



Fudo PAM 5.1 - Access Gateway Manual

Fudo Security

08.06.2022

1	About documentation	1
2	System overview	2
3	Logging into the Access Gateway	4
4	Secret Checkout and Checkin	6
4.1	Secret Checkout	6
4.2	Secret Checkin	7
5	Displaying passwords history	9
6	Displaying and editing accounts notes	11
7	Establishing connections	13
7.1	Connecting via the access request	13
7.2	Connecting over RDP and SSH in browser	15
7.3	Connecting over RDP on Microsoft Windows 7 and 10	18
7.4	Connecting over RDP on Mac OS X	19
7.5	Connecting over RDP on Ubuntu Linux	22
7.6	Connecting over SSH on Microsoft Windows 7 and 10	23
7.7	Connecting over SSH on Mac OS, Linux	25
8	Change Password	28
9	Troubleshooting	29

About documentation

Conventions and symbols

This section covers conventions used throughout this documentation.

italic

Uster interface elements.

example

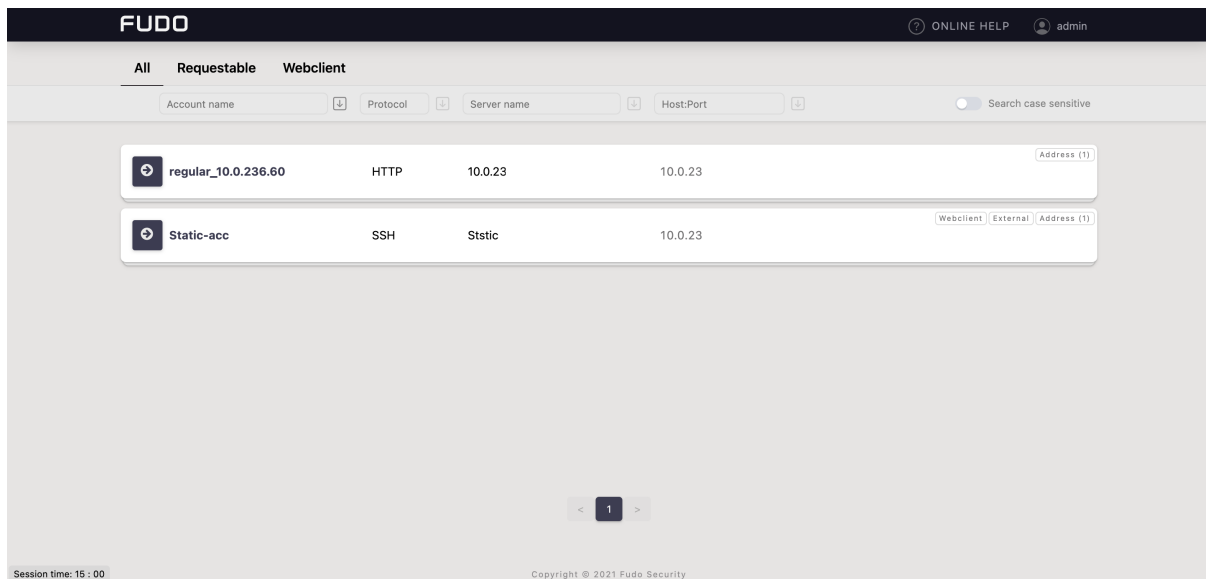
Example value of a parameter, API method name or code example.

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

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

System overview

Access Gateway enables initiating connections with monitored servers available for the logged-in user.



The Access Gateway also allows:

- taking an account password and automatically giving it back after a specified timeout.

Note: More information on this under the *Secret Checkout and Checkin* page.

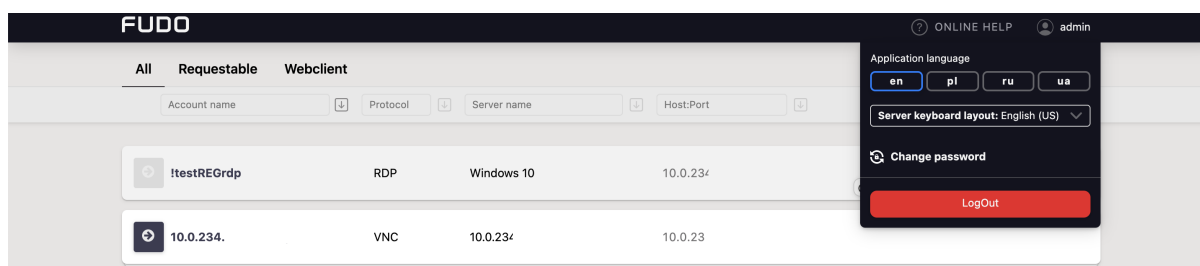
- viewing a password history to selected accounts, managed by FUDO's password vault module.

Note: Check more details at the *Displaying passwords history* page.

- selecting one of the available keyboard layouts:
 - English (US),
 - German,
 - German (Swiss),
 - Norwegian, and
 - Turkish-Q.

Warning: Keyboard layouts are available for connections via RDP protocol in browser only for now.

- setting interface language to English, Polish, Russian, or Ukrainian.



Related topics:

- *Logging into the Access Gateway*
- *Secret Checkout and Checkin*
- *Displaying passwords history*
- *Displaying and editing accounts notes*
- *Establishing connections*
- *Change Password*
- *Troubleshooting*

Logging into the Access Gateway

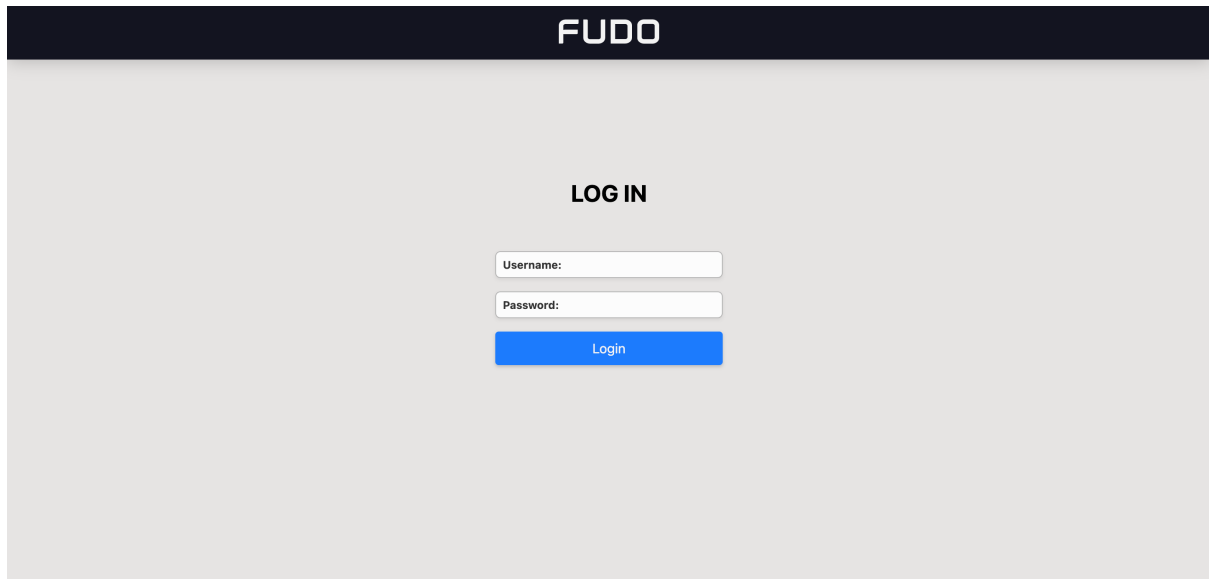
Note:

- Access Gateway 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.
 - *Access Gateway* supports Single Sign On for Active Directory accounts. Refer to system documentation for information on how to enable the SSO in Access Gateway.
-

1. Open web browser and direct it to the IP address of the Access Gateway.
-

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*

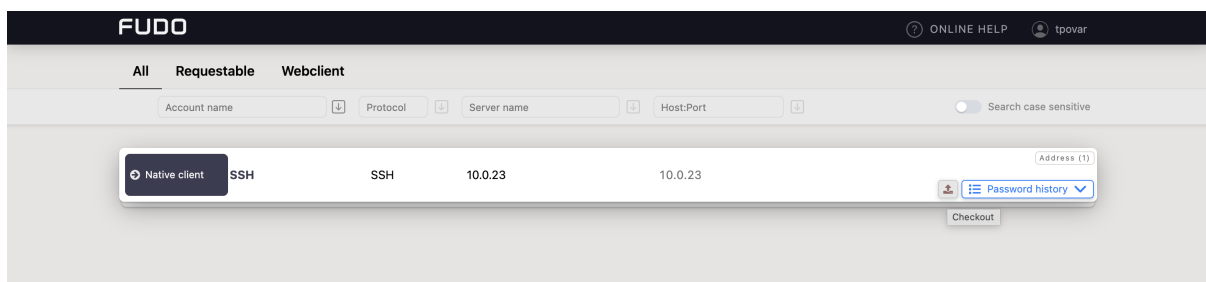
Secret Checkout and Checkin

An account secret can be temporarily taken by the authorized user and given back after their work is done. The user takes the password by sending a request for the secret *checkout*. Then, the secret is given back by the user's manual *checkin* or if the administrator set the duration for the user, the secret is returned automatically after that time is over.

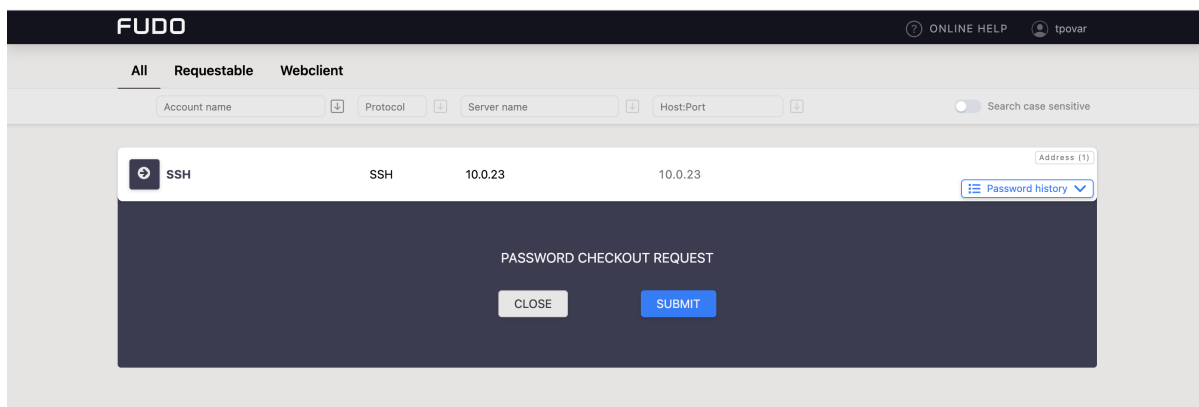
4.1 Secret Checkout

Follow the steps to *checkout* the account secret:

1. Find an account whose password you want to take, hover mouse on it to display more options.
2. Click the  icon.



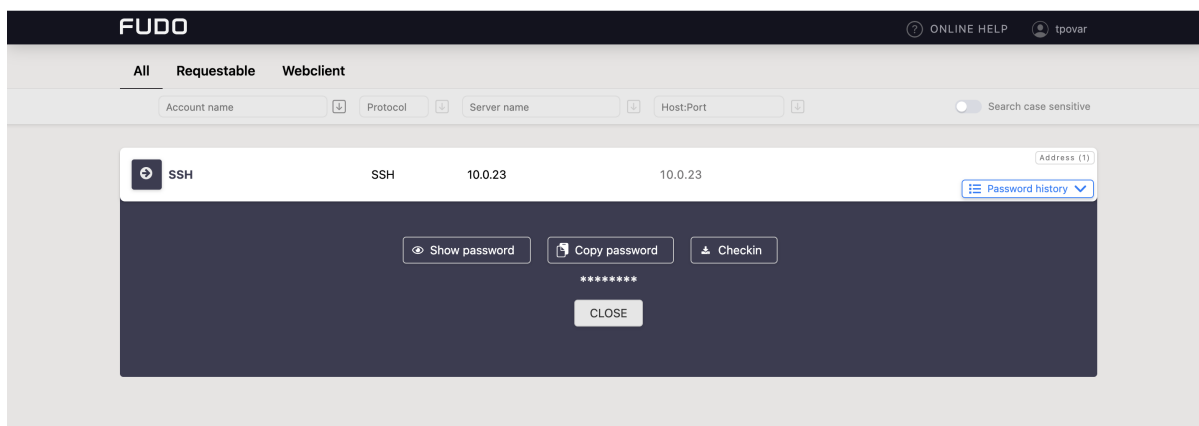
3. Click *SUBMIT*.

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





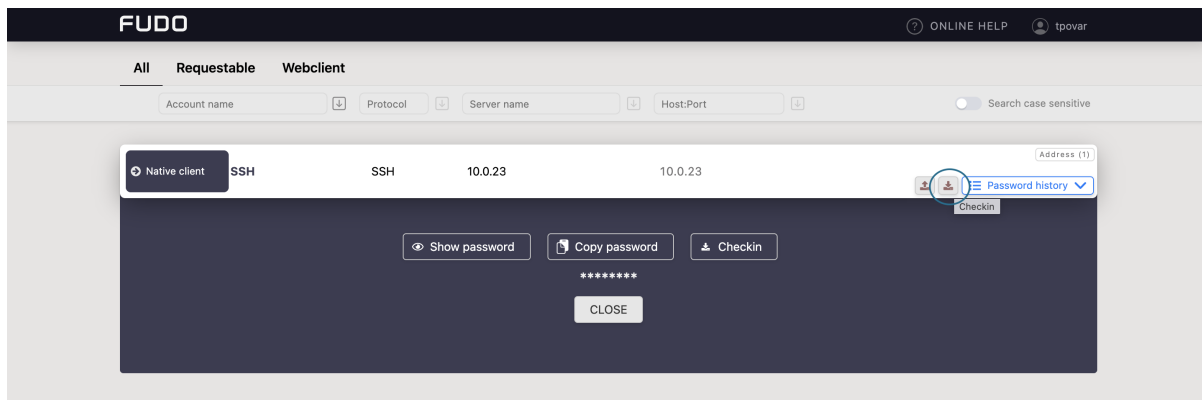
4.2 Secret Checkin

Follow the steps to *checkin* the account secret:

1. Find an account whose password you want to give back, hover mouse on it to display more options.
2. Click the  icon.

or

click the  icon to open the Checkout modal window and click  Checkin.



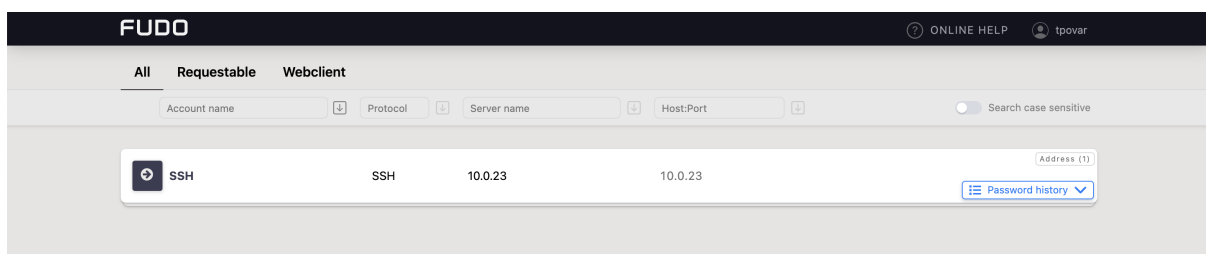
Related topics:

- *Displaying passwords history*

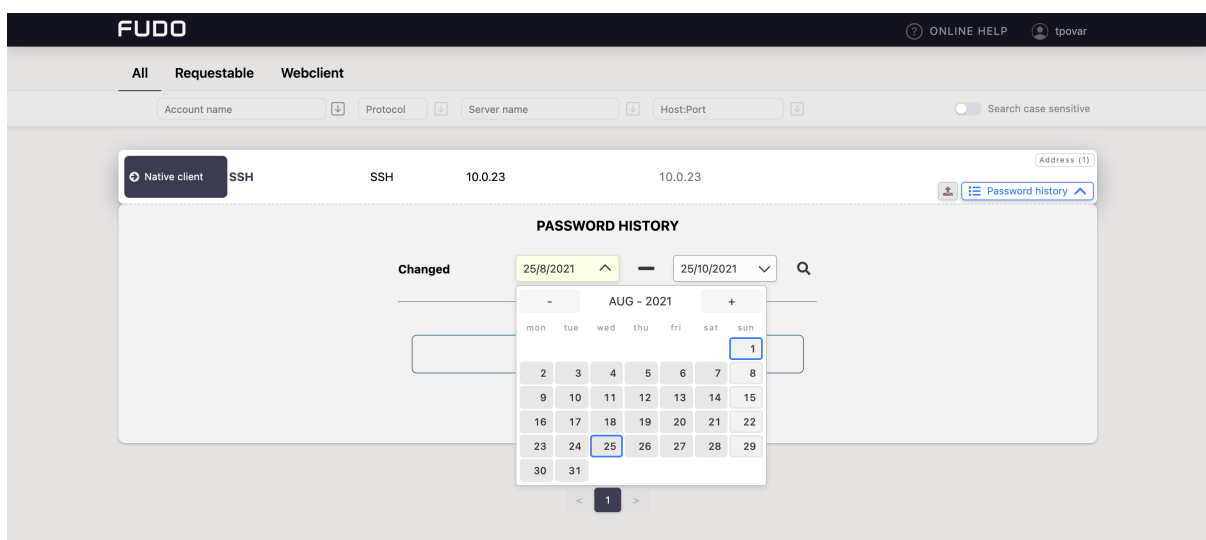
Displaying passwords history


Account password may be changed manually by the user, or automatically by the Fudo PAM system, based on the given settings and with given frequency. It is possible to see how and when the password was changed. Follow the steps to do so:

1. Find account which passwords history you want to view.
2. Click *Password history* drop-down list.



3. Choose the timeline when the password had been changed.



4. Click  to view selected password.

Related topics:

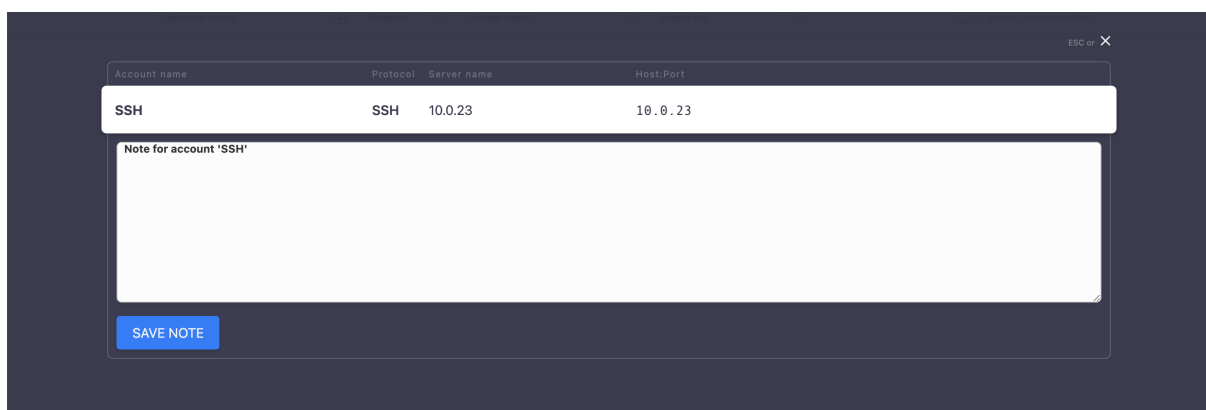
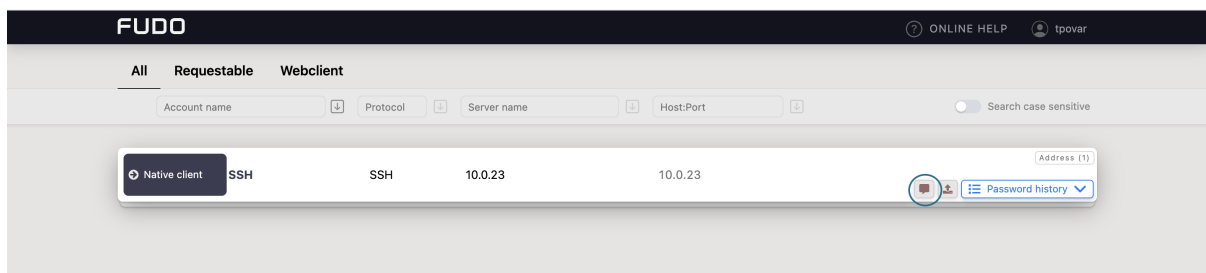
- *Change Password*

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.

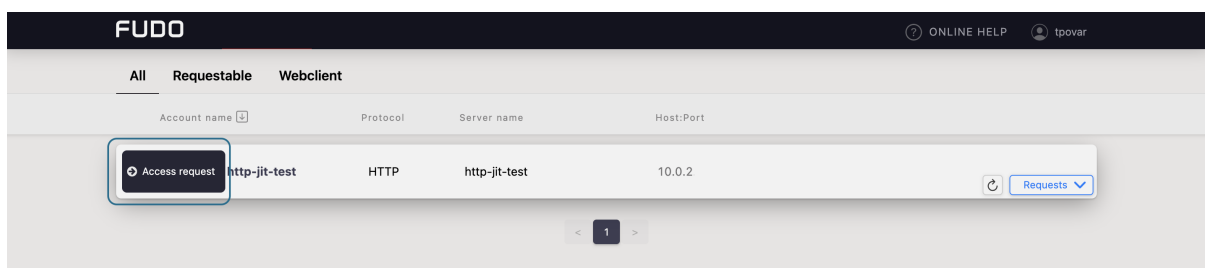
7.1 Connecting via the access request

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

7.1.1 Sending access request

In order to send a request, hover your mouse over the particular account to see more options. Next, follow the steps:

1. Click the *Access request* button.



2. Choose a type of the request: **immediate** or **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.

The screenshot shows the Fudo PAM 5.1 interface for configuring a request. At the top, there are tabs for 'All', 'Requestable', and 'Webclient'. Below this is a table with columns for 'Account name', 'Protocol', 'Server name', and 'Server host'. The table contains one row with the following data: 'jit-test', 'HTTP', 'jit-test-http', and '10.0.2'. Below the table, there is a 'REQUEST TYPE:' section with two buttons: 'Immediate' (which is selected) and 'Scheduled'. A message states: 'Access to the resources will be granted immediately after the operator's consent. You will be informed about this [e-mail, slack, push notification].'. Below this is a 'TIME:' section with a slider ranging from 0h to 24h, with a marker set at 2h. There is a 'REASON (REQUIRED):' text area. At the bottom right, there is a blue 'SEND REQUEST' button.

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.

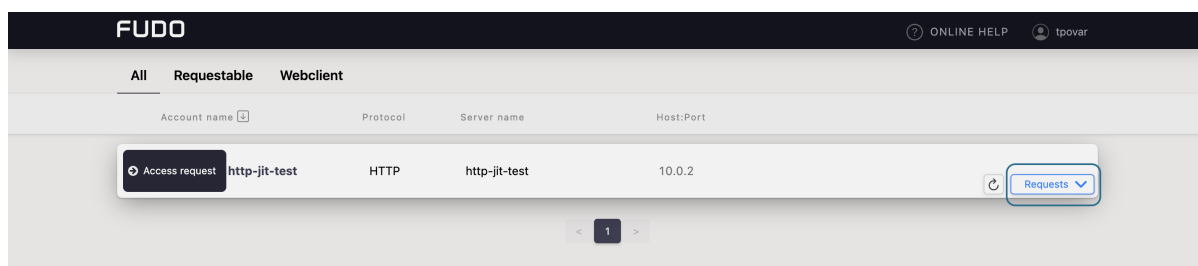
The screenshot shows the Fudo PAM 5.1 interface for configuring a request. At the top, there are tabs for 'All', 'Requestable', and 'Webclient'. Below this is a table with columns for 'Account name', 'Protocol', 'Server name', and 'Server host'. The table contains one row with the following data: 'jit-test', 'HTTP', 'jit-test-http', and '10.0.2'. Below the table, there is a 'REQUEST TYPE:' section with two buttons: 'Immediate' and 'Scheduled' (which is selected). A message states: 'Access to the resources will be granted temporary after the operator's consent. You will be informed about this [e-mail, slack, push notification].'. Below this is a 'DATE RANGE:' section with two dropdown menus: 'Start date: 13/4/2021' and 'End date: 13/5/2021'. There is a 'REASON (REQUIRED):' text area. At the bottom right, there is a blue 'SEND REQUEST' button.

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

3. Define the request time.
4. Click to send the request.

7.1.2 Watching request status

Status of the pending requests, as well as the requests history, are available under the *Requests* drop-down list having a mouse over the account.



Here you can observe the process of voting, including seeing a number of required votes and how much voices is left for access to be granted.

Time	Value	Status	Reason	Votes
Fr, July 30th 2021, 10:26	2h	EXPIRED	Test2	0/1
Fr, July 30th 2021, 10:26	2h	EXPIRED	Test	0/1
Tu, July 13th 2021, 9:13	2h	EXPIRED	Try again	1/2
			granted by admin	We, April 14th 2021, 3:59 ok
Tu, July 13th 2021, 9:13	2h	REJECTED	g	1/1
We, April 14th 2021, 16:55	2h	REVOKED	Try	1/1

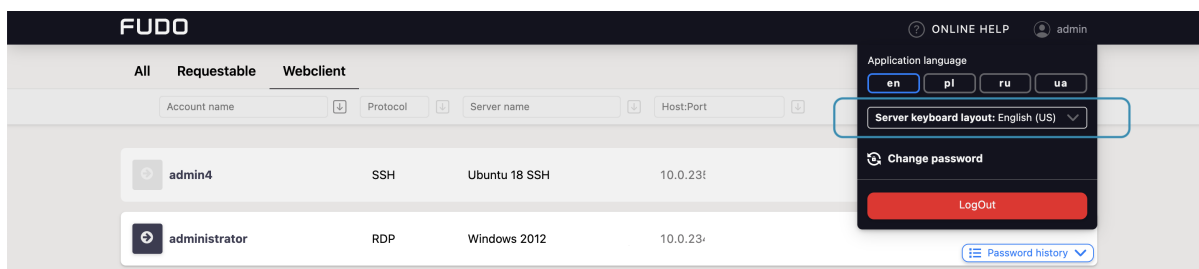
Note: When the access has been already granted, the user can send another request from the requests history bar by selecting the *+ New request* button.

7.2 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.

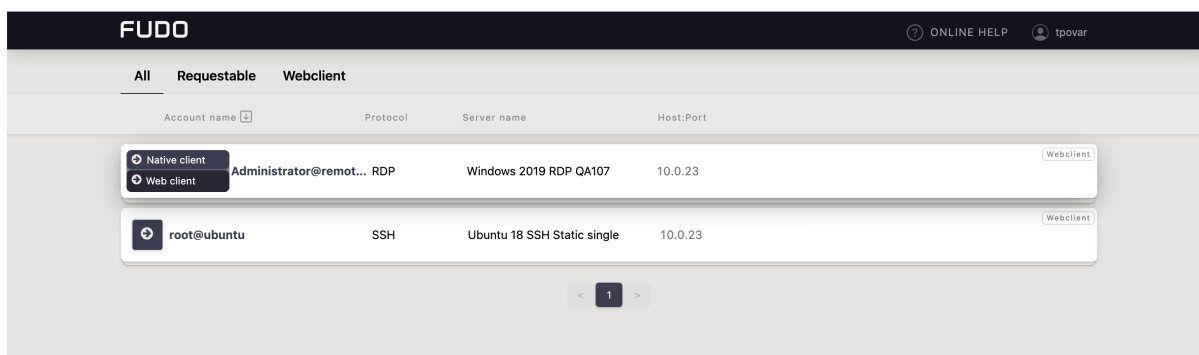
Note: Connecting to the server over **RDP protocol** in browser, select one of the available keyboard layouts:

- *English (US)*,
- *German*,
- *German (Swiss)*,
- *Norwegian*, and
- *Turkish-Q*.



Follow the steps to use the Webclient feature for RDP or SSH connection:

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.

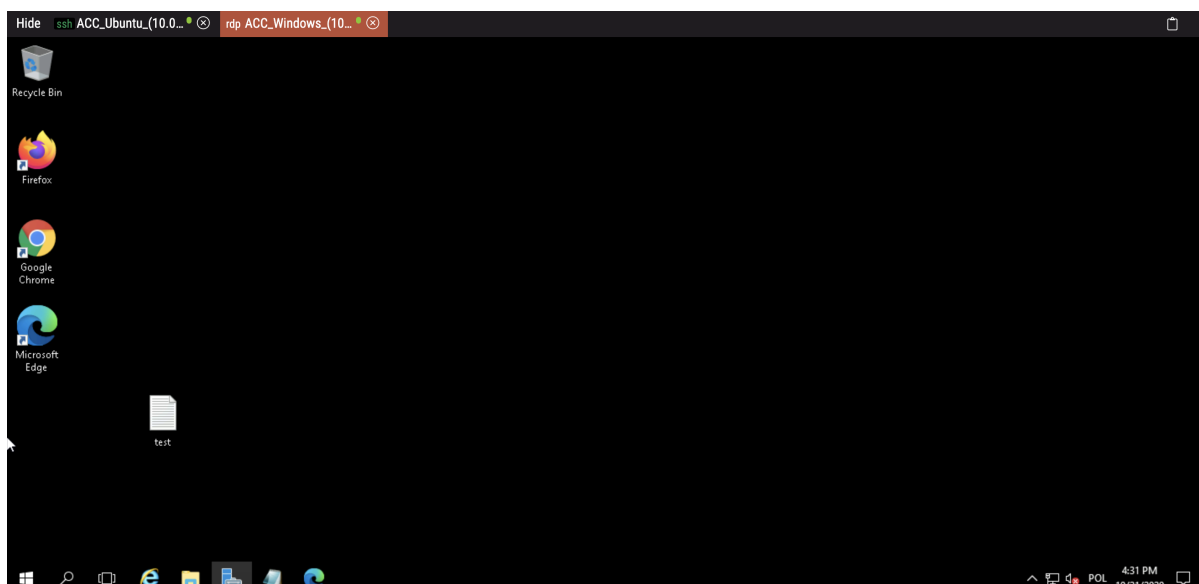


3. If the account has more than one server address configured, choose the one you want to connect to and click *Connect*.

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).

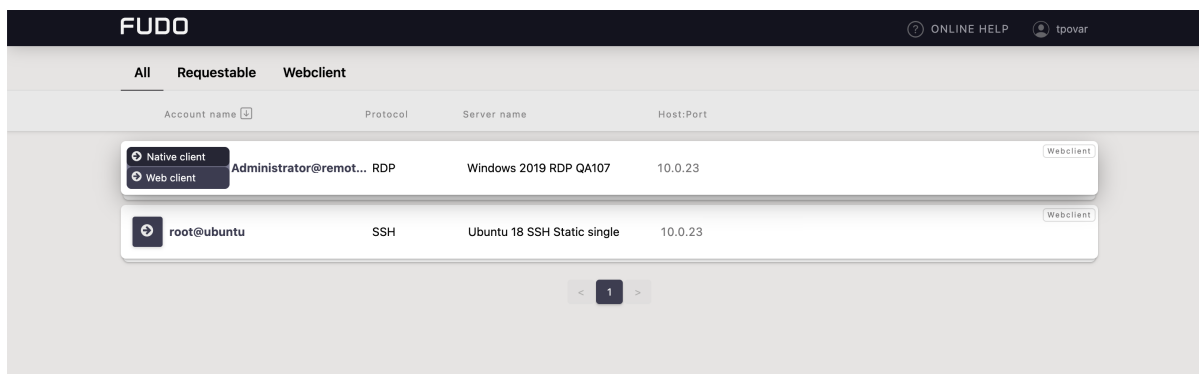
 A screenshot of a terminal window. The title bar shows 'ssh ACC_Ubuntu_(10.0...)' and 'rdp ACC_Windows_(10...'. The terminal output displays system information as of 'Wed 21 Oct 2020 01:43:50 PM UTC'. It lists system load (0.62), usage of / (53.1% of 19.56GB), memory usage (61%), swap usage (23%), processes (232), and users logged in (1). It also lists IPv4 and IPv6 addresses for ens18. A message about MicroK8s high availability clustering is shown, along with a link to 'https://microk8s.io/high-availability'. At the bottom, it indicates that 10 updates can be installed immediately, 0 of which are security updates, and a system restart is required. The prompt is 'admin1@ubuntu-qa:~\$'.

Related topics:

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

7.3 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.



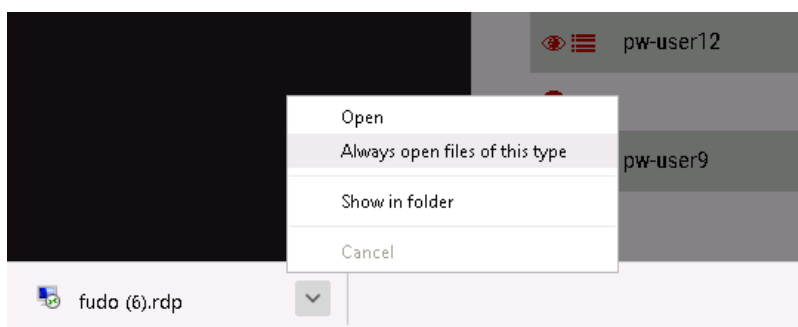
3. Choose the listener, via which you want to connect.



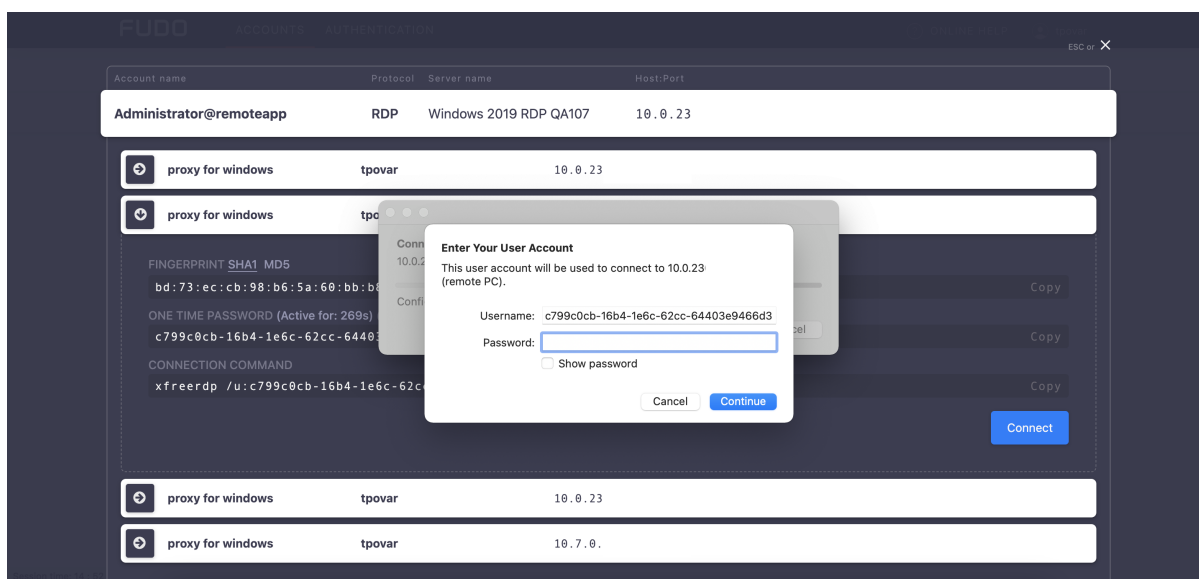
4. Click *Connect*.

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.



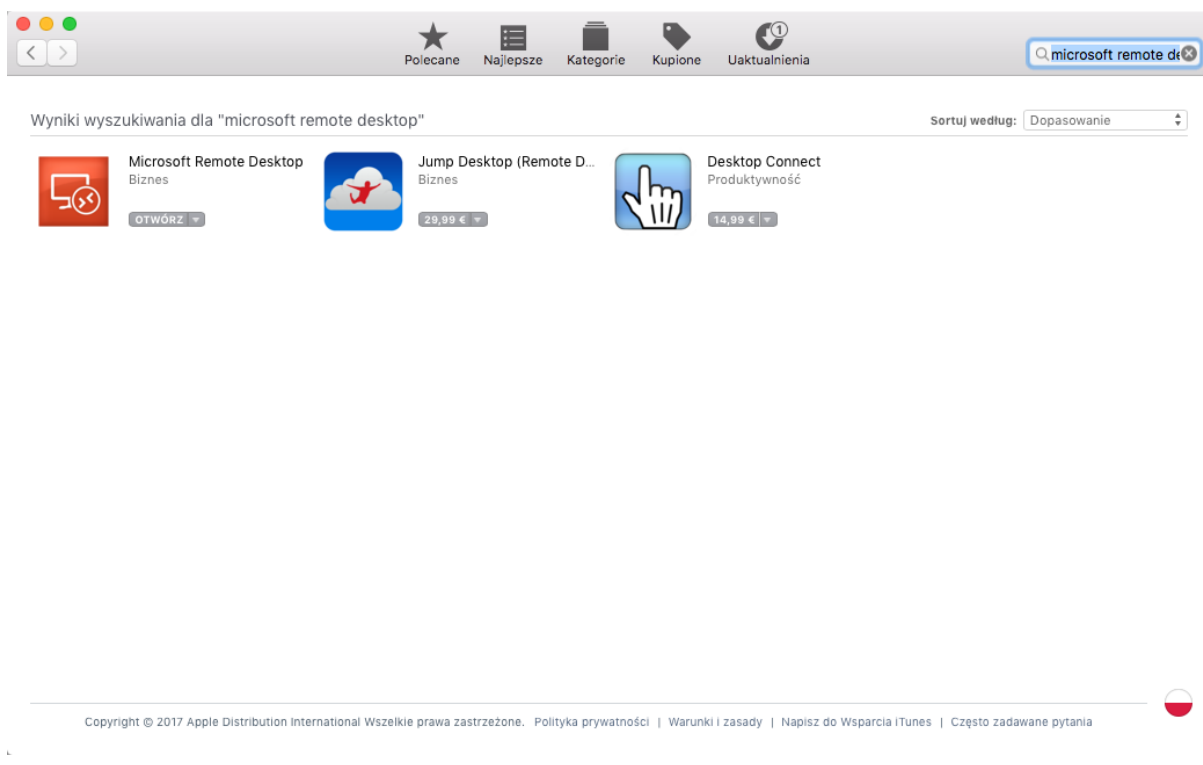
6. Click *Continue* to connect to the server despite the certificate alert.

Related topics:

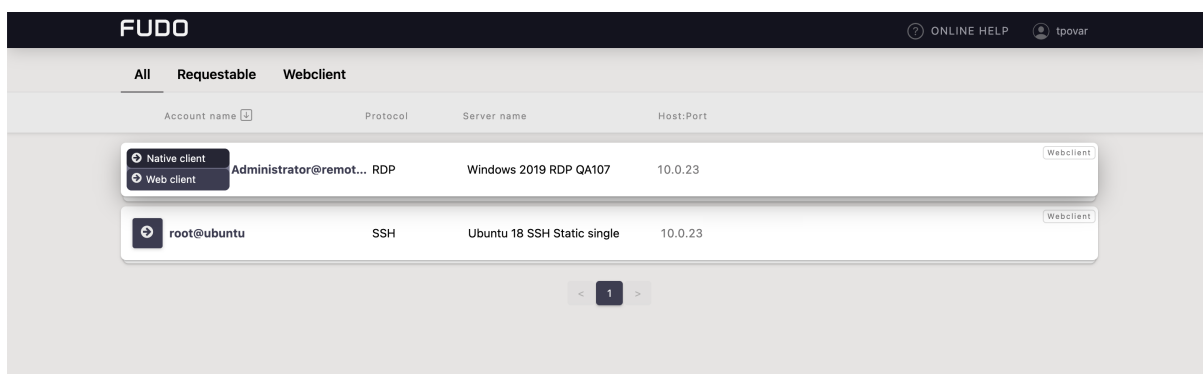
- [Connecting over RDP on Mac OS X](#)
- [Connecting over RDP on Ubuntu Linux](#)

7.4 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.



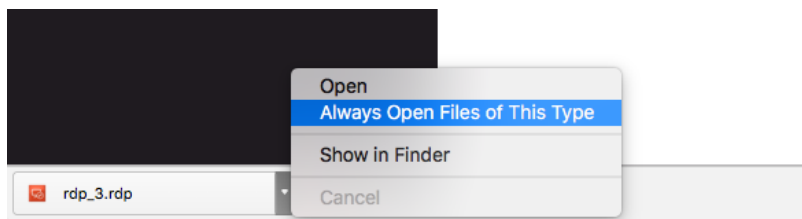
3. Choose the listener, via which you want to connect.



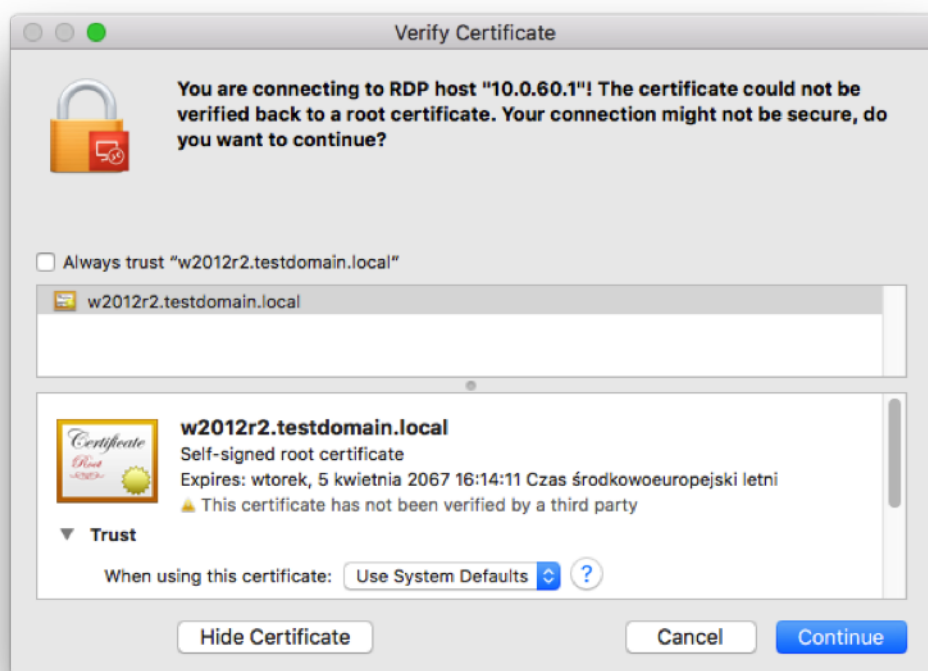
4. Click *Connect*.

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.



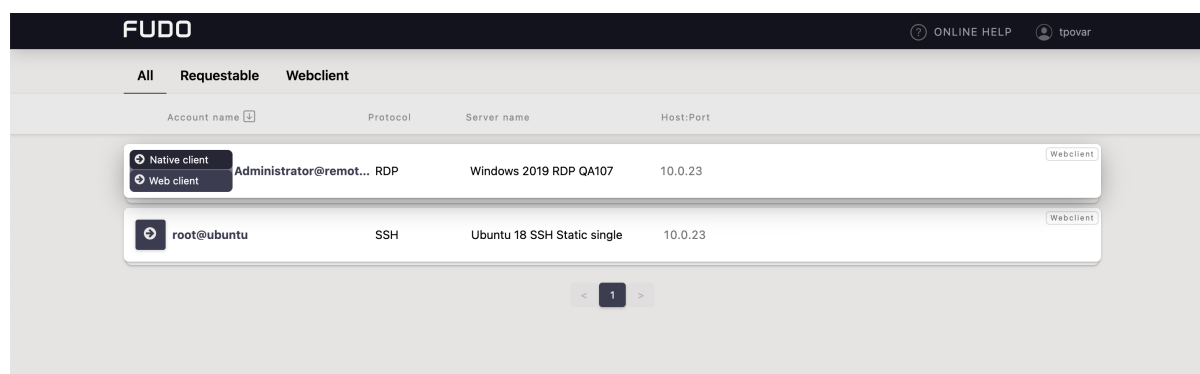
Related topics:

- [Connecting over RDP on Microsoft Windows 7 and 10](#)
- [Connecting over RDP on Ubuntu Linux](#)

7.5 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.



- Choose the listener, via which you want to connect.
- 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*

7.6 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.

- Download and install *WinSCP*.

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

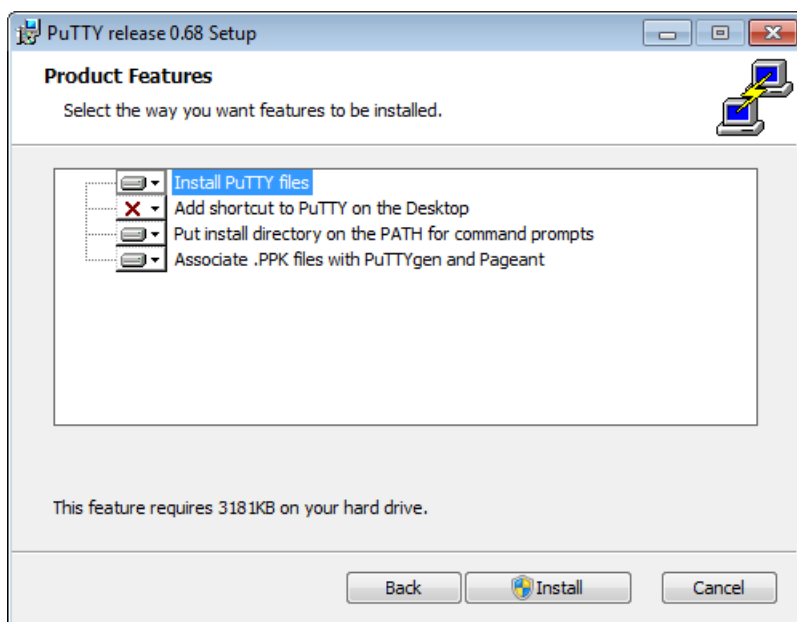
Note: Verify the checksum value to make sure that the integrity of the binary file has not been compromised.

- Download and install *PuTTY*.

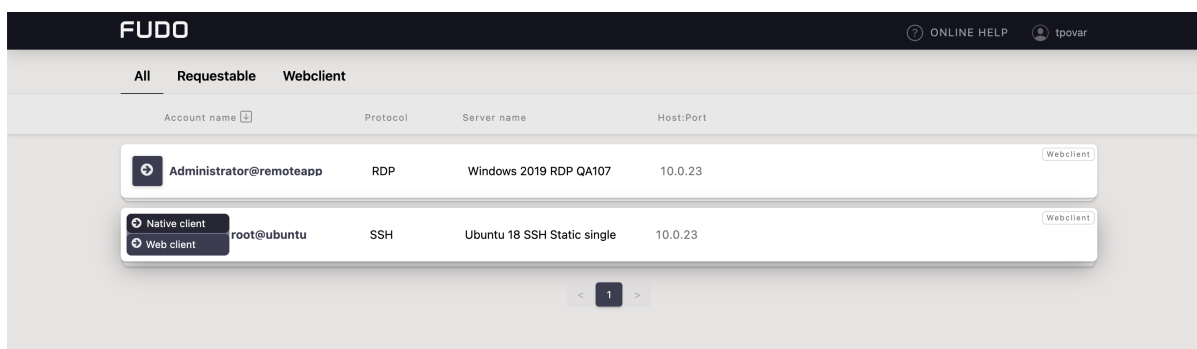
<https://winscp.net/download/putty-0.75-installer.msi>

Note:

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



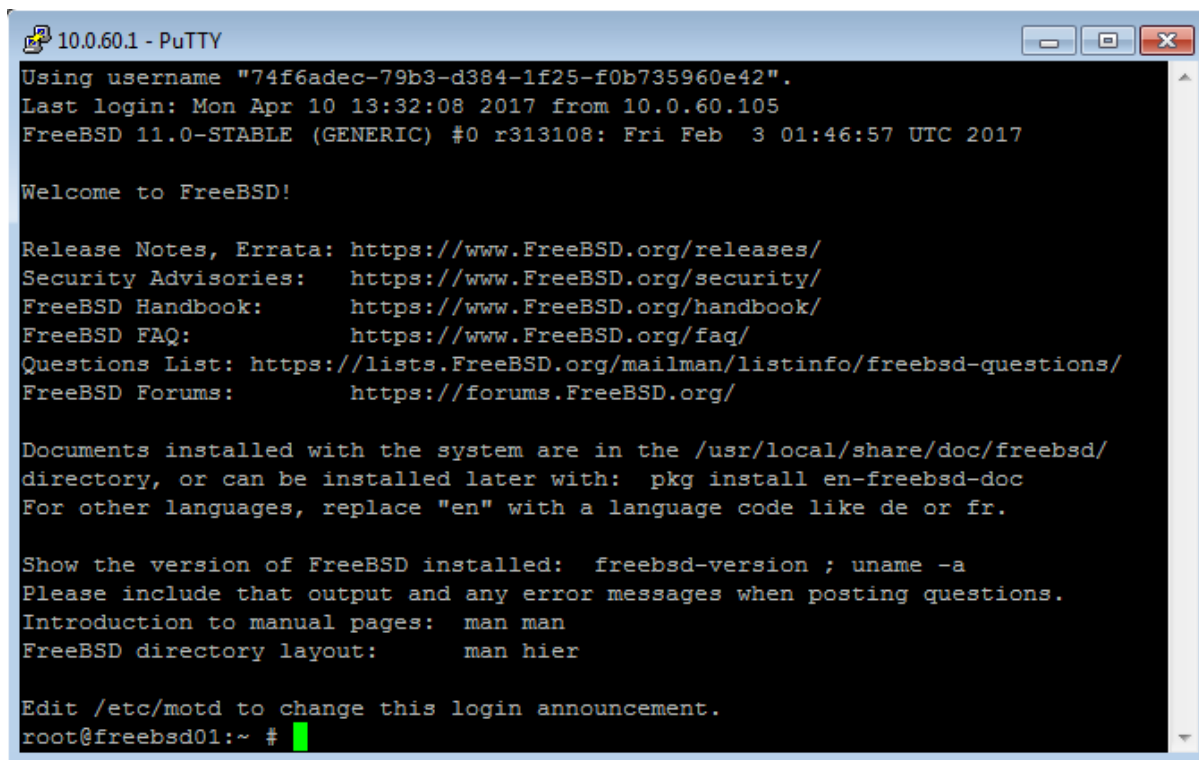
3. Log in to the Access Gateway.
4. Find desired account and server, hover your mouse over to show more options.
5. Select the *Native client* button.



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.



```

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:~ #

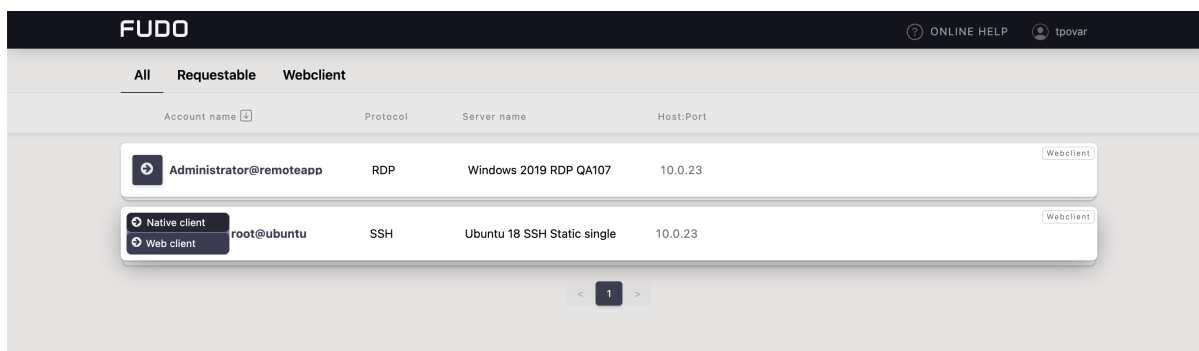
```

Related topics:

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

7.7 Connecting over SSH on Mac OS, Linux

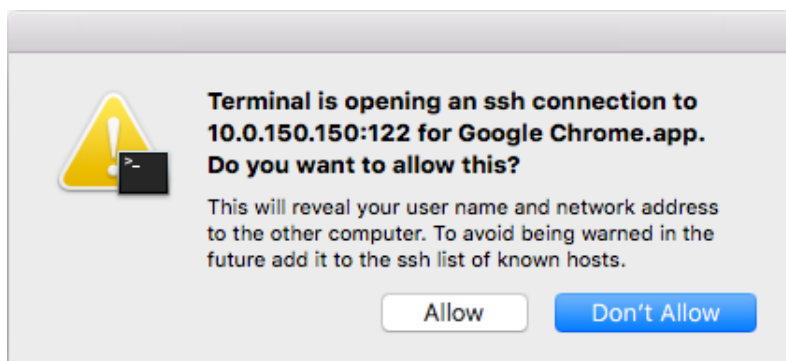
1. Find desired account and server, hover your mouse over to show more options.
2. Select the *Native client* button.



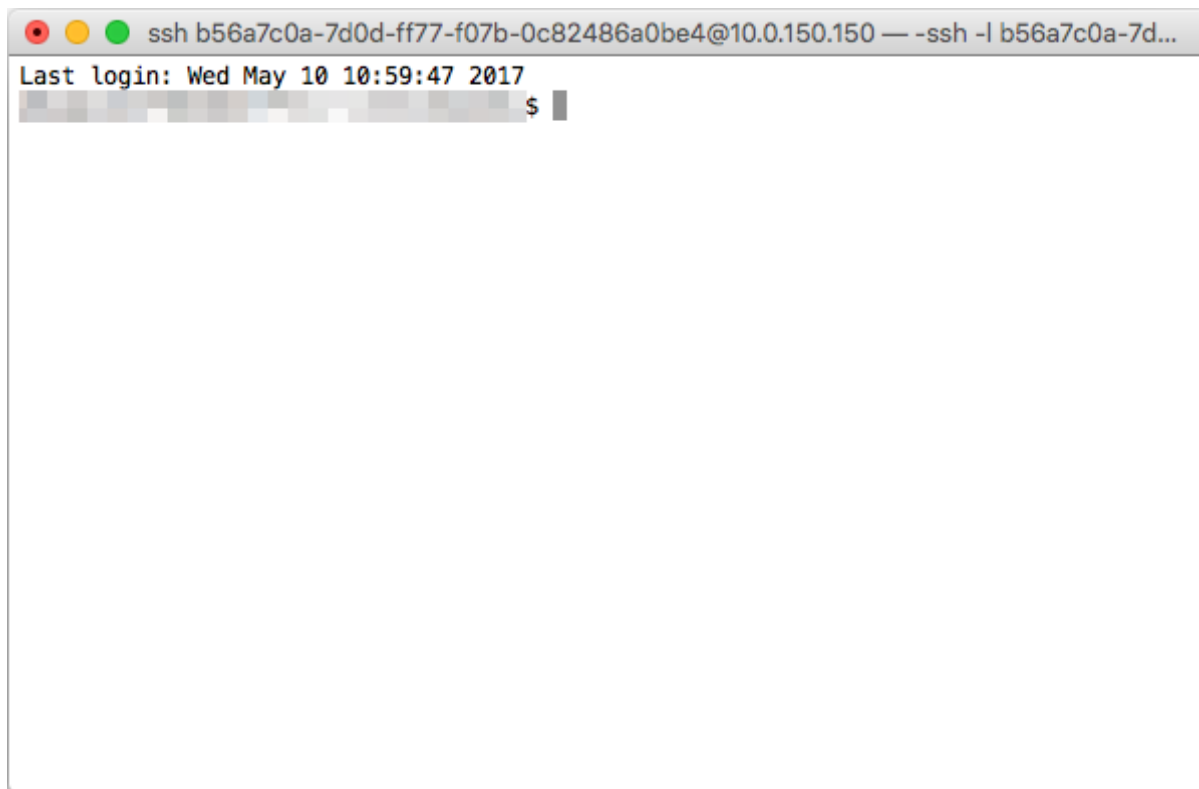
3. Choose the listener, via which you want to connect.



4. Click *Connect*.
5. Click *Allow* to open the Terminal.



6. The connection has been established.

**Related topics:**

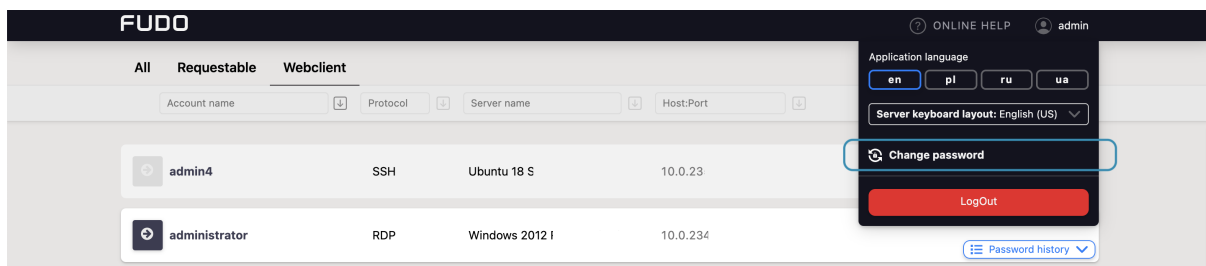
- *Connecting over RDP on Mac OS X*
- *Connecting over RDP on Microsoft Windows 7 and 10*
- *Connecting over RDP on Ubuntu Linux*

Change Password

Fudo PAM Access Gateway 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*.

Related topics:

- *Displaying passwords history*

 Troubleshooting

Problem	Symptoms and solution description
Cannot log in to the Access Gateway	<p>Symptoms:</p> <ul style="list-style-type: none"> • The user cannot log in. <p>Solution:</p> <ul style="list-style-type: none"> • Make sure you are entering correct login credentials. • Contact system administrator to verify whether you have Access Gateway access privileges. • Contact system administrator to verify the Access Gateway time policy settings.
Accounts list is missing objects.	<p>Solution:</p> <ul style="list-style-type: none"> • Contact your system administrator to make sure you have access to required safes. <p>Symptoms:</p> <ul style="list-style-type: none"> • Cannot connect to selected server. <p>Reason: connection takes place outside the timeframe defined by the access time policy.</p> <p>Solution: contact system administrator to verify your time policy settings.</p>