Fudo PAM 5.2 - Access Gateway Manual

Fudo Security

30.05.2022

Contents

CHAPTER 1

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.

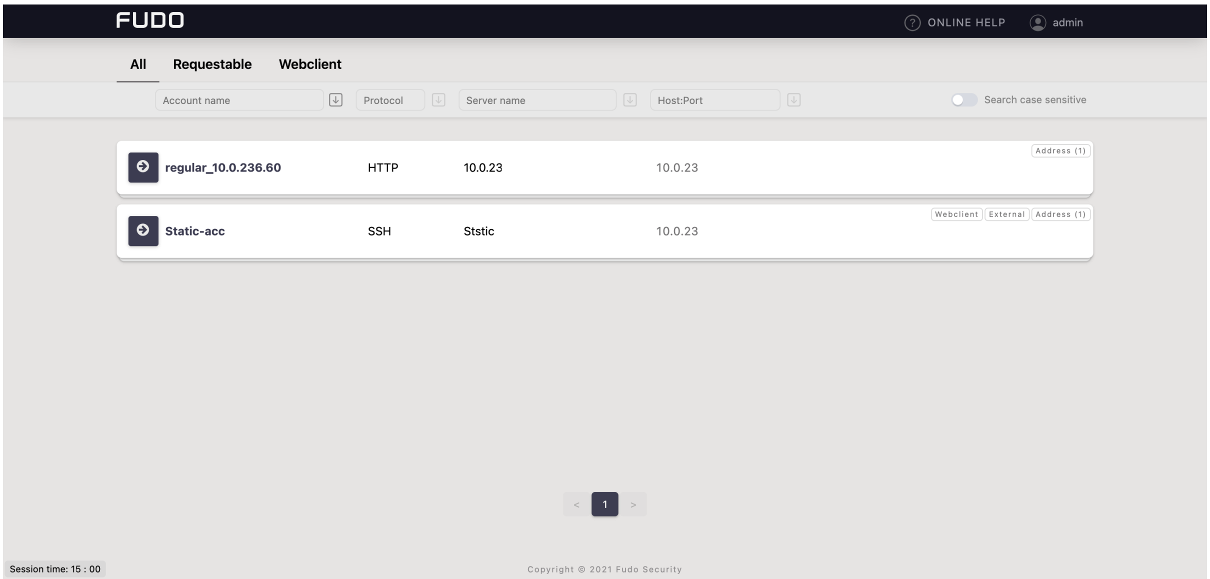
Note: Additional information closely related with described topic, e.g. suggestion concerning given procedure step; additional conditions which have to be met.

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

CHAPTER 2

System overview

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



Account name	Protocol	Server name	Host:Port	
regular_10.0.236.60	HTTP	10.0.23	10.0.23	Address (1)
Static-acc	SSH	Ststic	10.0.23	Webclient External Address (1)

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.

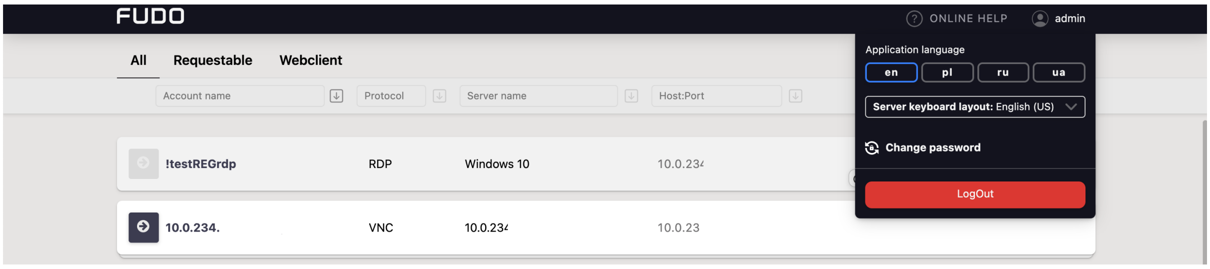
- viewing a password history to selected accounts, managed by FUDO's password vault module.

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.



Server keyboard layout: English (US)

Account name	Protocol	Server name	Host:Port
!testREGrdp	RDP	Windows 10	10.0.234
10.0.234.	VNC	10.0.234	10.0.23

Related topics:

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

CHAPTER 3

Logging into the Access Gateway

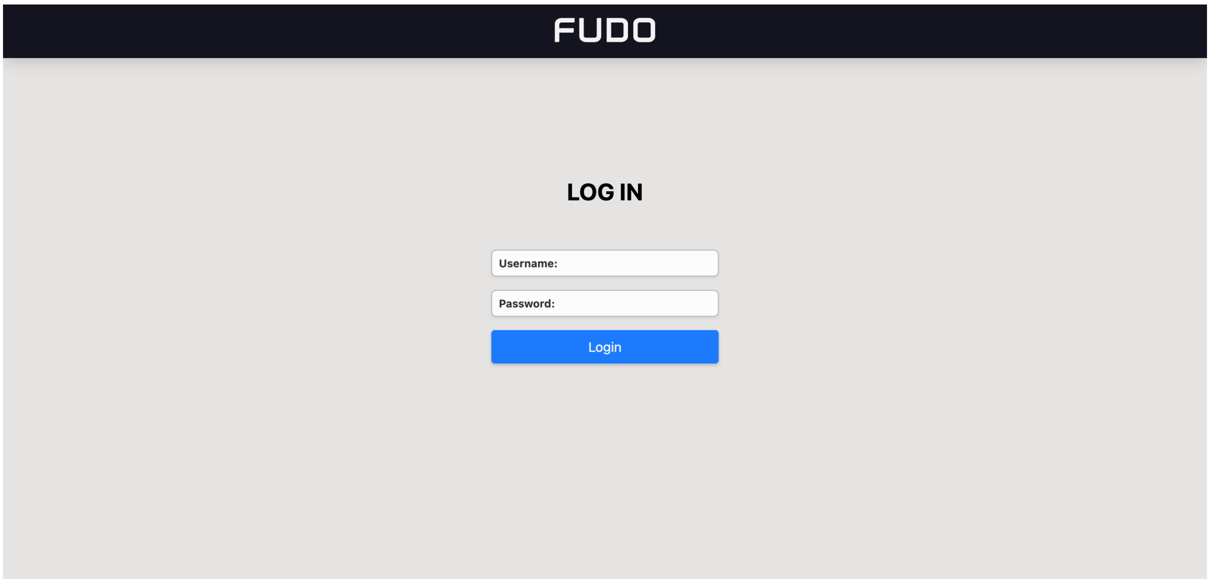
Note:

- 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.
- *Access Gateway* also allows loggin in with Azure or Okta profile. An authorized administrator can set the OpenID Connect globally for the whole system instance.

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*

CHAPTER 4

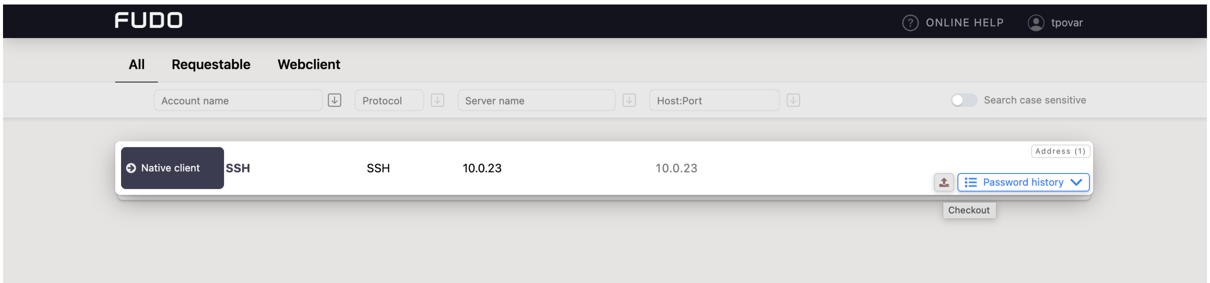
Secret Checkout and Checkin

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.

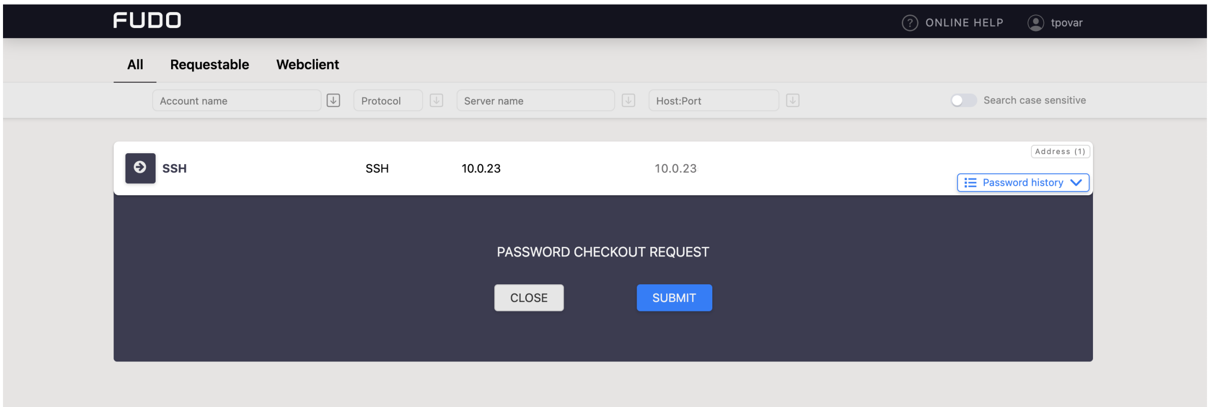
4.1 Secret Checkout

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.



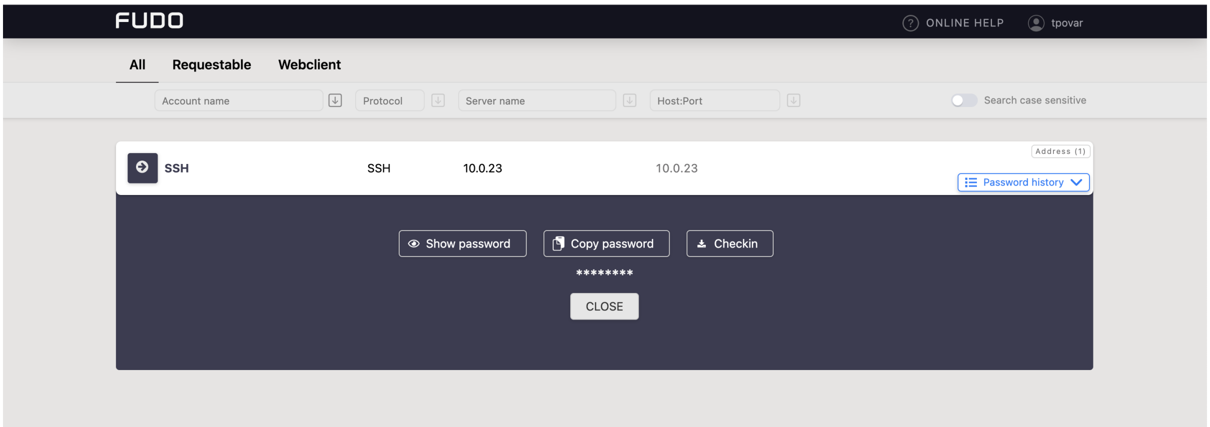
3. Click *SUBMIT*.



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.



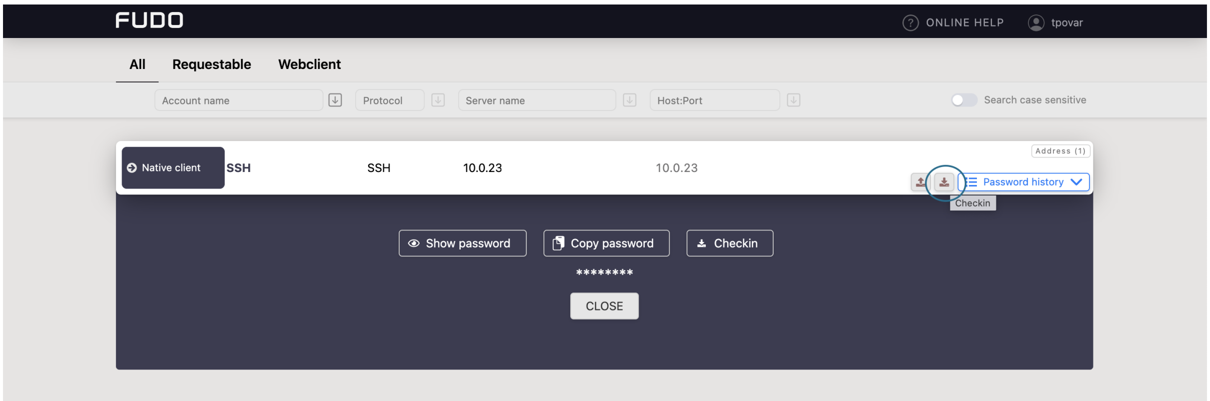
4.2 Secret Checkin

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:

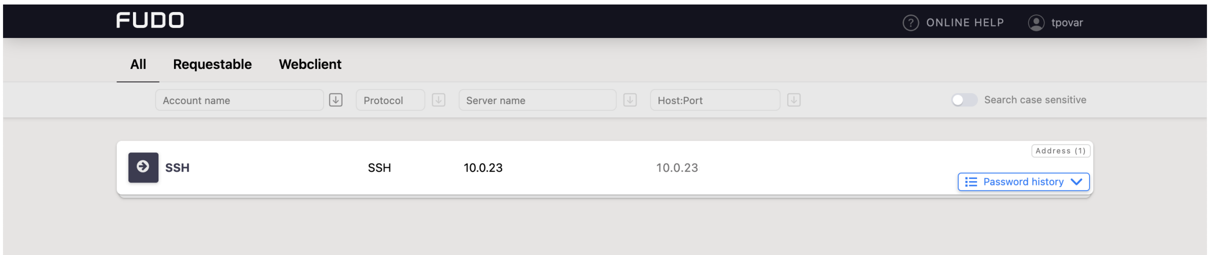
- *Displaying passwords history*

CHAPTER 5

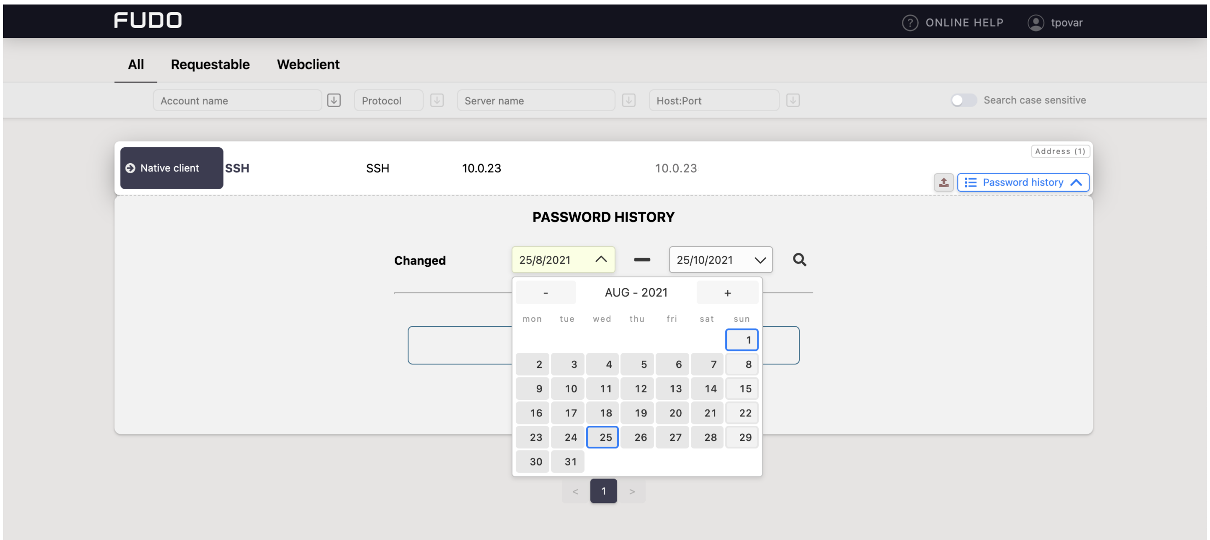
Displaying passwords history

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*

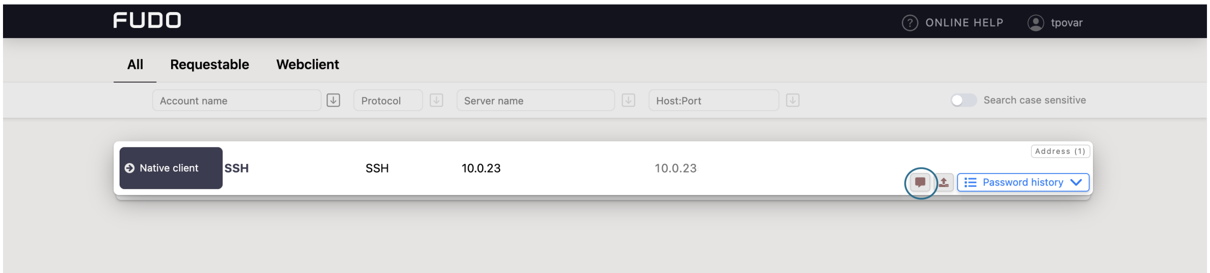
CHAPTER 6

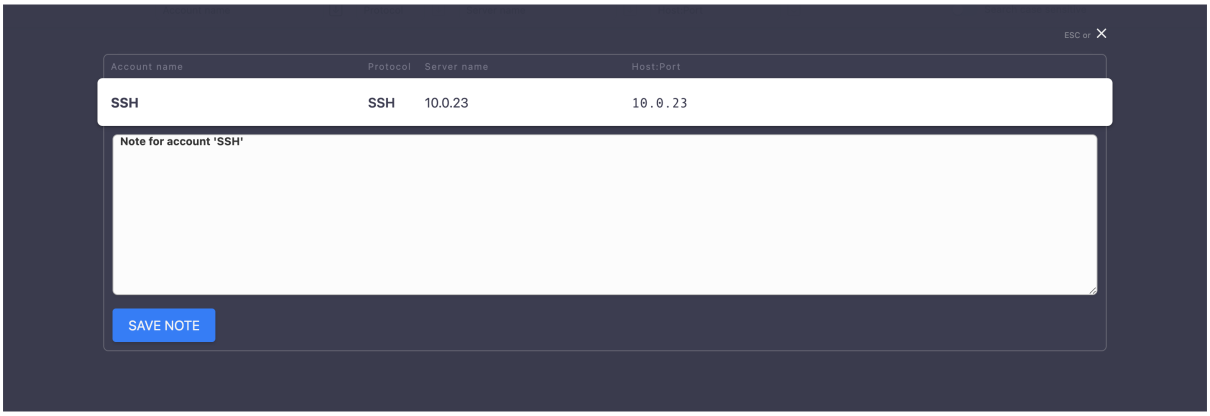
Displaying and editing accounts notes

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.

CHAPTER 7

Establishing connections

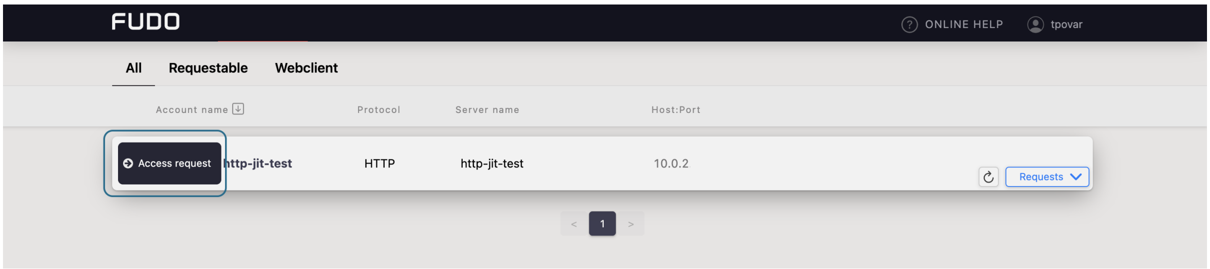
7.1 Connecting via the access request

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:

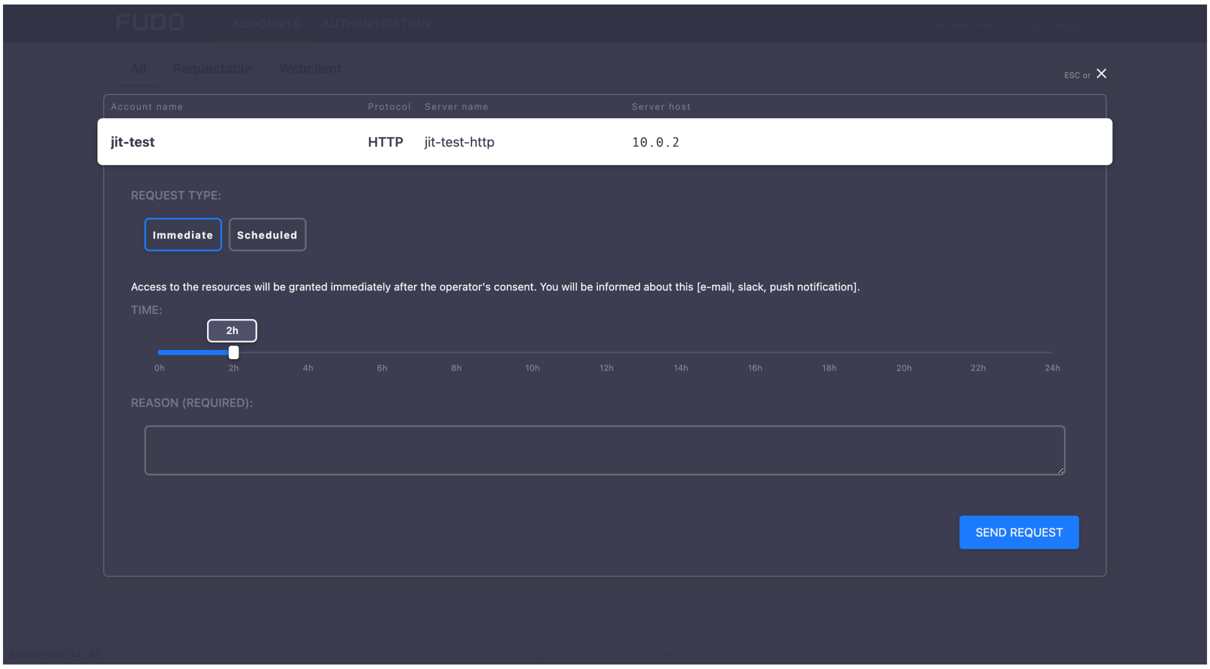
1. Click the *Access request* button.



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.



Account name	Protocol	Server name	Server host
jit-test	HTTP	jit-test-http	10.0.2

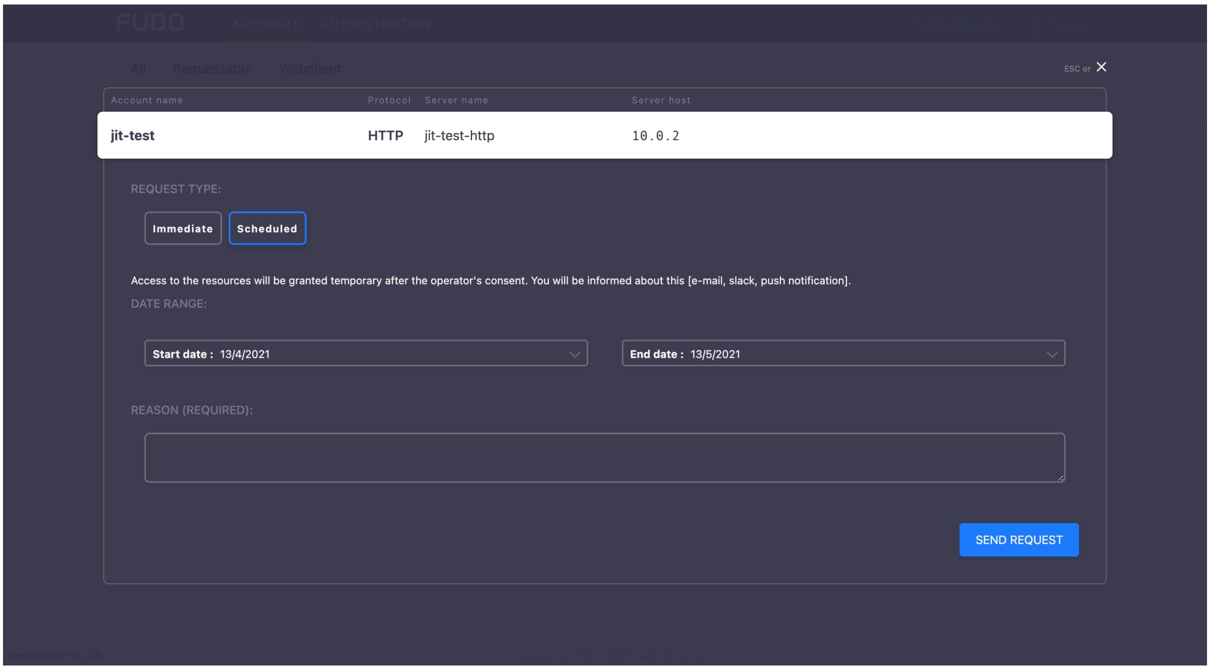
REQUEST TYPE: Immediate (selected)

Access to the resources will be granted immediately after the operator's consent. You will be informed about this [e-mail, slack, push notification].

TIME: 2h

REASON (REQUIRED):

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.



Account name	Protocol	Server name	Server host
jit-test	HTTP	jit-test-http	10.0.2

REQUEST TYPE: Scheduled (selected)

Access to the resources will be granted temporary after the operator's consent. You will be informed about this [e-mail, slack, push notification].

DATE RANGE:

Start date : 13/4/2021

End date : 13/5/2021

REASON (REQUIRED):

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

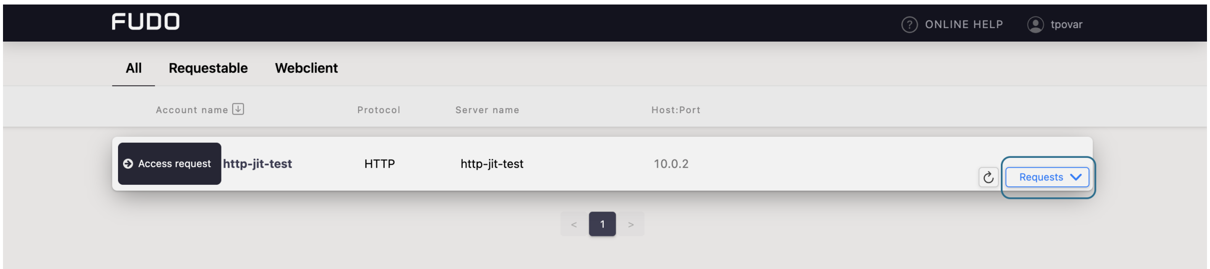
3. Define the request time.
4. Click to send the request.

7.1.2 Watching request status

You can receive 2 types of e-mail notifications about your request:

- `Access Request accepted` - the request was approved by the required amount of the administrators.
- `Access Request rejected` - the request was denied.

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



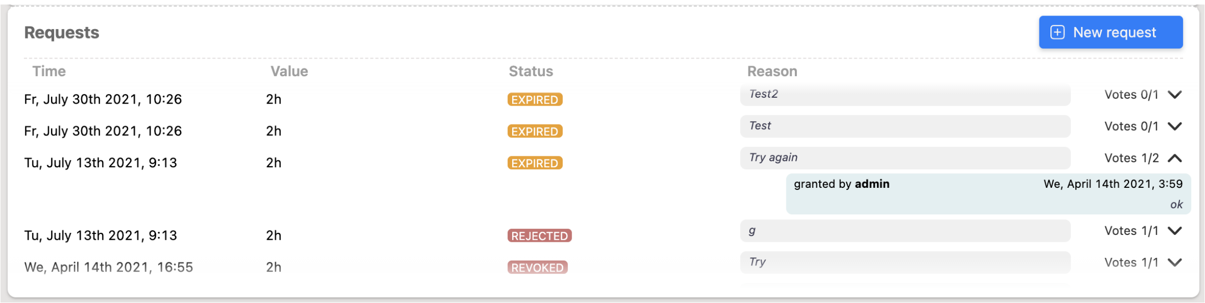
FUDO ONLINE HELP tpovar

All Requestable Webclient

	Account name	Protocol	Server name	Host:Port	
Access request	http-jit-test	HTTP	http-jit-test	10.0.2	Requests

< 1 >

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.



Requests | New request

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

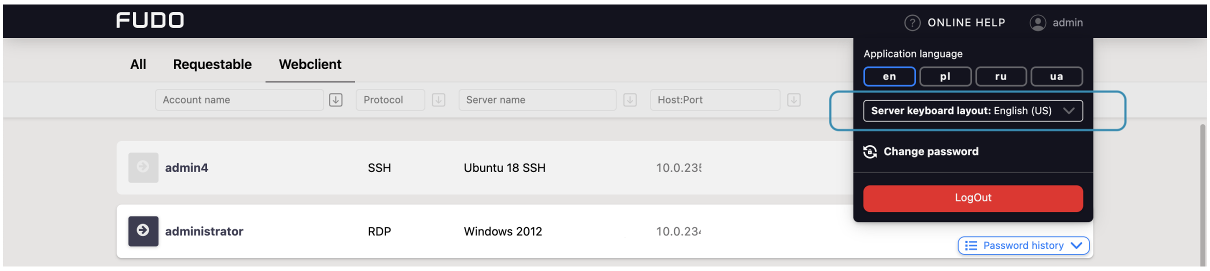
Note: When the access has been already granted, the user can send another request from the requests history bar by selecting the + *New request* button.

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*.



FUDO

ONLINE HELP admin

All Requestable Webclient

Account name	Protocol	Server name	Host:Port
admin4	SSH	Ubuntu 18 SSH	10.0.23
administrator	RDP	Windows 2012	10.0.23

Application language

en pl ru ua

Server keyboard layout: English (US)

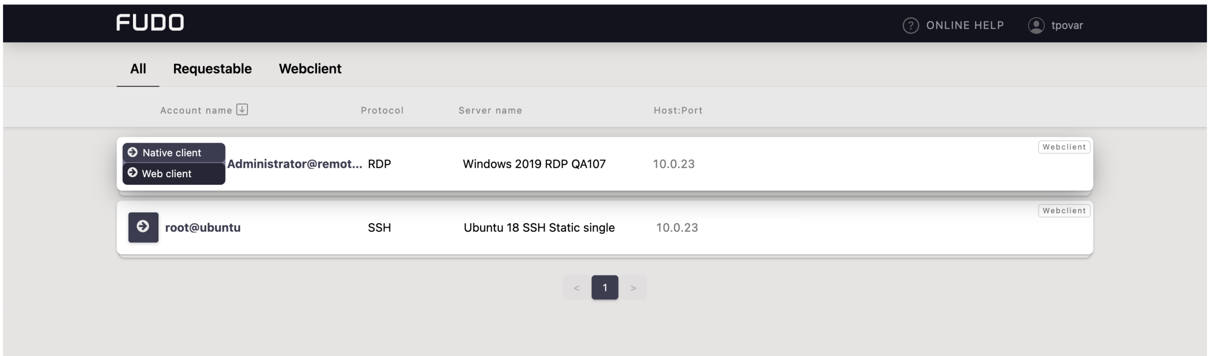
Change password

LogOut

Password history

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.



FUDO

ONLINE HELP tpovar

All Requestable Webclient

Account name	Protocol	Server name	Host:Port	
Native client Web client Administrator@remot...	RDP	Windows 2019 RDP QA107	10.0.23	Webclient
root@ubuntu	SSH	Ubuntu 18 SSH Static single	10.0.23	Webclient

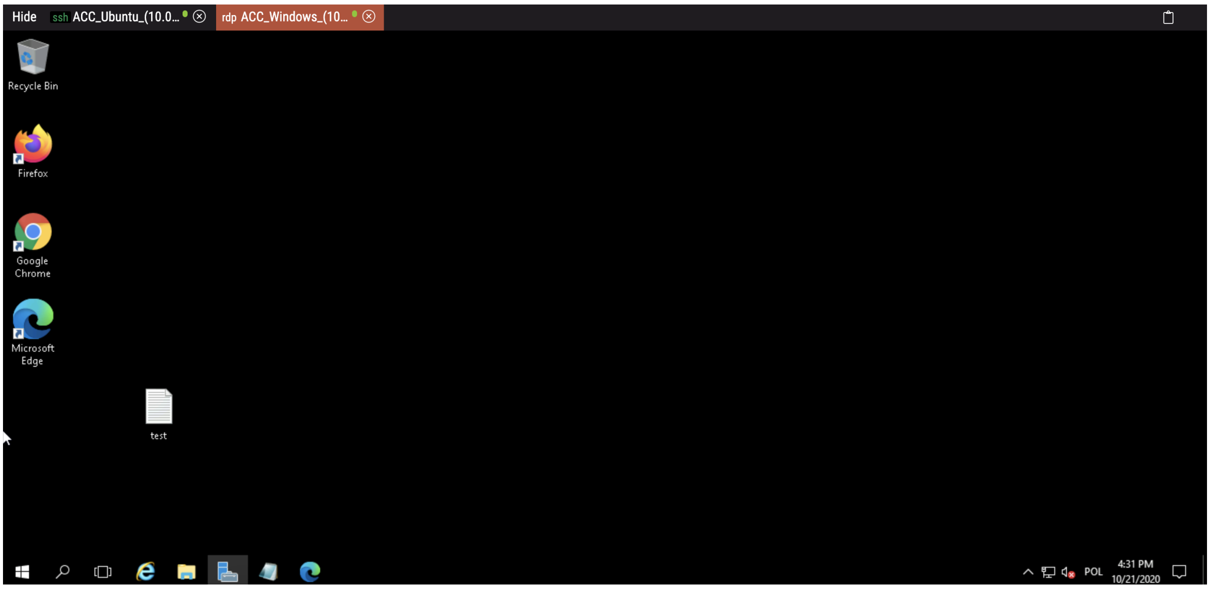
< 1 >

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:

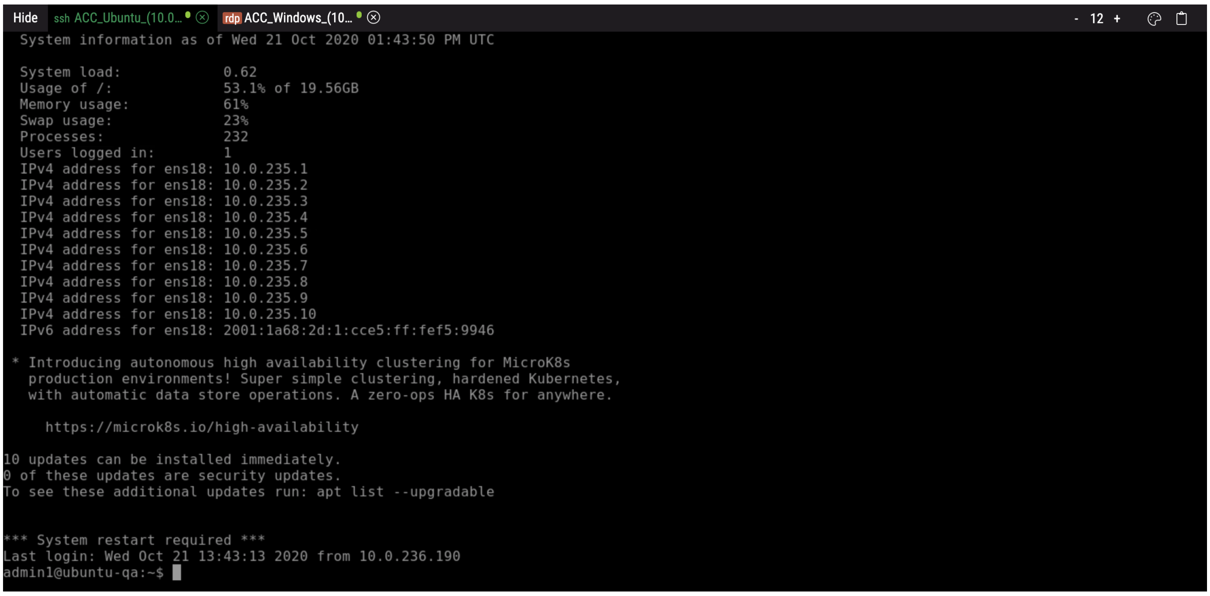
- *Hide* / *Show* button that minimizes / maximizes the connection window.
- a tab displays a protocol type, the listener name and the connection state:
  - 🟡 connection is establishing.
  - 🟢 session is connected.
  - 🔴 session is disconnected.
- *clipboard* feature allows copying a text fragment for 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).



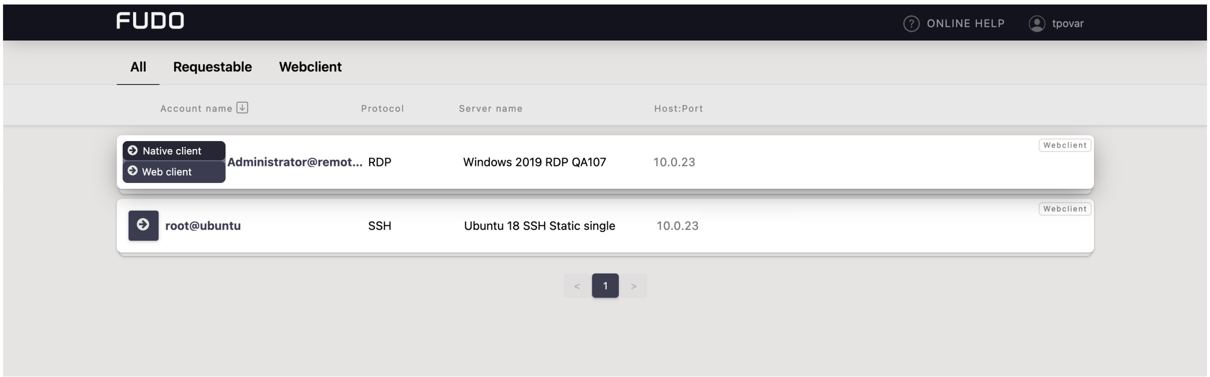
```
  System information as of Wed 21 Oct 2020 01:43:50 PM UTC

  System load:            0.62
  Usage of /:             53.1% of 19.56GB
  Memory usage:           61%
  Swap usage:             23%
  Processes:              232
  Users logged in:        1
  IPv4 address for ens18: 10.0.235.1
  IPv4 address for ens18: 10.0.235.2
  IPv4 address for ens18: 10.0.235.3
  IPv4 address for ens18: 10.0.235.4
  IPv4 address for ens18: 10.0.235.5
  IPv4 address for ens18: 10.0.235.6
  IPv4 address for ens18: 10.0.235.7
  IPv4 address for ens18: 10.0.235.8
  IPv4 address for ens18: 10.0.235.9
  IPv4 address for ens18: 10.0.235.10
  IPv6 address for ens18: 2001:1a68:2d:1:cce5:ff:fef5:9946

 * Introducing autonomous high availability clustering for MicroK8s
   production environments! Super simple clustering, hardened Kubernetes,
   with automatic data store operations. A zero-ops HA K8s for anywhere.

     https://microk8s.io/high-availability

10 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


*** System restart required ***
Last login: Wed Oct 21 13:43:13 2020 from 10.0.236.190
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*

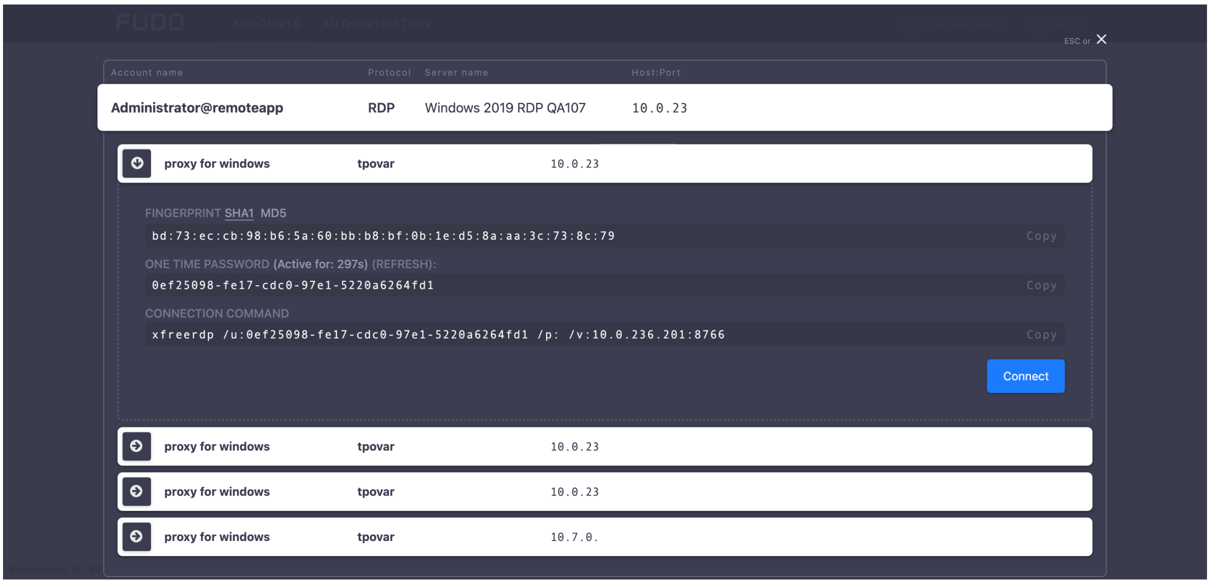
7.3 Connecting over RDP on Microsoft Windows 7 and 10

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



Account name	Protocol	Server name	Host:Port
Administrator@remot...	RDP	Windows 2019 RDP QA107	10.0.23
root@ubuntu	SSH	Ubuntu 18 SSH Static single	10.0.23

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



Account name	Protocol	Server name	Host:Port
Administrator@remoteapp	RDP	Windows 2019 RDP QA107	10.0.23

proxy for windows	tpovar	10.0.23

FINGERPRINT SHA1 MD5

```
bd:73:ec:cb:98:b6:5a:60:bb:b8:bf:0b:1e:d5:8a:aa:3c:73:8c:79
```

ONE TIME PASSWORD (Active for: 297s) (REFRESH):

```
0ef25098-fe17-cdc0-97e1-5220a6264fd1
```

CONNECTION COMMAND

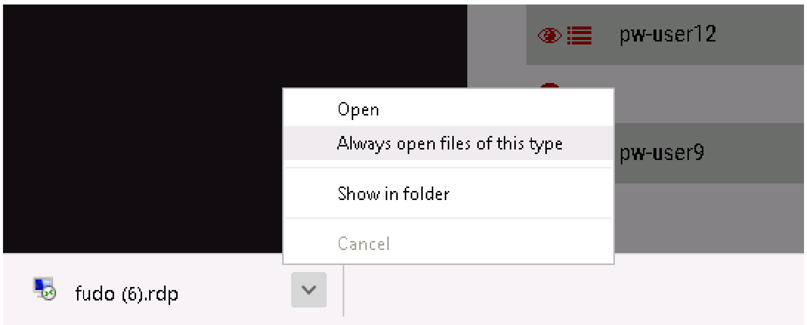
```
xfreerdp /u:0ef25098-fe17-cdc0-97e1-5220a6264fd1 /p: /v:10.0.236.201:8766
```

proxy for windows	tpovar	10.0.23
proxy for windows	tpovar	10.0.23
proxy for windows	tpovar	10.7.0.

4. Click *Connect*.

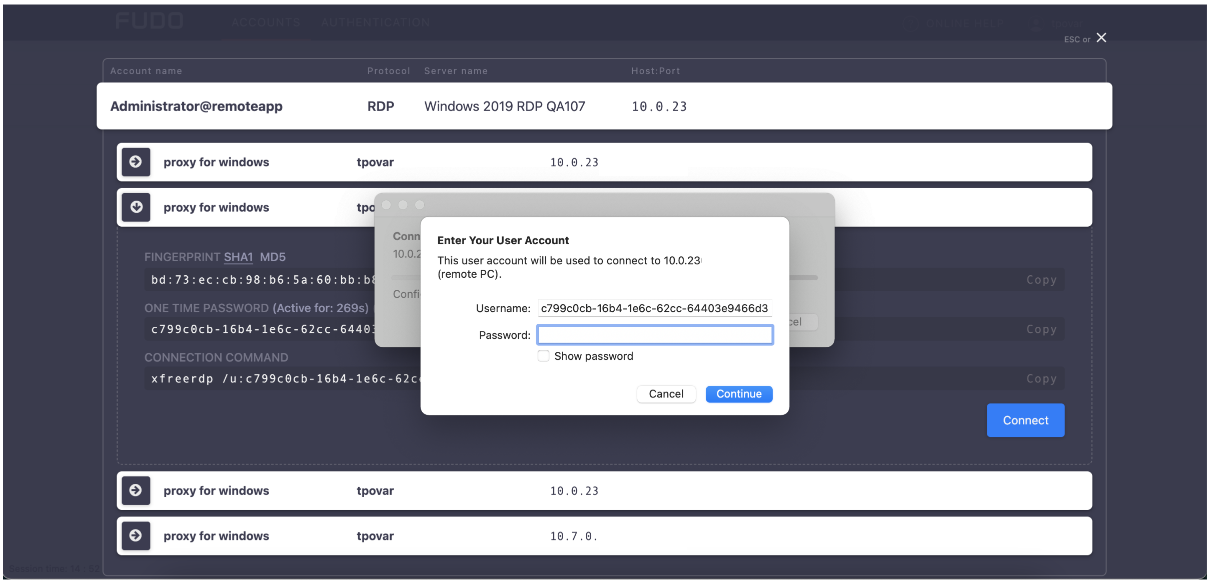
Note:

- *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.



Account name	Protocol	Server name	Host:Port
Administrator@remoteapp	RDP	Windows 2019 RDP QA107	10.0.23
proxy for windows		tpovar	10.0.23
proxy for windows		tpo	
proxy for windows		tpovar	10.0.23
proxy for windows		tpovar	10.7.0.

FINGERPRINT SHA1 MD5

```
bd:73:ec:cb:98:b6:5a:60:bb:b
```

ONE TIME PASSWORD (Active for: 269s)

```
c799c0cb-16b4-1e6c-62cc-6440
```

CONNECTION COMMAND

```
xfreerdp /u:c799c0cb-16b4-1e6c-62c
```

Enter Your User Account

This user account will be used to connect to 10.0.23 (remote PC).

Username: c799c0cb-16b4-1e6c-62cc-64403e9466d3

Password:

□ Show password

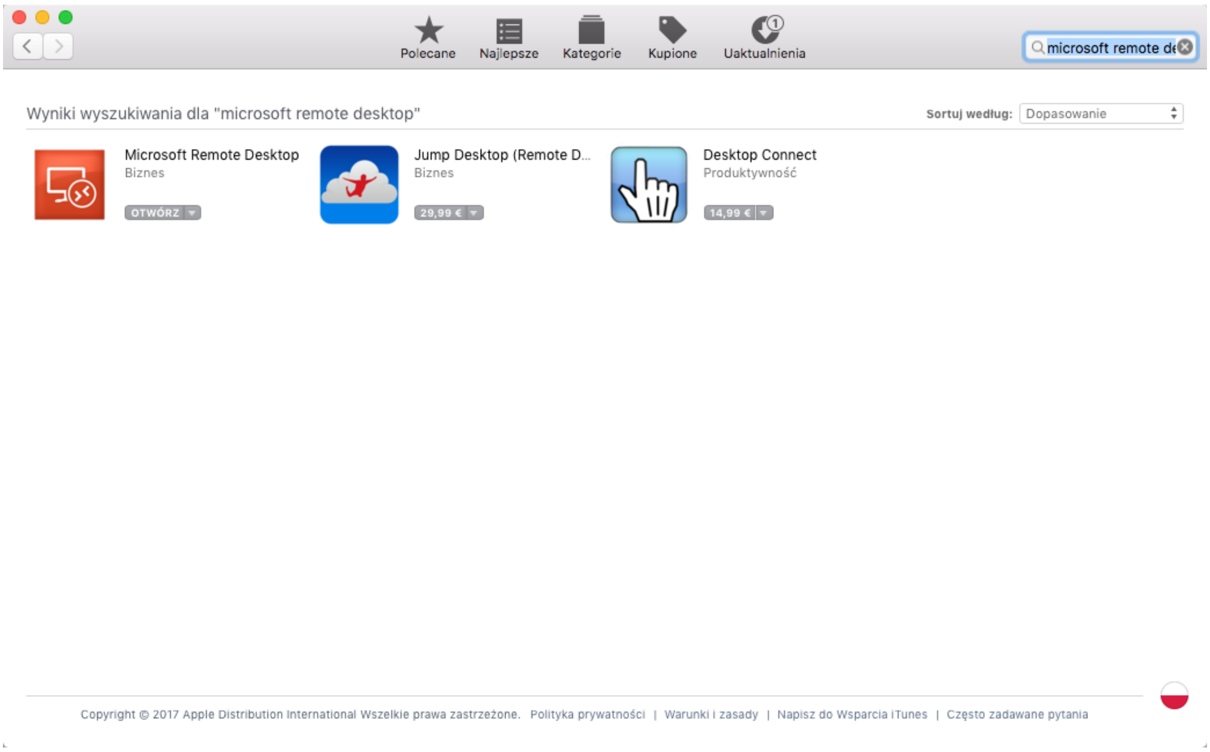
6. Click *Continue* to connect to the server despite the certificate alert.

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*.



Wyniki wyszukiwania dla "microsoft remote desktop"

Sortuj według: Dopasowanie

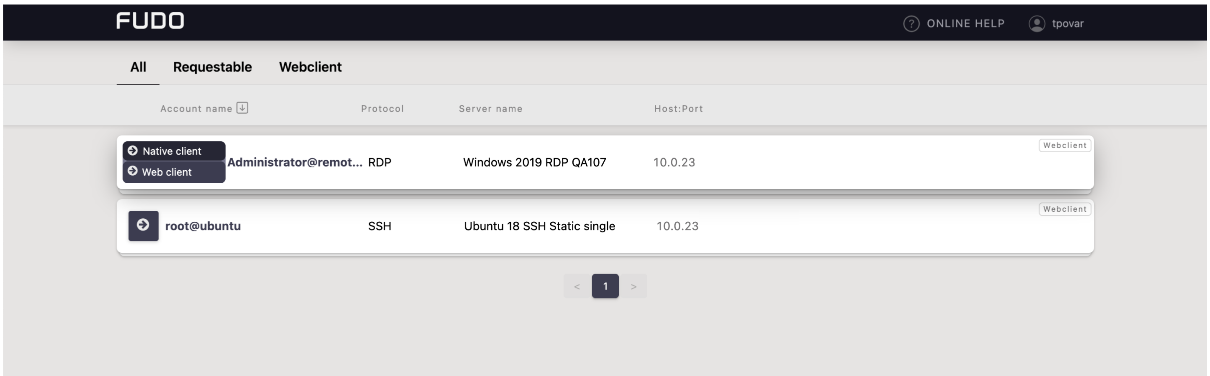
Microsoft Remote Desktop
Biznes

Jump Desktop (Remote D...
Biznes

Desktop Connect
Produktywność

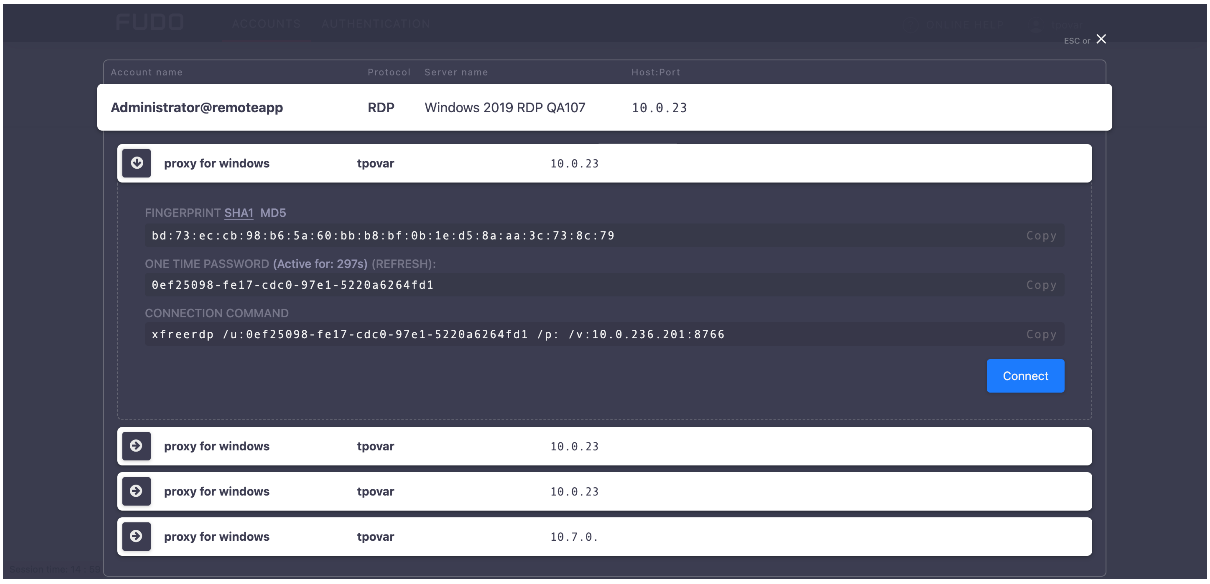
Copyright © 2017 Apple Distribution International Wszelkie prawa zastrzeżone. Polityka prywatności | Warunki i zasady | Napisz do Wsparcia iTunes | Często zadawane pytania

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



Account name	Protocol	Server name	Host:Port
Administrator@remot...	RDP	Windows 2019 RDP QA107	10.0.23
root@ubuntu	SSH	Ubuntu 18 SSH Static single	10.0.23

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



ESC or ✕

Account name	Protocol	Server name	Host:Port
Administrator@remoteapp	RDP	Windows 2019 RDP QA107	10.0.23

proxy for windows	tpovar	10.0.23

FINGERPRINT SHA1 MD5

```
bd:73:ec:cb:98:b6:5a:60:bb:b8:bf:0b:1e:d5:8a:aa:3c:73:8c:79
```

Copy

ONE TIME PASSWORD (Active for: 297s) (REFRESH):

```
0ef25098-fe17-cdc0-97e1-5220a6264fd1
```

Copy

CONNECTION COMMAND

```
xfreerdp /u:0ef25098-fe17-cdc0-97e1-5220a6264fd1 /p: /v:10.0.236.201:8766
```

Copy

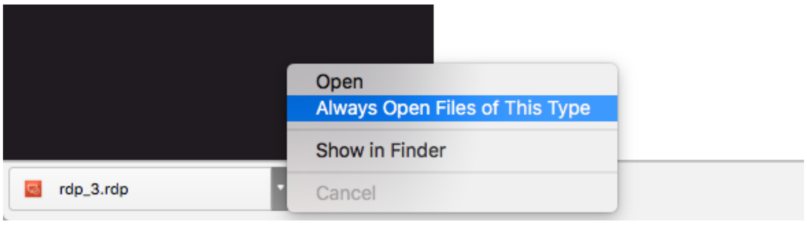
Connect

proxy for windows	tpovar	10.0.23
proxy for windows	tpovar	10.0.23
proxy for windows	tpovar	10.7.0.

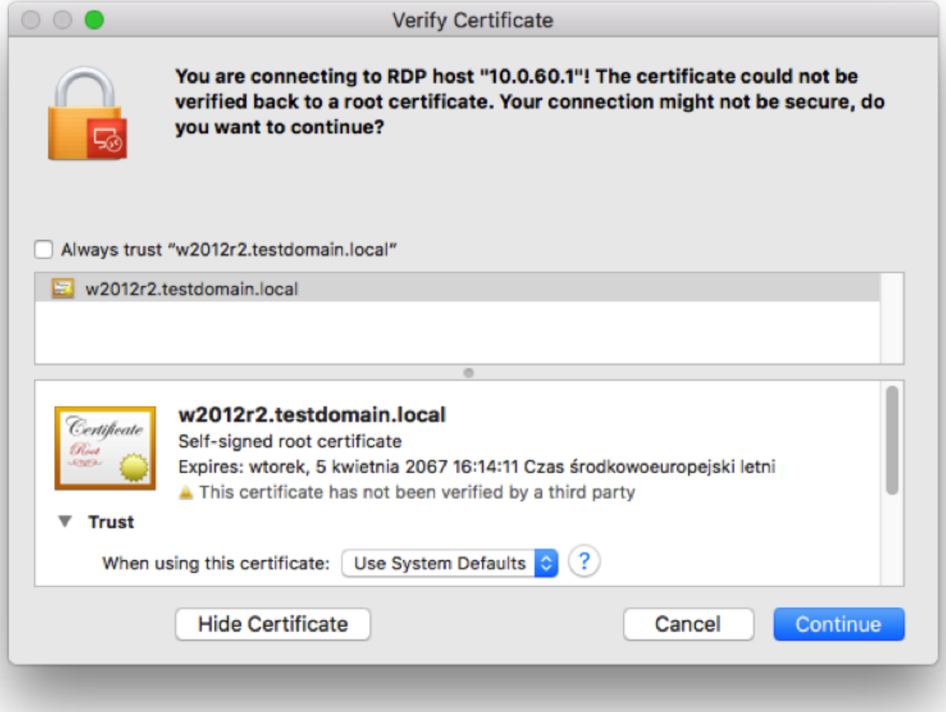
4. Click *Connect*.

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.



You are connecting to RDP host "10.0.60.1"! The certificate could not be verified back to a root certificate. Your connection might not be secure, do you want to continue?

□ Always trust "w2012r2.testdomain.local"

w2012r2.testdomain.local

w2012r2.testdomain.local
Self-signed root certificate
Expires: wtorek, 5 kwietnia 2067 16:14:11 Czas środkowoeuropejski letni
⚠ This certificate has not been verified by a third party

When using this certificate: Use System Defaults

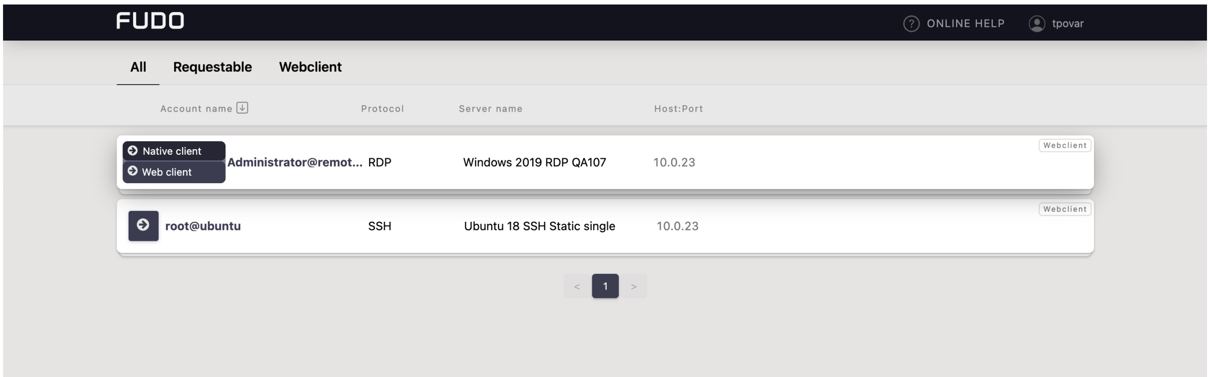
Related topics:

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

7.5 Connecting over RDP on Ubuntu Linux

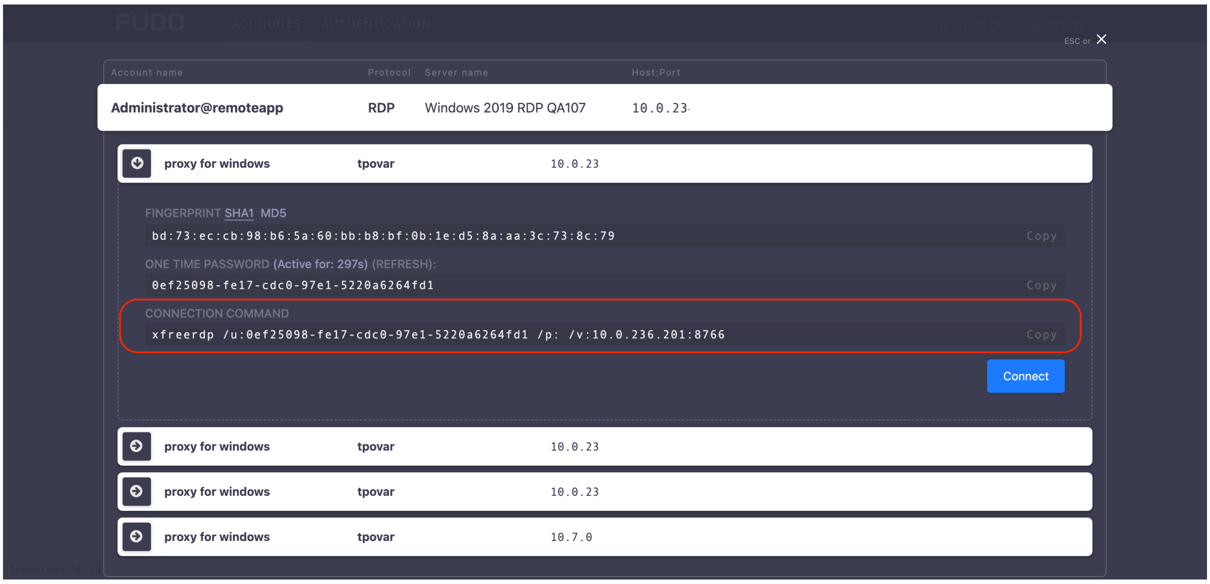
Note: Establishing RDP connections on Ubuntu 16.04 LTS requires installing `xfreerdp`. Execute `sudo apt-get install freerdp-x11`, to install it before proceeding with connecting over RDP protocol.

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



Account name	Protocol	Server name	Host:Port
Administrator@remot...	RDP	Windows 2019 RDP QA107	10.0.23
root@ubuntu	SSH	Ubuntu 18 SSH Static single	10.0.23

3. Choose the listener, via which you want to connect.
4. Copy generated string.



Account name	Protocol	Server name	Host:Port
Administrator@remoteapp	RDP	Windows 2019 RDP QA107	10.0.23

proxy for windows tpovar 10.0.23

FINGERPRINT SHA1 MD5

```
bd:73:ec:cb:98:b6:5a:60:bb:b8:bf:0b:1e:d5:8a:aa:3c:73:8c:79
```

ONE TIME PASSWORD (Active for: 297s) (REFRESH):

```
0ef25098-fe17-cdc0-97e1-5220a6264fd1
```

CONNECTION COMMAND

```
xfreerdp /u:0ef25098-fe17-cdc0-97e1-5220a6264fd1 /p: /v:10.0.236.201:8766
```

proxy for windows tpovar 10.0.23

proxy for windows tpovar 10.0.23

proxy for windows tpovar 10.7.0

5. 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.

1. Download and install *WinSCP*.

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

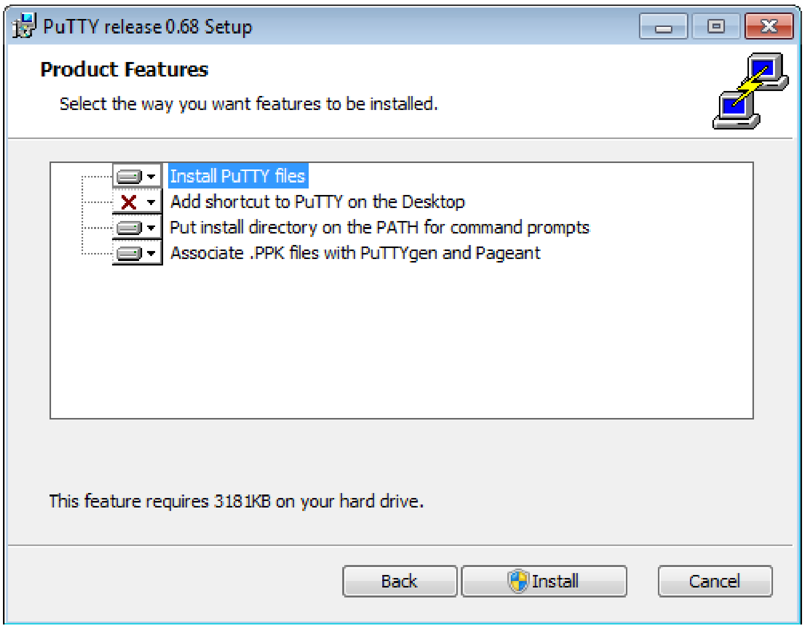
Note: Verify the checksum value to make sure that the integrity of the binary file has not been compromised.

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.



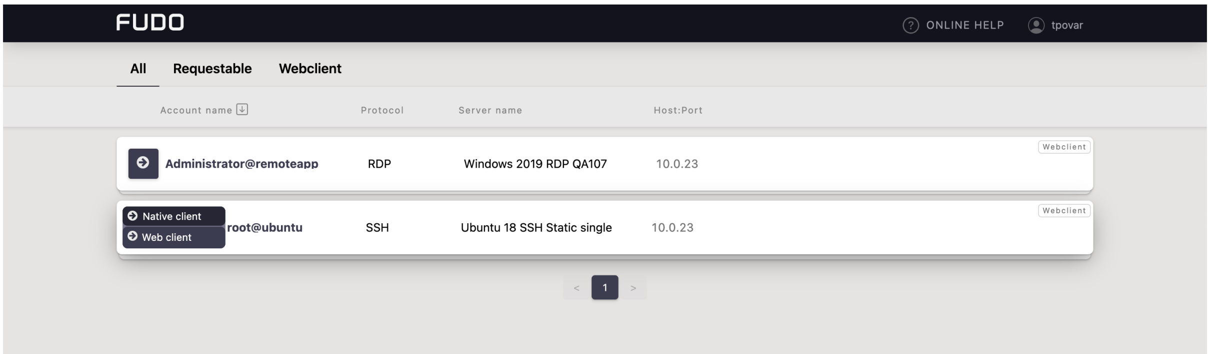
Product Features

Select the way you want features to be installed.

- Install PuTTY files
- Add shortcut to PuTTY on the Desktop
- Put install directory on the PATH for command prompts
- Associate .PPK files with PuTTYgen and Pageant

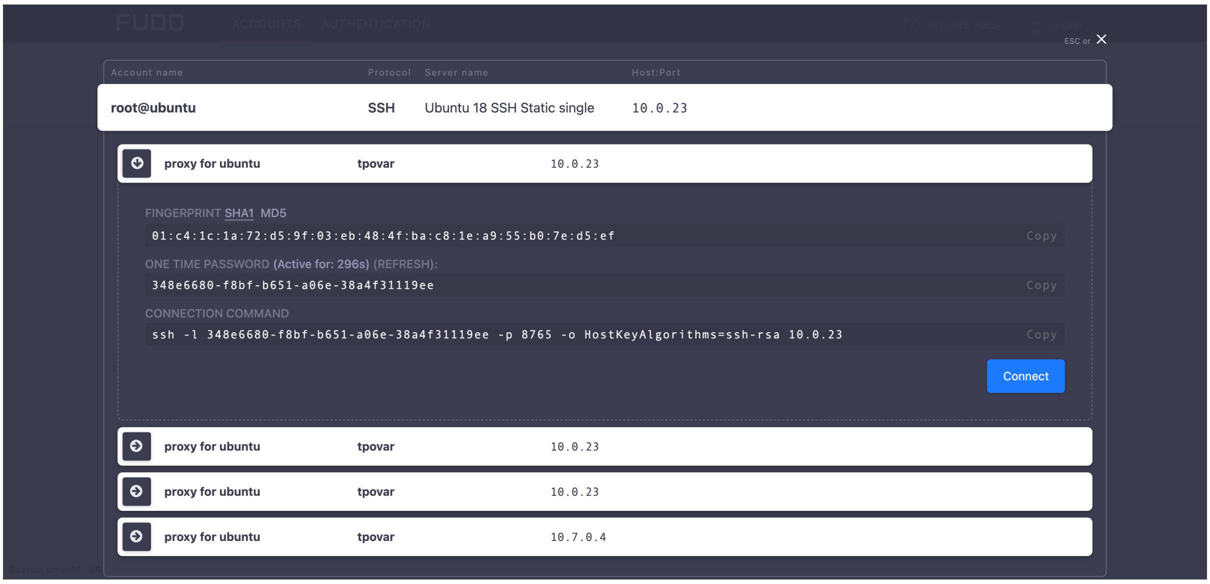
This feature requires 3181KB on your hard drive.

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.



Account name	Protocol	Server name	Host:Port
Administrator@remoteapp	RDP	Windows 2019 RDP QA107	10.0.23
root@ubuntu	SSH	Ubuntu 18 SSH Static single	10.0.23

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



Account name	Protocol	Server name	Host:Port
root@ubuntu	SSH	Ubuntu 18 SSH Static single	10.0.23

proxy for ubuntu	tpovar	10.0.23

FINGERPRINT SHA1 MD5

```
01:c4:1c:1a:72:d5:9f:03:eb:48:4f:ba:c8:1e:a9:55:b0:7e:d5:ef
```

ONE TIME PASSWORD (Active for: 296s) (REFRESH):

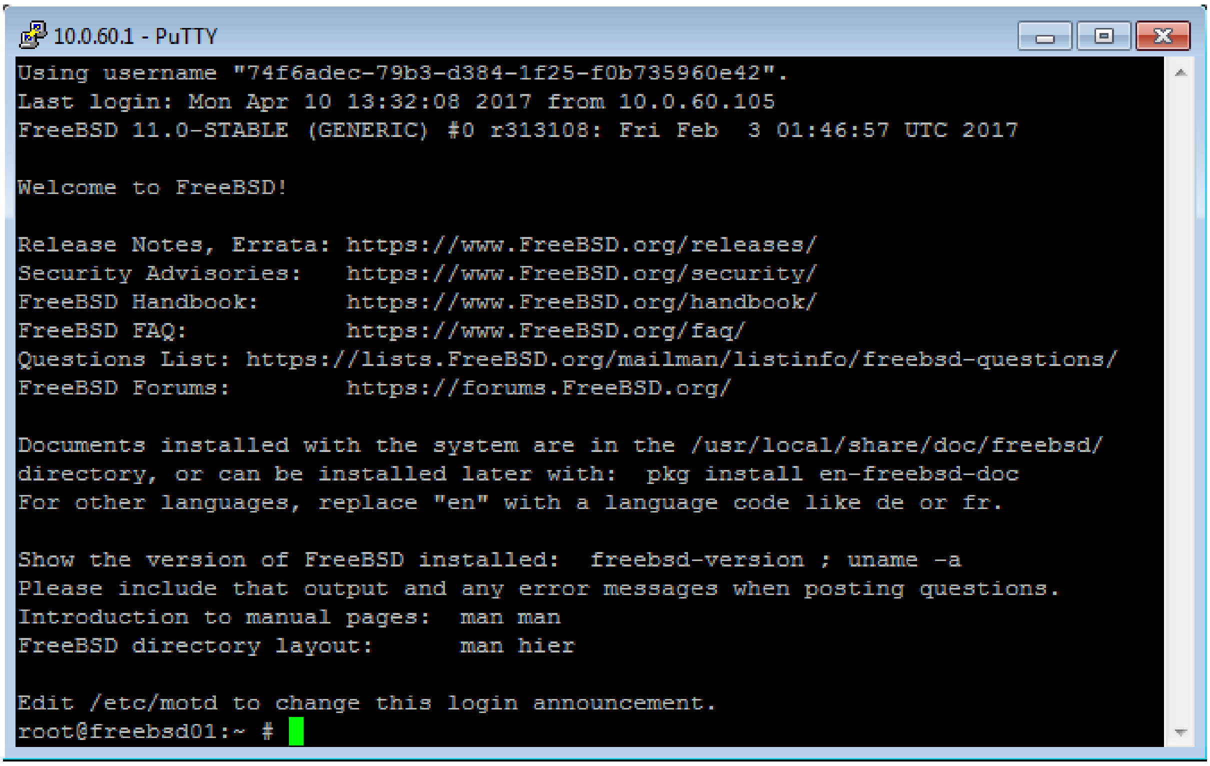
```
348e6680-f8bf-b651-a06e-38a4f31119ee
```

CONNECTION COMMAND

```
ssh -l 348e6680-f8bf-b651-a06e-38a4f31119ee -p 8765 -o HostKeyAlgorithms=ssh-rsa 10.0.23
```

proxy for ubuntu	tpovar	10.0.23
proxy for ubuntu	tpovar	10.0.23
proxy for ubuntu	tpovar	10.7.0.4

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.



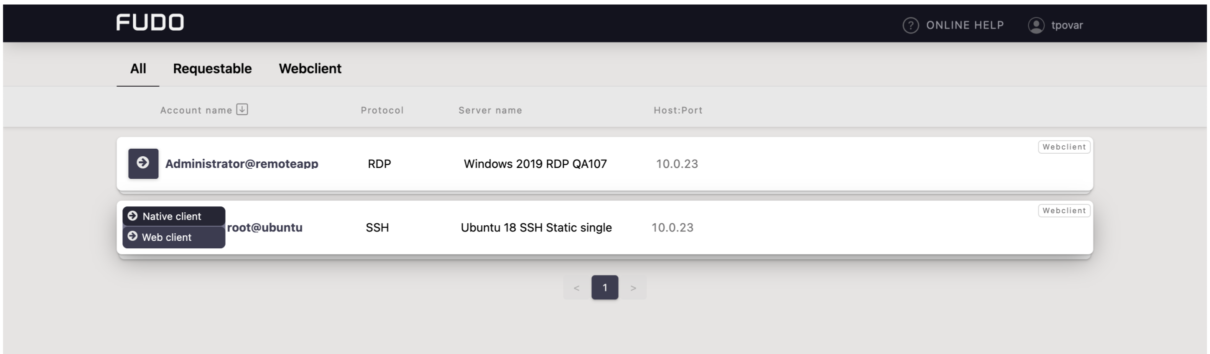
```
Using username "74f6adec-79b3-d384-1f25-f0b735960e42".
Last login: Mon Apr 10 13:32:08 2017 from 10.0.60.105
FreeBSD 11.0-STABLE (GENERIC) #0 r313108: Fri Feb  3 01:46:57 UTC 2017

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*

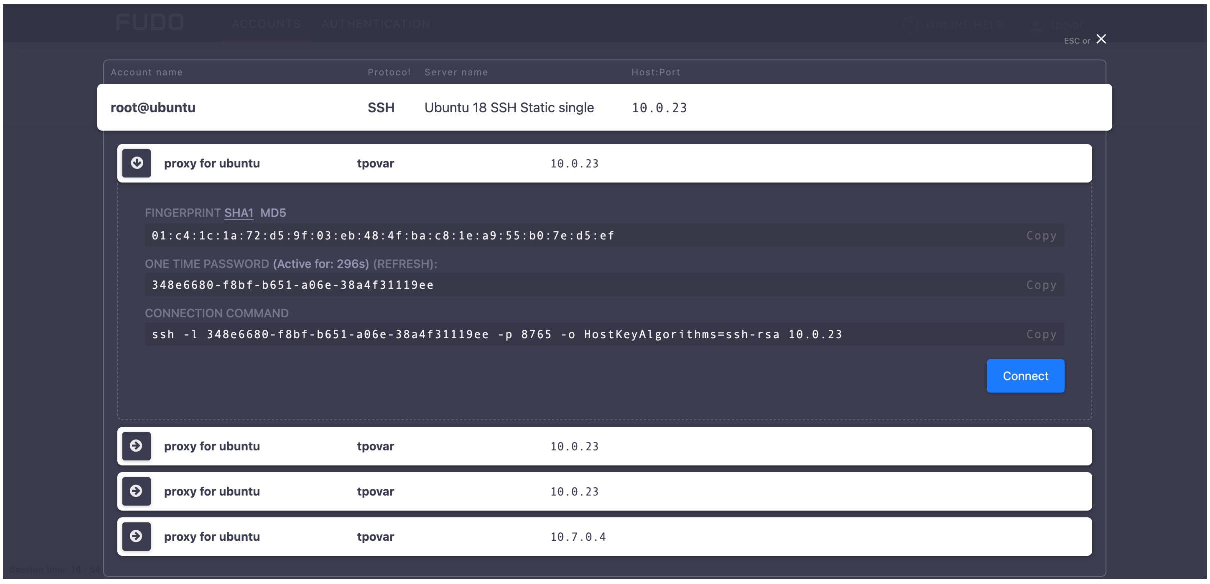
7.7 Connecting over SSH on Mac OS, Linux

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



Account name	Protocol	Server name	Host:Port
Administrator@remoteapp	RDP	Windows 2019 RDP QA107	10.0.23
root@ubuntu	SSH	Ubuntu 18 SSH Static single	10.0.23

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



Account name	Protocol	Server name	Host:Port
root@ubuntu	SSH	Ubuntu 18 SSH Static single	10.0.23
proxy for ubuntu	tpovar		10.0.23

FINGERPRINT SHA1 MD5

```
01:c4:1c:1a:72:d5:9f:03:eb:48:4f:ba:c8:1e:a9:55:b0:7e:d5:ef
```

ONE TIME PASSWORD (Active for: 296s) (REFRESH):

```
348e6680-f8bf-b651-a06e-38a4f31119ee
```

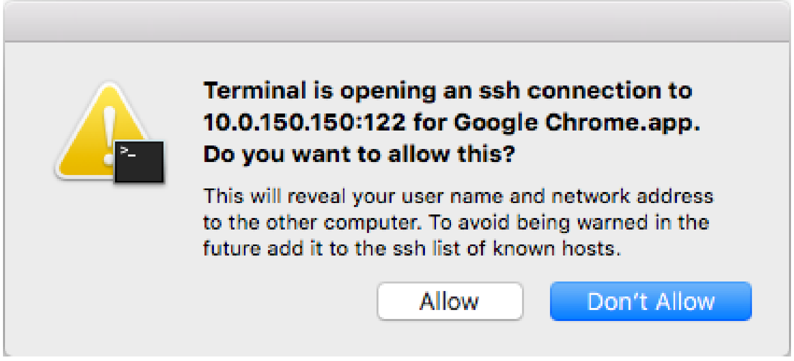
CONNECTION COMMAND

```
ssh -l 348e6680-f8bf-b651-a06e-38a4f31119ee -p 8765 -o HostKeyAlgorithms=ssh-rsa 10.0.23
```

proxy for ubuntu	tpovar	10.0.23
proxy for ubuntu	tpovar	10.0.23
proxy for ubuntu	tpovar	10.7.0.4

4. Click *Connect*.

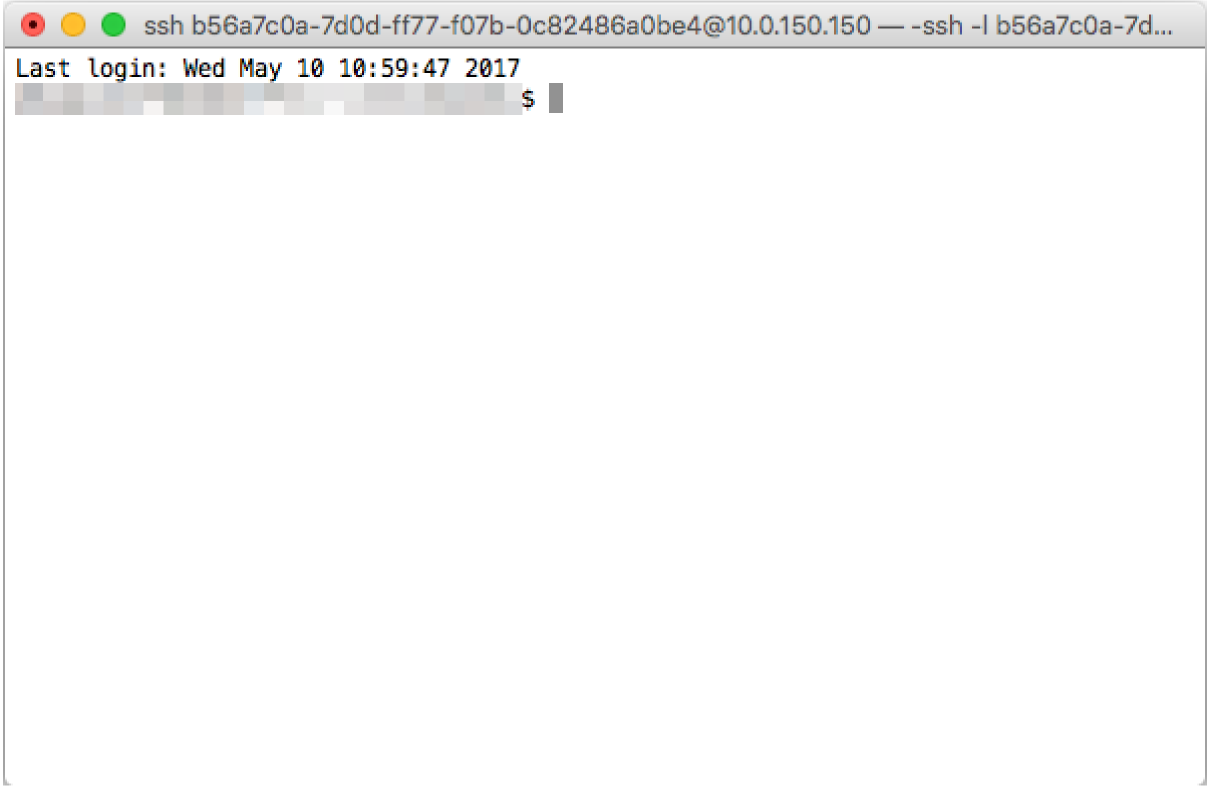
5. Click *Allow* to open the Terminal.



Terminal is opening an ssh connection to 10.0.150.150:122 for Google Chrome.app. Do you want to allow this?

This will reveal your user name and network address to the other computer. To avoid being warned in the future add it to the ssh list of known hosts.

6. The connection has been established.


ssh b56a7c0a-7d0d-ff77-f07b-0c82486a0be4@10.0.150.150 — -ssh -l b56a7c0a-7d...

```
Last login: Wed May 10 10:59:47 2017
[redacted]$ 
```

Related topics:

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

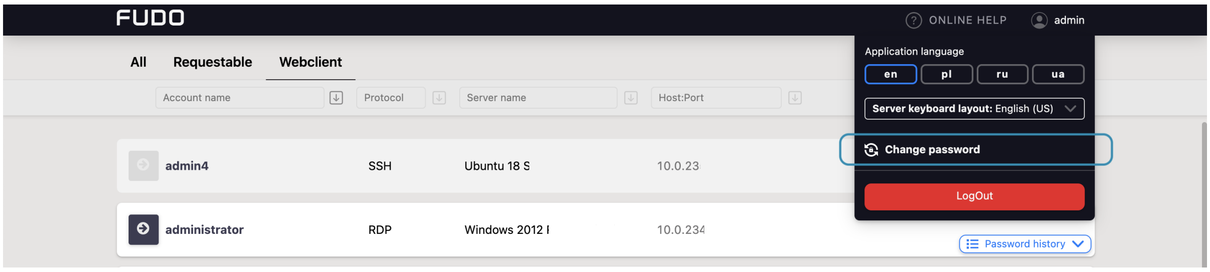
CHAPTER 8

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.



Account name	Protocol	Server name	Host:Port
admin4	SSH	Ubuntu 18 S	10.0.23
administrator	RDP	Windows 2012 I	10.0.234

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

Related topics:

- *Displaying passwords history*

CHAPTER 9

Troubleshooting

Problem	Symptoms and solution description
Cannot log in to the Access Gateway	**Symptoms:** • The user cannot log in.
	Solution: • 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.

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.