FUDO | PAM

Fudo PAM 5.0 – User Portal Manual

Release 1.0

Fudo Security Inc.

08.12.2021

Contents

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

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

CHAPTER 2

System overview

User Portal enables initiating connections with monitored servers available for the logged-in user.

The user portal also allows:

- checking out an account password and make its automatic checkin after a specified timeout.
- viewing a password history to selected accounts, managed by FUDO's password vault module.

English, Polish, Russian, and Ukrainian languages are available as an application language.
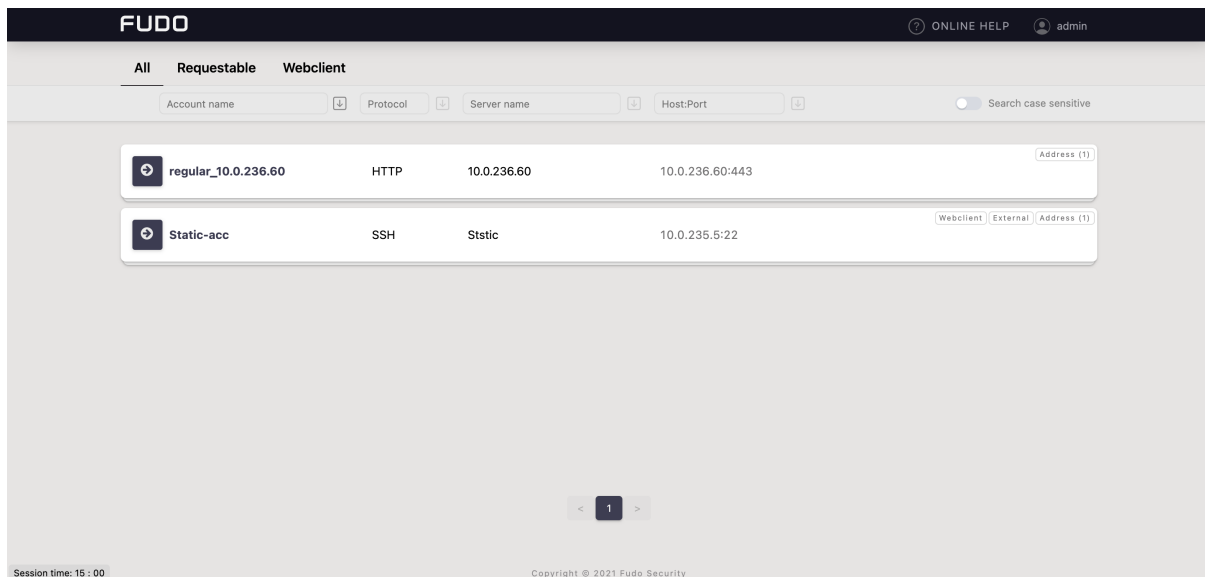
# Logging into the User Portal

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.
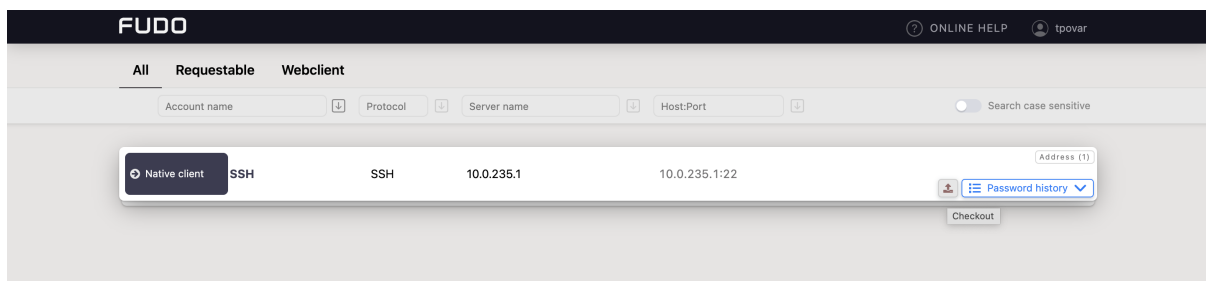3. Enter the username, password and click *LOGIN*.
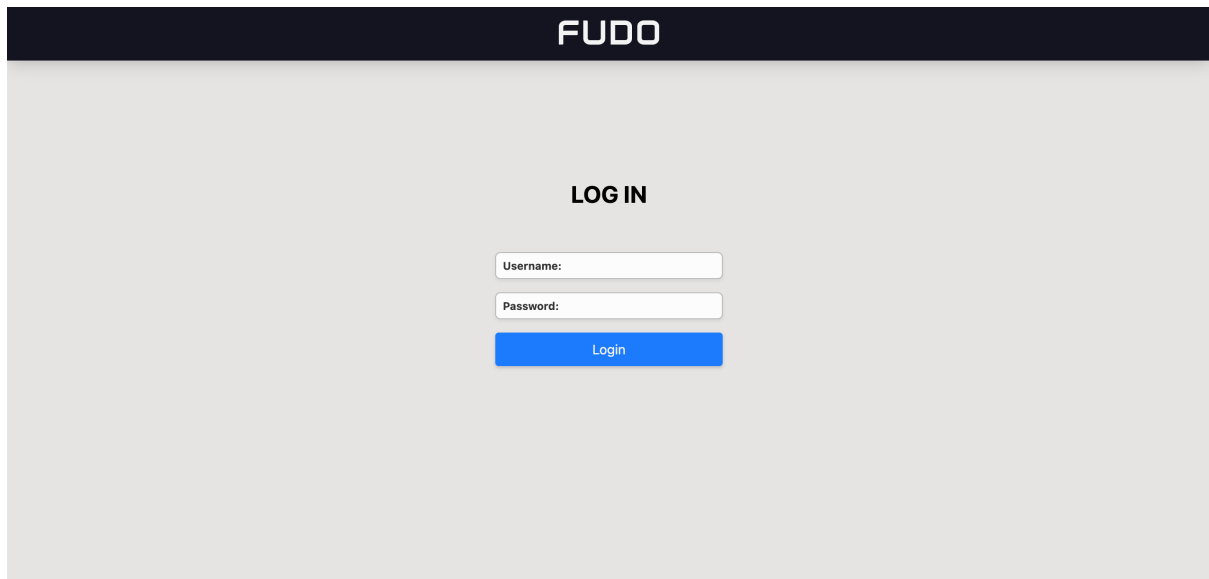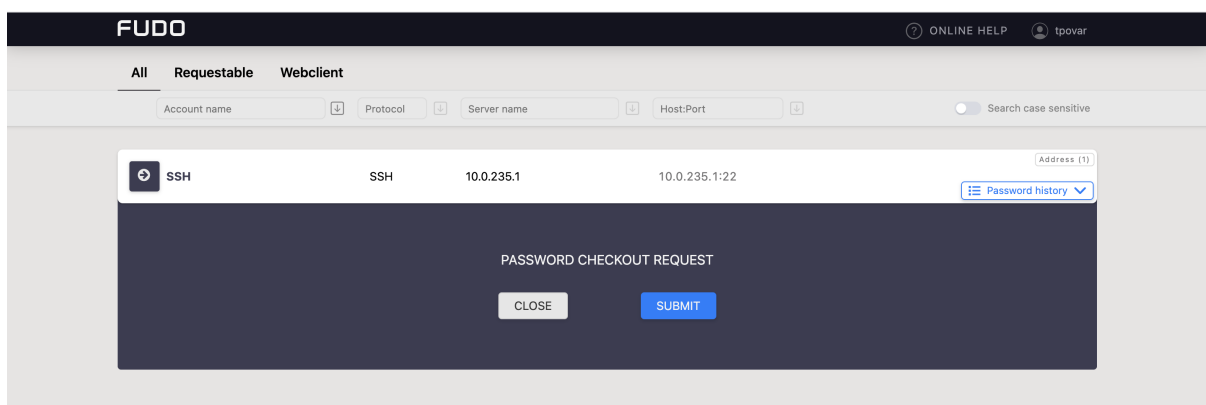
Related topics:

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

Secret Checkout and Checkin

4.1 Secret Checkout

1. Find an account whose password you want to checkout, hover mouse on it to display more options.

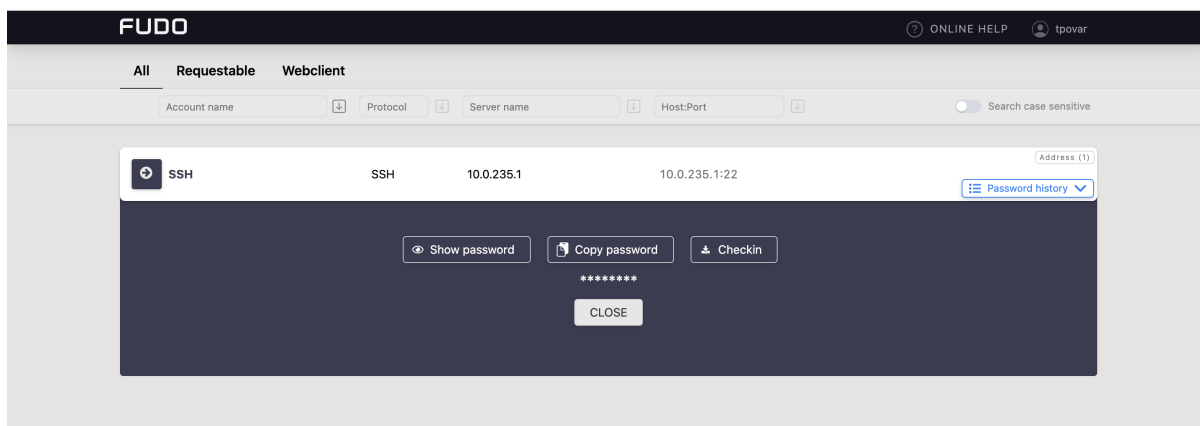2. Click the 🔖 icon.

3. Click *SUBMIT*.

Note:

- Prompt for password checkout reason is optional for the safe configuration.

- Depending on the configuration, password checkout may require system administrator's approval.

- If the password is currently taken by the other user, wait until it's returned or use the *FORCE CHECKOUT* option.

4. Click:

    - *Show password* to disclose the password.

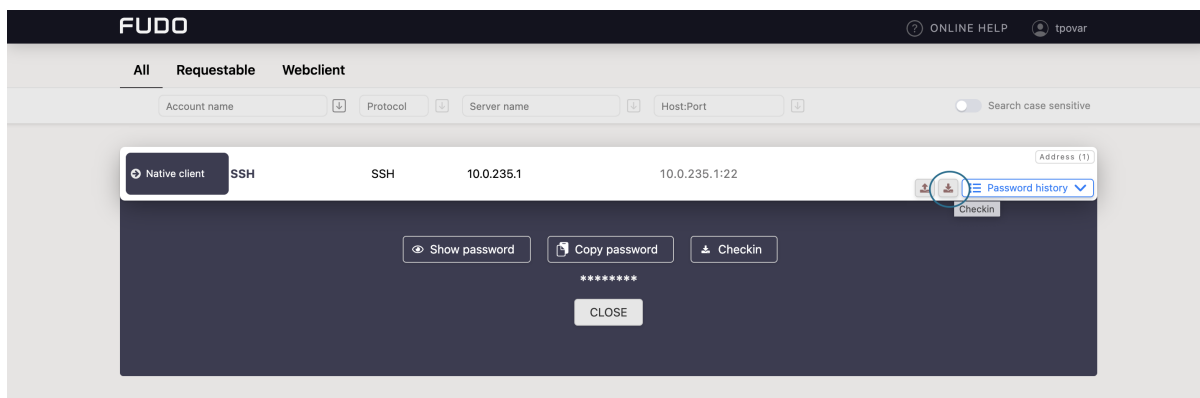   - *Copy password* to copy the password to system clipboard.

4.2 Secret Checkin

1. Find an account whose password you want to return, hover mouse on it to display more options.

2. Click ![icon] icon.

or

click the ![icon] icon to open the *ACCOUNT PASSWORD* modal window and click ![icon] Checkin.

Displaying and editing accounts notes

Notes are created by the system administrator and they provide additional information on server access.

Note: Notes access is granted by the system administrator on *safe* object level. Depending on system settings, users can access notes in read-only or read and write modes.

1. Find account which note you want to access, hover mouse on it to display more options.

2. Click a comment icon to open the note.
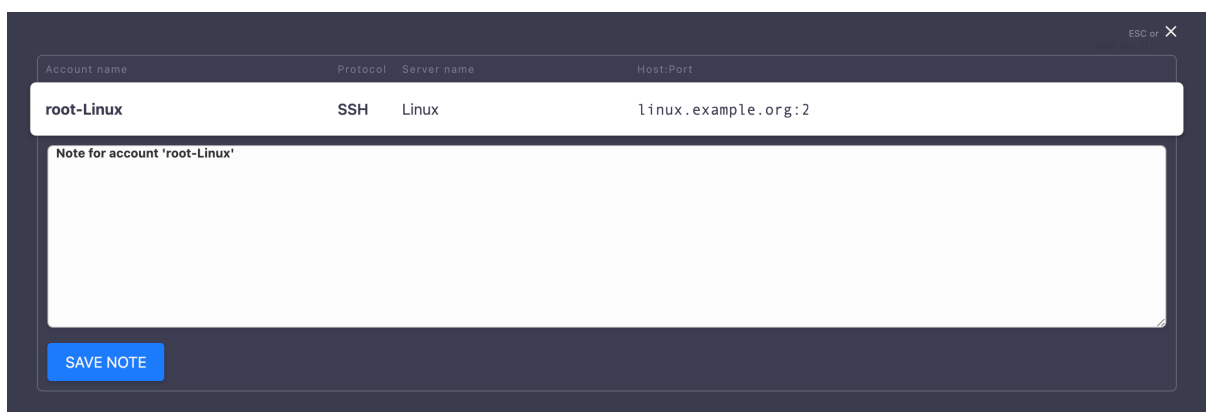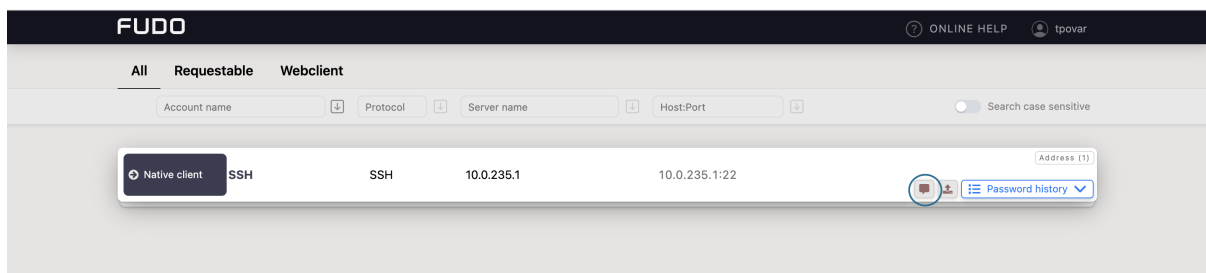
3. Add or edit the note and click *SAVE NOTE* to store changes. Click on the Cancel button on the upper right corner or press the *Esc* key on your keyboard to close the modal without

changes.

Note: Notes' editing requires *write* access right assigned by the system administrator.

6.1 Connecting via the access request

A user can send a request for access to the resources via the portal.

In order to send a request, hover your mouse over the particular account.

Click the *Access request* button. In the opened window choose a type of request, define its time, and send the request.
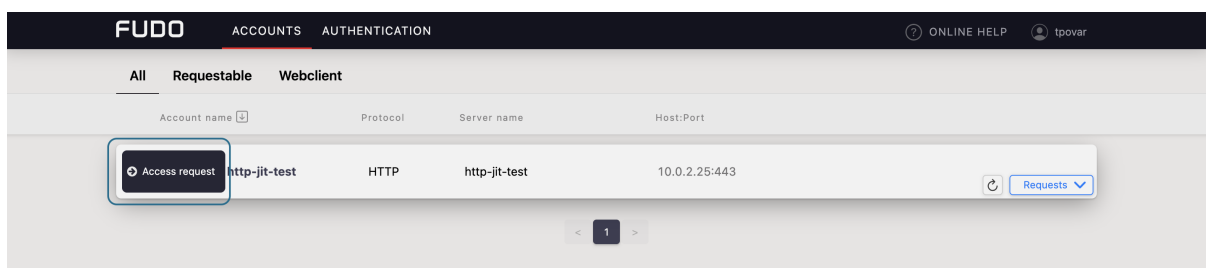
Two types of requests are available: **immediate** and **scheduled**.

Immediate requests can be set from now up to the next 24 hours.

When a user sends an immediate request, its access time starts when the request is accepted. Then, the user has 24 hours to start their session. When the user starts the session, the system counts the session time, which the user had requested, and terminates connection when the requested session time is over. If the user does not use the access and does not connect for 24 hours after access is granted, the access becomes expired.

For the **scheduled** type of requests, the user chooses a start date and an end date, which means access will be granted for a whole day from the start date till the end date.


For both types of requests, the *Reason* field is required in order to activate the sending.

The requests history, as well as the status of the pending requests, is available under the *Requests* drop-down list having a mouse over the account.
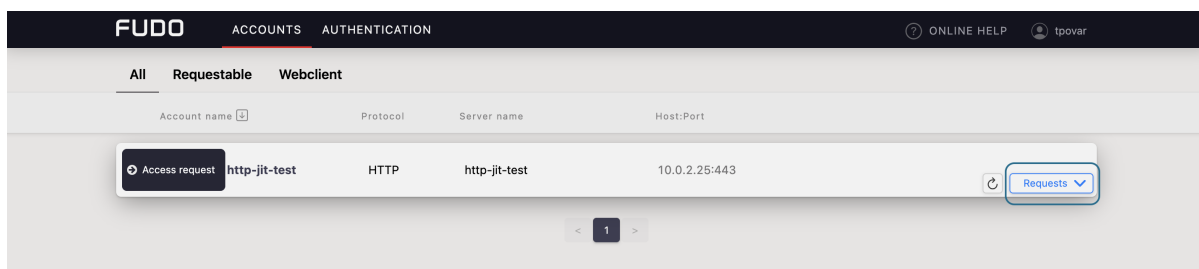
Here also the user can observe the process of voting, including a number of required votes and how much is left for access to be granted.
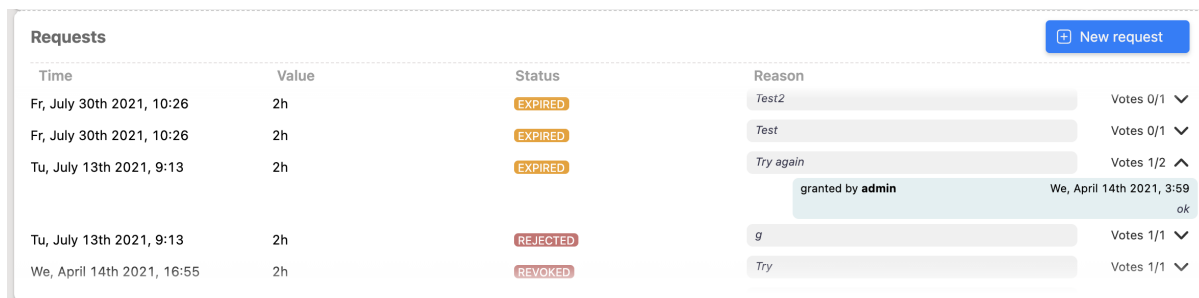

When the access has been already granted, the user can send another request from the requests history bar by selecting the *+ New request* button.

6.2 Connecting over RDP and SSH in browser

Connecting over RDP and SSH in browser is available via the Webclient feature. Filter the Webclient-supported accounts by choosing the *Webclient* tab.

1. Find desired account and server, hover your mouse over to display more options.

2. Click the *Web client* button next to the account you want to use to connect to the server.
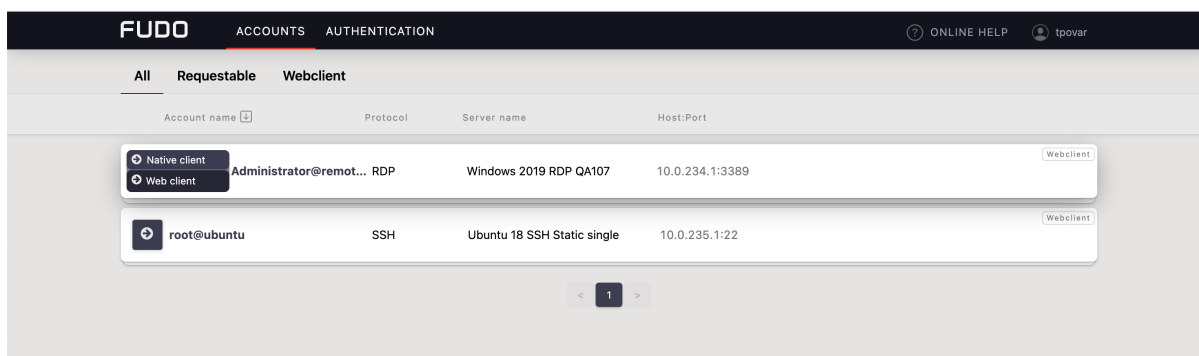

3. If the account has more than one server address configured, choose the one you want to connect to and click *Connect*.

Note: Each session is opened in a separate browser tab.

For the sessions, based on RDP and SSH protocols, panel tab has embedded the following features:

- *Hide* / *Show* button that minimizes / maximizes the connection window.

- a tab displays a protocol type, the listener name and the connection state:

    - 🟡 connection is establishing.

    - 🟢 session is connected.

    - 🔴 session is disconnected.

- *clipboard* feature allows copying a text fragment for the later paste.
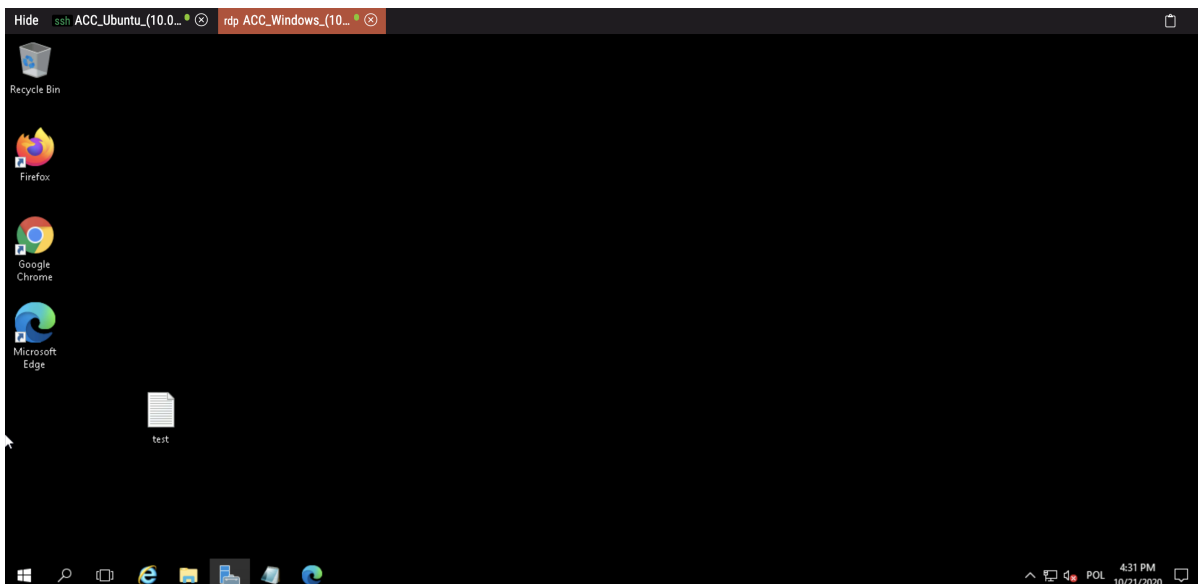
Note: Hovering over a particular tab shows the preview of the session.

Additionally, for the sessions based on SSH protocol, there are features that allow customizing the view:

- *font size*, and

- *a terminal color scheme* (default scheme is black-white, also available gray-black, green-black and white-black).

Related topics:

- *Connecting over RDP on Mac OS X*

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

- *Connecting over RDP on Ubuntu Linux*

6.3 Connecting over RDP on Microsoft Windows 7 and 10

1. Find desired account and server, hover your mouse over to show more options.

2. Select the *Native client* button.
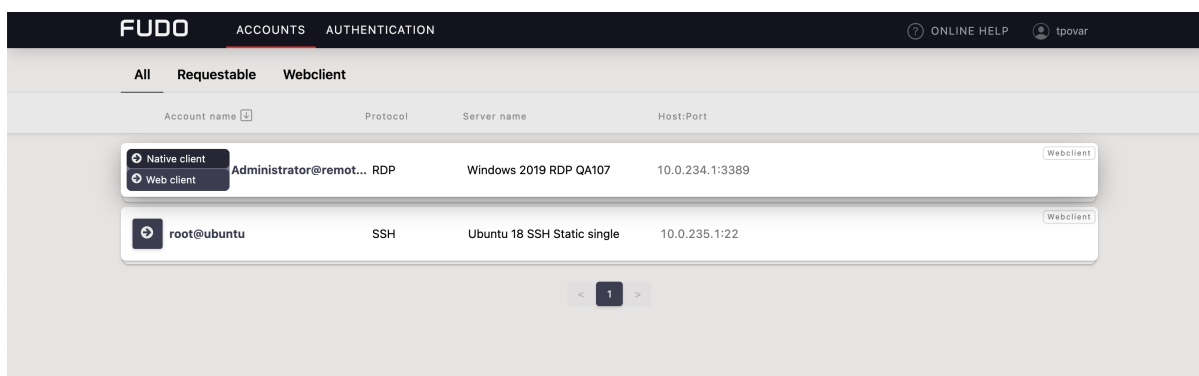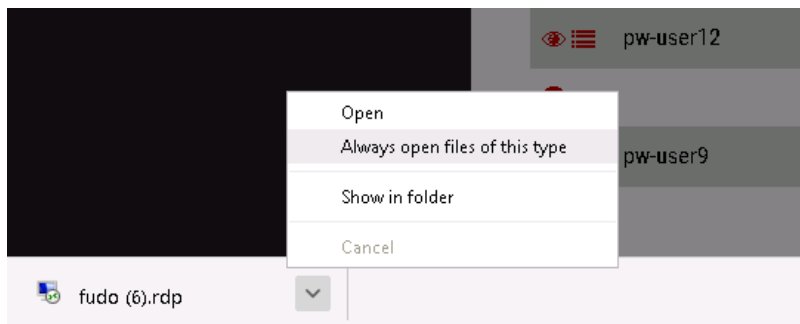

3. Choose the listener, via which you want to connect.

4. Click *Connect*.

Note:

- *Google Chrome* will automatically save the file.

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

5. Click *Continue* in the credentials prompt window without providing the password.

6. Click *Continue* to connect to the server despite the certificate alert.

Related topics:

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

6.4 Connecting over RDP on Mac OS X

Note: To establish RDP connections on Mac OS X, download and install *Microsoft Remote Desktop*.

1. Find desired account and server, hover your mouse over to show more options.

2. Select the *Native client* button.

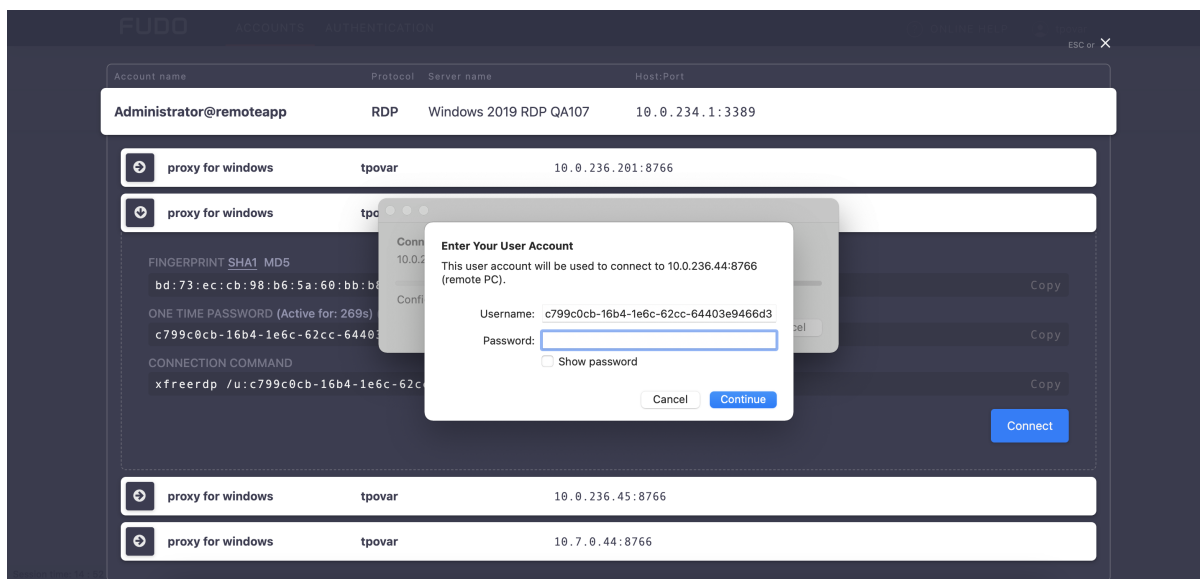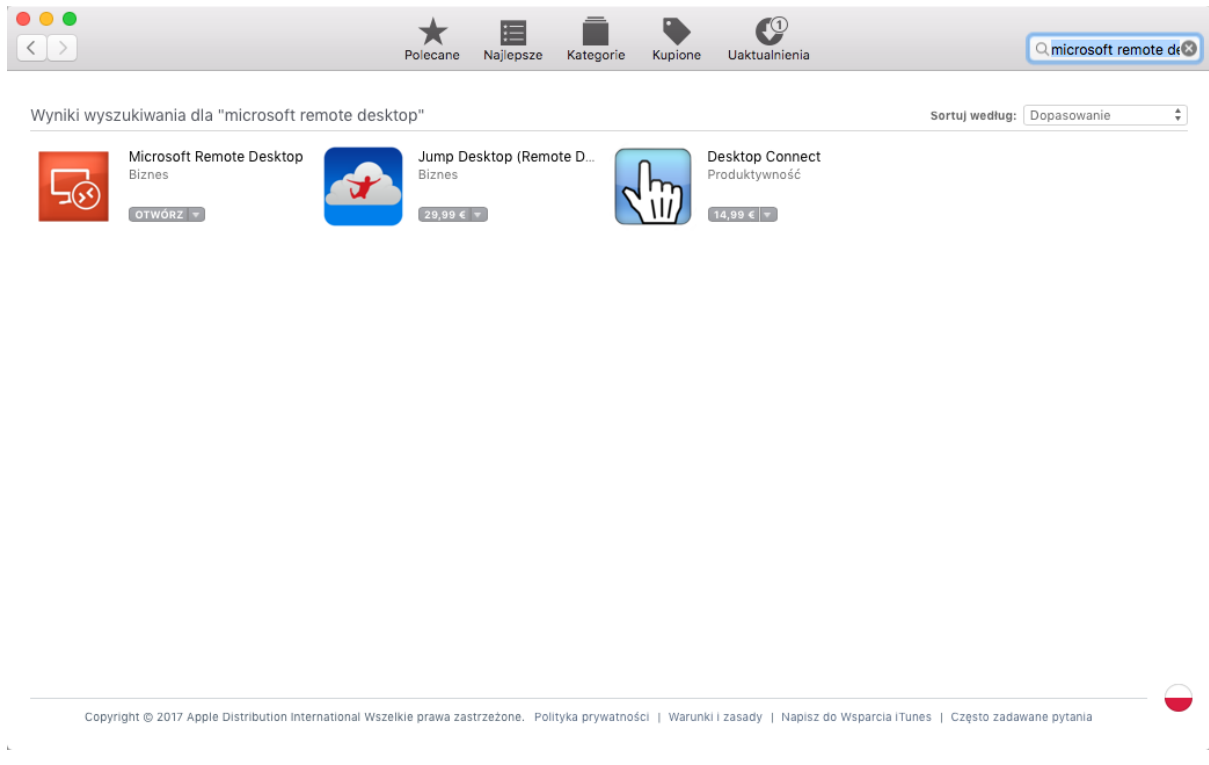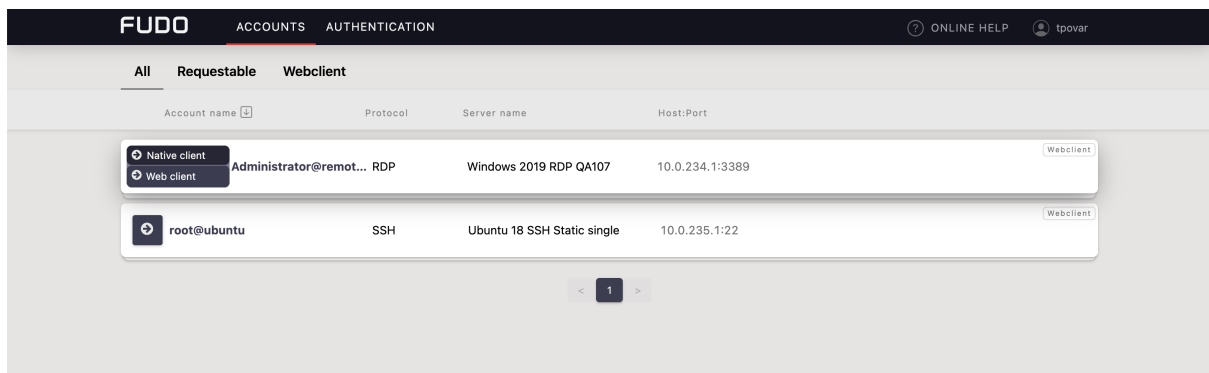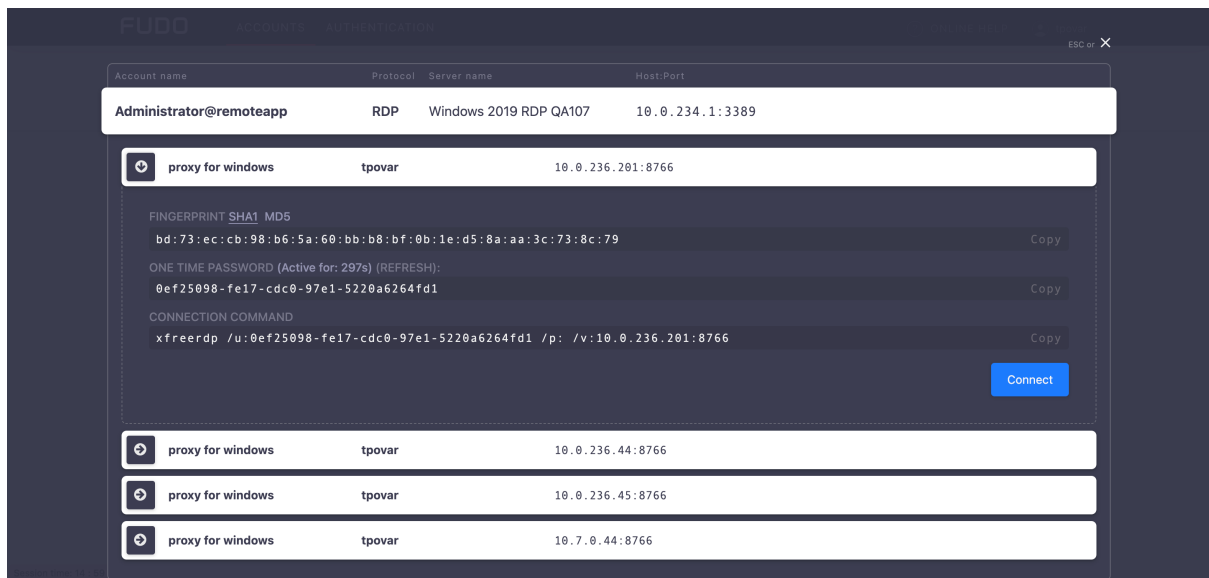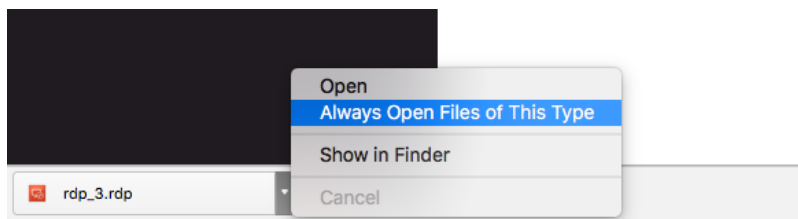3. Choose the listener, via which you want to connect.

4. Click *Connect*.

Note:

- *Google Chrome* will automatically save the file.

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

5. 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*

6.5 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. Find desired account and server, hover your mouse over to show more options.

2. Select the *Native client* button.

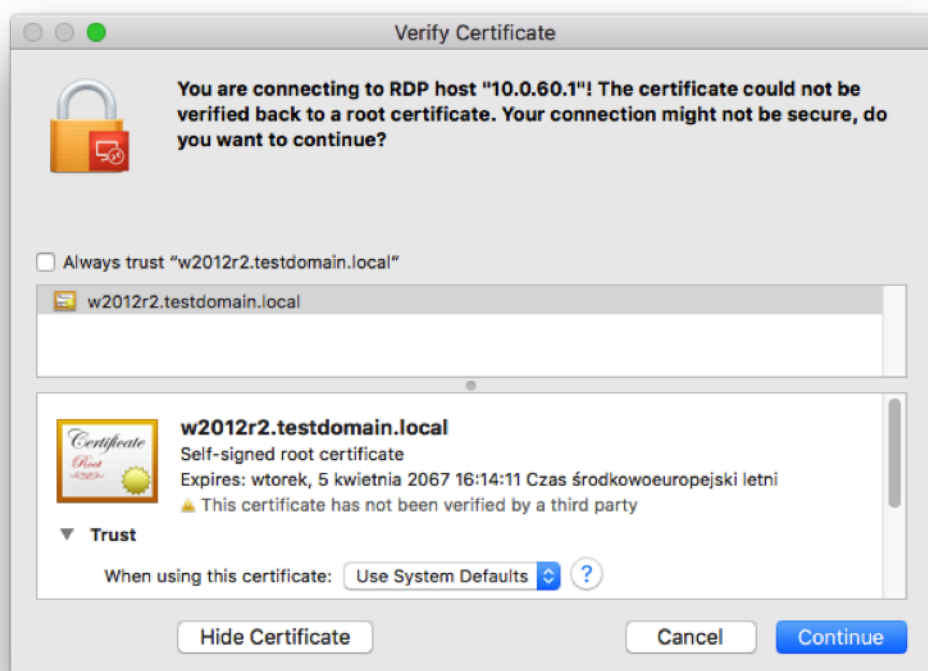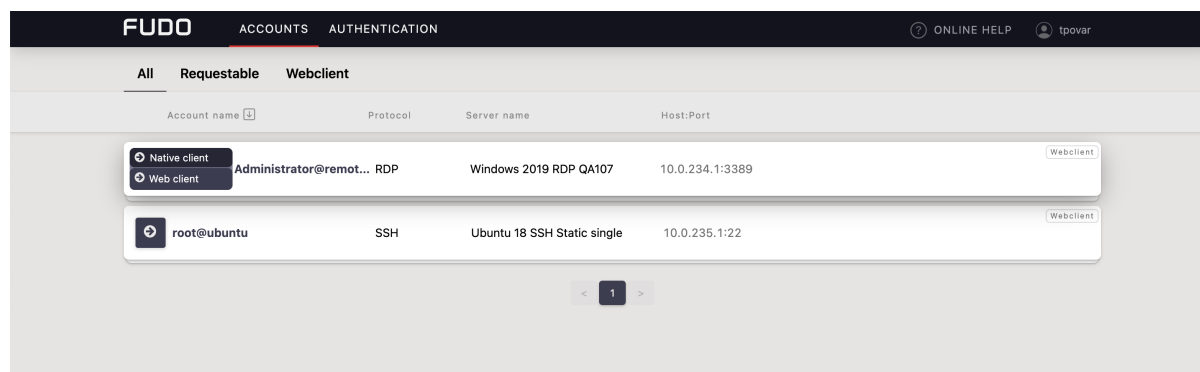3. Choose the listener, via which you want to connect.

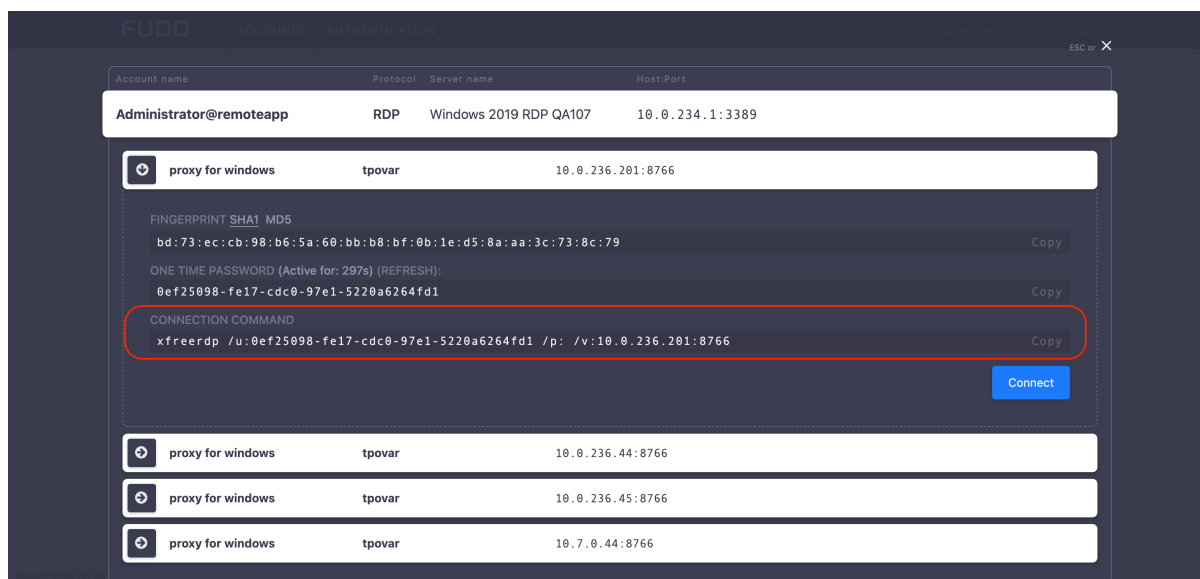4. Copy generated string.

5. Execute command in terminal window.

Related topics:

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

6.6 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.

1. Download and install *WinSCP*.

    `https://winscp.net/download/WinSCP-5.19.2-Setup.exe`

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

2. Download and install *PuTTY*.

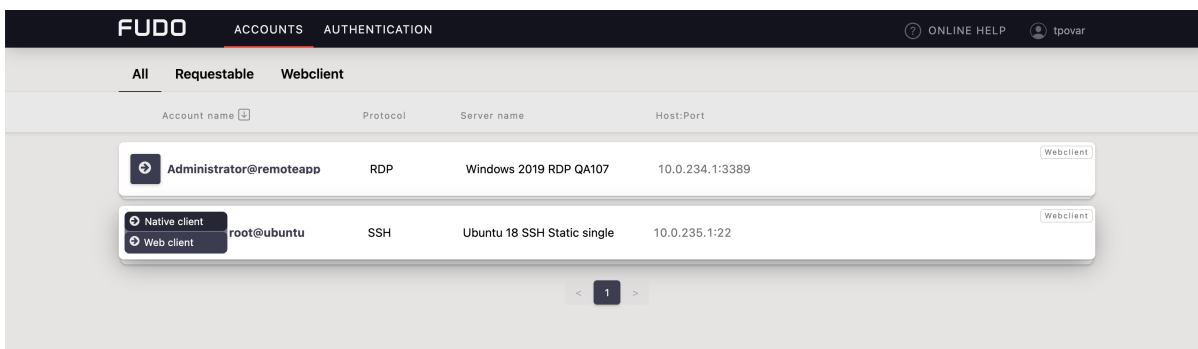   `https://winscp.net/download/putty-0.75-installer.msi`

Note:

- Install *PuTTY* in the default installation location: `C:\Program Files (x86)\PuTTY\`.
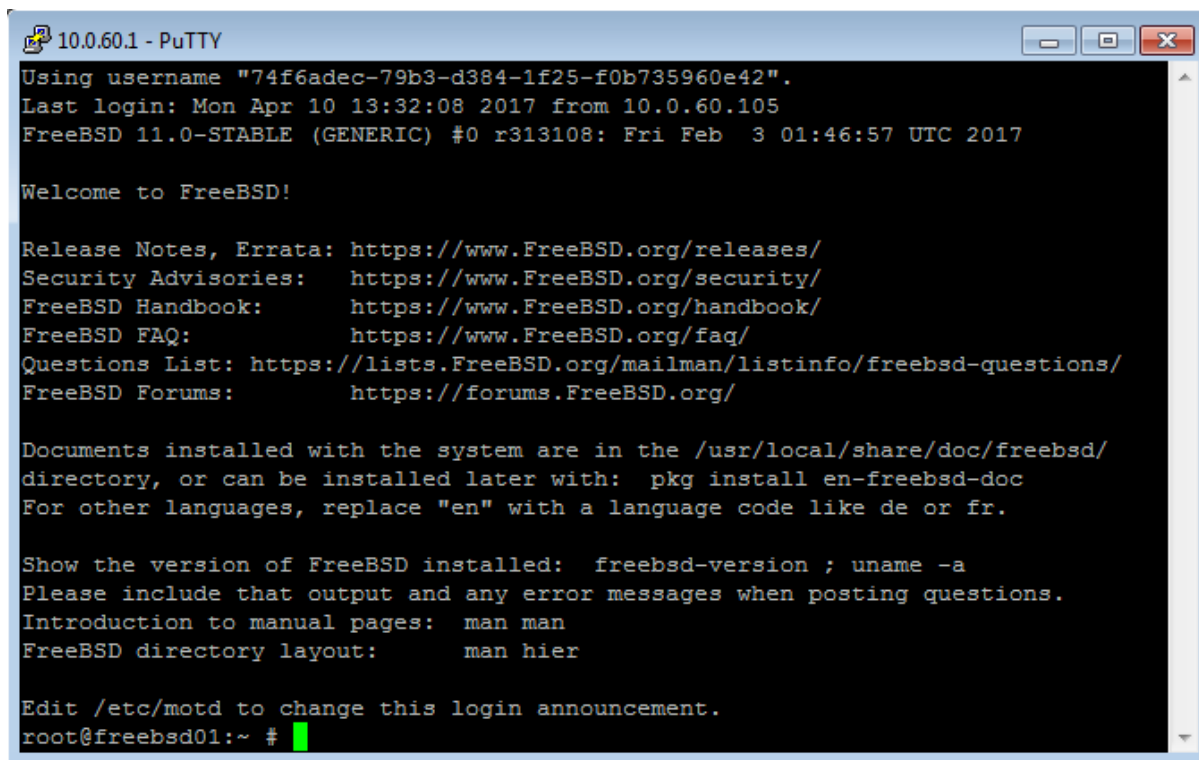- During installation select default features set.
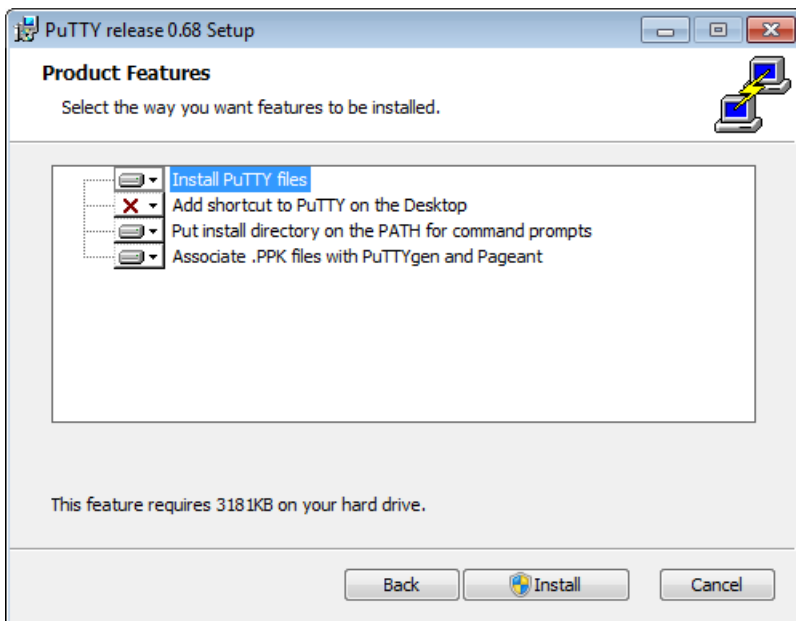
3. Log in to the User Portal.

4. Find desired account and server, hover your mouse over to show more options.

5. Select the *Native client* button.

6. Choose the listener, via which you want to connect.

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.

Related topics:

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

6.7 Connecting over SSH on Mac OS, Linux

1. Find desired account and server, hover your mouse over to show more options.

2. Select the *Native client* button.

3. Choose the listener, via which you want to connect.

4. Click *Connect*.

5. Click *Allow* to open the Terminal.

6. The connection has been established.

```
Last login: Wed May 10 10:59:47 2017
                                  $
```
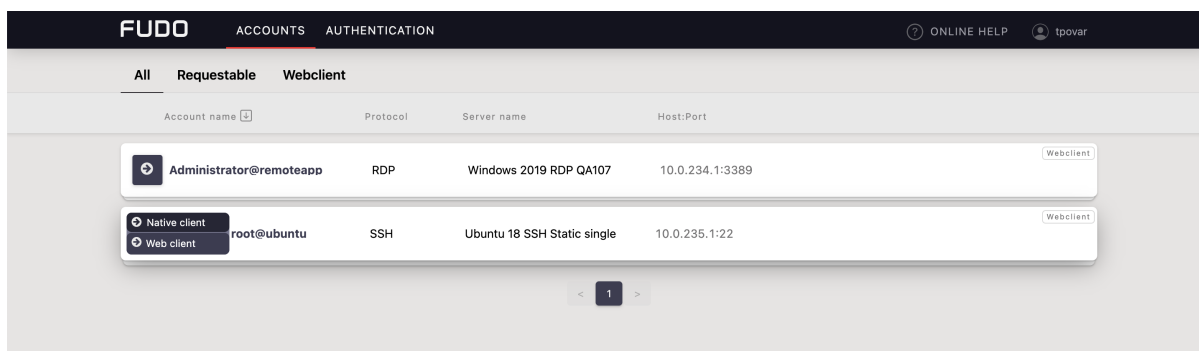
Related topics:

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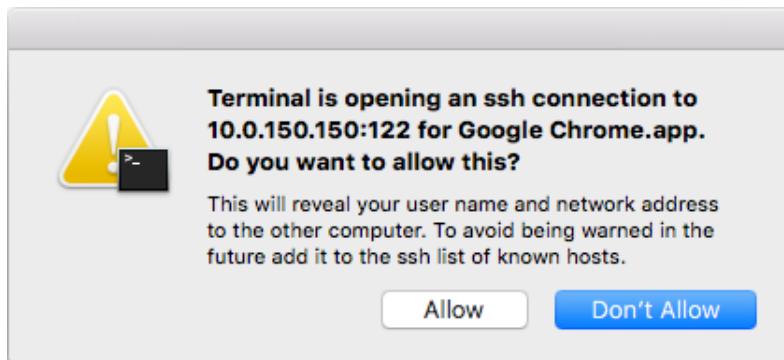- *Connecting over RDP on Ubuntu Linux*

CHAPTER 7

Change Password

Fudo PAM User Portal allows changing a static password as well as a password enabled as a part of multi-factor authentication.

In order to change the password, follow the steps:

1. Click on your login name on the upper right corner.

2. Select the *Change password* button.
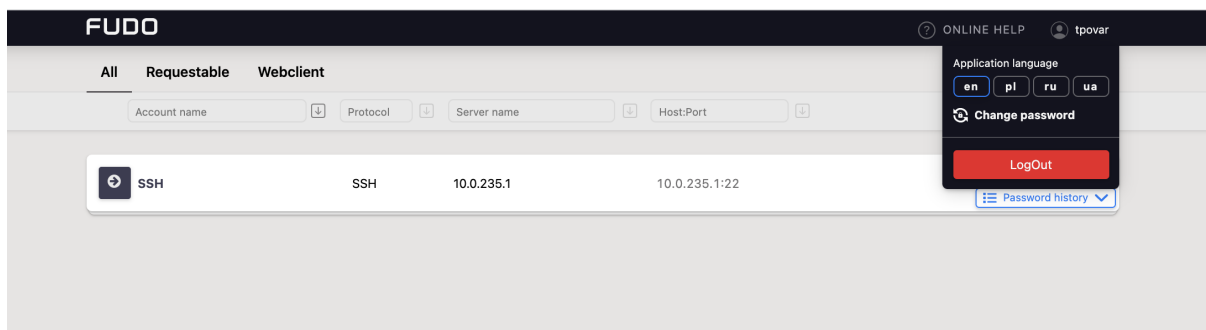
3. Follow the displayed messages and provide a new password. Once done, click *Save.*

Troubleshooting

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:** • Contact your system administrator to make sure you have access to required safes.
	Symptoms: • 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.