Fudo Enterprise 6.0 - Access Gateway Manual

Fudo Security

15.04.2026

Contents

CHAPTER 1

About Documentation

Conventions and symbols

This documentation is written using the following conventions:

- *italic* - this formatting is used to mark user interface elements.
- `example` - this formatting is used to write example value of a parameter, API method name or code example.
- Note field:

> **Note**
>
> Note field usually contains additional information closely related with described topic, e.g. suggestion concerning given procedure step; additional conditions which have to be met.

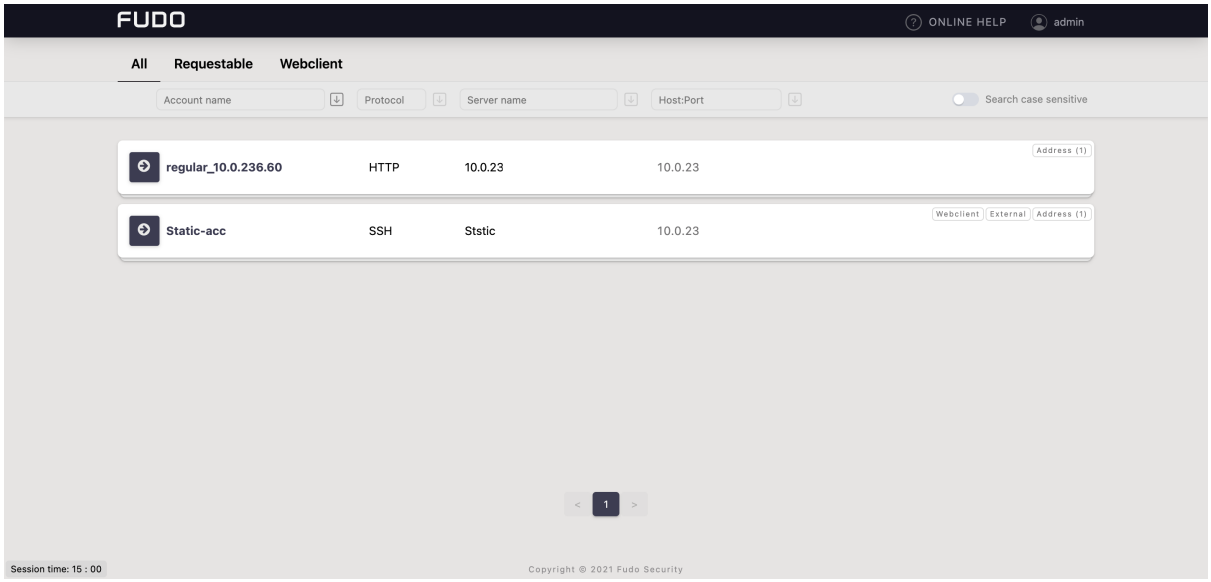
- Warning field:

> **Warning**
>
> Warning field usually contains essential information concerning system's operation. Not adhering to this information may have irreversible consequences.

CHAPTER 2

System Overview

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



The User 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`, `Ukrainian` or `Kazakh`.

Note

Availability of the particular language is specified in the license.

Related topics:

- *Logging into the User Access Gateway*
- *Secret Checkout and Checkin*
- *Displaying Passwords History*
- *Displaying and Editing Accounts Notes*
- *Establishing Connections*
- *Change Password*
- *Troubleshooting*

CHAPTER 3

Logging into the User Access Gateway

Note

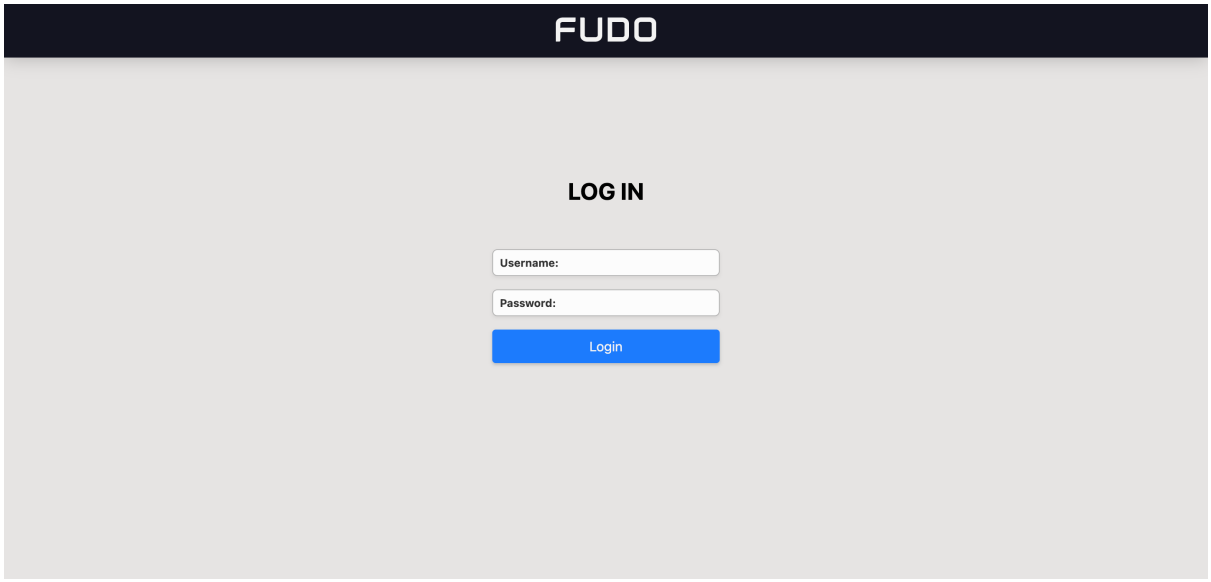
- User Access Gateway is compatible with the following web browsers:
  - Google Chrome, Mozilla Firefox, Microsoft Edge for Microsoft Windows.
  - Google Chrome, Mozilla Firefox for Ubuntu.
  - Google Chrome, Mozilla Firefox, Safari dla systemu operacyjnego Mac OS X.
- *User Access Gateway* supports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

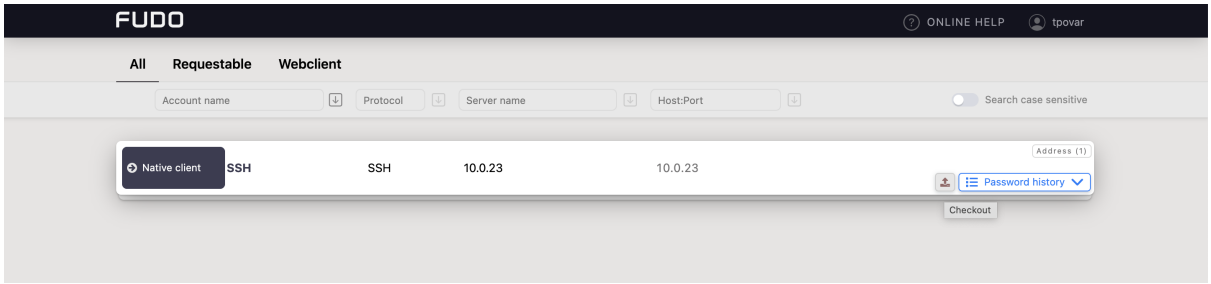
Secret Checkout and Checkin

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.

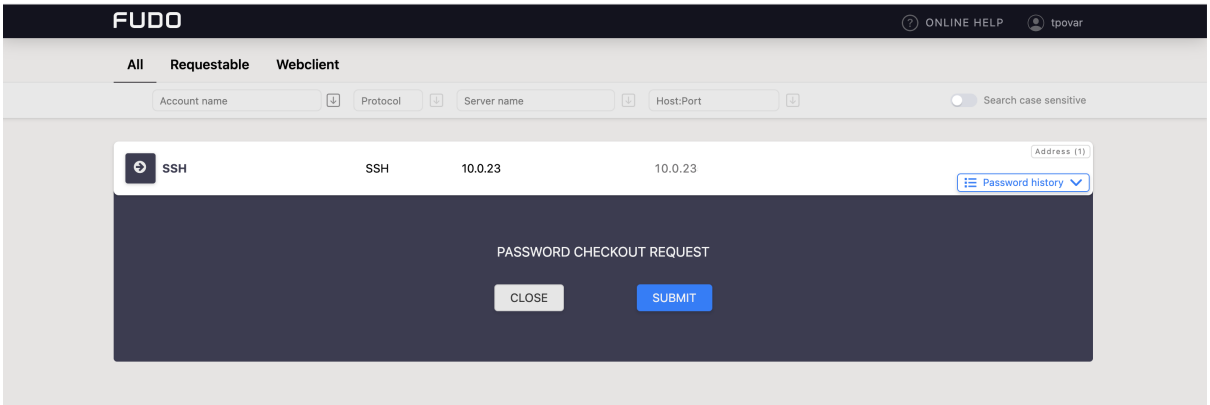
4.1 Secret Checkout

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.



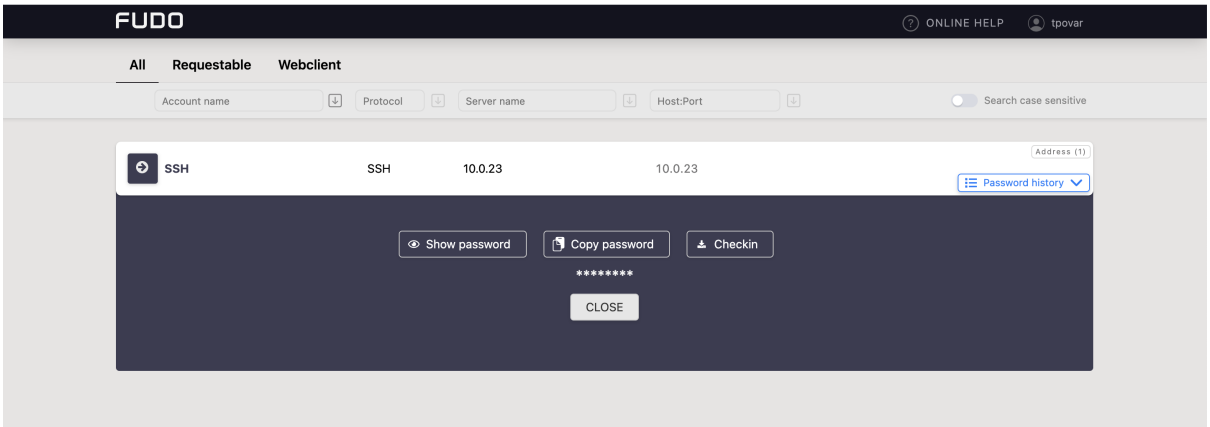
3. Click *SUBMIT*.



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.



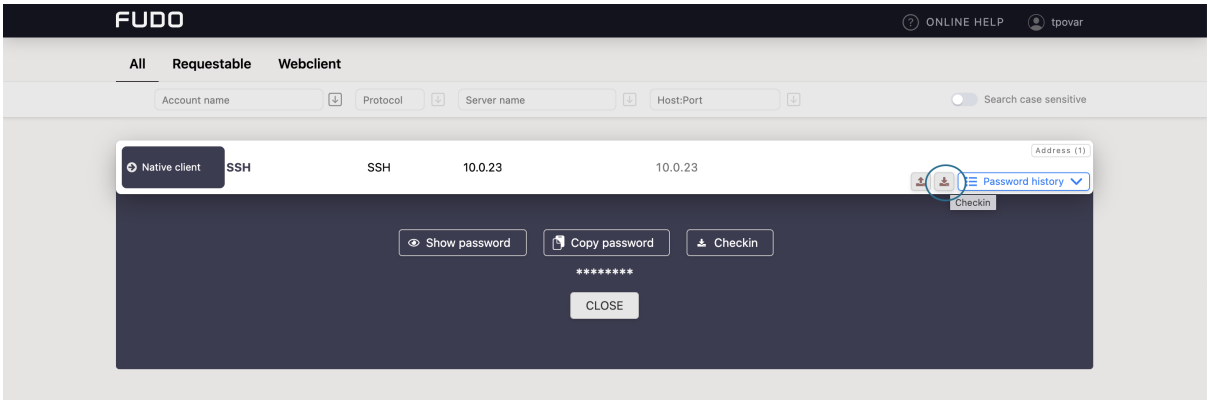
4.2 Secret Checkin

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:

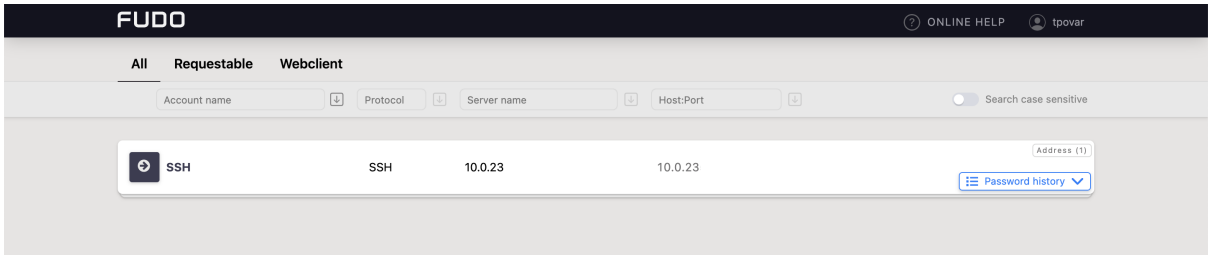
- *Displaying Passwords History*

CHAPTER 5

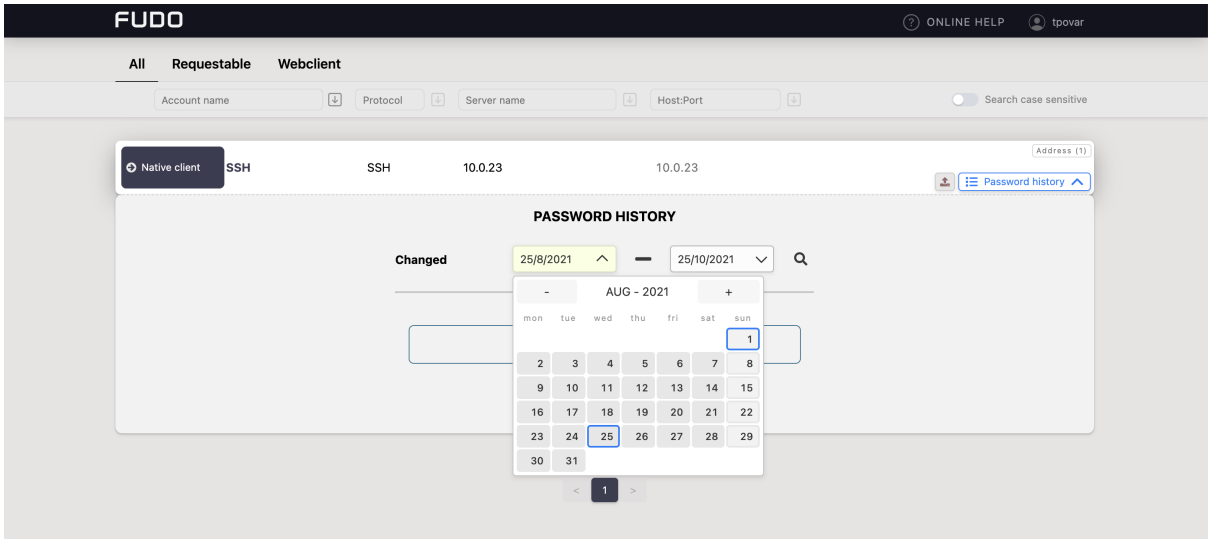
Displaying Passwords History

Account password may be changed manually by the user, or automatically by the Fudo Enterprise 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

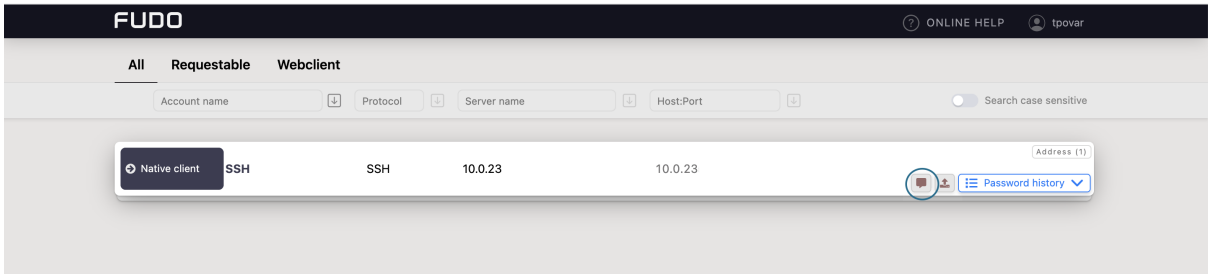
Displaying and Editing Accounts Notes

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

Password Vault

The Password Vault module in User Access Gateway provides a secure, centralized system for managing passwords and secrets. It allows users to store, organize, and share credentials within their organization while maintaining personal secrets separately.

Password Vault consists of two main components:

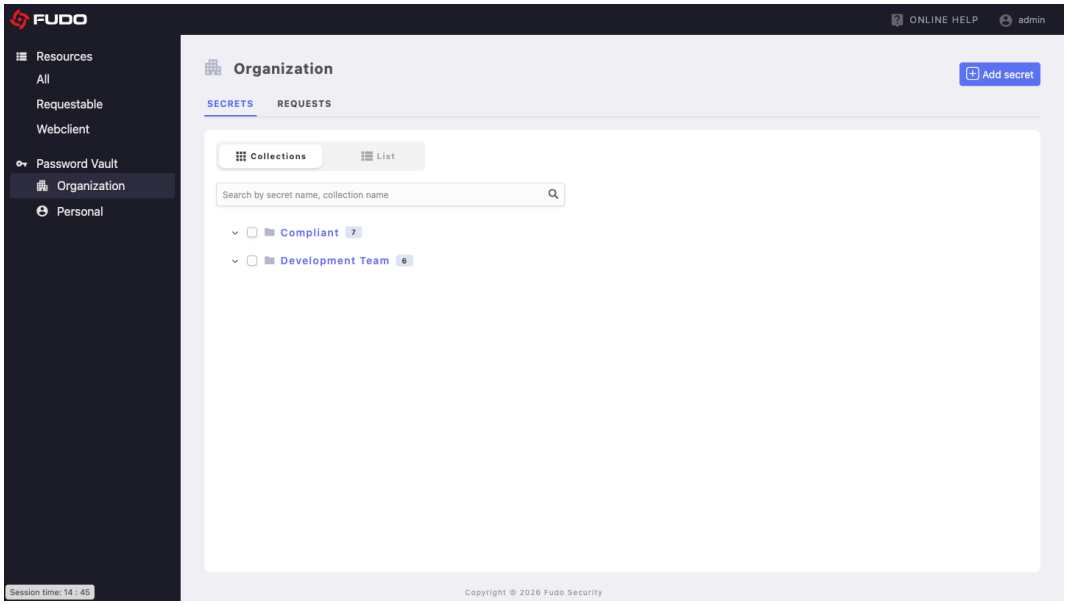
- **Organization Vault** - Managed by the organization, contains shared secrets and collections accessible based on user permissions.
- **Personal Vault** - Private space for individual users to store their personal credentials.

The following sections describe the main areas of Password Vault and how to work with secrets and collections.

7.1 Overview

7.1.1 Accessing Password Vault

1. Log in to User Access Gateway with your credentials.
2. In the left sidebar, locate the **Password Vault** section.
3. You will see two options:
    - **Organization** - For company-wide shared secrets
    - **Personal** - For your private credentials



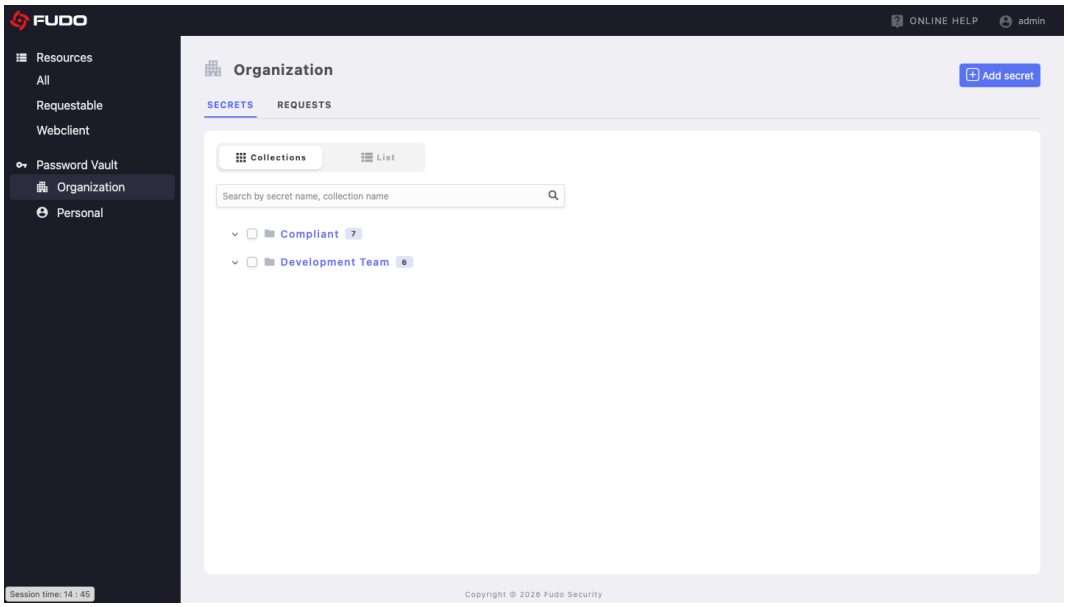
7.1.2 Viewing Secrets and Collections

The interface provides two view modes:

- **Collections View** (default) - Displays secrets organized in a hierarchical collection structure
- **List View** - Shows all accessible secrets in a table format

Collections View

Collections View is the default view, displaying secrets organized in a hierarchical collection tree.



Search and Filter

Use the search bar to quickly find secrets:

1. Type the secret name or collection name in the search field
2. Use filters to narrow results:

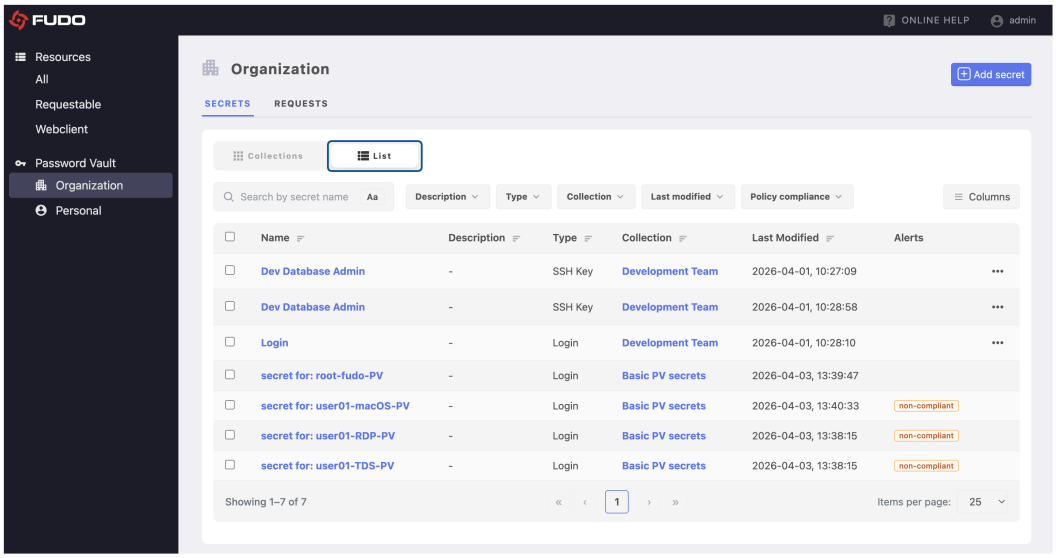
- Click on collection folders to filter by collection
- The number next to each collection shows how many secrets it contains

List View

The List view provides a comprehensive table of all accessible secrets.

Switch to List View

1. Click the **List** button in the view toggle

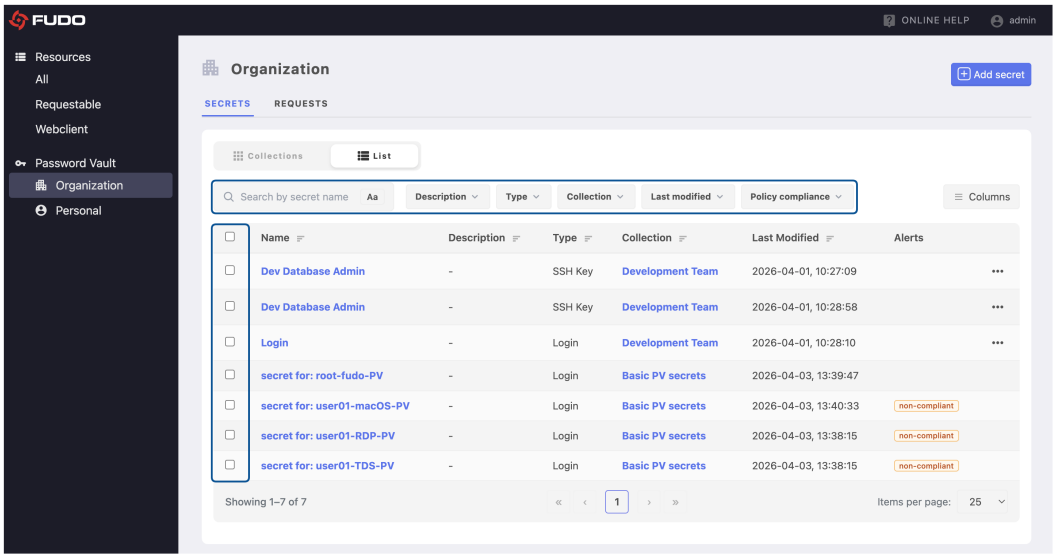


Sort and Filter

The table displays:

- **Name** - Secret name (click to open)
- **Description** - Brief description
- **Type** - Login, SSH Key, Note, etc.
- **Collection** - Parent collection name
- **Last Modified** - Date and time of last change
- **Alerts** - Shows if password meets security policies

1. Click column headers to sort
2. Use the search bar to filter results
3. Select multiple secrets using checkboxes for bulk operations

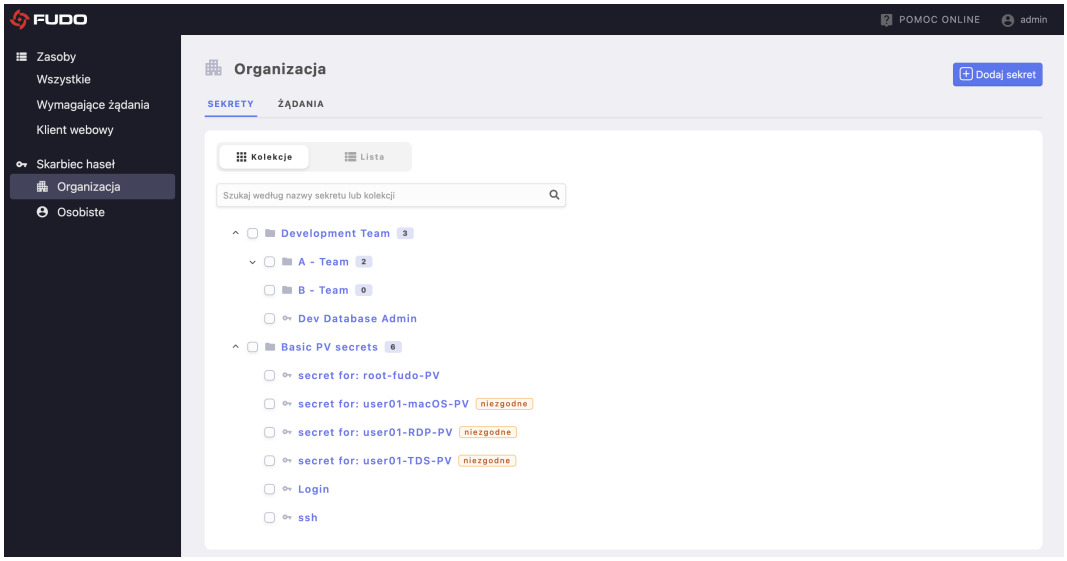


7.2 Organization Vault

The Organization Vault contains secrets and collections managed at the organizational level. Access to these secrets is controlled through a permission system.

7.2.1 Accessing Organization Vault

1. Click on **Organization** under **Password Vault** in the left sidebar.
2. The main view opens showing your accessible collections.



7.2.2 Understanding User Permissions

In the Organization Vault, access to secrets is managed through permissions assigned by the system administrator. Depending on the permission level granted for a collection, users may be able to view secret names, request access to secret values, reveal and copy secret data, or fully manage secrets.

View on Request

- View secret names and collections
- Request one-time access to a secret values (requires an admin's approval)
- Cannot modify or delete secrets

View

- View the details of all secrets in a collection at any time
- Reveal and copy secret values
- Cannot modify or delete secrets

Full Edit

- All **View** capabilities, plus:
- Modify existing secrets
- Move secrets between collections
- Delete secrets
- Add new secrets to collections

No Permission

- Cannot view or access any secrets.

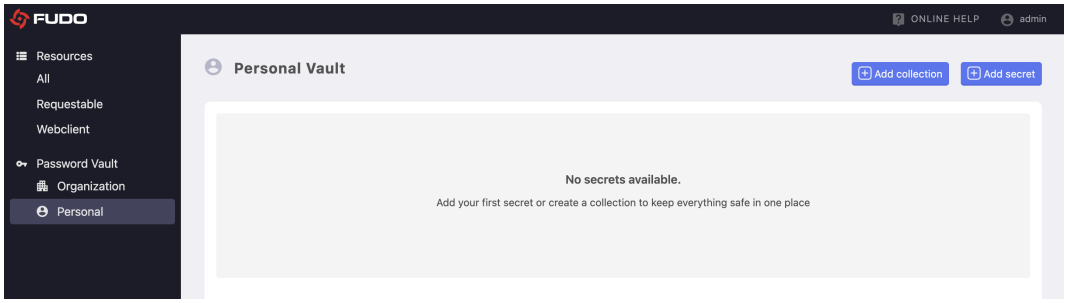
> **Note**
>
> If you need access to Password Vault or additional access to selected collections, contact your administrator.

7.3 Personal Vault

Your *Personal Vault* is a private space for storing personal credentials that only you can access, giving you complete privacy, full control over your secrets, and full edit rights by default.

7.3.1 Accessing Personal Vault

1. Click on **Personal** under **Password Vault** in the left sidebar.
2. Your personal vault opens, showing your collections and secrets.
3. If this is your first time, you'll see a welcome message prompting you to create your first collection.



7.3.2 Key Features

Creating and Managing Secrets

In your Personal Vault, you can:

- Add any type of secret (Login, SSH Key, Note, API Key, Certificate)
- Edit and update secret information at any time
- Move secrets between your collections
- Delete secrets permanently

> **Note**
>
> For detailed instructions on managing secrets, see *Adding a New Secret*.

Organizing with Collections

Collection management is available only in the Personal Vault:

- Create unlimited collections and nested structures
- Organize secrets by project, client, or any system that works for you
- Move and reorganize collections as needed
- Delete empty collections when no longer needed

> **Note**
>
> For detailed instructions on managing collections, see *Managing Collections (Personal Vault)*.

7.3.3 Differences from Organization Vault

Feature	Personal Vault	Organization Vault
Access Control	Full control (owner only)	Permission-based (admin managed)
Collection Management	Create/edit/delete via UAG	Admin managed only
Approval Required	No	Yes (for restricted access)
Visibility	Private to user	Visible to authorized users

7.3.4 Getting Started

To begin using your Personal Vault:

1. Create your first collection - see *Managing Collections (Personal Vault)*.
2. Add your first secret - see *Managing Secrets*.
3. Organize and manage as needed using the features described above.

7.4 Managing Secrets

Secrets store sensitive information such as login credentials, API keys, certificates, SSH keys, and notes. Each secret is assigned to a collection for organization and access control.

Note

The process for creating secrets is identical in both Organization and Personal Vaults. The key differences are:

- **Organization Vault**: Requires appropriate permissions from your administrator. You need *Full Edit* permission for the target collection.
- **Personal Vault**: You have full control by default. No admin approval needed for your personal collections.

Warning

For Organization Vault: You must have appropriate permissions to add secrets. If you do not have access, contact your Fudo administrator.

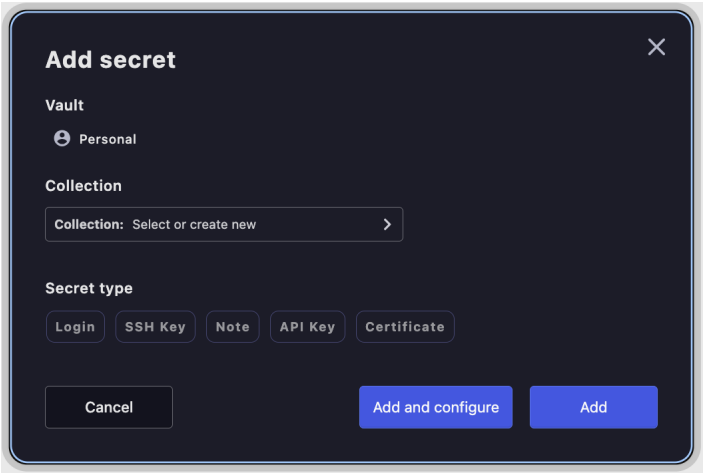
7.4.1 Adding a New Secret

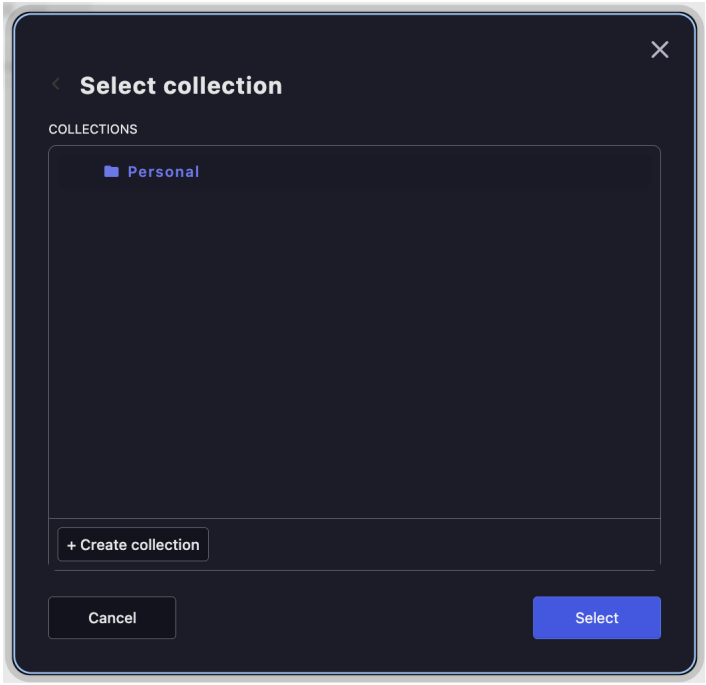
Note

Available Secret Types:

- **Login**: Username/password credentials with domain and URL information
- **SSH Key**: SSH private keys for server access
- **Note**: Plain text notes for storing non-credential information
- **API Key**: API tokens and keys for service authentication
- **Certificate**: Digital certificates and private keys

1. Select *Password Vault* > *Organization* or *Personal*.
2. Click *Add secret*.

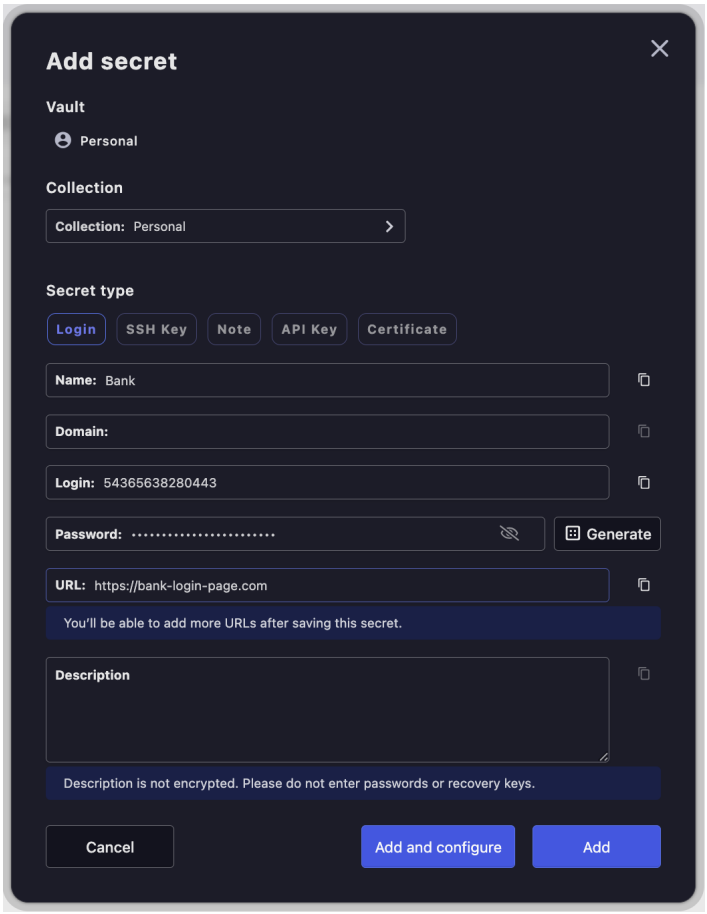




3. Select the collection where the secret will be stored by clicking the *Collection* dropdown.
4. Click *Select*.
5. Choose the appropriate secret type (Login, SSH Key, Note, API Key, Certificate).

For Login Secrets:

- Fill in the required fields:
  - *Name*: Enter a descriptive name for the secret
  - *Domain*: Target domain or server address
  - *Login*: Username or account name
  - *Password*: You can use the *Generate* button for secure passwords
  - *URL*: Enter the related website or service URL
  - *Description*: Optional additional information (not encrypted)

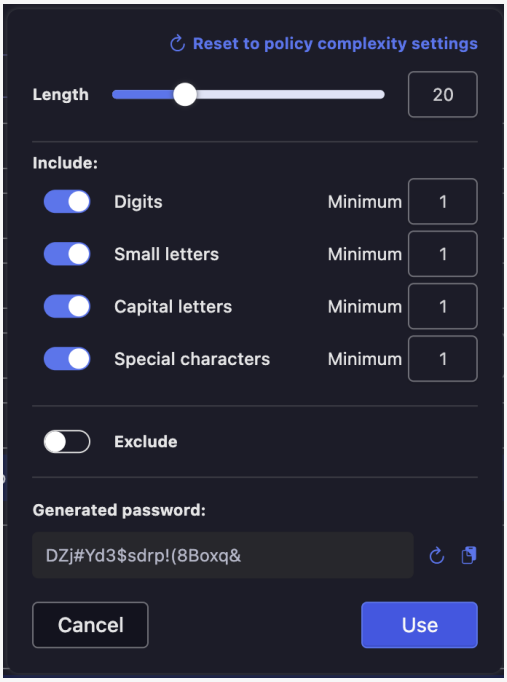


Note

Password Generator:

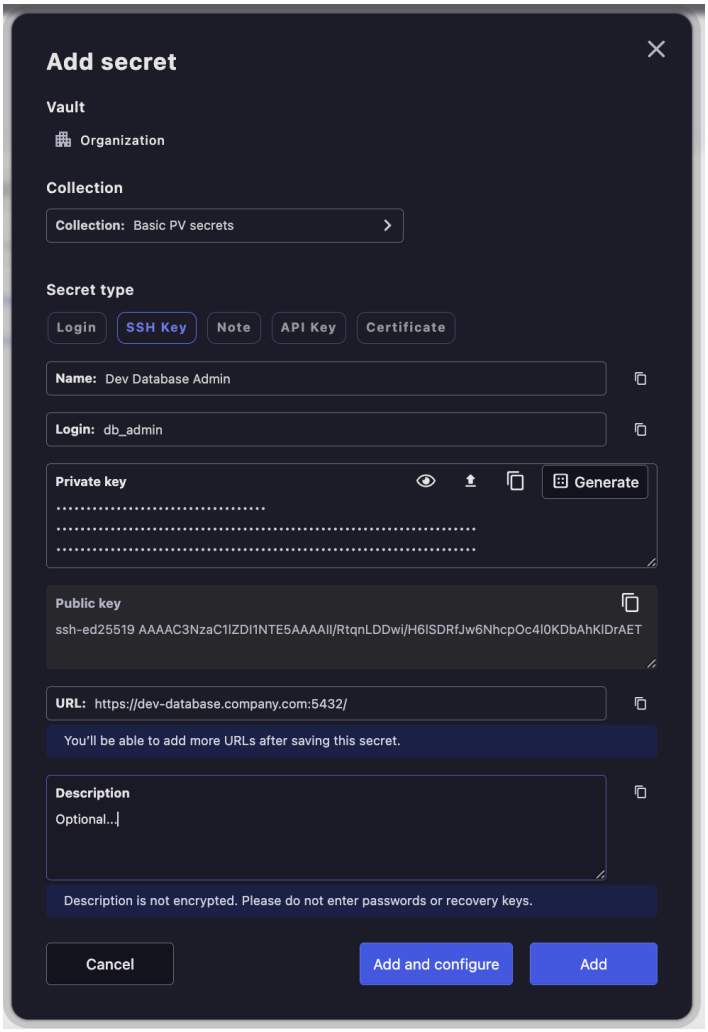
The integrated password generator (*Generate* button) provides secure password creation with customizable options:

- **Length**: Set password length (default: 20 characters)
- **Character Types**: Include digits, small letters, capital letters, special characters
- **Minimum Requirements**: Set minimum count for each character type
- **Exclude Options**: Exclude ambiguous or specific characters
- **Generated Password**: Preview and copy the generated password



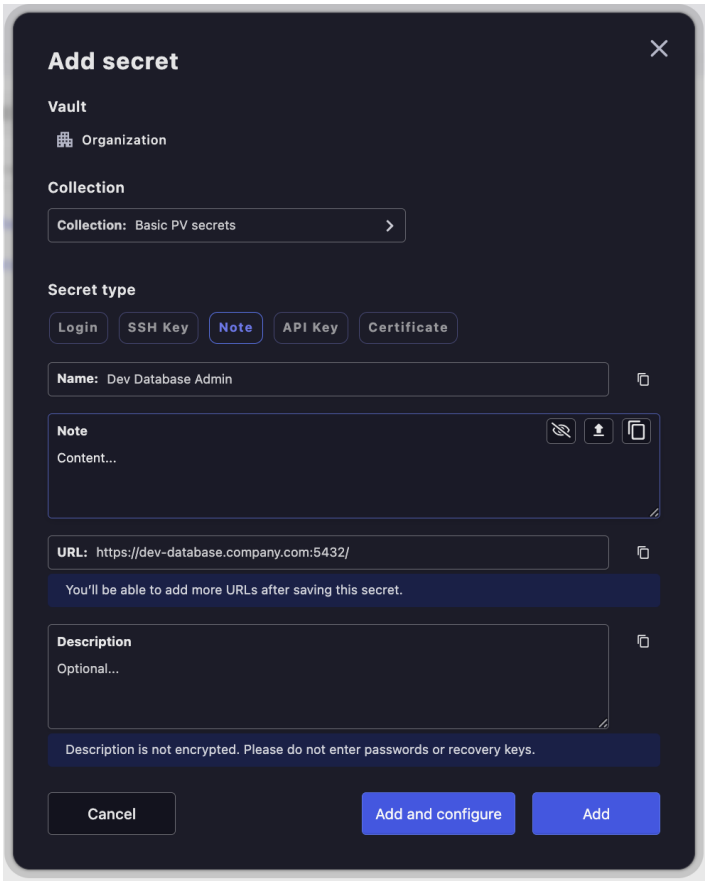
For SSH Key Secrets:

- Fill in the required fields:
  - Name: Enter a descriptive name for the secret
  - Login: Enter the username or account name
  - Private key: Enter the private key, or click *Generate* to generate both private and public keys
  - URL: Enter the related website or service URL
  - Description: Optional additional information (not encrypted)



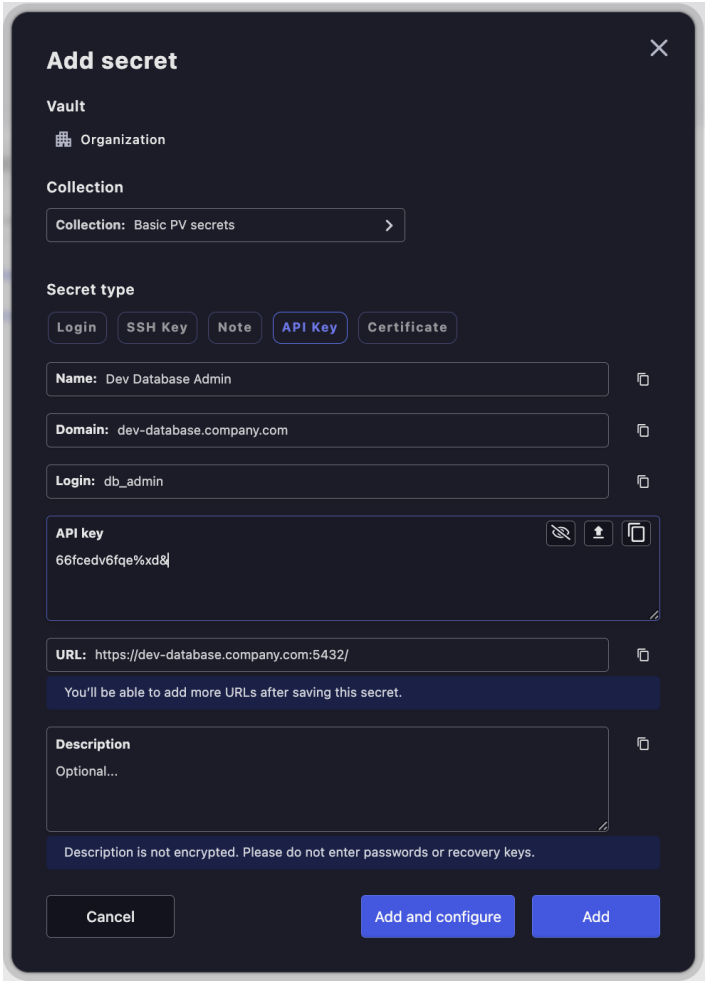
For Note Secrets:

- Fill in the required fields:
  - Name: Enter a descriptive name for the secret
  - Note: Enter the note content
  - URL: Enter the related website or service URL
  - Description: Optional additional information (not encrypted)



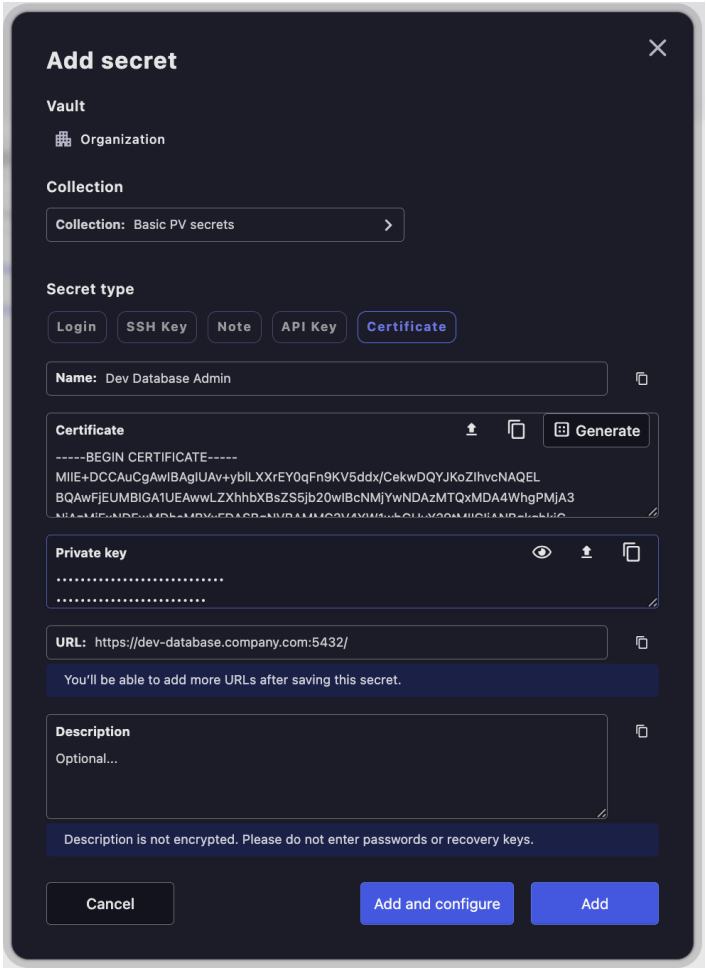
For API Key Secrets:

- Fill in the required fields:
  - Name: Enter a descriptive name for the secret
  - Domain: Enter the target domain or server address
  - Login: Enter the username or account name
  - API key: Enter or upload the API key
  - URL: Enter the related website or service URL
  - Description: Optional additional information (not encrypted)



For Certificate:

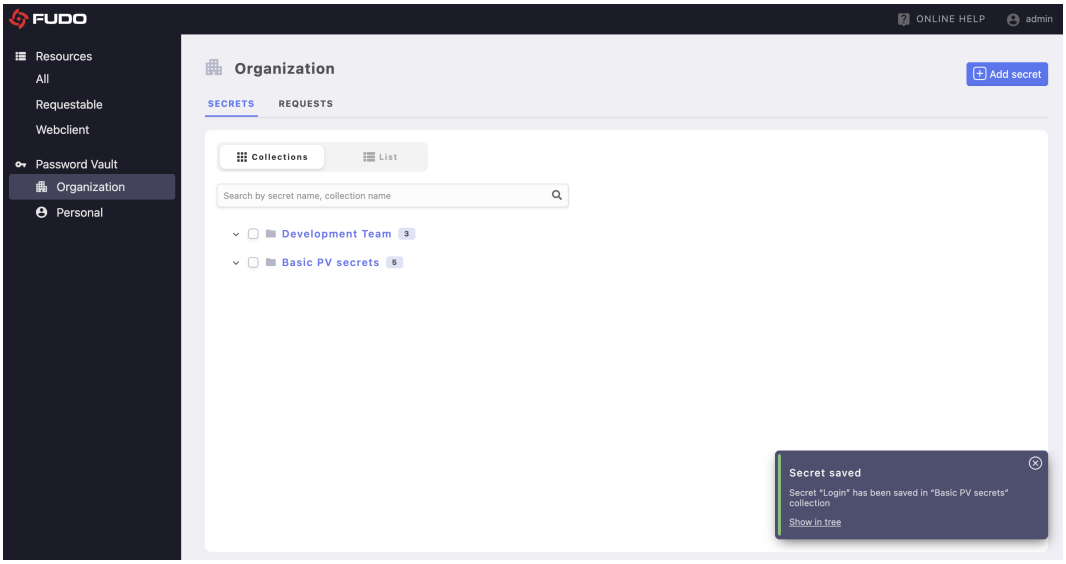
- Fill in the required fields:
  - Name: Enter a descriptive name for the secret
  - Certificate: Upload or generate certificate
  - Private Key: Upload your Private Key
  - URL: Enter the related website or service URL
  - Description: Optional additional information (not encrypted)



7. Click *Add* to create the secret and close the window, or *Add and configure* to create the secret and open its configuration window, where you can continue the setup.

Success Confirmation:

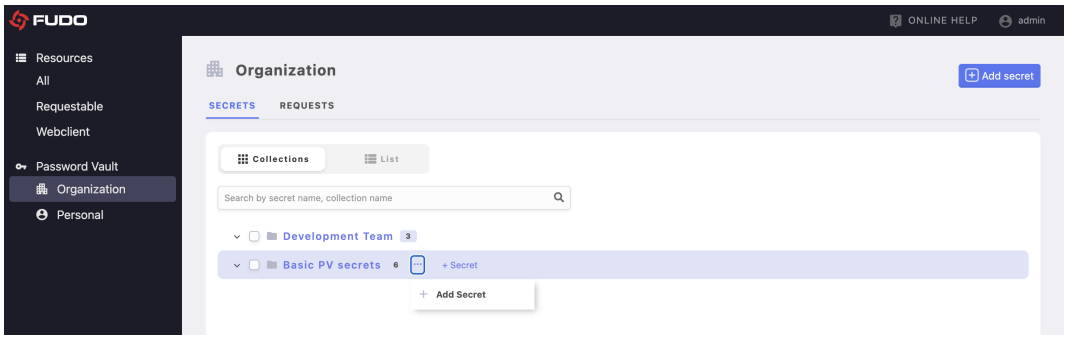
After creating a secret, you will see a confirmation message and the collection's secret count will be updated:



Alternative Creation Methods:

You can also create secrets using quick actions:

1. **From Collection Hover Menu**: Hover over a collection and click *+ Secret*
2. **From Context Menu**: Click the three-dot menu (...) on a collection and select **Add Secret**



7.4.2 Accessing Secret Editing

Secrets can be edited to update their information, change passwords, modify URLs, or update descriptions. There are multiple ways to access and edit secrets in the Password Vault.

Method 1: From Collections View

1. Navigate to the collection containing the secret.
2. Expand the collection to view its secrets.
3. Click on the secret name to edit.

Method 2: From List View

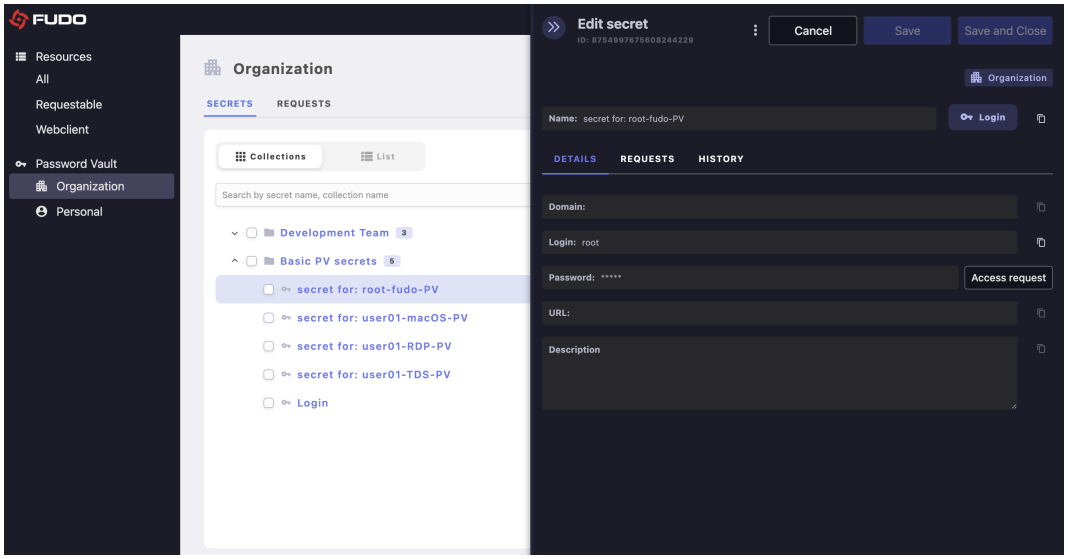
1. Select *Password Vault* > *Organization* or *Personal*.
2. Click *List* to switch to list view.
3. Click on the secret name to open the edit panel.

Edit Secret Panel

The secret edit panel provides comprehensive editing capabilities with the following tabs:

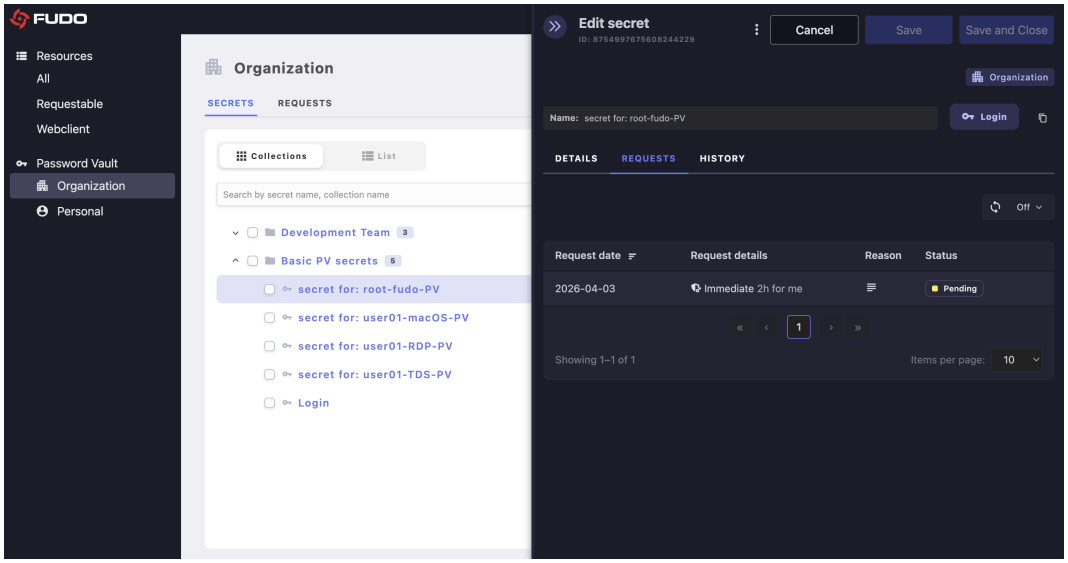
DETAILS TAB

The Details tab is the main editing interface for secret information where you can modify all core attributes of the secret.



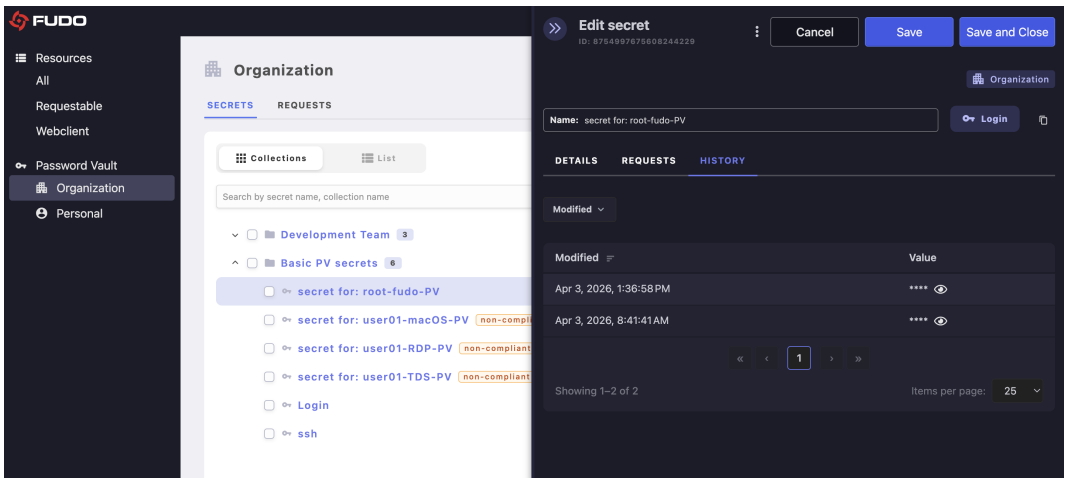
REQUESTS TAB

The REQUESTS tab allows you to review access requests related to the selected secret.



HISTORY TAB

The HISTORY tab allows you to track changes made to the selected secret over time.



7.4.3 Moving Secrets Between Collections

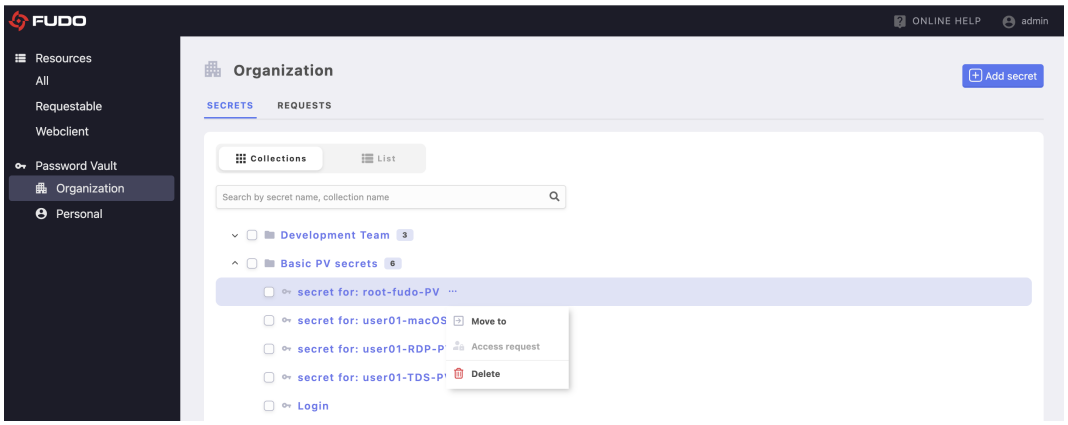
Secrets can be moved between collections to reorganize your password vault structure, adjust access permissions, or reflect changes in team organization. Moving secrets updates their access control based on the target collection's permissions.

> **Note**
>
> Moving a secret to a different collection will change its access permissions based on the target collection's user and role assignments.

There are several methods to move secrets between collections:

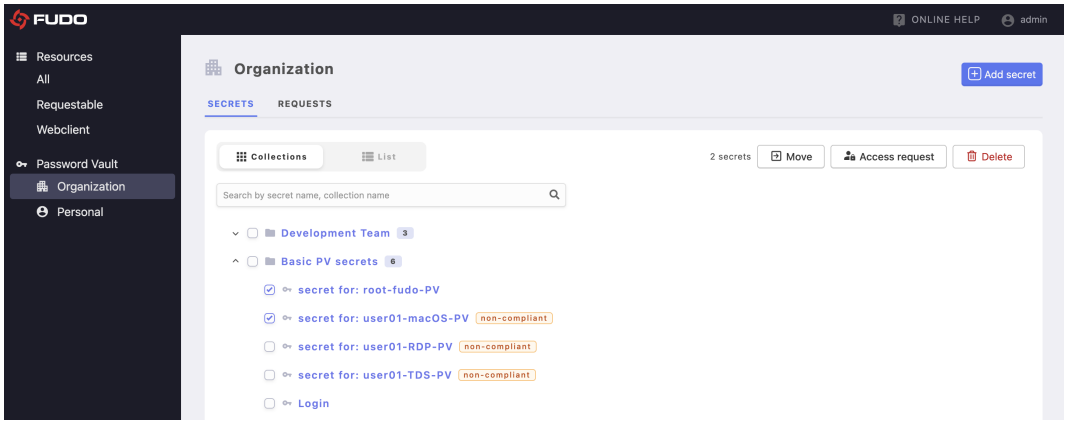
Method 1: Moving Using Context Menu

1. Hover over the secret you want to edit to reveal the options menu.
2. Click the three dots (...) button to open the context menu.
3. Select *Move to*.
4. Select the target collection from the tree structure.
5. Click *Select* to confirm the move operation.



Method 2: Bulk Move in Collections View

1. Select *Password Vault* > *Organization* or *Personal*.
2. In *Collections* view, select multiple secrets by checking their checkboxes.
3. Click the *Move* button that appears in the action bar.
4. Select the target collection from the tree structure.
5. Click *Select* to confirm the move operation.



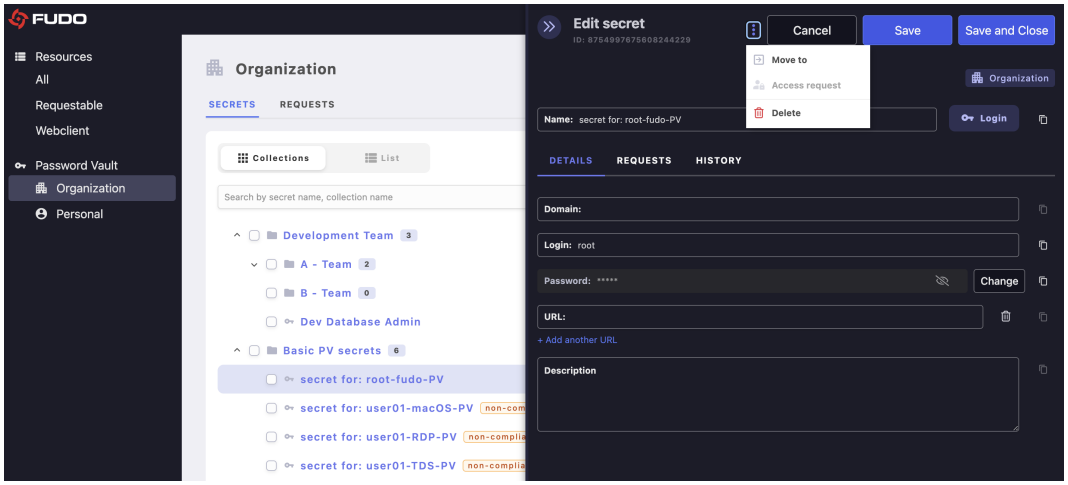
Method 3: Bulk Move in List View

This method allows you to move multiple secrets at once.

1. Select *Password Vault* > *Organization* or *Personal*.
2. Click *List* to switch to list view.
3. Select the checkboxes next to the secrets you want to move.
4. Click the *Move* button that appears in the action bar.
5. Select the target collection from the tree structure.
6. Click *Select* to confirm the move operation.

Method 4: Moving During Edit

1. Open any secret for editing.
2. Click the three dots (...) button next to the secret ID In the edit panel and select *Move to*.
3. Select the target collection from the tree structure.
4. Click *Select* to confirm the move operation.
5. Save the secret.



Related topics:

- *Adding a New Secret*
- *Accessing Secret Editing*

7.4.4 Reveal Secret

Users with **View** or **Full Edit** permission can reveal and copy secret values directly from the selected secret.

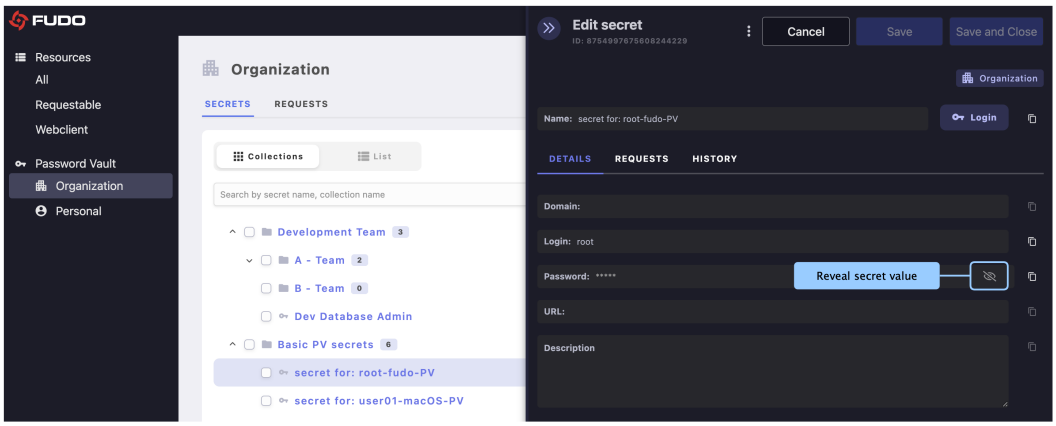
Reveal Hidden Values

To reveal secret:

1. Click the name of the selected secret to open the secret edit panel.
2. Locate the field containing the secret value for the selected secret type.

> **Note**
>
> For security reasons, secret values are hidden by default and are revealed only when you choose to display them.

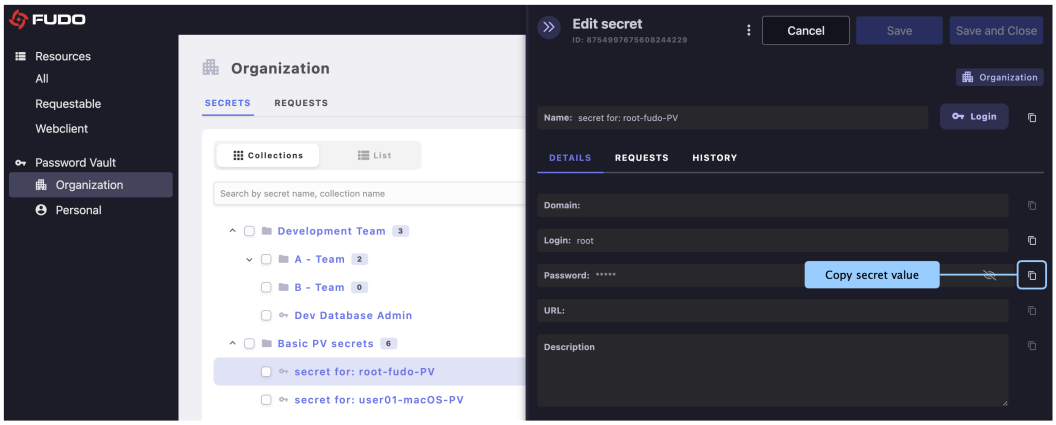
3. Click the **eye icon** next to the secret value field.
4. The secret becomes visible in plain text.
5. Click the eye icon again to hide it.



Copy Values

To copy secret value:

1. Click the name of the selected secret to open the secret edit panel.
2. Locate the field containing the secret value for the selected secret type.
3. Click [copy] icon next to the secret value field.
4. The value is copied to your clipboard.



Note

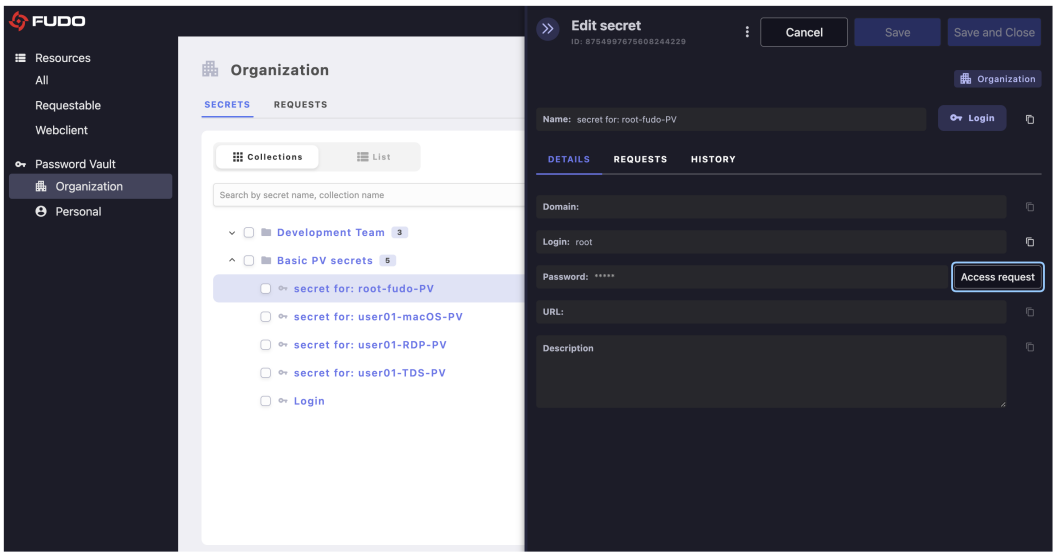
- Each reveal and copy action is logged for security auditing purposes.
- If you do not have **View** or **Full Edit** permission for a secret, see *Requesting Access to a Secret*.

7.4.5 Requesting Access to a Secret

Users with **View on Request** permission cannot view secret values directly. To access them, they must submit a request from the selected secret. Secret values can be viewed only after approval by an administrator.

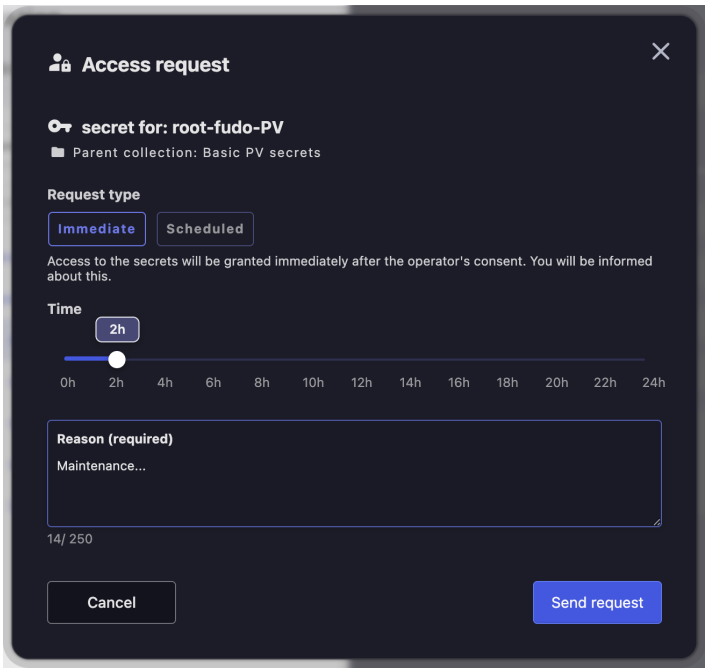
To request access to a secret:

1. Click the name of the selected secret to open the secret edit panel.
2. Click the **Access request** button.



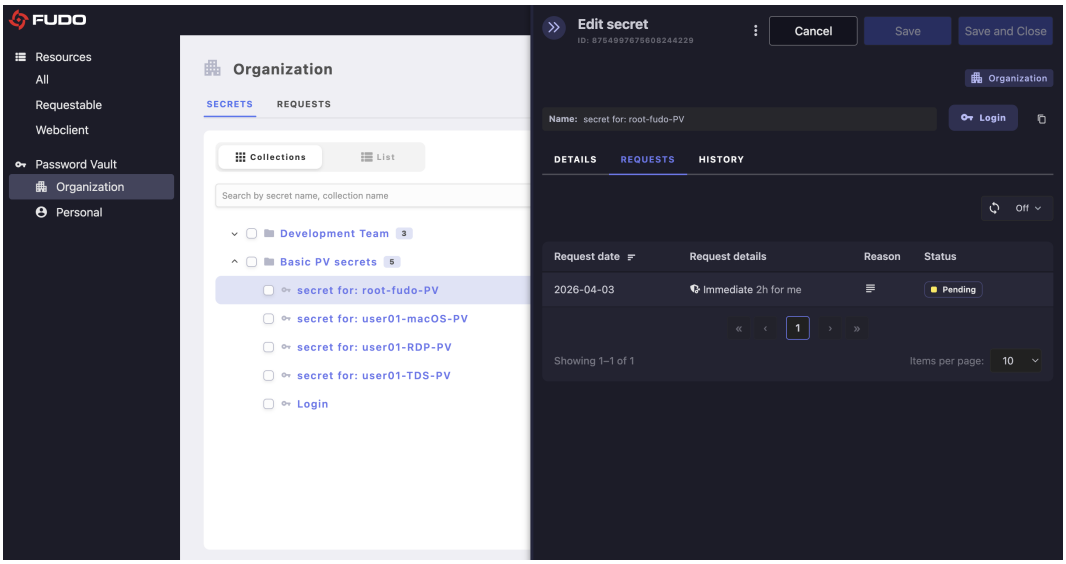
3. In the request window, configure the following fields:
   - **Request type** – select **Immediate** or **Scheduled**
   - **Time** – specify the requested access time

- **Reason** – enter the reason for the request (required)



4. Click **Send request**.

After sending the request, you can track its status in the **REQUESTS** tab of the selected secret.



7.4.6 Deleting Secrets

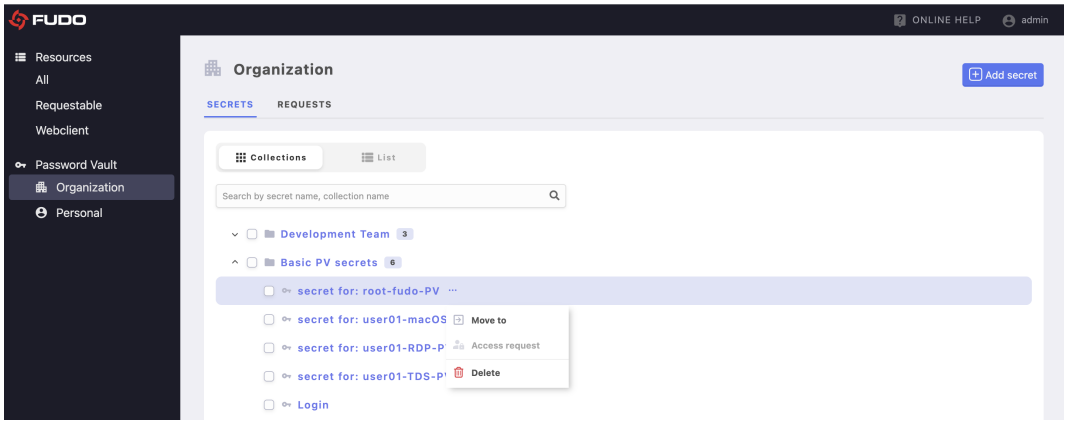
Secrets can be deleted when they are no longer needed or when credentials have been decommissioned. Before deleting secrets, ensure you understand the impact on users and applications that may depend on them.

> **Warning**
>
> Deleting a secret is a permanent action that cannot be undone. Ensure you have backups or alternative access methods before proceeding with deletion.

There are several methods to delete secrets from the Password Vault:

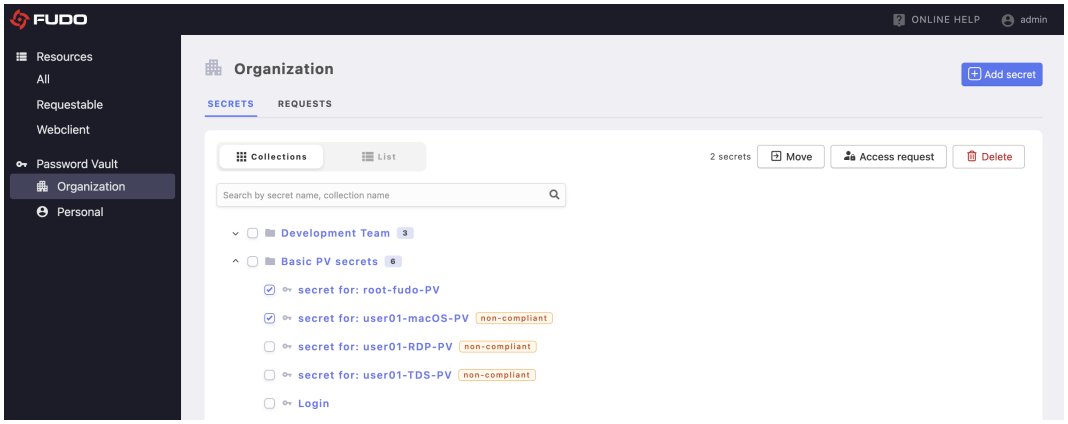
Method 1: Using Context Menu

1. Hover over the secret you want to delete to reveal the options menu.
2. Click the three dots (...) button to open the context menu.
3. Select *Delete*.
4. Confirm the deletion in the warning dialog.



Method 2: Bulk Delete in Collections View

1. Select *Password Vault* > *Organization* or *Personal*.
2. In *Collections* view, select multiple secrets by checking their checkboxes.
3. Click the *Delete* button that appears in the action bar.
4. Review the warning message and confirm the deletion.



Method 3: Bulk Delete in List View

This method allows you to delete multiple secrets at once.

1. Select *Password Vault* > *Organization* or *Personal*.
2. Click *List* to switch to list view.
3. Select the checkboxes next to the secrets you want to delete.
4. Click the *Delete* button that appears in the action bar.
5. Review the warning message and confirm the deletion.

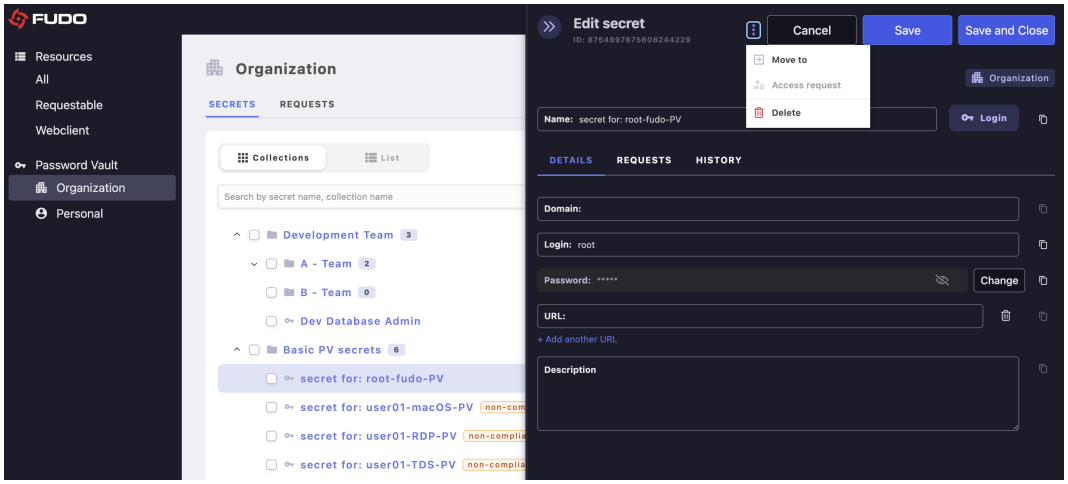
Method 4: Bulk Delete in List View

This method allows you to delete multiple secrets at once.

1. Select *Password Vault* > *Organization* or *Personal*.
2. Click *List* to switch to list view.
3. Select the checkboxes next to the secrets you want to delete.
4. Click the *Delete* button that appears in the action bar.
5. Review the warning message and confirm the deletion.

Method 4: Delete from Edit Panel

1. Open any secret for editing.
2. Click the three dots (...) button next to the secret ID in the edit panel.
3. Select *Delete* from the dropdown menu.
4. Confirm the deletion in the warning dialog.



Related topics:

- *Adding a New Secret*
- *Accessing Secret Editing*

7.4.7 Password Policy Compliance

Password security policies can be configured in the system to help maintain organizational standards.

> **Note**
>
> A secret is marked with the `non-compliant` compliance indicator if it violates one or more policies.

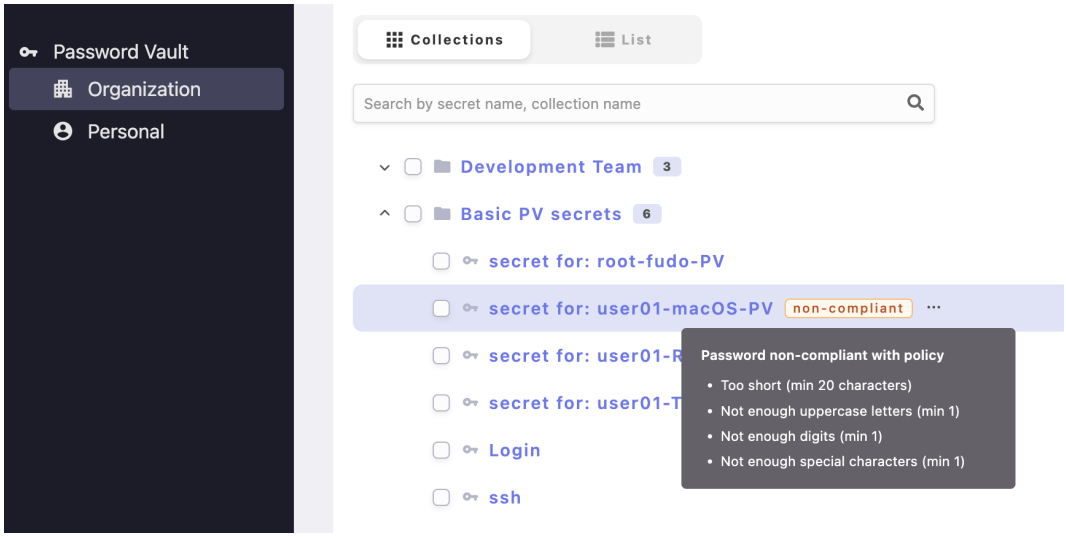
Common Policy Violations

A secret becomes non-compliant when:

- Password is too short (minimum length requirement)
- Lacks required character types (uppercase, lowercase, numbers, symbols)
- Password has expired based on rotation schedule
- Matches known breached passwords
- Reuses a previous password

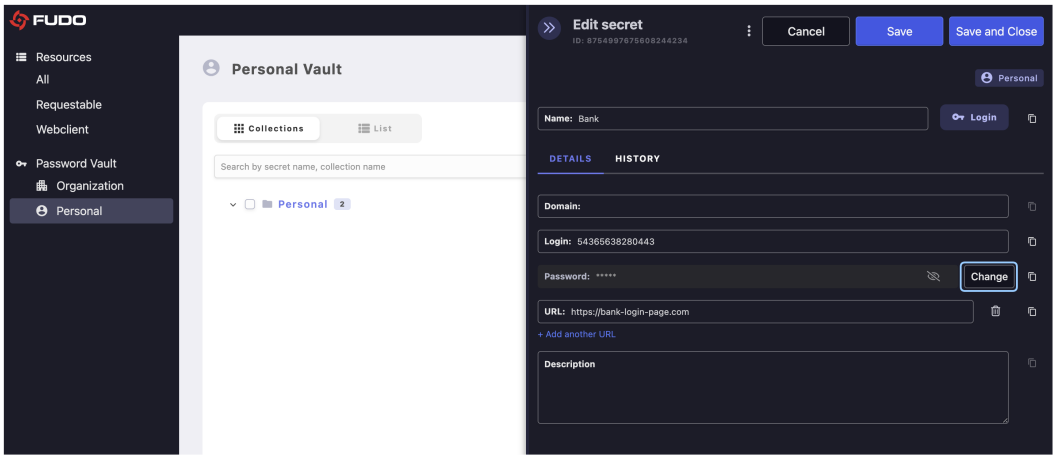
To see which policy requirements a secret violates:

1. Hover over the `non-compliant` indicator to display a tooltip listing the policy requirements not met by that secret.

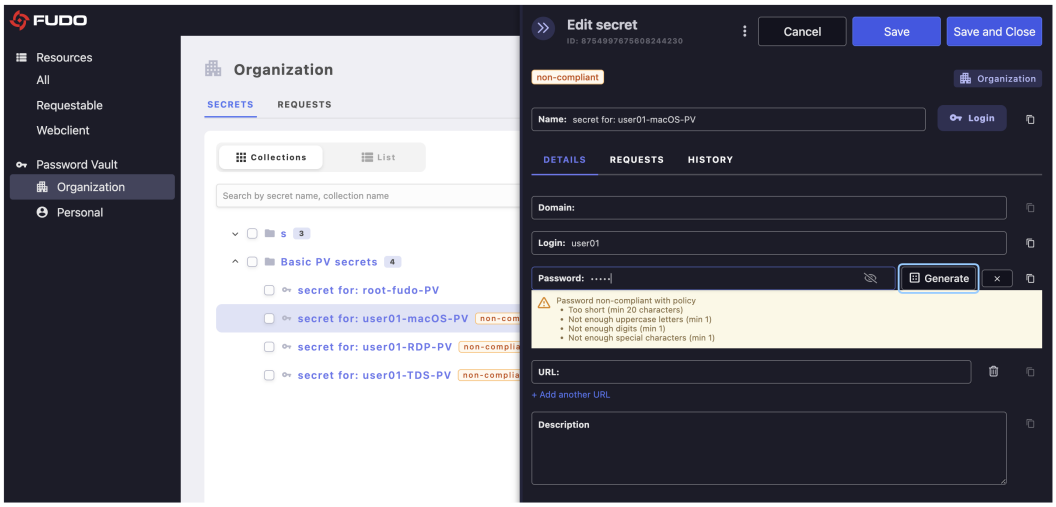


Fixing Non-Compliant Passwords

1. Open the non-compliant secret.
2. Click **Change**.



3. Either:
   - Click **Generate** for an automatic compliant password.
   - Manually create a password following the displayed requirements.



5. Save the changes.

7.5 Managing Collections (Personal Vault)

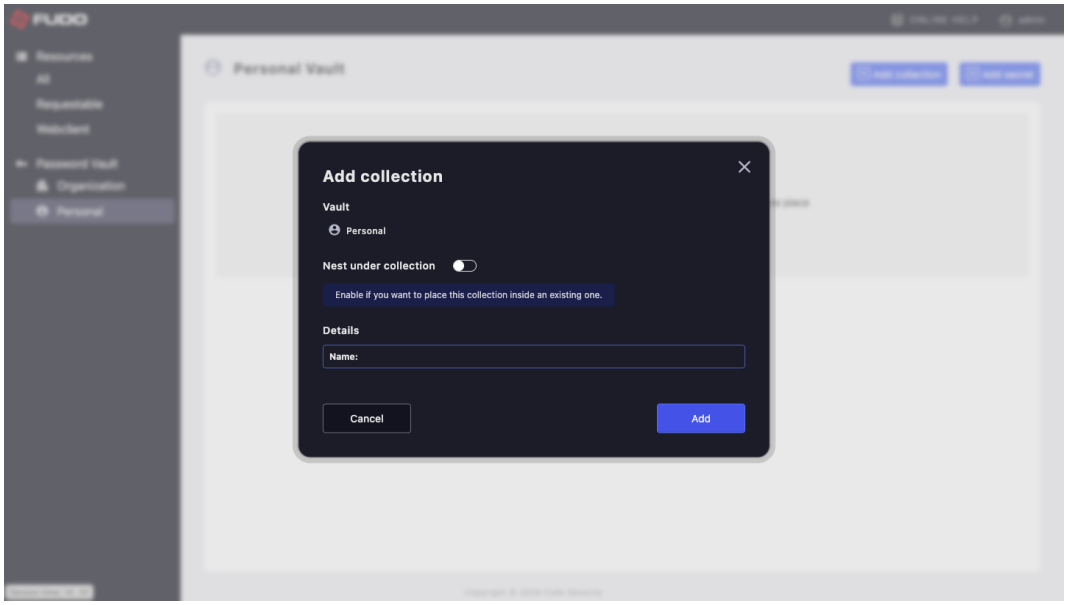
Collections help organize your personal secrets into logical groups. Collection management is only available in the Personal Vault through the User Access Gateway.

> **Note**
>
> **Collections can only be created and managed in the Personal Vault.** Organization Vault collections are managed by administrators through the main Fudo Enterprise system, not through the User Access Gateway.

7.5.1 Creating Collections

Collections help organize your personal secrets into logical groups.

1. Navigate to *Password Vault* > *Personal*.
2. Click *+ Add collection*.
3. The *Add collection* dialog opens.



4. *Name* (required) - Enter a descriptive collection name
5. *Nest under collection* (optional) - Toggle ON to place this collection inside an existing one:

- This creates a hierarchical structure
- Helps organize related collections

6. Click Add to create the collection

7.5.2 Editing Collection Name

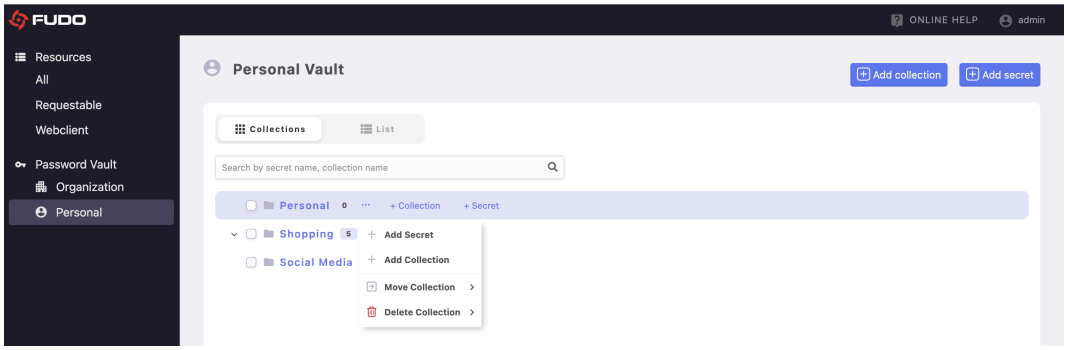
To edit an existing collection:

1. Navigate to the collection in your Personal Vault.
2. Click the collection to open the edit panel.
3. Modify the collection name.
4. Click *Save* to apply changes.
4. Click Save to apply changes.

7.5.3 Moving Collections

You can reorganize your collection hierarchy at any time:

1. Hover over the collection you want to move to reveal the options menu.
2. Click the three dots (...) button to open the context menu.
3. Select *Move Collection* from the context menu.
4. You can then choose whether to move only the contents of the collection or the collection together with its contents.



5. In the dialog, select the target collection under which the collection will be nested, or to which its contents will be moved.
6. Click *Select* to permanently remove the collection.

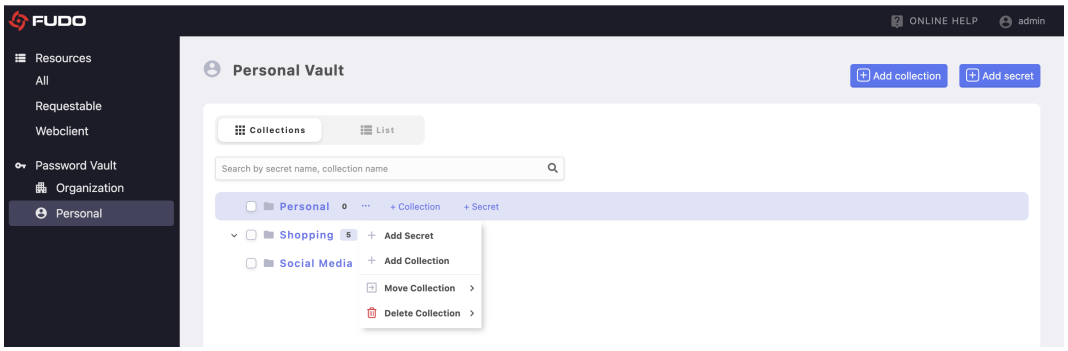
7.5.4 Deleting Collections

Collections can be deleted when they are no longer needed. Before deleting a collection, ensure that all important secrets are moved to other collections or backed up, as this action cannot be undone.

Warning

Deleting a collection is a permanent action that cannot be undone. All secrets within the collection will also be deleted unless moved to another collection first.

1. Hover over the collection you want to delete to reveal the options menu.
2. Click the three dots (...) button to open the context menu.
3. Select *Delete Collection* from the context menu.
4. You can then choose whether to delete only the contents of the collection or the collection together with its contents.



5. In the confirmation dialog, review the collection name.
6. Click *Delete* to permanently remove the collection.

Warning

Deleting a parent collection affects all nested collections.

CHAPTER 8

Establishing Connections

8.1 Connecting via Access Request

You can send a request for access to the resources via the User Access Gateway. There are available two types of the access requests: immediate and scheduled.

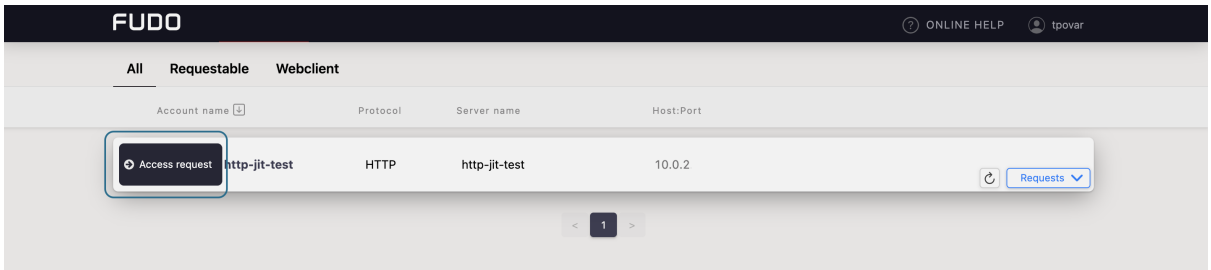
Immediate requests can be set from now up to the next 24 hours. When an immediate request is sent, its access time starts when the request is accepted. Then, you have 24 hours to start your session. When you start the session, the system counts the session time, which was requested, and terminates connection when the requested session time is over. If you do not use the access and do not connect for 24 hours after access is granted, the access becomes expired.

The scheduled type of requests requires selecting a time period in the future, including exact time and date.

8.1.1 Sending Access Request

In order to send a request, follow the steps:

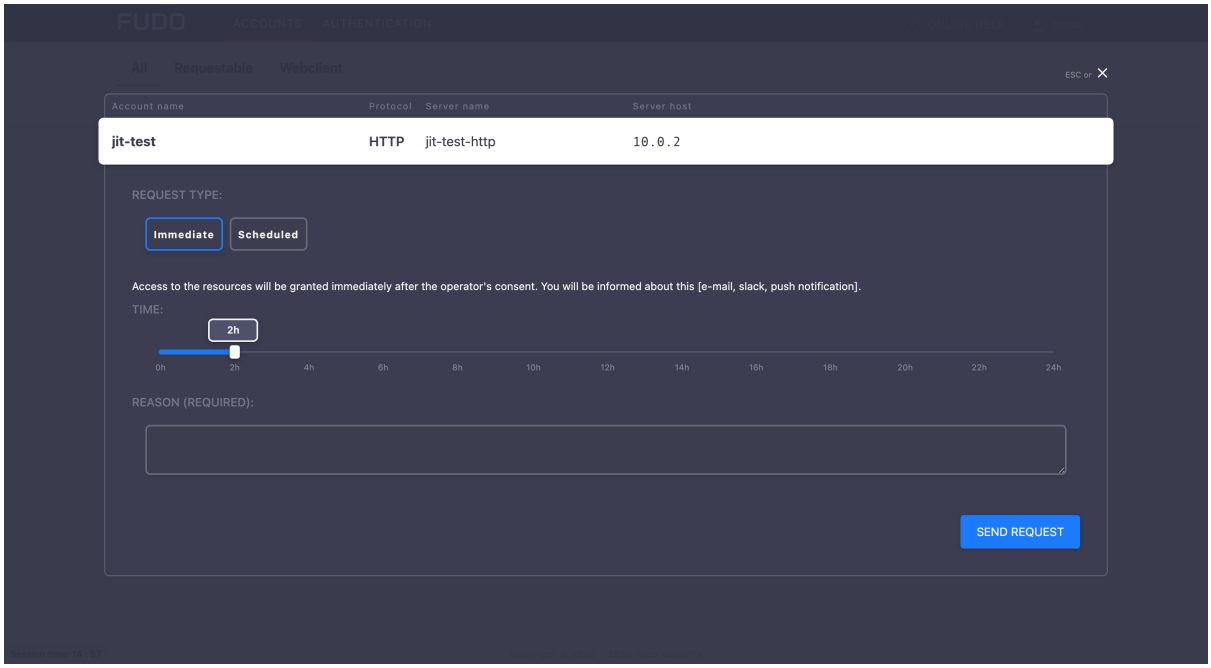
1. Hover the mouse over the particular account to see more options.
2. Click the *Access request* button.

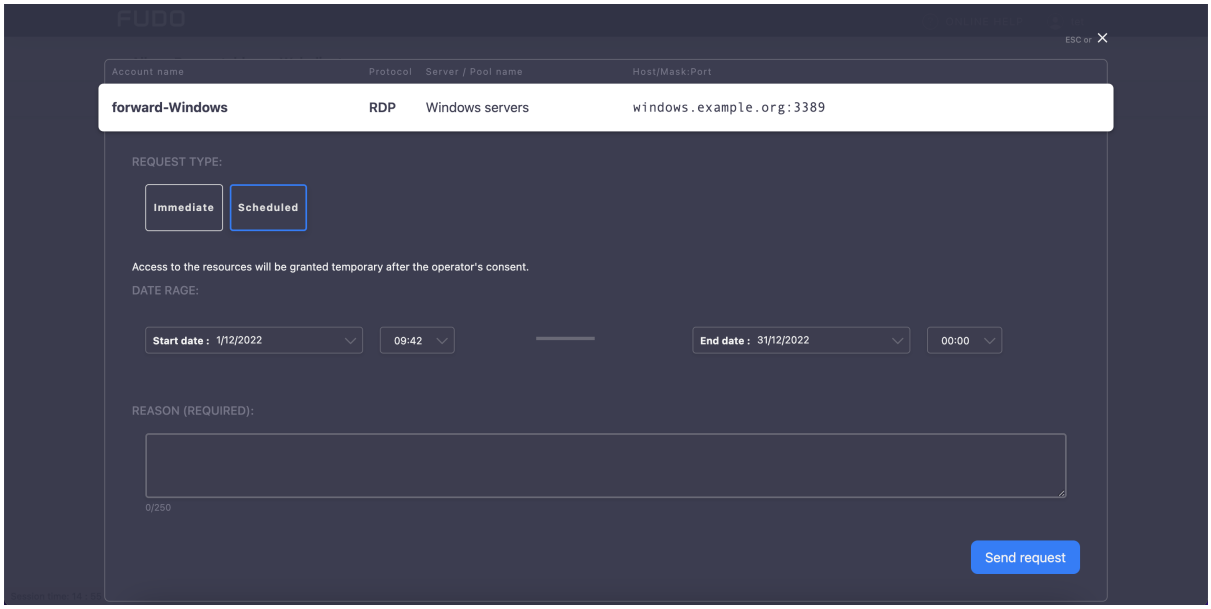


3. Select a type of the request: immediate or scheduled.

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

4. Define the request time.





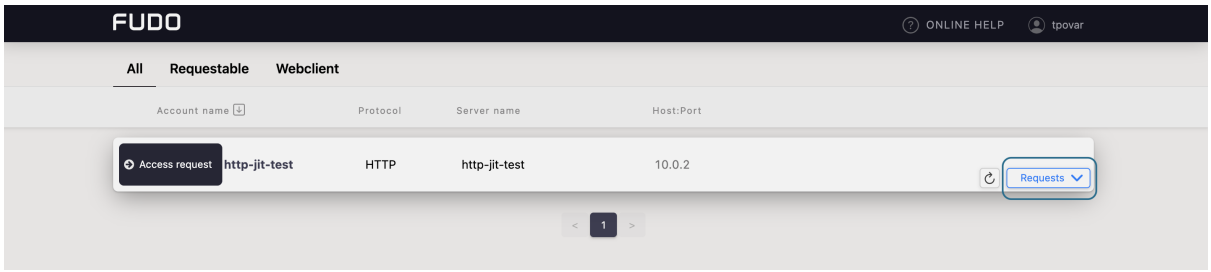
5. Click the *Send request* button.

8.1.2 Watching Request Status

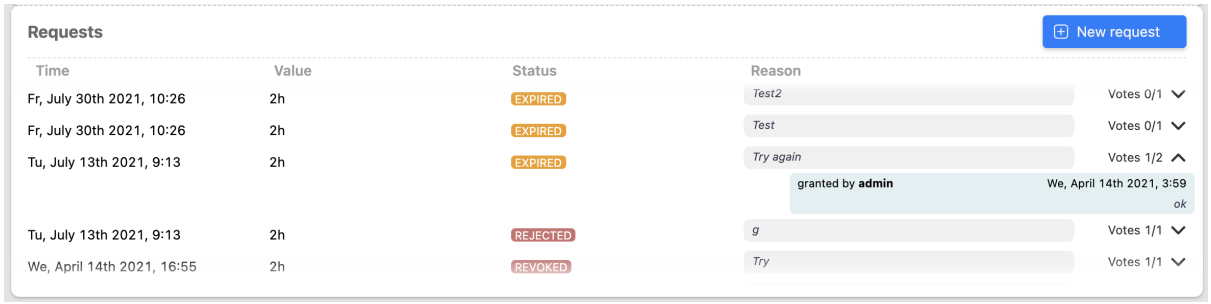
You can receive 2 types of e-mail notifications about your request:

- `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 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.



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.

8.2 Connecting Over RDP, VNC and SSH in Browser

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

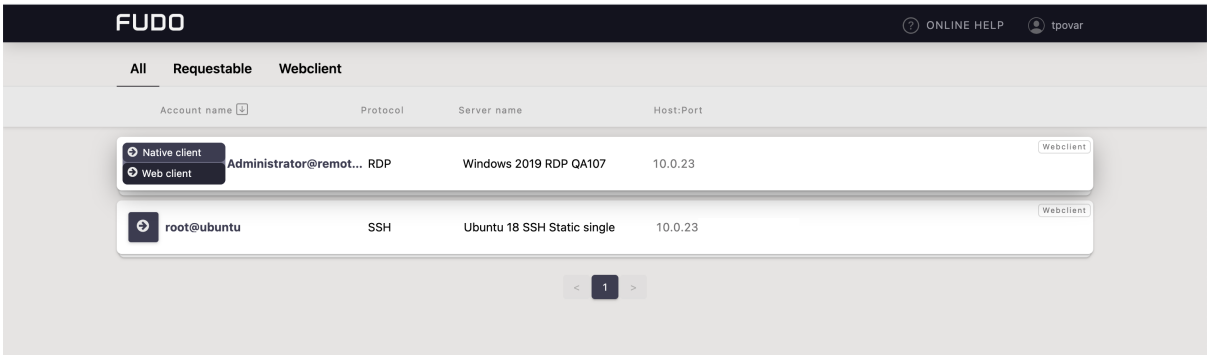
Note

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, VNC 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.



Note

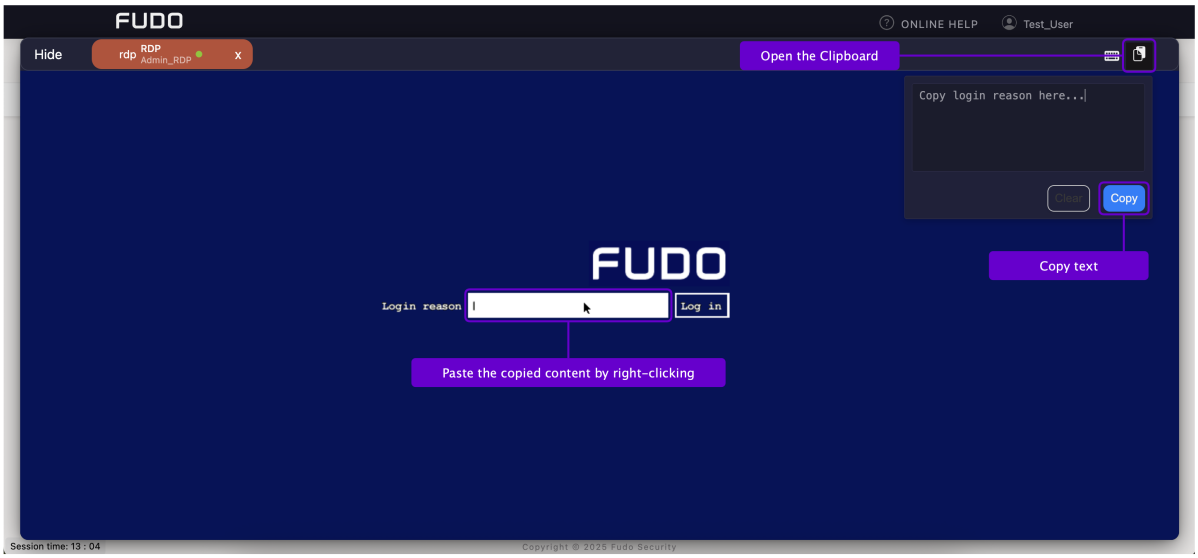
Each session is opened in a separate browser tab.

8.2.1 Providing a Login Reason in an RDP Session

If an RDP session is initiated using an account added to a Safe with the *Login reason* option enabled, the user will be prompted to provide a reason before logging in to the target system.

Pasting the Login Reason Text From the Clipboard:

To simplify entering the login reason, you can use the **Clipboard** feature available in the top-right corner of the User Portal interface.



1. Click the clipboard icon in the top-right corner of the screen.
2. Paste or type the text you want to use as the login reason.
3. Click the **Copy** button to move the text to the session clipboard.
4. Go to the field where the login reason must be entered.
5. To paste the text, **right-click** in the input field.

Note

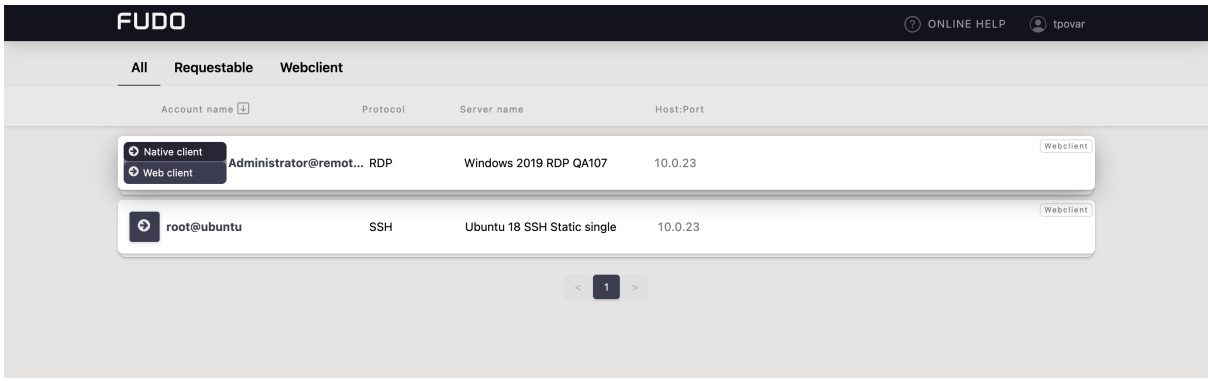
Keep in mind that the clipboard has a character limit for the **Login reason** field: a maximum of **60 characters** for Polish and English text, and **40 characters** for Cyrillic. If the copied text exceeds this limit, it may be truncated or not copied at all.

Related topics:

- *Webclient Features*
- *Connecting Over RDP on MAC OS X*
- *Connecting Over RDP on Microsoft Windows 7 and 10*
- *Connecting Over RDP on Ubuntu Linux*

8.3 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.

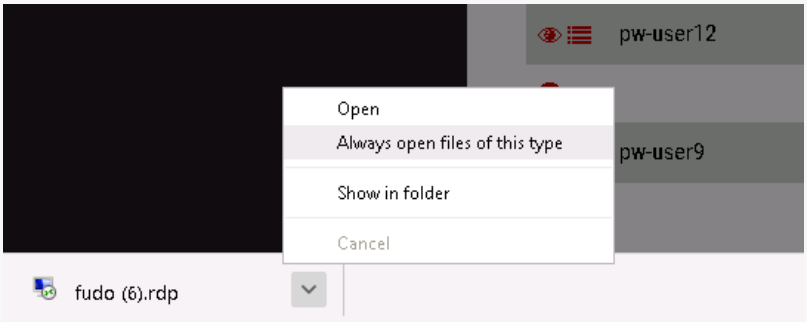


3. Choose the listener, via which you want to connect.

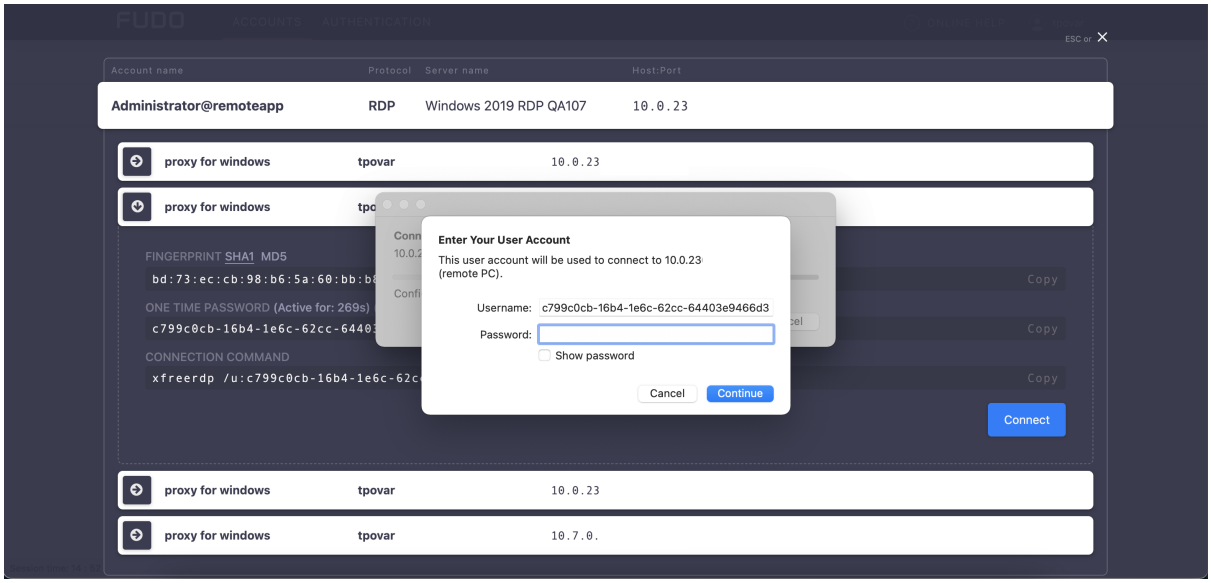
4. Click *Connect*.

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.

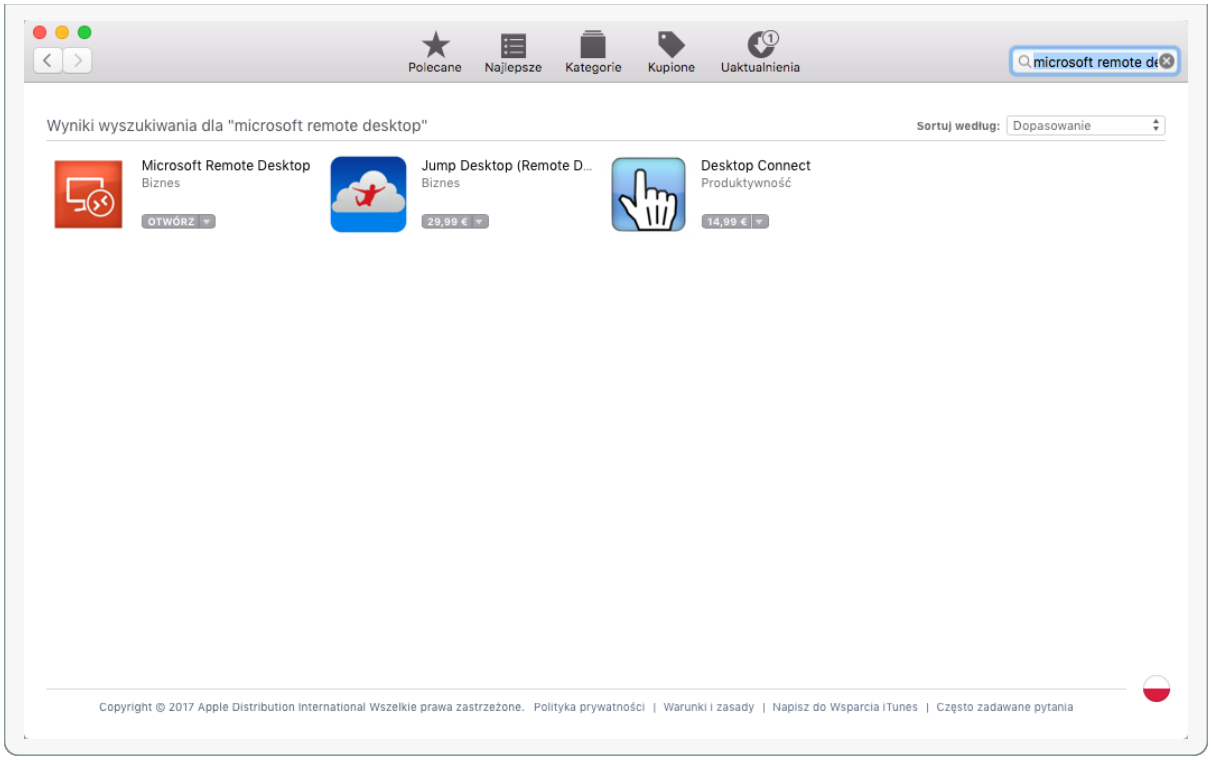
Related topics:

- *Connecting Over RDP on MAC OS X*
- *Connecting Over RDP on Ubuntu Linux*

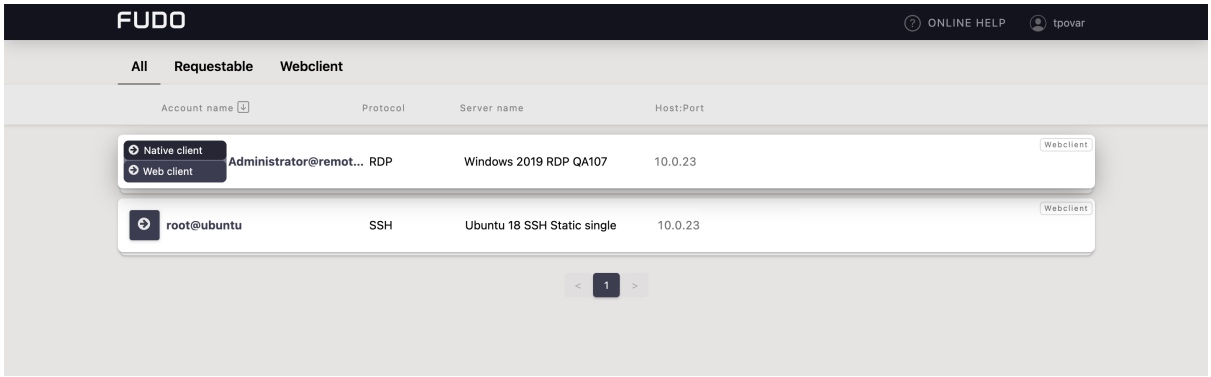
8.4 Connecting Over RDP on MAC OS X

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.

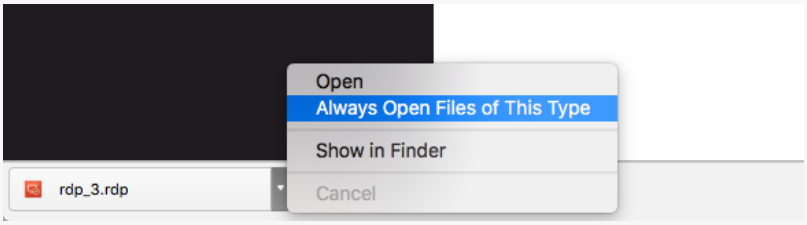


3. Choose the listener, via which you want to connect.

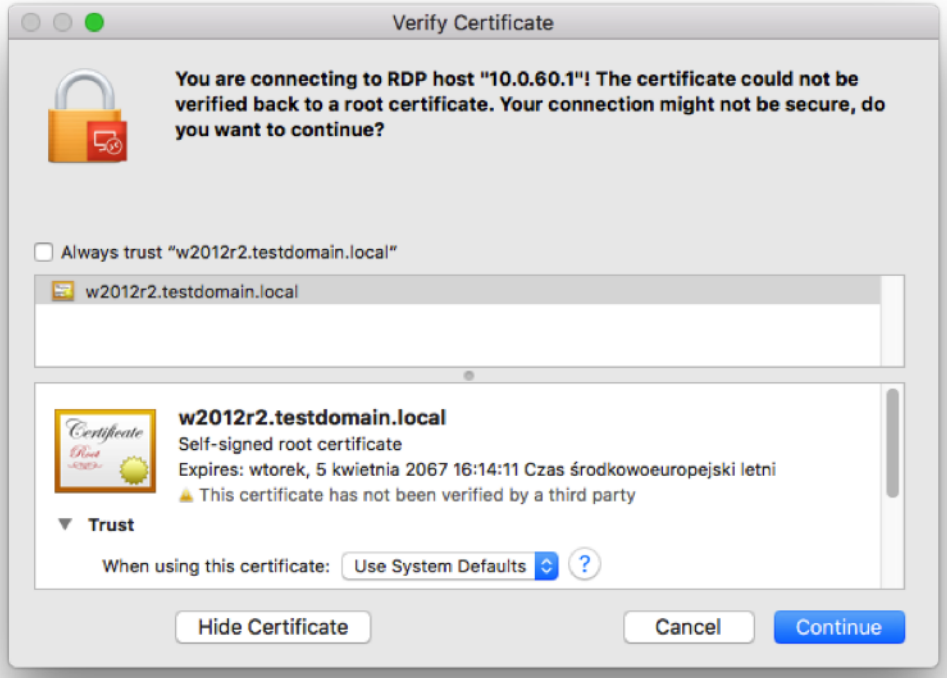
4. Click *Connect*.

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.



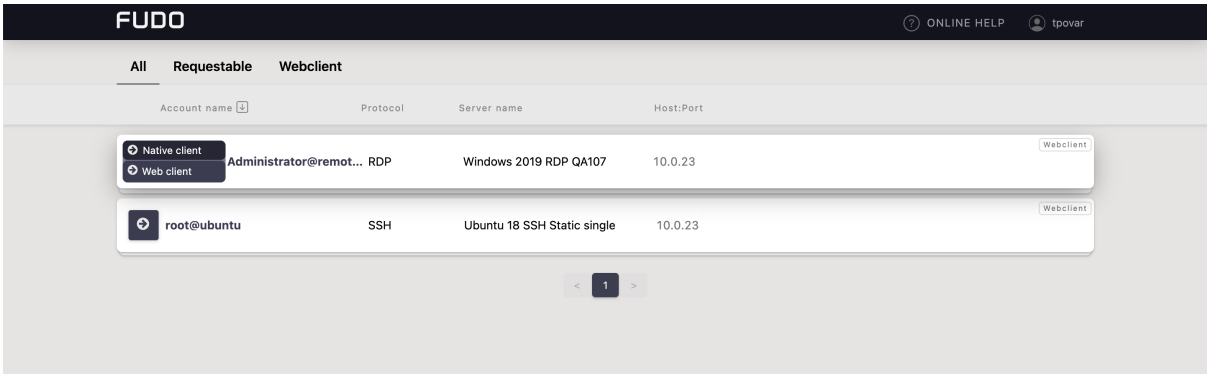
Related topics:

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

8.5 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*

8.6 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

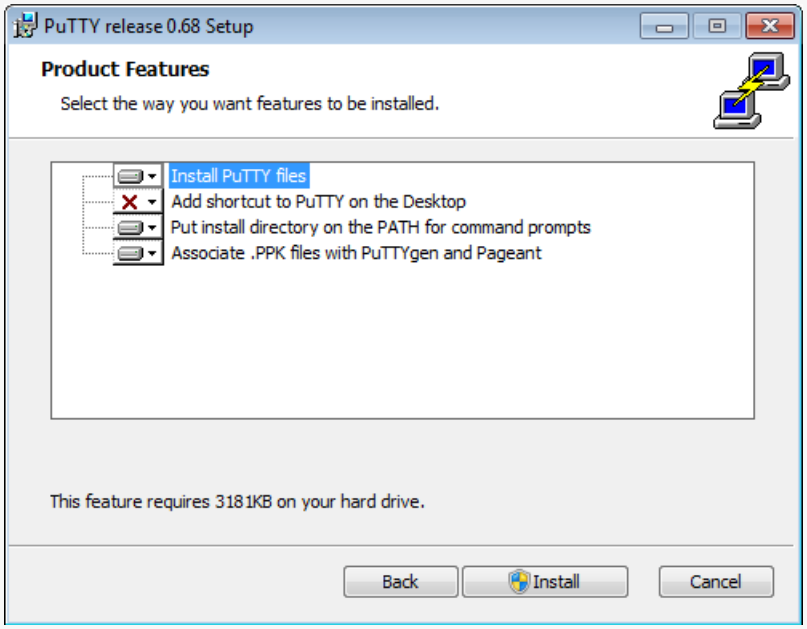
Verify the checksum value to make sure that the integrity of the binary file has not been compromised.

2. Download and install *PuTTY*.

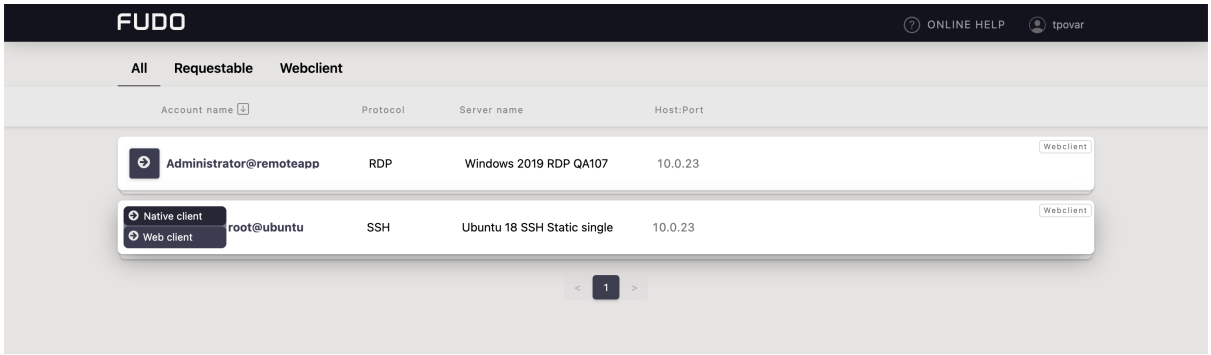
   `https://winscp.net/download/putty-0.75-installer.msi`

Note

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

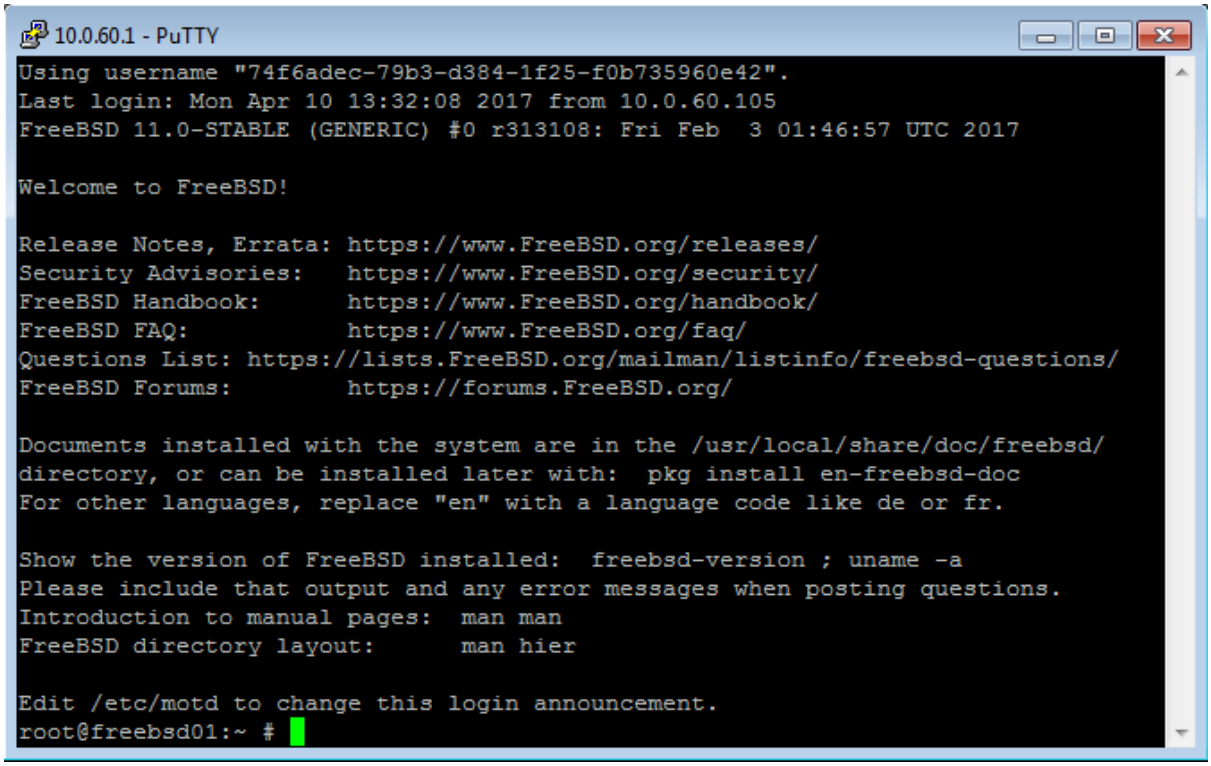


3. Log in to the User Access Gateway.
4. Find desired account and server, hover your mouse over to show more options.
5. Select the *Native client* button.



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.

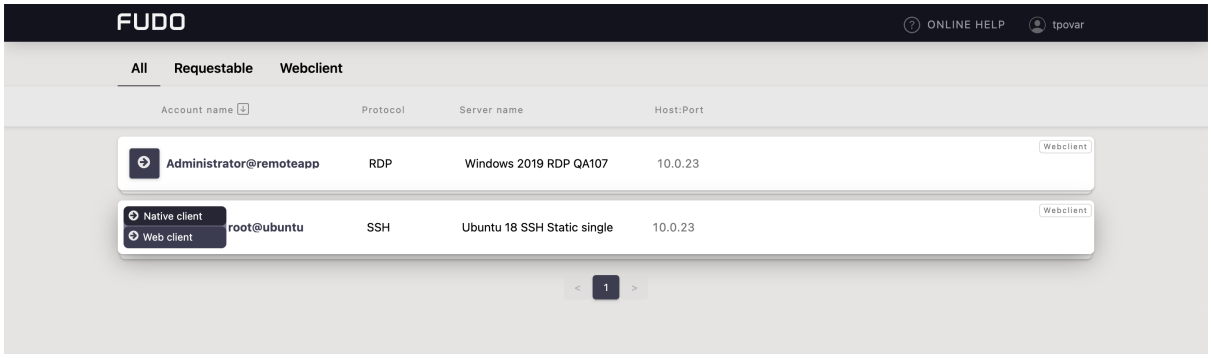


Related topics:

- *Connecting Over RDP on MAC OS X*
- *Connecting Over RDP on Microsoft Windows 7 and 10*
- *Connecting Over RDP on Ubuntu Linux*

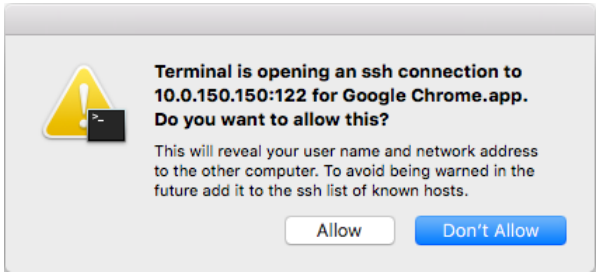
8.7 Connecting Over SSH on Mac OS, Linux

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:

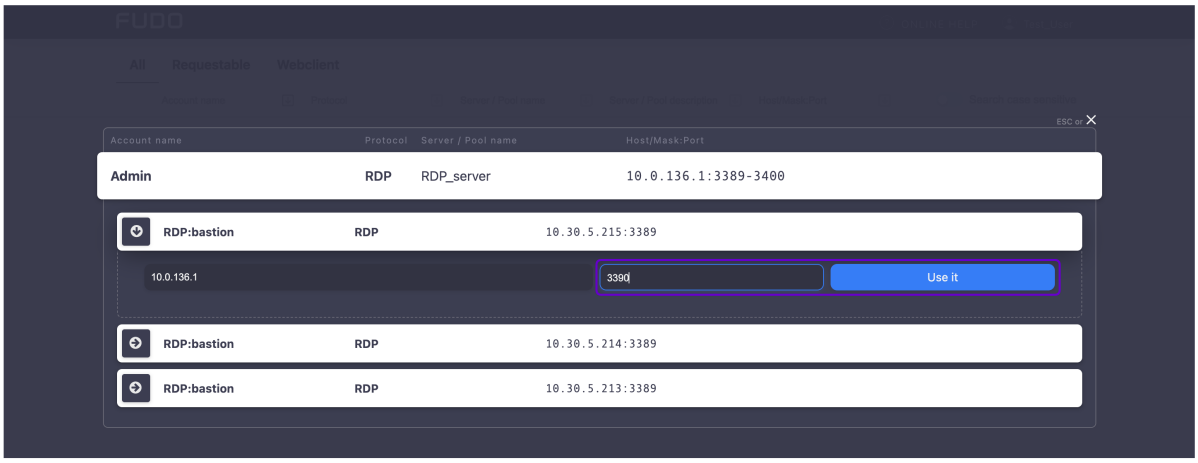
- *Connecting Over RDP on MAC OS X*
- *Connecting Over RDP on Microsoft Windows 7 and 10*
- *Connecting Over RDP on Ubuntu Linux*

8.8 Connecting to a Server with a Port Range

Native Client

After hovering over the account you want to use for the connection and selecting the Native Client option, follow these steps:

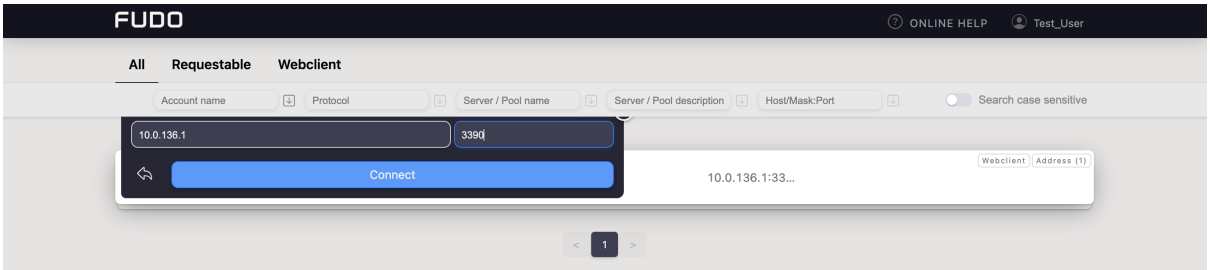
1. Select from the dropdown list the address of the server with a port range that you want to connect to (in case of a server pool).
2. In the **Port** field, enter a port selected from the range specified during the configuration of the given server.
3. Click the **Use** button.
4. Click the **Connect** button to retrieve or obtain the connection details for the appropriate server protocol.



Web Client

After hovering over the account you want to use for the connection and selecting the Web Client option, follow these steps:

1. Select from the dropdown list the address of the server with a port range that you want to connect to (in case of a server pool).
2. In the **Port** field, enter a port selected from the range specified during the configuration of the given server.
3. Click the **Connect** button to establish a connection in the browser.

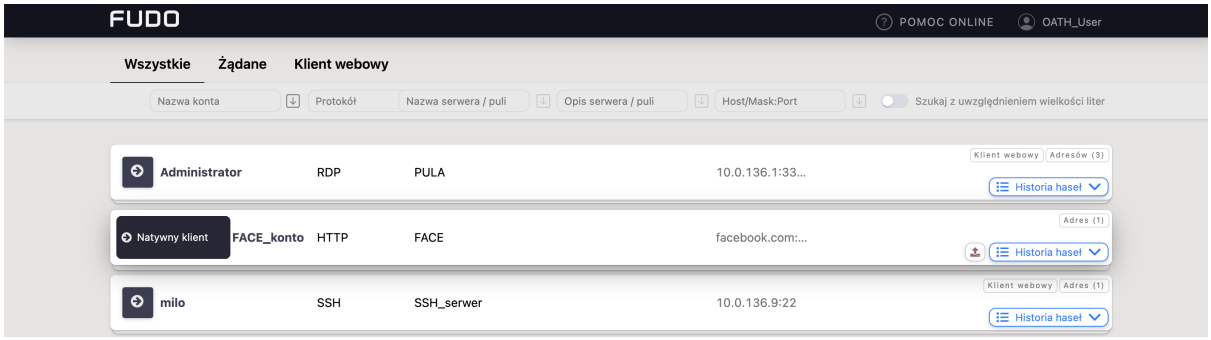


Related topics:

- *Connecting Over RDP on MAC OS X*
- *Connecting Over RDP on Microsoft Windows 7 and 10*
- *Connecting Over RDP on Ubuntu Linux*

8.9 Connecting via HTTP

1. Log in to the User Portal.
2. Find the account and server you want to connect to.
3. Hover over the account to see the available options.
4. Click the *Native client* button next to the selected account to connect to the target server.



5. Click *Connect*.

6. The connection will be established and you will be redirected to a new browser window.

Note

- With **version 5.6.4** (or the 5.6.3 hotfix), an HTTP session redirects the main browser window to the URL opened in the popup, instead of simply closing the popup window.
- If the redirected page does not load correctly, try reloading it using the **Ctrl + R** keyboard shortcut.
- Additionally, this behavior allows users to navigate back after the redirection. The keyboard shortcuts for navigating back depend on the browser and operating system, for example:
  - **Windows / Linux**: Left Alt + Left Arrow
  - **macOS (Chrome)**: Right Option + Left Arrow
  - **macOS (Edge / Safari)**: Right Option + Left Arrow

Related topics:

- *Webclient Features*
- *Connecting Over RDP on MAC OS X*
- *Connecting Over RDP on Microsoft Windows 7 and 10*
- *Connecting Over RDP on Ubuntu Linux*

CHAPTER 9

Webclient Features

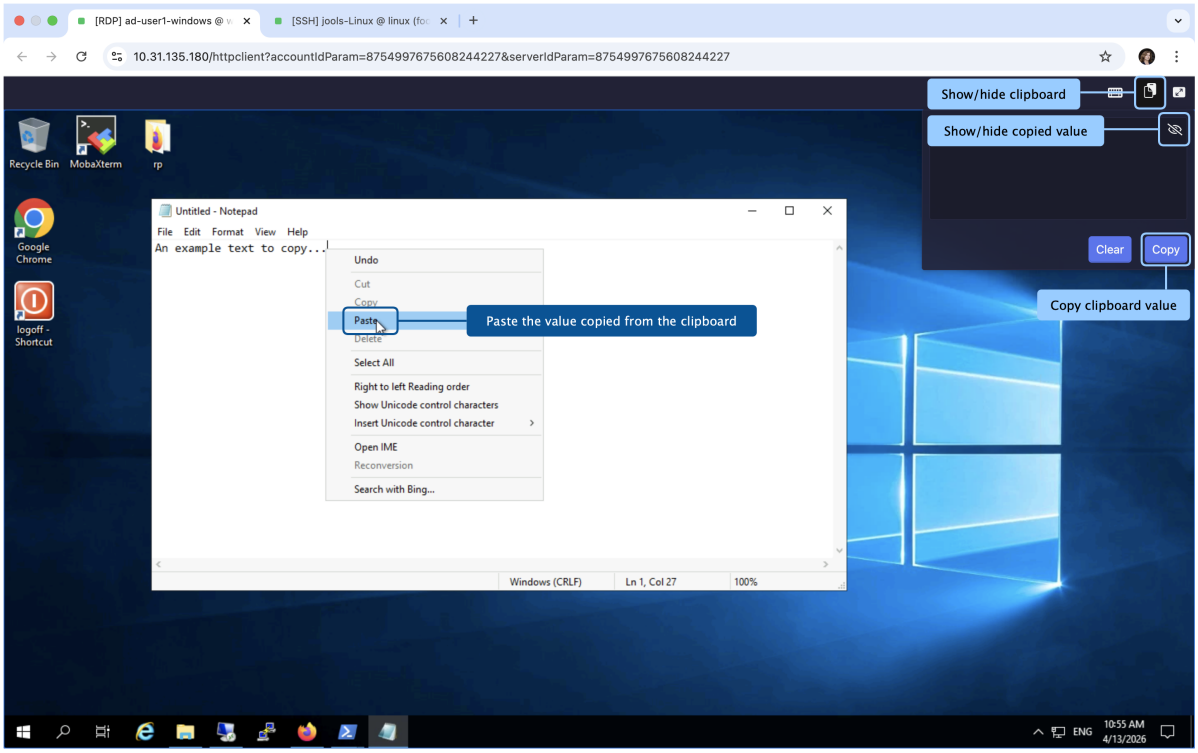
> **Note**
>
> The availability of toolbar elements depends on the protocol of the established session.

Available Webclient features:

- Browser tabs showing the protocol type, server name, account used to establish the session, and connection status:
  - connection is establishing,
  - session is connected,
  - session is disconnected.

> **Note**
>
> Full session information preview is available when you hover over the tab.

- The *Clipboard* button allows you to copy a piece of text to the system clipboard on the session server side. Just paste the text into the clipboard window and press *Copy*.
- Sensitive content in the Webclient clipboard can be hidden using the eye icon, allowing copied values such as passwords to be masked instead of displayed in clear text.



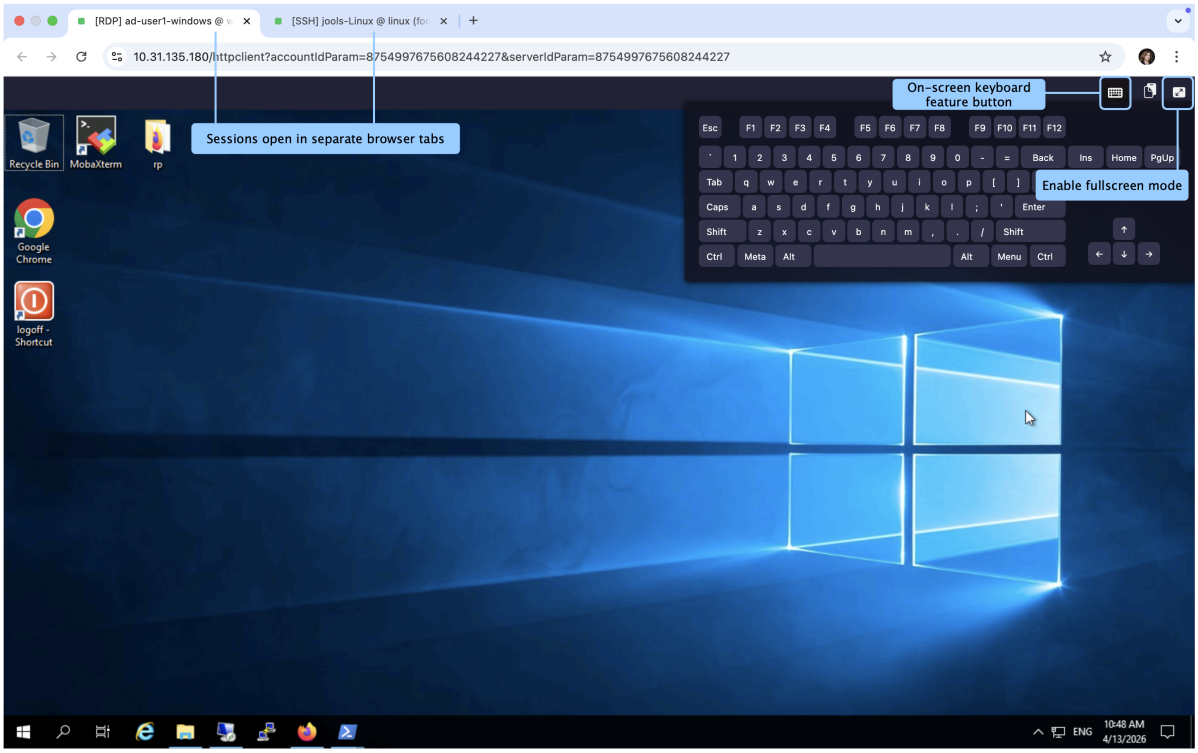
Note

Hovering over a particular tab shows the preview of the session.

- *On-screen keyboard* feature button.
- *Fullscreen Mode* button, which allows you to hide the Webclient toolbar and get a cleaner session view.

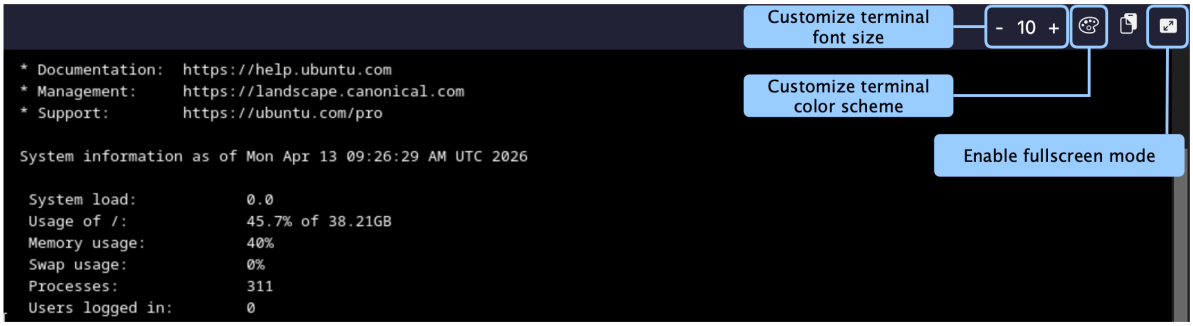
Note

Starting from version 6.0, Webclient sessions open in separate browser tabs, providing more space for the active session.



Additionally, for the sessions based on SSH protocol, there are features that allow customizing the view. You can change font size and a terminal color scheme. Four themes are available:

- black-white - default scheme,
- gray-black,
- green-black,
- white-black.



Related topics:

- *Connecting Over RDP, VNC and SSH in Browser*
- *Connecting Over RDP on MAC OS X*
- *Connecting Over RDP on Microsoft Windows 7 and 10*
- *Connecting Over RDP on Ubuntu Linux*

CHAPTER 10

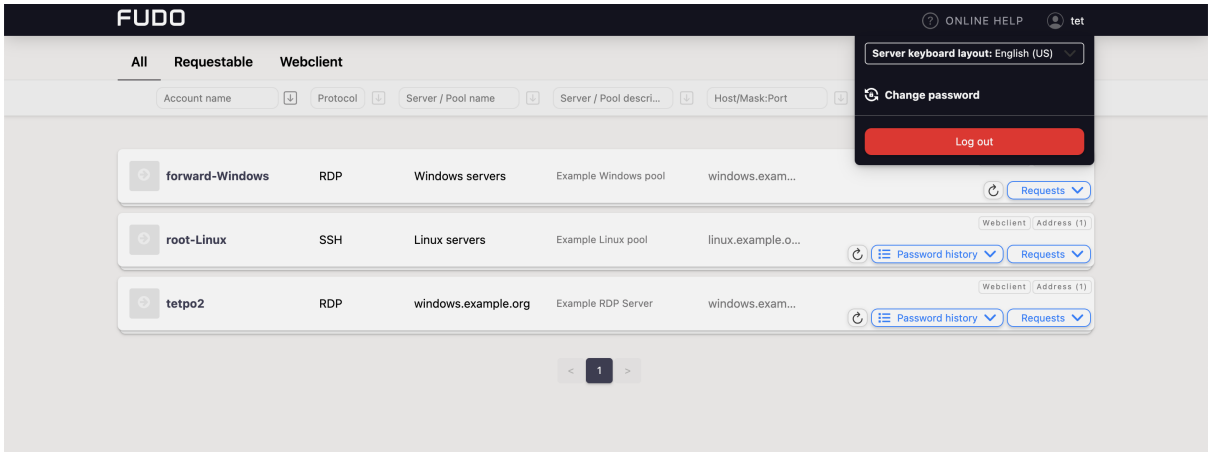
Change Password

Fudo Enterprise User Access Gateway allows changing a static password as well as a password enabled as a part of multi-factor authentication.

> **Note**
>
> A password change performed in UAG will also update the password stored in the User Directory when user synchronization is enabled. This functionality is available if we provide the credentials of an account with sufficient rights in the External Authentication method configuration in the Fudo Enterprise Admin Panel. For more information, see For more information, see the External Authentication configuration guide.

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*

CHAPTER 11

Troubleshooting

Problem	Symptoms and solution description
Cannot log in to the User 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 User 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.