Fudo Enterprise 6.3 - Access Gateway Manual

Fudo Security

29.10.2026

Contents

1 Table of Contents **1**
1.1 About Documentation . . . 1
1.2 System Overview . . . 1
1.3 Logging into the User Access Gateway . . . 3
1.4 Authentication Methods . . . 4
1.5 Fudo Officer App . . . 13
1.6 Secret Checkout and Checkin . . . 16
1.7 Displaying Passwords History . . . 17
1.8 Displaying and Editing Accounts Notes . . . 18
1.9 Password Vault . . . 19
1.10 Establishing Connections . . . 60
1.11 Webclient Features . . . 80
1.12 Sharing Your Session . . . 85
1.13 Troubleshooting . . . 87

CHAPTER 1

Table of Contents

1.1 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:

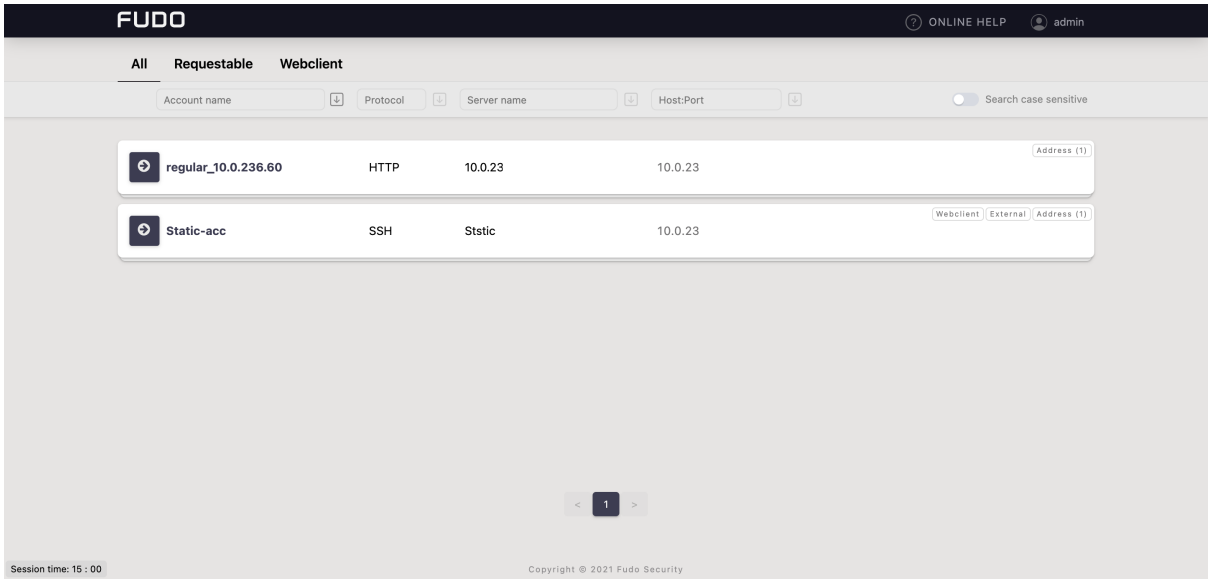
> **Note**
>
> Note field usually contains additional information closely related with described topic, e.g. suggestion concerning given procedure step; additional conditions which have to be met.

- Warning field:

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

1.2 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)`,
  - `French` (AZERTY),
  - `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, kazakh, german, uzbek, italian and french.

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*
- *Authentication Methods*
- *Troubleshooting*

1.3 Logging into the User Access Gateway

Note

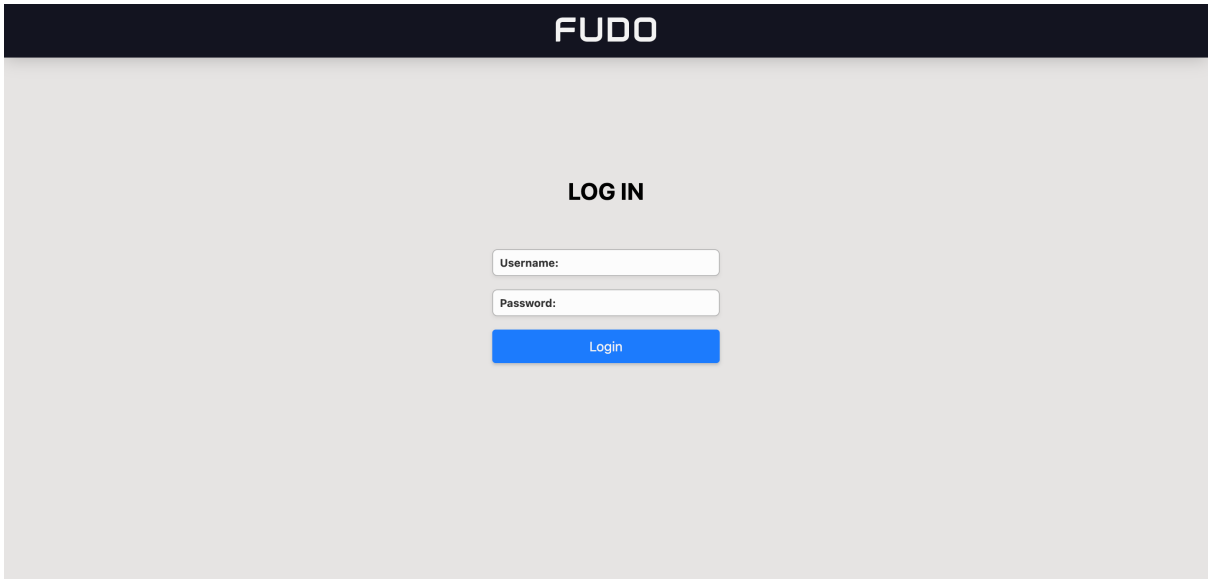
- User Access Gateway is compatible with Google Chrome, Mozilla Firefox, and Microsoft Edge on Microsoft Windows, Ubuntu, and macOS.
- User Access Gateway supports Single Sign On for Active Directory accounts. Refer to system documentation for information on how to enable the SSO in Access Gateway.
- User Access Gateway supports login via Azure or Okta. Authorized administrators can configure OpenID Connect globally for the entire 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*

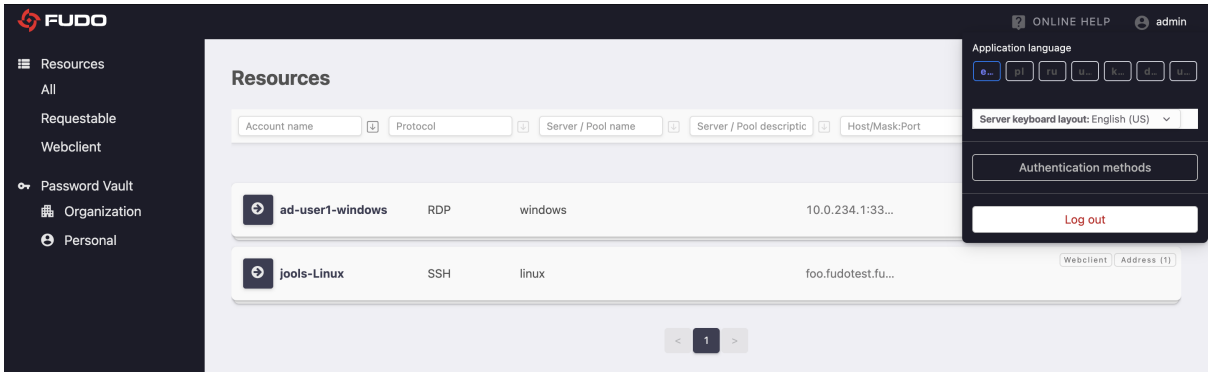
1.4 Authentication Methods

The User Access Gateway allows users to configure their own authentication methods, including multi-factor authentication options like OATH and FIDO2/Passkey.

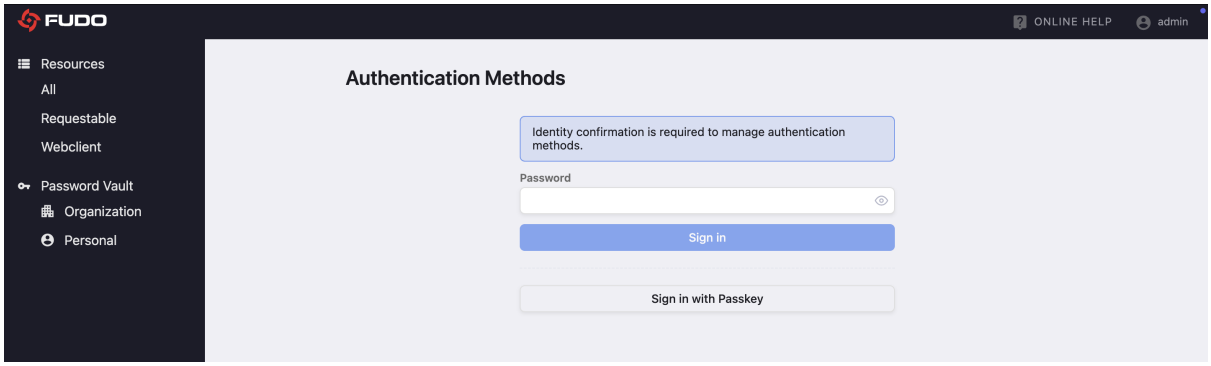
1.4.1 Accessing Authentication Method Management

To access authentication method settings:

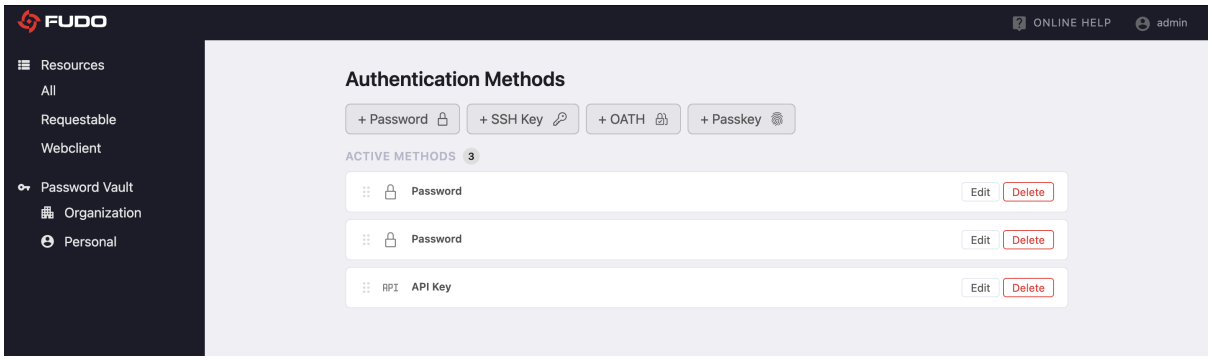
1. Log in to the User Access Gateway
2. Open the user menu in the upper-right corner
3. Click *Authentication methods*



4. Enter your current password to access the settings



After authentication, you will see a list of your current authentication methods and the ability to add new ones.



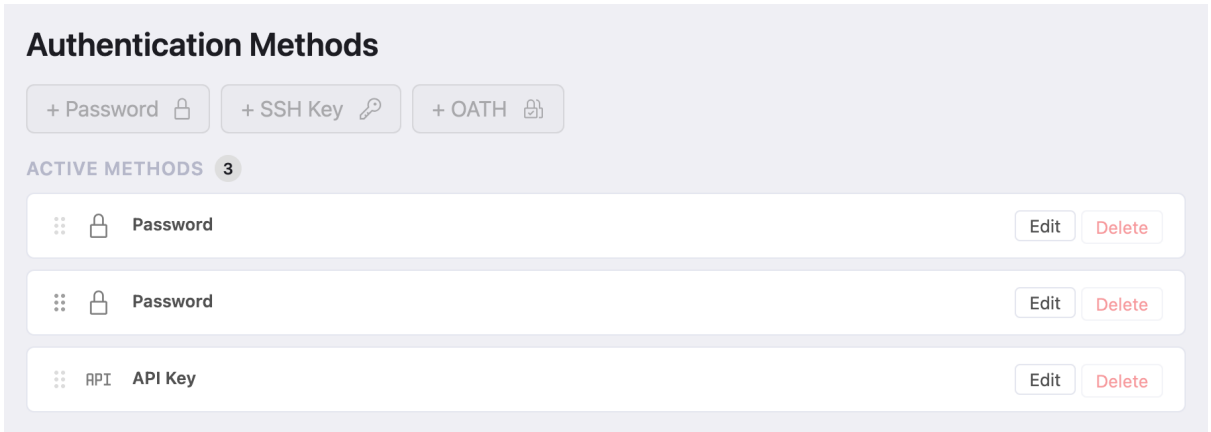
Note

Access to authentication method configuration requires authentication with any method except OpenID Connect.

1.4.2 Methods You Are Allowed to Manage

Your administrator decides which types of authentication methods you can add and remove on your own. The choice is made in the Admin Panel and applies to all User Access Gateway users.

If a method type is not allowed, its add button is greyed out and shows the message *Adding and removing this authentication method is blocked by the administrator.* The *Delete* button of every method of that type is greyed out with the same message.



Your existing methods are never removed by this setting. They stay on the list, you can still

log in with them, and you can still edit them - changing your password, for example, remains available even when adding a password method is blocked.

Note

Some methods are always created by an administrator and can never be removed in the User Access Gateway: *API Key*, *Certificate*, *DUO*, *SMS* and *External authentication*. Their *Delete* button is greyed out with the message *This authentication method cannot be removed.* You can still edit them.

Note

The + Passkey button is not displayed at all when FIDO2 has not been configured by an administrator. This is different from a method being blocked - a blocked method is shown greyed out, an unconfigured one is not shown.

If you need a method that is not available to you, contact your Fudo system administrator.

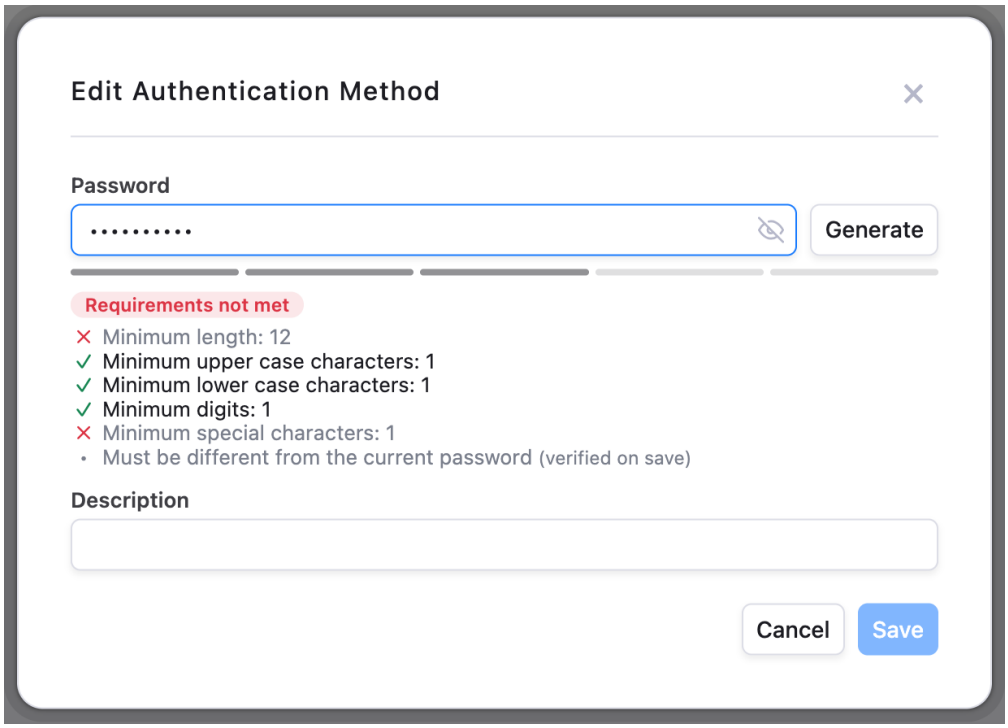
1.4.3 Password Authentication

Password is the primary authentication method. You can change your password at any time.

Changing Password

To change your password:

1. In the active methods list, click *Edit* next to *Password*.
2. Enter a new password, or click *Generate* to create a random one and click *Use*.
3. Click *Save*.



Warning

The password must meet the requirements specified in the system's password complexity policy. The requirements are listed under the password field and checked as you type; the password can be saved only when all of them are met.

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 the External Authentication configuration guide.

Note

For a user authenticated with the **Active Directory** external authentication method, when the password change is enforced by the domain controller, Fudo performs it using the **Kerberos** protocol, provided that Kerberos was used during the user's authentication. For more information, see the Kerberos authentication settings.

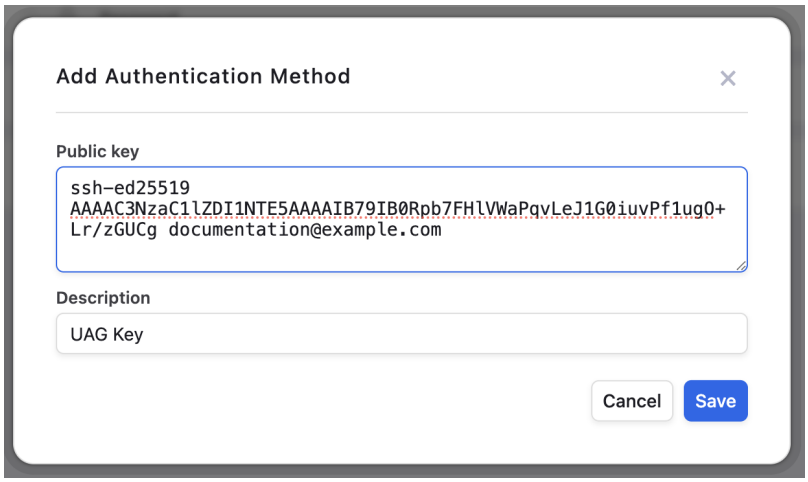
1.4.4 SSH Key Authentication

SSH keys allow for secure authentication without the need to use a password during SSH sessions.

Adding an SSH Key

To add an SSH key:

1. In the authentication methods section, click *+ SSH Key*
2. Enter a name for the key (for easy identification)
3. Paste the content of your public SSH key
4. Click *Save*



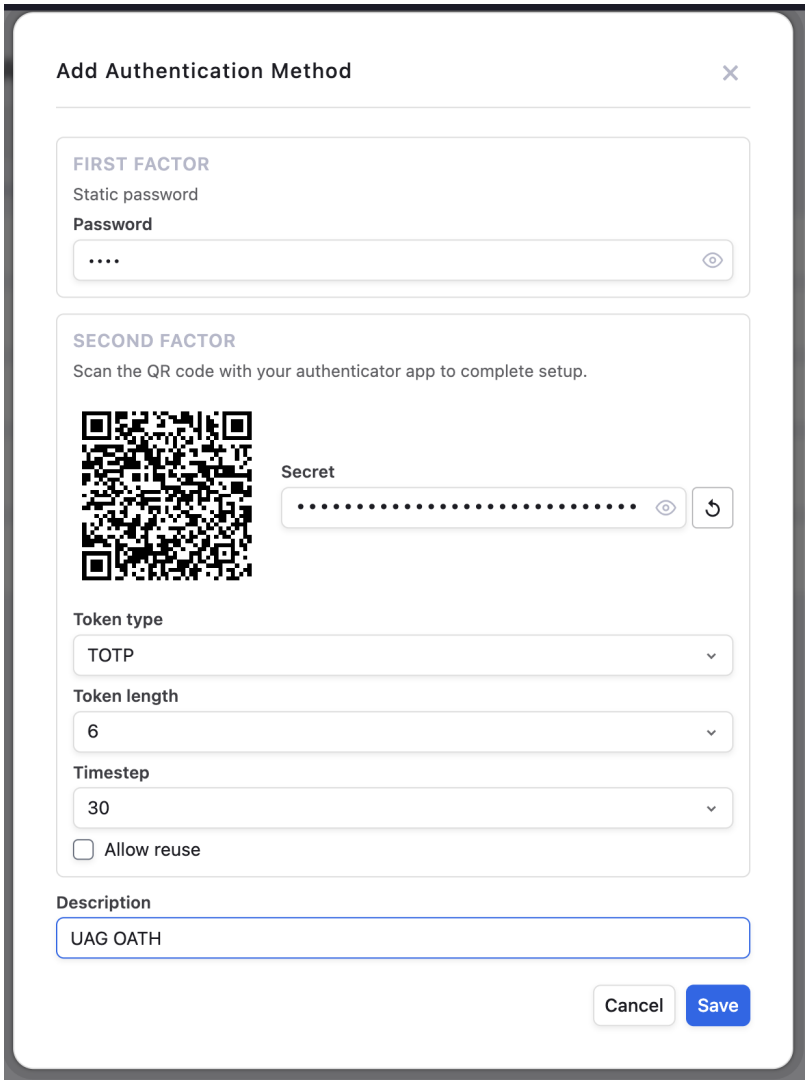
1.4.5 OATH Authentication

OATH is a two-factor authentication method using time-based codes generated by an authenticator app.

Configuring OATH

To configure OATH authentication method:

1. In the authentication methods section, click *+ OATH*
2. In the *First factor* section, provide the static password for the account
3. In the *Second factor* field, select `TOTP (time-based)` as the token type
4. Specify the token length (typically 6 digits)
5. Select the required timestep value (typically 30 seconds)
6. (Optional) Enable *Allow reuse* to permit the same valid TOTP code to be accepted more than once within its current time window
7. Scan the displayed QR code with an authenticator app (e.g., Google Authenticator, Authy)
8. Enter the current code from the app for verification
9. Click *Save*



Allow Reuse Option

The `Allow reuse` option enables the same valid TOTP code to be accepted more than once within its current time window. This feature is particularly useful for scenarios where parallel access is required.

Use Cases:

- Scripted SSH access
- Ansible playbooks
- Parallel scp or rsync operations
- CI runners connecting to multiple systems
- Access through multiple bastion hosts
- Bulk RDP gateway hand-offs

Default Behavior:

By default, the `Allow reuse` option is disabled. Each TOTP code can be used only once. After successful verification, another attempt using the same code will be rejected.

When Enabled:

When `Allow reuse` is enabled:

- The same TOTP code can be accepted multiple times within its current time window
- You can use the same TOTP code for multiple parallel connections within one timestep
- Once the timestep expires, the previous code becomes invalid and a new code is required

> **Note**
>
> The `Allow reuse` option is available only for TOTP (time-based) tokens. HOTP (counter-based) tokens do not support code reuse.

1.4.6 FIDO2 Authentication (Passkey)

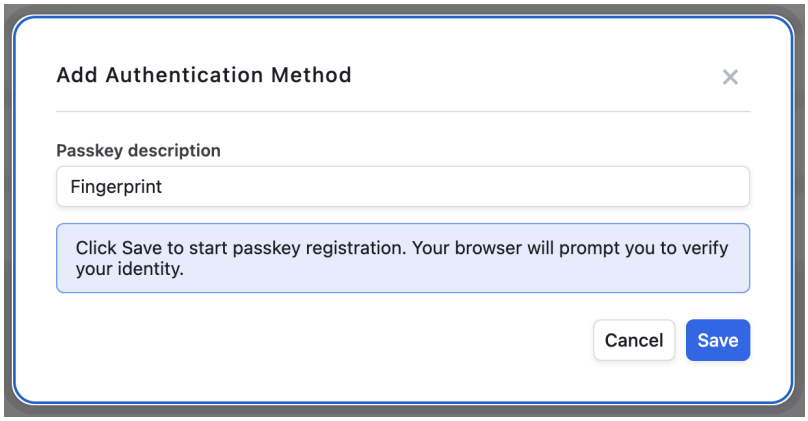
FIDO2/Passkey is a modern passwordless authentication method using hardware keys, biometrics, or password managers.

Configuring FIDO2/Passkey

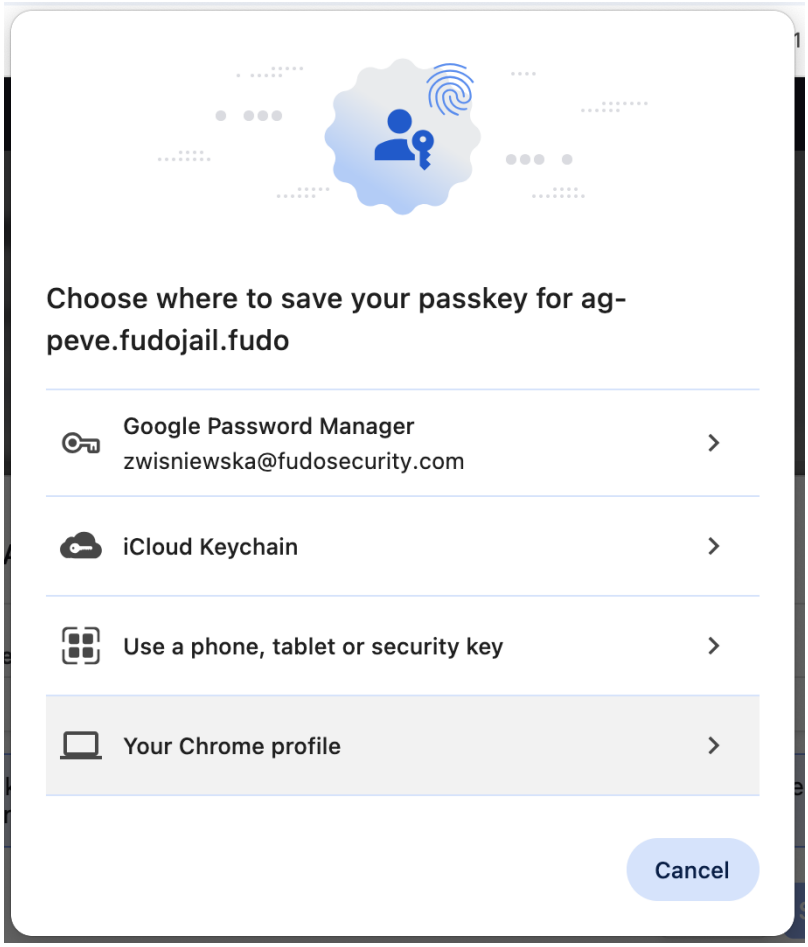
> **Note**
>
> To configure and use passkeys in the User Access Gateway, FIDO2/Passkey authentication must first be configured by an administrator in the Admin Panel, and the administrator must allow users to manage the *Passkey* method themselves. Contact your Fudo system administrator if passkey authentication is not available.

To configure a FIDO2/Passkey authentication method:

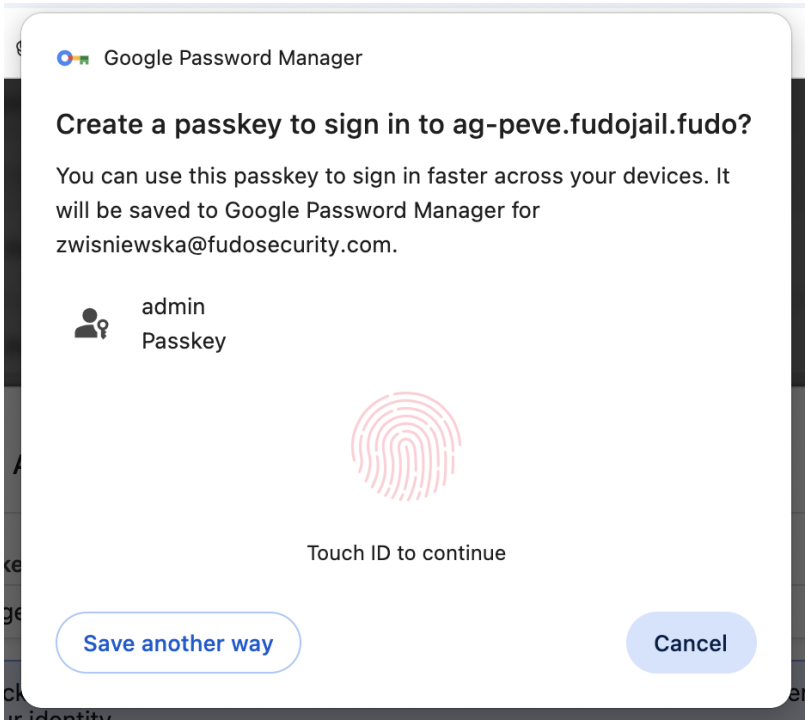
1. In the authentication methods section, click *+ Passkey*
2. Enter a name for your Passkey



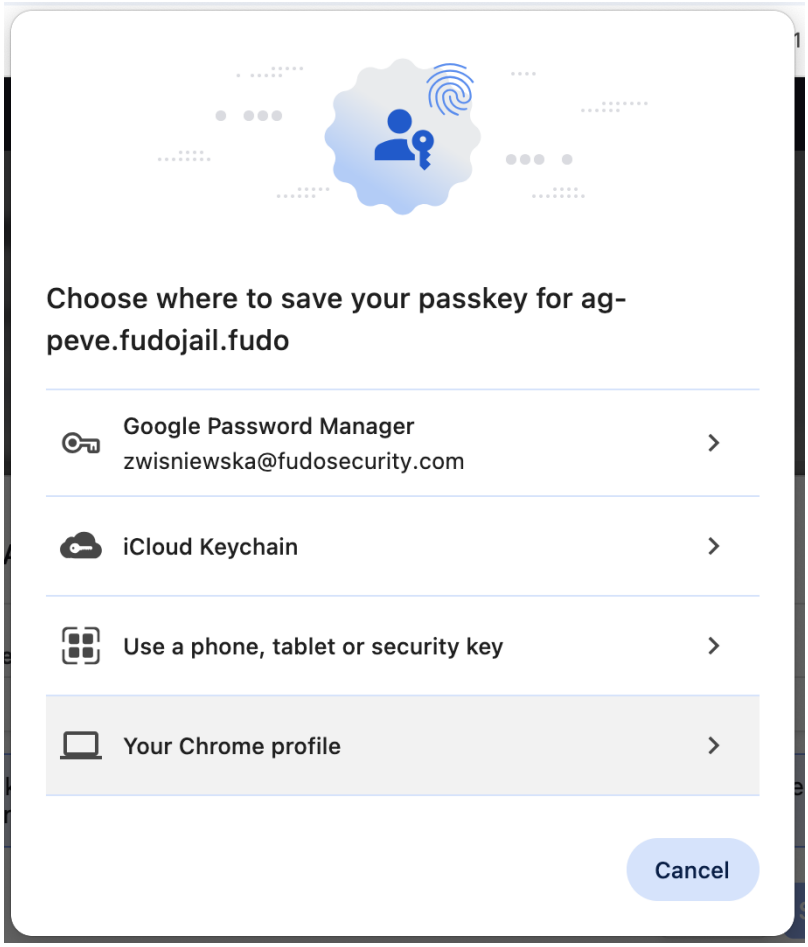
3. Follow your browser or password manager instructions:
    - Choose your authentication method (hardware key, biometrics, password manager)



4. Confirm your identity (touch the key, use fingerprint, Face ID) and save the Passkey in your chosen location



5. After successful creation, you will see a confirmation



Supported FIDO2 Methods

The system supports the following FIDO2 authentication methods:

- **Hardware keys** - YubiKey
- **Built-in biometrics** - Touch ID (macOS)
- **Password managers** - 1Password, Google Password Manager, Apple Passwords
- **Mobile devices** - Used as security keys via Bluetooth/NFC

Using FIDO2/Passkey Authentication

After configuring a FIDO2 method:

1. On the login page, enter your username
2. Click the Login with Passkey button (appears only when FIDO2 is configured)
3. Confirm your identity using the configured method
4. The system will automatically verify the cryptographic signature and grant access

Warning

Passkeys created in the User Access Gateway cannot be used in the Admin Panel due to different Relying Party identifiers.

1.4.7 Removing an Authentication Method

To remove one of your authentication methods:

1. In the authentication methods section, find the method on the *Active methods* list
2. Click *Delete*
3. Confirm the removal

You can only remove a method type that you are also allowed to add. If the Delete button is greyed out, hover over it to see the reason:

- *Adding and removing this authentication method is blocked by the administrator.* - the administrator has not allowed you to manage this method type. Ask your administrator to remove the method for you, or to allow the method type.
- *This authentication method cannot be removed.* - the method was created by an administrator and has no self-service equivalent, so only an administrator can remove it.

Note

Removing a method is intentionally tied to adding it. This prevents a situation in which you delete a credential that you would not be able to create again yourself.

Related topics:

- *Authentication Methods*
- *Displaying Passwords History*

1.5 Fudo Officer App

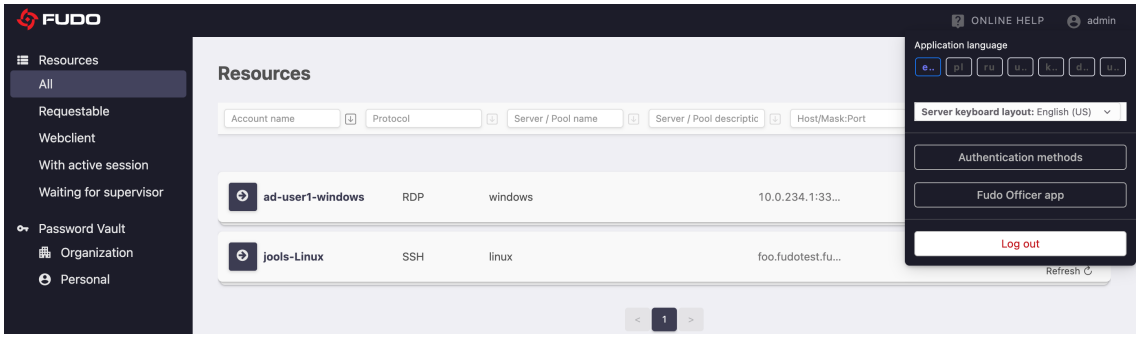
The Fudo Officer mobile app gives you access to your personal and organization secrets on your phone. You can pair the app with your account in the User Access Gateway.

Note

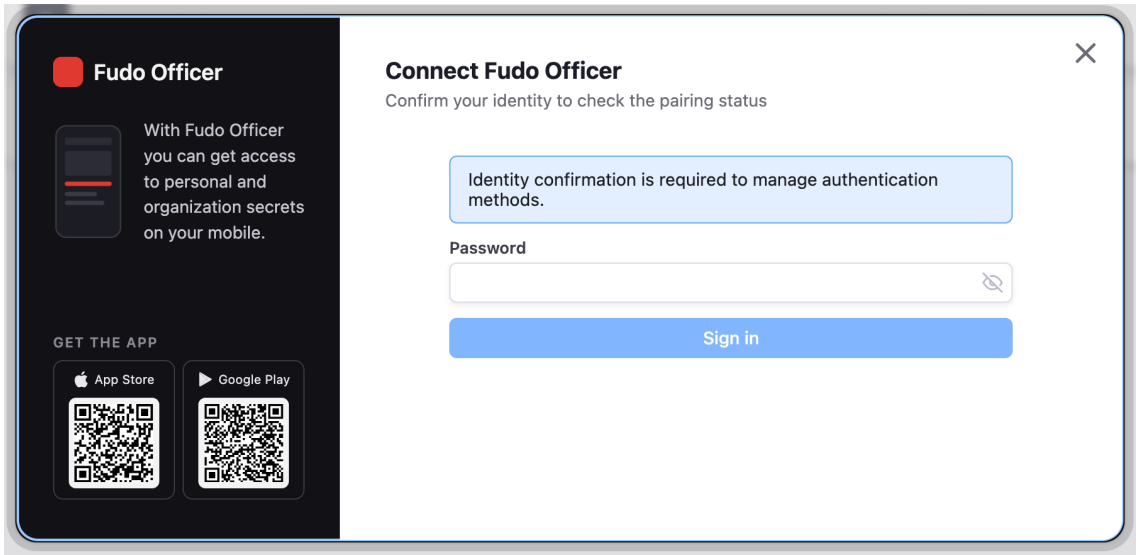
- Before you start, your administrator has to initiate pairing for your account.
- Install the Fudo Officer app from the App Store or Google Play.
- Your account can be paired with one device only.
- If *Fudo Officer app* is not available in your user menu, ask your administrator to enable it.

Connecting Fudo Officer

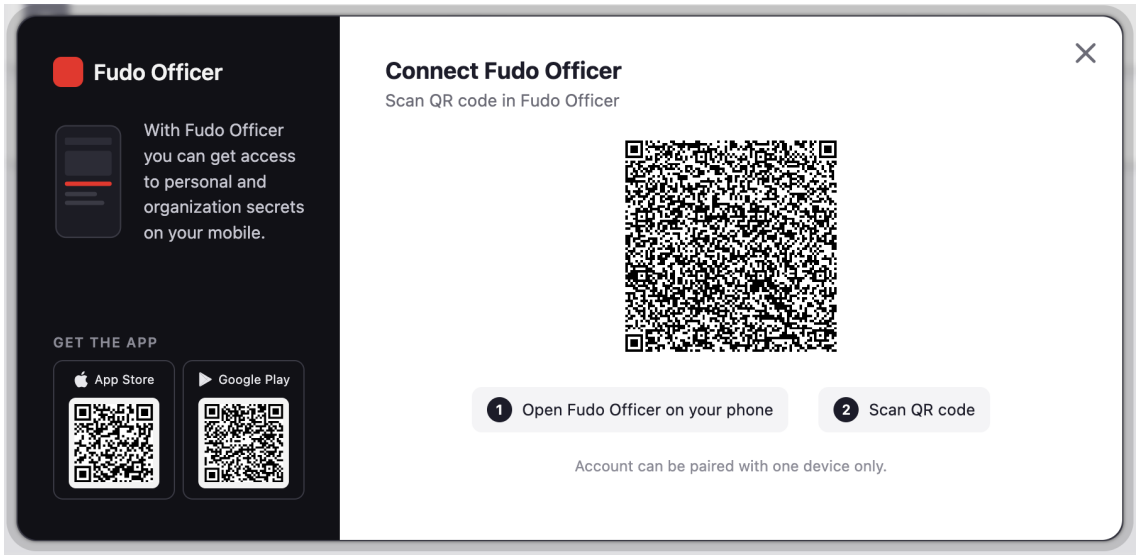
1. Click your user name in the top-right corner and select *Fudo Officer app*.



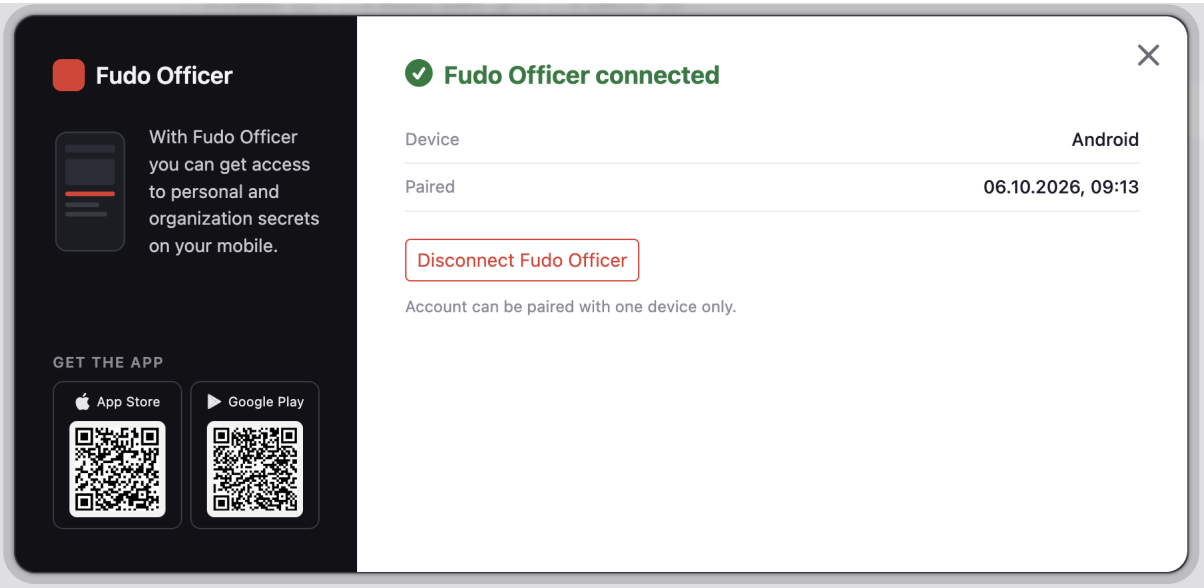
2. Confirm your identity, the same way as when you manage your authentication methods:
   - Enter your password and click *Sign in*. If your account uses an additional authentication method, for example a one-time code, enter it when prompted.
   - Alternatively, if you have a Passkey, click *Sign in with Passkey*.



3. Open Fudo Officer on your phone and scan the displayed QR code.

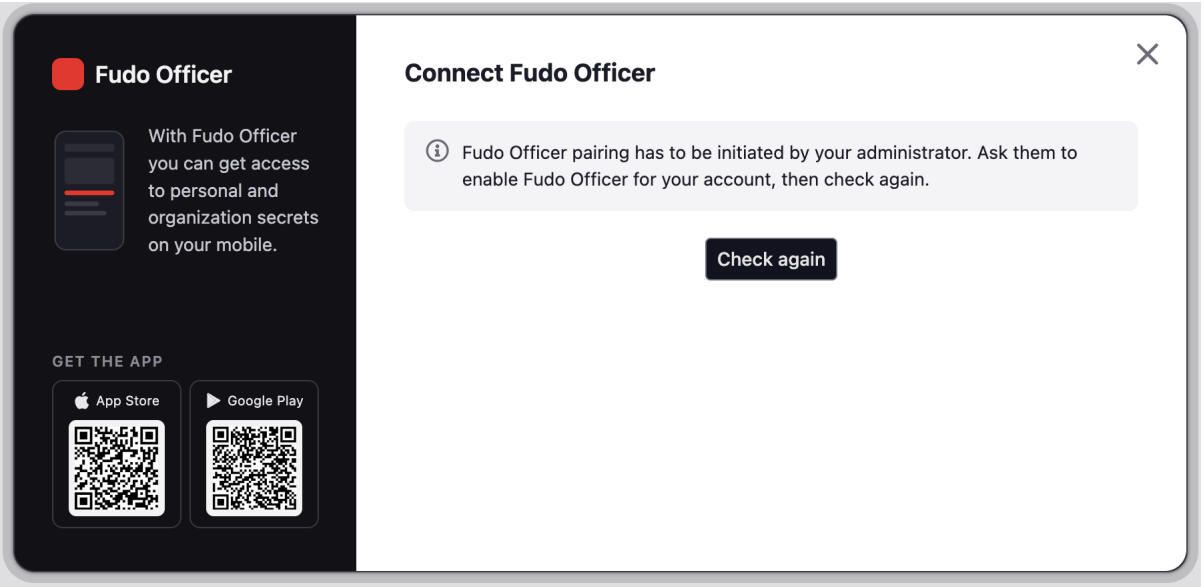


When the pairing is complete, the window shows *Fudo Officer connected* with the device name and the pairing date.



Note

If the window says that pairing has to be initiated by your administrator, ask your administrator to enable Fudo Officer for your account, and then click *Check again*.



Disconnecting Fudo Officer

1. Click your user name in the top-right corner and select *Fudo Officer app*.
2. Click *Disconnect Fudo Officer* and confirm.

After disconnecting, the app no longer has access to your account. To connect it again, your administrator has to initiate pairing again.

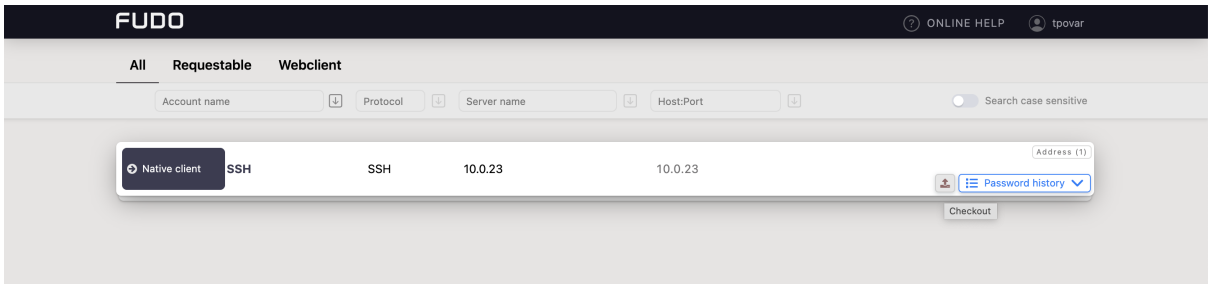
1.6 Secret Checkout and Checkin

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.

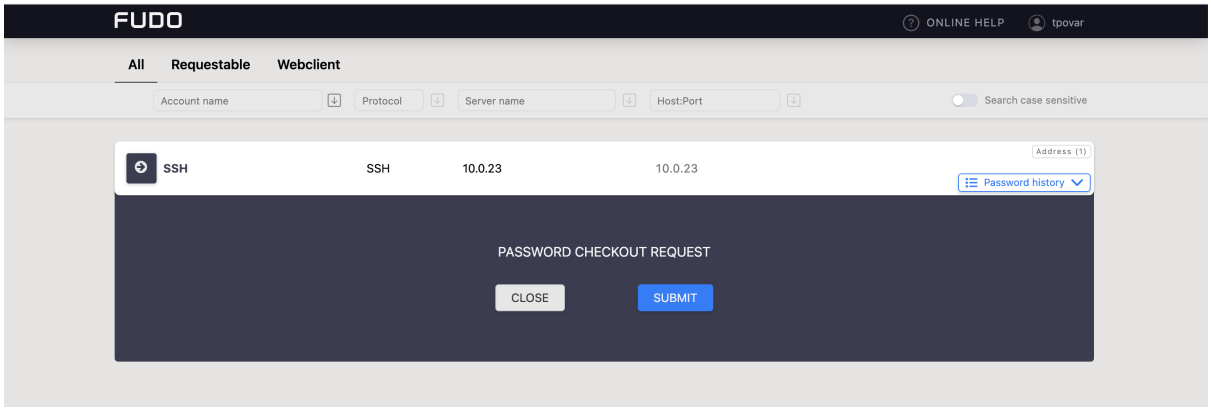
1.6.1 Secret Checkout

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.



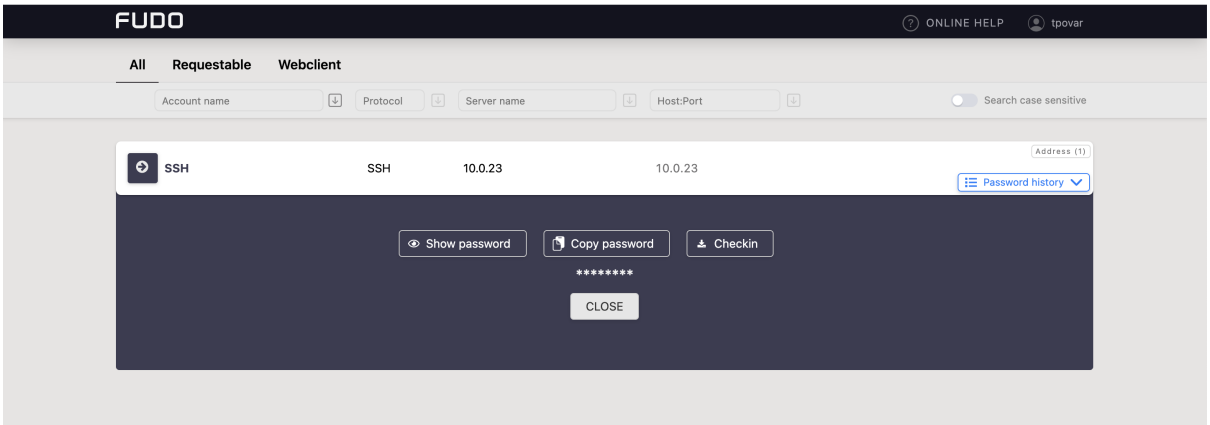
3. Click *SUBMIT*.



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.



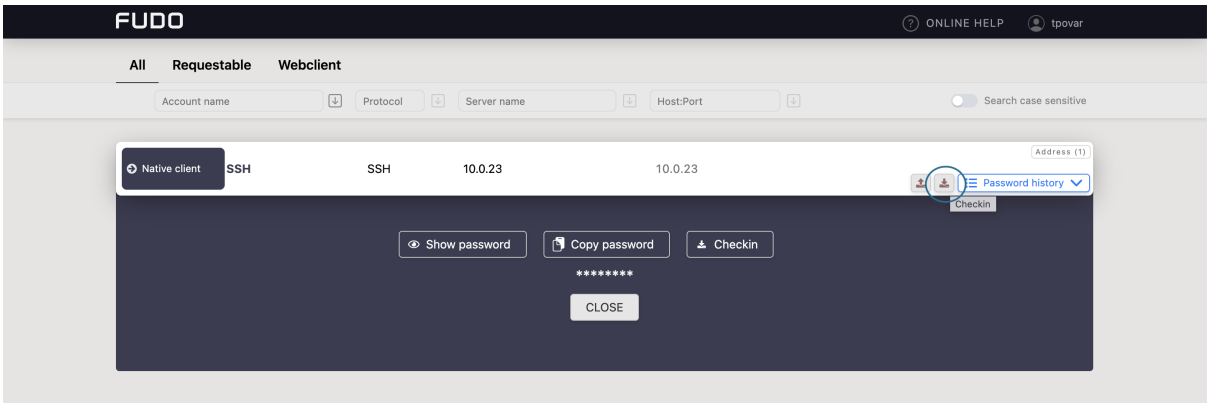
1.6.2 Secret Checkin

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.



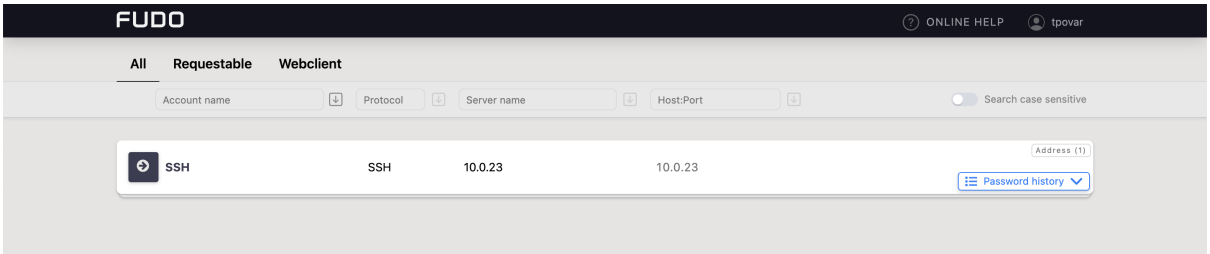
Related topics:

- *Displaying Passwords History*

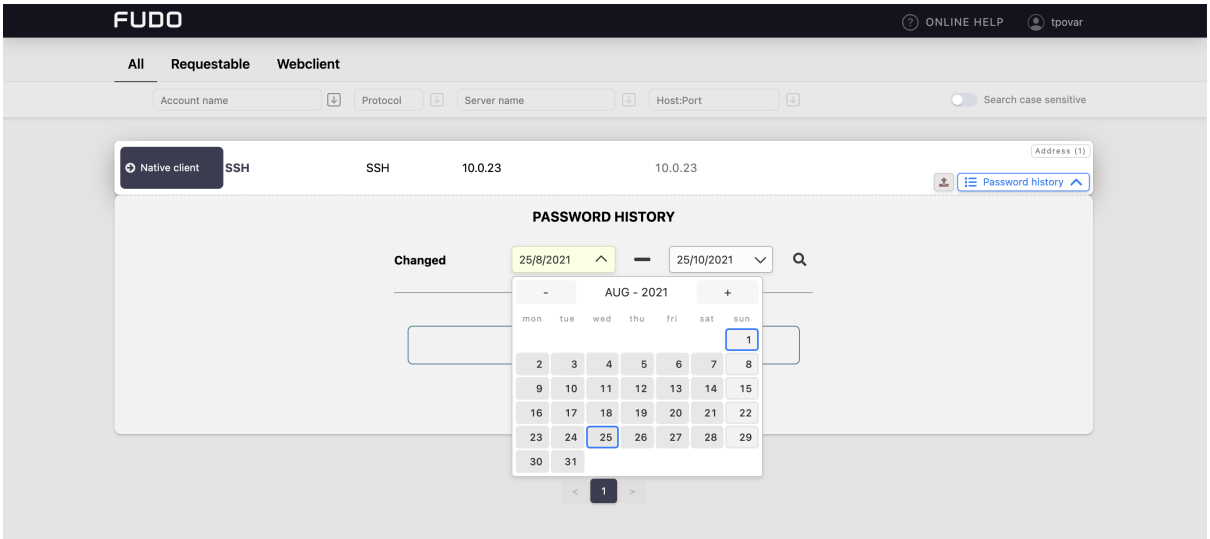
1.7 Displaying Passwords History

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:

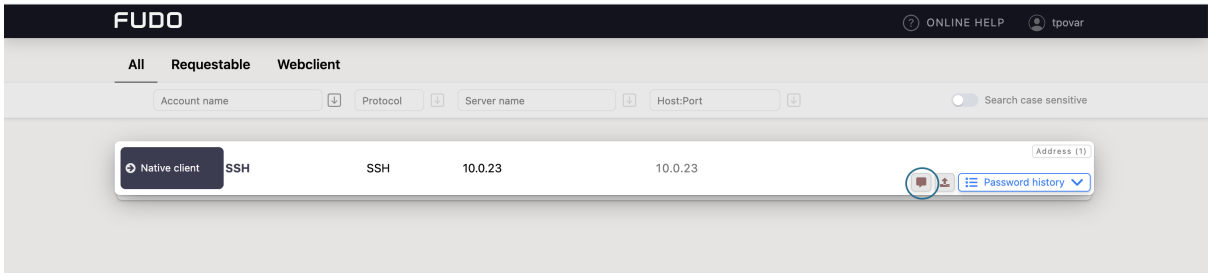
- *Authentication Methods*
- *Displaying Passwords History*

1.8 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.

1.9 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:

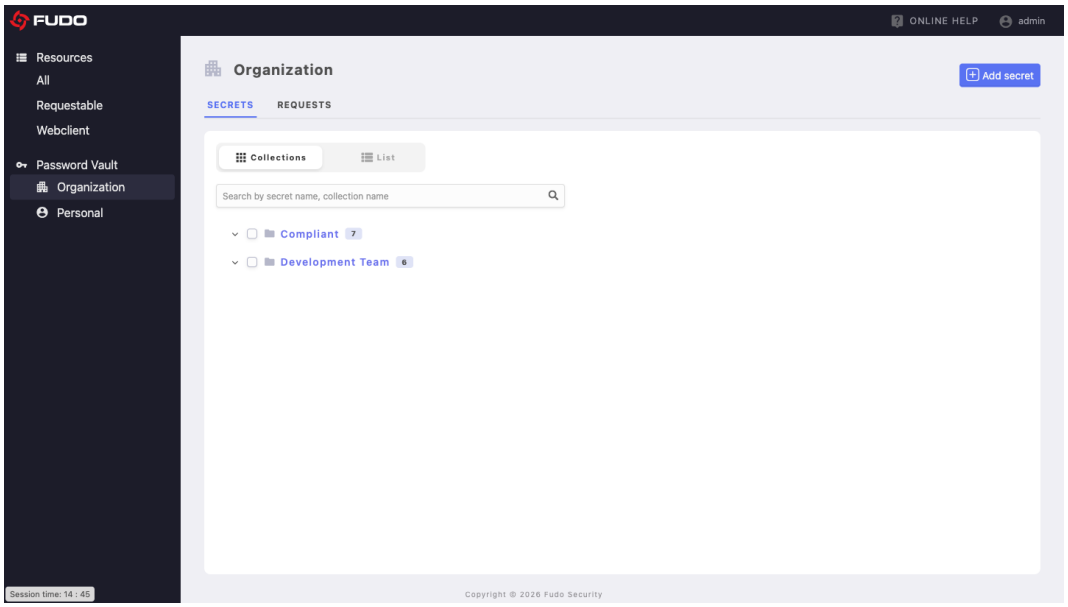
- **Organization Vault** - Managed by the organization, contains shared secrets and collections accessible based on user permissions.
- **Personal Vault** - Private space for individual users to store their personal credentials.

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

1.9.1 Overview

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



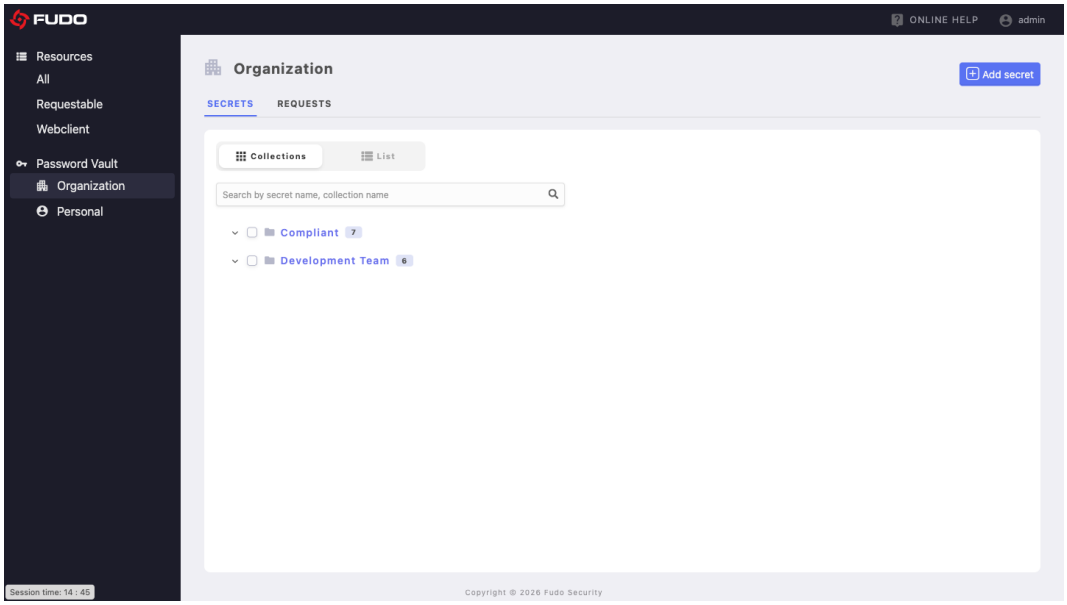
Viewing Secrets and Collections

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:

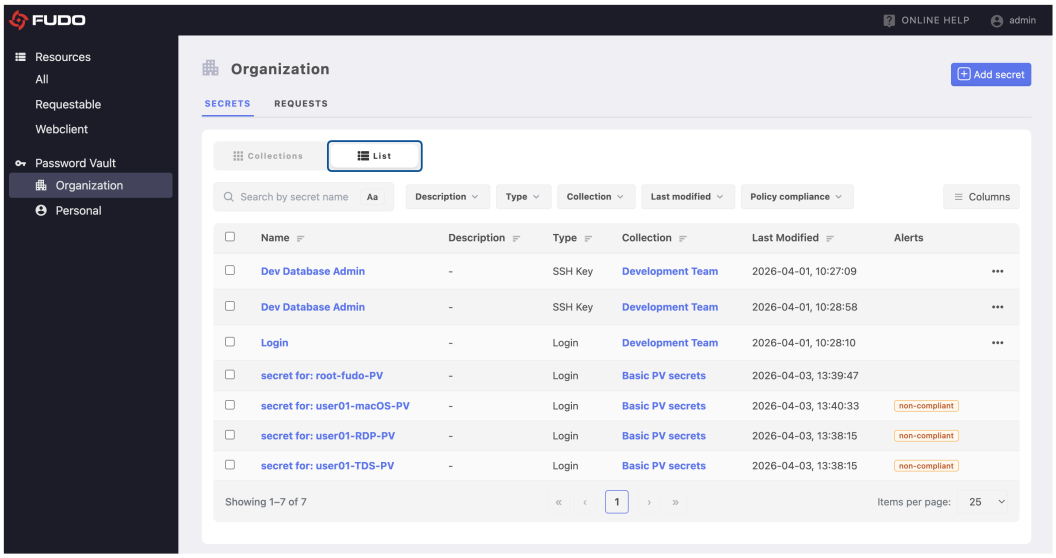
1. Type the secret name or collection name in the search field
2. Use filters to narrow results:
    - Click on collection folders to filter by collection
    - The number next to each collection shows how many secrets it contains

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

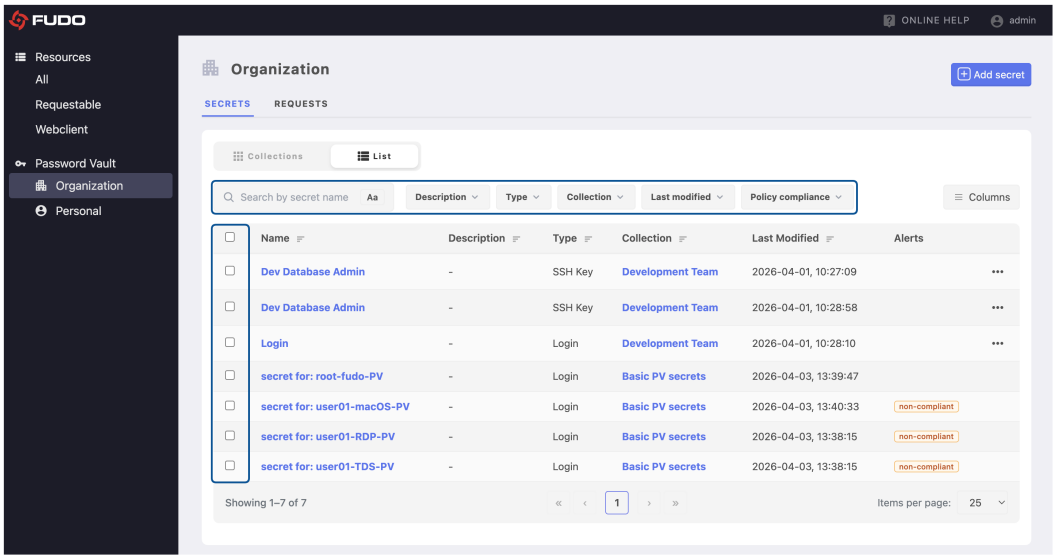


Sort and Filter

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

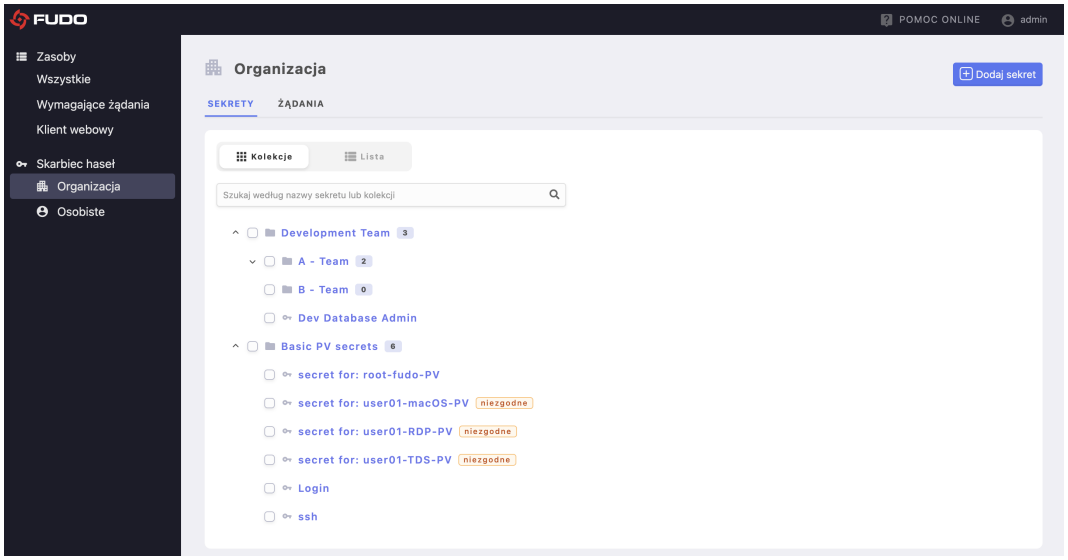


1.9.2 Organization Vault

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

Accessing Organization Vault

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



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

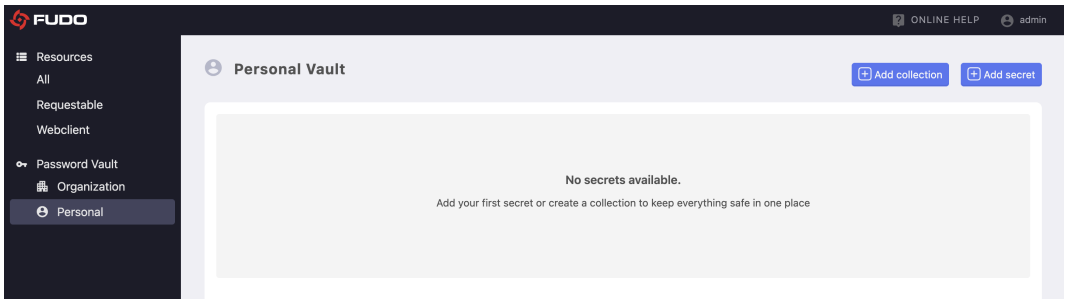
If you need access to Password Vault or additional access to selected collections, contact your administrator.

1.9.3 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.

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.



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)*.

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

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.

1.9.4 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.

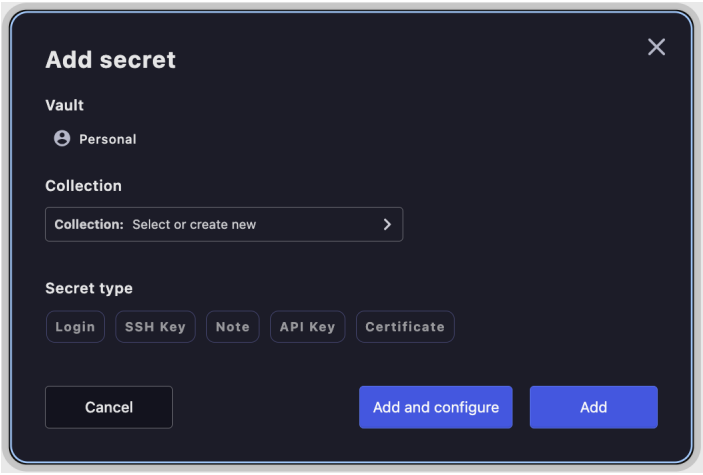
Adding a New Secret

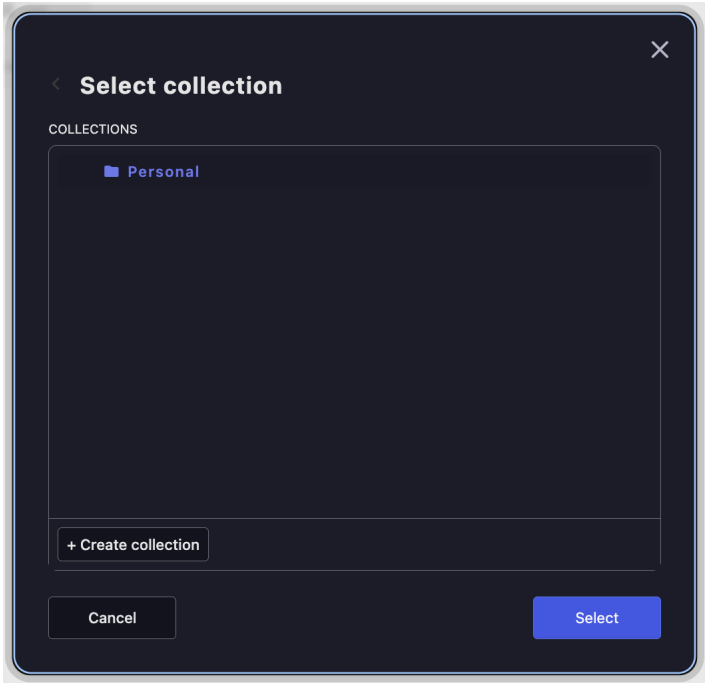
Note

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*.

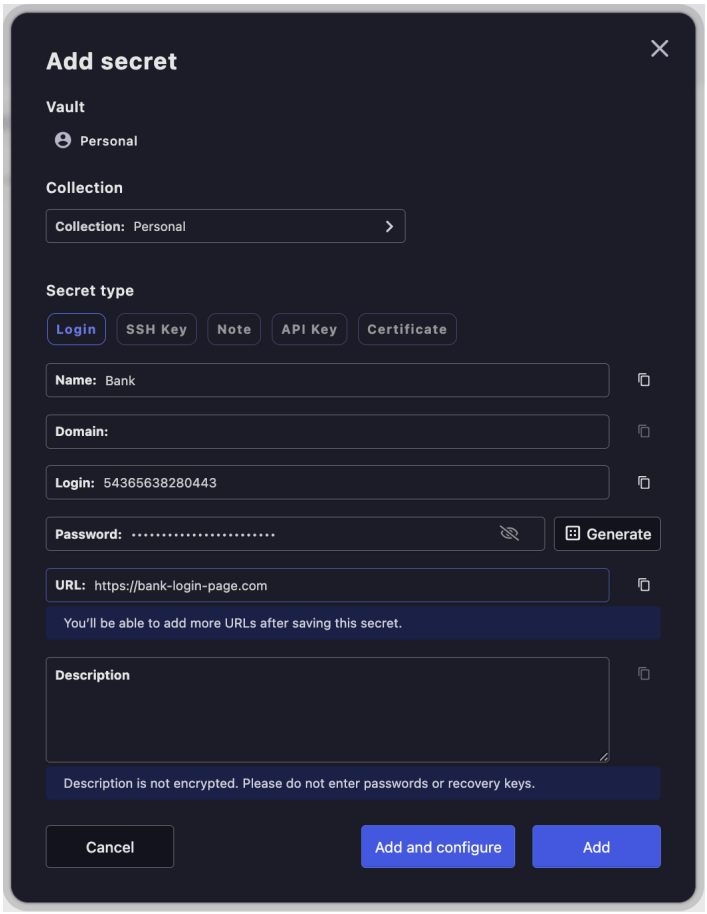




3. Select the collection where the secret will be stored by clicking the *Collection* dropdown.
4. Click *Select*.
5. Choose the appropriate secret type (Login, SSH Key, Note, API Key, Certificate).

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)

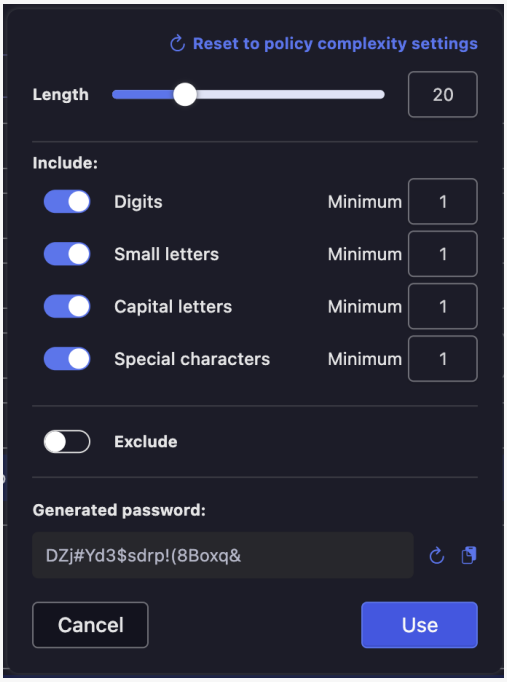


Note

Password Generator:

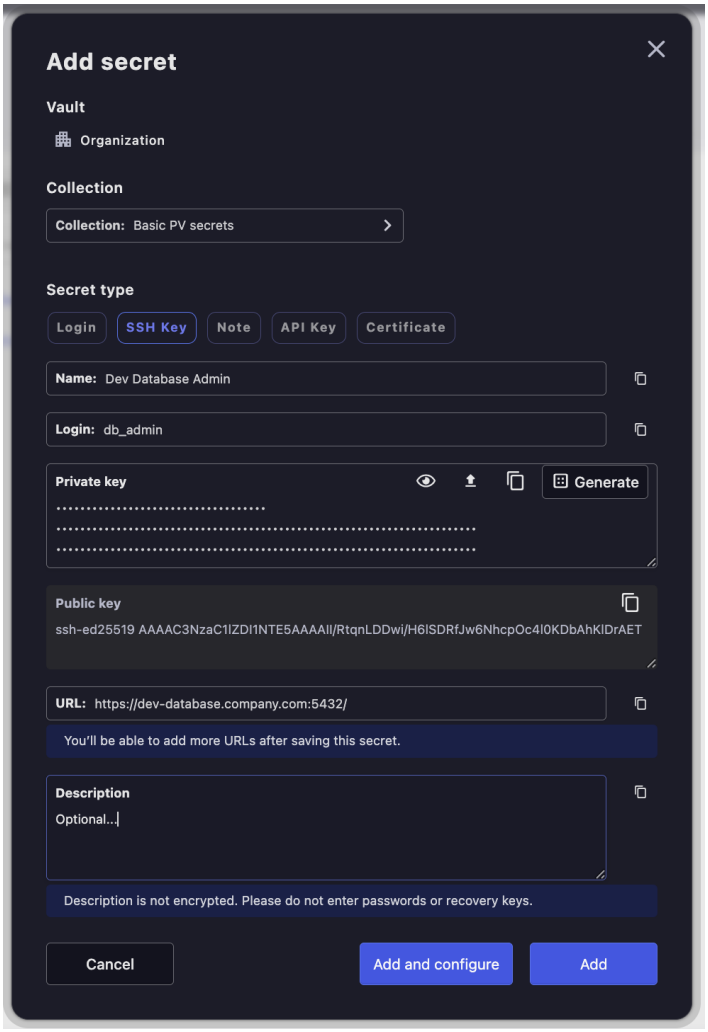
The integrated password generator (*Generate* button) provides secure password creation with customizable options:

- **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



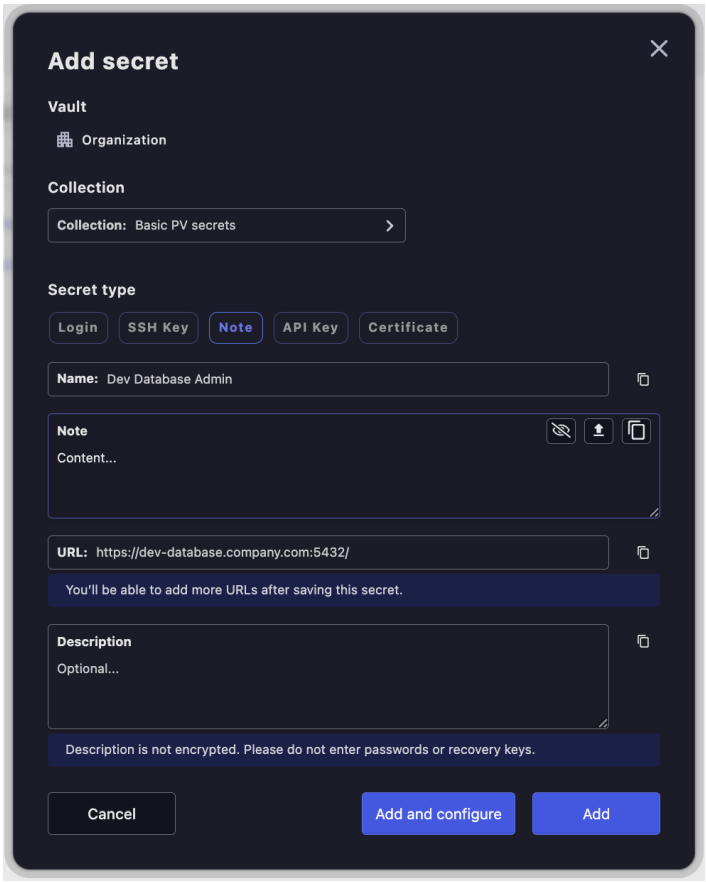
For SSH Key Secrets:

- 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)



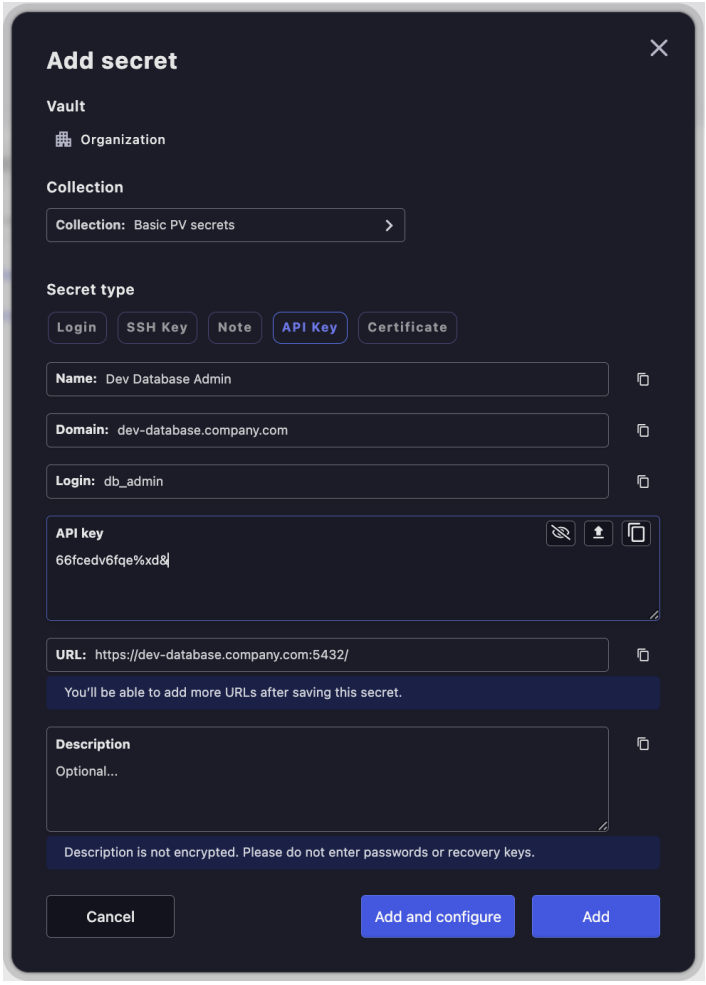
For Note Secrets:

- 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)



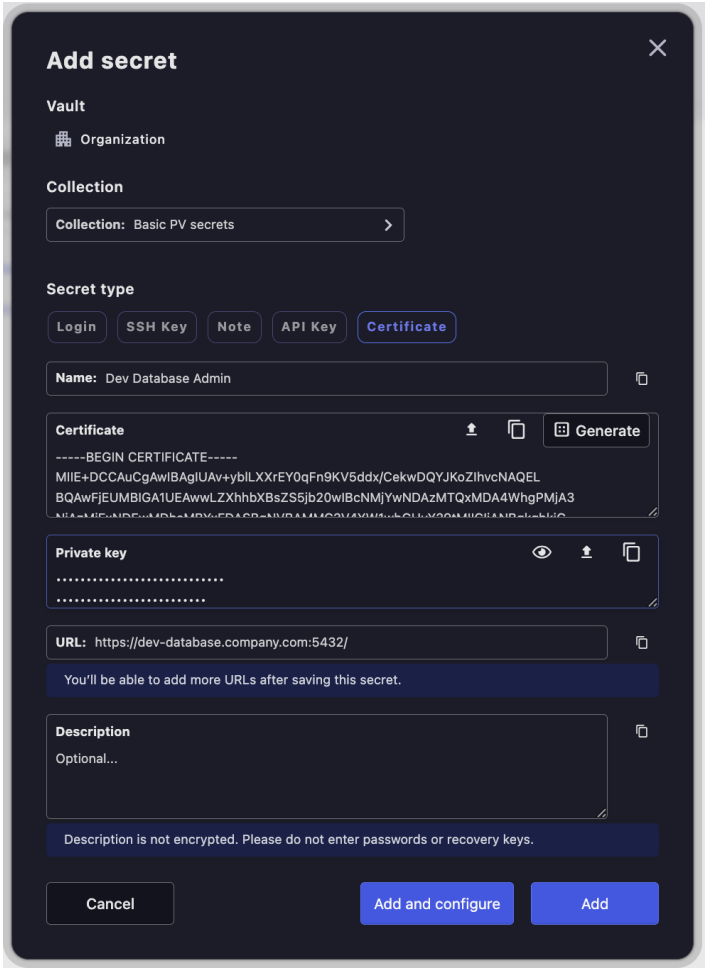
For API Key Secrets:

- 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:

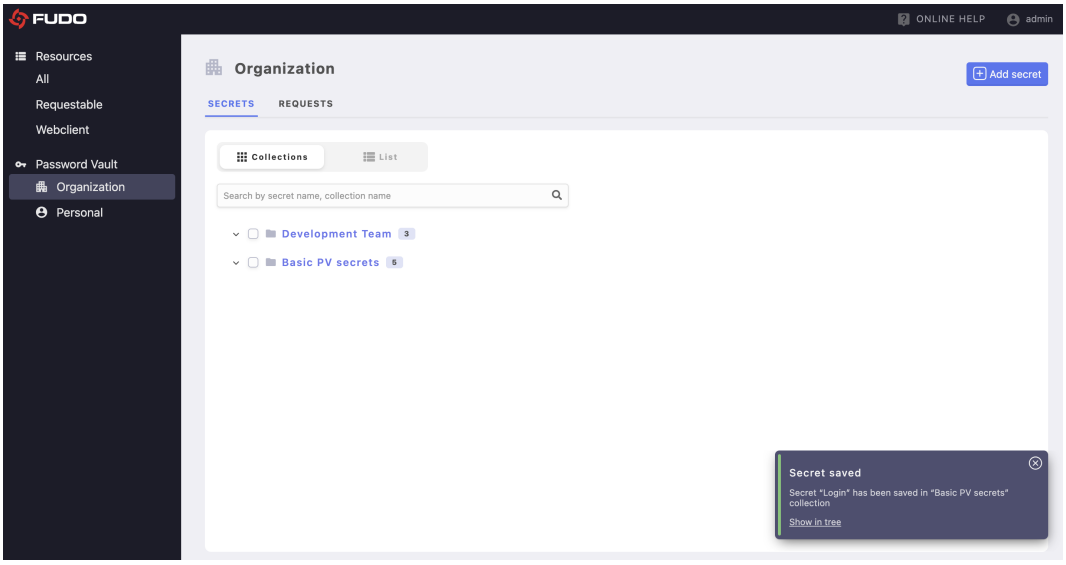
- Fill in the required fields:
  - Name: Enter a descriptive name for the secret
  - Certificate: Upload or generate certificate
  - Private Key: Upload your Private Key
  - URL: Enter the related website or service URL
  - Description: Optional additional information (not encrypted)



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:

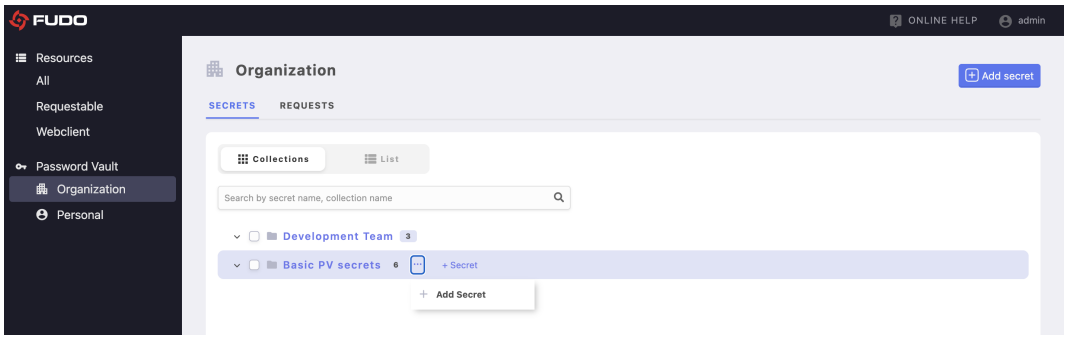
After creating a secret, you will see a confirmation message and the collection's secret count will be updated:



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**



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

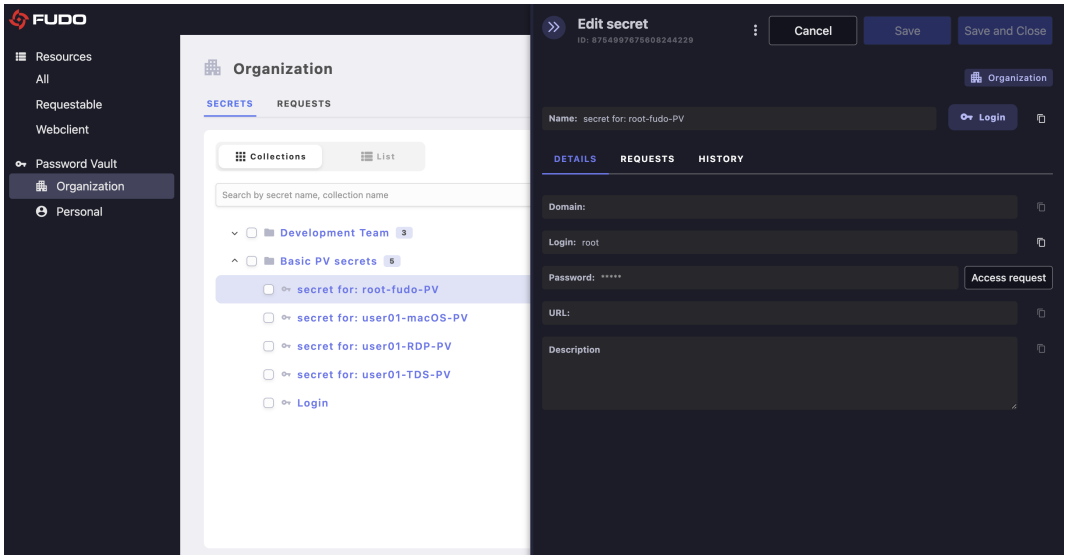
1. Select *Password Vault* > *Organization* or *Personal*.
2. Click *List* to switch to list view.
3. Click on the secret name to open the edit panel.

Edit Secret Panel

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

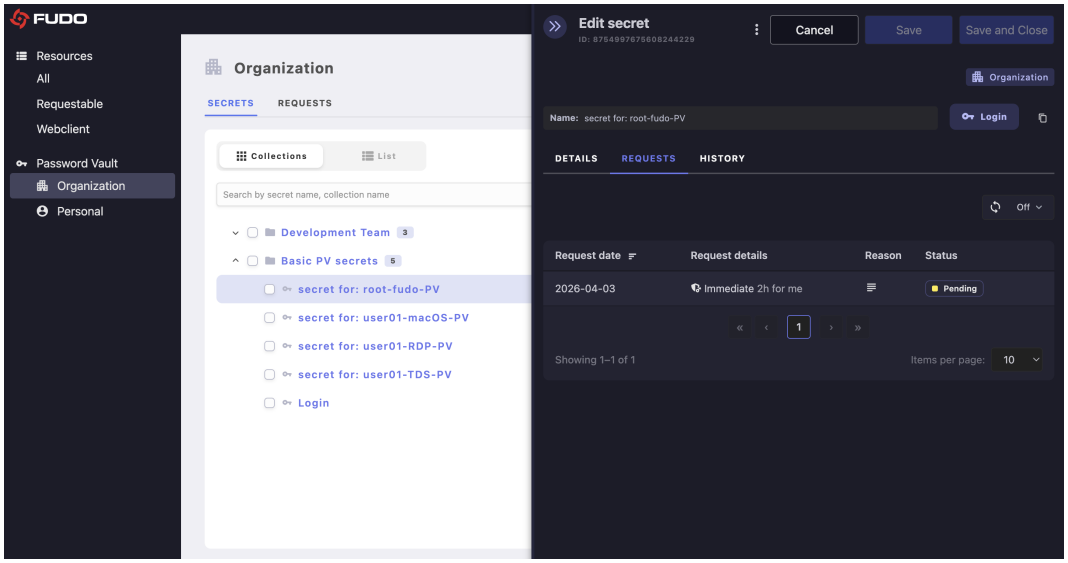
DETAILS TAB

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



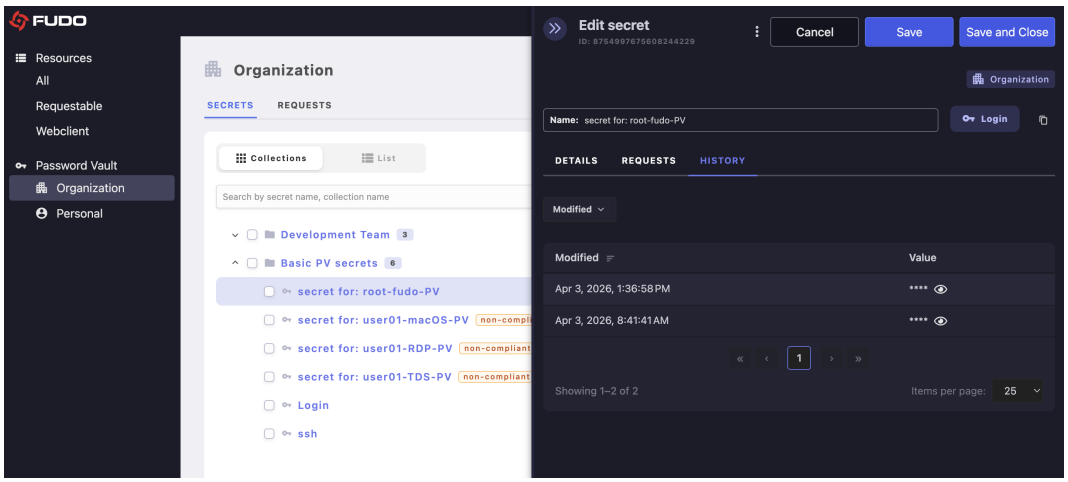
REQUESTS TAB

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.



Moving Secrets Between Collections

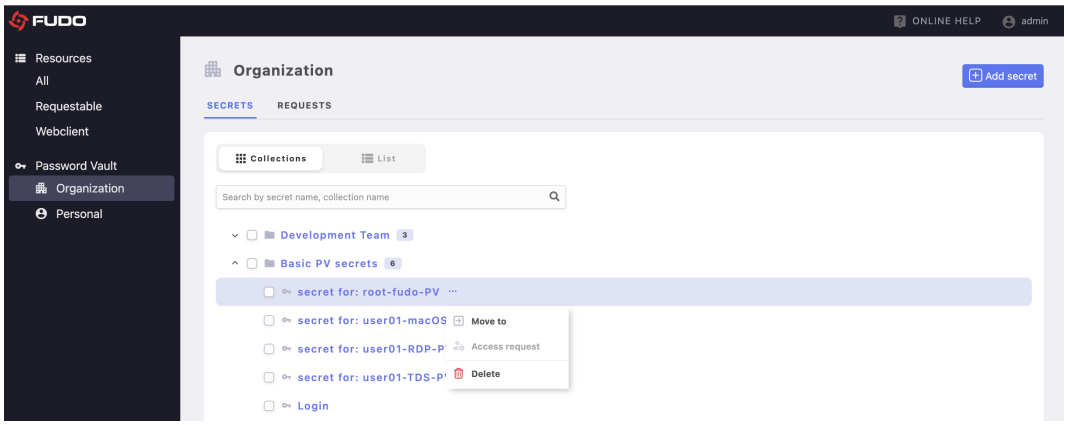
Secrets can be moved between collections to reorganize your password vault structure, adjust access permissions, or reflect changes in team organization. Moving secrets updates their access control based on the target collection's permissions.

> **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:

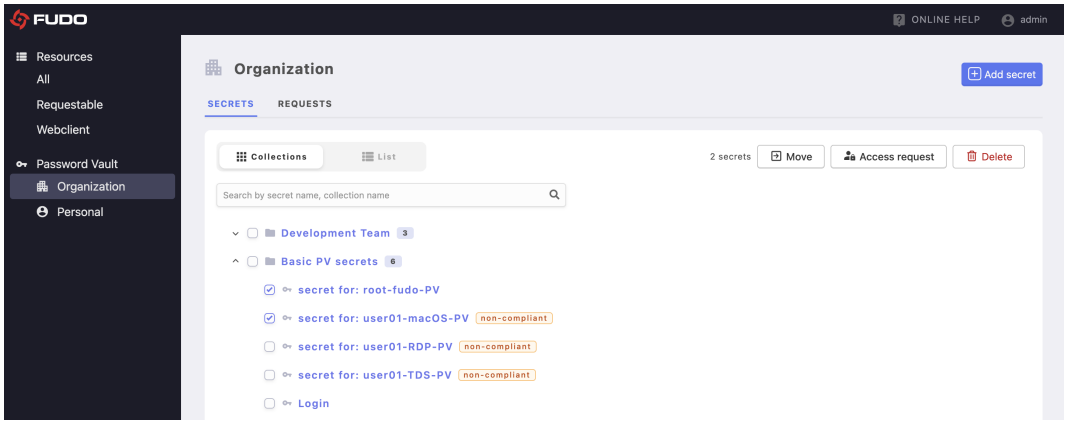
Method 1: Moving Using Context Menu

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.



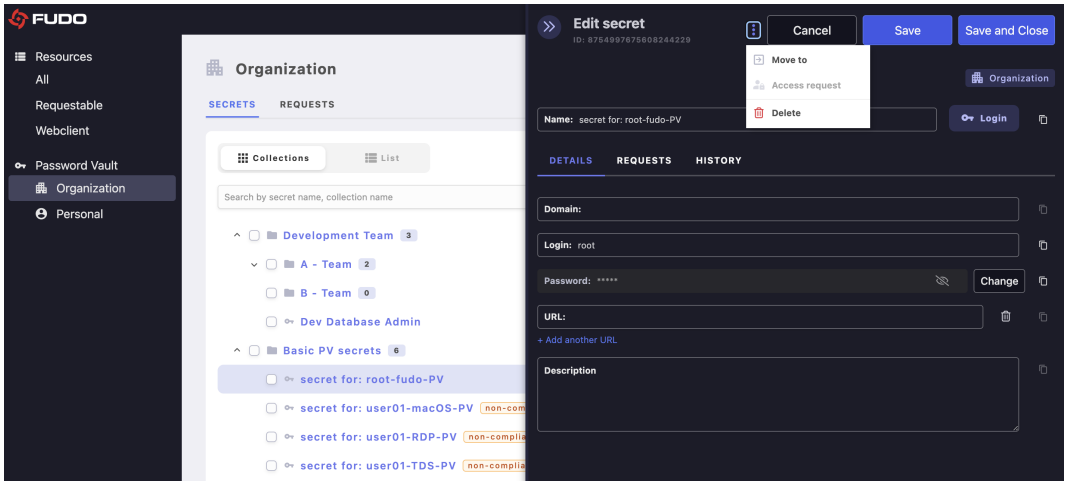
Method 3: Bulk Move in List View

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*

Reveal Secret

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

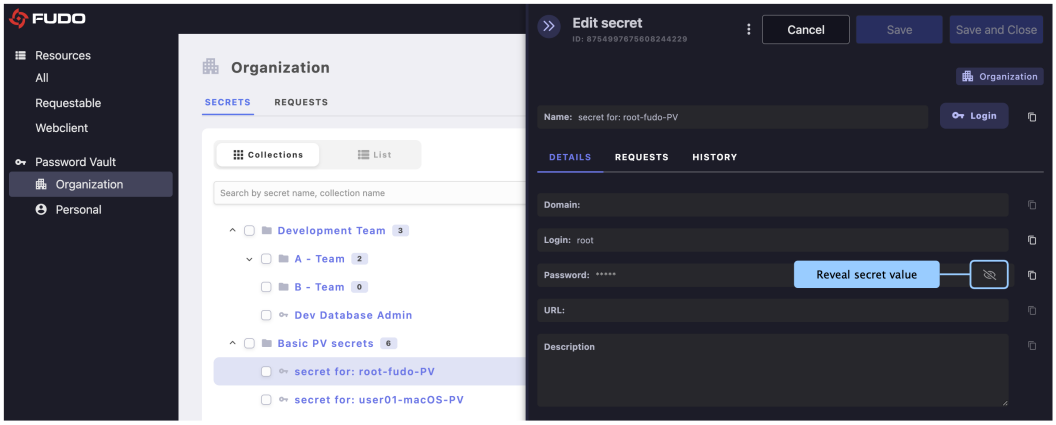
Reveal Hidden Values

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.

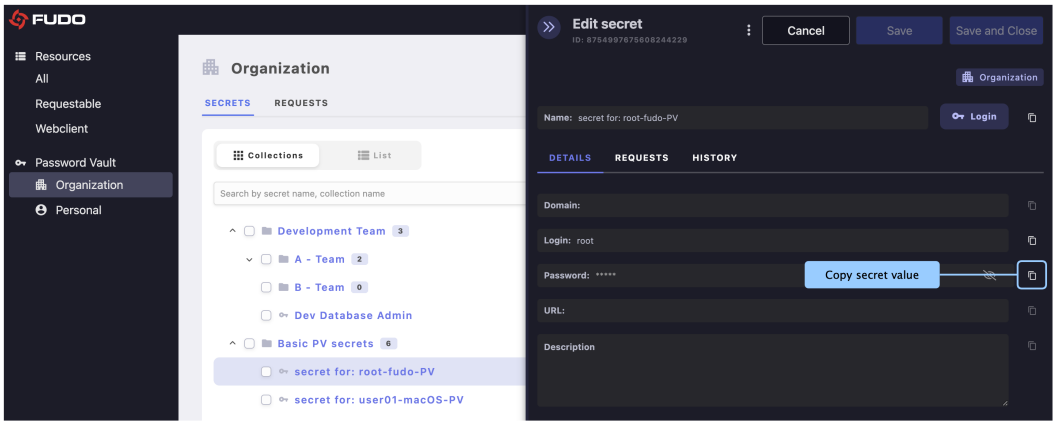
3. Click the **eye icon** next to the secret value field.
4. The secret becomes visible in plain text.
5. Click the eye icon again to hide it.



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

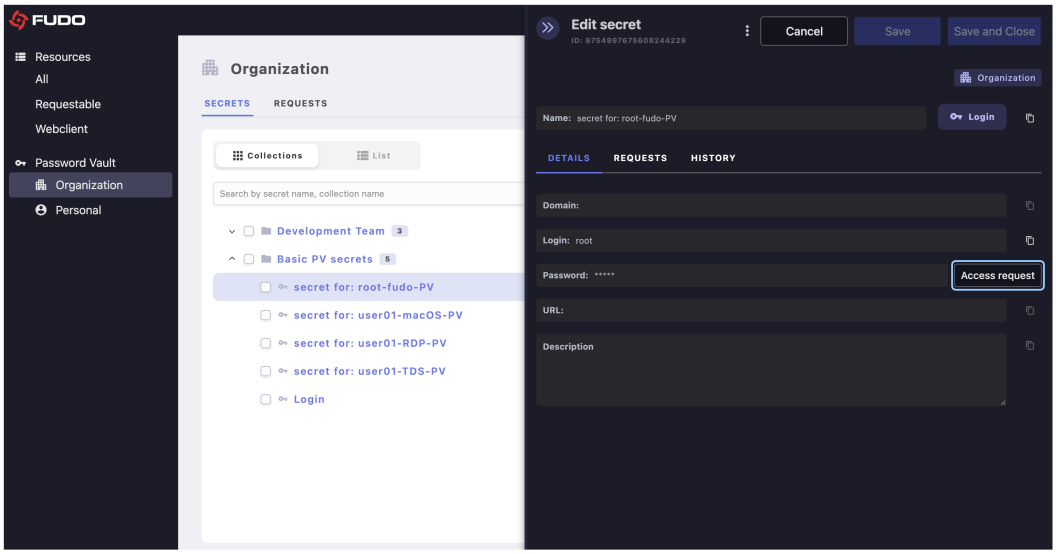
- Each reveal and copy action is logged for security auditing purposes.
- If you do not have **View** or **Full Edit** permission for a secret, see *Requesting Access to a Secret*.

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.

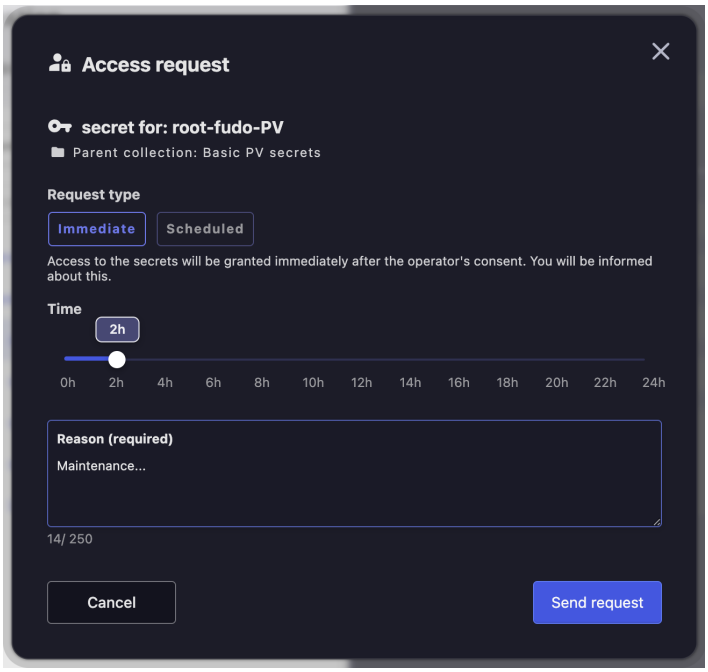
To request access to a secret:

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



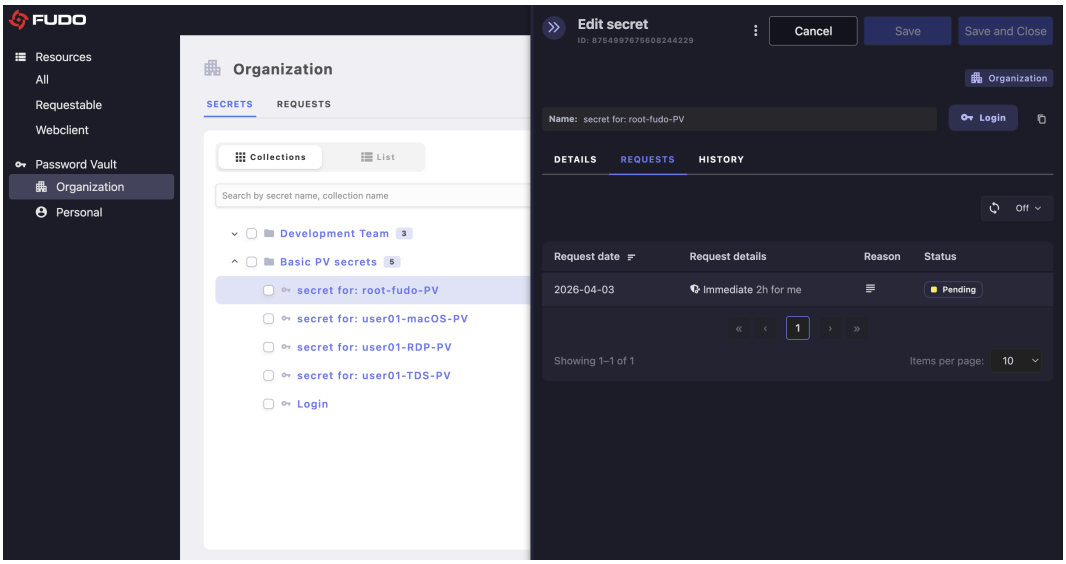
3. In the request window, configure the following fields:
   - **Request type** – select **Immediate** or **Scheduled**
   - **Time** – specify the requested access time

- **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.



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.

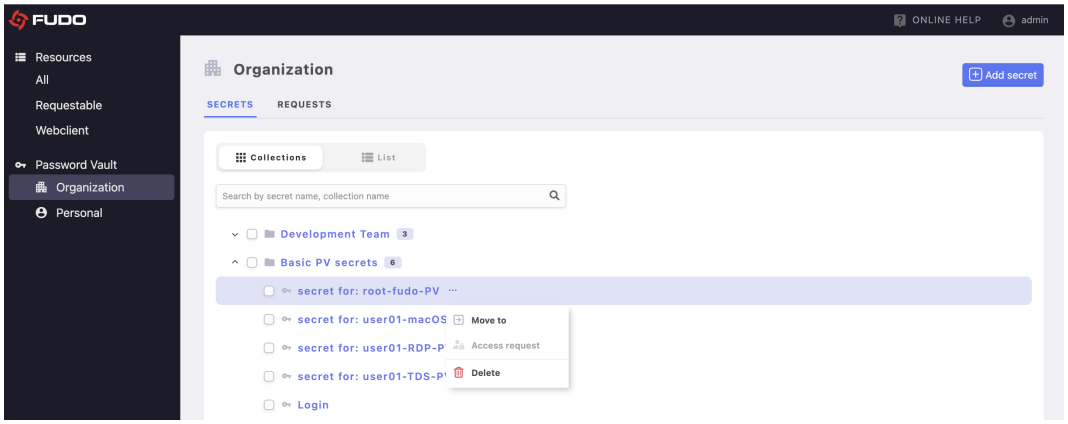
Warning

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:

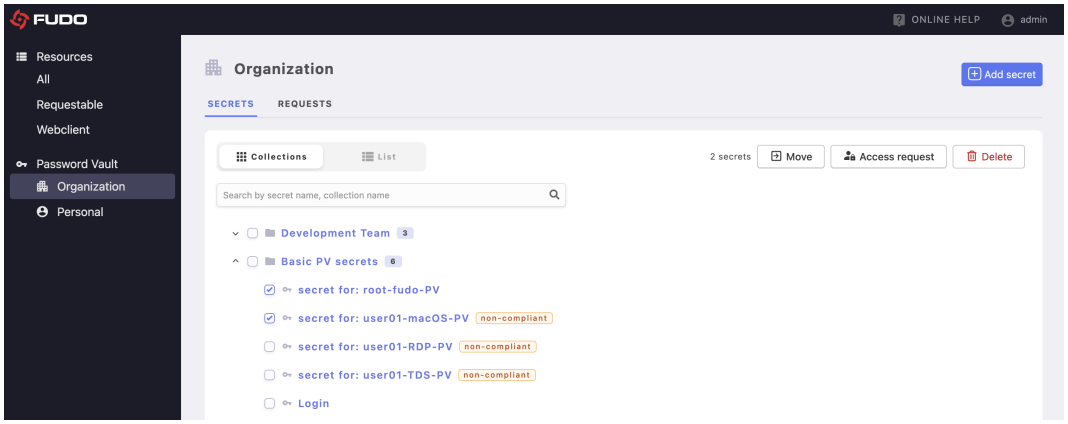
Method 1: Using Context Menu

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.

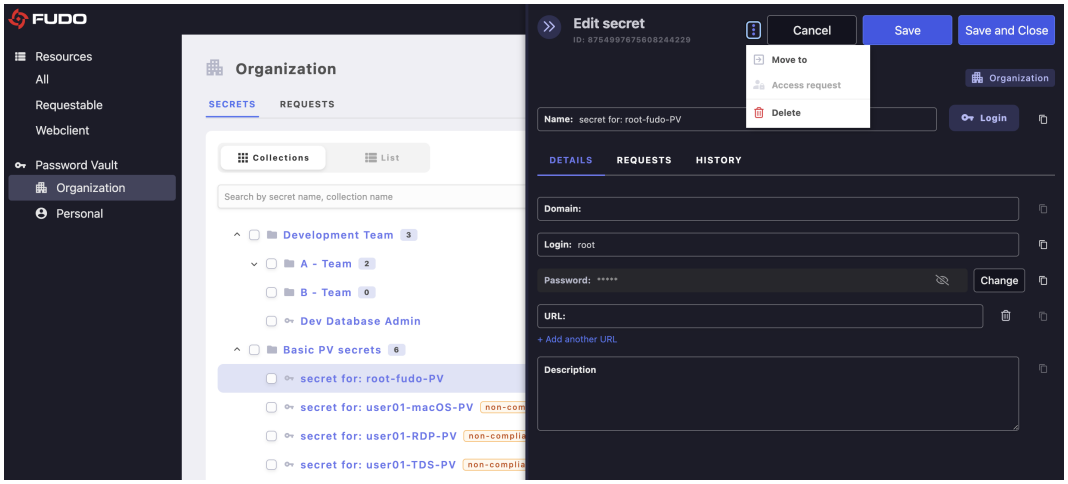
Method 4: Bulk Delete in List View

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*

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.

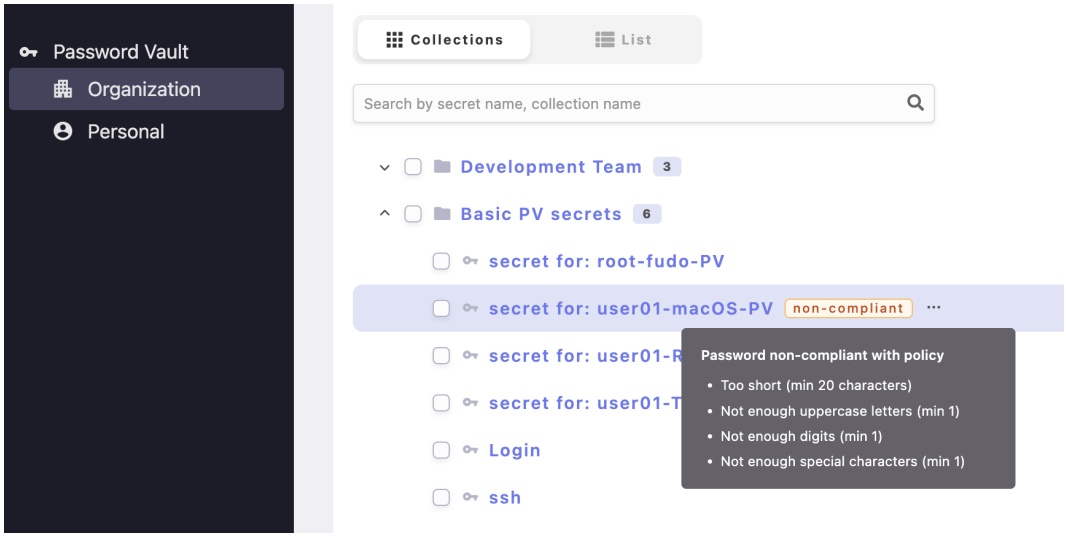
Common Policy Violations

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

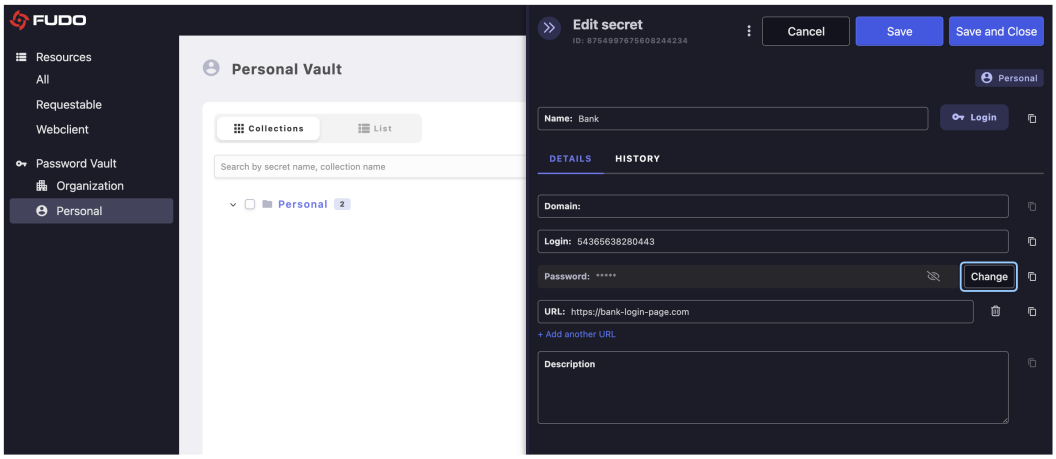
To see which policy requirements a secret violates:

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

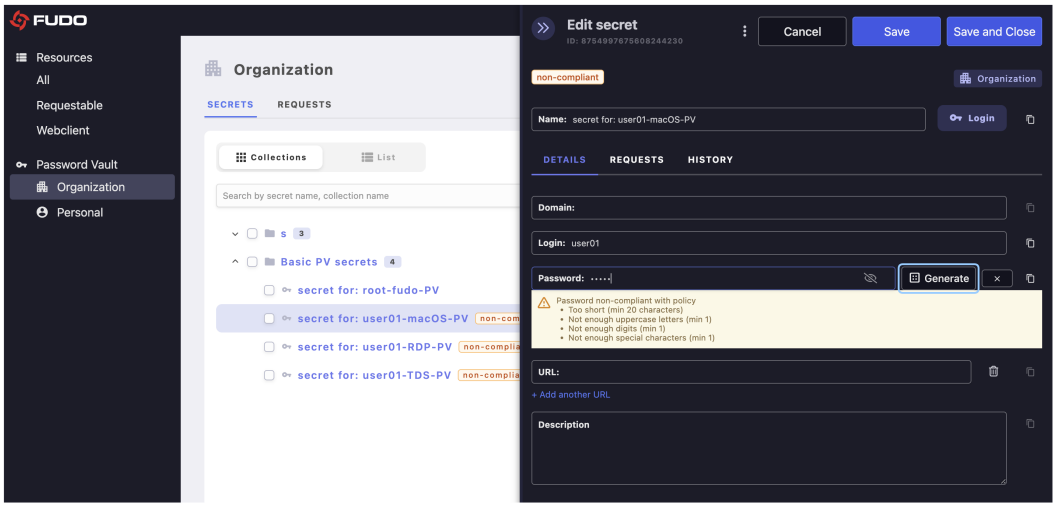


Fixing Non-Compliant Passwords

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.

1.9.5 Managing Collections (Personal Vault)

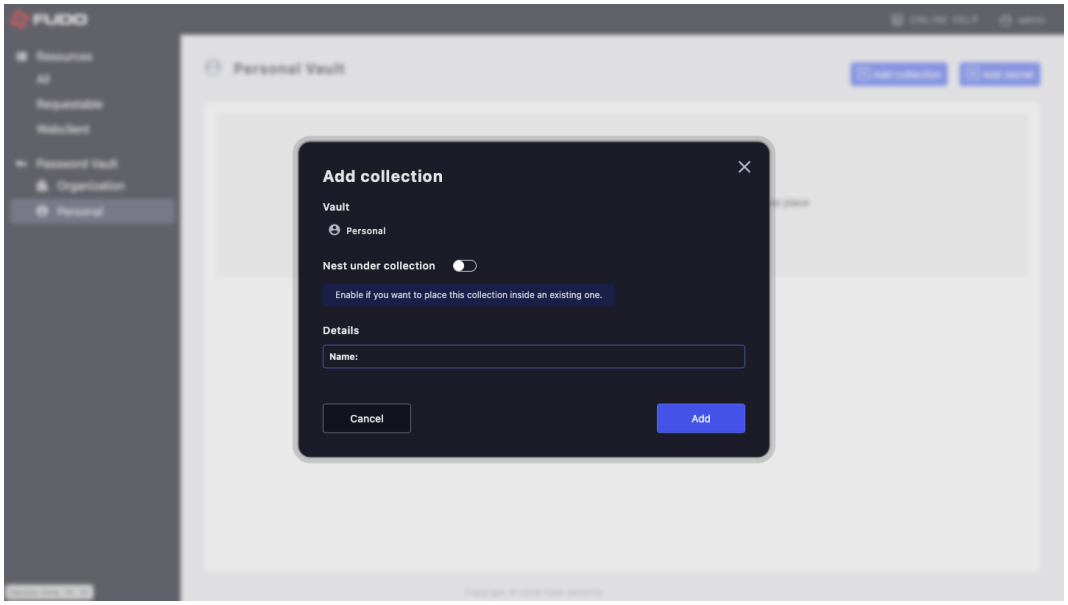
Collections help organize your personal secrets into logical groups. Collection management is only available in the Personal Vault through the User Access Gateway.

> **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.

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

Editing Collection Name

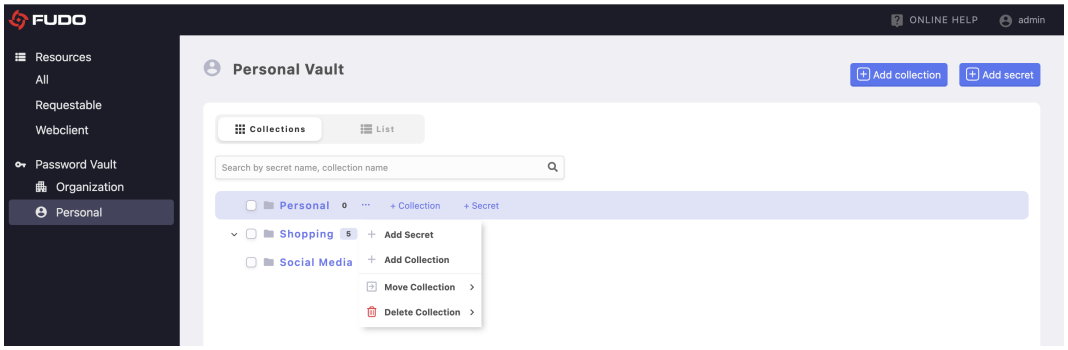
To edit an existing collection:

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.

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.

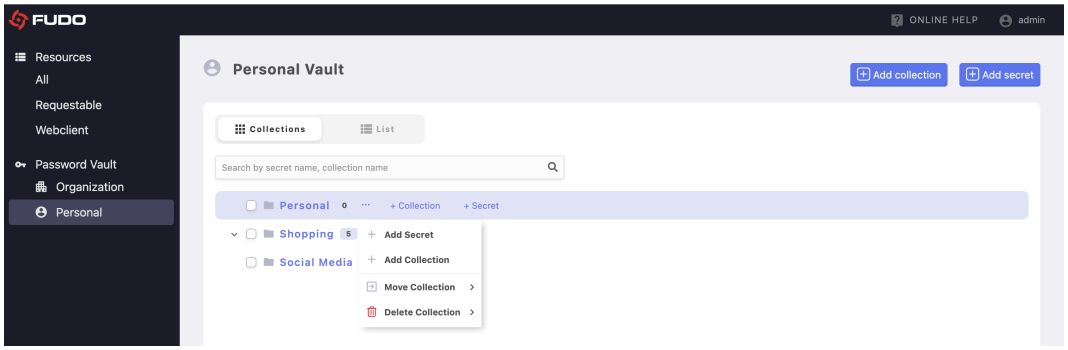
Deleting Collections

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.

1.9.6 Fudo Password Vault Browser Extension

The Fudo Password Vault browser extension lets users access secrets stored in Fudo Enterprise directly from supported desktop browsers: Chrome, Firefox, and Safari.

After signing in with their Fudo Enterprise user credentials and providing the User Access Gateway address, users can browse available collections, search for secrets, and open linked websites directly from the extension. When a login form is recognized, the extension can suggest autofilling the matching secret, making access to web resources faster and more convenient.

The extension also supports Password Vault access workflows. If a secret requires approval, users can request access directly from the browser. Once access is granted, a notification is displayed on the page. For secrets protected with exclusive checkout, the extension shows how much time remains before the checkout expires.

Users who have a Personal Vault can also create and edit their own secrets and collections directly in the extension, without opening the User Access Gateway in a separate tab.

Note

The extension is available to customers with a Full Password Vault license. It supports desktop browser versions only and is available in English and Polish.

Installation

Install the extension from your browser's official add-on store, then pin it to the toolbar for quick access.

Chrome and other Chromium-based browsers

Install the extension from the Chrome Web Store. If the link is unavailable, search the store for **Password Vault** by Fudo Security.

Firefox

Install the extension from Firefox Add-ons. If the link is unavailable, search the store for **Fudo Password Vault**.

Safari

Install the extension from the Mac App Store, then enable it under *Safari* > *Settings* > *Extensions*. If the link is unavailable, search the store for **Fudo Password Vault**.

Note

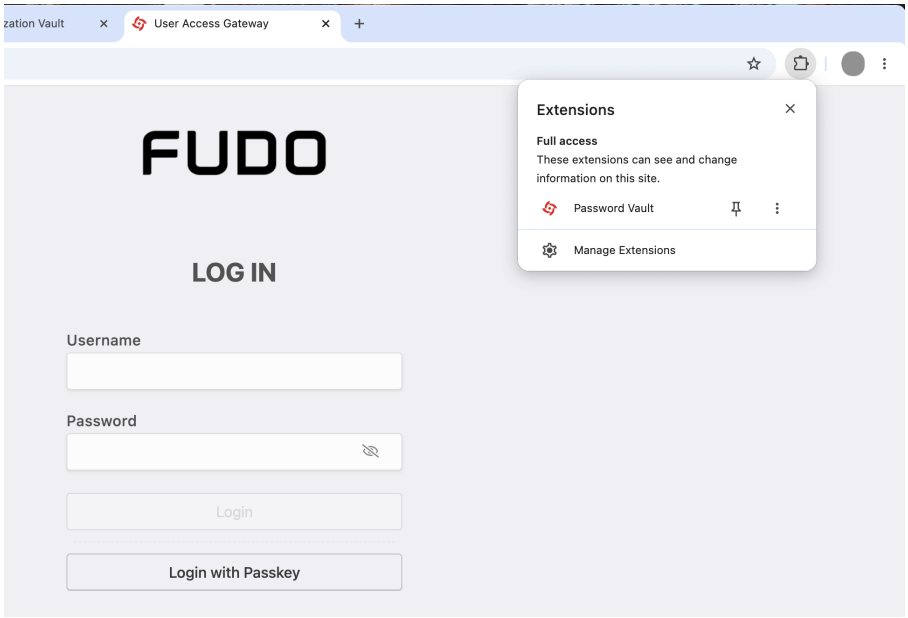
Safari also requires you to grant the extension access to websites. To grant access:

1. Open *Safari* > *Settings* (*Cmd+,*) > *Extensions*.
2. Select **Password Vault** in the left sidebar.
3. Click **Edit Sites...**.

4. At the bottom of the list, set **When visiting other sites:** to **Allow**.
5. Close Settings.

Opening the Extension

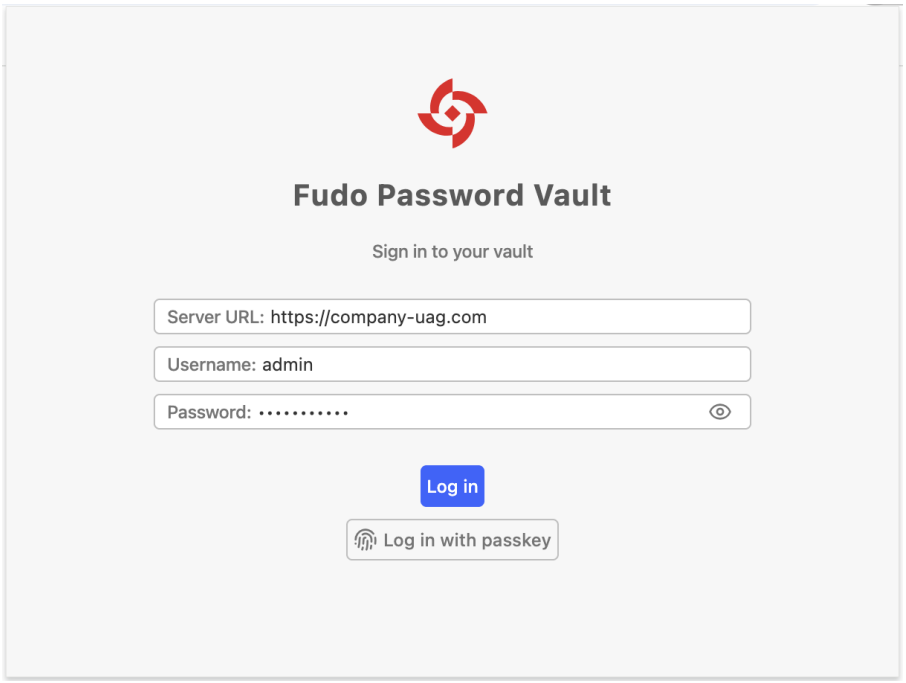
After installation, open the extension from the browser toolbar. In Chrome, click the **Extensions** (puzzle) icon, then select **Password Vault**; you can also pin it to the toolbar for quicker access.



Signing In

To start using the extension:

1. Open the extension from the browser toolbar.
2. Enter the User Access Gateway address of your Fudo Enterprise instance in the **Server URL** field.
3. Enter your Fudo Enterprise user **Username** and **Password**.
4. Click **Log in**.



Note

The connection to the User Access Gateway must use HTTPS with a publicly trusted certificate (issued by a public certificate authority).

Once signed in, the extension connects to User Access Gateway Fudo Enterprise and displays the secrets you are allowed to access.

Signing in with a passkey

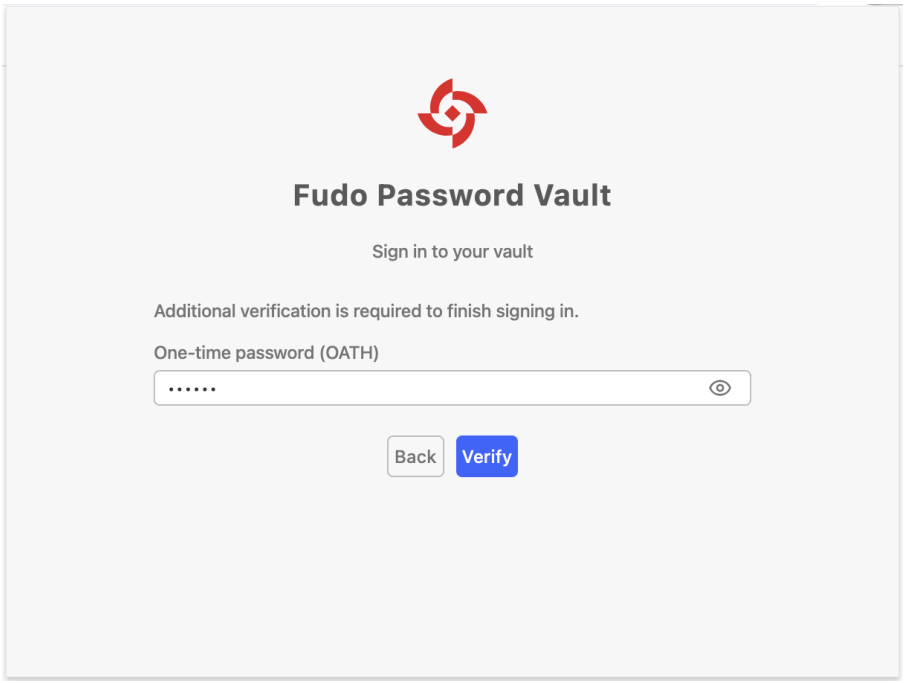
If your account is configured for FIDO2/Passkey authentication, click **Log in with passkey** below the **Log in** button instead of entering a password. The browser then prompts you for your passkey and completes the sign-in.

Note

Passkey sign-in works only when the **Server URL** is a hostname (FQDN), not an IP address - a browser will not use a passkey for an address such as `https://192.168.1.10/`. For details, see the FIDO2/Passkey authentication chapter.

Providing a second authentication factor

If your account requires a second authentication factor, the extension replaces the login form with a verification screen after you submit your credentials. The screen names the method the server expects - for example **One-time password (OATH)** - and provides a field for your response. Methods that require token enrollment additionally display an enrollment QR code.



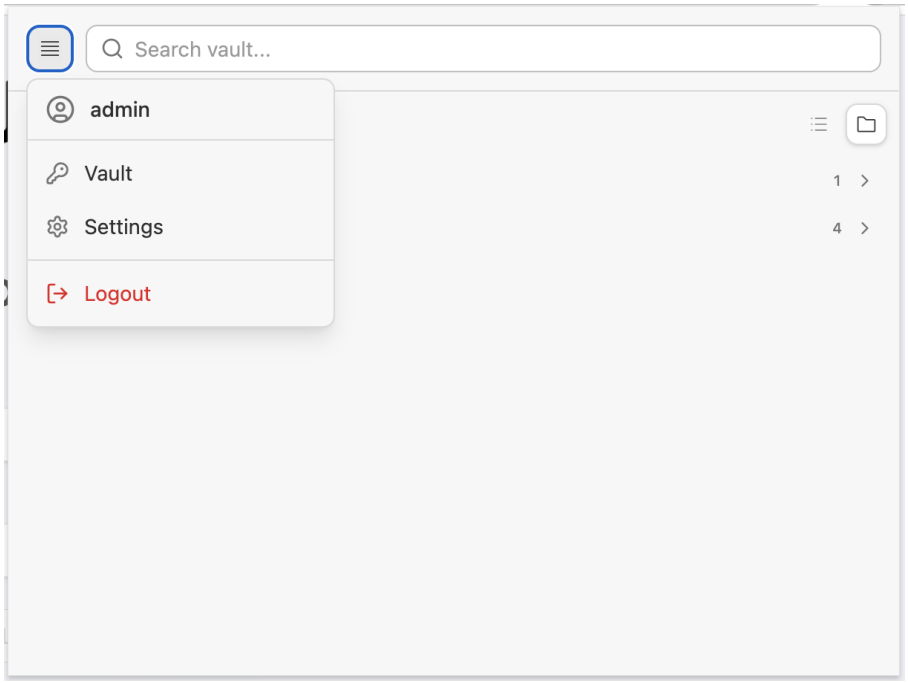
Enter the code provided by your authentication method and click **Verify**, or click **Back** to return to the login form. If the code is not accepted, the sign-in attempt is cancelled and you have to start over with **Back to sign in**.

Important

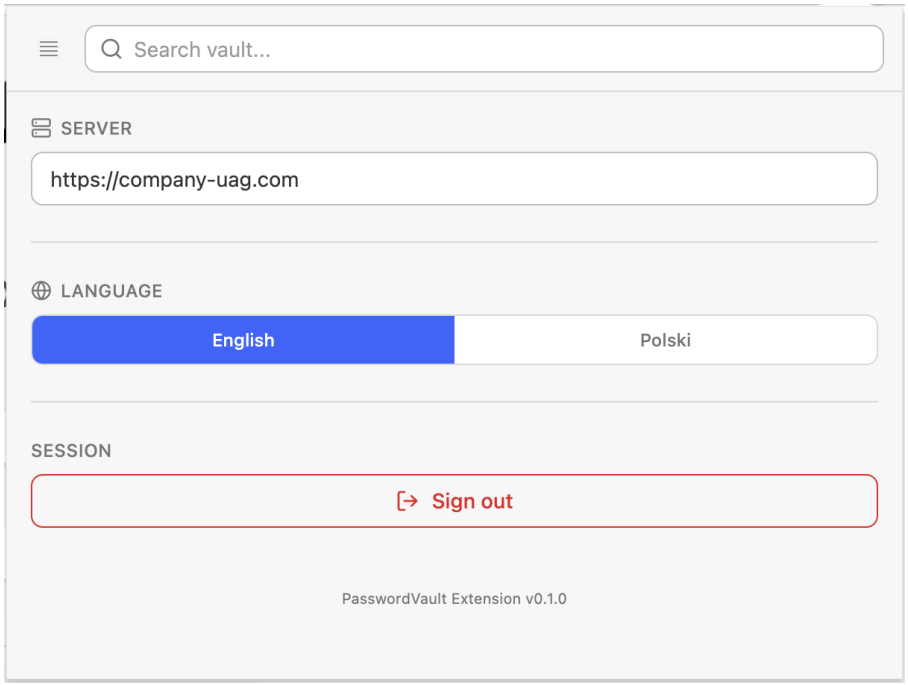
The available second-factor methods come from your user configuration in the Fudo Enterprise Admin Panel. The extension does not configure authentication - it only follows what the server requires.

Extension Menu and Settings

The menu button in the top-left corner opens the extension menu, which provides access to the **Vault**, the **Settings**, and the **Logout** option.

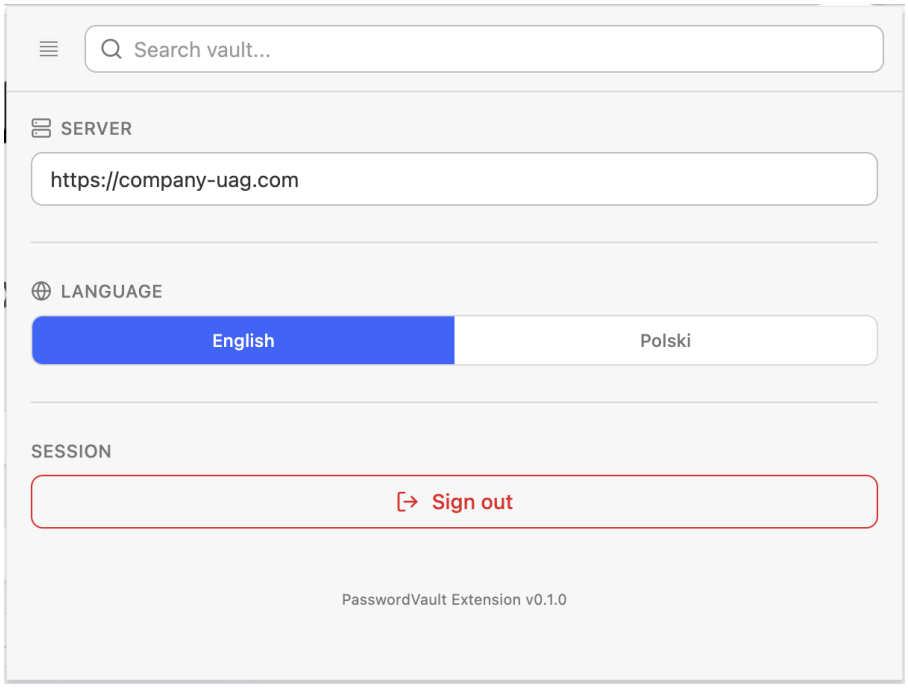


On the **Settings** screen you can review the **Server** (User Access Gateway) address and switch the interface **Language** between English and Polish.



Signing Out

To end your session, open the extension menu and select **Logout**, or click **Sign out** in the **Session** area of the **Settings** screen.



Browsing Collections and Secrets

After signing in, you can switch between a **collection view** and a **secret list view** using the buttons in the top-right corner, limit the list to a single vault with the **All** / **Organization** / **Personal** buttons, and use the **Search vault** field to find a secret by name.

Important

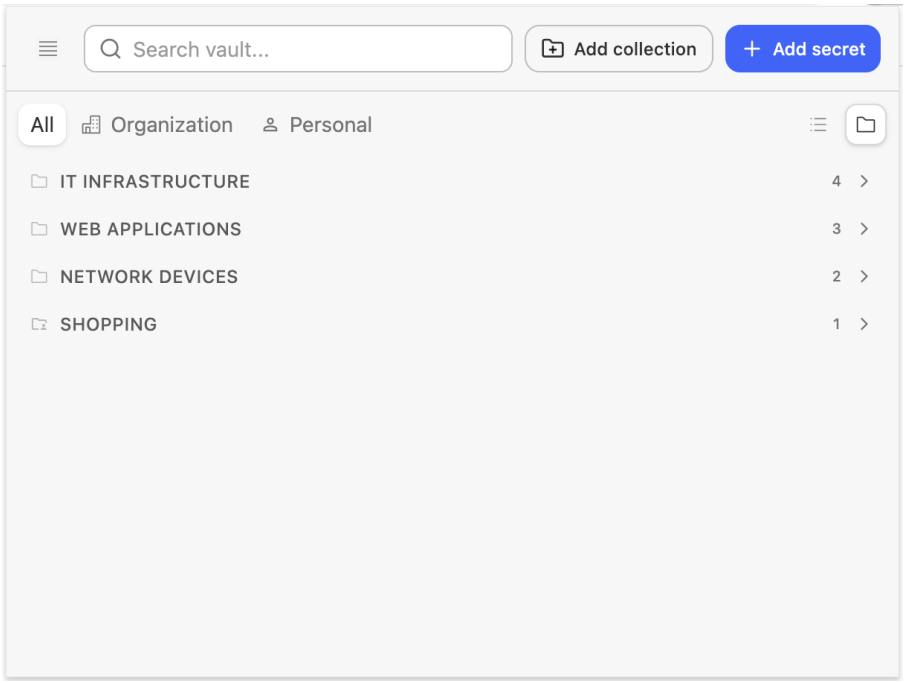
The extension reflects the same permissions configured in the Password Vault: you see only the collections and secrets you have been granted access to through object rights.

Filtering by vault

The buttons above the list limit it to secrets from one vault:

- **All** - secrets from both vaults. This is the default.
- **Organization** (building icon) - only secrets from the Organization Vault.
- **Personal** (person icon) - only your own secrets from the Personal Vault.

With the **All** filter active the two kinds can still be told apart: in the list view each secret carries the icon of its vault, and in the collection view personal collections use a different folder icon than organization ones.

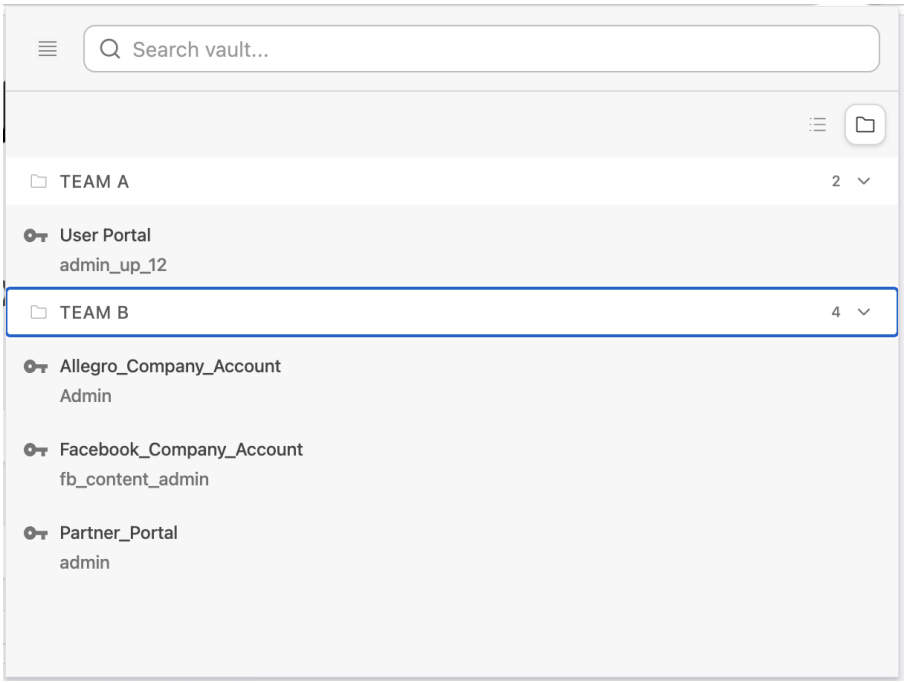


Important

The **Search vault** field searches **only within the selected vault**. With **Personal** selected you will not find an organization secret, and the other way round. If a secret you expect is missing from the results, switch the filter back to **All**.

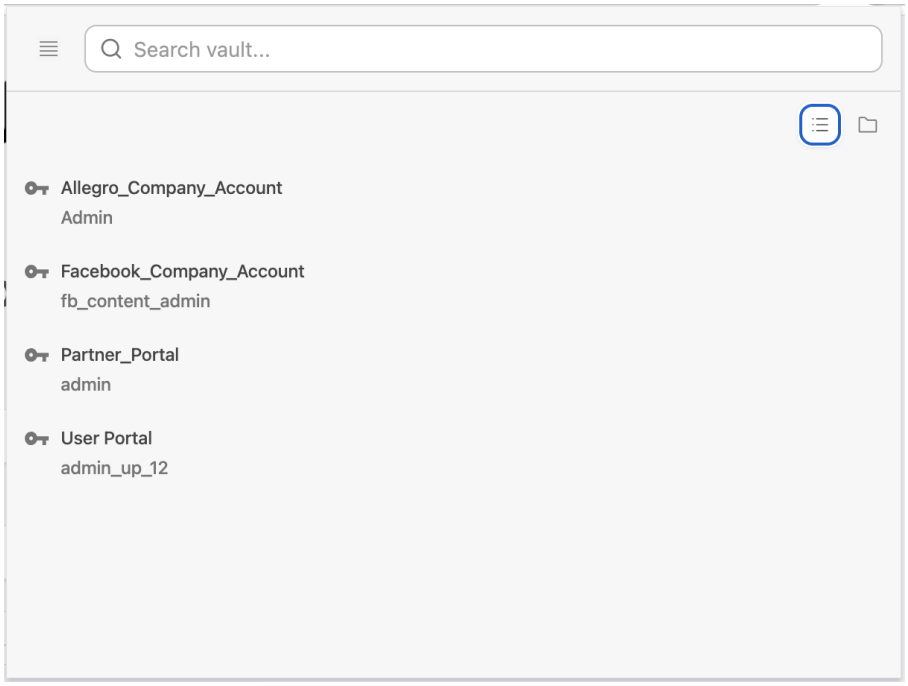
Collection view

The collection view groups secrets under the collections they belong to.



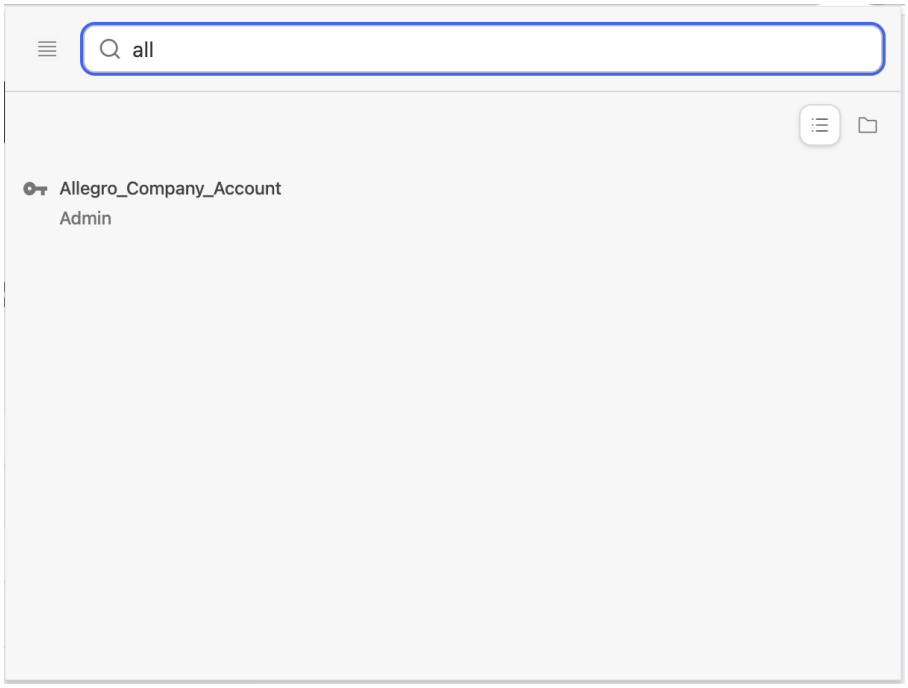
Secret list view

The list view shows all available secrets in a single flat list.



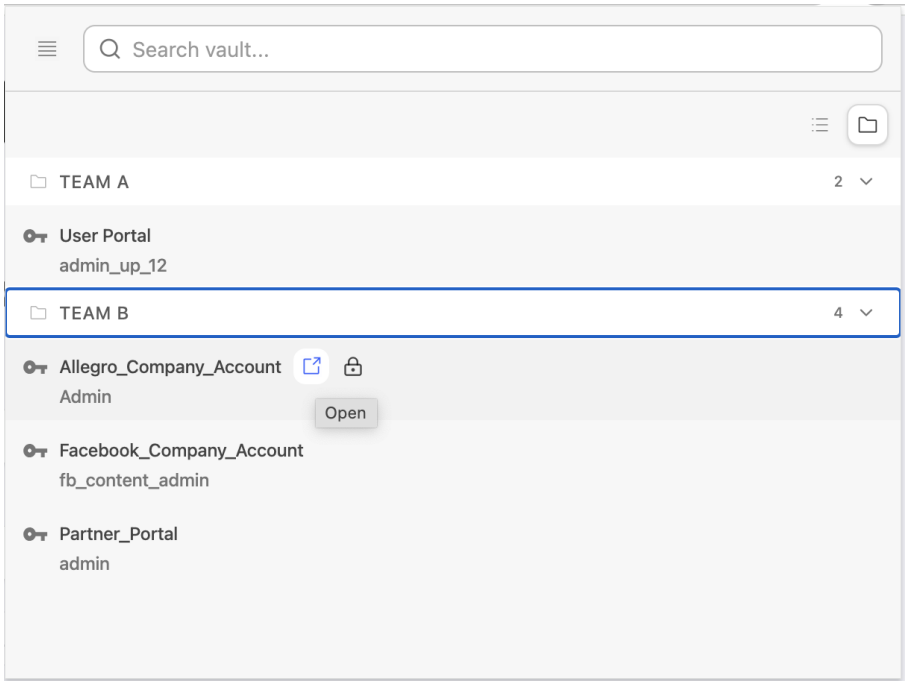
Search

Type in the **Search vault** field to filter secrets by name. The search covers only the vault selected with the **All** / **Organization** / **Personal** buttons.



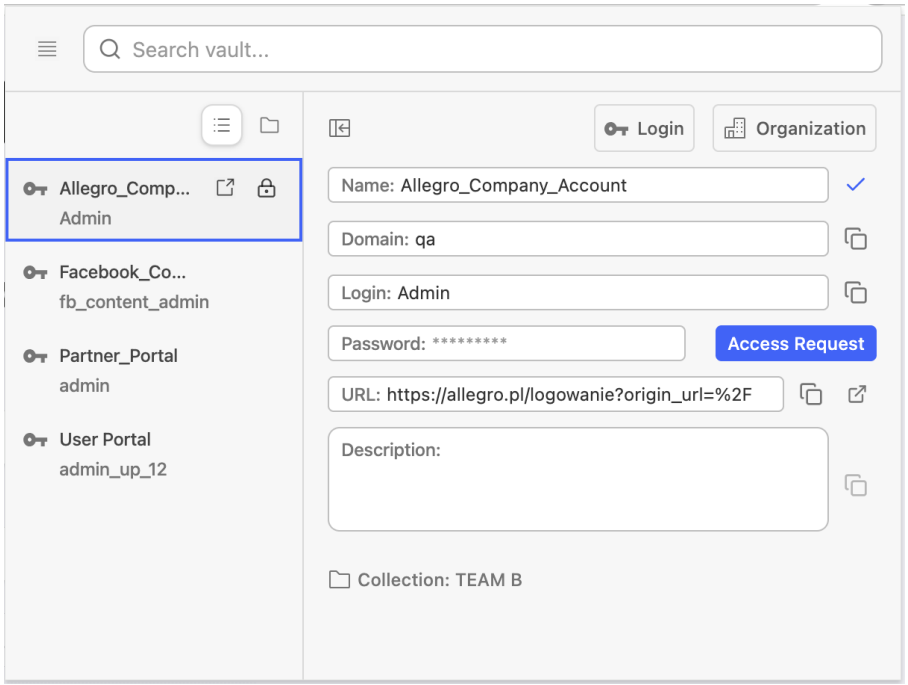
Opening a linked website

Each secret shows an **Open** icon that links to the website the secret is associated with. Selecting it opens the linked website directly in the browser.



Viewing secret details

Selecting a secret opens its details, where you can review fields such as **Name**, **Domain**, **Login**, **Password**, **URL**, and **Description**, and copy individual values to the clipboard.



Note

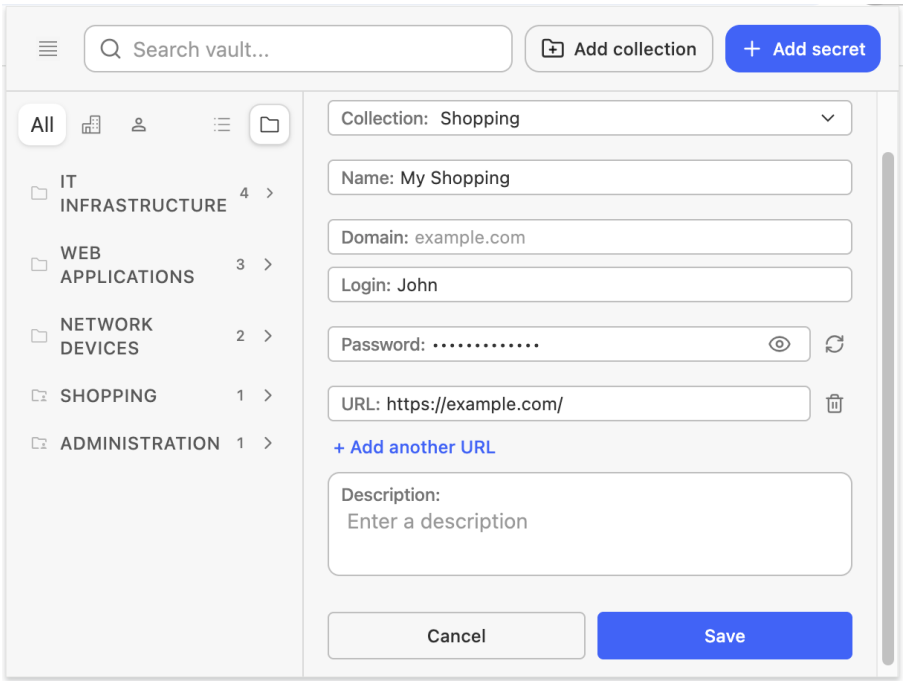
When a password is copied to the clipboard, it is automatically cleared after 30 seconds.

Creating and Editing Personal Secrets

Secrets and collections created in the extension always go to your **Personal Vault**. Organization Vault content is managed by administrators in the Fudo Enterprise Admin Panel and cannot be created or edited from the browser.

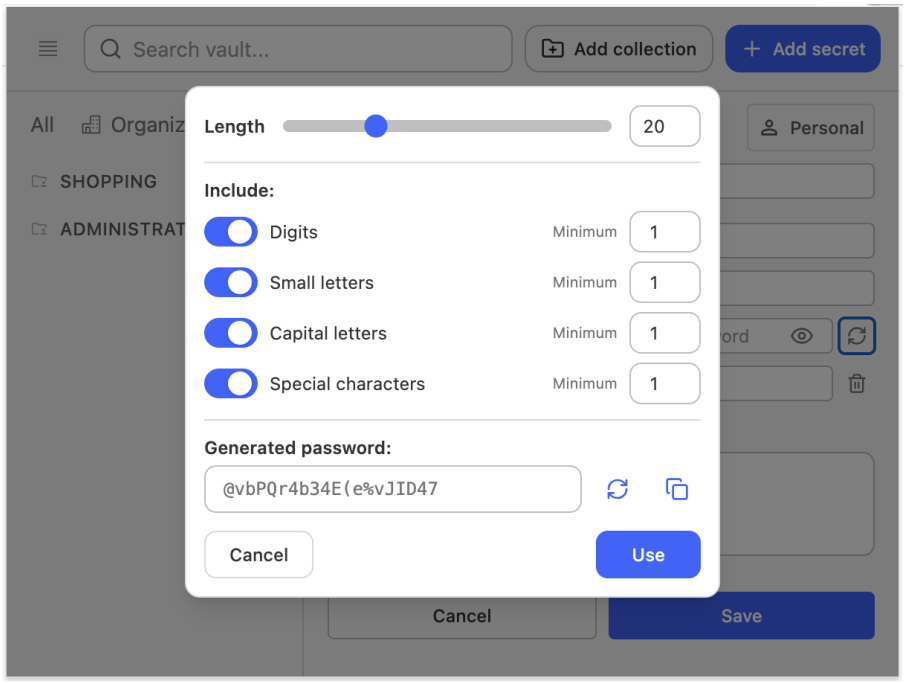
Creating a secret

1. Click **Add secret** in the top bar.
2. Select the **Collection** the secret belongs to. Only personal collections are listed. If you do not have any yet, the form shows **No personal collections available** - create a collection first.
3. Fill in the secret fields:
   - **Name** (required) - the name the secret is listed under.
   - **Domain** - the domain the credentials belong to.
   - **Login** (required) - the user name stored in the secret.
   - **Password** (required) - the password stored in the secret.
   - **URL** - the address the secret is matched against when autofilling. Click + **Add another URL** to store more addresses.
   - **Description** - optional notes.
4. Click **Save**.



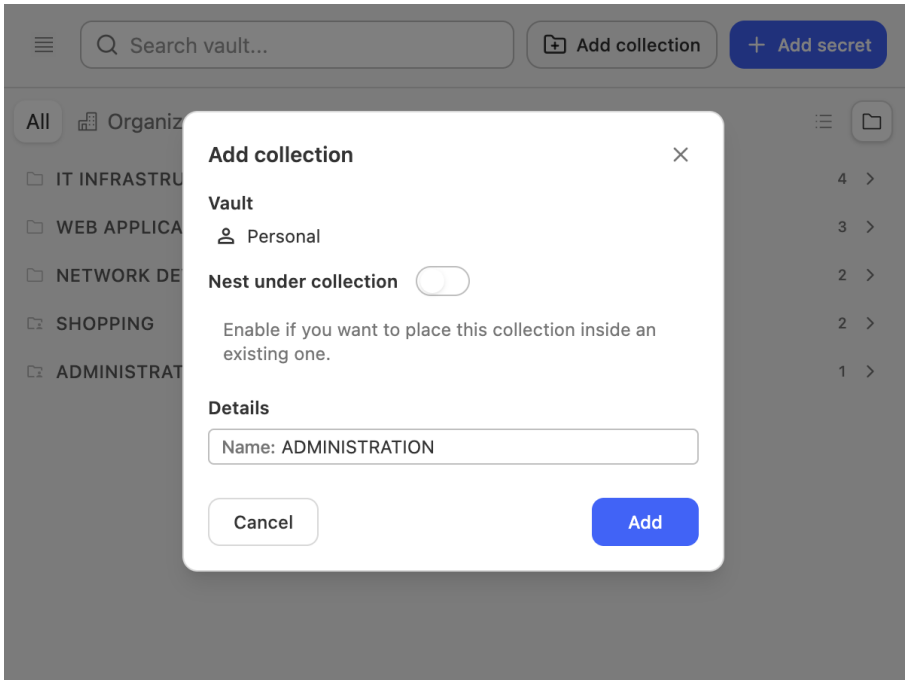
Generating a password

Instead of typing a password, click the generator icon next to the **Password** field. In the dialog that opens set the **Length**, switch on the character groups to **Include** (**Digits**, **Small letters**, **Capital letters**, **Special characters**) and the **Minimum** number of characters from each of them. The result appears under **Generated password** - use the icons next to it to draw another password or copy it to the clipboard, then click **Use** to insert it into the form.



Creating a collection

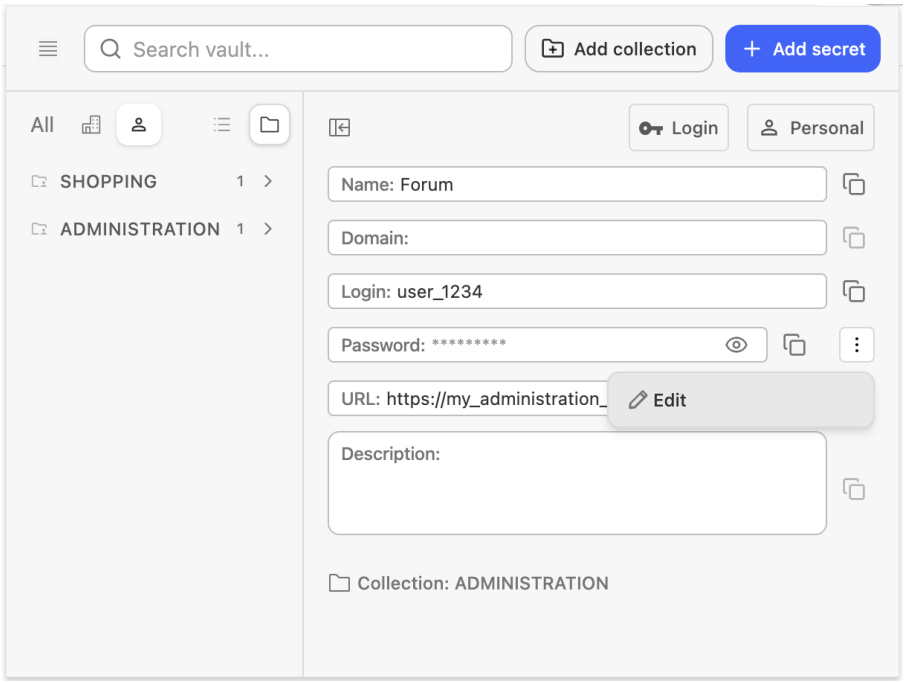
1. Click **Add collection** in the top bar.
2. The **Vault** is always **Personal** and cannot be changed.
3. To place the new collection inside an existing one, enable **Nest under collection** and select the parent collection.
4. Under **Details**, enter the collection **Name**.
5. Click **Add**.



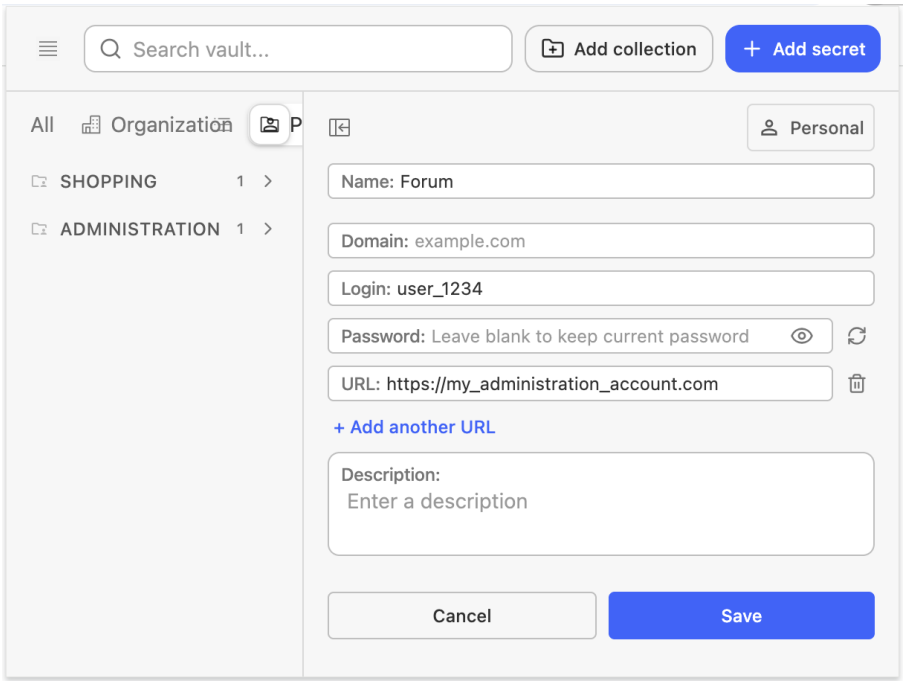
Editing a secret

Open a personal secret, click the three-dot (**More actions**) button next to the **Password** field

and select **Edit**.



The form is the same as when creating a secret, except that the collection cannot be changed. Leave the **Password** field empty to keep the current password.

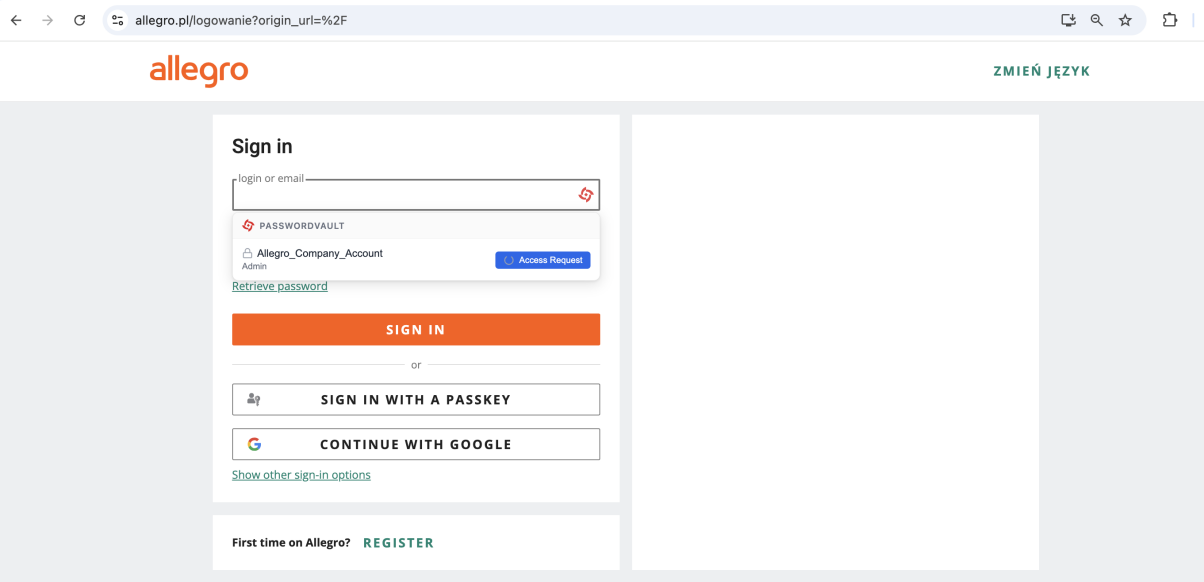


Note

Edit is available only for secrets from the Personal Vault. For organization secrets the **More actions** menu has no **Edit** entry.

Autofilling Credentials on Websites

When you open a page whose login form is recognized, the extension displays a suggestion bar offering to autofill the matching secret. Selecting the suggestion fills in the stored credentials, making access to web resources faster and more convenient.

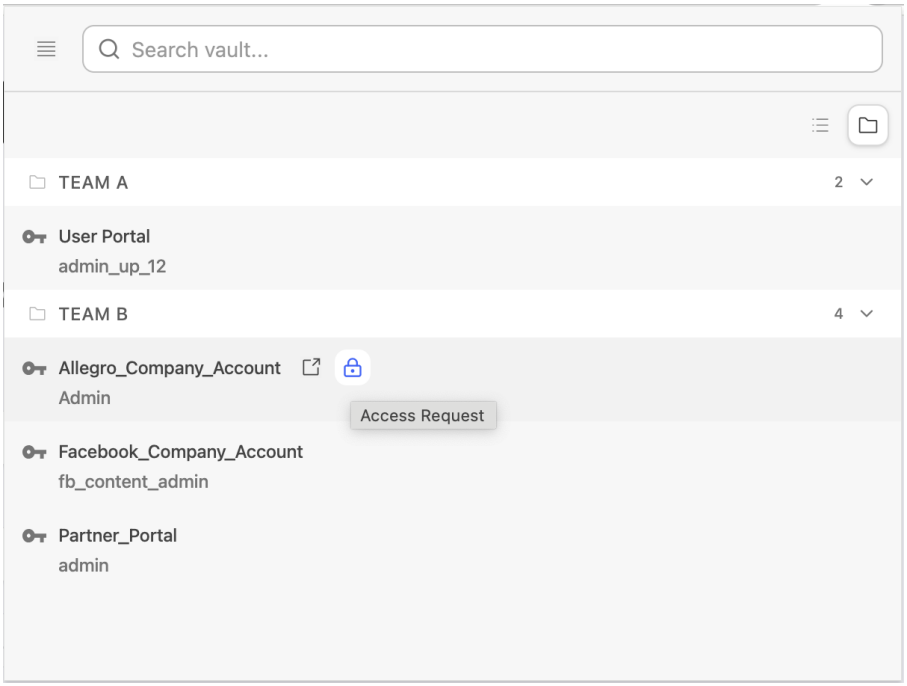


Access Requests, Exclusive Checkout, and Revoked Access

The extension supports Password Vault access workflows directly from the browser.

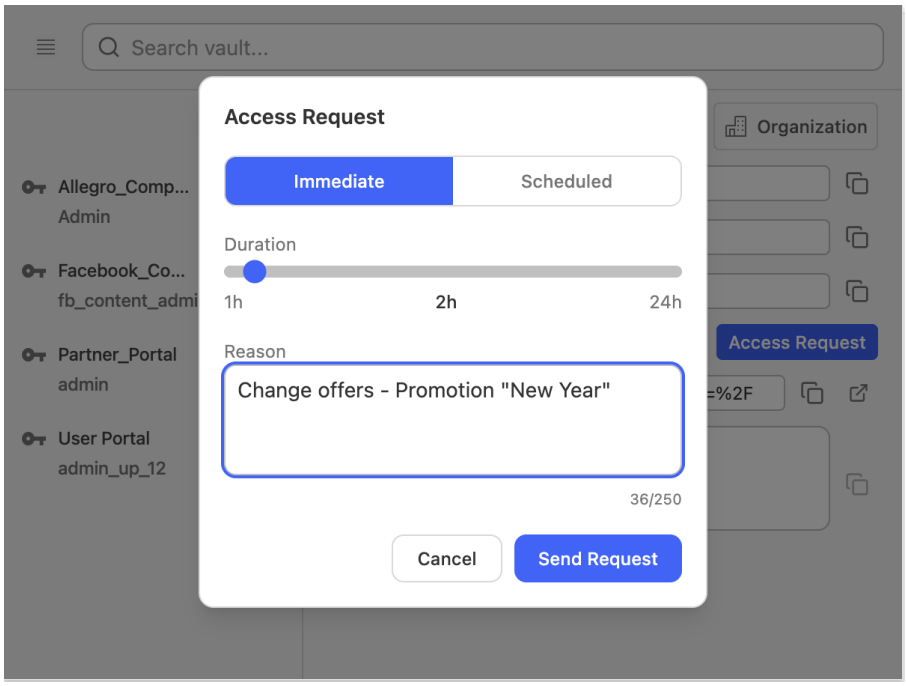
Requesting access

If a secret is configured for access on request, it is marked with a padlock (**Access Request**) icon. Hover over the secret and click the icon to request access.

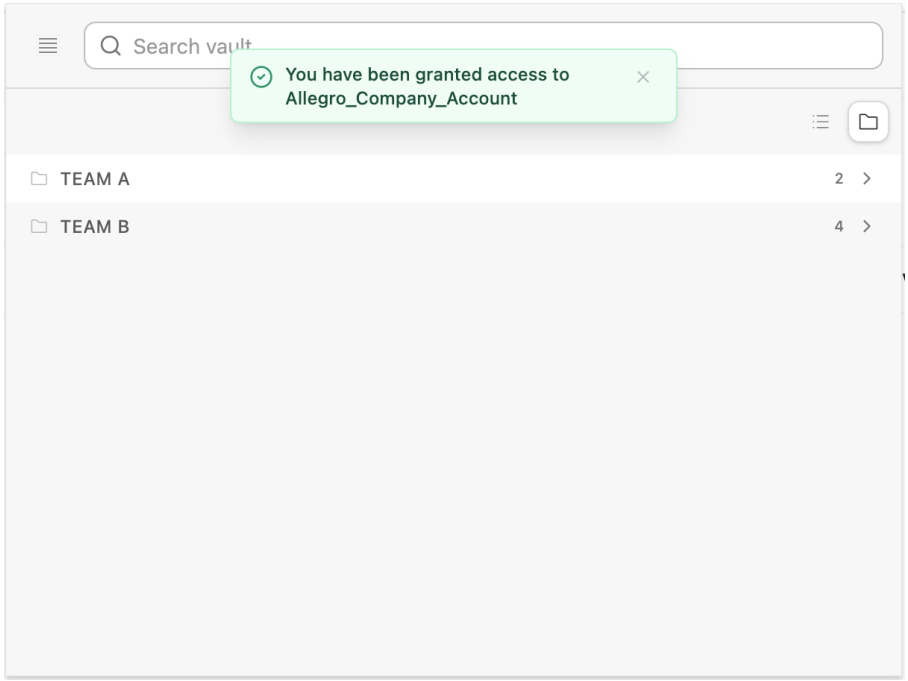


In the **Access Request** form, choose whether access should be granted **Immediate**ly or

Scheduled for later, set the **Duration, enter a **Reason** for the request, and click **Send Request**.

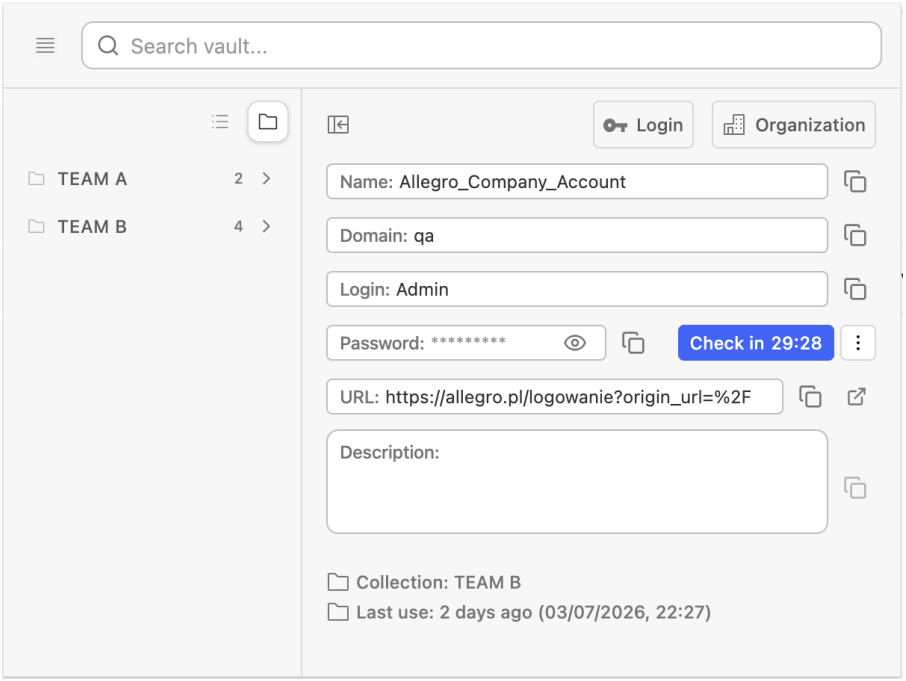


Once access is granted, the extension displays a confirmation notification.



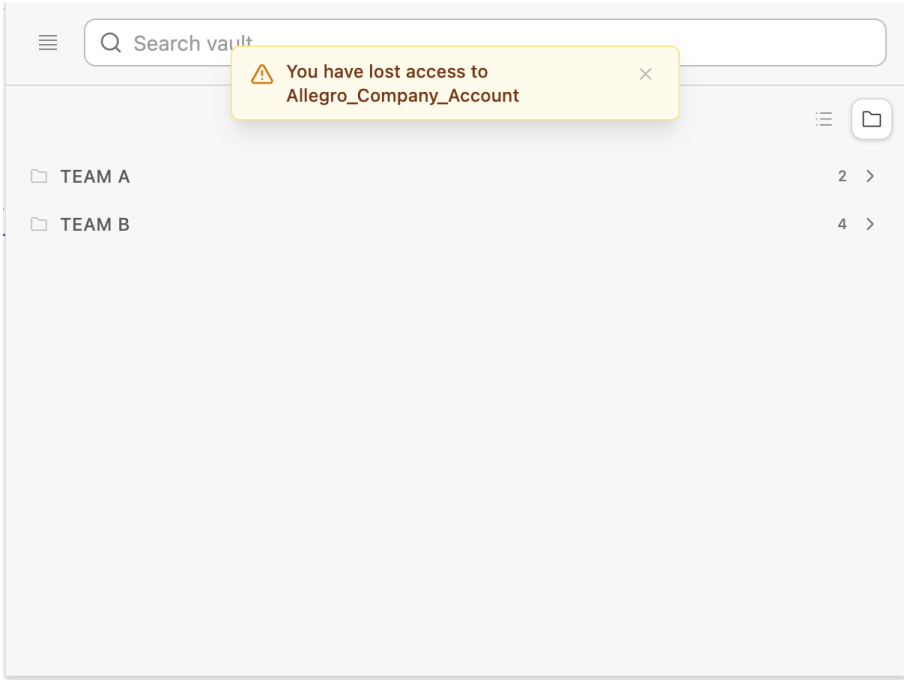
Exclusive checkout

For secrets protected with exclusive checkout, the **Check in** button in the secret details displays a countdown showing how much time remains before the checkout expires.



Revoked access

If your access to a secret is revoked, a crossed-out icon appears next to it and the secret is marked with an **Access refused** button in the list. The extension also displays a notification informing you that access has been lost.



1.10 Establishing Connections

1.10.1 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.

Note

For some accounts an access request is required only at certain hours. If the administrator configured the safe for time-based Just-in-Time access, you can connect directly during the hours covered by your daily access policy, and you have to send an access request outside those hours. Such an account is not shown as blocked outside its hours - the request option is offered instead. Sending a request is also possible during the covered hours, even though it is not required then.

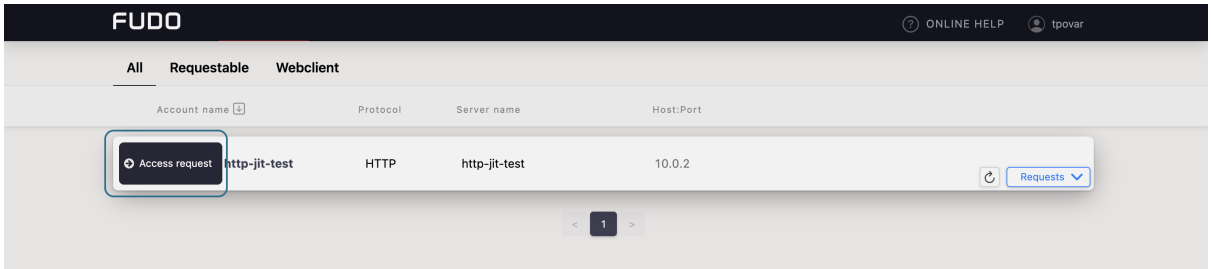
Caution

A session started during the hours covered by your daily access policy is terminated when those hours end, unless an approved access request covers the remaining time.

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.

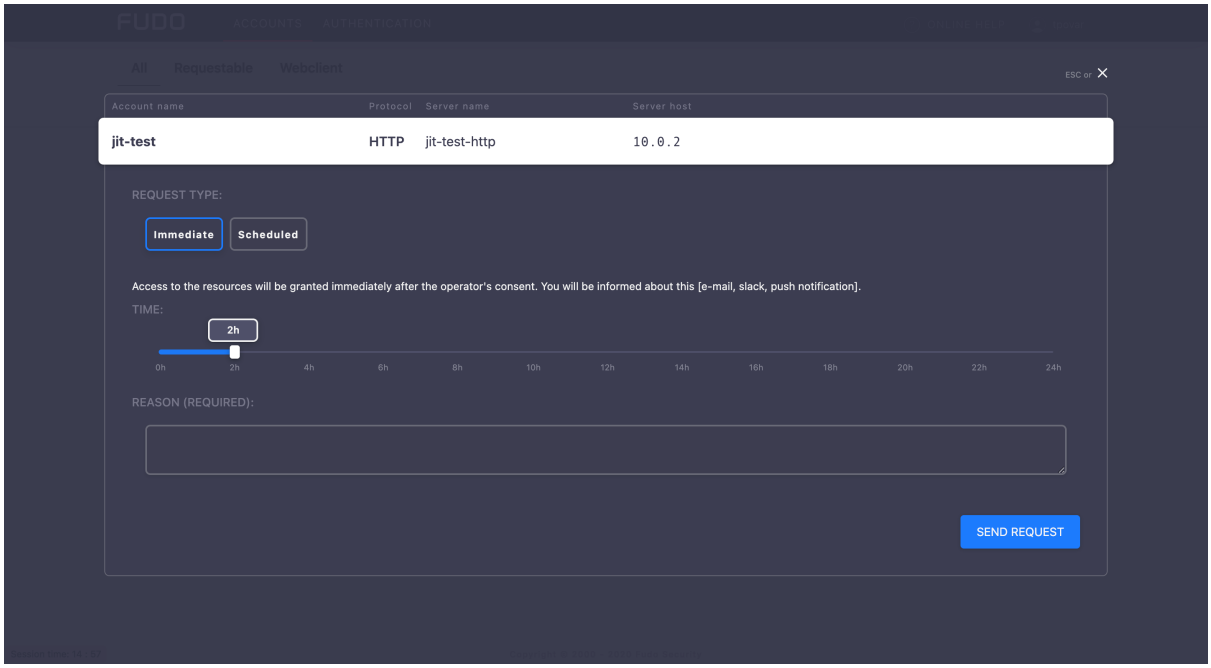


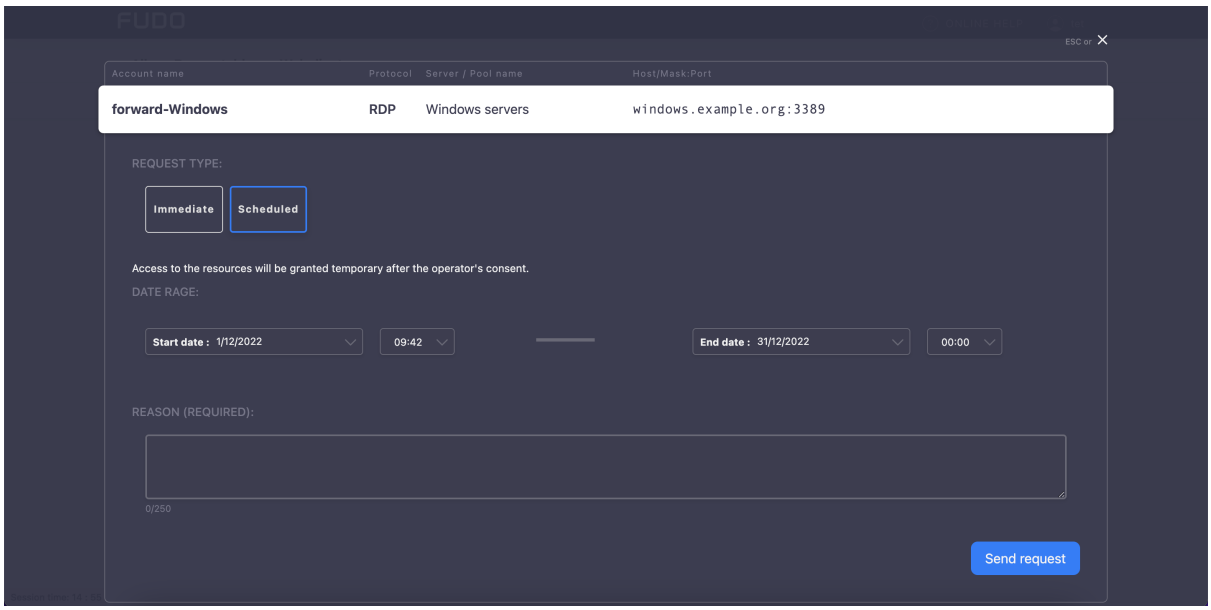
3. Select a type of the request: immediate or scheduled.

Note

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

4. Define the request time.



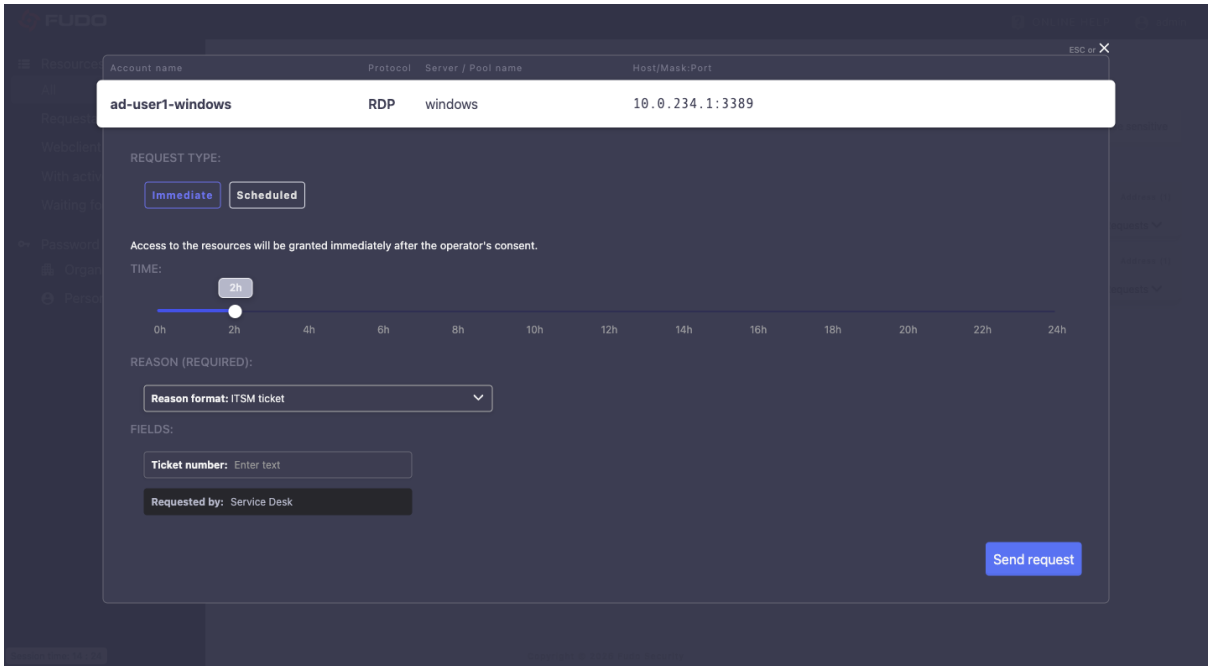


5. Click the *Send request* button.

Reason format

If the administrator has defined reason formats, the request window shows a *Reason format* list. The default option is *Free-form text*, which works as before - you type the reason yourself.

Selecting a format replaces the text box with the fields of that format. Fill them in and the reason is composed for you.



Note

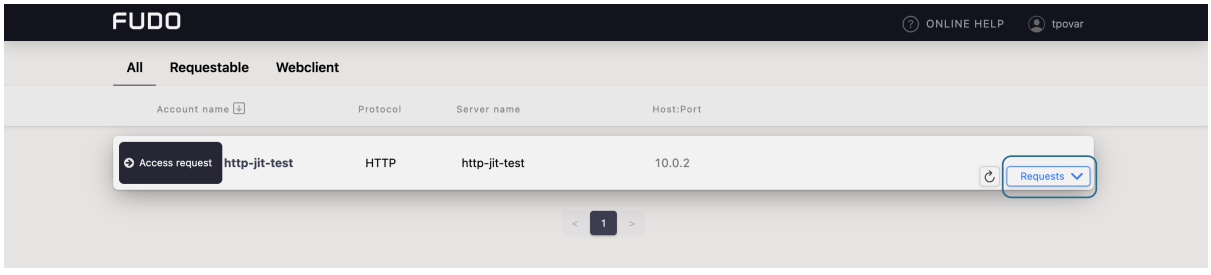
- **All fields of a format must be filled in**, otherwise the request cannot be sent.
- Some fields may already contain a value that cannot be changed - the administrator set it as a fixed part of the reason.
- A field description may appear under the format name if the administrator provided one.
- If the format is changed by the administrator while you are filling in the form, the request is rejected with the message *The reason does not match the selected format. Refresh the format and try again.* Reload the page and send the request again.

Watching Request Status

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

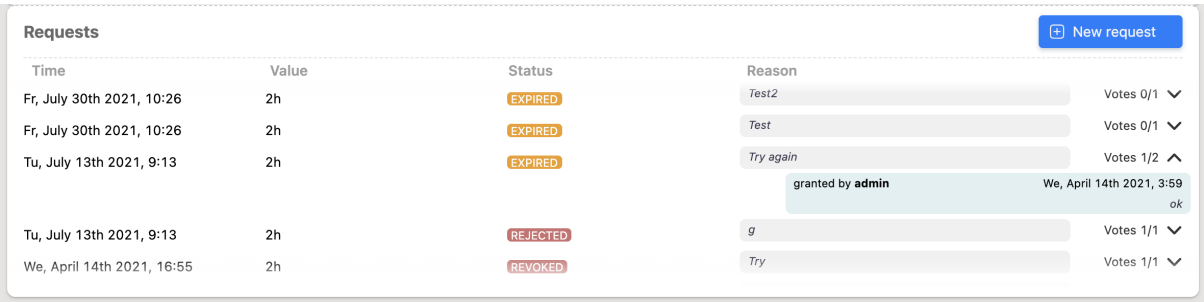
- `Access Request accepted` - the request was approved by the required amount of the administrators.
- `Access Request rejected` - the request was denied.

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.

1.10.2 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.

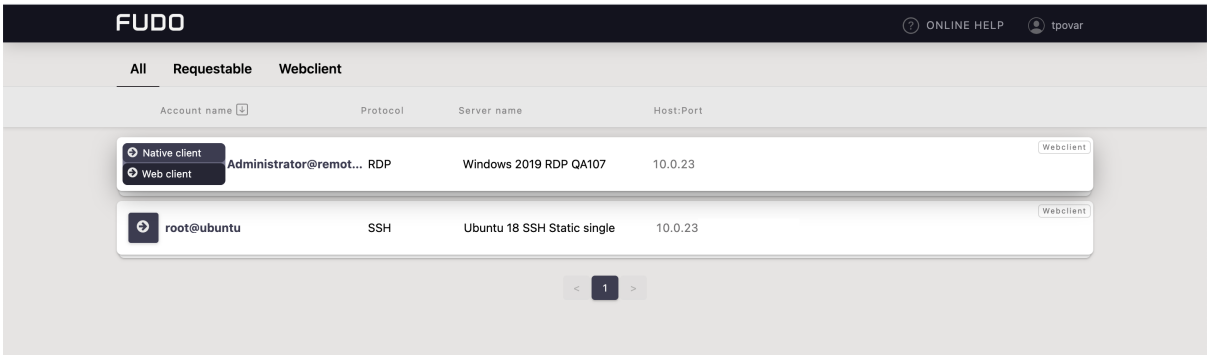
Note

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

- *English (US)*,
- *German*,
- *German (Swiss)*,
- *French* (AZERTY),
- *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.

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

After opening the session, copy the login reason text on your computer, return to the session, and right-click in the login reason field.

For details on copying and pasting text, see *Webclient Features*.

Note

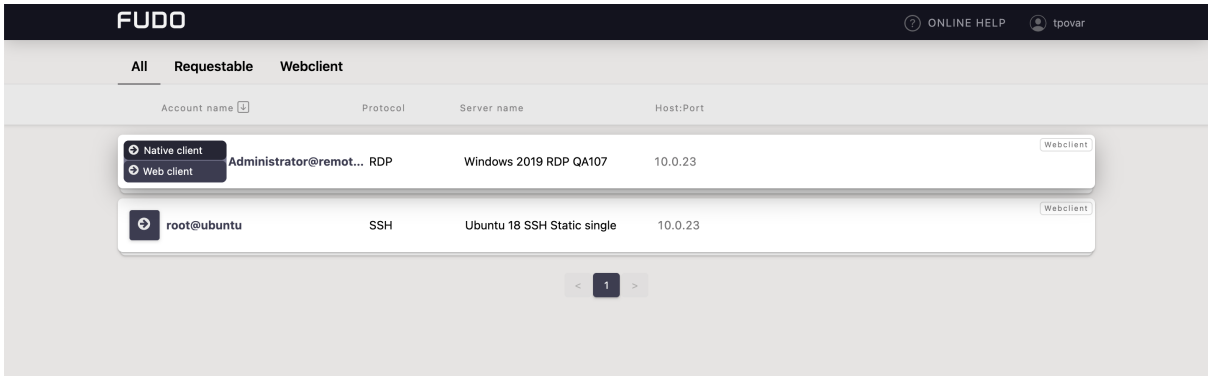
Keep in mind that the clipboard has a character limit for the **Login reason** field: a maximum of **60 characters** for Polish and English text, and **40 characters** for Cyrillic. If the copied text exceeds this limit, it may be truncated or not copied at all.

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*

1.10.3 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.

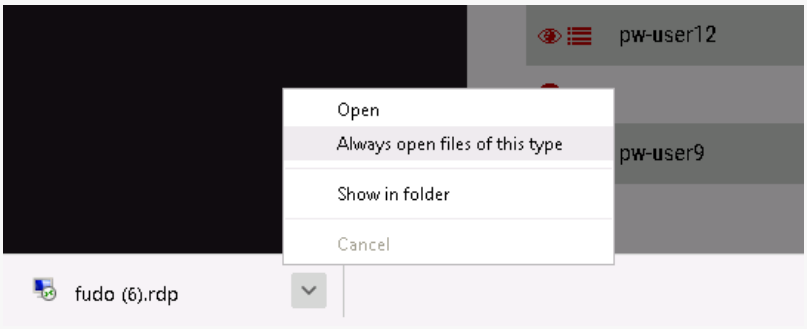


3. Choose the listener, via which you want to connect.

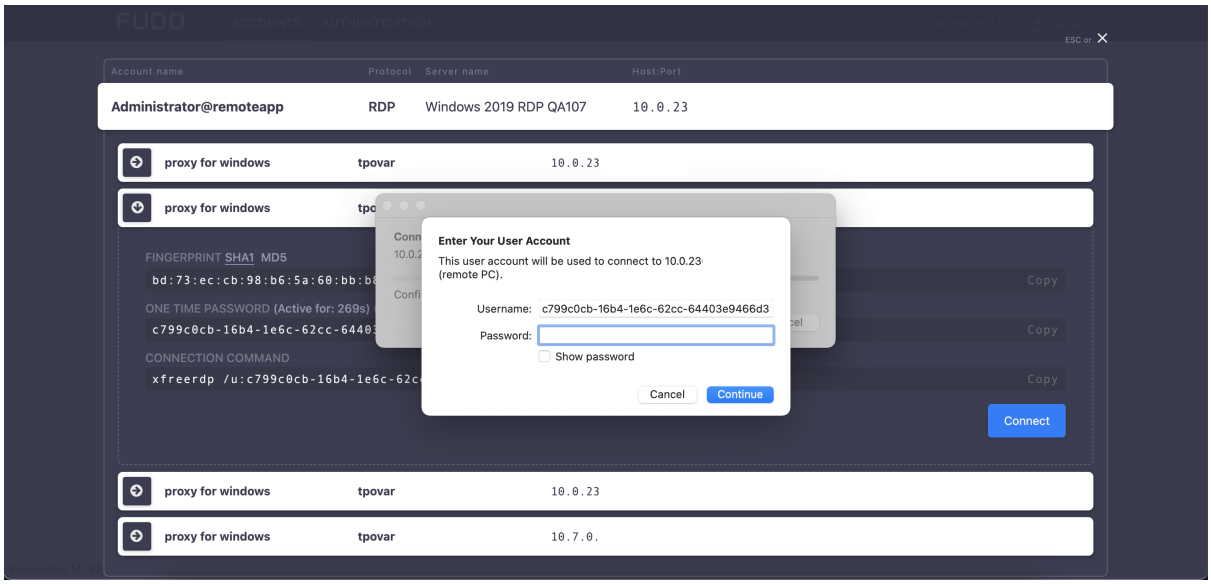
4. Click *Connect*.

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.

Note

Since the April 2026 Windows update, the Remote Desktop client verifies the signature of connection definition files. Files generated by the User Access Gateway are usually signed, so you can select *Don't ask again for connections to this publisher* and the warning will not be shown again for that publisher. If the warning says the publisher is unknown, the file is not signed and the warning appears on every connection. Contact your administrator to find out which certificate signs the files.

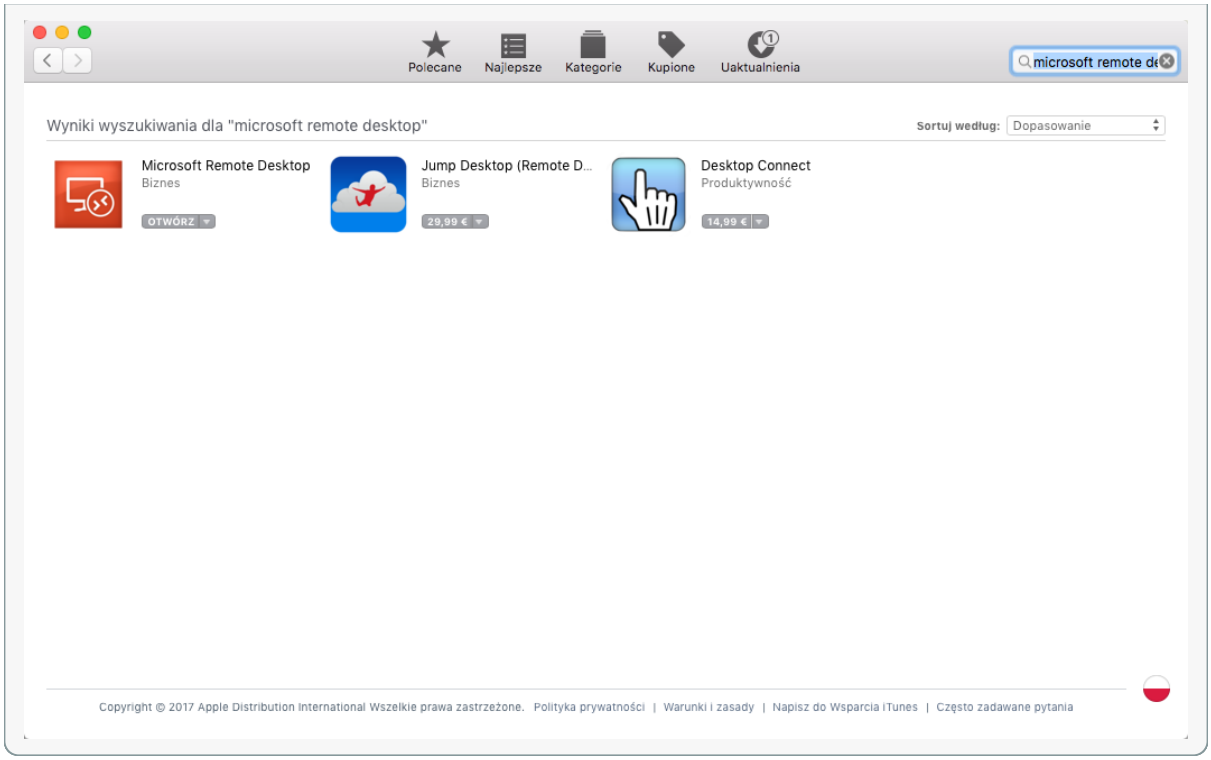
Related topics:

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

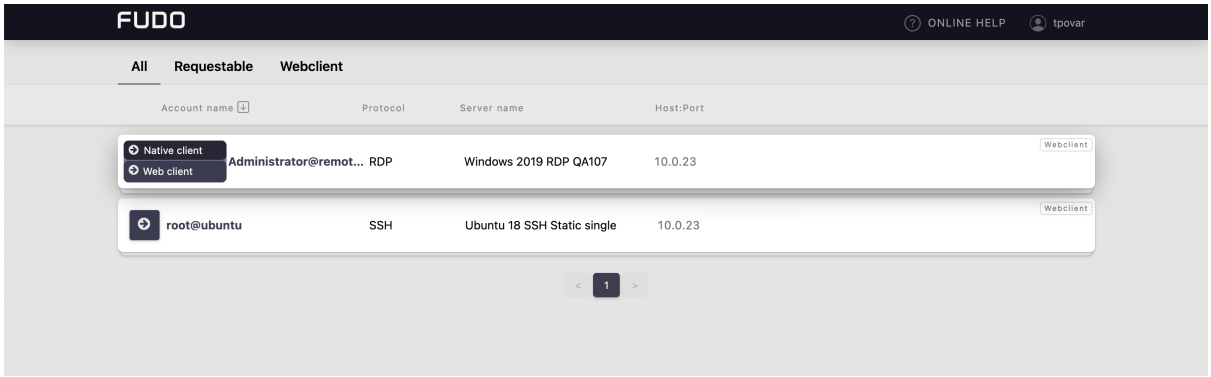
1.10.4 Connecting Over RDP on MAC OS X

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.

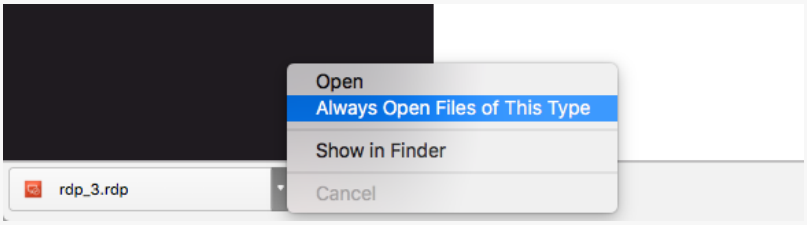


3. Choose the listener, via which you want to connect.

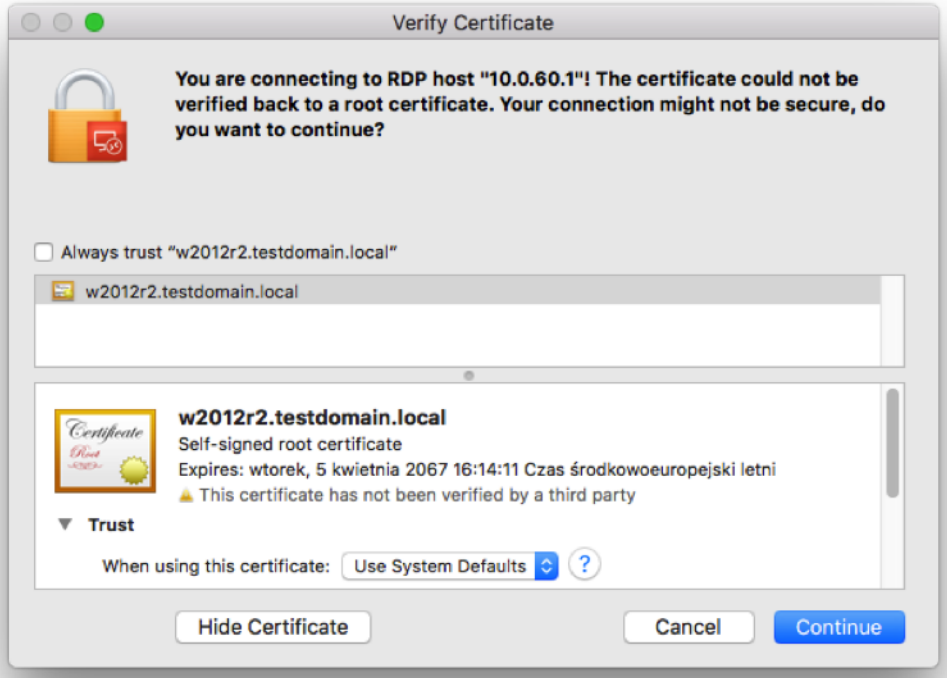
4. Click *Connect*.

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.



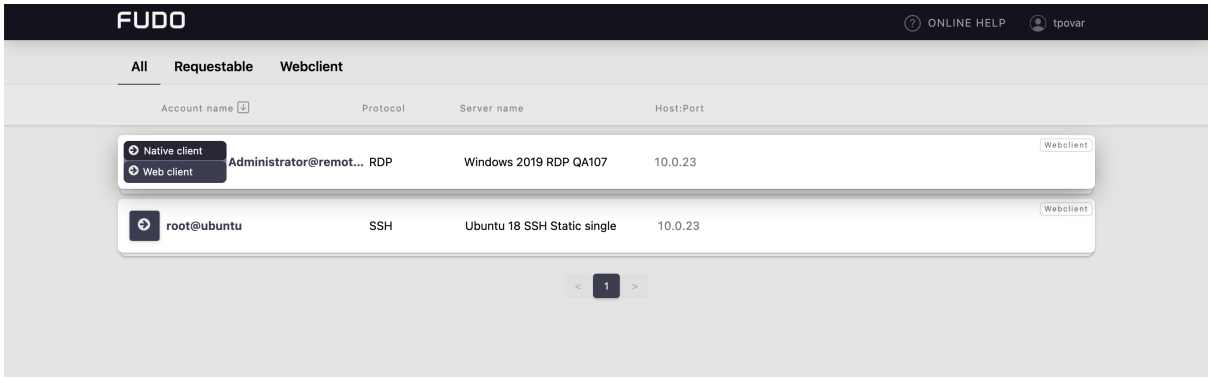
Related topics:

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

1.10.5 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*

1.10.6 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

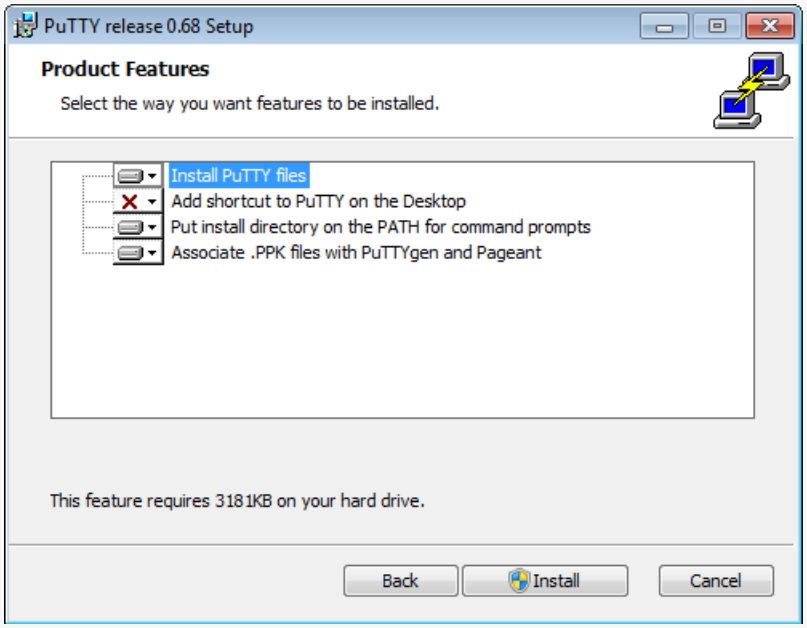
Verify the checksum value to make sure that the integrity of the binary file has not been compromised.

2. Download and install *PuTTY*.

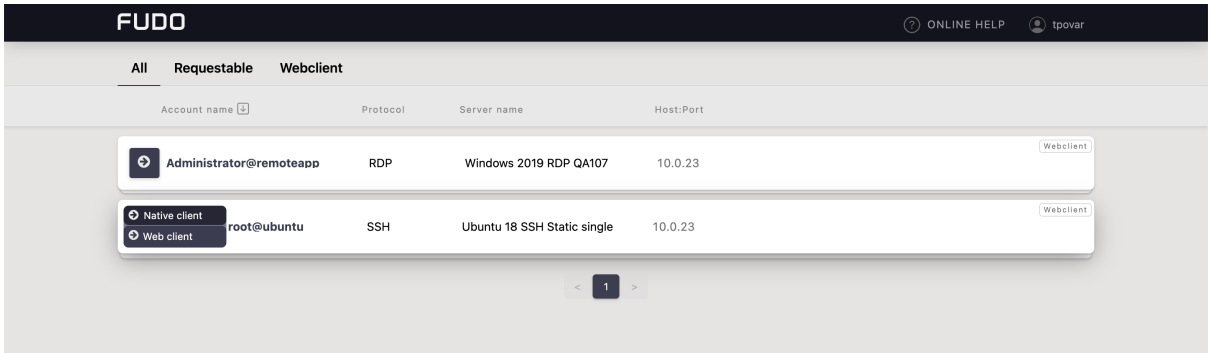
   `https://winscp.net/download/putty-0.75-installer.msi`

Note

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

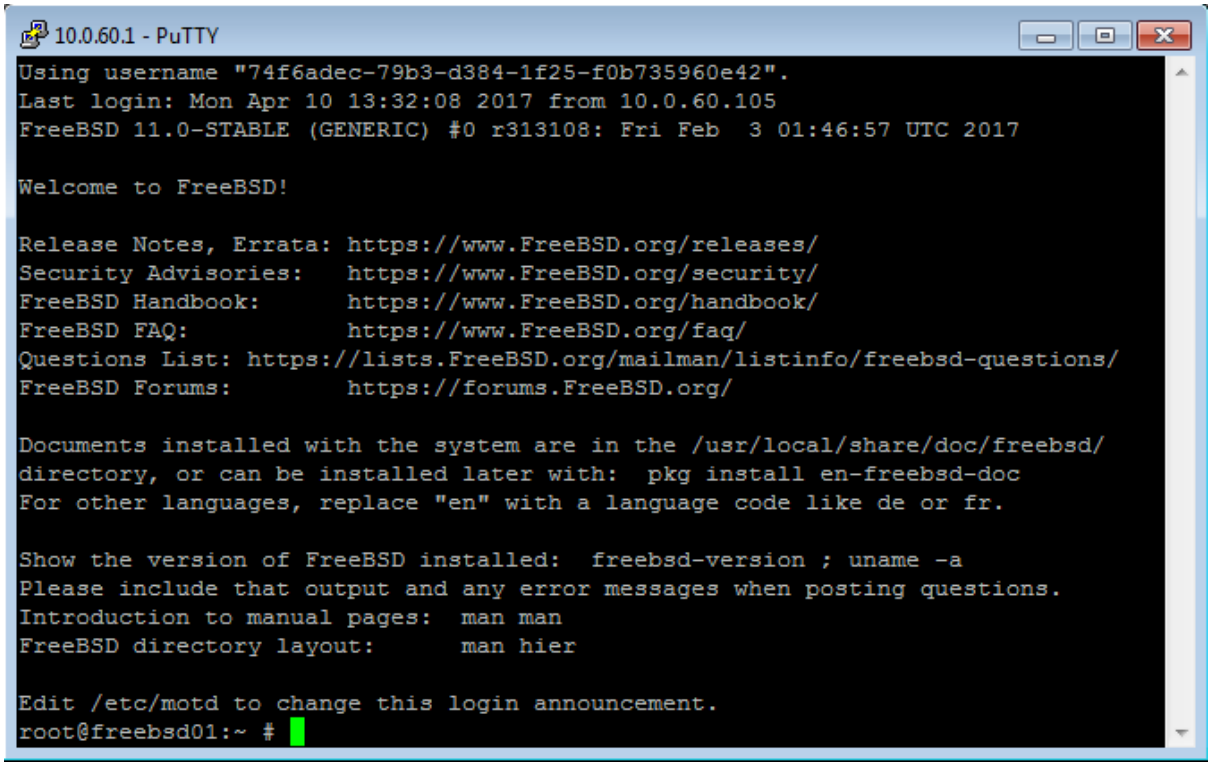


3. Log in to the User Access Gateway.
4. Find desired account and server, hover your mouse over to show more options.
5. Select the *Native client* button.



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.

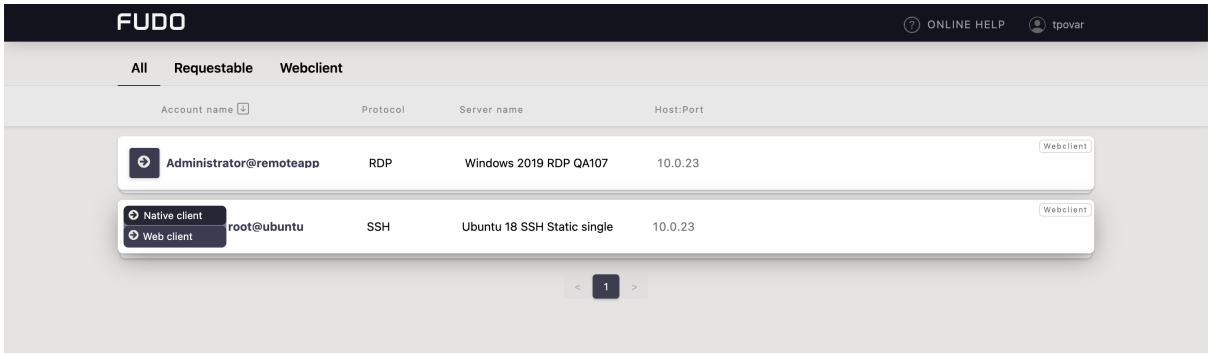


Related topics:

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

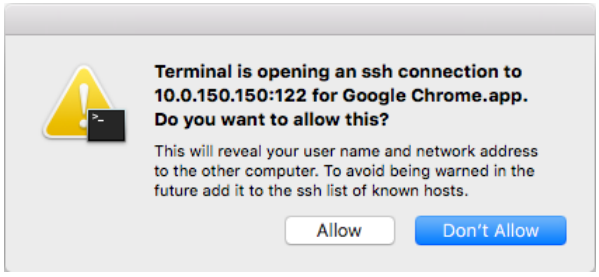
1.10.7 Connecting Over SSH on Mac OS, Linux

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:

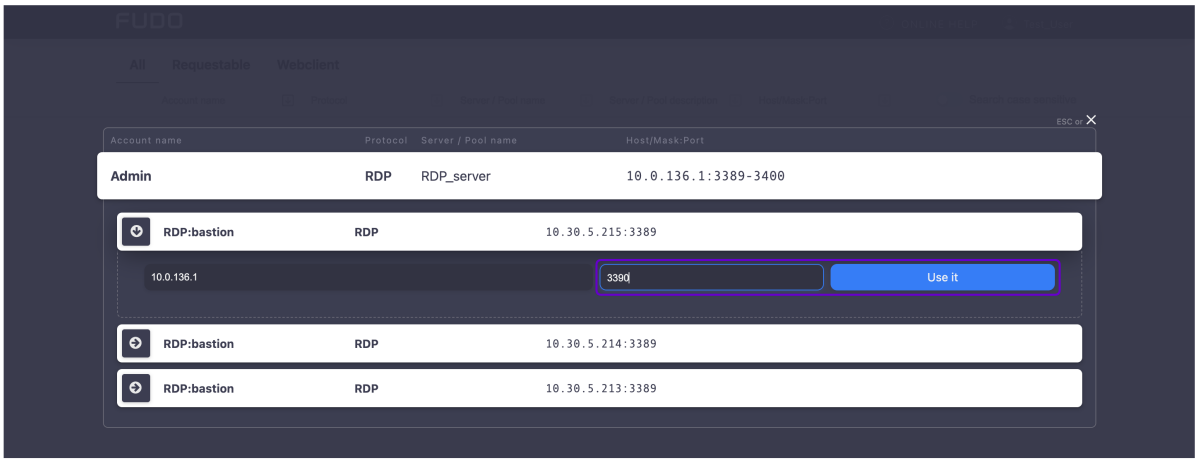
- *Connecting Over RDP on MAC OS X*
- *Connecting Over RDP on Microsoft Windows 7 and 10*
- *Connecting Over RDP on Ubuntu Linux*

1.10.8 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:

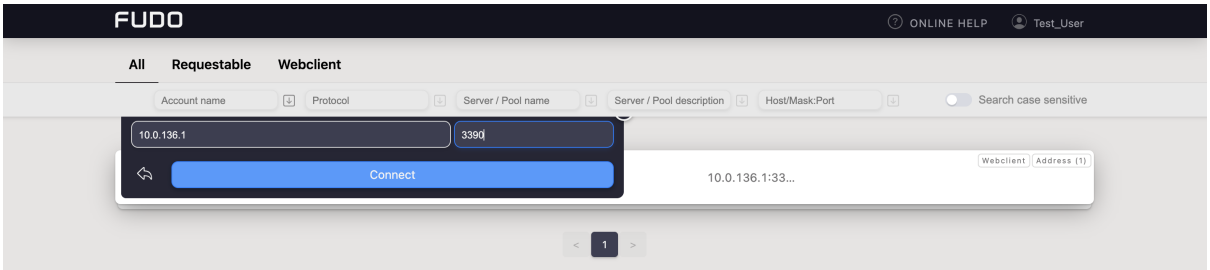
1. Select from the dropdown list the address of the server with a port range that you want to connect to (in case of a server pool).
2. In the **Port** field, enter a port selected from the range specified during the configuration of the given server.
3. Click the **Use** button.
4. Click the **Connect**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

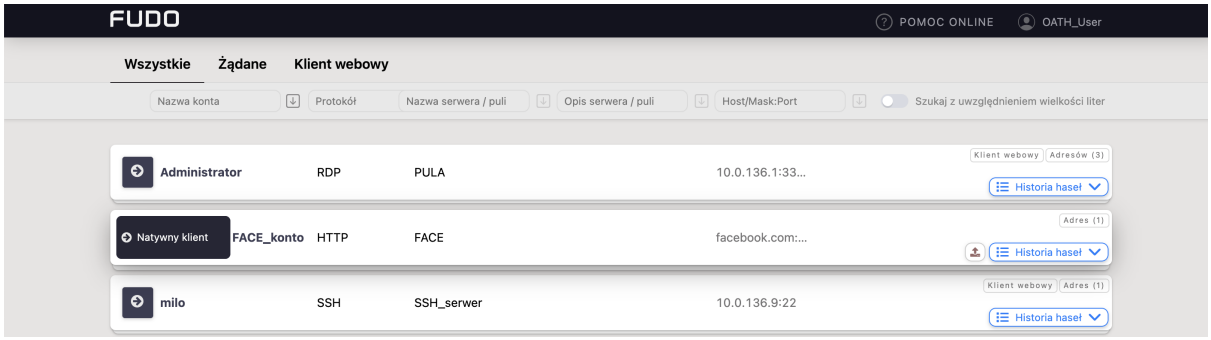


Related topics:

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

1.10.9 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.

Browser Access Modes in Rendered HTTP Sessions

Rendered HTTP sessions can be opened in one of the following browser access modes. The available mode depends on the safe settings configured by the administrator.

Single-Tab Kiosk Mode

In single-tab kiosk mode, the rendered HTTP session is displayed in a locked-down browser view. The browser interface is hidden, including the address bar and browser navigation controls.

In this mode:

- Only one browser tab is available.
- The address bar is not displayed.
- Browser navigation controls, such as back, forward, and refresh, are not displayed.
- The context menu opened with the right mouse button is disabled.
- Pop-up windows are redirected to the current page and replace its content.

Full Browser Access

In full browser access mode, the rendered HTTP session is displayed with the browser interface visible.

In this mode:

- Multiple browser tabs are available.
- The address bar is displayed.
- Browser navigation controls, such as back, forward, and refresh, are available.
- You can open and switch between browser tabs.
- There is no tab limit.
- Access to restricted browser tools, such as developer tools and browser settings, remains blocked.

Pop-up Window Behavior

In rendered HTTP sessions, the behavior of pop-up windows depends on the browser access mode and safe settings.

- In single-tab kiosk mode, pop-up windows are redirected to the current page and replace its content.
- In full browser access mode, pop-up windows can be converted to browser tabs, depending on the safe settings.
- If converting pop-up windows to browser tabs is disabled, pop-up windows may open outside the browser view and cover the session content.

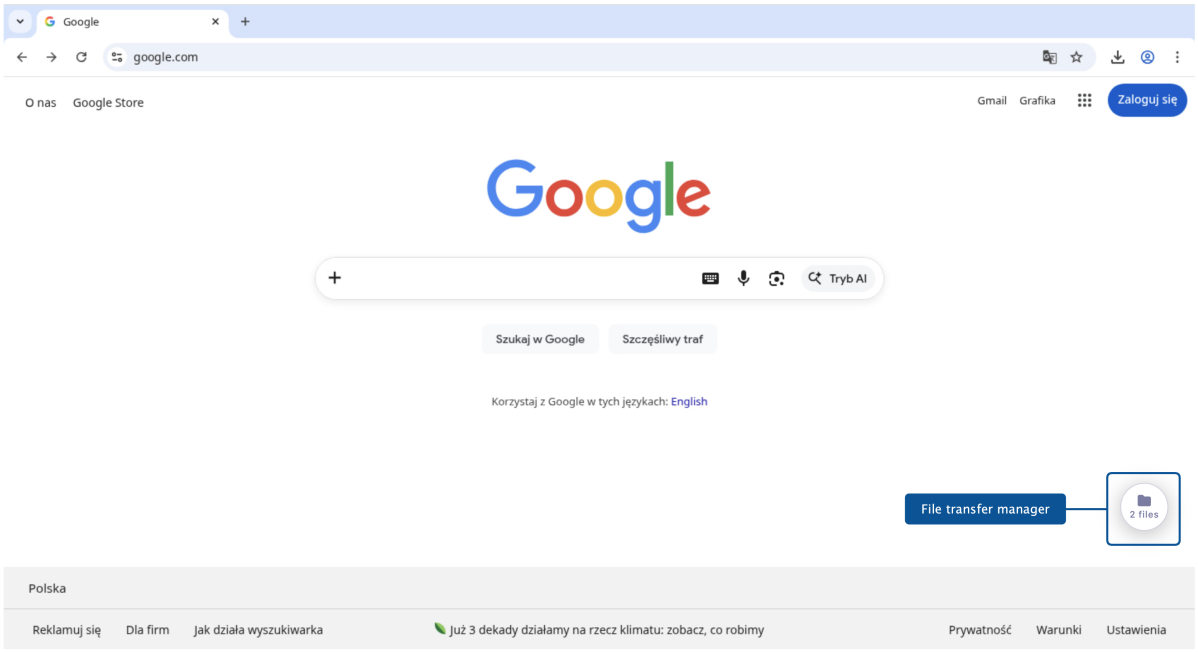
If the redirected page does not load correctly, try reloading it using the **Ctrl** + **R** keyboard shortcut.

If a pop-up window replaces the current page, you can 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

File Transfer in Rendered HTTP Sessions

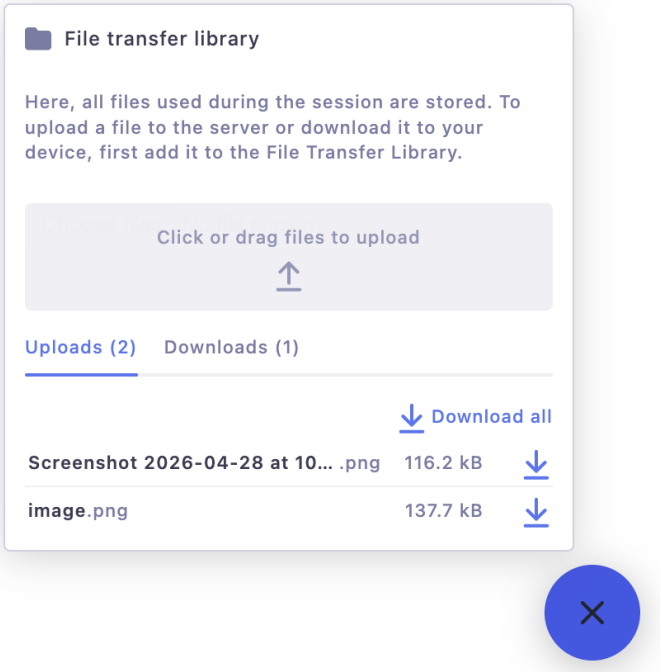
If file upload or file download is allowed for the safe, a floating file transfer manager button is displayed on the session screen.



You can move the file transfer manager button to another location on the screen. By default, it is usually displayed in the lower-right corner of the session window.

Click the file transfer manager button to open a modal window with the following tabs:

- **Uploads** - allows you to upload files from your local device to the rendered HTTP session.
- **Downloads** - displays files downloaded in the browser during the rendered HTTP session.



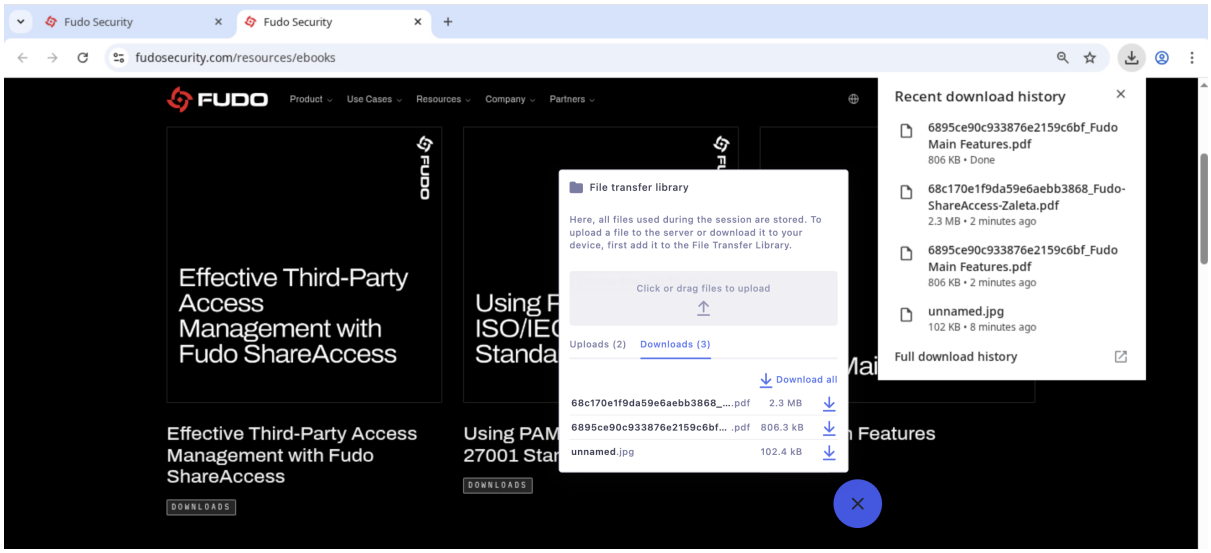
Uploading Files

To upload a file to the session, open the **Uploads** tab and do one of the following:

- Click the **Click or drag to upload** field and select a file from the file browser.
- Drag and drop the file into the **Click or drag to upload** field.

Downloading Files

Files downloaded in the browser are displayed in the **Downloads** tab.



Note

- File upload and file download permissions are controlled separately by the administrator in the safe settings. Depending on the safe configuration, only upload, only download, both actions, or neither action may be available in the rendered HTTP session.
- The total storage available for uploaded and downloaded files in a session is set by the administrator in the safe settings; the default limit is 500 MB.

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*

1.11 Webclient Features

Note

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

Available Webclient features:

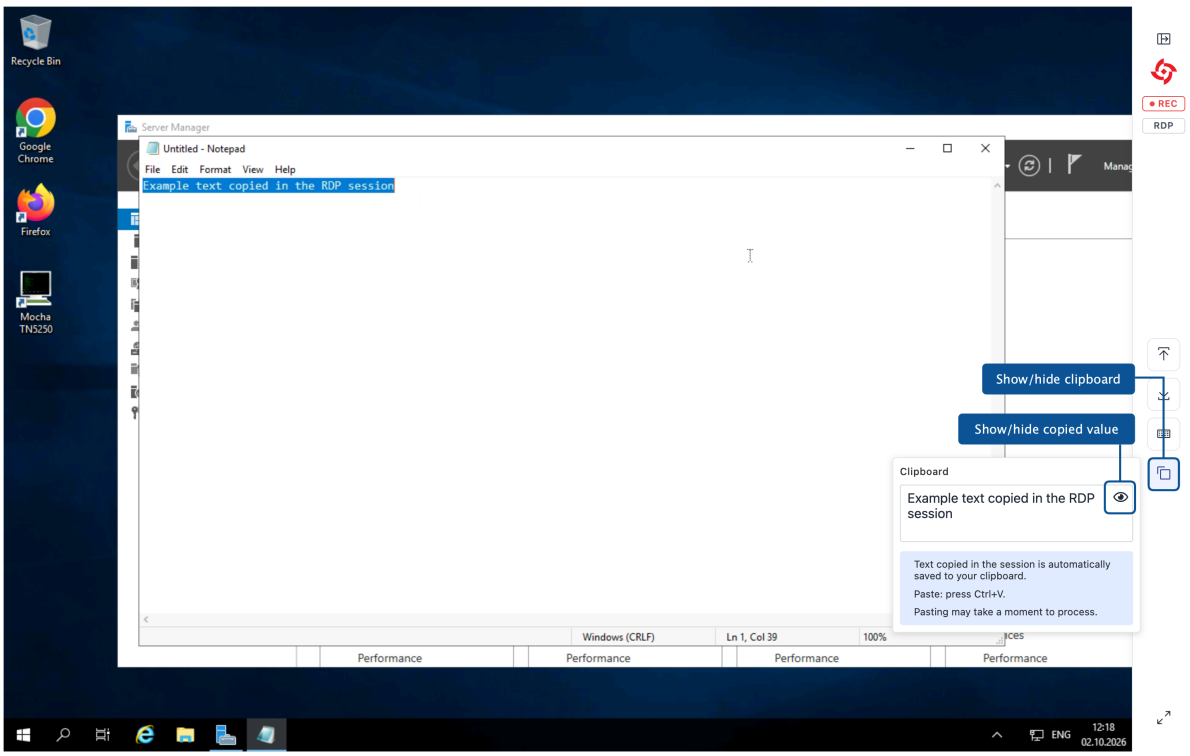
- Browser tabs showing the protocol type, server name, account used to establish the session, and connection status:

- 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 opens a panel with the most recently copied or pasted text and keyboard shortcuts for SSH and RDP sessions.
- 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.



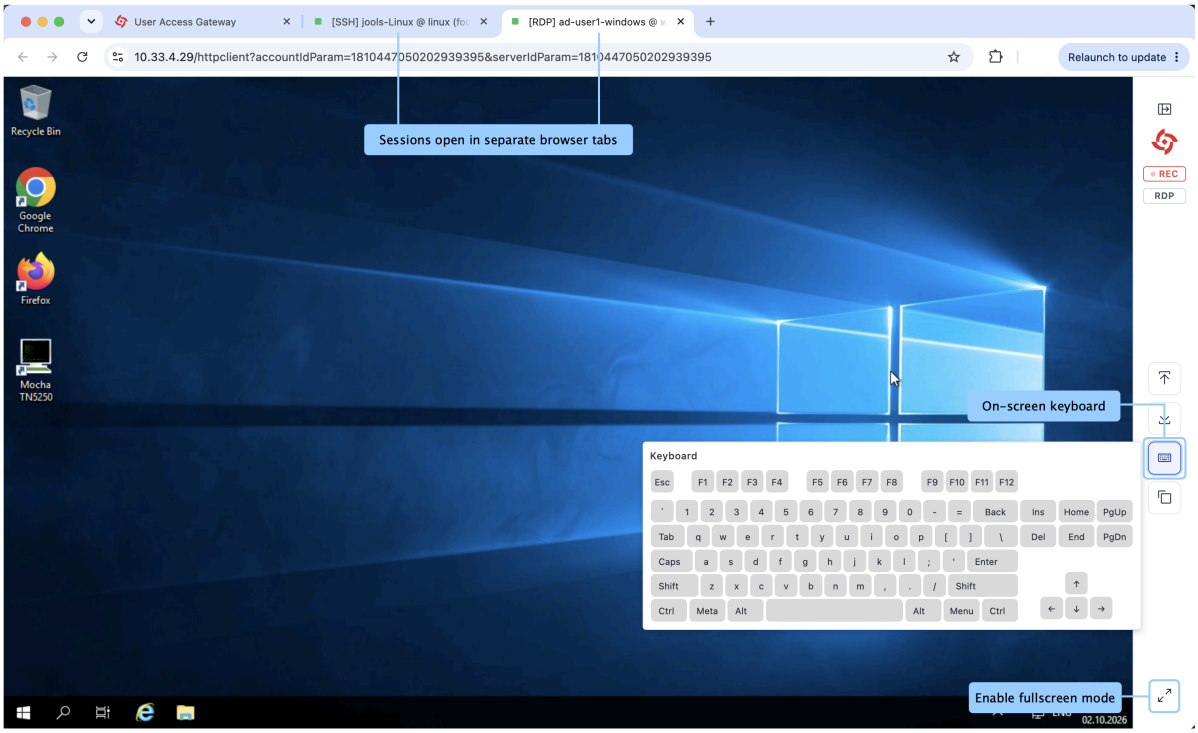
Note

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.

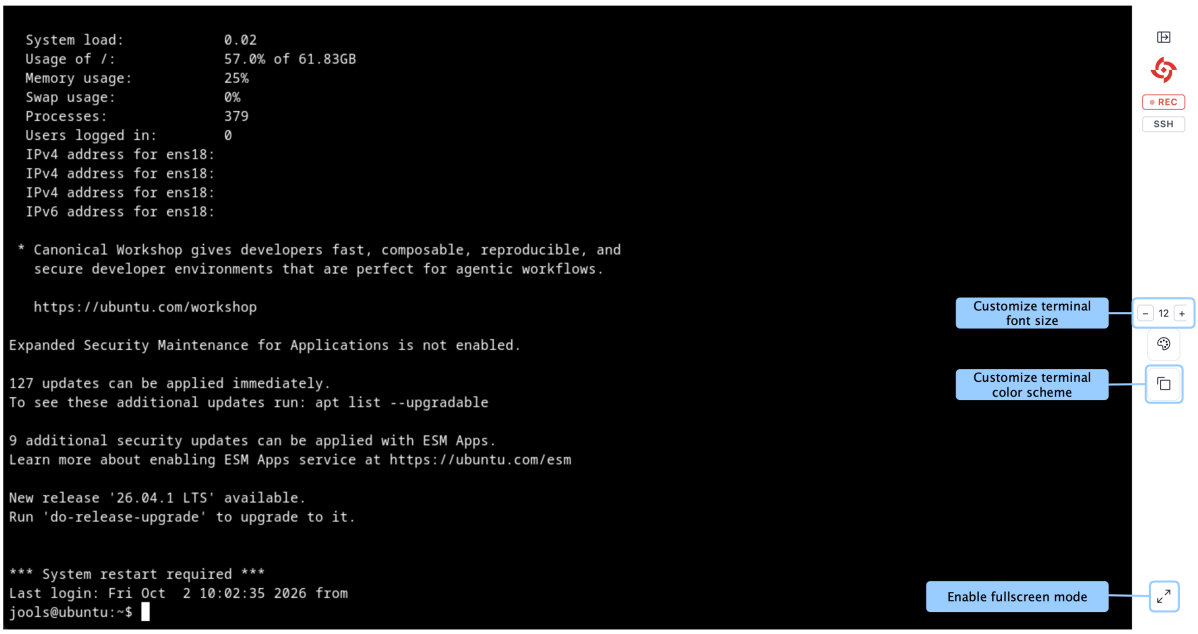
Note

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.



Copying and Pasting Text

Starting from version 6.3, SSH and RDP Webclient sessions exchange text directly with your computer's clipboard, without using the clipboard panel.

- **SSH:** select text and use `Ctrl+Shift+C` to copy it, or `Ctrl+Shift+V` to paste text. You can also use *Copy* and *Paste* from the right-click menu. `Ctrl+C` interrupts the running command.
- **RDP:** use `Ctrl+C` to copy text and `Ctrl+V` to paste it.

Note

The shortcuts use `Ctrl` on macOS as well; `Cmd+C` and `Cmd+V` are not supported.

Only text copied after the session has been opened is transferred. Pasting into an RDP session requires **Clipboard Redirection** to be enabled for the safe.

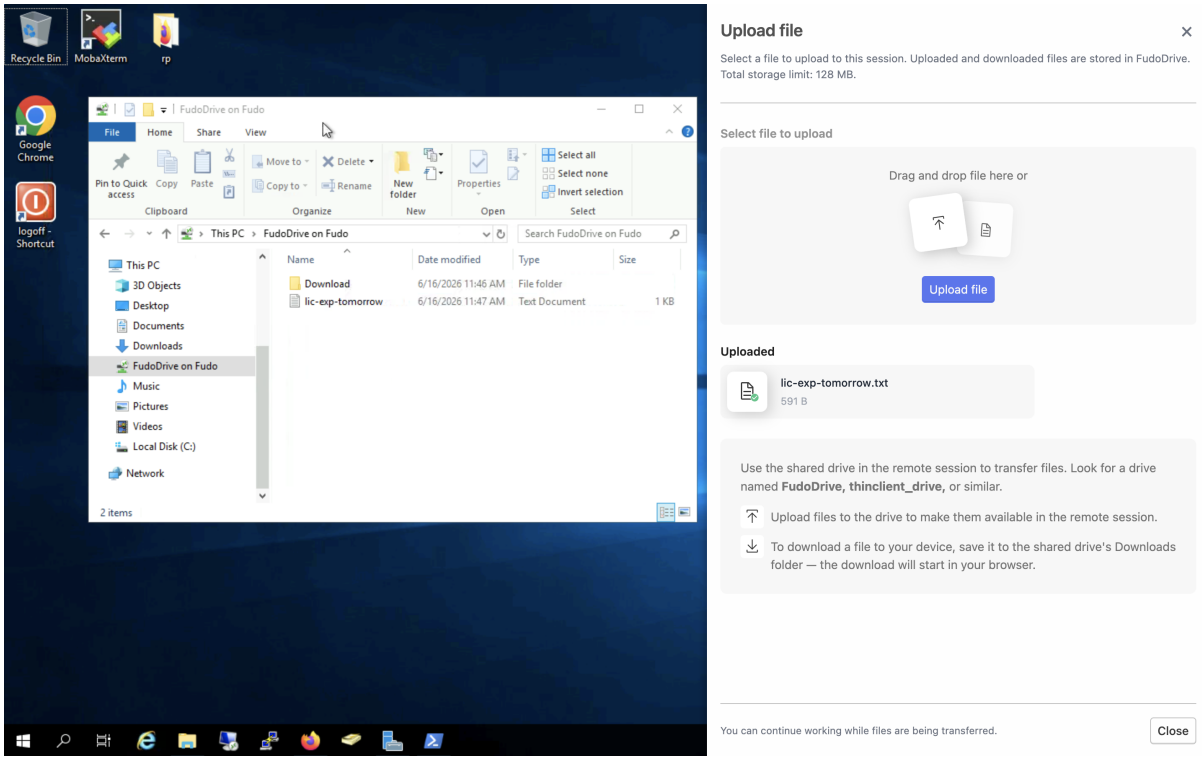
When pasting, allow the browser to read your clipboard. In Chrome, accept the permission request; in Firefox, click the *Paste* button displayed by the browser. If access is blocked, allow it in the site settings and reload the session.

File Transfer in RDP Sessions

RDP Web Client sessions support uploading and downloading files. Files are stored on a per-session shared drive with a total storage limit (uploads and downloads combined) set by the administrator in the safe settings; the default limit is **128 MB**. The file transfer panel shows the limit that applies to the session. Only individual files can be transferred (uploading folders is not supported).

Note

The administrator enables file upload and file download separately for each safe. The upload icon is displayed in the sidebar only when file upload is enabled, and the download icon only when file download is enabled. Neither icon is displayed when **Device redirection** is disabled for the safe.



To upload a file:

1. In the session sidebar, click the upload icon to open the file transfer panel.
2. Click *Upload file*, select a file from your device, and click *Open*. Alternatively, drag and drop the file into the file transfer panel.

Note

The file is placed on the **shared session drive** and becomes available in the remote session:

- In Windows environments, the drive is available as **FudoDrive** and is shown in File Explorer under **Redirected drives and folders**.
- In Ubuntu environments, it is shown as **thinclient_drive**.

To download a file:

1. In the remote session, save the file to the *Downloads* folder on the shared drive.
2. The download starts automatically in your browser.

Important

You can continue working in the session while files are being transferred. When the **session ends**, the shared drive and all its **files are permanently deleted** and the file transfer **history is cleared**, so reconnecting starts with an empty drive.

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*

1.12 Sharing Your Session

You can give another person access to a session you are running, without asking an administrator for help. This is useful when you need a second pair of eyes on what you are doing, or when a colleague has to take over part of the work.

Note

The option is available only when your administrator has enabled session sharing for the safe the session belongs to. If you do not see the *Share session* icon, contact your administrator.

A link you create always:

- requires the recipient to **sign in** to Fudo Enterprise before they can see the session,
- allows the recipient to **interact** with the session, not only watch it,
- stops working when your session ends.

Important

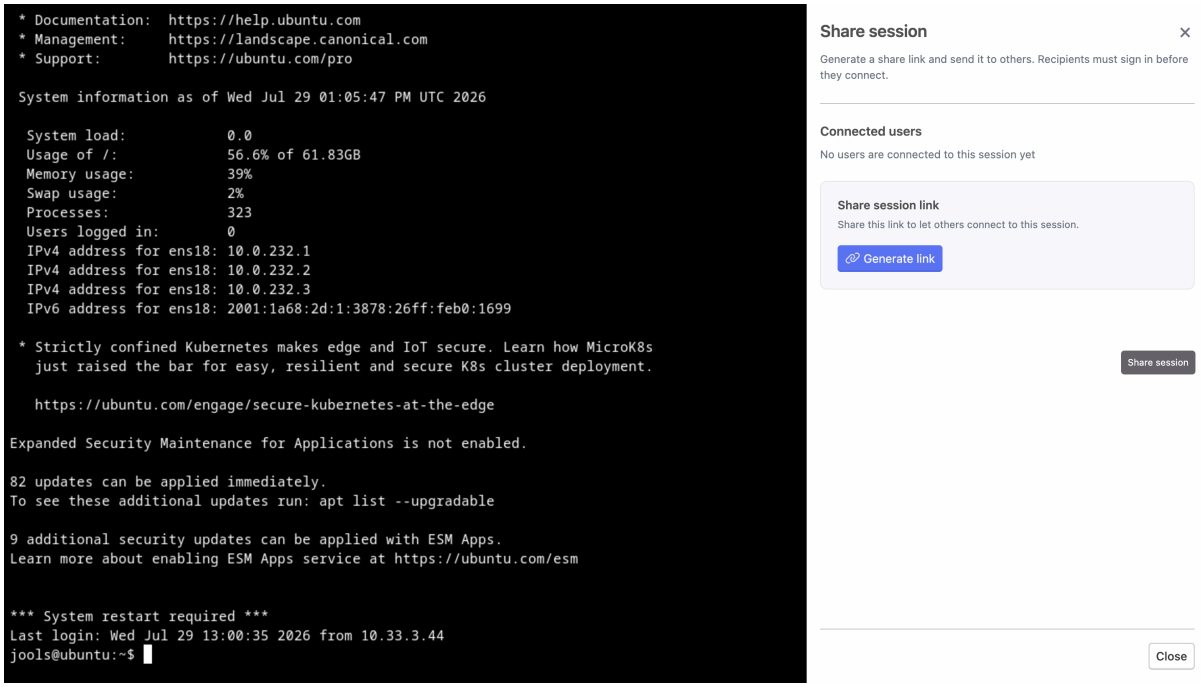
Anyone who signs in to Fudo Enterprise and has your link can join the session. Send the link only to people who should see what happens in it.

Sharing a Running Session

To share a session you are currently running, proceed as follows.

1. In the Web Client session, click *Share session* in the side toolbar.

2. Click *Generate link*.



3. Copy the link and send it to the person who should join the session.

The *Connected users* list in the same panel shows who is currently connected to your session. As long as nobody has joined, it displays *No users are connected to this session yet.*

Ending the Sharing

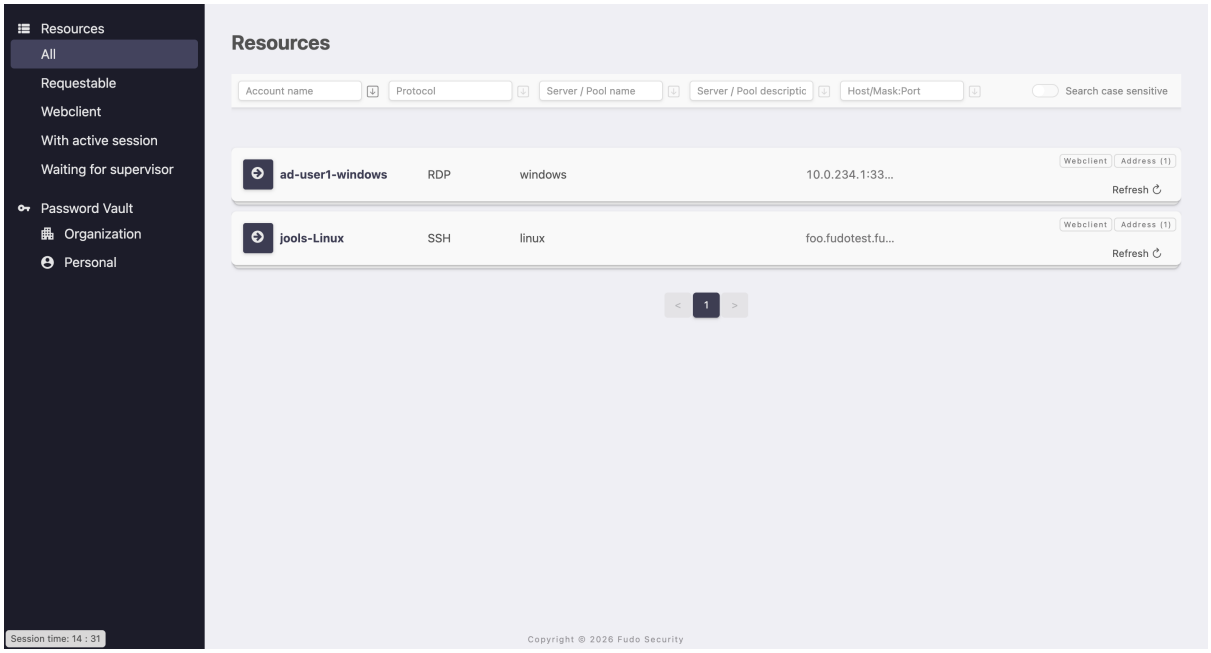
To stop sharing the session, click *Deactivate* in the *Share session* panel. The link stops working immediately and anyone connected through it is disconnected.

Your link also stops working on its own as soon as the session ends, so you do not have to deactivate it before you disconnect.

Finding Your Shared Sessions

The *Resources* list provides two filters that help you find sessions related to sharing:

- **With active session** - resources on which you currently have a running session,
- **Waiting for supervisor** - sessions that cannot start until the required number of supervisors is watching them.



Related topics:

- *Webclient Features*
- *Connecting Over RDP, VNC and SSH in Browser*

1.13 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. If the safe is configured for time-based Just-in-Time access, send an access request for the account instead of connecting directly.

Problem	Symptoms and solution description
A section is greyed out and cannot be opened.	**Symptoms:** • The *Resources* or *Password Vault* section is greyed out and does not react to clicks. • Pointing at the section displays the message *This module is disabled for your account. Contact your administrator.* • Entering the address of the section directly in the browser does not open it either.
	Reason: the corresponding module - PSM or Password Vault - has been disabled for your account by the administrator.
	Solution: contact your system administrator to have access to the module restored.