



FUDO
S E C U R I T Y

Fudo PAM 3.10 - User Portal
Manual

Release is not supported

Wheel Systems

07.12.2023

1	About documentation	1
2	System overview	2
3	Logging into the User Portal	4
4	Displaying passwords	6
5	Displaying passwords history	8
6	Establishing connections	10
6.1	Connecting over RDP on Microsoft Windows 7 and 10	10
6.2	Connecting over RDP on Mac OS X	13
6.3	Connecting over RDP on Ubuntu Linux	16
6.4	Connecting over SSH on Microsoft Windows 7 and 10	18
6.5	Connecting over SSH on Mac OS	21
7	Requesting access to safe	24
8	Authentication	26
9	Troubleshooting	27

About documentation

Conventions and symbols

This section covers conventions used throughout this documentation.

italic

Uster interface elements.

example

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

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

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

System overview

User portal enables initiating connections with monitored servers available to the logged in user.

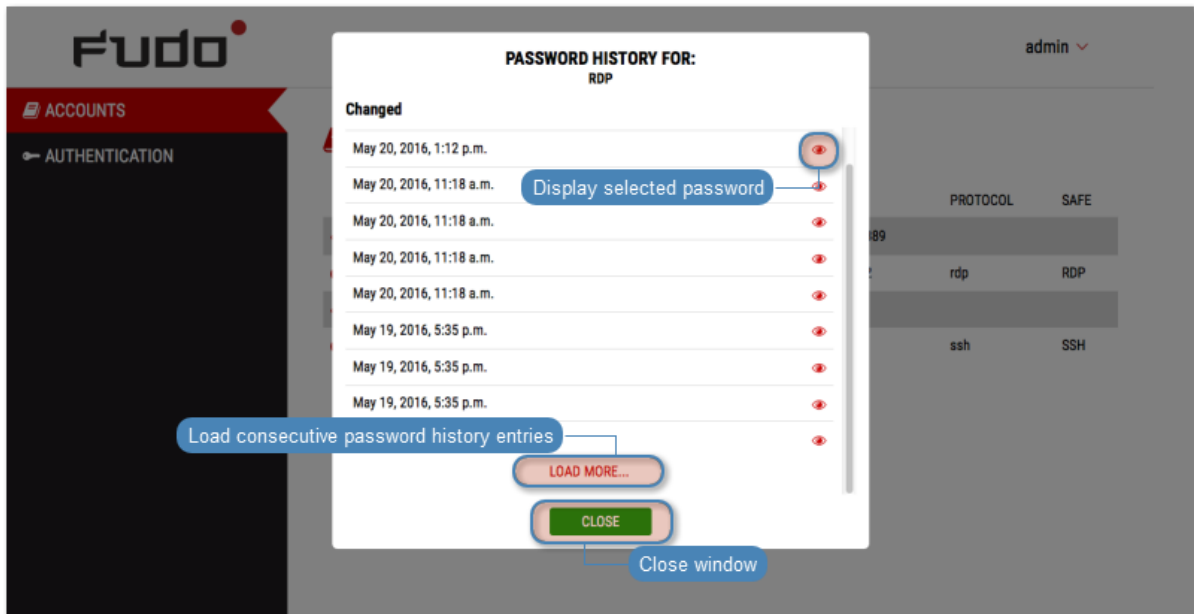
The screenshot shows the FUDO user portal interface. The top left features the FUDO logo and a navigation menu with 'ACCOUNTS' and 'AUTHENTICATION'. The top right shows a user menu for 'admin'. The main content area is titled 'LIST OF ACCOUNTS' and contains a table with the following data:

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

Callouts from the interface indicate the following actions:

- 'Show account password' points to the RDP row.
- 'Show passwords history' points to the SSH row.
- 'Connect to server using selected listener' points to the listener column.

The system also enables viewing the password to selected accounts and browsing passwords history to accounts managed by FUDO's password vault module.



Logging into the User Portal

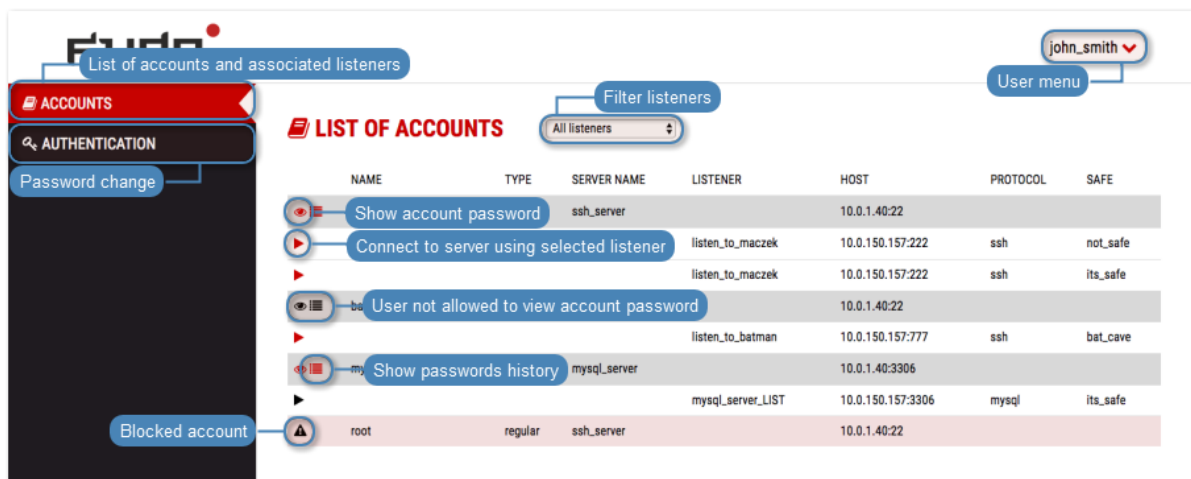
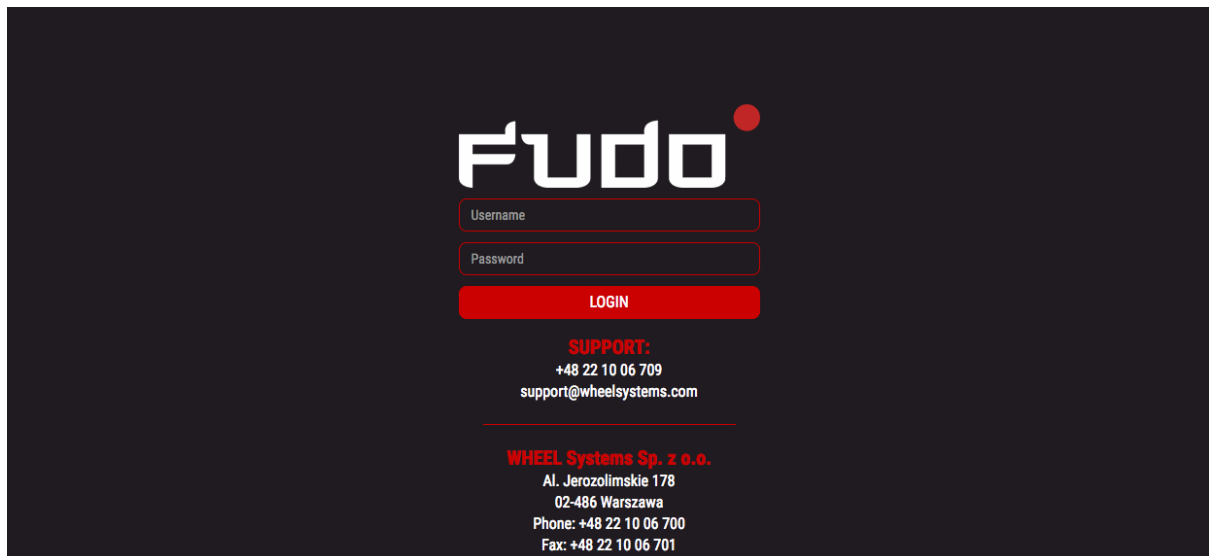
Note:

- User Portal is compatible with the following web browsers:
 - Google Chrome, Mozilla Firefox, Internet Explorer for Microsoft Windows.
 - Google Chrome, Mozilla Firefox for Ubuntu.
 - Google Chrome, Mozilla Firefox, Safari dla systemu operacyjnego Mac OS X.
- *User Portal* supports Single Sign On for Active Directory accounts. Refer to system documentation for information on how to enable the SSO in User Portal.

-
1. Open web browser and direct it to the IP address of the User Portal.

Note: You can obtain the IP address from your system administrator.


2. Accept the security alert exception to display the login page.
3. Enter the username, password and click *LOGIN*.

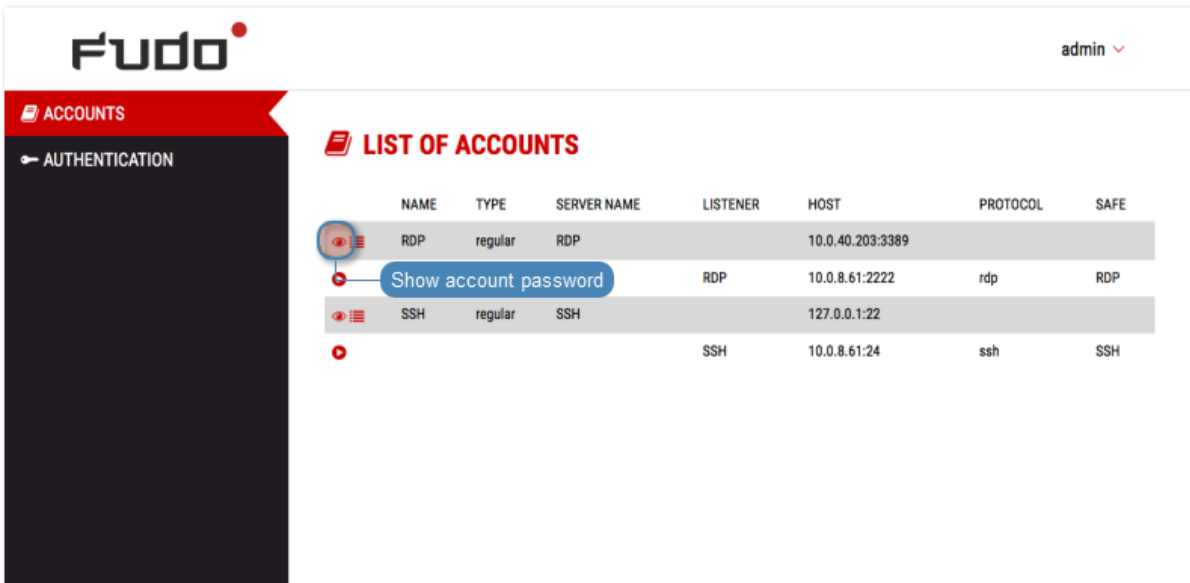


Related topics:

- *Connecting over RDP on Mac OS X*
- *Connecting over RDP on Ubuntu Linux*

Displaying passwords

1. Select *ACCOUNTS*.
2. Find account to which password you want to view.
3. Click  icon.



The screenshot shows the Fudo web interface. The top left has the Fudo logo and a navigation menu with 'ACCOUNTS' selected. The top right shows the user 'admin'. The main content area is titled 'LIST OF ACCOUNTS' and contains a table with the following data:


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

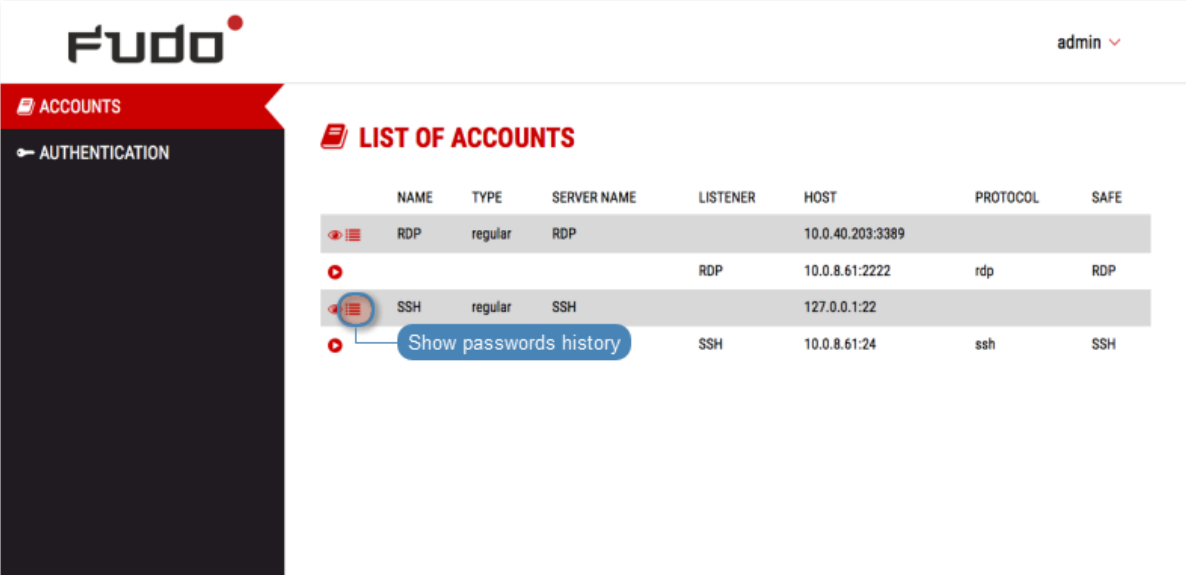
4. Confirm password display request.

The screenshot shows the Fudo user portal interface. At the top left is the 'Fudo' logo. In the top right corner, the user is logged in as 'admin'. A central dialog box asks 'Are you sure you would like to display password?' with 'CLOSE' and 'SHOW' buttons. Below the dialog is a table titled 'LIST OF ACCOUNTS' with columns for NAME, TYPE, SERVER NAME, LISTENER, HOST, PROTOCOL, and SAFE. The table contains four rows of account information.





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

Displaying passwords history

1. Select *ACCOUNTS*.
2. Find account which passwords history you want to view.
3. Click  icon.

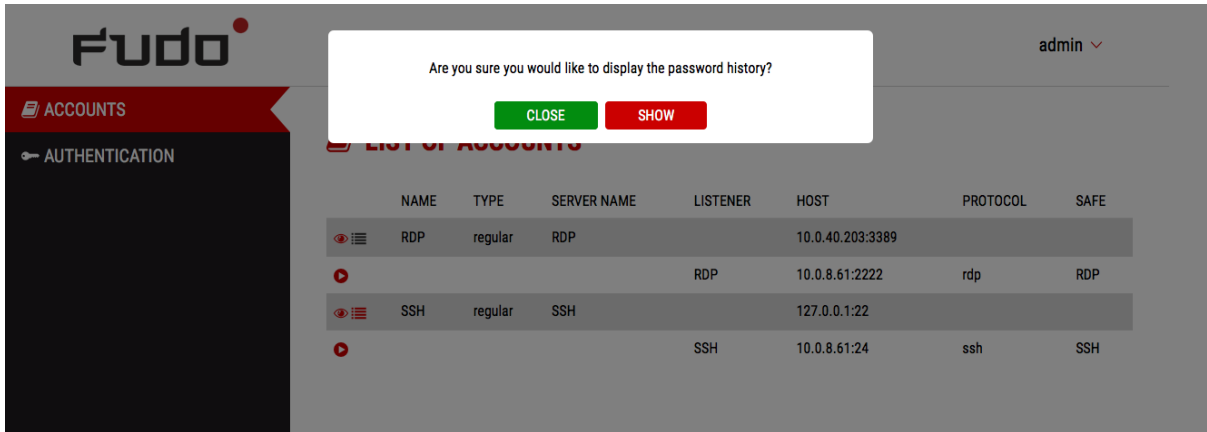


The screenshot shows the Fudo web interface. The top left has the 'Fudo' logo and a user dropdown menu showing 'admin'. A red navigation bar contains 'ACCOUNTS' and 'AUTHENTICATION'. The main content area is titled 'LIST OF ACCOUNTS' and contains a table with the following data:

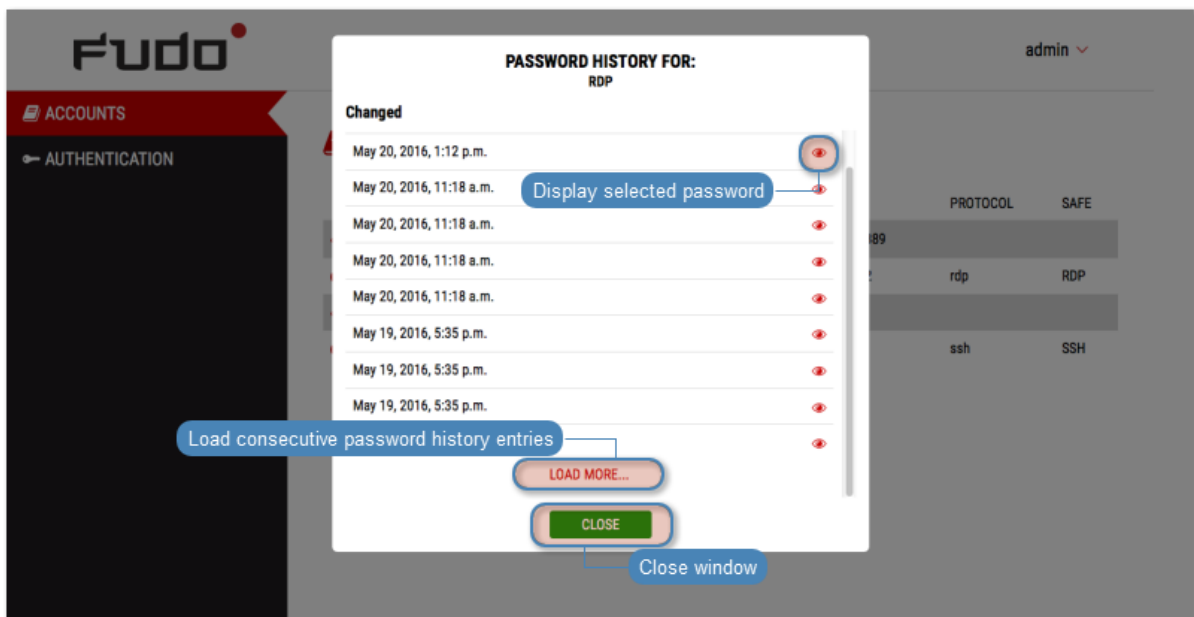
	NAME	TYPE	SERVER NAME	LISTENER	HOST	PROTOCOL	SAFE
	RDP	regular	RDP		10.0.40.203:3389		
				RDP	10.0.8.61:2222	rdp	RDP
	SSH	regular	SSH		127.0.0.1:22		
				SSH	10.0.8.61:24	ssh	SSH

A blue callout box with the text 'Show passwords history' points to the list icon in the third row of the table.

4. Confirm passwords history display request.

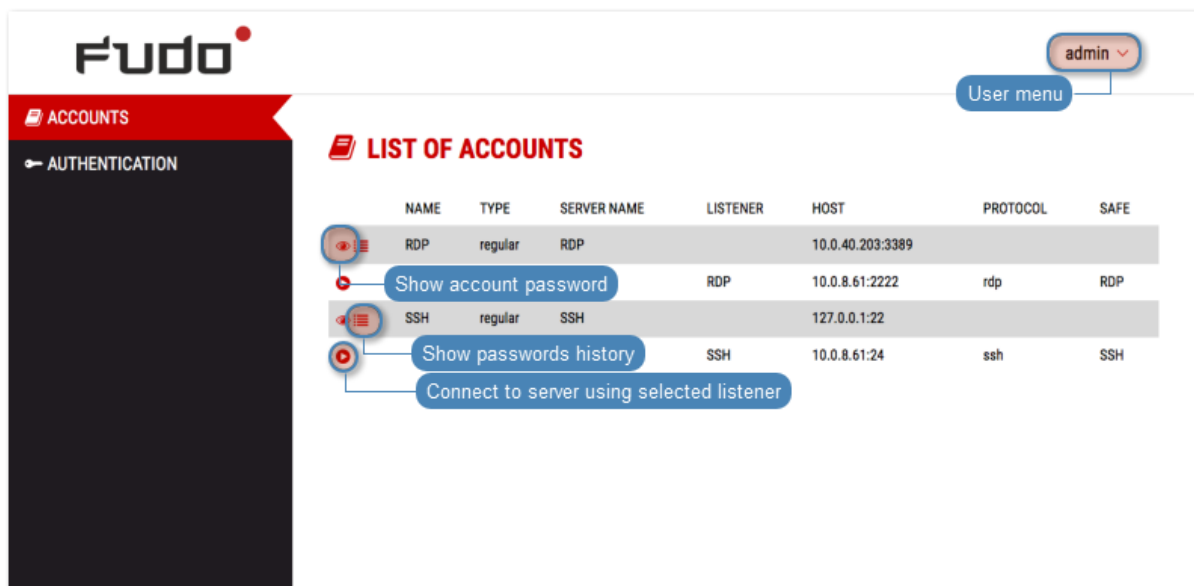


5. Click  to view selected password.





6.1 Connecting over RDP on Microsoft Windows 7 and 10

1. Log in to the User Portal and select *ACCOUNTS*.
2. Find desired account and server.

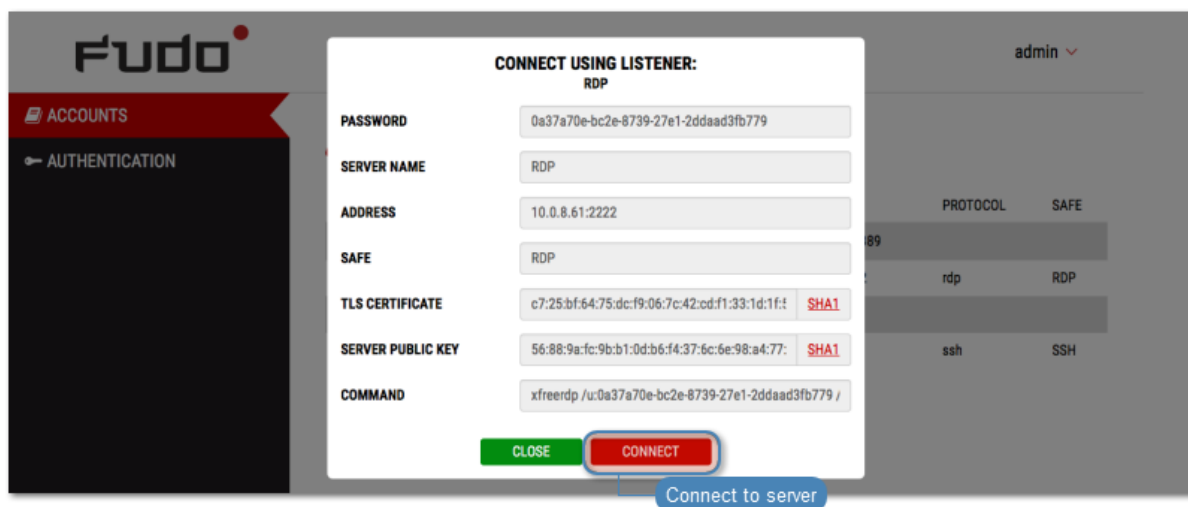


3. Select desired listener and click  icon.

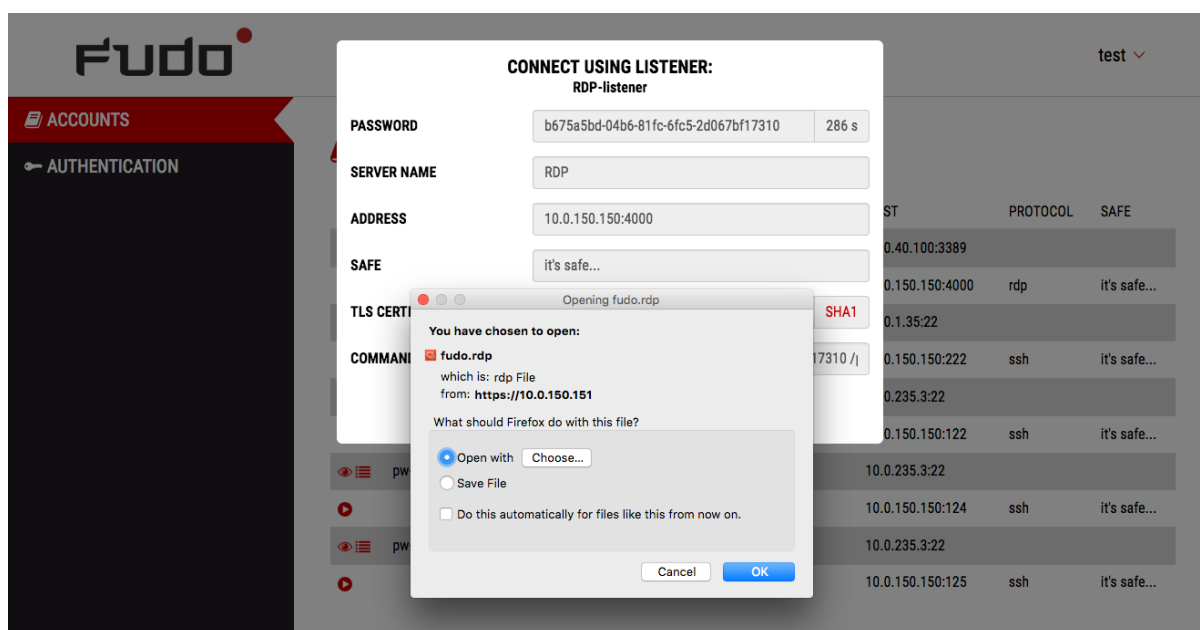
Note:

- The list contains both internal and external listening addresses.
- In case there is the  icon displayed next to the safe instead of the  icon, you must *fill in access request form*.

- Click *CONNECT* to launch client application appropriate for selected listener with connection parameters forwarded.

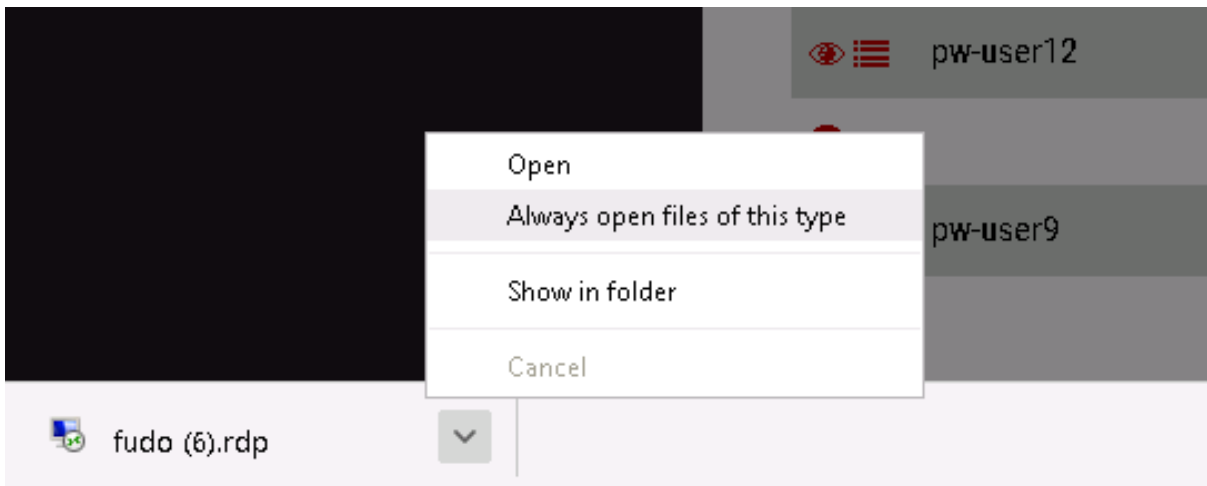


- Save the connection definition file or launch a dedicated RDP protocol client.

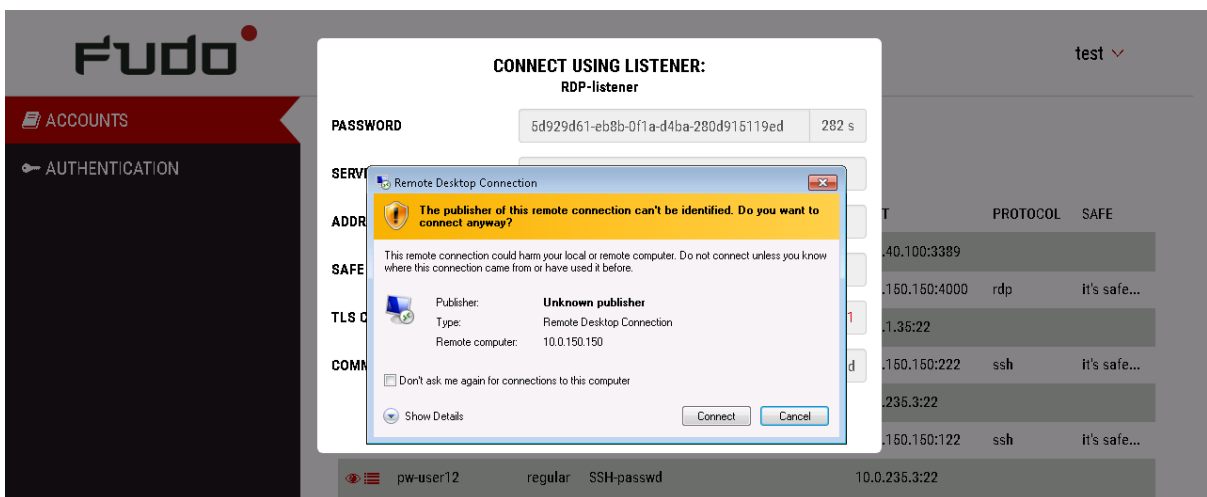


Note:

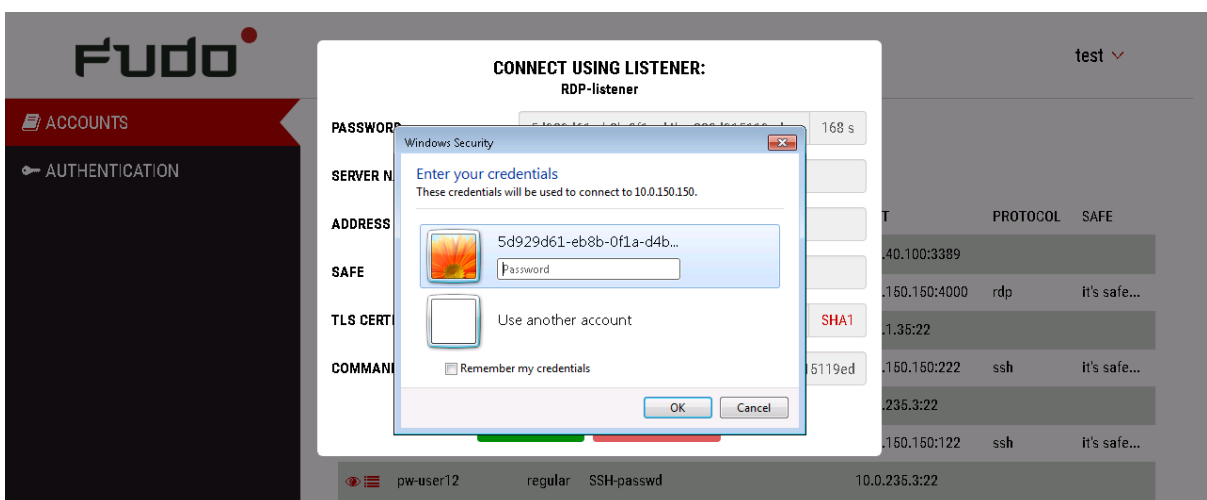
- *Google Chrome* will automatically save the file.
- Select the *Always open this file type* option to automatically start the client app.



6. Click *Connect* in the RDP client app window.

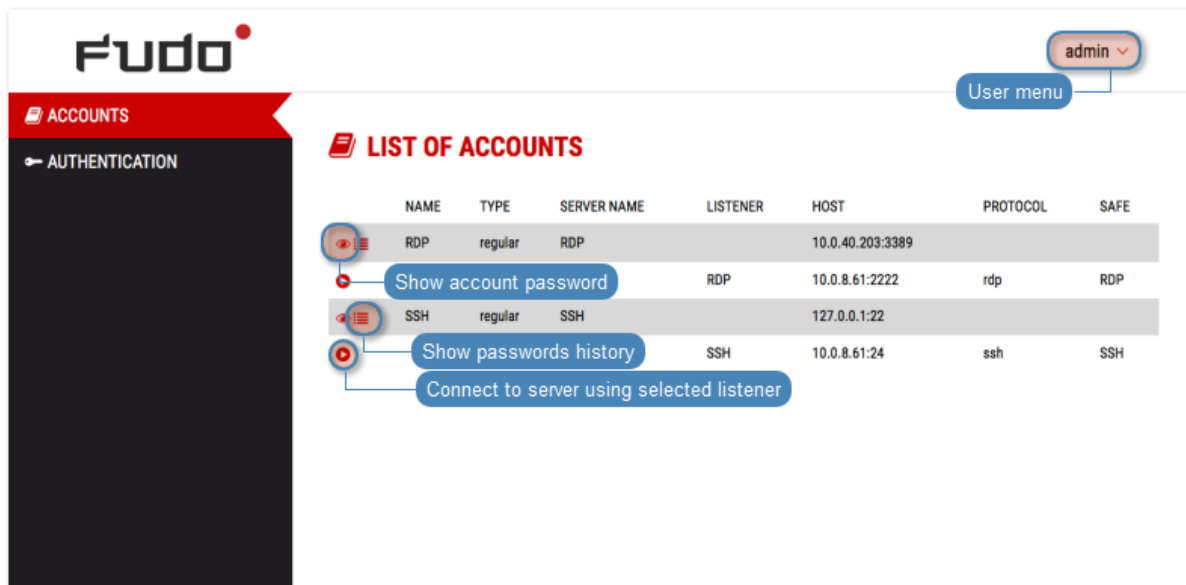


7. Click *OK* in the credentials prompt window without providing the password.





8. Click *Yes* to connect to the server despite the certificate alert.

1. Log in to the User Portal and select *ACCOUNTS*.
2. Find desired account and server.

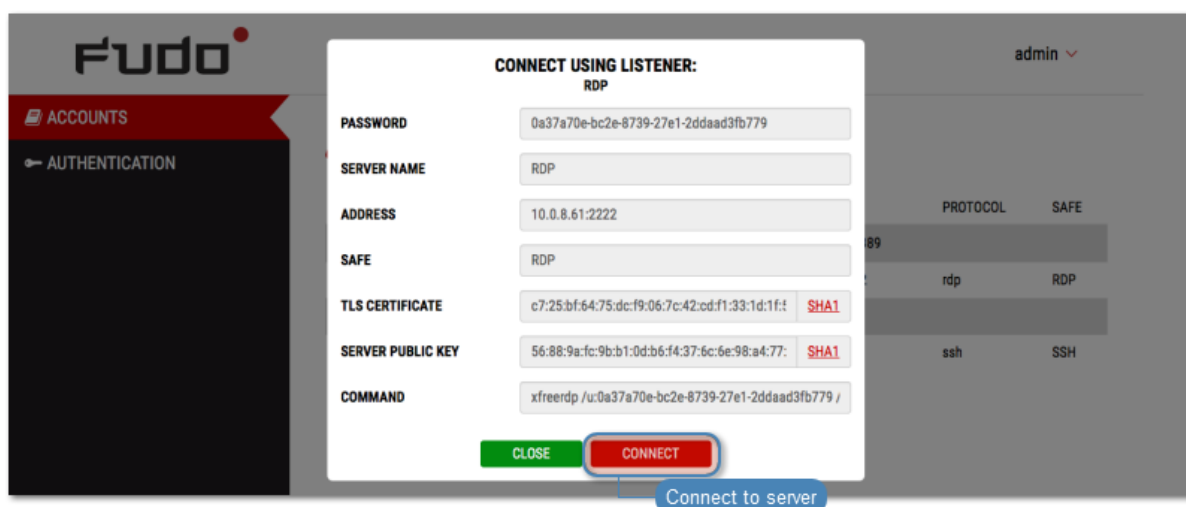


3. Select desired listener and click  icon.

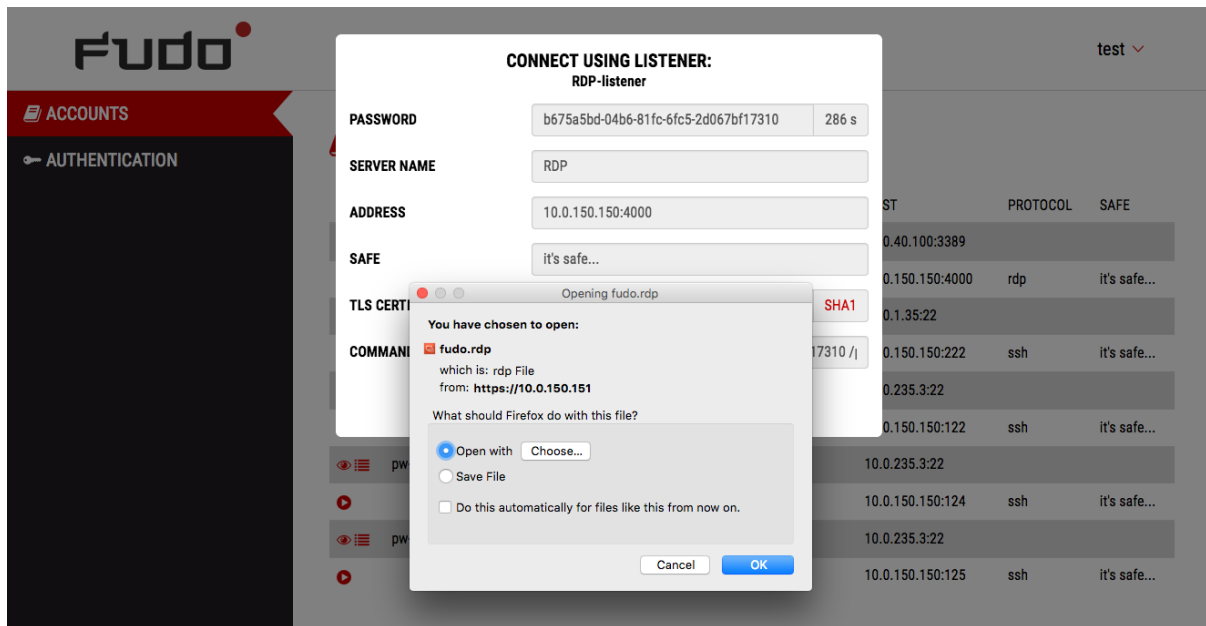
Note:

- The list contains both internal and external listening addresses.
- In case there is the  icon displayed next to the safe instead of the  icon, you must *fill in access request form*.

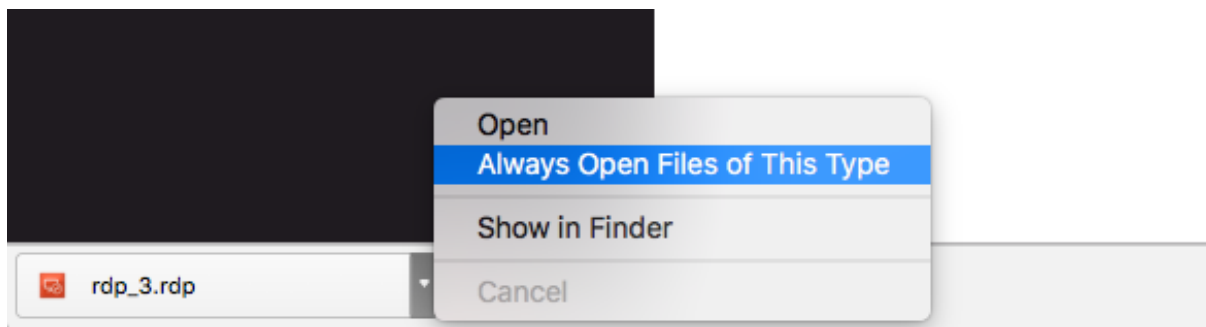
4. Click *CONNECT* to launch client application appropriate for selected listener with connection parameters forwarded.



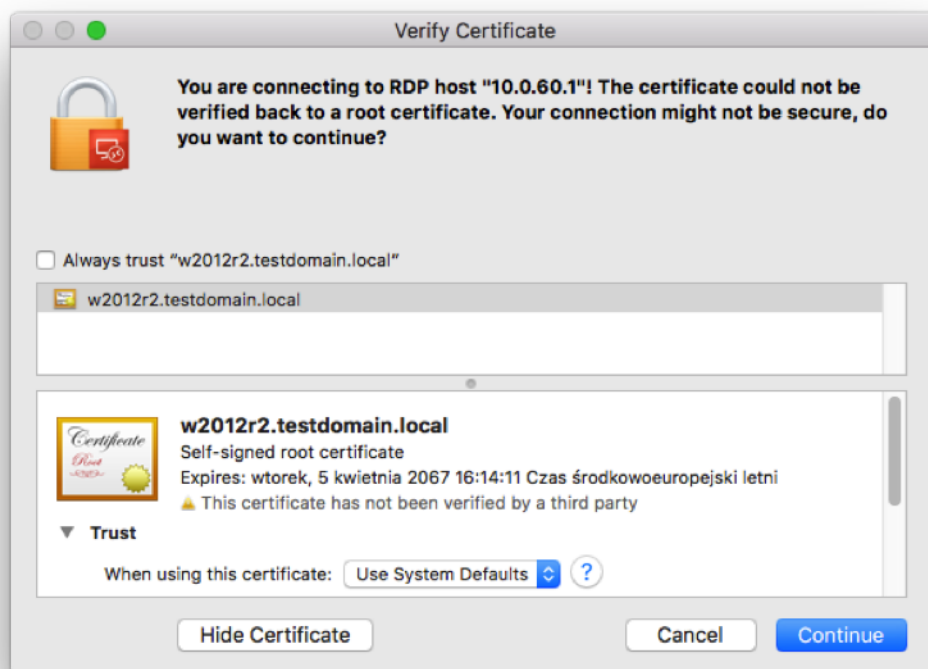
5. Save the connection definition file or launch a dedicated RDP protocol client.

**Note:**

- *Google Chrome* will automatically save the file.
- Select the *Always open this file type* option to automatically start the client app.



6. Click *Continue* to accept the certificate and initiate connection with selected server.



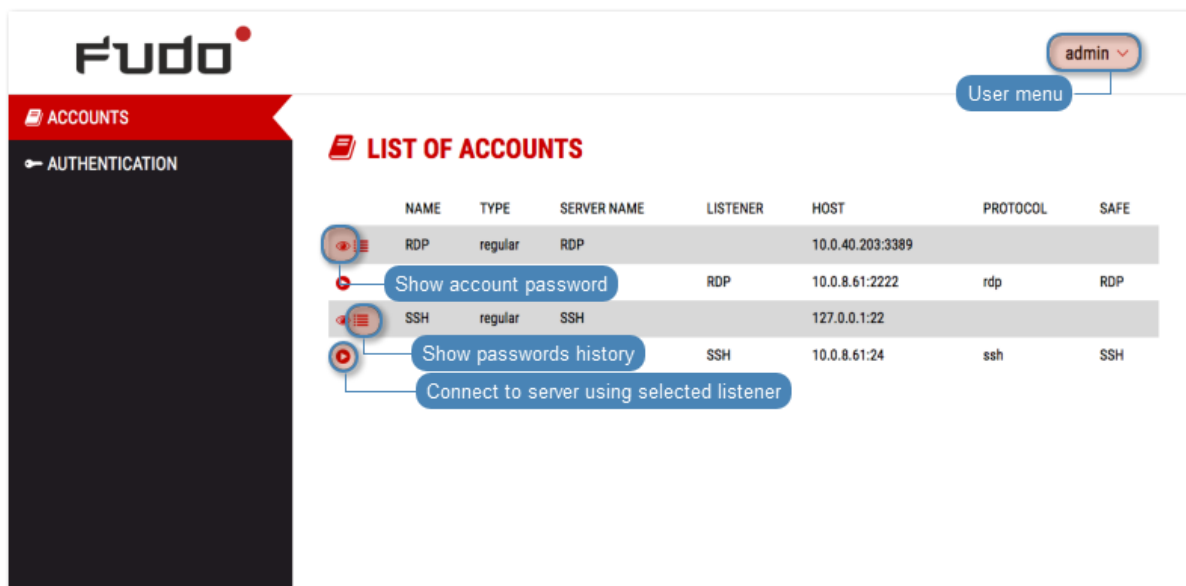
Related topics:

- *Connecting over RDP on Microsoft Windows 7 and 10*
- *Connecting over RDP on Ubuntu Linux*

6.3 Connecting over RDP on Ubuntu Linux



Note: Establishing RDP connections on Ubuntu 16.04 LTS requires installing `xfreerdp`. Execute `sudo apt-get install freerdp-x11`, to install it before proceeding with connecting over RDP protocol.

1. Log in to the User Portal and select *ACCOUNTS*.
2. Find desired account and server.

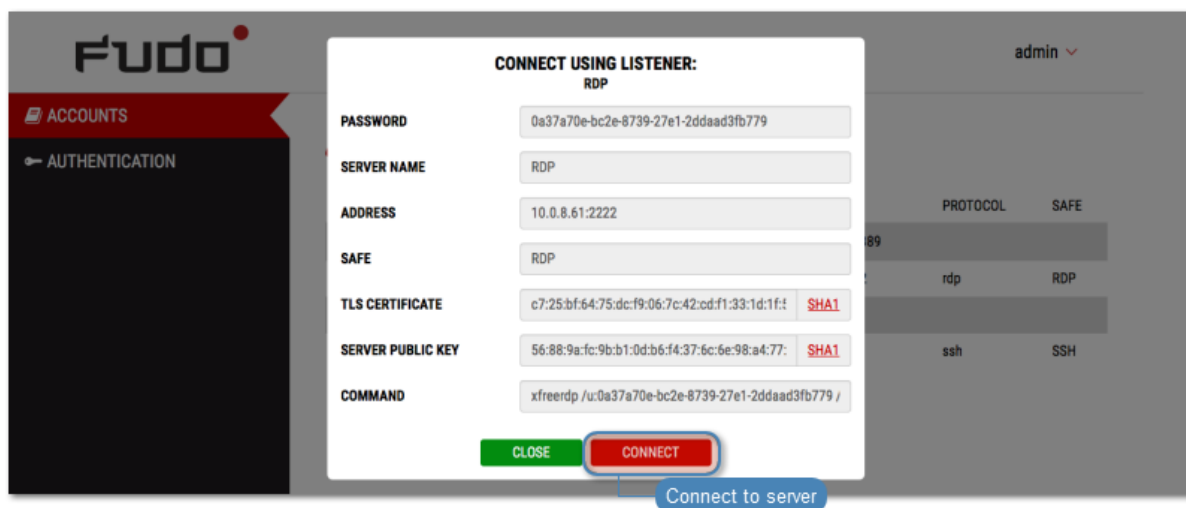


3. Select desired listener and click  icon.

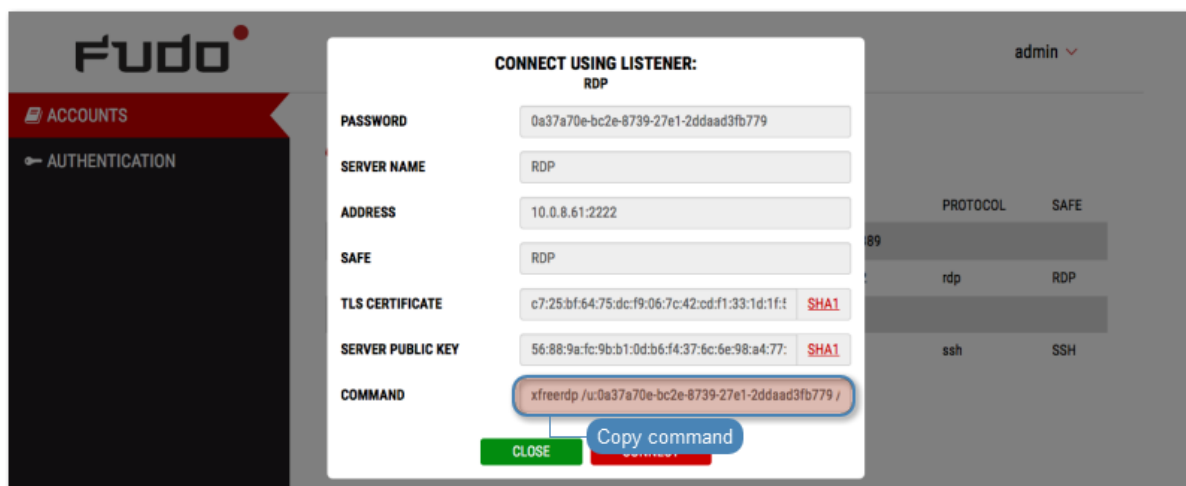
Note:

- The list contains both internal and external listening addresses.
- In case there is the  icon displayed next to the safe instead of the  icon, you must *fill in access request form*.

4. Click *CONNECT* to launch client application appropriate for selected listener with connection parameters forwarded.



5. Copy generated string.



- Execute command in terminal window.

Related topics:

- *Connecting over RDP on Mac OS X*
- *Connecting over RDP on Microsoft Windows 7 and 10*

6.4 Connecting over SSH on Microsoft Windows 7 and 10

Note: To automatically initiate SSH connections you must install *PuTTY* and configure association between client the app and the SSH protocol. To do the latter it is advised to install *WinSCP*, which will perform necessary configuration changes. Both programs must be in their 32-bit versions.

- Download and install *WinSCP*.

<https://winscp.net/download/WinSCP-5.9.5-Setup.exe>

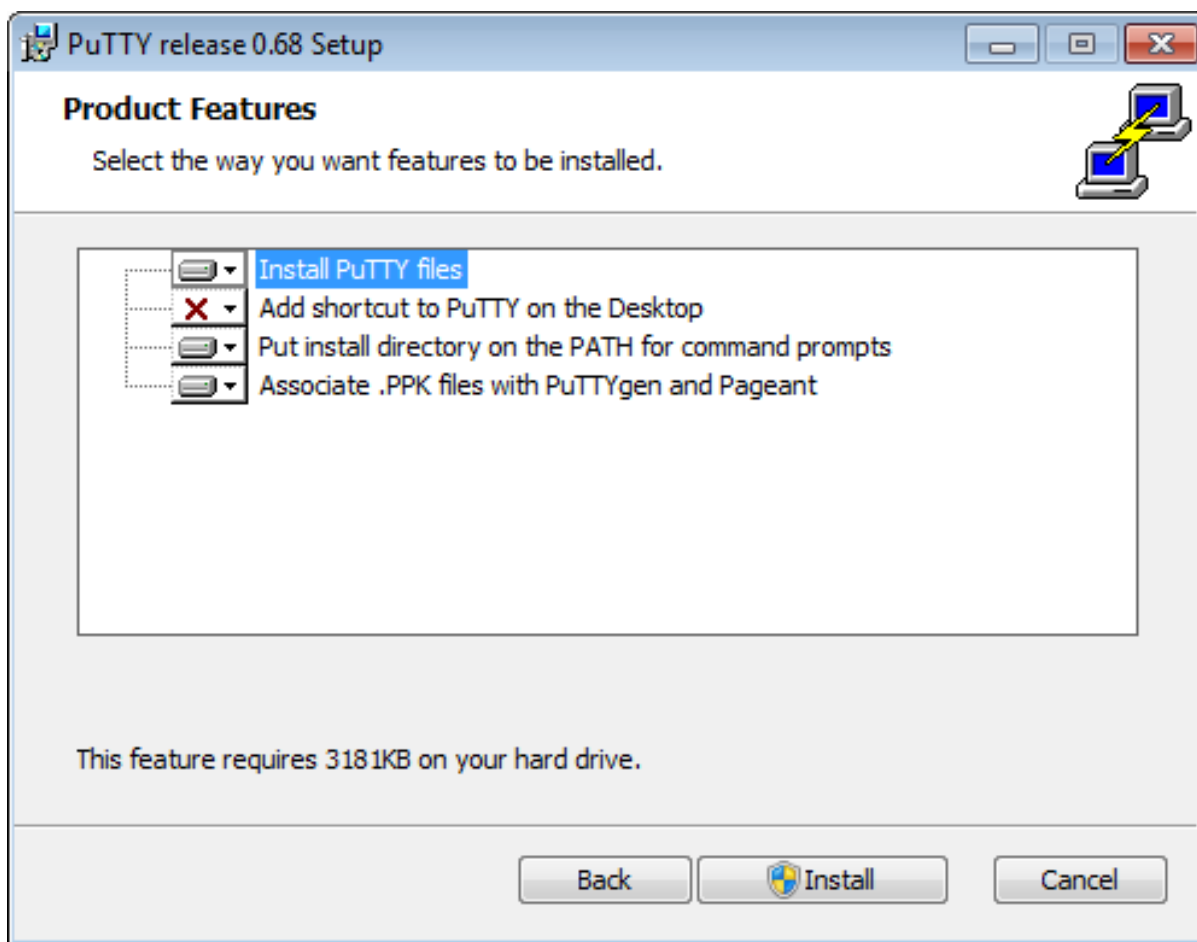
Note: Verify the checksum value to make sure that the integrity of the binary file has not been compromised.

- Download and install *PuTTY*.

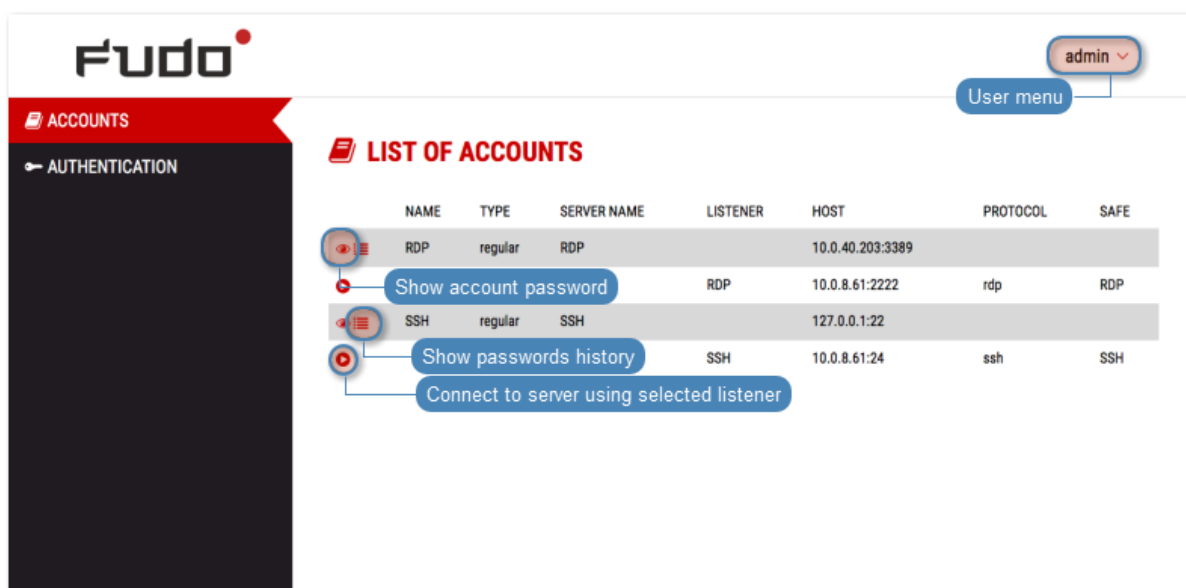
<https://winscp.net/download/putty-0.68-installer.msi>

Note:

- Install *PuTTY* in the default installation location: C:\Program Files (x86)\PuTTY\.
- During installation select default features set.





3. Log in to the User Portal.
4. Select *ACCOUNTS*.
5. Find desired account and server.

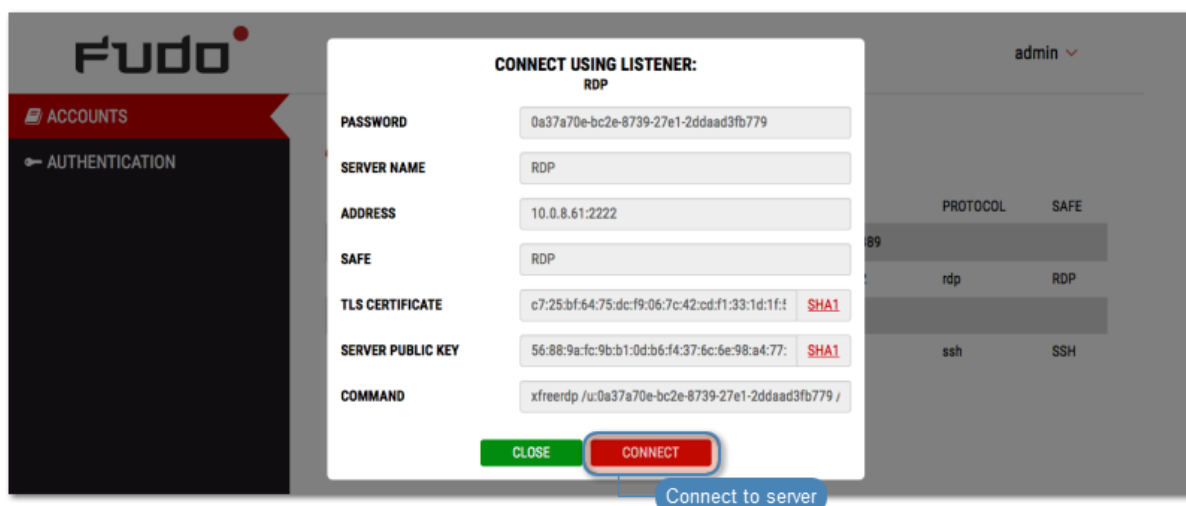


6. Select desired listener and click  icon.

Note:

- The list contains both internal and external listening addresses.
- In case there is the  icon displayed next to the safe instead of the  icon, you must *fill in access request form*.

7. Click **CONNECT** to launch client application appropriate for selected listener with connection parameters forwarded.



8. In the *Launch application* select *WinSCP:SFTP,FTP,WebDAV and SCP* and click *Open*.

9. The connection has been established.

```

10.0.60.1 - PuTTY
Using username "74f6adec-79b3-d384-1f25-f0b735960e42".
Last login: Mon Apr 10 13:32:08 2017 from 10.0.60.105
FreeBSD 11.0-STABLE (GENERIC) #0 r313108: Fri Feb  3 01:46:57 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:  https://www.FreeBSD.org/security/
FreeBSD Handbook:    https://www.FreeBSD.org/handbook/
FreeBSD FAQ:         https://www.FreeBSD.org/faq/
Questions List:      https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:     https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:     man hier

Edit /etc/motd to change this login announcement.
root@freebsd01:~ #

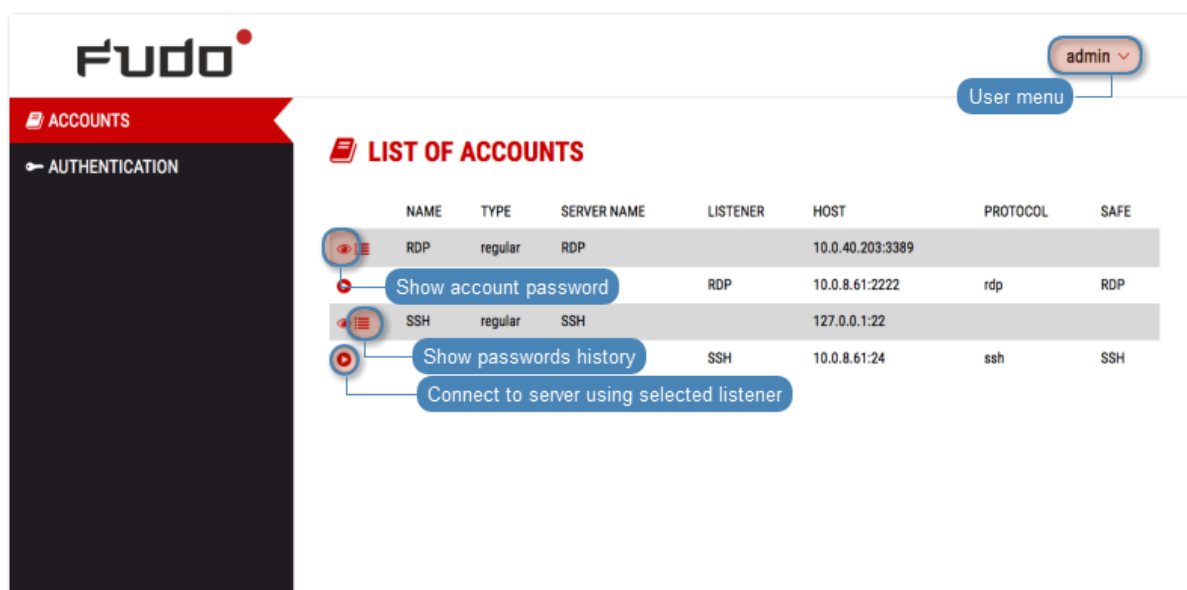
```

Related topics:

- *Connecting over RDP on Mac OS X*
- *Connecting over RDP on Microsoft Windows 7 and 10*
- *Connecting over RDP on Ubuntu Linux*



6.5 Connecting over SSH on Mac OS

1. Log in to the User Portal and select *ACCOUNTS*.
2. Find desired account and server.

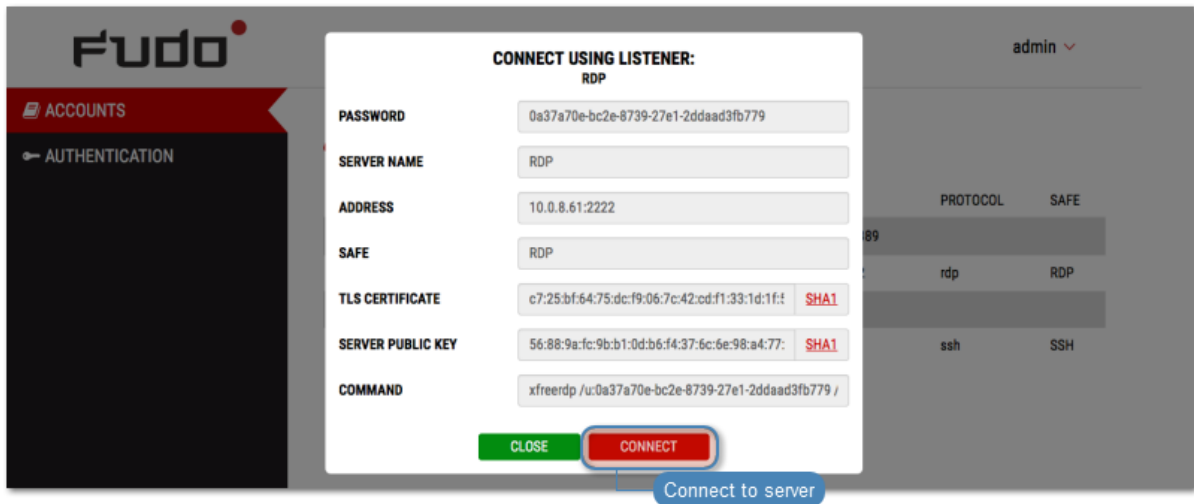


3. Select desired listener and click  icon.

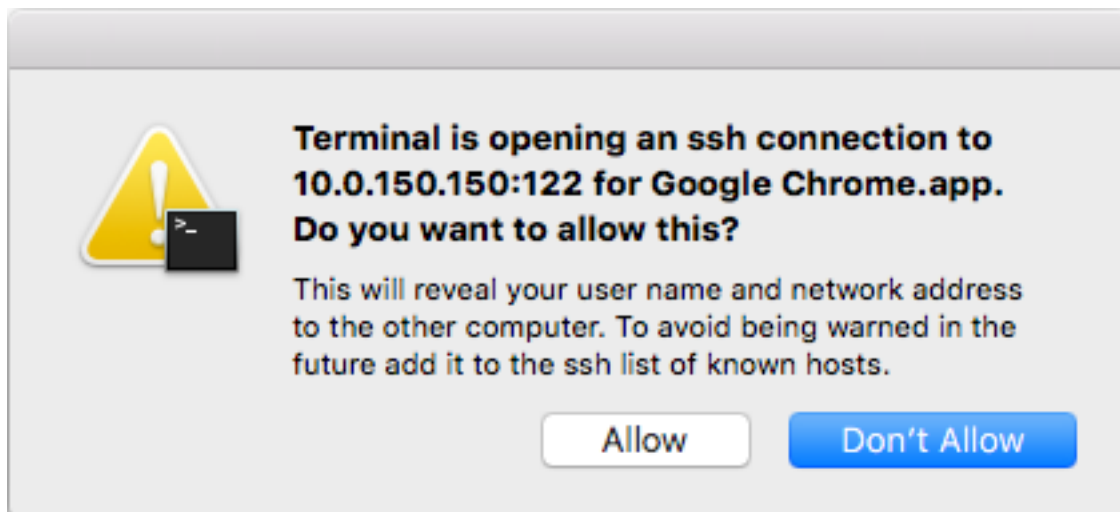
Note:

- The list contains both internal and external listening addresses.
- In case there is the  icon displayed next to the safe instead of the  icon, you must *fill in access request form*.

4. Click *CONNECT*.



5. Click *Allow* to open the Terminal.



6. The connection has been established.



Related topics:


- *Connecting over RDP on Mac OS X*
- *Connecting over RDP on Microsoft Windows 7 and 10*
- *Connecting over RDP on Ubuntu Linux*

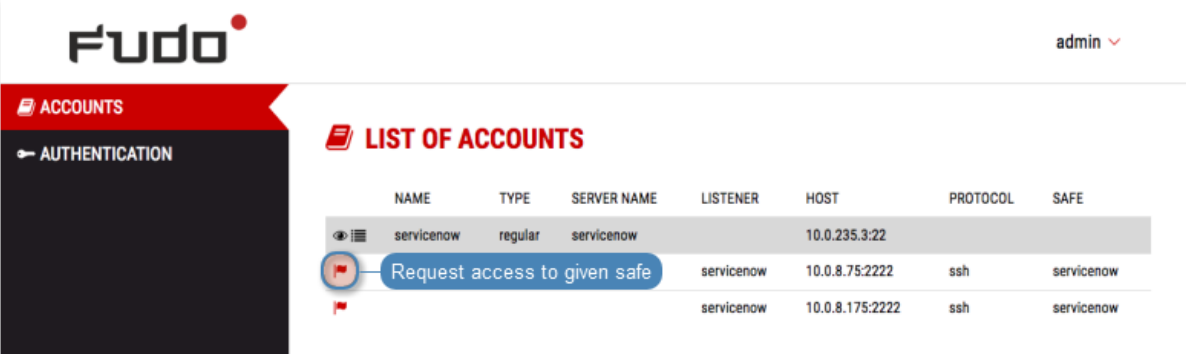
Requesting access to safe

Note:

- Using this feature requires ServiceNow ticketing system.
- Usernames on Wheel Fudo PAM and *ServiceNow* must be the same to ensure correct requests processing.

To request access to safe, proceed as follows.

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

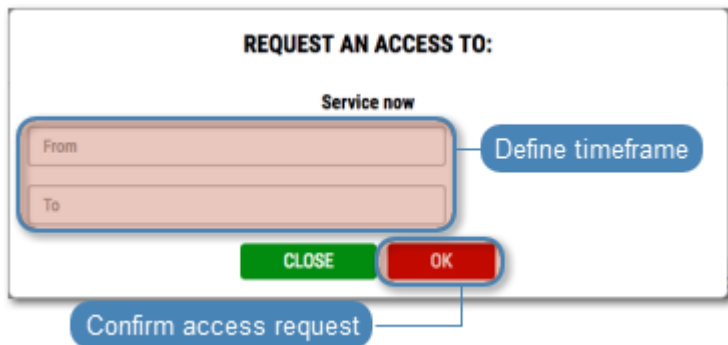


The screenshot shows the Fudo user portal interface. The top left has the Fudo logo and a navigation menu with 'ACCOUNTS' and 'AUTHENTICATION'. The top right shows the user 'admin'. The main content area is titled 'LIST OF ACCOUNTS' and contains a table with the following data:

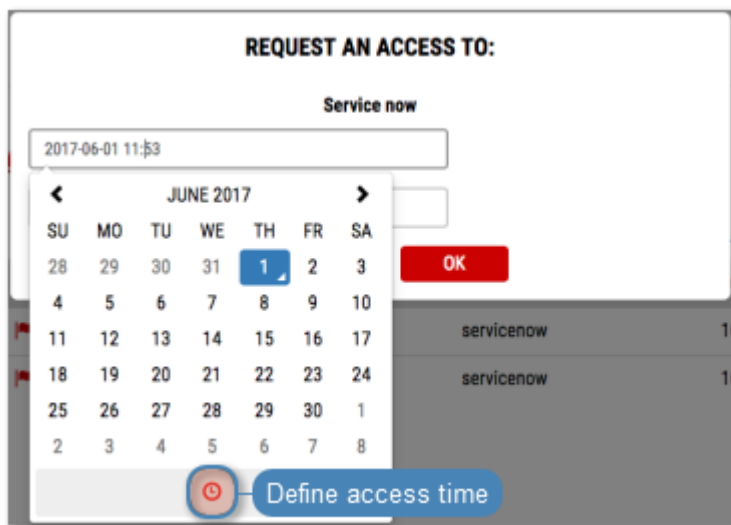
NAME	TYPE	SERVER NAME	LISTENER	HOST	PROTOCOL	SAFE
servicenow	regular	servicenow		10.0.235.3:22		
			servicenow	10.0.8.75:2222	ssh	servicenow
			servicenow	10.0.8.175:2222	ssh	servicenow

A blue button labeled 'Request access to given safe' is positioned over the second row of the table. A red flag icon is visible to the left of the button.

3. Define time period and click *OK*.



Note: Click the  icon to access time settings.



Authentication provides an overview of authentication methods assigned to the logged in user.

Changing static password

1. Select *AUTHENTICATION*.
2. Provide old and new passwords and click *SAVE*.

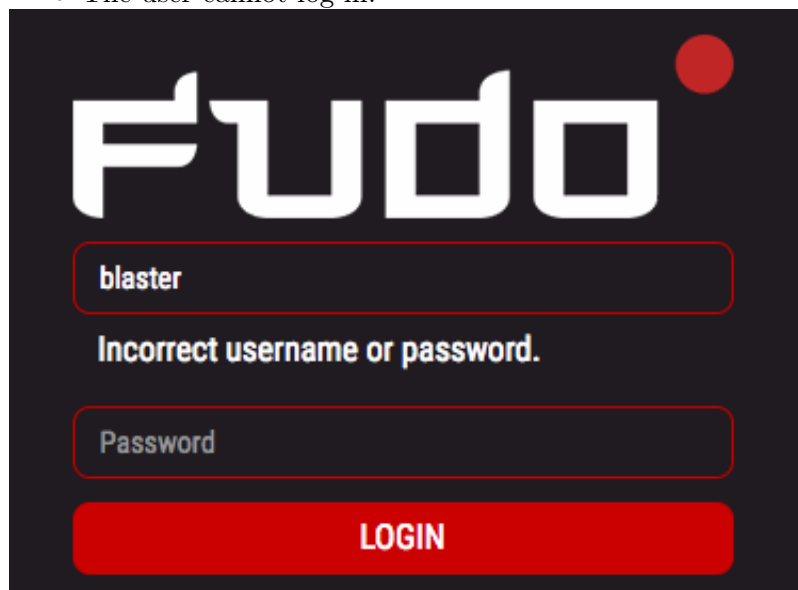
The screenshot shows the Fudo web interface. At the top left is the 'Fudo' logo. At the top right, the user 'admin' is logged in. The main navigation bar includes 'ACCOUNTS' and 'Manage authentication methods'. A red sidebar menu has 'AUTHENTICATION' selected. The main content area is titled 'EXTERNAL AUTHENTICATION' and contains a text input field for 'EXTERNAL AUTHENTICATION SERVER' with the value 'AD 127.0.0.1:10'. Below this is the 'STATIC PASSWORDS' section, which includes three text input fields labeled 'OLD PASSWORD:', 'NEW PASSWORD:', and 'REPEAT PASSWORD:'. At the bottom right of the form are 'RESET' and 'SAVE' buttons. A blue callout box points to the 'SAVE' button with the text 'Save new password'.

Problem	Symptoms and solution description
---------	-----------------------------------

Cannot log in to the User Portal

Symptoms:

- The user cannot log in.

**Solution:**

- Make sure you are entering correct login credentials.
 - Contact system administrator to verify whether you have User Portal access privileges.
 - Contact system administrator to verify the User Portal time policy settings.
-

Problem	Symptoms and solution description
Accounts list is missing objects.	Solution: <ul style="list-style-type: none">• Contact your system administrator to make sure you have access to required safes.
	Symptoms: <ul style="list-style-type: none">• Cannot connect to selected server.
	Reason: connection takes place outside the timeframe defined by the access time policy.
	Solution: contact system administrator to verify your time policy settings.