting a defined pattern. For more information refer to *Policies*.

- 1. Select *Management* > *Sessions*.
- 2. Click Add filter and select Active.
- 3. Select Yes from the drop-down list.
- 4. Find desired session and click the playback icon to start playback.
- 5. Click Terminate.

Note: Terminating connection automatically blocks given user.



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

## **Related topics:**

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

# 12.6 Joining live session

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

To join currently established session, proceed as follows.

- 1. Select Management > Sessions.
- 2. Click Add filter and select Active.
- 3. Select Yes from the drop-down list.
- 4. Find desired session and and click the play icon to start playback.
- 5. Click Join.



## **Related topics:**

- Replaying sessions
- Sharing sessions
- Filtering sessions

# 12.7 Sharing sessions

Wheel Fudo PAM enables sharing given session with another user.

## Sharing a session

To share a session, proceed as follows.

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

De admin	win-2003	RDP	rdp-podmiana	07.11.2014 11:28	07.11.2014 15:11	3:43:43	4%	10.0 MB	● <b>&gt; 5</b> BC ±
Open	session play	/er							

3. Click Share.

0	00			Se	ssion 6	719237	190812	96898				R <sub>M</sub>
	https:	//10.0	.8.63/apps	/play/67	719237	190812	296898	8/				
Welc	ome to 1	reeBSD										
Befo	re seek	ng tech	nical support	, please	use the	followin	g resou	rces:				
o S a f	ecurity t http: or your	advisor /ww.Fr release	ies and updat eeBSD.org/rel first as it'	ed errata eases/ - s updated	informa always c frequer	tion for consult t	all re he ERRA	leases ar TA sectio	n n			
0 T a h (2 i	he Handl long with ttp://w or fetcl -letter n /usr/:	wook and the m w.Free led via languag local/sh	I FAQ document mailing lists, SSD.org/search pkg_add -r la ge code, e.g. mare/doc/freeb	s are at can be s /. If th ng-freebs en), they sd.	http://w earched e doc pa d-doc, w are als	ww.FreeB by going ackage ha where lan so availa	SD.org/ to s been : g is the ble for	and, installed a matted	l			
If y `una as a unfa manu	ou stil me -a', questio miliar al page	have a along w on to th with Free If yo	question or with any relevue questions@F eeBSD's direct ou are not fam	problem, ant error reeBSD.or ory layou iliar wit	please t message g mailir t, pleas h manual	take the es, and e og list. se refer l pages,	output o mail it If you to the l type `m	are hier(7) an man'.				
Bdit	/etc/m	td to o	hange this lo	gin annou	ncement.							
fbad	9-radiu	# c		<b>.</b>								
									_			
									S	hare session -		
►	»	»» K	> 00:04:15				0	0:00:09	<b>6</b> Info	Oetails     Oetails     O	🕈 Share	) 2
Ċ	Termina	ate P	ause 🔹 Joi	n							Live	e View!
	00:04:	10			C	0:04:15				00:04:2	0	
						c d		ls		mk dir	G	d
_												

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
Close Share
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	s sessior	n sharing op	utions

3. Click the *revoke* icon to deactivate given URL.

Session shari	ing manager	nent	Add filter ~	Generate r
URL	Valid from	Valid to URL has ex	pired 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	0
			Revoke the URL	
				Close

## **Related topics:**

- Replaying sessions
- Joining sessions
- Filtering sessions

# 12.8 Commenting sessions

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

## Adding a comment

- 1. Select Management > Sessions.
- 2. Find desired session and click the playback icon to start playback.
- 3. Click Details.
- 4. Click the lower part of the timeline to add a comment.
- 5. Define time interval which applies to this comment.

Note: Click and drag either side of the tag to change the starting/ending time.

- 6. Add comment.
- 7. Click Submit.



## Editing a comment

- 1. Select *Management* > *Sessions*.
- 2. Find desired session and click the playback icon to start playback.
- 3. Click Details.
- 4. Find and click desired comment.
- 5. Click the edit icon.
- 6. Change the comment and *Submit*.

## Deleting a comment

- 1. Select Management > Sessions.
- 2. Find desired session and click the playback icon to start playback.
- 3. Click Details.
- 4. Find and click desired comment.

- 5. Click the trashcan icon.
- 6. Click *Delete* to delete the comment.

Edit comment Delete comment
0:02:26 - 0:02:31
#tag2
admin 2014-12-30 14:18
reply
Add a reply 2014-12-30 14:20 Delete reply Edit replay
Reply 🖘
#tag2

#### Replying to a comment

- 1. Select *Management* > *Sessions*.
- 2. Find desired session and click the playback icon to start playback.
- 3. Click Details.
- 4. Find and click desired comment.
- 5. Click Reply.
- 6. Enter message and click *Submit*.

## **Related topics:**

• Sensitive features

## 12.9 Exporting sessions

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

To export a session, proceed as follows.

- 1. Select Management > Sessions.
- 2. Find desired session and click the session export icon.

Management	۲	Fudo <sup>®</sup>										🕹 admin
		Sessions	.al Active	🖹 Delete	CCR			▼ Add filter ~	Generate report	Search		0 0
E Sessions		000010110					_					_
		User User	Server			Protoco	Connec Click	to access s	ession conversio	n and dowi	nload option	ns —
Servers		anonymo	us RDP-10.0.	8.103-		RDP	anonymous	2016-01-11	12:31 2016-01-11 13:37	1:06:24 8%	24.0 MB	- 10 E
-d Postiona		□ ► anonymo	us RDP-0-TL	5-10.0.40.100-	ANONYMOUS	RDP	anonymous	2016-01-11	12:13 2016-01-11 12:27	0:14:22 63%	26.4 MB	<b>**</b> **

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.

Management <	Fudo			۵.	admin 🕤 🥐
Jashboard	Downloade 🗍 Delete				
E Sessions	Downloads				
쓭 Users	D ID Session ID	Size	Format	Resolution	
Servers	7 848388532111147069	0 bytes	DivX5 (AVI)	Monitor conversion progress	2
	6 848388532111147083	0 bytes	DivX5 (AVI)	Autodetect	
• Bastions	5 848388532111147076	444.5 KB	DivX5 (AVI)	Autodetect	*
+ Connections	4 848388532111147076	465.6 KB	Flash Video (FLV)	Autodetect	*
	3 848388532111147076	4.5 MB	MJPEG (very high quality)	Download converted material	
V Folicies	2 848388532111147075	22.1 MB	MPEG-2 (very popular codec)	Autodetect	*
▲ Downloads	1 848388532111147076	529.9 KB	Xvid (AVI)	Autodetect	Ŧ
🔒 Reports					

## **Related topics:**

- Filtering sessions
- Sharing sessions
- Viewing sessions
• Joining sessions

# 12.10 Deleting sessions

To delete a recorded session, proceed as follows.

- 1. Select Management > Sessions.
- 2. Find and select desired session.
- 3. Click Delete.
- 4. Confirm deleting selected sessions.

**Note:** Wheel Fudo PAM can automatically delete sessions after certain time, specified by the retention parameter. Refer to the *Backups and retention* topic for more on data retention.

#### **Related topics:**

- Filtering sessions
- Sharing sessions
- Replaying sessions
- Exporting sessions

# 12.11 OCR processing sessions

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

#### Automated sessions processing

To have RDP and VNC sessions automatically processed, proceed as follows.

- 1. Select Management > Connections.
- 2. Find and click desired connection.
- 3. Select OCR sessions option.
- 4. Select the language of processed material.

Management <	Fudo	
Je Dashboard		
E Sessions	Connection	
嶜 Users	General	_
B Servers	ID 848388532111147016	
• Bastions	Name ssh-przekazywanie-0 11	1
+ Connections		
Policies	Blocked	
🕹 Downloads	Notifications 2 Session start 2 Session finish Session ioin 2 Session leave	
🔒 Reports	Session policy match	
■ Productivity	Users O Q	
Settings OCR RDP	and VNC sessions ng Complete ¢	E.
System	OCR sessions 2	
O Network configuration	OCR language DEnglish Dolish	
☑ Notifications	Norwegian Russian	
@ Timestamping	Delete session data a Define the language of processed material Js	

4. Click Save.

#### Processing selected sessions

To process selected sessions, proceed as follows.

- 1. Select Management > Sessions.
- 2. Select desired RDP or VNC sessions and click OCR.

Management	۲	FU	do*									📥 ad	min	- ?
		Sess	ions	.al Act	tive 🔒	Delete	OCR	▼ Add filter ~	- Generate repor	nt Se	earch	0	Q	~
E Sessions	F.		Sele	ct des	ired se	ssions		En la calactería de la cal	0		0			
* Users			admin	fudo4	SSH	ssh	2015-05-07 11:18	2015-05-07 1	11:19 0:00:18	100%	27.0 KB		•	±
Servers	Pro	CASS -	select	ed ma	terial -	ssh	2015-05-07 11:10	2015-05-07 1	1:10 0:00:31	100%	43.0 KB	2.5	5	*
-∉ Bastions			aumm	10004	John	ssh	2015-05-05 13:06	2015-05-05 1	3:06 0:00:00	0%	4.0 KB	-9.5	5	*
+ Connections		⊳►	admin	fudo4	SSH	ssh	2015-05-05 13:06	2015-05-05 1	3:06 0:00:00	0%	4.0 KB	- 95	5	*
\$ CONTROLION		□ ►	admin	fudo4	SSH	ssh	2015-05-05 13:06	2015-05-05 1	3:06 0:00:00	0%	4.0 KB	2.5	5	*

Note: Filtering options allows for selecting processed or unprocessed objects.

3. Confirm processing selected sessions.

#### **Related topics:**

- Filtering sessions
- Accounts

# 12.12 Timestamping selected sessions

To timestamp selected sessions, proceed as follows.

- 1. Select Management > Sessions.
- 2. Select desired sessions and click  $\mathit{Timestamp}.$

м	lanagement <	Fudo										
đ	I Dashboard	Sessions	🕆 Delete	OCR	@ Timestamp	🔒 Generate	report			T Add filter	∽ Se	arch.
E	Sessions	Se	lect desired	d sessions								
-		D User	Protoco	10	Server	Account	Safe	Started at *	Finished at	Duration	Activity	Size
	Servers	anonyi anonyi	nous ICA		citrix	ica-anon	citrix-anon	2017-02-16 16:51	2017-02-17 07:52	15:00:42	0%	131
	P	rocess sele	cted materi	al	citrix	ica-anon	citrix-anon	2017-02-16 16:49	2017-02-16 16:51	0:02:24	42%	792
8	Accounts				citrix	ica-anon	citrix-anon	2017-02-16 16:46	2017-02-16 16:46	0:00:04	0%	83.0
2		Anony	nous ICA		citrix	ica-anon	citrix-anon	2017-02-16 16:45	2017-02-16 16:46	0:00:05	0%	123
	Safes	anony	nous ICA		citrix	ica-anon	citrix-anon	2017-02-16 16:43	2017-02-16 16:45	0:02:05	48%	443

3. Click Confirm.

Timestamp confirmation	🔒 Generate report		×
Are you sure you want to timestamp 1 session	n?		
		Cancel	Confirm

Note: Click the <sup>O</sup> to view the timestamp data.

# **Related topics:**

- Filtering sessions
- Accounts

# CHAPTER 13

Reports

Reporting service generates detailed statistics of users access sessions.

Full reports are generated periodically (daily, weekly, monthly, quarterly) by the system and can be accessed by users with the **superadmin** role assigned. Reports generated periodically upon users with **admin** or **operator** requests, will include only information regarding sessions objects which they have access permission assigned to.

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

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

#### Subscribing to a periodic report

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

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

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

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

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

Management <	Fudo <sup>*</sup> Administration panel Display available subscription management options
I Dashboard	Paparte Delete / Manage subscriptions
E Sessions	Choose the report definition
쌸 Users	my_very_own_filter  Caily Weekly Monthly Quarterly Every year
+ Connections	Select report generation frequency
Servers	
D Policies	Add another report subscription
	Store changes

#### Cancelling a periodic report subscription

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

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

Management <	Fudo <sup>*</sup> Administration panel Display available subscription management options
Dashboard	Benorts Delete / Manage subscriptions
E Sessions	
쌸 Users	my_very_own_filter
+ Connections	Cancel the given report subscription
Servers	•
Policies	
🛓 Downloads	2 Reset
	Store changes

#### Generating reports on demand

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

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

Management <	Fudo	Add filte	ring parameters		🛔 admin 🐇 🤶 📍
Jashboard	Sessions	Active   Delete	OCR T Add filter ~ + Gen	erate report Search	0 Q~
E Sessions	Generate	a report based on	the current filtering parameter		
쓭 Users	Generate			- Q ×	
🖴 Servers		Filter na	me	8	
•# Bastions					
+ Connections	User Serve	r Protocol Connec	tion Started at - Finished at	Duration Activity Size	
<b>V</b> Policies	admin mssq	al MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0% 3.0 KB	● ` 동안소
*. Downloada	admin mssq	al MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0% 8.0 KB	> 이 타 문 초
in Downloads	admin mssq	ql MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0% 3.0 KB	이 아들 문 소
Reports	admin mssq	al MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0% 3.0 KB	이 아들 문 것 수
	admin mssq	al MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0% 8.0 KB	이 아들은 소
Productivity	🗆 🕨 admin mssq	al MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0% 3.0 KB	0 N 60 11 A

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

Management <	≓udo'	🛔 admin 🐇 🤶 📍
M Dashboard	Sessions	oQ∽
E Sessions	0000010	
嶜 Users	By protocol MS SQL (TDS) O O, X	
⊖ Servers	Filter name	
- Bastions		
+ Connections	Report 6871947604880523309 preated successfully.	×
<b>V</b> Policies	Click the report's identifier to view its content	
📥 Downloads	User Server Protocon Connection Stantio at Printmed at Duration Activity Size	
	▷ ▶ admin mssql MS SQL (TDS) mssql 2015-06-02 05:51 2015-06-02 05:51 0:00:00 0% 3.0 KB	
Heports	Admin mssql MS SQL (TDS) mssql 2015-06-02 05:51 2015-06-02 05:51 0:00:00 0% 8.0 KB	이 아들 문 소
E Productivity	□ ► admin mssql MS SQL (TDS) mssql 2015-06-02 05:51 2015-06-02 05:51 0:00:00 0% 3.0 KB	- • • • ±

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

### Opening and downloading reports

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

Management	۲.	Fudo <sup>*</sup>				📥 adm	in - ?
		Reports 8 Delete			T Add filter ∨		tions
		Toporto					-
쓸 Users			Created at	Title		Created by	
Servers		6871947604880523300	2015-08-19 01:00:03	Daily (2015-08-18) - System	n default report	system	₽
	Di	splay the reports list	2015-08-18 07:22:59	Report generated by admin	1	admin	B
•@ Bastions		6871947604880523298	2015-08-18 07:05:31	Report generated by admin	n	admin	₽
+ Connections		6871947604880523297	2015-08-18 01:00:02	Daily (2015-08-17) - System	n default report	system	B
D Policies		6671947604880523296	2015-08-17 01:00:03	Weekly (2015-08-16) - Syst	tem default report	system	
V Folicids		68719476 Click to dis	play given report -	Daily (2015-08-16) - System	n default report	system	p)
📥 Downloads		6871947604880523294	2015-08-16 01:00:01	Daily (2015-08-15) - System	n default report	system	B
		6871947604880523293	2015-08-15 01:00:01	Daily (2015-08-14) - System	n default report	system	B
		0 0071047004000600000	0016 00 14 01-00-00	Delle 2001E-00-125 Custon	-		n.

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

Management <	Fudo						🛔 admin 🕤 📍
💷 Dashboard	Banart 04020052014144	2045				Cs	
E Sessions	Report 046306532111147	040			Cours the		And Connect
쯀 Users					Save the	report in selec	ted format
🖴 Servers	Report criteria						
•@ Bastions	<ul> <li>From date = 2015-12-10</li> <li>To date = 2015-12-10</li> </ul>						
+ Connections	Servers						
Policies	Server	Number of	Number of	Sessions total	Sessions total	Average session	Average session
A Developed	RDP-10.0.35.53-WindowsXP	sessions 1	users 1	0:00	181.0 KB	0:00	181.0 KB
Z Downloads	RDP-10.0.40.100- Windows2012	1	1	0:24	2.3 MB	0:24	2.3 MB
🔒 Reports	RDP-10.0.40.202-Windows8	1	1	0:03	27.9 MB	0:03	27.9 MB
= Descharthilte	SSH-10.0.35.1	12	1	1:34	14.5 MB	0:07	1.2 MB
E. Productivity	Usens						
Settings	Users						
The Output	User Number of sessions	Number of servers	Sessions tota	l time Sessions t	otal size Averag	ge session time Av	erage session size
System	user0 15		4	2:02	44.8 MB	0:08	3.0 MB

### **Deleting reports**

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

# Related topics:

- Notifications
- Filtering sessions

# CHAPTER 14

Efficiency analyzer

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

# 14.1 Overview

Overview displays data on users' activity in selected time interval.

**Note:** Activity rating is based on the user's interaction with the monitored system. Wheel Fudo PAM divides the time into 60 seconds long time intervals and monitors the activity within the interval. Lack of any actions in a given time period accounts such as a non-productive time.

To view the users' activity rundown, proceed as follows.

- 1. Select *Management* > *Productivity*.
- 2. Select the *Overview* tab.
- 3. Define the users' list filtering.
- 4. Click *Generate report* to generate rundown of the displayed data in HTML, CSV or PDF format.

Note: The report can be accessed in the *Reports* section.

Management <	Fudo							🛔 admin 🐇 🤶 📍
Jashboard	Overview	Session analysis	Comparison				Add filter ~	Generate report
E Sessions	Overview	Session analysis	Companison				$\square$	
쓸 Users		Date from	Add a filter, to lin	nit the numbe	r of element	s on the list -		
+# Connections	ak ta aart tal							
🖴 Servers	Summary	ble content						
Policies	Organization/User	Bession	s total time	Active time	Idie time	Productivity	Sessions	Servers
🕹 Downloads	Total	434:58	3	88:47	346:11	20%	296	19
⊖ Reports	Unassigne	Show users	within the given	organization	188:51	22%	181	16
■ Productivity	dewelopmen	Hide users v	within the given o	rganization	18:21	41%	31	1
	user-33	31:10		12:49	18:21	41%	31	1
Settings	serwis ~	160:53	3	21:54	138:59	13%	84	2
system 🔁	user-25	157:02	2	21:01	136:01	13%	80	1
Ø <sup>e</sup> Network configuration	user-26	3:51		0:53	2:58	22%	4	1
Management <	Fudo							🛔 admin 🐇 🤶
Management <		Session analysis	Comparison				Add filter ~	<b>å admin ∽</b> ? Generate report
Management < Im Dashboard Im Sessions	Fudo <sup>•</sup> Overview	Session analysis	Comparison				Add filter ~	<b>å admin ∨</b> ? Generate report
Management < Dashboard    Sessions    설 Users	Fudo <sup>*</sup> Overview	Session analysis	Comparison 2014-10-01	to	2014-11-01		Add filter ~	<b>å edmin ~ ?</b> Generate report
Management             Ш Dashboard             ⊟ Sessions             ≝ Users + Connections	Fudo <sup>•</sup> Overview	Session analysis Date from	Comparison 2014-10-01	to	2014-11-01		Add filter ~	<b>å admin ∨ ?</b> Generate report
Management        Imagement        Image        Image        Image        Image        Image        Image        Image        Image	Cverview Summary	Session analysis Date from	Comparison 2014-10-01	to	2014-11-01		Add filter ~	<b>å admin ∨ ?</b> Generate report
Management	Coverview Overview Summary Organization/Lier	Session analysis Date from	Comparison 2014-10-01	Active time	2014-11-01	Productivity	Add filter ~	≗admin ∨ ? Generate report
Management	Coverview Overview Summary Organization/User Total	Session analysis Date from Session	Comparison 2014-10-01	Active time  88:47	2014-11-01 Ide time 346:11	Productivity 20%	Add filter ~ Cessions 296	<b>≜ admin ∨</b> ? Generate report Servers 19
Management	Cverview Overview CrgarizationUser Total Unassigned ~	Session analysis Date from Session 434:54 242:51	Comparison 2014-10-01 c blaf time	Active time 88:47 54:04	2014-11-01 Ide time 346:11 188:51	Productivity 20% 22%	Add filter ~ Sessions 296 181	<b>≜ admin ∨</b> ? Generate report Servers 19 16
Management	Cverview Overview Summary OrganizationUser Total Unassigned ~ Gewelopment	Session analysis Date from Session 434:50 242:50 31:10	Comparison 2014-10-01	to Active time 88:47 54:04 12:49	2014-11-01 Ide time 346:11 188:51 18:21	Productivity 20% 22% 41%	Add filter ~ Sessions 296 181 31	A admin v ? Generate report Servers 19 16 1
Management        Imagement        Imagement	Cverview Overview Summary OrganizationUse Unassigned ~ dewelopment user-sta	Session analysis Date from Eession 434:59 242:50 31:10 Show users	Comparison 2014-10-01 a total time 5 from the giv <u>en o</u>	Active time 88:47 54:04 12:49 rganization o	2014-11-01 Ide Sme <b>348:11</b> 188:51 18:21 18:21	Productivity 20% 22% 41% 41%	Add filter ~ Escalors 296 181 31 31	A admin v ? Generate report Servers 19 16 1 1 1
Management        Imagement        Imagement	Coverview Overview Summary Organization/User Total Unassigned ~ dewelopment ~ user-\$3 servits ~	Session analysis Date from Session 434:54 242:55 31:10 Show users 160:55	Comparison 2014-10-01 a total time from the given of 3	Active time 88:47 54:04 12:49 rganization o 21:54	2014-11-01 Ide time 346:11 188:51 18:21 18:21 138:59	Productivity 20% 22% 41% 41% 13%	Add filter ~ Bessions 290 181 31 31 31 84	A admin > ? Generate report
Management	Cverview Overview Summary OgencationUser Total Unassigned ~ dewelopment user-:3 servis ~ user-:5	Session analysis Date from Beston 434:54 242:55 31:10 Show users 180:53 157:02	Comparison 2014-10-01 a bold the from the given o	Active time 88:47 54:04 12:49 rganization o 21:54 21:01	2014-11-01 Life time 346:11 188:51 18:51 18:21 138:59 138:59 136:01	Productivity 20% 22% 41% 41% 13% 13%	Add filter ~ Sessions 290 181 31 31 31 84 80	<ul> <li>▲ admin ×</li> <li>?</li> <li>Generate report</li> <li>Servers</li> <li>19</li> <li>16</li> <li>1</li> <li>1</li> <li>2</li> <li>1</li> <li>1</li> <li>2</li> <li>1</li> </ul>

# **Related topics:**

- Productivity analysis Sessions analysis
- Productivity analysis Comparison
- Sessions

# 14.2 Sessions analysis

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



# Users activity rating

Users activity rating allows identifying sessions which do not exceed the required user activity level. Further material analysis helps determining the reason for low activity in the given session and draw relevant conclusions.

**Note:** The listing does not cover time periods longer than 31 days. In case the defined time interval is longer than that, only data from the first 31 days is presented.



Activity threshold < 20 > Below threshold:	sessions for the given day		
W T F S S M T W T F S S M T W T F S S M	Oct. 24, 2014		
dewelopment	Sessions time: 1-29	12:49	31:10 41%
User-33	Active time: 0:22	12:49	31:10 41%
servis Click to display only data on the given organization	Idle time: 1:07	<mark>21</mark> :54	160:53 <mark>14%</mark>
user-25	Sessions count: 1 Productivity: 25.96	21:01	157:02 13%
user-26		0:53	3:51 23%
Unassigned		54:04	242:55 22%
		0:03	0:03 100%
Hover over a given element to dispay detailed informatio		0:07	0:18 39%

# **Related topics:**

- Productivity analysis Overview
- Productivity analysis Comparison

# 14.3 Activity comparison

Efficiency analyzer module enables comparing users/organizations activity in given time periods.

To compare users/organizations, proceed as follows.

- 1. Select Management > Productivity.
- 2. Select the *Comparison* tab.
- 3. Select object types being compared.
- 4. Select the time interval.
- 5. Add objects to the comparison and define starting date for each object.
- 6. Click *Confirm* to compare selected objects.

# Related topics:

- Productivity analysis Sessions analysis
- Productivity analysis Overview
- Sessions

# CHAPTER 15

Administration

This section covers Wheel Fudo PAM administration topics.

# 15.1 System

# 15.1.1 Date and time

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

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

#### Changing date and time settings

Note: Manual time setting is disabled if there are NTP servers configured.

To change the Wheel Fudo PAM's system clock settings, proceed as follows.

- 1. Select Settings > System.
- 2. Change date and time parameters in the *Date and time* section.

Management	< Fudo	•				🛔 admin 🗸  ?
Jashboard	General	Upgrade	Liconso	Diagnostics		
E Sessions	General	opgrade	License	Diagnostics		
뿔 Users	Date and	Select tim	ezone	]		
🖴 Servers		Timezone	Warsaw		*	
• Bastions		Date & time	2016-02-07	23:40	1	
+ Connections				Set the date and time		
C Policies	NTP serv	/ers			, 	
🛓 Downloads						
⊖ Reports					^	
E Productivity			+			

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.

Management	< Fudo	🛔 admin 🐇 🤶 📍
I Dashboard	General Ungrade License Diagnostics	
E Sessions		
<b>쓸</b> Users	Date and time	
🖴 Servers	Timezone Warsaw 🛊 🕸	
•@ Bastions	Date & time 2016-02-07 23:40	
+ Connections	Add NTP server	
Policies	NTP servers Provide hostname or IP address	
📥 Downloads	r tovide hostname of in address	
🖨 Reports		
Productivity		

4. Click Save.

#### Editing an NTP server definition

To edit an NTP server definition, proceed as follows.

- 1. Select Settings > System.
- 2. Find and change desired NTP server configuration parameters in the NTP servers section.

Management	<	Fudo				🛔 admin 🗸 💡 🤶
Jashboard		General Ung	rade License	Diagnostics		
E Sessions		General Opg	License	Diagnostics		
曫 Users		Date and time				
🖴 Servers		Timez	Warsaw		\$	
📲 Bastions		Date & t	ime 2016-02-08	15:07		
+ Connections						
Policies		NTP servers				
🛓 Downloads			ni pogi ata or			
🔒 Reports			pepoornipion		^	
E Productivity	Click to edit	NTP server's IP a	address/hostnan	ne of the		

3. Click Save.

# Deleting an NTP server definition

To remove and NTP server definition, proceed as follows.

- 1. Select Settings > System.
- 2. Find desired NTP server definition in the NTP servers section and click the X icon.

Management <	Fudo		🛔 admin 🕤 🤶
Jashboard	General Ungrade	License Diagnostics	
E Sessions	opgrade	Liberto Plagrouto	
🔮 Users	Date and time		
🖴 Servers	Timezone	Warsaw 🗘 🛊	
-@ Bastions	Date & time	2016-02-08 15:07	
+ Connections			
U Policies	NTP servers		
🕹 Downloads			
🖨 Reports			
■ Productivity		Remove NTP server	

3. Click Save.

**Related topics:** 

• Timestamping

# 15.1.2 SSL certificate

SSL certificate allows prevent phishing attacks.

#### Configuring SSL certificate

To configure SSL certificate, proceed as follows.

- 1. Select Settings > System.
- 2. Click the *Browse* button next to the *HTTPS Certificate* field in the *FUDO HTTPS certificate* section and point to the location of the SSL certificate file in PEM format.

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

Management <	Fudo	🛔 admin 🐇 🤶 ?
Jashboard	General Upgrade License Diagnostics	
E Sessions		
볼 Users	Date and time	
🖴 Servers	Timezone 🛛 🗘 🛊	
•@ Bastions	Date & time 2016-02-08 15:07	
+ Connections		
C Policies	NTP servers	
📥 Downloads		
🖨 Reports	phpon.nep.org	
■ Productivity	+	
Settings	FUDO HTTPS certificate	
🗁 System	Upload certificate in PEM format	
On Network configuration	HTTPS certificate Wyblerz plik Nie wybrano pliku	
Notifications	HTTPS private key Wybierz plik Nie wybrano pliku	
@ Timestamping	Upload private key	
At External authentication	SSH access	
III External passwords repositories	Enabled 🛛	
Resources		
Backups and retention	Sensitive features	
a Cluster	Activating these reatures requires a consent of two superadmin users.	
LDAP synchronization		
$\equiv$ Events log		
© 16 days 19993999 % oracle10-25511.dl Master		
	C Reset V Save	

4. Click Save.

#### **Related topics:**

- Security measures
- Servers

# 15.1.3 Deny new connections

Enabling this option results in a denial of all new connections requests.

Blocking new connections

- 1. Select Settings > System.
- 2. Select *Deny new connections* option in the *Session* section.
- 3. Click Save button.

#### **Related topics:**

• Network interfaces configuration

# 15.1.4 SSH access

SSH access option enables remote access to Wheel Fudo PAM for servicing and maintenance purposes.

# Enabling SSH access

To enable SSH access, proceed as follows.

- 1. Select Settings > System.
- 2. Select Enabled option in the SSH access section.

Management <	Fudo	🛓 admin 🗸 🤶
Jashboard	General Ungrade License Diagnostics	
E Sessions	deneral opgrade License Diagnostics	
🖶 Users	Date and time	
🖴 Servers	Timezone Warsaw	¢ at
•@ Bastions	Date & time 2016-02-08 15:07	
+ Connections		
Policies	NTP servers	
🕹 Downloads		
🔒 Reports	pl.pool.ntp.org	×
■ Productivity	+	
Settings	FUDO HTTPS certificate	
🖙 System		
O Network configuration	HTTPS certificate Wybierz plik Nie wybrano pliku	
Notifications	HTTPS private key Wybierz plik Nie wybrano pliku	
@ Timestamping		
e External authentication	SSH access	
III External passwords repositories	Enabled	
🖾 Resources	Enable SSH service access	
Backups and retention	Sensitive features	
🛔 Cluster	Activating these features requires a consent of two superadmin users.	
LDAP synchronization	anow keyboard input	
© 16 days 19993999 % oracle10-25511 da Master		
	2 Reset 🗸	Save

3. Click Save button.

# Related topics:

• Network interfaces configuration

# 15.1.5 Reset account

Reset account enables resetting Wheel Fudo PAM to factory settings.

Enabling reset account

To enable reset account, proceed as follows.

- 1. Select Settings > System.
- 2. Select *Enabled* option in the *Reset account* section.
- 3. Click Save button.

# Related topics:

• Network interfaces configuration

# 15.1.6 Sensitive features

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

#### Enabling displaying keyboard input

**Note:** Keystrokes are not displayed in the session player by default. Enabling keystrokes display requires a consent from two **superadmin** users.

To enable keyboard input display, proceed as follows.

- 1. Select Settings > System.
- 2. Select Show user input in the Sensitive features section to initiate the feature.
- 3. Click Save.

Management <	Fudo	🛓 admin 🗸 🤶
Jashboard	General Upgrade	Liconso Disgnostics
E Sessions	General Opgrade	LICENSE DIAGNOLICA
👑 Users	Date and time	
🖴 Servers	Timezone	Warsaw 🗘 🗧
•# Bastions	Date & time	2016-02-08 15:07
+ Connections		
C Policies	NTP servers	
🕹 Downloads		
⊖ Reports		pi.pool.ntp.org
■ Productivity		+
Settings	FUDO HTTPS certific	cate
🗁 System		
O Network configuration	HTTPS certificate	Wybierz plik Nie wybrano pliku
Notifications	HTTPS private key	Wybierz plik Nie wybrano pliku
C Timestamping		
e External authentication	SSH access	
III External passwords repositories	Enabled	
Resources		
Backups and retention	Sensitive features	
🚓 Cluster	Activating these features requir	res a consent of two superadmin users.
LDAP synchronization	Select to d	tisplay keyboard input in session player
≡ Events log		
© 16 days £ \$55933959 % oracle10-25511.d. Master		
		Ø Reset ✓ Save

4. Notify another system administrator that the keyboard input showing feature has been initiated and requires a confirmation.

# **Related topics:**

• Viewing sessions

# 15.1.7 System update

# Note:

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

#### 15.1.7.1 Updating system

#### Warning:

- Before updating the system it is advised to run a preliminary check to ensure that the current system configuration can be successfully upgarded to new version.
- During the system update, all current users' connections will be terminated.
- Use the *Deny new connections* option in the *Sessions* section in the system settings menu.
- 1. Select Settings > System.
- 2. Select the *Upgrade* tab.
- 3. Click Upload.
- 4. Browse the file system to find and upload the update image file (.upg).
- 5. Click Upgrade.

Management <	Fudo					🛔 admin 🗸 💡 🤶
Jashboard	General	Upgrade	License	Disgostics	× Remove upgrade snapshot	Delete      Our Upload
E Sessions	General	opgrade	License	Diagnostics		
쓸 Users	Version	Filename		Size	Upgrade check run status	
⊖ Servers	3.1-32574	fudo-3.1-	32574.upg	108.1 MB	Upgrade check has not been run	Run check (* Upgrade
•# Bastions					Upgrade system with selecte	ed image
+ Connections						

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

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

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

#### 15.1.7.2 Running update check

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

- 1. Select Settings > System.
- 2. Select the Upgrade tab.
- 3. Click Upload.
- 4. Browse the file system to find and upload the update image file (.upg).

5. Click Run check.

Management	<	Fudo							🛔 admin <  ?
		General	Ungrade	License	Diagnostics		× Remove upgrade snapshot	🔒 Delete	Upload
E Sessions	I.	adnora	opgrade	License	Diagnoonoo				
誉 Users		Version	Filename		Size	Upgrade check r	un status		
		3.1-32574	fudo-3.1-	32574.upg	108.1 MB	Upgrade check	has not been run	Run check	E Upgrade
							Upgrade check run -		
+ Connections									

Note:

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

#### 15.1.7.3 Deleting upgrade snapshot

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

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

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

Management		Fudo							🛔 admin 🐇 🤶 📍
Jashboard		General	Upgrade	License	Diagnostics		Remove upgrade snapshot	🖯 Delete	Upload
E Sessions	F.				Delete prev	vious system	version		
쓸 Users		Version	Filename		Size	Upgrade check ru	un status		
🖴 Servers		3.1-32574	fudo-3.1-	32574.upg	108.1 MB	Upgrade check	has not been run	Run check	E Upgrade
•l# Bastions									
+ Connections									

4. Confirm deleting previous system version.

### **Related topics:**

- System version restore
- Restarting system

# 15.1.8 License

#### Uploading new license

To upload a new license file, proceed as follows.

Note: New license will replace existing one.

- 1. Select Settings > System.
- 2. Select the *License* tab.
- 3. Click Upload.

Management <	Fudo <sup>*</sup>					👗 admin 🕤 📍
I Dashboard	General Ungrade Licer					( Upload
E Sessions		Diagnostics			Lipload license fi	
쑬 Users	Serial number	12345678			Opload license li	e
⊖ Servers	Expiration date	2016-03-31				
•# Bastions	License owner	Wheel Systems sp. zoo				
+ Connections	License type	test				
Policies	Accounting mode	host,port				
📥 Downloads	Cluster nodes limit	1				
🖨 Reports	Glaster Houes mint					
E Productivity	Number of servers	25	11 in use	14 available		
Settings	Usage statistics		License param	eters		
🗁 System	Date from	2015-11-01	to	2016-02-08		
© Network configuration	Concurrent connections	etatistics		2010-02-00		
Notifications	50-	statistics				
C Timestamping	4.5 -					
ae External authentication	3.5 -					
III External passwords repositories	2.5 -					
E Resources	2.0 - 1.5 -					
Backups and retention	1.0 - 0.5 -					
n Cluster	0.0	Wed 23	Thu 17	Fri DB	Mon 11	
LDAP synchronization	Number of concurrent sessions					

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

#### **Related topics:**

• System

# 15.1.9 Diagnostics

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

To run a diagnostic utility, proceed as follows.

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

Management <	Fudo		👗 admin 🗸 💡 📍
Dashboard	General Uno	rade License Diagnostics	Ownload service data
E Sessions	General Opg	nade Livenae Diagnostica	
嶜 Users	ping	Enter host address Execute	command
⊖ Servers		Host	
- Bastions		Options Output only Record route	
+ Connections	patcat		
Policies	netcat	Select optional execution parameters	
🕹 Downloads		Host Port A	
🖨 Reports	host		
■ Productivity		Host	
Settings			
🗁 System	traceroute		
¢ Network configuration		Host A	
☑ Notifications		Options Do not resolve hop addresses Use ICMP ECHO instead of	
C Timestamping		UDP datagrams Firewall evasion mode Set the "don't fragment" bit	
at External authentication			

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

# Related topics:

• Troubleshooting

# 15.2 Network settings

To change network settings select  $Settings > Network \ configuration$ .

Management <	≓urdn*
M Dashboard	Static routing configuration
Sessions	Interfaces Name & DNS Routing
쌸 Users	DNS servers configuration
🖴 Servers	% net0 08:00:27:5A:A3:A9 ♀ DHCP
accounts	
Safes	10.0.40.50 / 16 🗡 👁 🗙
Դ Listeners	10.0.40.51 / 16 🗲 🔾 🗙
h- Password changers	+
Policies	
📥 Downloads	Sheet1 08:00:27:90:12:05
🖨 Reports	
■ Productivity	+
Settings	
🛎 System	% net2 06:00:27:57:B2:BA
O <sup>e</sup> Network configuration	
☑ Notifications	+
☑ Timestamping	
a External authentication	% bridge0 02:00:8C:61:4E:00
## External passwords repositories	
Resources	172.128.0.10 / 24 <b>F</b> 🛛 🗙
Backups and retention	+
🚓 Cluster	
	spanning tree
≡ Events log	
	Conligure network bridge
2 days ii 12345678 3-30775	S Reset Save

# 15.2.1 Network interfaces configuration

# 15.2.1.1 Managing physical interfaces

# Defining IP address

Defined IP addresses are physical interface's aliases, which are used in server's *configuration* procedures (Local address field in proxy configuration).

**Note:** If the list of the assigned IP addresses is empty and the is no option to define an IP address, check if given interface is a member of a bridge.

To define an IP of a physical network interface, proceed as follows.

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

Note: + will be inactive if the *DHCP* option is enabled on the given interface.

- 3. Choose additional options for the IP address being defined.
- Enable access to administration panel on given IP address. Note that the management IP address is also used for replicating data between cluster nodes.
   Make the alias a virtual IP address which will be take over by another cluster node in case of the master node's failure.
  - Enable access to *User portal* on given IP address.
  - 4. Click Save.

Management <	Fudo	Enable access to FUDO administration panel through this IP address
🖬 Dashboard		Enable User portal access through this IP address
E Sessions	Interfaces Name & DNS Routing	Make the alias a virtual IP address which will be automatically taken over by another cluster node in case of the master node's failure
쑬 Users	% net0 00:0C:29:AF:54:E8	Delete IP address
⊖ Servers		
Accounts	10.0.235.153 / 16	Obtain IP address from a DHCP server
Safe: Enter IP address and i	network mask / 16 🖌 🖉 🚮	(g1 \$) ×
ሕ Listeners	(+)	Assign IP address to redundancy group
n- Password changers	Add IP alias to network	interface
V Policies	x net1 00:0C:29:AF:54:F2	© Active ODHCP
🛓 Downloads		
🖨 Reports	Interface is not active.	
Productivity		
Settings	0.0.0.0 / 16 🗲 🤤 📥	, <b>x</b>
🖨 System	+	
¢ Network configuration		
☑ Notifications	4	C Reset Save

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

00	Interface active and connected.
<u>بن</u>	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.

Management <	Fudo <sup>*</sup>	🛔 admin < 💡
🖩 Dashboard	Interfaces Name & DNS Bouting	
E Sessions		
쓸 Users	S net0 00:00:28.AF.54.E8	Q Active OHCP
⊖ Servers	Delete IP address	
Accounts	10.0.235.153 / 16 🗡 🛛 📥 💌	
Safes	10.0.235.154 / 16 🗲 🔾 🔐 rg1 💠 🗙	
ふ Listeners	•	
n- Password changers		
C Policies	× net1 00:00:29:AF:54:F2	Q Active OHCP
🕹 Downloads		
🖨 Reports	Interface is not active.	
■ Productivity		
Settings	0.0.0.0 / 16 🗲 <table-cell> 🛦 🗙</table-cell>	
🖨 System	+ Store and apply changes	
Ø <sup>e</sup> Network configuration		
☑ Notifications	C Reset Save	X Bridge P VLAN

# $Disabling\ network\ interface$

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.

Management <	Fudo admin ~ ?
🖬 Dashboard	Interfaces Name & DNS Bouting
E Sessions	
촬 Users	% net0 00:00:28:AF:54:E8
⊖ Servers	Deactivate selected interface
Accounts	
Safes	10.0.235.154 / 16 🗲 😪 🚓 rg1 💠 🗙
み Listeners	
n- Password changers	
Policies	X net1 00:00:29:AF:54:F2 Q DHCP
📩 Downloads	
🔒 Reports	Interface is not active.
E Productivity	
Settings	0.0.0.0 / 16 🖌 🐼 🚠 🗙
🖨 System	+ Save configuration changes
¢ <sup>e</sup> <sub>6</sub> Network configuration	
☑ Notifications	C Reset Save

3. Click Save.

# 15.2.1.2 Defining IP address using system console

In case the web administration interface cannot be accessed, IP address can be defined using console connection.

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

FUDO, S/N 12345678, firmware 2.1-23500.
To reset FUDO to factory defaults, login as "reset". To fix admin account and change network settings, login as "admin" with an appropriate password.
FUDO (fudo.wheelsystems.com) (ttyv0)
login:

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



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

```
FUDD, S/N 12345678, firmware 2.1-23500.
To reset FUDD to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.
FUDD (fudo.wheelsystems.com) (ttyv0)
login: admin
Password:
Last login: Wed Jun 22 10:50:38 on ttyv0
*** FUDD configuration utility ***
Logged into FUDD, S/N 12345678, firmware 2.1-23500.
1. Show status
2. Reset network settings
0. Exit
Choose an option (0):
```

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

FUDO, S/N 12345678, firmware 2.1-23500. To reset FUDO to factory defaults, login as "reset". To fix admin account and change network settings, login as "admin" with an appropriate password. FUDO (fudo.wheelsystems.com) (ttyv0) login: admin Password: Last login: Wed Jun 22 10:50:38 on ttyv0 \*\*\*\* FUDO configuration utility \*\*\* Logged into FUDO, S/N 12345678, firmware 2.1-23500. 1. Show status 2. Reset network settings 0. Exit Choose an option (0): 2 Are you sure you want to continue? [y/N] (n):

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

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

```
To reset FUDD to factory defaults, login as "reset".

To fix admin account and change network settings,

login as "admin" with an appropriate password.

FUDD (fudo.wheelsystems.com) (ttyv0)

login: admin

Password:

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

*** FUDD configuration utility ***

Logged into FUDD, 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 Reset network settings 0. Exit Choose an option (0): 2 Are you sure you want to continue? [y/N] (n): y Choose new management interface (net1 net0): net0 Enter new net0 address (10.0.150.150/16): 10.0.150.150/16 8. Enter network gate and press *Enter*.

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

To reset FUDO to factory defaults, login as "reset". To fix admin account and change network settings, login as "admin" with an appropriate password. FUDO (fudo.wheelsystems.com) (ttyv0) login: admin Password: Last login: Wed Jun 22 10:56:52 on ttyv0 \*\*\* FUDO configuration utility \*\*\* Logged into FUDO, S/N 12345678, firmware 2.1-23500. 1. Show status 2. Reset network settings 0. Exit Choose an option (0): 2 Are you sure you want to continue? [y/N] (n): y Choose new management interface (net1 net0): net0 Enter new net0 address (10.0.150.150/16): 10.0.150.150/16 Enter new default gateway IP address (10.0.0.1):

### 15.2.1.3 Setting up a network bridge

Bridge deployment scenario requires setting up a network bridge.

To configure a network bridge, proceed as follows.

- 1. Select  $Settings > Network \ configuration$ .
- 2. Click Bridge.
- 3. Assign network interfaces or VLANs to the bridge.

**Note:** Setting up a network bridge requires removing all IP addresses directly assigned to interfaces which are selected as bridge members.

- 4. Enter IP address and network subnet in CIDR notation.
- 5. Select Spanning tree option to enable bridge loops prevention.
- 6. Select the *Management* option if the administration interface should be available under assigned IP addresses and click *Active*.
- 7. Click Save.

Resources	× bridge0		× Active OHCP
Backups and retention	Define bridge's IP ad	dress Remove bridge definition	
		Activate bridge	
$\Rightarrow$ LDAP synchronization	ssign IP address to redundancy group		
	Spanning tree D Ena	ble spanning tree mechanism	
	Members	0 Q)	
	Ass	ign physical network interfaces or VLANs	
	≭ vlan0		× VActive Q DHCP
	/ / a	¢ 🗙	
	+		
	VLAN		
	Parent interface net0	\$	

#### 15.2.1.4 Setting up virtual networks (VLANs)

VLAN networks allow separating broadcast domains.

To configure a VLAN on , proceed as follows.

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

4. Add IP addresses to given VLAN.

Note: Select *DHCP* option, to obtain IP address from a DHCP server.

**Note:** The IP addresses are aliases to the physical interface and are used in *servers configuration* as proxy server address.

- 5. Click Active to activate defined VLAN.
- 6. Click Save.

Settings	· ·	
		Enable configured VLAN
	≍ vlan0	× Q Active O DHCP
Enter IP address and networ	k mask	Assign IP address to redundancy group
Notifications	/	/ • • • • • • • • • •
4. External authentication	Ý	Enter VLAN's identifier
III External Add VLAN IP alias	VLAN	
	Parent interface	net0 ¢
Backups and retention	Select VLAN's	parent network interface
		C Reset Save 21 Bridge P VLAN

#### **Related topics:**

- Servers management
- Accounts

#### 15.2.2 Bypasses configuration

Bypasses enable to physically re-route network packages in case of a system failure.

**Note:** Bypasses configuration is not available if Wheel Fudo PAM is running in virtualized environment.

- 1. Select *Settings* > *Network configuration*.
- 2. Select *Bypasses* tab.
- 3. Select bypass mode.
  - Bypass mode permanently enabled this option enforces bypass mode on the network interface card. This mode may be used for maintenance purposes or when troubleshooting network issues.
  - Bypass mode enabled only in case of system failure network packets are re-routed only in case of a system failure or in case the Wheel Fudo PAM is powered off.

- Bypass mode disabled in case of system failure, the network packets will not be routed to the next network appliance.
- 4. Click Save.

### **Related topics:**

• Network interfaces configuration

# 15.2.3 Routing configuration

In default configuration, Wheel Fudo PAM directs all incoming traffic to defined gate. Static routing enables defining routes for packets coming from selected networks.

Note: When defining default route, enter default in the Network field.

Management <	FUDD <sup>®</sup> Administr	ration panel		🚢 admin 🗸	
I Dashboard	Interfaces Name &	DNS Bouting			
E Sessions	Interfaces Name a	DNS Houting		Default network	traffic route
矕 Users	Route Netv	work default	Gateway	10.0.0.1	×
+ Connections	Route Netv	work 172.128.0.16/32	Gateway	10.0.0.2	×
⊖ Servers					
C Policies					

# Adding a route

To add a route, proceed as follows.

- 1. Select  $Settings > Network \ configuration$ .
- 2. Select Routing tab.
- 3. Click Add route to define a new route.
- 4. Enter network address along with the network mask (e.g. 10.0.1.1/32) and gateway address.
- 5. Click Save.

#### Editing a route

To edit a route, proceed as follows.

- 1. Select  $Settings > Network \ configuration$ .
- 2. Select Routing tab.
- 3. Find and edit desired route entry.
- 4. Click Save.

### Deleting a route

To delete a route, proceed as follows.

- 1. Select  $Settings > Network \ configuration$ .
- 2. Select *Routing* tab.
- 3. Find desired route entry and click the delete icon.
- 4. Click Save.

Management <	Fudo <sup>®</sup> Administration panel					🚢 admin 🗸	
I Dashboard	Interfaces Na	me & DNS	Bouting				
E Sessions	interfaces Ha	ne a prio	nouting				
쑬 Users	Route	Network	default		Gateway	10.0.0.1	×
+ Connections	Route	Network	172.128.0.16/3	2	Gateway	10.0.0.2	×
🗇 Servers				Select 1	to delete	e given route entry	
Policies							
📥 Downloads							
🖨 Reports							
Settings							
¢ Network configuration							
O Date & time							
Notifications							
Timestamping							
a External authentication	S	ave confi	ouration ch	anges	_		
A HTTPS Certifcate	0		guration ch	anges			
Resources			l l	C Reset	Save		+ Add Route

#### **Related topics:**

- Network interfaces configuration
- Time servers configuration

# 15.2.4 DNS servers configuration

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

Management	<	Fudo			🛔 admin 🐇 🤶 ?
Jashboard		Interfaces	Name & Dh		
E Sessions		interlaces	Name & Dr	Provide FUDO hostname	
쓭 Users			Hostname	fudo.wheelsystems.com	
🖴 Servers			DNS	10.0.0.1	
Bastions			DNS	×	
+ Connections				Provide DNS server's IP address	
Policies					
🛓 Downloads					
🖨 Reports					
■ Productivity					
Settings					
🖨 System					
O <sup>e</sup> Network configuration					
Notifications					
@ Timestamping					
$a_{\rm e}$ External authentication				Add a DNS server	
III External passwords repositorie	s			C Reset Save	server

#### Adding a DNS server definition

To add a DNS server definition, proceed as follows.

- 1. Select  $Settings > Network \ configuration$ .
- 2. Switch to the Name & DNS tab.
- 3. Click Add new to define new DNS server.
- 4. Enter DNS server IP address.
- 5. Click Save.

#### Editing a DNS server definition

To edit DNS server definition, proceed as follows.

- 1. Select  $Settings > Network \ configuration$ .
- 2. Switch to the Name & DNS tab.
- 3. Find given DNS server and double-click desired field.
- 4. Change parameter value as needed.
- 5. Click Save.

#### Deleting a DNS server definition

To delete a DNS server definition, proceed as follows.

**Note:** Deleting a DNS server definition may cause interruptions in device operation, if system configuration uses hosts names instead of IP addresses.
- 1. Select *Settings* > *Network configuration*.
- 2. Switch to the Name & DNS tab.
- 3. Find and select given DNS server definition.
- 4. Click Delete.
- 5. Click Save .

### Related topics:

- Network interfaces configuration
- Time servers configuration

# 15.3 Notifications

Wheel Fudo PAM can send email notifications concerning defined connections (session start, session end, session inject start, session inject end). Notification service is configured when creating new or editing existing connection. Email notifications service requires configuring SMTP server.

To configure SMTP server, proceed as follows.

- 1. Select *Settings* > *Notifications*.
- 2. Select *Enabled* option.
- 3. Enter configuration parameters for the primary SMTP server.

Management	< Fudo	🛔 admin <  ?
M Dashboard	Sattings Undeline	
E Sessions	Enable email notifications service	
쓜 Users	Enabled	
⊖ Servers	Primary SMTP server Provide main SMTP server configuration parameters	
+∉ Bastions	Host smtp.wheelsystems.com	
+ Connections	Port 25	
Policies	Bind address Any \$	
📥 Downloads	Sender email fudo-dwt-40.50@wheelsvstems.com	
B Reports		
E Productivity	Nequires authentication	
Settings	User Houry	
😂 System	Password	
	Repeat password	
☑ Notifications	Use TLS 🖉 Test server connection	
C Timestamping	Test connection	

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

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

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

e, External authentication	Secondary SMTP serve	er Provide main SMTP server config	guration parameters
III External passwords repositories			
Resources	Host		
Backups and retention	Port	25	
🚓 Cluster	Bind address	Any \$	
LDAP synchronization	Sender email	noreply@fudo.wheelsystems.com	
≡ Events log	Requires authentication	0	
© 25 days i 12345676 9 2 3 00126 J. Not configured	User		
	Password		
	Repeat password		
	Use TLS	Test server connection	
		Test connection	

5. Enter server certificate in PEM format.

a External authentication	Secondary SMTP serv	er Provide main SMTP server config	guration parameters
External passwords repositories			
Resources	Host		
Backups and retention	Port	25	
🚓 Cluster	Bind address	Any 🗘	
LDAP synchronization	Sender email	noreply@fudo.wheelsystems.com	
≡ Events log	Requires authentication	•	
© 25 days i 12345676	User		
	Password		
	Repeat password		
	Use TLS	Test server connection	
		Test connection	

6. Click Save.

### **Related Topics:**

• Accounts

# 15.4 Trusted timestamping

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

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

### Enabling and configuring trusted timestamping

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

- 1. Select Settings > Trusted Timestamping.
- 2. Select *Enabled* option.
- 3. Select from the *Provider* drop-down list the institution providing trusted timestamping services.
- 4. Provide the certificate and the private key of the timestamping service.

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

5. Click Save.

Management <	Fudo <sup>*</sup>	👗 admin < 📿 🤶
Jashboard	Timestamping	
E Sessions	Enable timestamping service	
쓭 Users	Enabled	
⊖ Servers	Provider KIR \$	
•# Bastions	File with certificate and Wybierz pik Nie wybrano pliku	
+ Connections	format	
Policies	Password to file	
🛓 Downloads	Repeat password	
B Reports	Define configuration parameters	
■ Productivity		

### **Related topics:**

• Security measures

# 15.5 External authentication

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

- CERB,
- RADIUS,
- LDAP,
- Active Directory.

#### Authentication servers configuration page

Authentication servers configuration page enables adding new and editing existing authentication servers.

To open the authentication servers configuration page, select Settings > External authentication.

Management	< Fudo <sup>*</sup>	👗 admin 🗸 🔶
M Dashboard	Enternal authentionities	
E Sessions	External authentication	
쯓 Users	Туре	External authentication service type
Servers	Host :	Authentication server IP address and port number
+ Connections		FUDO IP address for commucation with the
Policies	Bind to 10.0.150.150	authentication server
🛓 Downloads	Delete	
🖨 Reports	Delete selected definitio	
E Productivity	Save configuration changes	
Settings	Poset changes	
👺 System	Reset changes	
Oc Network configuration	C Reset Save	+ Add external authentication source
	Add external authenticatio	n server

### Adding a new external authentication server

To add an external authentication server, proceed as follows.

- 1. Select *Settings* > *External authentication*.
- 2. Click + Add external authentication source.
- 3. Select authentication service type.
- 4. Provide configuration parameters depending on selected authentication system type.

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

### 5. Click Save.

## Editing authentication server definition

To edit an authorization server definition, proceed as follows.

- 1. Select *Settings* > *External authentication*.
- 2. Find the server definition and change its configuration as desired.
- 3. Click Save.

# Deleting authentication server definition

To delete authentication server definition, proceed as follows.

- 1. Select Settings > External authentication.
- 2. Find desired server definition and select the *Delete* option.
- 3. Click Save.

### **Related topics:**

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

# 15.6 External passwords repositories

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

# 15.6.1 CyberArk Enterprise Password Vault

## Adding a new passwords repository

- 1. Select Settings > External passwords repositories.
- 2. Click + Add server.
- 3. Select CyberArk Enterprise Password Vault from the Type drop-down list.
- 4. Enter object's name.
- 5. Provide the URL to the paswords server's API.
- 6. Provide application identification.
- 7. Define the account format string.
- 8. Click Save.

## Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

- 1. Select Settings > External passwords repositories.
- 2. Find the repository definition and change its configuration as desired.
- 3. Click Save.

## Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

- 1. Select Settings > External passwords repositories.
- 2. Find desired repository definition and select the *Delete* option.
- 3. Click Save.

# **Related topics:**

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

# 15.6.2 Hitachi ID Privileged Access Manager

### Adding a new passwords repository

- 1. Select Settings > External passwords repositories.
- 2. Click + Add server.
- 3. Select Hitachi ID Privileged Access Manager from the Type drop-down list.
- 4. Enter object's name.
- 5. Provide the URL to the paswords server's API.
- 6. Enter user login allowed to access passwords directory.
- 7. Provide user password in the *Password* and *Repeat password* fields.

8. Click Save.

## Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

- 1. Select Settings > External passwords repositories.
- 2. Find the repository definition and change its configuration as desired.
- 3. Click Save.

### Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

- 1. Select Settings > External passwords repositories.
- 2. Find desired repository definition and select the *Delete* option.
- 3. Click Save.

## **Related topics:**

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

# 15.6.3 Lieberman Enterprise Random Password Manager

### Adding a new passwords repository

- 1. Select Settings > External passwords repositories.
- 2. Click + Add server.
- 3. Select Lieberman Enterprise Random Password Manager from the Type drop-down list.
- 4. Enter object's name.
- 5. Provide the URL to the paswords server's API.
- 6. Define authention module assigned to the user who is allowed to access passwords repository.
- 7. Enter user login allowed to access passwords repository.
- 8. Provide user password in the Password and Repeat password fields.
- 9. Click Save.

### Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

- 1. Select Settings > External passwords repositories.
- 2. Find the repository definition and change its configuration as desired.
- 3. Click Save.

### Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

- 1. Select Settings > External passwords repositories.
- 2. Find desired repository definition and select the Delete option.
- 3. Click Save.

## **Related topics:**

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

# 15.6.4 Thycotic Secret Server

### Adding a new passwords repository

- 1. Select Settings > External passwords repositories.
- 2. Click + Add server.
- 3. Select Thycotic Secret Server from the Type drop-down list.
- 4. Enter object's name.
- 5. Provide the URL to the paswords server's API.
- 6. Enter user login allowed to access passwords repository.
- 7. Provide user password in the *Password* and *Repeat password* fields.
- 8. Define secret string format used for identifying objects on Thycotic Secret Server.
- 9. Click Save.

### Editing a passwords repository

To edit a passwords repository definition, proceed as follows.

- 1. Select Settings > External passwords repositories.
- 2. Find the repository definition and change its configuration as desired.
- 3. Click Save.

### Deleting a passwords repository

To delete a passwords repository definition, proceed as follows.

- 1. Select Settings > External passwords repositories.
- 2. Find desired repository definition and select the *Delete* option.
- 3. Click Save.

# **Related topics:**

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

### **Related topics:**

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

# 15.7 Resources

Wheel Fudo PAM enables customizing RDP and VNC login screen.

Customizable logo —
FUDD
Login
Global announcement
Welcome on FUDO
Please constact your FUDO administrator for more information.
Welcome on HDP-10.0.35.53-WindowsXP
Your actions could be recorded and stored in electronic format. Please conntact your FUDO administrator for more information.

# Changing logo

- 1. Select Settings > Resources.
- 2. Select the RDP or the VNC tab.
- 3. Click *Choose File* button and select desired image.

Note: Maximum image size is 512 x 512 px.

4. Click Save.

Management <	Fudo <sup>*</sup>	🛔 admin 🕤 📍
Jef Dashboard	PDP VMC	
E Sessions		
😁 Users	Logo	
⊖ Servers	Maximum image size: 512 x 512 px.	
• Bastions	Background color code: #02085A.	
+ Connections	wybierz płk. Nie wybrano pliku	
Policies		
📩 Downloads		
🖨 Reports	Restore default	
E Productivity	Global announcement	
Settings		
😂 System		
¢ Network configuration		
Notifications	Provide global login screen announcement	
C Timestamping		

## Restoring default logo

- 1. Select Settings > Resources.
- 2. Select RDP or VNC tab.
- 3. Select *Restore default* option.
- 4. Click Save.

# Defining global announcement

Global announcement is displayed on RDP and VNC login screen.

**Note:** Apart from global announcement, WHEEL Wheel Fudo PAM PAM also enables configuring local server message in server configuration form.

- 1. Select Settings > Resources.
- 2. Select RDP or VNC tab.
- 3. Enter desired message in the *Global announcement* section.
- 4. Click Save.

## **Related topics:**

• Quickstart - RDP

# 15.8 System version restore

In the case there is a problem with the current system revision, it is possible to restore the system to its previous version.

**Warning:** Restoring the system to the previous version will bring back the system's state prior the update. Session data and configuration changes in the current system revision will be lost.

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

- 1. Connect one of the USB flash drives containing the encryption key.
- 2. Select *Restart* from user options menu.

				Display user	options
Management <	Fuc	Administrati	on panel		📤 admin 🗸
I Dashboard	Ungrade	Upload ①	Delete selected		PL
E Sessions	opgrade				EN
👾 Users	Uersi Versi	an	Filename	Size	C Restart
	I 1-12	289	fudo-1-17289.upg	55.8 MB	nt system
+ Connections	I 1-12	361	fudo-1-17361.upg	56.4 MB	st system s
🖴 Servers					6+Logout
0 Policies					

3. Select the previous system revision to be loaded after restarting the system.

Note: Current system version is selected by default.

System res	tart	× Select the system version
Version	2.2-26195 (active)	÷
		Cancel Confirm

4. Click *Confirm* to proceed with restarting the system to the selected revision.

Warning: Restrating the system will terminate all current users' connections.

### **Related topics:**

- System initiation
- System update

# 15.9 System restart

Note:

- System restart requires USB flash drive with the encryption key connected to the device.
- Restrating the system will terminate all current users' connections.
- Use the *Deny new connections* option in the *Sessions* section in the system settings menu.
- 1. Connect one of the USB flash drives containing the encryption key.
- 2. Select *Restart* from user options menu.

					Display user	options
Management		Fudo	Administratio	on panel		📥 admin 🗸
I Dashboard	. De	arada	Upload ①	Delete selected		PL
E Sessions		grade				EN
营 Users	0	Version		Filename	Size	C'Restart
		1-17289		fudo-1-17289.upg	55.8 MB	ot system
++ Connections		1-17361		fudo-1-17361.upg	56.4 MB	it of otom is
🖴 Servers						6+Logout
10 Policies						

3. Select the previous system revision to be loaded after restarting the system.

Note:	Current system	version is	s selected	by	default
-------	----------------	------------	------------	----	---------

System res	tart	×
Marrian		Select the system version
Version	2.2-26195 (active)	÷
		Cancel Confirm
		Proceed with system restart

4. Click *Confirm* to proceed with restarting the system to the selected revision.

# **Related topics:**

- System initiation
- System version restore

# 15.10 SNMP

Wheel Fudo PAM's status can be monitored over SNMPv3 protocol.

# 15.10.1 Configuring SNMP

- 1. Select Settings > System.
- 2. Select *Enabled* option in the *SNMPv3* section.
- 3. From the *IP address* drop-down list select IP address, which will be used for SNMP communication.
- 4. Click Save.
- 5. Select Management > Users.
- 6. Click + Add.
- 7. Select service from the *Role* drop-down list and fill in the rest of the *General* section parameters.
- 8. Select password from the Authentication drop-down list and enter the password string.

Note:

- SNMP user password must be at least eight characters long.
- SNMP service authenticates the service account using the first defined password.
- 9. Select *Enabled* option in the *SNMP* section.
- 10. Select authentication methods from the Authentication method drop-down list.
- 11. Select the SNMP echryption algorithm from the *Encryption* drop-down list.
- 12. Clikc Save.

# 15.10.2 SNMP MIBs

Wheel Fudo PAM supports following MIBs:

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790) partly supported
- UCD-SNMP-MIB

# 15.10.3 Wheel Fudo PAM specific SNMP extensions

### MIB specification file

Provided MIB file specification can be uploaded to the SNMP manager to enable Wheel Fudo PAM specific SNMP extensions.

```
WHEEL-SYSTEMS-MIB DEFINITIONS ::= BEGIN
-- MIB definition for Wheel Systems products
_ _
IMPORTS
       MODULE-IDENTITY, OBJECT-TYPE, Integer32, Counter32, enterprises FROM SNMPv2-
\rightarrow SMI;
wheel MODULE-IDENTITY
       LAST-UPDATED "201702140000Z"
                                       -- 14 February 2017
        ORGANIZATION "www.wheelsystems.com"
        CONTACT-INFO
                 "Postal: Wheel Systems Inc. (USA)
                                        31 N 2nd Street 370,
                                        San Jose, CA 95113
                  Phone: +1 (415) 800 3230
                  email: info@wheelsystems.com"
        DESCRIPTION
        "Top-level infrastructure of the Wheel Systems enterprise MIB tree"
        REVISION
                    "201702140000Z"
       DESCRIPTION
        "First draft"
        ::= { enterprises 24410 }
products OBJECT IDENTIFIER ::= { wheel 1 }
fudo OBJECT IDENTIFIER ::= { products 1 }
sessionTable OBJECT-TYPE
        SYNTAX
                SEQUENCE OF SessionEntry
       MAX-ACCESS not-accessible
       STATUS
                   current
       DESCRIPTION
                "The table of active sessions on Fudo."
        ::= { fudo 1 }
sessionEntry OBJECT-TYPE
       SYNTAX SessionEntry
       MAX-ACCESS not-accessible
       STATUS current
       DESCRIPTION
```

(continues on next page)

(continued from previous page)

```
"An entry for one session type on Fudo. For example, information about
               active RDP sessions."
       INDEX { sessionIndex }
       ::= { sessionTable 1 }
SessionEntry ::= SEQUENCE {
       sessionIndex
                            Integer32,
                            OCTET STRING,
       sessionName
       sessionDescription OCTET STRING,
                          Counter32
       sessionActive
}
sessionIndex OBJECT-TYPE
       SYNTAX Integer32 (1..2147483647)
       MAX-ACCESS read-only
       STATUS
               current
       DESCRIPTION
               "A unique value for each supported sessions on Fudo."
       ::= { sessionEntry 1 }
sessionName OBJECT-TYPE
       SYNTAX
                OCTET STRING
       MAX-ACCESS read-only
       STATUS
               current
       DESCRIPTION
               "A name of session type"
       ::= { sessionEntry 2 }
sessionDescription OBJECT-TYPE
       SYNTAX OCTET STRING
       MAX-ACCESS read-only
       STATUS
               current
       DESCRIPTION
               "A description of session type"
       ::= { sessionEntry 3 }
sessionActive OBJECT-TYPE
       SYNTAX Counter32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
               "A number of active sessions of this type."
       ::= { sessionEntry 4 }
```

```
END
```

### **Related topics:**

- Security measures
- Troubleshooting

# 15.11 Backups and retention

Data retention

Wheel Fudo PAM implements two stage data retention. First data is moved from the internal storage to the external storage connected over fiber channel interface. After defined time period session data is automatically deleted.

To enable data retention service, proceed as follows.

- 1. Select Settings > Backups and retention.
- 2. Select Moving session data to external storage enabled option in the Data retention section.
- 3. Define how long data will be stored locally before it is moved to the external storage.
- 4. Select *Session data removal enabled* option to have the data automatically removed after specified time period.
- 5. Define how long data will be stored before being deleted.

Note: Global retention parameter values have lower priority than the values set in the *accounts*.

6. Click Save.

## System backup

Warning: Data backup contains confidential information.

Data stored on Wheel Fudo PAM can be backed up on an external server running **rsync** service. Backup service has to be enabled on Wheel Fudo PAM and requires uploading external server's public SSH key, to authorize access to Wheel Fudo PAM.

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

**Note:** Sessions data is stored on a compressed file system with compression ratio of up to 12:1. Data is decompressed upon being copied by **rsync** thus it will occupy more space on the target server than indicated by Wheel Fudo PAM storage usage. Make sure there is enough storage space on the target server to store uncompressed data.

To enable automated backups service, proceed as follows.

- 1. Select Settings > Backups and retention.
- 2. Select *Enabled* option in the *System backup* section.
- 3. Click Add SSH public key.
- 4. Paste or upload the remote server user's public SSH key.
- 5. Click Save.
- 6. Run rsync on the backup server:

rsync -avze ssh backup@fudo\_ip\_address:/ <destination\_folder>

Management <	Fudo & admin ~ ?
Dashboard	Backupe and retention
E Sessions	
🗑 Users	Data retention
⊖ Servers	Enabled
- Bastions	Delete session data after days
+ Connections	System backup
Policies	Cystem backup
📥 Downloads	To backup FUDO run rsync -avze ssh backup@10.0.150.150/ <target directory=""> on a remote host.</target>
🔒 Reports	Enabled D Enable sessions data backups creation on external servers
E Productivity	Public SSH key
Settings	Upload backup server user's public SSH key
😂 System	
© Network configuration	
Notifications	
C Timestamping	SHA1
4. External authentication	Delete D
III External passwords repositories	
Resources	Delete Oor Key
Backups and retention	
# Cluster	
LDAP synchronization	Add backup server's SSH key
	Store configuration changes
O 2:31:33.0882658 12345678 \$ 2:1-23003 Not configured	C Reset Save
	Reset changes

# Restoring system from backup

System restore service is provided by Wheelsystems technical support department on terms agreed in the SLA.

### **Related topics:**

- Exporting/importing system configuration
- Security measures

# 15.12 External storage

Wheel Fudo PAM enables storing session data on external storage devices connected to Fudo through a fiber channel interface.

Note: External storage in cluster configuration

- In cluster configuration, each node must have a dedicated WWN object.
- Data stored externally is not replicated between cluster nodes.

# 15.12.1 Configuring external storage

- 1. Select Settings > External storage.
- 2. Select fiber channel cards operating mode.
  - Failover data is transmitted using one fiber channel interface. If the card fails, the other one takes over ensuring continuous availability of the external storage device.
  - Load balancing both fiber channel interfaces are used to transfer data between Wheel Fudo PAM and the external storage device.
- 3. In the *External storage devices* section, select desired *WWN* object and click the icon.

Note: Click the  $\boldsymbol{\mathcal{C}}$  icon to refresh the list of available storage devices.

4. Click Save and proceed with enabling session data retention.

Management <	Fudo		
Jashboard	Conoral		
E Sessions	General		
📽 Users	General		
🗁 Servers	FC card #1	isp0	
Accounts			
ふ Listeners	FC card #2	isp1	•
Safes	Connection mode	load balancer	\$
A-Password changers			
Policies	External storage devices	C	
🕹 Downloads	WWN: 20000004cf2bd686	73.4 GB	م
🖨 Reports	WWN: 2000004cf2bd79a	73.4 GB	<b>Q</b>
■ Productivity			
Settings	WWN: 2000004cf4f77b6	73.4 GB	<b>%</b>
📂 System	WWN: 20000004cf9b0aa3	73.4 GB	<b>%</b>

# 15.12.2 Expanding external storage device

After resizing the WWN object, it must be expanded in Wheel Fudo PAM in order to take advantage of the additional storage space.

Warning: The storage device cannot be down-sized after it has been expanded.

- 1. Select Settings > External storage.
- 2. In the section describing the WWN object click Expand.

Management		👗 admin 🗸	?
III Dashboard	General		
E Sessions			
嶜 Users	General		
🖴 Servers	FC card #1 12345678		
🖉 Accounts	FC card #2 12345678		
Safes		-	
ふ Listeners	Connection mode failover	*	
+ Password changers	WWN: 20000004cf2bd686		
Policies	The mounted resource has been resized to 11 GB, click Expand to enlarge the volume. No	ote	
🛓 Downloads	that after expanding the volume it cannot be down-sized.		
🖨 Reports	Volume usage		
■ Productivity	2GB in use 8GB free		
Settings	Evnand		
🖒 System			

- 3. Confirm expanding external storage.
- 4. Click Save.

#### **Related topics:**

• Backups and retention

# 15.13 Exporting/importing system configuration

Wheel Fudo PAM enables exporting current system state, defined objects and configuration settings, which later can be used to initiate the system.

Warning: Exported configuration data contains confidential information.

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

# 15.13.1 Exporting system configuration

To export system configuration, proceed as follows.

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



# 15.13.2 Importing system configuration

**Warning:** Importing a configuration file and initiating system with imported data will delete all existing session data.

To import a system configuration file, proceed as follows.

1. Select *Import configuration* from the user menu.



- 2. Provide the path to the desired configuration file and click *Confirm*.
- 3. Click *Confirm* to proceed with initiating the system with the imported data.

## **Related topics:**

- Backups and retention
- System initiation
- System update

# 15.14 Cluster configuration

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

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

# 15.14.1 Initiating cluster

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

To initiate Wheel Fudo PAM cluster, proceed as follows.

- 1. Select Settings > Cluster.
- 2. Click *Create cluster*, to display cluster definition options.

Management	<	Fudo <sup>®</sup> Administration panel	👗 admin 🗸
M Dashboard		Cluster	
E Sessions		Giuster	Initiate cluster configuration
쑬 Users		Create cluster	
++ Connections		Join cluster	
⊖ Servers			
Policies			

- 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.

Management <	Fudo <sup>*</sup> Administration panel	🛓 admin 🗸
I Dashboard	Cluster	
E Sessions	UNITED STORES	
쓜 Users	Create cluster Cluster node name	
+ Connections	Name	
🖴 Servers	Description	
10 Policies	Description allowing resource	e identification
📩 Downloads		
🖨 Reports		
Settings		
Ø <sup>e</sup> Network configuration	Address	
O Date & time		
☑ Notifications	Address IP for communicating with cluster hodes	Submit
C Timestamping	Join cluster	finition
$a_{\rm t}$ External authentication		
HTTPS Certifcate		
Resources		

5. Click Submit.

Note: Message concerning cluster key can be ignored when initiating cluster.

#### Related topics:

- Adding cluster nodes
- Editing cluster nodes
- Deleting cluster nodes
- Forcing full data synchronization
- Security: Cluster configuration
- Redundancy groups
- Cluster configuration

### 15.14.2 Adding cluster nodes

**Warning:** Session and configuration data (connections, servers, users, external authentication servers) of the joining node are deleted and initiated with data replicated from the cluster.

To add a node to Wheel Fudo PAM cluster, proceed as follows.

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

Management <	FUゴロ <sup>®</sup> Administration panel		🛓 admin 🗸
M Dashboard	Cluster		
E Sessions			Initiating cluster node information
촬 Users	Name HACluster		
+ Connections	Description High Availability	Cluster	
🖴 Servers	,		
D Policies			
🛓 Downloads			
🖨 Reports			
Settings			
Φ <sup>θ</sup> <sub>0</sub> Network configuration	Address 10.0.8.64		
⑦ Date & time	Force full		
Notifications	Delete		
C Timestamping			
e External authentication			Add cluster node
A HTTPS Certifcate			
Resources		C Reset Save	+ Add 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.

$a_{t}$ External authentication	Cluster node name
HTTPS Certifcate	Name
	Description
Backups and retention	Cluster node description
	Address
	Force full  Synchronization
	Delete
	Store configuration
	C Reset Save + Add Node
	Reset changes

- 6. Click *Submit*, to add node definition.
- 7. Copy cluster key to clipboard.

- 8. Log in to administration panel of the joining node.
- 9. Select Settings > Cluster.
- 10. Click Join cluster.

Management <	Fudo <sup>®</sup> Administration panel	🚢 admin 🗸
	Chuster	
	(Juster	
🖆 Users	Create cluster	
	Join cluster	
	Join existing FUDO cluster	

11. Paste cluster public SSH key and click Submit.

Management <	Fude <sup>*</sup> Administration panel	📥 admin 🗸
I Dashboard	Chuster	
E Sessions	Under .	
쓸 Users	Create cluster	
+ Connections	Join cluster	
🖴 Servers	Cluster public ssh	
Policies	NEY	
📩 Downloads		
🖨 Reports		
Settings		
One of the second seco	Cluster initiating node's SSH key	
O Date & time	Chaster mitiating node 5 COT key	Submit
Notifications		Join cluster
C Timestamping		
a External authentication		
A HTTPS Certifcate		
Resources		

#### **Related topics:**

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

# 15.14.3 Editing cluster nodes

To modify a cluster node's configuration, proceed as follows.

- 1. Select Settings > Cluster.
- 2. Find and edit desired node parameters.
- 3. Click Submit.

### **Related topics:**

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

## 15.14.4 Deleting cluster nodes

To delete a cluster node, proceed as follows.

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

Management <	FUDD <sup>*</sup> Administration panel	📥 admin 🗸
Jashboard	Chuster	
E Sessions	Ciuster	
쓭 Users	Name HACluster	
+ Connections		
🖴 Servers	Description High Availability Cluster	
Policies		
📩 Downloads		
🔒 Reports		
Settinge	la l	
Ø <sup>e</sup> Network configuration	Address 10.0.8.64	
<ul> <li>Date &amp; time</li> </ul>	Force full Synchronization	
Notifications	Delete	
C Timestamping	Select option to exclude given node from cluster	
at External authentication	Concert option to exclude given node nom cluster	
A HTTPS Certifcate	Save configuration changes	
Resources	C Reset Save	+ Add Node

### **Related topics:**

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

# 15.14.5 Forcing full data synchronization

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

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

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

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

Management <	Fudo <sup>*</sup> Administration panel	📥 admin 🗸
Jashboard	Chuster	
E Sessions	Guater	
쑬 Users	Name HACluster	
+ Connections	Description High Availability Cluster	
🖴 Servers	Description right Prenating Onates	
Policies		
📩 Downloads		
🔒 Reports		
Settings		
¢ Network configuration	Address 10.0.8.64	
O Date & time	Force full	
Notifications	Select antion to enforce full data synchronization on given node	
@ Timestamping		
4 External authentication	Course of formation advances	
A HTTPS Certifcate	Save conliguration changes	
Resources	C Reset Save	+ Add Node

# **Related topics:**

- Adding cluster nodes
- Editing cluster nodes
- Deleting cluster nodes
- Security: Cluster configuration

# 15.14.6 Redundancy groups

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

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

### Adding redundancy groups

To add a redundancy group, proceed as follows.

1. Select Settings > Cluster.

- 2. Switch to the *Redundancy groups* tab.
- 3. Click + Add redundancy group.
- 4. Define group properties.

Parameter	Description
Name	Descriptive name of the redundancy group.
ID	Redundancy groups identifier (1-255).
Priority	Redundancy group priority (0-254), the lower the number the higher the
	priority.
	Redundancy group with higher priority assumes the <i>master</i> role and
	handles all requests to monitored servers accessed through IP addresses
	assigned to this group. In case given cluster node crashes, user requests
	are directed to on of the remaining nodes with the highest priority defined
	for given redundancy group.
Interface	Network interface used for communicating with other cluster nodes.

Management <	Fudo <sup>*</sup>	👗 admin <  ?
I Dashboard	Nodes Redundancy groups	
E Sessions	Hodes Hodenaulty groups	
쌸 Users	Enable failover On	
⊖ Servers	Enable failover mechanizm	
• Bastions	Name	
+ Connections	Group ID	
Policies		
📩 Downloads	Priority 0	
🔒 Reports	Network interface Enforce slave role \$	
■ Productivity	Provide configuration parameters	
Settings		
😂 System		
¢ <sup>®</sup> Network configuration		
Notifications	Click to add redundancy group	
C Timestamping		
e External authentication	V Neset V Save	y group

5. Click Save.

### Editing redundancy groups

To modify a redundancy group, proceed as follows.

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

Management <	Fudo		🛓 admin 🗸 🧳
Dashboard	Noder Bedundaneu gr		
E Sessions	Nodes Redundancy gro	bupa	
쓭 Users	Enable failover	On	
⊖ Servers	•••• T		
- Bastions		r.	
+ Connections	Name	Group 255	*
V Policies	Group ID	255	*
📩 Downloads	Priority	0	*
⊖ Reports	Network interface	net1 \$	
■ Productivity	Delete	odify configuration parameters	
Settings	entres annous		
😂 System			
¢ Network configuration	Name	grupa243	*
Notifications	Group ID	243	*
@ Timestamping	Priority	0	*
ae External authentication	Network interface	nett *	
III External passwords repositories	Network Intellabe	-	
Resources	Delete		
Backups and retention			
📥 Cluster		Store changes	
LDAP synchronization		C Reset Save	+ Add redundancy group

# 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.

Management <	Fudo		🛓 admin 🗸 🧳
Jashboard	Nodes Redundancy or	oups	
E Sessions			
👻 Users	Enable failover	On	
⊖ Servers	<b>1</b> Terran		
•l# Bastions			1.
+ Connections	Name	Caroup 255	ран (т. 1997) 1997 — При стан (т. 1997) 1997 — При стан (т. 1997)
Policies	Group ID	255	*
🛓 Downloads	Priority	0	*
🖨 Reports	Network interface	net1 4	
■ Productivity	Delete		
Settings	1	Delete selected redundancy group	
🝃 System			
¢\$ Network configuration	Name	grupa243	*
Notifications	Group ID	243	*
@ Timestamping	Priority	0	*
a, External authentication	Network interface	nott A	- -
III External passwords repositories	Network Interlace		
Resources	Delete		
Backups and retention			
🚓 Cluster		Store changes	
LDAP synchronization		C Reset Save	+ Add redundancy group

## Demoting a redundancy group

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

To demote a redundancy group, proceed as follows.

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

Management <	Fudo		🛔 admin 🗸 🥊 🤶
Dashboard	Nodas Redundancy a		
E Sessions	Nodes Redundancy gr	oups	
뿔 Users	Enable failover	On	
⊖ Servers	<b>J</b> Tennora		
•∉ Bastions			
+ Connections	Name	Group 255	*
V Policies	Group ID	255	*
📥 Downloads	Priority	0	*
B Reports	Network interface	net1 4	
■ Productivity	Delete	0	
Settings	militine I Dawona		
😂 System	Demote se	elected redundancy group	
¢ Network configuration	Name	grupa243	*
Notifications	Group ID	243	*
@ Timestamping	Priority	0	~ ]*
a, External authentication			
## External passwords repositories	Network Interface	neti	9
Resources	Delete	0	
Backups and retention			
🚓 Cluster		Store changes	
		Streset Save	+ Add redundancy group

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

### Enforcing a slave role

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

To enforce a permanent slave role on a redundancy group, proceed as follows.

- 1. Select Settings > Cluster.
- 2. Switch to the *Redundancy groups* tab.
- 3. Find desired redundancy group and select Enforce slave mode from the *Interface* dropdown list.
- 4. Click Save.

### **Related topics:**

- Security: Cluster configuration
- Initiating cluster
- Cluster configuration

# 15.15 Events log

System log is an internal registry of users activities which influence system state (login information, administrative actions, etc.).

To display system log contents, select Settings > System log.

Management Add filte	r to limit the nur	mber of dis	played log	entriesExport events log entries&admin ~ ?
M Dashboard	Events log			Add filter > Export logs / Configure syslog Search Q
E Sessions				
誉 Users	Timestamp	Log level	Component	
0.0	2014-12-22 14:08:25	Info	fudoauth	User admin authenticated using password logged in from IP addres: 10.0.1.35.
🖂 Servers	2014-12-22 14:07:29	Info	fudoauth	User admin authenticated using password logged in from IP addres: 10.0.1.36.
+ Connections	2014-12-22 12:59:39	Info	fudoauth	User admin authenticated using password logged in from IP addres: 10.0.1.36.
10 Policies	2014-12-22 12:06:10	Info	gui	User admin created connection RDP (771109632230817793).
	2014-12-22 12:05:45	Info	fudod	Reloading configuration.
La Downloads	2014-12-22 12:05:45	Info	gui	User admin created server WINDOWS 2000 (771109632230817793).
🖨 Reports	2014-12-22 12:02:20	Info	gui	User admin created user "tomek" (771109632230817794).
The Departmenting in the	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'granted_to_users' from '[77110963223
	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'language' from 'en' to 'pl'.
Settings	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'valid_to' from 'None' to '[u'2015-01-21'
😂 System	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'valid_since' from 'None' to '[u'2014-12
and black and a second second second	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'account_validity' from 'None' to '30'.
© Network configuration	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'granted_users' from '[ <simplelazyobje< td=""></simplelazyobje<>
Notifications	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'phone' from '' to '733569593'.
2 Timestamping	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'organization' from 'None' to 'Wheel Sys
C Threatamping	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'full_name' from " to 'TD'.
e External authentication	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'email' from '' to 't.dwornicki@wheelsyst
III External passwords repositories	2014-12-22 12:02:20	Info	gui	User admin changed user tomek (771109632230817794). Changed field: 'name' from " to 'tomek'.
	2014-12-22 12:00:59	Info	fudoauth	User admin authenticated using password logged in from IP addres: 10.0.1.36.
Resources	2014-12-22 12:00:48	Info	gui	User admin changed network interfaces settings.
Backups and retention	2014-12-22 12:00:48	Info	gui	User admin deleted address 192.168.1.1 from interface net0
љ. Cluster	2014-12-22 12:00:48	Info	fudod	Reloading configuration.
	2014-12-22 11:59:51	Info	gui	User admin changed network interfaces settings.
	2014-12-22 11:59:51	Info	gui	User admin added address 10.0.45.90/16 to interface net0 with enabled management and disabled cluster address
≡ Events log	2014-12-22 11:59:51	Info	fudod	Reloading configuration.
	2014-12-22 11:59:20	Info	fudoauth	User admin authenticated using password logged in from IP addres: 192.168.1.150.
© 2:09:53.724216 i 11221122	2014-12-22 11:59:02	Info	fudoocrd	Started successfully.
% 2-20062	2014-12-22 11:58:59	Info	eventd	Started successfully.
	2014-12-22 11:58:59	Info	dbrecvd	Started successfully.

### External syslog servers

Adding a Syslog server

To add a *Syslog* server, proceed as follows.

- 1. Select Settings > Events log.
- 2. Click *Configure syslog* to display syslog servers configuration settings.
- 3. Select *Enable events logging on syslog servers* option to activate sending logs to defined syslog servers.
- 4. Click +.
- 5. Provide server's IP address and port number.
- 6. Click Save.

Note: Log entries sent to syslog servers are formatted as follows:

```
[<log_level>] (<component_name>) (object_name: object_id) <message>
Example:
```

[INF0] (fudordp) (fudo\_server: 848388532111147015) (fudo\_session: 848388532111147219) (fudo\_user: 848388532111147012) (fudo\_connection: 848388532111147014) User user0 authenticated using password logged in from IP addres: 10.0.40.101.

## Editing Syslog server definition

To edit a *Syslog* server definition, proceed as follows.

- 1. Select Settings > Events log.
- 2. Click *Configure syslog* to display syslog servers configuration settings.
- 3. Find and edit desired syslog server definition.
- 4. Click Save.

Deleting Syslog server definition

To delete a *Syslog* server definition, proceed as follows.

- 1. Select Settings > Events log.
- 2. Click *Configure syslog* to display syslog servers configuration settings.
- 3. Find desired server definition and click the i icon.
- 4. Click Save.

## Exporting events log

To export events log entries, proceed as follows.

- 1. Select Settings > Events log.
- 2. Click *Export logs* and select where to save exported log entries.

# **Related topics:**

- Security
- Managing servers

# 15.16 Integration with CERB server

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

### **CERB** server configuration

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

			Click to add	new client defi	nition.		
CERB - Adminis	stration p	pane	(version v1.5)				
Main menu	~	List	of clients				
🌡 Users	+		Client IP	Name	Server Radius password	Blockage	
SS Groups	+	1	127.0.0.1	None	<b>a</b> /		
🙀 Services	+	2	10.0.35.1		<b>₽</b>		
💂 Occurrences diary	+						
Cence Licence	+						
😰 Settings	+						
🐺 Radius clients	=						
C Add there lient							
C Delete the client							
🖲 Block the client							
🚯 Unblock the client		14		> > 2			

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

Enter FUDO	configuration parameters.	
lding a Radius client		
Client IP: 👷	10.0.6.61	
Client name: 🐰	FUDO	
Password: 👳	•••••	Generate
Clear/Defau	It settings Save	Close
Click to store configuratio	n settings.	

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

- 2. Adding user group.
- Select  $Groups > Add \ group$  to define Wheel Fudo PAM users who will be authorized by the CERB server.

	—	Click	to define new user group.			
CERB - Administration panel (version v1.5) polski   english   log out						
Main menu	~	List	of groups			
🌡 Users	+		Group name Comment			
St Groups	Ξ	1	cerb:admins			
Add group		2	fudo_grupa			
Belete group						
Services	+					
📃 Occurrences diary	+					
Eicence	+					
Settings	+					
🐺 Radius dients	+					
logged in as: admin						
date and time on the ser 2012-12-20 11:44	ver:	14	4 Page 1 of 1 ▷ ▷ 2	Displaying 1 - 2 of 2		

• Enter group's name (fudo\_users) and click Save.

Provie	de basic inform	ation.			
Adding group					×
Group basic settings					
Group name: 👷 fudo_users					0.0
Comment: 👷 FUDO users					<i>2</i>
Additional attributes Services	Server Radius (e	external) options			
Attribute name	Attribute value			Add an attribute	Delete an attribute
Attribute name		Attribute value			
c	lear/Default setting	gs Sare		lose	
			)		
Click to add group de	finition.				

- 3. Adding user.
- Select  $Users > Add \ user$  to open new user definition window.

	Clie	ck to define new	v user.						
CERB - Administration	pane	el (version v1.5)							
Main menu 🔍		All users 🛛 🥃	Active u	sers 🛛 🔁 Bl	ocked users	🕞 Expired us	ers 🛛 🕥 Users synchronize	d with Active	Directory
👌 Users 📃	Gro	ups : All groups		~	Search:	Type in a searc	hed phrase		2
& Add Nser		User name		Comment			Authentication module	St	
Delete user	1	admin					Static password		
🖧 Block user	2	cerbuser		Testowy u	tytkownik Fl	JDO-CERB	🛯 CerbToken	۲	
lublock user									
S Groups +									
Services +									
Provide the second seco									
Elicence +									
Settings +									
Radius clients +									
logged in as:			_						
admin		Page 1	of 1					Displaying	1 - 2 of 2
date and time on the server: 2012-12-20 11:49	4	All methods	🗓 Cerb	Token	CerbToken	🚽 SMSToken	Static password 🛛 🕄	Radius	

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

any use				
User's settings				
User name: 👷	john_smith			
Comment: 👷	John Smith			
Authentication module: 👷	CerbToken (time-based, multi-profile)			
Authentication options Ad	ditional attributes Groups Account's expiration			
Type of token:	literal 🗸			
Generation frequency:	10 seconds			
Token's length:	6			
Static password:	Set a static password			
Application's identification:				
	Clear/Default settings Save Close			

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

• Assign user to previously created fudo\_users group and click Save.

Wybierz z	akładkę aby przy	vpisać użytkownikowi grupę.	
Dodawanie użytkownika			×
Ustawienia użytkownika			
Nazwa użytkownika: 👷	jan.kowalski		
Opis: 👳	Jan Kowalski		
Moduł uwierzytelnienia: 👳	CerbToken (czas	owy, wieloprofilowy)	
Opcje uwierzytelnienia Atrybuty	/ dodatkowe	Jpy Okres ważności konta	
fudo_users	<b>€</b>	cerb:admins test_users	
	Przypisz u	użytkownikowi grupę.	
	'yczyść/Domyślne w	vartości Zapisz Th Zamknij	
Kliknij aby dodać	użytkownika.		

- 4. Configuring service.
- Select *Service* > *Add service* to open new service definition window.

		Clie	ck to define new servi	ce.				
CERB - Administration panel (version v1.5) pole								log out
Main menu	~	List	t of services					
🖁 Users	+		Service name	C	omment	Attribute NAS-IP-Ad	Attribute NAS-I	
SS Groups	+	1	cerb:mgmt					
🙀 Services	Ξ	2	fudo					
Add service								
Belete service								
📃 Occurrences diary	+							
Eicence	+							
Settings	+							
🐺 Radius clients	+							
logged in as: admin								
date and time on the serve 2012-12-20 12:05	er:							
		14			æ		Displaying	1 - 2 of 2

• Provide name identifying authorization service (cerb\_fudo) and service description.
• Add fudo\_users group to service and click Add.

Enter b	asic service informati	on.	)	
lding a service				l
Service data			_	
Service name: 👷	cerb_fudo			
Comment: 👷	Authenticating (	user		
Advanced Additional a	ttributes Groups		Click to assign a group.	
Selected			Available	
fudo_users			cerb:admins	٦
			fudo_grupa	
				1
		to s	opico	
	Assign user group	10 3	ervice.	
	Add (	5	Cancel	
			Click to store service definition.	

#### Wheel Fudo PAM server configuration

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

Management <	Fudo <sup>*</sup> Administration panel & sdmin ~	
M Dashboard	External authentication	
E Sessions		1
쓥 Users		
+ Connections		
⊖ Servers		
V Policies		
📩 Downloads		
⊖ Reports		
Settings		
A <sup>o</sup> Network configuration		
② Date & time		
Notifications		
C Timestar Access external au	nentication sources configuration page	
External authentication	Click to add external authentication service	
HTTPS Certifcate		
Resources	CReset Save + Add External Authentication Source	

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

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

• Click Save.

		Select 'Cerb' type and provide	host information
	Туре	Cerb \$	
	Host	10.0.35.52	
	Port	1812	
В	ind to	10.0.8.64 \$	Select IP address for communicating with CERB ser
Se	ervice	fudo	Provide service parameter as configured in CERB fo authenticating FUDO users
S	Secret		
Repeat s	secret		Provide RADIOS client password as delined in CER

- 2. Adding user.
- Select Management > Users.
- Click Add.

umin v
Add filter ~
Status
Active
Active
Active
Blocked
Active
Active
Active
Active
ISSWORD Active
Active
Active
ISSWORD Active
Active
Active

• Provide basic user information.

Note: Username must match the user name defined on CERB server.

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

Create user	Provide user information	
eneral	Trovide discrimination	
Usemame	ian.kowalski	
Pala		
Hole	user 🕴	
Synchronize with LDAP	0	
Blocked	0	
Full name	Jan Kowalski	
Email	jan@kowalski.pl	
Organization		
Phone		
AD Domain		,
LDAP Base		
ermissions		
Granted users	Q	
uthentication		
Туре	External Authentication +	
External	Cerb 10.0.35.52 service:fudo \$	
authentication source		
Selec	t external authentication option a	and choose previously add
Tune		
1359	•	
Delete		
	C Reset 🗸 Save	
	Save user definition	

- 3. Adding connection.
- Select Management > Connections.
- Click + Add.

Management <	Fuda	Administration panel	📥 admin 🗸	
Dashboard	Connection	s Add connection Block Ur	iblock Delete Ad	ld filter ~
Access connections	managemer	nt page	Servers	Status
Add con	nection defir	nition	www.mobter.com , www.mbank.com.pl	Active
+ Connections	MYSQL	administrator, user1, user2, user3, user4, user5	root@MYSQL-10.0.35.52	Active
Servers      Policies	RDP- FORWARD	administrator	RDP-10.0.8.102 , RDP-TLS-10.0.8.103	Active
📩 Downloads	RDP- REPLEACE	user1, user2, user3, user4, user5, z	administrator@RDP-10.0.35.54, administrator@RDP-TLS-10.0.8.103 , admin@RDP-10.0.40.102-hardening , administrator@RDP- 10.0.35.54-15	Active
Reports	SSH- REPLACE	fudo_user1, fudo_user2, fudo_user3, fudo_user8, fudo_user9, user1, user2, user3,	root@10.0.35.52 - SSH	Active
Settings		user4, user5, z		
¢ <sup>e</sup> Network configuration	TELNET	admin, administrator, user1, user2, user3, user4, user5	TELNET-10.0.35.52	Active
O Date & time	UNC			Active
Notifications	anonymous	anonymous	www.ipko.pl , 10.0.35.53	Active
	oracle-test	user1	cerb@10.0.7.11 - ORACLE	Active
Le Timestamping	i test		RDP-10.0.35.54	Active

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

Create connection	on	
General		
Name	web_server Provide connection name	
Notifications	Session start Session finish Session inject open Session inject close Session policy match	ation options
Users	ImAnwalabl	
Retention time (in days)	Define session data retention	
RDP Functionality	<ul> <li>✓ Clipboard redirection ✓ Sound redirection ✓ Device redirection</li> <li>✓ Dynamic Virtual Channels ✓ Audio input redirection ✓ Multimedia redirection</li> </ul>	
SSH Functionality	ଟ୍ଟ Sessions ଟି Port forwarding ଟି Terminal ଟି Environment ଟି X11 ଟି SSH Agent forwarding ଟି Shell ଟି SCP	
VNC Functionality	Client Cut Text @ Server Cut Text	
Permissions		
Granted users	6	
Servers		
Server	RDP-10.0.35.54	
Policy	•	
Replace user?	Forward original login ¢	
Replace secret?	Forward original password	
Se	lect server and choose user authentication mode	
	C Reset Save	
Sa	ve connection definition	

# 15.17 System maintenance

The following section contains descriptions of maintenance procedures.

#### 15.17.1 Backing up encryption keys

Encryption keys stored on USB flash drives are necessary to initialize the file system, which stores session data. If the USB flash drive is lost or damaged, it will be impossible to boot the system and access session data.

#### Microsoft Windows

**Warning:** After connecting the flash drive to your computer, do not initiate or format it. Ignore the system message about it not being able to read data and proceed with the backup procedure.

1. Download and install HDD Raw Copy Tool.

http://hddguru.com/software/HDD-Raw-Copy-Tool/ (portable version is also available)

- 2. Start the program.
- 3. On the source drive selection window, choose the USB drive with the encription key and click *Continue*.

BUS         MODEL         FIRMWARE         S           SATA         ST1000DM003-9YN162 (C:)         CC48         1           SATA         SanDisk SDSSDHP256G         X2306RL         3           USB         Generic Flash Udisk (D:)         0000         b	ERIAL NUMBER 154D6GRM 113375042199	LBA 1,953,525,168	CAPACITY 1000.2 GB
USB Generic Flash Udisk (D:) 0000 b		300,110,172	256.06 GB
FILE IMAGE of Generic Flash Udisk 0000 b	pa9359411649 pa9359411649	7,864,192 7,864,192	4026.46 MB 4026.46 MB

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

📓 HDD Raw	Copy Tool 1.10 Free	-		×
SOURCE: TARGET:	[2] Generic Flash Udisk 0000 [4026.46 MB] [FILE] C:\Users\wheel\Documents\pen.imgc Copyri	ght ©2005-2013 HDI	A DGURU.(	COM
12/15/20 12/15/20 12/15/20 12/15/20 12/15/20	16 3:22:01 PM 16 3:22:01 PM HDD Raw Copy Tool 1.10; http://hddguru.com 16 3:22:01 PM 16 3:22:01 PM Source: [2] Generic Flash Udisk 0000 [4026.46 MB] 16 3:22:01 PM Target: [FILE] C:\Users\wheel\Documents\pen.imgc			< >
Current	task progress Stop	START	>	
[2] Generic F	ash Udisk 0000 [4026.46 MB] >>> [FILE] C:\Users\wheel	\Documents\pen.in	ngc	

6. Once the following message occurs

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

A HOD Raw	Copy Tool 1.10 Fre	e				-		$\times$
SOURCE: TARGET:	[2] Generic Fla [FILE] C:\Users	sh Udisk 0000 [4 \wheel\Document	4026.46 MB] s\pen.imgc		Copyright (	02005-2013 HD	DGURU	About
COPY					cohlugure		000110	
12/15/20 12/15/20 12/15/20 12/15/20 12/15/20	16 3:22>41 PM Co 16 3:26:37 PM Re 16 3:26:37 PM So 16 3:26:37 PM Av 16 3:26:37 PM Op	pying ad Error occurred a urce was unplugge eraze speed: 12.9 peration terminated	at offset 2,493,44 d, aborting MB/s d at offset 2,493	18,192; LBA 4,8 ,448,192 LBA 4	70,016 (The sy: 4,870,016	stem cannot fir	nd the fi	~
< Current	task progress						>	
62% c	complete	12.9 MB/	5					
Curren	nt sector: 4,	874,112		Stop		START		

- 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.

HDD RAW COPY TOOL 1.10       Free       WWW.HDDGURU.COM         BUS       MODEL       FIRMWARE       SERIAL NUMBER       LBA       CAPACITY         SATA       STI000DM003-9YN162 (C:)       CC48       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         HLE       Double-click to open file          USB       Open Disk Management Console         Copyrright @ 2005-2013 HDDGURU.COM       Please select TARGET       Continue >>>       Continue >>>	TARGET Device Selection - HDD Raw Copy Tool 1.10	Free				×
BUS       MODEL       FIRMWARE       SERIAL NUMBER       LBA       CAPACITY         SATA       ST1000DM003-9YN162 (C:)       CC48       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           Copen Disk Management Console         Copyright ©2005-2013 HDDGURU.COM       Please select TARGET       Continue >>>       Continue >>>       Continue >>>	HDD RAW COPY TOOL 1.10 Free			WWW.HDDGUF	IU.COM	
Copyright © 2005-2013 HDDGURU.COM Please select TARGET Continue >>>	BUS     MODEL       SATA     ST1000DM003-9YN162 (C:)       SATA     SanDisk SDSSDHP256G       USB     Generic Flash Udisk (D:)       FILE     Double-click to open file	FIRMWARE CC48 X2306RL 0000	SERIAL NUMBER 154D6GRM 313375042199 ba9359411649	LBA 1,953,525,168 500,118,192 7,864,192	CAPACITY 1000.2 GB 256.06 GB 4026.46 MB	
Disks found 3						

10. Click Continue.

- 11. Click START.
- 12. The copying will end once the following message occurs:

Operation terminated at offset....

HDD Raw Copy Tool 1.10 Free	-		×
SOURCE:         [0] IMAGE of Generic Flash Udisk 0000 [4026.46 MB]           TARGET:         [2] Generic Flash Udisk 0000 [4026.46 MB]           Copyright © 200	05-2013 HDC	A GURU.C	bout :OM
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         L2/15/2016 3:39:38 PM       Operation terminated at offset 2,493,448,192         L2/15/20	START	>	•
[0] IMAGE of Generic Flash Udisk 0000 [4026.46 MB] >>> [2] Generic Flash Udisk 0000	[4026.46 N	AB]	

13. Close the application and disconnect the USB drive.

#### Mac OS X

- 1. Start the terminal.
- 2. Execute the sudo -s command and enter password.
- 3. Execute the diskutil list to list connected drives.
- 4. Find the drive with the following partitions layout:

```
/dev/disk2 (external, physical):
#: TYPE NAME SIZE IDENTIFIER
0: GUID_partition_scheme *8.0 GB disk2
1: F649773F-1CD6-11E1-9AD2-00262DF29F0D 3.1 KB disk2s1
2: 2B163C2B-1FE5-11E1-8300-00262DF29F0D 1.0 KB disk2s2
```

- 5. Execute the dd if=/dev/disk2 of=fudo\_pen.img bs=1m command, where if points to the USB drive.
- 6. Disconnect the flash drive and connect the new one.
- 7. Execut the dd if=fudo\_pen.img of=/dev/disk2 bs=1m command.
- 8. Execute the sync command.
- 9. Disconnect the USB flash drive from your computer.

#### Linux

- 1. Start the terminal.
- 2. Execute the sudo -s command and enter password.
- 3. Execute the dmesg | less command to determine the USB flash drive identifier.
- 4. Execute the dd if=/dev/disk2 of=fudo\_pen.img bs=1m command, where if points to the USB drive.
- 5. Disconnect the flash drive and connect the new one.
- 6. Execut the dd if=fudo\_pen.img of=/dev/disk2 bs=1m command.
- 7. Execute the sync command.
- 8. Disconnect the USB flash drive from your computer.

#### Related topics:

- Events log
- Frequently asked questions

#### 15.17.2 Monitoring system condition

Monitoring system condition allows preventing system failures and overloads, ensuring Wheel Fudo PAM Wheel Fudo PAM remains operational.

#### Monitoring active sessions

- 1. Login to Wheel Fudo PAM administration panel.
- 2. Select Management > Dashboard.
- 3. Check the number of currently running user sessions.

Note: Wheel Fudo PAM supports up to 300 RDP connections.

#### Monitoring network bandwidth

- 1. Login to Wheel Fudo PAM administration panel.
- 2. Select Management > Dashboard.
- 3. Check current network transfer rate.

**Note:** Wheel Fudo PAM features 1Gbps network interface cards. In case the current network bandwidth usage exceeds 500Mbps, users may notice a decrease in system communication performance.



**Related topics:** 

- System log
- Frequently asked questions

#### 15.17.3 Hard drive replacement

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

#### Replacing a hard drive

1. Move the front bezel release latch to the left and take the front bezel off.



2. Push the hard drive tray lever release button and pull the lever to take out the tray from the chassis.



- 3. Unscrew the screws securing the hard drive and take out the hard drive from the tray.
- 4. Install replacement hard drive in the tray and secure it with the screws.
- 5. Install the hard drive tray back in the server.

**Note:** Wheel Fudo PAM will automatically detect the change in the storage array state and will start rebuilding the data structure. The duration of the array rebuilding process depends on the volume of data stored on the server.

#### Related topics:

- $\bullet \ Hardware \ overview$
- Frequently asked questions

# CHAPTER 16

# Reference information

# 16.1 RDP connections broker

Connections broker enables users to reconnect to their existing sessions on a specific server within a pool of load-balanced resources.

If the broker identifies an existing user session on another server, the connection will be redirected to it and the user will be prompted to login again.



**Note:** To successfully redirect a connection, the server identified by the broker must be defined on Wheel Fudo PAM, it must listen on default RDP port (3389) and user must be allowed to connect to given server.

#### **Related topics:**

- Data model
- RDP
- Servers
- Accounts

# 16.2 Error codes

Error code	Error message and description
FSE0001	Internal system error
FSE0002	FUDO certificate error.
FSE0003	Unable to change configuration settings.
FSE0004	Configuration import error
FSE0005	Unable to initialize \${disk}.
	Replace defective drive.

**Note:** Hard drives numbering starts from 0. If there is a problem with the hard drive number 1, physically it's the second drive in the top row.

FSE0006	Invalid license
FSE0007	Unable to find license file
FSE0008	Unable to attach hard drive \${disk}.
FSE0009	Upgrade failed.
FSE0010	License expired.
FSE0020	System backup error.
FSE0024	Hard drive belongs to another FUDO (\${diskserial}) \${disk}.
FSE0026	Cluster communication error.
FSE0028	Unable to join node to cluster.
FSE0031	Timestamping service communication error.
FSE0032	Unable to timestamp session.
FSE0033	Unknown timestamping service provider.
FSE0040	Cluster communication error. Local FUDO version is %s than %s FUDO
	version.
FSE0046	There is no filter called %s.
FSE0048	Error authenticating user over RADIUS.
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.
FSE0061	Incorrect password repository configuration: login is empty.
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.

Continued on next page

Error code	Error message and description
FSE0066	Unable to block user %jd.
FSE0067	Error connecting to Lieberman ERPM server %s: incorrect URL in con-
	figuration.
FSE0068	Error connecting to Lieberman ERPM server %s: incorrect protocol spec-
	ified.
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.
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 at-
	tempt%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).
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.
FSE0098	Error fetching password from Thycotic server %s: unable to get password
	for user %s for the %s server.
FUE0099	Connection terminated.
FUE0101	Unable to find matching HTTP connection.
FUE0103	HTTP connection error.
FUE0106	Authentication failed: %s.
FUE0108	MySQL connection error.
FUE0110	Oracle connection error.
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.
FUE0124	SSH connection error.
FUE0125	User %s failed to authenticate after %d attempts. disconnecting.
FUE0127	Invalid authentication method: expected passwordor sshkey. aot %s.
	I I

Table 1 -continued from previous page

Continued on next page

Error code	Error message and description
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).
FUE0132	Client requested incorrect terminal dimensions (%dx%d).
FUE0133	MSSQL connection error.
FUE0134	TN3270 connection error.
FUE0135	Unknown TN3270 command: %02x.
FUE0136	Telnet connection error.
FSE0137	Unable to read private key.
FSE0138	Server's certificate does not match configured certificate.
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.
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.
FAE0153	Session indexing failure.
FAE0154	Session conversion failure for session %s.
FAE0165	Error authenticating user <user_name>.</user_name>
FAE0189	<i>Error saving NTP servers: <server_name>.</server_name></i>
FAE0232	MySQL session playback error.
FAE0267	Error generating report %d: %s.
FSE0283	Unable to process pattern: %s.
FSE0285	Unable to read certificate.
FSE0286	No peer certificate received.
FSE0290	Unable to add server %s because %s is listening on same IP address and
	port.
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
- DGD0000	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.
FUE0314	Invalid pixel format.
FUE0315	Unable to fetch standard RDP certificate.
FUE0316	Protocol security negotiation failure.
FUE0317	Unable to establish connection to server %s.
г UEU317	Unable to establish connection to server %s.

Table 1 – continued from previous page

Continued on next page

Error codo	Error massage and description
	Unable to fetch SSL contificate
F UE0310	Bad login field configured on convert Error while proceeding year %
FSE0330	Error while processing user Assaut Control value of user %.
FUE0246	Client cent a nachet biggen then %d butce
F UE0340	Client sent a packet orgger than %a oytes.
F 5E0347	FUDO version: \${rversion}.
FSE0348	Unable to get configuration settings.
FUE0351	Client sent unsupported NTLM v1 response.
FSE0352	Bastion requires login and server delimited with one of '%s' (%s).
FSE0355	Inconsistent data, starting recovery replication to node \${name}.
FUE0359	Server rejected X11 connection: %.*s.
FUE0360	Server requires unsupported X11 authentication: %.*s.
FSE0362	Unable to propagate ARP.
FUE0363	User %s has no access to host %s:%u.
FUE0365	RDP server %s:%u has to listen on the default RDP port in order to
	redirect sessions.
FSE0366	<i>Error connecting to CyberArk server %s: incorrect URL in configuration.</i>
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.
FSE0372	Unable to invalidate OTP password %jd.
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 delimited with a '%s' character (login: %s)
FSE0378	Unable to establish connection, could not find a server (login: %s).
FSE0379	Unable to establish connection, could not find specified transparent server
1,520010	(tcp://%s:%u) (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.
	Unblock the safe in question to allow users to connect to servers which
	use this safe.
FSE0420	Unable to authenticate user %s against server %s.
FSE0461	Invalid data from AD server.
FAE0464	User %s is not allowed to login from address %s.
	Add the specified IP address in the user object configuration in the $API$
	section.

Table 1 -continued from previous page

# 16.3 Fudo 2.2 to Fudo 3.0 parameters mapping

This topic describes how certain parameters from Fudo  $2.2~\mathrm{map}$  to Fudo  $3.0~\mathrm{data}$  model.

## 16.3.1 Connection

Management <	Fudo					Management <	FU	do <b>'</b>			
I Dashboard	Connection						A.000	unt			
E Sessions	Connection				-		ACCO	Junt			
曾 Users	General						Gene	ral			
⊖ Servers	Name			10				Name			*
<b>-</b> ∉ Bastions						Accounts					
++ Connections	Blocked	0				Safes		Blocked			
D Policies	Notifications	<ul> <li>Session start</li> <li>Session ioin</li> </ul>	<ul> <li>Session finish</li> <li>Session leave</li> </ul>					Туре	regular		¢ =
* Downloads		Session policy match						Session recording	all		
A Paparta	Users			୍ତ୍				ocosion recording			
	Session recording	Complete						OCR sessions			
	contracting	o singhold		•				Delete session data after			days
Settings	OCR sessions					En Deselvetivity					
System	Delete session data after			days	J	Settings		0			
© Network configuration	Time policies							Granted users			ંચ
Notifications	Protocol functionality						Serve	r			
C Timestamping	recoordinationality					Notifications		Server	SSH-0-10.0.35.52		e :
At External authentication	RDP 🗹	<ul> <li>Clipboard redirection</li> <li>Device redirection</li> </ul>	<ul> <li>Sound redirection</li> <li>Dynamic Virtual Channels</li> </ul>			C Timestamping					
III External passwords repositories		Audio input redirection	Multimedia redirection			≪ External authentication	Crede	entials			
Resources	Maximum RDP sessions resolution	Any		¢		External passwords repositorie		Domain			
Backups and retention	SSH 💋	Sessions	Port forwarding			Resources					
🚓 Cluster		Z X11	SSH Agent forwarding			Backups and retention		Login			
LDAP synchronization		SFTP	SCP			🖞 Cluster		Replace secret with			•
≡ Events log	VNC 🗹	Client Cut Text	Server Cut Text					Password change policy	Static, without restrictions		¢
	Permissions					≡ Events log	Pass	word changer			
© 0.04:11.988641i 12545678							1 400	ford onlangor			
	Granted users			୍ତ୍		9 3-30968				C Reset Save	
	Servers										
	Server			•							
	Policies			୍							
	Replace user										
	Replace secret										
	Delete										
		2R	eset Save			+ Add server					



#### 16.3.2 Server

Management <	Fudo			Management <	Fudo			
Je Dashboard	0 mm m			Jashboard	Listense			
E Sessions	Server			E Sessions	Listener			
쌸 Users	General			설 Users	General			
🖴 Servers	Name			Servers		Name		*
+@ Bastions				Accounts				
+ Connections	Blocked	0		Safes	В	Blocked		
Policies	Protocol	RDP	¢	ন Listeners	Pi	rotocol	RDP	¢ #
🛓 Downloads	Security	Enhanced RDP Security (TLS) + NLA	\$	n- Password changers	s	Security	Enhanced RDP Security (TLS) + NLA	\$
🔒 Reports	Anonymous			Policies	Annound	cement		
■ Productivity	Ask for login reason			Downloads				
Settinas	Description			Reports     Requirements				li -
system				Settings				
🕫 Network configuration	Permissions			Svstem	Permissions			
☑ Notifications	Granted users		୍ର୍	☆ Network configuration	Constant	d		0.0
C Timestamping	Destination heat			☑ Notifications	Chanto	4 49619		° ų
& External authentication	Destination nost			C Timestamping	Connection			
III External passwords repositories	Address	Port 3389		ペ External authentication		Mode		¢ =
Resources	Server certificate		0	External passwords repositories				
Backups and retention				Resources				
å Cluster				Backups and retention			C Reset Save	
LDAP synchronization								
≡ Events log								
			SHA1					
O 2:14:27.818244å 12345678 9 2:1-23500 d. Not configured	Drews							
	Ргоху							
	Mode		¢					
		C Reset Save						

# 16.4 Data model migration from Wheel Fudo PAM version 2.2 to 3.0

This topic describes data model migration mechanisms that are applied when performing upgrade from Wheel Fudo PAM version 2.2 to 3.0.

**Note:** In case of unsuccessful upgrade to version 3.0 data model issues which caused upgrade procedure to fail can be found in the system events log.

#### 16.4.1 Server

*Servers*, which have the same IP address and port number assigned are replaced with a single object. Name of the resulting object is a concatenation of the servers' names in ascending order, separated by comma.

**Warning:** If there are two servers with the same IP address and port number assigned but with different protocol, description, external password repositorie, RDP security level, HTTP settings, TLS settings, certificates or public keys, upgrade will fail.

#### 16.4.2 Safe (previously connection)

- Anonymous connection becomes a *safe* object, which can be deleted.
- For each *bastion* object (a group of servers operating in *bastion* mode, assigned to the same *bastion*) and associated connection, there is a *safe* object created using the following naming convention: <connection name> > <bastion name>.
- For each server operating in *gateway*, *proxy* or *transparent* mode, migration procedure creates a *safe* object named <connection name> > <server name.
- Automatically created *safe* object inherits connection's access rights, granted privileges, protocols settings, notifications settings and LDAP mapping.
- OCR settings, sessions recording and session data retention parameters are moved to corresponding *account* objects.
- Time policies are replicated as user specific regulations applicable to each safe.

Note: Click selected safe on user's configuration form to display time access settings.

Preferred language	English		ŧ	*
	Click to define access time policy to the safe			
Safes	RDP SSH portal	0	Q	
Full name				
Email				

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

#### 16.4.3 Account (previously login credentials)

For each login credentials sections in every connection, migration mechanism creates a separate *account* object.

- If login credentials contain the user login string the resulting account is of the *regular* type and its name is a combination of the login and server's name <login> @ <final server name>.
- If login credentials do not contain the user login string and concern credentials forwarding connection, the resulting account object is of the *forward* type and it is named **forward** for <final server name>.
- If login credentials do not contain the user login and are used for anonymous connections, the resulting account object is of the *anonymous* type and it is named **anonymous** for <final server name>.
- Duplicated loign credentials are replaced by a single *account* object. Object's management rights, OCR settings, sessions recording settings, session data retention settings are inherited from the connection object that the *account* object derives from.

**Warning:** If login credentials contain the login string but do not contain the secret (if the login is substituted but the secret field remains empty) the data migration process will fail.

#### 16.4.4 Listener (previously *bastion* or part of a server)

- For each server operating in *proxy*, *transparent* or *gateway* mode, there is a *listener* object created with the same connection mode.
- Newly created object inherits server's access rights, TLS settings and RDP security level parameter.
- Server announcement setting is also passed on to the *listener* object.
- Listener is assigned to all safes that have been created based on connections which were associated with the server that the listener derived from.
- Bastion becomes a listener operating in the *bastion* mode. Access rights and bastion settings are transferred to the listener. The listener is assigned to all safes that have been created based on connections associated with at least one server from the bastion that the listener derived from.

#### 16.4.5 Sessions

• Each session has its safe, server and account identifiers updated accordingly. If a session concerned a server, which was not operating in *bastion* mode, it also has the listener identifier set.

## 16.5 Supported protocols

This topic describes in detail Wheel Fudo PAM protocols support.

#### 16.5.1 Citrix StoreFront (HTTP)

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Notes:

- Session player displays raw text without graphical rendering.
- Lack of bastion mode support results from protocol's limitations. Citrix StoreFront itself provides access to a bastion of hosts. When logging to Citrix StoreFront, user can select desired host to connect to over ICA protocol.

#### 16.5.2 HTTP

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Notes:

- Session player displays raw text without graphical rendering.
- Bastion mode is not supported due to limitations of the protocol.
- Access to external resources is not monitored.
- Following redirections is not supported.

#### 16.5.3 ICA

Supported connection modes:

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

Supported client applications:

• Citrix Receiver.

#### 16.5.4 Modbus

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Notes:

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

#### 16.5.5 MS SQL (TDS)

Supported connection modes:

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

Supported client applications:

- SQL Server Management Studio,
- sqsh.

#### 16.5.6 MySQL

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Supported client applications:

- Official MySQL client,
- PyMySQL libraries for Python.

#### Notes:

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

#### 16.5.7 Oracle

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

Supported connection modes:

- Gateway,
- Proxy,
- Transparent.

Supported client applications:

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

#### Notes:

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

#### 16.5.8 RDP

Supported connection modes:

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

Supported client applications:

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

Notes:

- When authenticating Fudo users against AD (or other external source) the TLS+NLA (Network Level Authentication) is not supported; TLS mode is used instead. NLA mode on server side is supported.
- RemoteApp support is in development.

#### 16.5.9 SSH

Supported connection modes:

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

Supported features:

- Connections multiplexing,
- SCP,
- Ports redirection.

#### Notes:

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

#### 16.5.10 Telnet

Supported connection modes:

- Bastion,
- Gateway,
- Proxy,

• Transparent.

Notes:

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

#### 16.5.11 Telnet 3270

Supported connection modes:

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

#### Notes:

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

Supported client applications:

- IBM Personal Communications,
- c3270.

#### 16.5.12 Telnet 5250

Supported connection modes:

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

#### Notes:

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

Supported client applications:

- IBM Personal Communications,
- tn5250.

#### 16.5.13 VNC

Supported connection modes:

- Bastion,
- Gateway,
- Proxy,

• Transparent.

Supported client applications:

- TightVNC,
- RealVNC.

#### 16.5.14 X11

X11 protocol is supported within the SSH protocol.

Supported servers:

- Xorg,
- Xming,
- XQuartz.

# 16.6 ICA configuration file

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

#### 16.6.1 Plik ICA do połączeń bez TLS

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

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

#### 16.6.2 Plik ICA do połączeń bez TLS

```
[ApplicationServers] <connection name>=
```

(continues on next page)

(continued from previous page)

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

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

#### Tematy pokrewne:

- ICA
- Model danych

# CHAPTER 17

# AAPM (Application to Application Password Manager)

## 17.1 Overview

The AAPM module enables secure passwords exchange between applications.

An essential part of the AAPM module is the fudopv script. It is installed on the application server and it communicates with the Wheel Fudo PAM Secret Manager module to retrieve passwords.

# 17.2 fudopv

#### **Execution** parameters

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

Command/option/parameter	Description
Commands	
getcert	Fetch Wheel Fudo PAM SSL certificate.
$\verb"getpass < type > < account >$	Fetch password to selected account.
	type:
	• direct - direct, unmonitored connection;
	• fudo - connection monitored by the <i>PSM</i> mod-
	ule
Options	
-c <path></path>	Use configuration file from provided path.
cfg <path></path>	
-h,help	Show options and parameters list.

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

	🏠 zmroczkowski — -bash — 148×40
Zbigniews-MacBook-Pro:~ zmroczkowski\$ chmod 700 fudopv	l

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

Note:

- Select Management > Users.
- Click +Add.
- Enter user's name.
- Define account's validity period.
- Select user from the *Role* drop-down list.
- Assign safe and click the object to open its properties.

Management <	Fudo <sup>*</sup>
Jul Dashboard	User 🖒 Copy user
E Sessions	
嶜 Users	General
🗇 Servers	ID 848388532111147042
Accounts	Synchronize with LDAP
Safes	Login fudopv2
ふ Listeners	
n- Password changers	Blocked
Policies	
🕹 Downloads	Account validity Indefinite
🔒 Reports	Role user
■ Productivity	
Settings	Preferred language English Click to access safe's properties
System	Safes portal

• Select the *Reveal password* option.

Access time policy						×
Enable time policy		I	Reveal password			
00:0 Select	to enable	passwo	ord retrieval -		23:59	
Monday						
Tuesday						
Wednesday						
Thursday						
Friday						
Saturday						
Sunday						
				C	ancel	ок

- In the *Authentication* section, select Password or One time password from the *Type* dropdown list.
- In case of static password authentication, type in the password in *Password* and *Repeat* password fields.
- In the API section, click the + icon and enter the IP address of the server, which will be requesting passwords using fudopv script.
- Click Save.

4. Run fudopv getcert command to initiate the configuration.



Note: fudopv configuration files are stored in the .fudopv folder in user's home folder.

5. Open fudopv.cfg file in a text editor of your choice.



Section	Description
[FUDO]	
address	Wheel Fudo PAM's IP address.
cert_path	Path to the Wheel Fudo PAM's SSL certificate files.
[CONN]	
bind_ip	IP address of the server, running the fudopv script. The IP address must be
	the same as the IP address defined in the $API$ section in user configuration.
[AUTH]	
username	User login as defined in step 3.
otp	Path to the otp.txt file containing the one time password.
secret	Path to the secret.txt file containing user's static password.

#### Note:

- In the [FUDO] section, in the address line, enter the Wheel Fudo PAM IP address.
- Leave the cert\_path line as is, it will be updated automatically after successfully running the fudopv getcert command.
- In the [CONN] section, uncomment the bind\_ip line and provide the IP address of the server running the fudopv script.
- In the [AUTH] section, in the username line, provide the login of the user object defined in step 3.
- Depending on the users authentication method, comment the corresponding line defining the authentication secret information.

For example:

```
[FUD0]
address=10.0.0.8.61
cert_path=<CERT_PATH>
#[CONN]
bind_ip=10.0.0.8.11
[AUTH]
username=fudopv
#otp=/Users/zmroczkowski/.fudopv/otp.txt
secret=/Users/zmroczkowski/.fudopv/secret.txt
```

6. Run fudopv getcert command to fetch Wheel Fudo PAM's SSL certificate.

	🏠 zmroczkowski — -bash — 148×40
cG9ydDEjMCEGA1UEAwwaRIVETyBUZW1wb3JhcnkgQ2VydGImaWNH hkIG9w0BCQEW0HN1cHBvcnRAd2hIZWxzeXN0ZW1zLmNvbTAeFw0x NDJaFw0yNjA1MzAw0DE4NDJaMIHoMQswCQYDVQQGEwJQTDEPMA0G NDk1MRQwEgYDVQQIDAttYXpvd2lIY2tpZTERMA8GA1UEBwWIV2Fy BgNVBAkMDXVsLk9jaG9ja2EgMUYxITAfBgNVBAoMGFdoZWVsIFNE IHogby5vLjEWMBQGA1UECwwNV2hIZWwgU3VwcG9ydDEjMCEGA1UE ZW1wb3JhcnkgQ2VydGImaWNhdGUxJzAIBgkqhkiG9w0BCQEWGHN1 ZWxzeXN0ZW1zLmNvbTCCAIIwDQYJKoZIhvcNAQEBBQADggIPADCC dSr7DqZ4kVuJoI7V/jhVIXA0CRpY5IFbcKHiNGFXn3vBueNr9ope ZfRcWJ8HbpoVWo6qFYKGmpr0esRLR71301Xs0vzNNfsmqP2vC9wk ZqpydVbAcmr0u7ZSIjsFBd2LEFyULme9cIsd3e805kLY0femZBCc WABvInzUrgbqrvaJKeIU37LtRyHZCa5/o1auxnp+EwI0ngI0Rqwc j+p010KXfYN9cJ3+950QYfupMPSN9dF/0+IbaThrRnm5NPXUMXL dX1bJ/tUyAI7VDru7Vyn09/uUNtcJm7/8nifVda4WIN0aQe43nyr +bs+0ziLarQqMH27MWK6c7XXNd+PDqVnNk0Q09f0YZYf4UP+7pD 5mv00L200CAQNKJJ7D/TtR9vpJBDv9PXV67+p2ZAty9asjAq/Iu6 3rPQH2nC6WAW9Cd14GX1mxhey0Da5f1EJ0eEwEAX0XzDeGzq/ZR7 0jbYn2N19ICfFCo71bGDAKAIDIZZ1100uaGSX9tBkTgLGdr1IFKr yN/snn45UdwWzyk9BM84z/0w4Rr7cPjLtYDSzdHAgMBAAGjeDB2 MAAwKQYJYIZIAYb4QgENBBwGkzVRE8gVGVtcG9YXJ5IENIcnRp A1UdDgQWBBSXBvJ7BT1XBe8BxZHvQK9ILSnTbTAfBgNHSMBAGjeDB2 MAAwKQYJVIZIAYb4QgENBBwGkzVRE8gVGVtcG9YXJ5IENIcnRp A1UdDgQWBBXBvJ7BT1XBe8BxZHvQK9ILSnTbTAfBgNHSMBAGjeDB2 MAAwKQYJVIZIAYb4QgNBAdphkiG9w0BAQ0FAA0CAgEAqPzZVty1 N5I3mrd2J0nxGBNMaohdTqfZLLXRRe5szrZXyhK1VxItIJa1and Ur2s9hwABwSKEujrIpnT+rukqB6E50VCjucr3GVub/xe+ssCHJA AMj10Yi2PTjyo15v9WixQA74IIJPAhV4ed4N9gSM0cLCceQmEDjo IfXDqFuRs6Xj2zaczYQWNK6RgBL600yngSt5Ey1vScHyTKXSRLw rLAxcjdGK+Aq7PFJJIMwz1vxtnrysvrDwjpq80KhNdUS9xFgnxG6 aB5BFJNW/Hhm7GghTMc+vBFTIkt5fXd2+TGdtinZaX7rdkH7JRKS Li4To10STL/3VtbrzVdXqT8QpiLF23IAKMWhDkeqZPwqGmhw0xcr cwdrsUShy01D20A1bHUyzc0G/s9MasNctqkc2918ypnPuhQAZLf ZWKX80TftGZAx3Y80LH0kbQwCzEzwFXdpGBEzwiYE9JFmNGVIn21 kqdng0QQNKiuojE9KKZT242T+32UWUpfJjfkhNazHQq4AeQ1FzQ8 yf0IGHrrafLJ39Qg2dtNhJoe END CERTIFICATE	dGUxJzA1Bgkq NjA2MDEw0DE4 ALUEEQw6MD1t c3phd2ExFjAU c3R1bXMgU3Au AwwQR1VETy8U cHEvcnRAd2h1 AgoCggIBALc4 dj/bwFiqb4p+ Hq1LKDwdBMKE Syv2FoR0w5Rj S5oBdxmcdbJL MuaAVb3fxJLC FBFFXY0N0qS1 UXmmg8Tb/BMY 562Cbwe6he8c Jo7zjWc0400Y MAKGA1UdEw0C Zn1jYXR1MB86 gBSX8vJ7B11X N6UsD5oKUQj7 ttGBCTq17eVp XHqXxevX7Txn Nxv1UW1zZYhs adAtav5LJmi g3EAE9V8802gA p9G2j8Zrc5HT TgSEu3yA1T2e CDxPg1WV/LFX L2H23rdXLkwX H5HFzz?uhx7N
SHA1 Fingerprint: 2cba43a291fdcf71849ae1dfa9e19bcfc2 Do you want to accept this certificate (yes/no)?: ye Certificate has been succesfully dowloaded. Configuration file has been updated. Zbigniews-MacBook-Pro:~ zmroczkowski\$	795df8 s

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

	📄 .fudopv —	- vi fudopv.cfg — 1	148×40
<pre>[FUD0] address=10.0.45.47 cert_path=/Users/zmroczkowski/.fudopv/gui.cert.pem</pre>			
#[CONN] bind_ip=10.0.1.35			
[AUTH] username=fudopv2 #otp=/Users/zmroczkowski/.fudopv/otp.txt secret=/Users/zmroczkowski/.fudopv/secret.txt ~			
~			
~			
~			
~			
~			
~			
2010 2010			
~			
~			
~			
~			
~			
~			
~			
~			
~			
~			
~			
~			
~			
"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	
Туре	Copy the string and save it in the otp.txt file
One time password	6c48b1e5d90746421e1791f41ae44f6724aa702d70c5ecc541af14bfd60db3c0
Delete	0

- The otp.txt file will be automatically updated each time the fudopv getpass command is run.
- 8. Run command:

• fudopv getpass direct <account\_name>, to fetch password to connect directly to the server.



• fudopv getpass fudo <account\_name>, to fetch password to establish monitored connection with the target host.

	🏠 zmroczkowski — -bash — 148×40
[Zbigniews-MacBook-Pro:~ zmroczkowski\$ ./fudopv getpass 499551c7-0c14-f8b4-5056-84e7d801b220Zbigniews-MacBook-	: fudo gc-konto-ssh Pro:~ zmroczkowski\$

**Warning:** Correct operation of the fudopv script requires disabling the login reason prompt option in the safe's properties.
ID	848388532111147017		
Name	gc-sejf		
Blocked			
Blocked Login reason	Make sure that the I	login reason option is disabled	
Blocked Login reason Notifications □	Make sure that the I	login reason option is disabled	
Blocked Login reason Notifications	Make sure that the I     Session start     Session join	login reason option is disabled Session finish Session leave	
Blocked Login reason Notifications 🗆	Make sure that the I     Session start     Session join     Session policy match	login reason option is disabled Session finish Session leave	

# 17.3 API interface

AAPM's API interface is described in detail in the Wheel Fudo PAM 3.1 - API documentation manual.

#### **Related topics:**

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

# CHAPTER 18

# Troubleshooting

# 18.1 Booting up

Problem	Symptoms and solution
wheel Fudo PAM does not	• Males gues that both newer supplies are connected to
boot up	• Make sure that both power supplies are connected to
boot up	power outlets. Not connecting both power supplies will
	negult in gound alarma
	result in sound alarm.
	• Make sure that encryption key is properly connected.
	• In case the problem is a result of unsuccessful system up-
	date, wait a few minutes. During that time, Wheel Fudo
	PAM will detect the problem and will restore previous
	TAM will detect the problem and will restore previous
	system revision.
	-

# 18.2 Connecting to servers

Problem	Symptoms and solution
Cannot connect to server	Symptoms:
	• User cannot log in.
	Podłączanie pulpitu zdalnego
	Sesja usług pulpitu zdalnego została zakończona. Połączenie z komputerem zdalnym zostało utracone, prawdopodobnie z powodu problemów z łącznością sieciową. Spróbuj ponownie połączyć się z komputerem zdalnym. Jeśli ten problem będzie nadal występował, skontaktuj się z administratorem sieci lub pomocą techniczną.
	OK Pomo <u>c</u>
	• Events log entry: Authentication failed: Invalid username kowalski or password.
	<ul> <li>Solution:</li> <li>Verify that user definition exists in Wheel Fudo PAM database.</li> <li>Make the login credentials are correct.</li> <li>Make sure that the client software does not have outdated credentials stored.</li> </ul>
	Symptoms: events log entry: Unable to establish connection to server zbigniew (10.0.35.53:3399).
	Cause: incorrect server configuration.
	<ul> <li>Solution:</li> <li>Verify that the server in question is properly configured (IP address, port number).</li> <li>Check if the server is reachable from Wheel Fudo PAM:</li> </ul>
	<ol> <li>Log in to Wheel Fudo PAM administration panel.</li> <li>Select Settings &gt; System, Diagnostics tab.</li> <li>Enter server address in the Ping section and execute command and test host's availability.</li> </ol>

Problem	Symptoms and solution
When logging in not all of the users see the Wheel Fudo PAM logon screen.	<ul> <li>Cause:</li> <li>Credentials stored in RDP client result in users being automatically logged in to remote host.</li> <li>Credentials stored in RDP client, user is successfully automatically automatically here.</li> </ul>
	PAM logon screen is not displayed. Next, Wheel Fudo PAM forwards user credentials to target server but they are no longer valid which results in Windows gina being displayed.
	Symptoms:
	$\bullet\ {\rm Client\ software\ message:\ Connection\ closed\ by\ remote}$
	host.
	• Events log entry: Failed to authenticate against the server as user root using password.
	Course, incompact large and anticla
	Cause: incorrect login credentials.
	<b>Solution:</b> provide correct login credentials in server configura- tion.
	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 Wheel Fudo PAM administration panel and
	unblock the server.

Problem	Symptoms and solution	n
Connection is terminated	<ul> <li>Symptoms:</li> <li>User tries to log in to server monitored by Wheel Fudo PAM, after entering username and password session is immediately terminated.</li> <li>Events log entry: TLS certificate verification failed.</li> </ul>	
	Solution:	
	Download new target	both the host section.
	Destination host	
	Address Server public key	10.0.35.1     Port     22       Click to download server certificate       ssh-rsa       AAAAB3NzaC1yc2EAAAADAQABAAABAQDTy6vf0NsMYuiOCRfcz/3bEFcroo
		WKf+bB6wW1XKRu8UqR0xZnMEpNpy6cRtZDbpmWEBNN4iM7yosy3gAgD S16TErm6ukVK0JYKIHF4Qqp+8d2OhgKBHtwmXZff4QFyQmMUbA4MhL/cC LTn0Jc2du1512cX5xFdh05LUaBB6xbV0hbXLSQLQUP+JA53Qo5M9m1Wk bJkofQ5AQV7pdsKTU93O6GB00IDoz3JpPbTKnn/dhNBilfpmHSbIPTrgPasO9 C/lhL2PVFiBeqvvwK67CKgW6UrjhHPPLquHayA0YuIVTJveBumg/CpQ0Zqt7U OUsZ2M22ezQwJxPdvbf6V
		09:de:23:81:72:c1:f7:c7:12:9a:df:6c:cb:cd:ad:d6:f4:50:ac:c0 SHA1
	<ul><li>Symptoms:</li><li>After entering terminated.</li><li>Events log entresidente</li></ul>	username and password the connection is y: RDP connection error.
	<b>Solution:</b> check if in the <i>Encryption level</i>	the <i>General</i> tab in TCP-Rdp properties, option is not set to FIPS Compliant.
Cannot connect to server	Symptoms: • Cannot log in not allowed t • Events log e user0 not all	to server with error message User user0 to connect to server. ntry: Authentication failed: User lowed to connect to server.
	Cause: user is not a	ssigned 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 wheel Fudo PAM administration panel and
	unblock the user in question.
User has to provide login	Symptoms: user connecting over BDP protocol enters login
credentials twice	credentials and immediately afterwards is asked again for the
	same login information.
	Cause: server is a part of an infrastructure managed by con-
	nections broker which has detected an active user's session on
	another server.
	Symptoms: user connecting over SSH protocol enters login
	credentials and immediately afterwards is asked again for login
	information.
	Cause: in <i>connection</i> object options for login and password
	substitution are enabled but the input fields are left blank which
	results in two fold authentication - first time against wheel
	Fudo FAM and second time against the target nost.
Cannot connect to server	Symptoms:
Cannot connect to server over RDP protocol	<ul><li>Symptoms:</li><li>User connecting over RDP is disconnected a moment after</li></ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms:</li> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms:</li> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms:</li> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms:</li> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms:</li> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms:</li> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms:</li> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms:</li> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 2280</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms:</li> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> <li>Symptoms: <ul> <li>Events log entry: User user0 has no access to host.</li> </ul> </li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> <li>Symptoms: <ul> <li>Events log entry: User user0 has no access to host 192.168.0.1:3389</li> </ul> </li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> <li>Symptoms: <ul> <li>Events log entry: User user0 has no access to host 192.168.0.1:3389</li> </ul> </li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> <li>Symptoms: <ul> <li>Events log entry: User user0 has no access to host 192.168.0.1:3389</li> </ul> </li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> <li>Symptoms: <ul> <li>Events log entry: User user0 has no access to host 192.168.0.1:3389</li> </ul> </li> <li>Cause: connections broker determines an existing user session on another server and redirects user to that host but it is not</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> <li>Symptoms: <ul> <li>Events log entry: User user0 has no access to host 192.168.0.1:3389</li> </ul> </li> <li>Cause: connections broker determines an existing user session on another server and redirects user to that host but it is not configured on Wheel Fudo PAM or the user does not have suf-</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> <li>Symptoms: <ul> <li>Events log entry: User user0 has no access to host 192.168.0.1:3389</li> </ul> </li> <li>Cause: connections broker determines an existing user session on another server and redirects user to that host but it is not configured on Wheel Fudo PAM or the user does not have sufficient access rights to connect to given server.</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> <li>Symptoms: <ul> <li>Events log entry: User user0 has no access to host 192.168.0.1:3389</li> </ul> </li> <li>Cause: connections broker determines an existing user session on another server and redirects user to that host but it is not configured on Wheel Fudo PAM or the user does not have sufficient access rights to connect to given server.</li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> <li>Symptoms: <ul> <li>Events log entry: User user0 has no access to host 192.168.0.1:3389</li> </ul> </li> <li>Cause: connections broker determines an existing user session on another server and redirects user to that host but it is not configured on Wheel Fudo PAM or the user does not have sufficient access rights to connect to given server.</li> <li>Solution: <ul> <li>Make sure that the server object exists.</li> </ul> </li> </ul>
Cannot connect to server over RDP protocol	<ul> <li>Symptoms: <ul> <li>User connecting over RDP is disconnected a moment after establishing connection.</li> <li>Events log entry: RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</li> </ul> </li> <li>Cause: connection is redirected to a host which does not listen on port number 3389.</li> <li>Solution: configure server in question so it accepts user connections on port number 3389.</li> <li>Symptoms: <ul> <li>Events log entry: User user0 has no access to host 192.168.0.1:3389</li> </ul> </li> <li>Cause: connections broker determines an existing user session on another server and redirects user to that host but it is not configured on Wheel Fudo PAM or the user does not have sufficient access rights to connect to given server.</li> <li>Solution: <ul> <li>Make sure that the server object exists.</li> <li>Add user to proper connection object.</li> </ul> </li> </ul>

# 18.3 Logging to administration panel

Problem	Symptoms and solution
Cannot log in to adminis- tration panel	<ul> <li>Make sure that Wheel Fudo PAM IP address is correct.</li> <li>Set Wheel Fudo PAM IP address from the console as described in the Wheel Fudo PAM System documentation in the Network interfaces configuration topic.</li> <li>Make sure that the IP address in question has the management access option enabled.</li> </ul>

Management	< Fudo <sup>®</sup>	💄 admin 🗸 💡
Jashboard	Interfaces Name & DNS Bouting	
E Sessions		
嶜 Users	<b>∞ net0</b> 08:00:27:4D:38:58	
🕀 Servers 🛛 FUDO administra	ation panel accessible through selected IP address	
• Bastions	10.0.40.80 / 16	
+ Connections	10.0.40.81 / 16	
Policies	10.0.40.82 / 16	

# 18.4 Session playback

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

# 18.5 Cluster configuration

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

# CHAPTER 19

# Frequently asked questions

- 1. How many user sessions can be stored on Wheel Fudo PAM at once?
- 2. How Wheel Fudo PAM supports sessions archiving?
- 3. How to calculate storage space required for archiving sessions?
- 4. How users can hide their activities on servers which they access through Wheel Fudo PAM?
- 5. How to determine unauthorized access attempts to supervised servers?

6. Is it possible to hide the Wheel Fudo PAM login screen when connecting over the RDP protocol?

- 7. Why the users list in the connection's properties is incomplete?
- 8. Why is a user removed from the LDAP/AD server still present on Wheel Fudo PAM?
- 9. How frequently are users' definitions synchronized with an LDAP/AD server?

10. I see \* instead of the keystrokes in the session player. Is it possible to see the actual keyboard input?

11. Can I deactivate a session URL?

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

Wheel Fudo PAM is delivered with 20TB of hard drive space dedicated to storing users sessions.

Size of the stored session is determined by user's activity. A minute of recorded connection takes on average:

RDP	1 MB active user session (no activity generates almost no data).
	Definite session size depends on the screen resolution, color
	depth and actual user activity.
SSH	50 kB active session.

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

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

**Note:** Wheel Fudo PAM allows specifying how long sessions data should be stored, and will automatically delete session data after a certain time, determined by *retention* parameter, elapses.

#### 2. How Wheel Fudo PAM supports sessions archiving?

All sessions are stored on Wheel Fudo PAM internal storage space. In addition to that, Wheel Fudo PAM allows exporting sessions in native format or a video record.

#### 3. How to calculate storage space required for archiving sessions?

File size of sessions in native format are the same as in question 1. In case of video record, file size depends on the codec and resolution settings.

# 4. How users can hide their activities on servers which they access through Wheel Fudo PAM?

In case of the SSH protocol, Wheel Fudo PAM supports SCP channel and monitors all transferred files, including scripts. This allows auditing given session searching for malicious code embedded in software sent to the server.

Protection of other communication channels (e.g. web browser or other applications) are task for different kind of solutions. There is no solution similar to Wheel Fudo PAM which are able to monitor such channels, thus it is important to create proper server configuration by the system administrator.

#### 5. How to determine unauthorized access attempts to supervised servers?

Unauthorized access and DoS attacks attempts, can be determined by analyzing event log entries. Each ERROR or WARNING severity entries should be closely examined. Cases of login timeout errors can be potential DoS attack attempts.

# 6. Is it possible to hide the Wheel Fudo PAM login screen when connecting over the RDP protocol?

Hiding the Wheel Fudo PAM login screen requires using the Enhanced RDP Security (TLS) + NLA security mode.

#### 7. Why the users list in the connection's properties is incomplete?

The users list in the connection's properties does not contain users synchronized with the LDAP service. To assign a connection to an LDAP synchronized user, define a group mapping in the *LDAP synchronization properties* or disable the synchronization option for the given user.

# 8. Why is a user removed from the LDAP/AD server still present on Wheel Fudo PAM?

Deleting a user object from an AD or an LDAP server requires performing the full synchronization to reflect those changes on Wheel Fudo PAM. The full synchronization process is triggered automatically once a day at 00:00, or can be triggered manually in the LDAP synchronization settings view.

#### 9. How frequently are users' definitions synchronized with an LDAP/AD server?

New users definitions and changes in existing objects are imported from the directory service periodically every 5 minutes. The full synchronization process is triggered automatically once a day at 00:00.

# 10. I see \* instead of the keystrokes in the session player. Is it possible to see the actual keyboard input?

Presenting keyboard input qualifies as a sensitive feature and it is disabled by default. Enabling displaying keystorkes in the session player requires a consent from two **superadmin** users. Refer to the *Sensitive features* topic for the details on enabling this functionality.

#### 11. Can I deactivate a session URL?

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

# CHAPTER 20

Glossary

- **DNS** Domain Name Server name server service which maps IP addresses to hosts names which are easier to remember.
- SSH Secure Shell networking protocol for secure communication with remote systems.
- **Syslog** Events logging standard in computer systems. Syslog server collects and stores log data from networked devices, which can be later used for analysis and reporting.
- **Fingerprint** Characters string being a result of a hash function on input data, allowing to determine if the input data has been altered.
- **RDP** Remote Desktop Protocol remote access protocol to computer systems running Microsoft operating system.
- **VNC** Remote access protocol to graphical user interfaces.
- **RADIUS** Remote Authentication Dial In User Service networking protocol used to control access to different services within IT infrastructure.
- **Static password** Basic user authorization method which uses login and password combination to determine users's identity.
- **Public key** Authentication method which uses a pair of keys private (held only by the user) and public (publicly available) to determine user's identity.
- **CERB** Complete user authentication and authorization solution, supporting different authentication methods i.e., mobile token (mobile phone application), static password, SMS onetime passwords, etc.
- **LDAP** Lightweight Directory Access Protocol distributed catalog services management and access protocol in IP networks.

Active Directory Users authorization and authentication in Windows domain.

**AD** Active Directory - users authorization and authentication in Windows domain.

- **CIDR** Short notation of network addressing, in which the IP address is written according to the IPv4 standard, and the subnet mask is provided as a number of 1 in the subnet mask in binary system (192.168.1.1 255.255.255.0; 192.168.1.1/24).
- **heartbeat** Network packet used for informing other cluster nodes about machine's current state. If a cluster node does not receive a heartbeat packet in a given timeframe, it will take over the master node role and will start processing users' requests.
- anonymous safe An anonymous safe has at least one anonymous account assigned to it and it can only have that type of accounts assigned. You cannot assign users to anonymous safes.
- **AAPM** AAPM (Application to Application Password Manager) module enables secure password exchange between applications.
- Efficiency Analyzer Efficiency Analyzer module delivers statistical information on users' activity.
- **PSM (Privileged Session Management)** PSM module is used for recording remote access sessions.

server

- **servers** Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.
- **listener** Listener determines server connection mode (proxy, gateway, transparent, bastion) as well as its specifics.
- **user** User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.
- **account** Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); password changing policy as well as the password changer itself.
- safe Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.
- **hot-swap** Hot-swap mechanism enables replacing hardware components without the necessity to turn the system off.
- time policy Time policy mechanism enables defining time periods during which users are allowed to connect ot monitored hosts.
- password changer Tool which enables facilitating automated password changing on a server.
- **policy** Mechanism which enables defining patterns which in case of being detected will trigger defined actions.
- shared session User session which was joined by another user.
- **fudopv** AAPM module script, installed on the server, which enables secure password exchange between applications.
- SSH access Service access to Wheel Fudo PAM over SSH protocol.

VLAN Virtual networks mechanism, enabling separation of broadcast domains.

- **DHCP** Mechanism for dynamic IP addressing management i LAN networks.
- **timestamp** Session data hash value, which enables verifying that the data has not been modified.
- **external authentication server** Server storing user data used for verification of user login credentials when connecting to Wheel Fudo PAM or the monitored server.
- **passwords repository** Passwords repository manages password to privileged accounts on monitored hosts.
- **data retention** Data retention mechanism automatically deletes session data after define time period transpires.
- **redundancy group** Defined group of IP addresses, which in case of a system failure, will be seamlessly carried over to another cluster node to maintain the availability of the services.
- **RDP connections broker** Remote sessions management mechanism for server farms.
- **PSM** PSM (Privileged Session Monitoring) module enables monitoring and recording remote access sessions.
- WWN World Wide Name unique object identifier in external storage solutions.

### Index

## A

AAPM, **332** account, **332** Active Directory, **331** AD, **331** administration configuration export/import, 263 anonymous safe, **332** API users, 92

# С

CERB, **331** CIDR, **332** Citrix servers, 108 configuration Network configuration, 233, 241 notifications, 245 users synchronization, 102 connection mode bastion, 14 gateway, 13 proxy, 13 transparent, 13 creating servers, 108

## D

data retention, 333
deleting
 servers, 135
deployment scenario
 bridge, 12
 forced routing, 12
DHCP, 333
DNS, 331

# Е

editing servers, 132 Efficiency Analyzer, **332** external authentication server, **333** 

### F

 $\begin{array}{l} \texttt{Fingerprint}, \ \textbf{331} \\ \texttt{fudopv}, \ \textbf{332} \end{array}$ 

### Н

heartbeat, **332** hot-swap, **332** HTTP servers, 109

### I

ICA servers, 111

### L

LDAP, **331** listener, **332** 

## Μ

Modbus servers, 114 MS SQL servers, 115 MySQL servers, 117

# Ν

Network configuration network bypass configuration, 241 network interface configuration, 233 network configuration routing, 242

### 0

Oracle servers, 119

### Ρ

password changer, passwords repository, policy, **332** PSM, **333** PSM (*Privileged Session Management*), Public key,

# R

RADIUS, **331** RDP, **331** RDP servers, 121 RDP connections broker, **333** RDP connections broker, 293 redundancy group, **333** 

## S

safe, **332** server, 332 servers, 332 servers Citrix, 108 creating, 108 deleting, 135  $\tt editing,\, 132$ HTTP, 109 ICA, 111 Modbus, 114 MS SQL, 115 MySQL, 117 Oracle, 119RDP, 121 ssh, 123 Telnet, 125 Telnet 3270, 127 Telnet 5250, 129 VNC, 131 sessions commenting, 205 filtering, 192 play and preview, 196 shared session, 332SSH, 331 sshservers, 123 SSH access, 332

Syslog, 331 T Telnet servers, 125 Telnet 3270 servers, 127 Telnet 5250 servers, 129 time policy, 332 timestamp, 333 U user, 332 users access rights, 92 ADL 00

Static password, 331

API, 92 roles, 92 users synchronization, 102 configuration, 102

## V

```
VLAN, 332
VNC, 331
VNC
servers, 131
```

# W

WWN, **333**