BeyondTrust

Password Safe Cloud 23.1
User Guide

TC:6/1/2023

Table of Contents

Password Safe Cloud User Guide

Password Safe Cloud includes a web-based interface for executing password and remote session requests and approvals. You can launch the Password Safe web portal by selecting **Password Safe** from the left navigation menu in the BeyondInsight management console. The web portal is configured by your Password Safe administrator.

Password Safe Cloud's random password generator algorithm does not use any common phrases or dictionary words as inputs or in its generation. It selects each password character randomly from the list of allowable characters, numerals, and symbols to build the password.

A Password Safe user is authorized to log in to the Password Safe portal and perform specific tasks, as determined by the privileges assigned to that user.

Select a Display Language

The Password Safe web portal can be displayed in the following languages:

- Dutch
- English
- French
- Japanese
- Korean
- Portuguese
- Spanish

If your BeyondInsight administrator has the option enabled, you can select a language from the list on the **Log In** page or by clicking the **Profile and preferences** button, and then selecting it from the **Language** list.

Note: *If no languages are available, please contact your BeyondInsight administrator.*

Log In to the Web Portal

Your Password Safe administrator configures login credentials for the web portal. Contact your administrator if you are unsure which credentials to use. Potential authentication methods include:

- **Password Safe:** Enter your Password Safe credentials and then click **Login**.
- **Active Directory:** Enter your Active Directory credentials, select a domain from the list, and then click **Login**.
- **LDAP:** Enter your LDAP credentials, select an LDAP server from the list, and then click **Login**.
- **RADIUS:** Enter your Password Safe credentials and then click **Login**. Enter RADIUS code and then click **Submit**.
- **Smart Card:** Select a certificate and then enter the smart card PIN.
- **SAML:** Follow the procedure for your third-party authentication type.

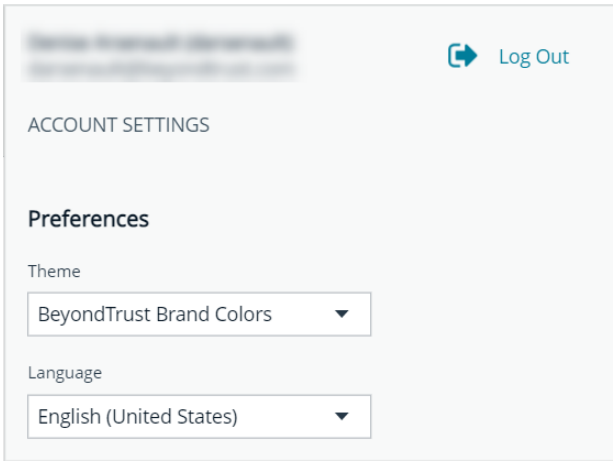
Note: *If presented with a pre-login banner, you must click **OK** before you can enter your credentials.*

Change and Reset Login Passwords

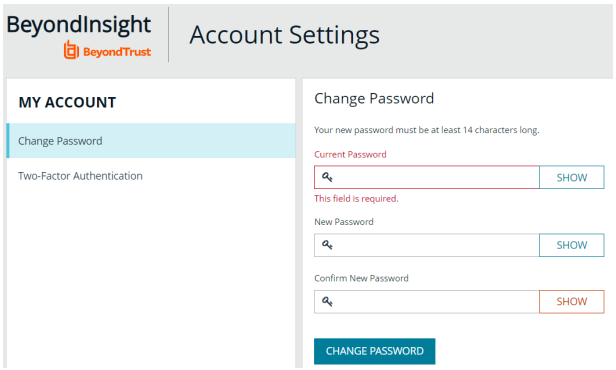
Change Password and Two-Factor Authentication Settings

If you are logging in with a BeyondInsight local user account, you can change your password and two-factor authentication app from the **Account Settings** page. You cannot change your password if you are logging in with Active Directory or LDAP credentials, or if your account is locked out.

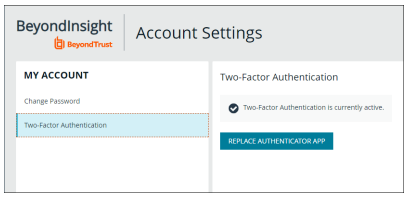
1. In the console, click the **Profile and preferences** icon in the top-right corner.
2. Click **Account Settings**.



3. Update your password, and then click **Change Password**.



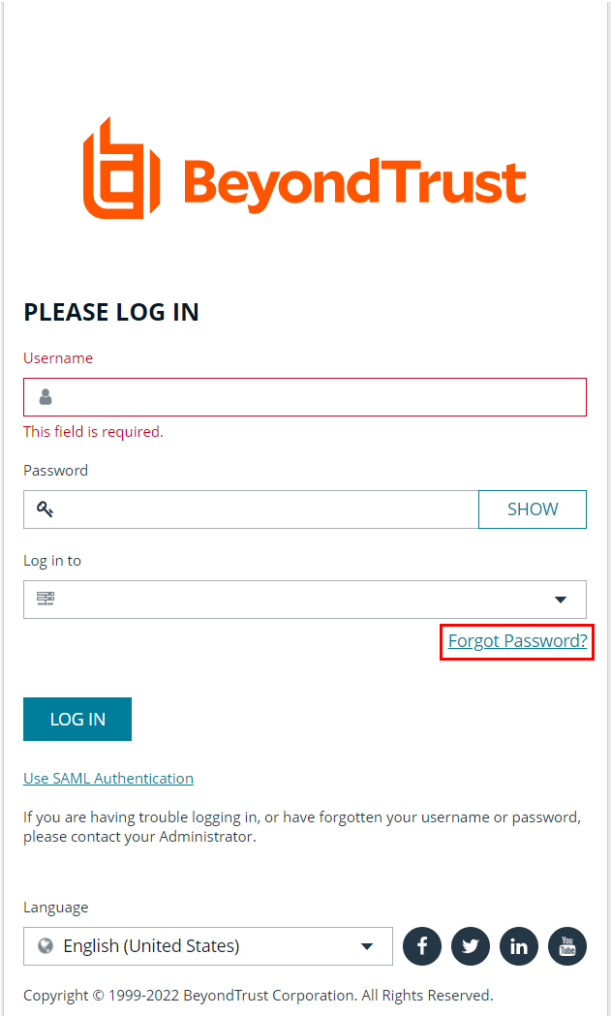
4. If your account has two-factor authentication enabled and registered with a device, you can update the authenticator app as follows:
   - Select **Two-Factor Authentication** from the **My Account** pane.
   - Click **Replace Authenticator App**.
   - Click **Reconfigure Authenticator App** to register a new authenticator app.



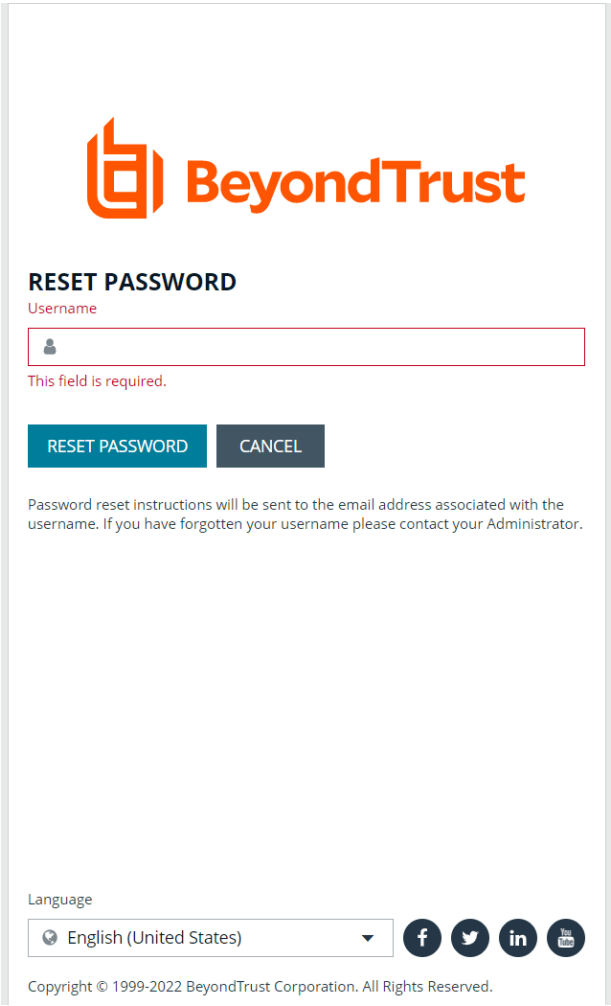
Reset Password

If you forget your console password, you can reset it as follows:

1. Click the **Forgot Password** link.



2. Enter your username, and then click **Reset Password**. An email containing a reset link is sent to the address associated with your username.



3. Click the link in the email to be taken to the **Enter New Password** page, where you can change your password.

Note: *Resetting the console password is not available to users logging in with Active Directory or LDAP credentials.*

Navigate the Password Safe Web Portal

Depending upon the permissions assigned to your user account, the Password Safe portal displays the following tabs:

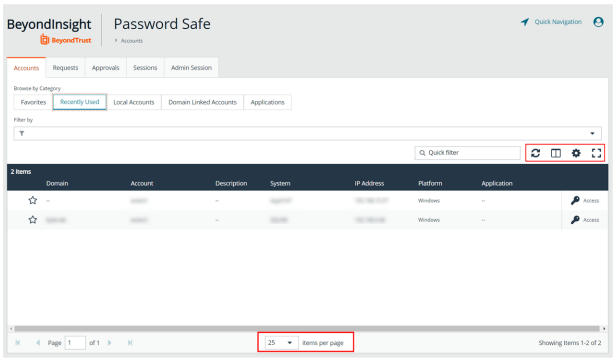
- Accounts
- Requests
- Approvals
- Sessions
- Admin Sessions

An overview of each tab is described in the below sections.

Set Grid Display Preferences

You can set display preferences on Password Safe grids, using the following options represented by icons above the grid:

- **Columns Chooser:** Select the columns to change the column headings and information displayed in the grid.
- **Grid Configuration:** Choose the grid layout: **Compact**, **Default**, or **Expanded**.
- **Expand Grid:** Enlarge the display area. When selected, the icon changes to **Collapse Grid**. Click it to collapse the grid back to its original display.

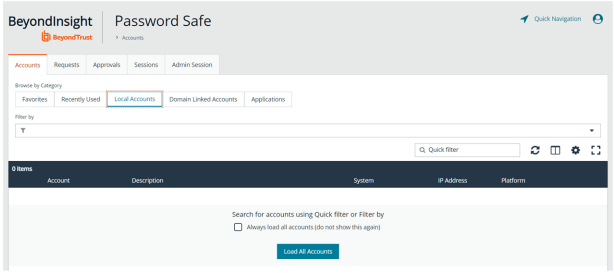


An option to change the number of displayed **Items per page** is located below the grid. The changes appear dynamically as they are selected.

View Managed Accounts

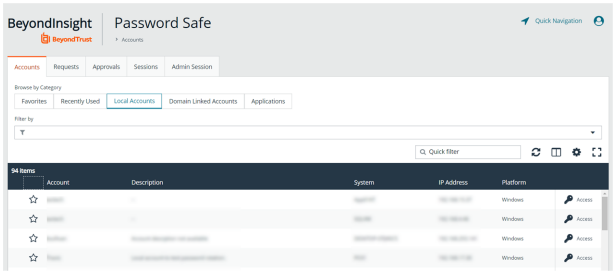
The **Accounts** tab lists the managed accounts for which you have permissions to request access to retrieve passwords and start sessions. From this grid, you can initiate an access request for the listed accounts. From the **Accounts** tab, populate the list of managed accounts in the grid using any one of the following options:

- Click the **Browse by Category** buttons: **Favorites**, **Recently Used**, **Local Accounts**, **Domain Linked Accounts**, and **Applications**, to filter the list by category.
- Select filter criteria from the **Filter by** dropdown to filter by selected account properties.
- Search for accounts using the **Quick Filter** option.
- Click **Load All Accounts** to load all accounts in the organization.



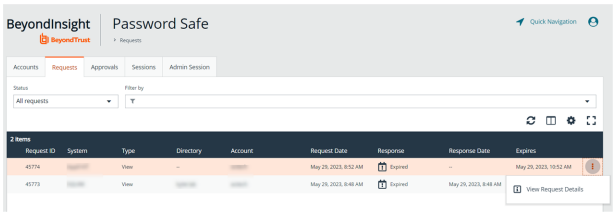
Tip: For optimum efficiency, the web portal screen resolution should be no less than 1280 × 800 pixels.

*Note: When you first log in to the Password Safe web portal, no accounts are available in the **Favorites** tab. Click the star for the account to add it to the **Favorites** tab. Click **Refresh** above the grid to update the listed accounts.*



View Requests

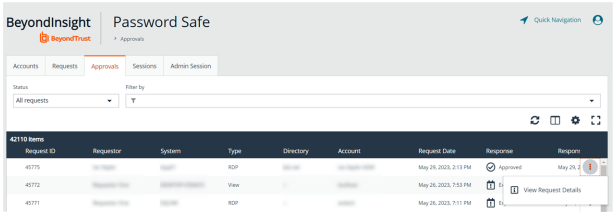
The **Requests** tab displays for users who have been assigned the **Requestors** role for any managed systems in Password Safe. It lists all requests that you have made. You can filter by approved and pending requests and view the request details by clicking the vertical ellipsis for the request, and selecting **View Request Details**.



View Approvals

The **Approvals** tab displays for users who have been assigned the **Approver** role for any managed systems in Password Safe and for Password Safe administrators. Approvers can view all requests for managed systems for which they have been assigned the **Approver** role. Password Safe administrators can view all requests for all managed systems. You can filter the requests by approved and pending requests, view request details, and approve or deny requests.

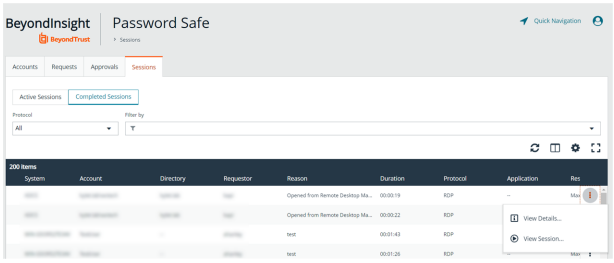
To view details of the request, click the vertical ellipsis for the request, and then click **View Request Details**.



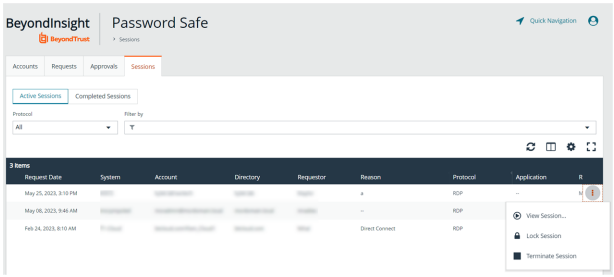
View Sessions

The **Sessions** tab displays for users who have been assigned one or both of the two session reviewer roles for any managed systems: **Recorded session reviewer** and **Active session reviewer**. Depending on the roles assigned to your user account, you can view active or completed sessions using the buttons above the grid. By default sessions for all protocols are displayed. You can filter the list of sessions to display only RDP or only SSH sessions using the **Protocol** dropdown.

To view details of a completed session or to view the session, click the vertical ellipsis for the session, and then select **View Details** or **View Session** as required.



To view, lock, or terminate an active session, click the vertical ellipsis for the session, and then click **View Session**, **Lock Session**, or **Terminate Session** as required.



> ***Note:*** *Admin sessions are listed in the grid only for users who have read permissions to the* ***Password SafeAdmin Session Reviewer*** *feature, as assigned by your Password Safe administrator.*

Admin Session Tab

The **Admin Sessions** tab displays only for users who have full control permissions to the **Password SafeAdmin Session** feature and for Password Safe administrators. Admin sessions allow you to open ad hoc RDP and SSH sessions without going through the request process and allow you to select a node associated with another region to act as a proxy for the session. This is useful in larger environments when assets you need to access are not in your region. From **Admin Session** tab, you can start a session immediately by completing the form and clicking **Connect**.

> *For more information on submitting requests and starting sessions, please see the following:*
>
> - *"Request a Password from Password Safe" on page 10*
> - *"Request and Start Sessions in Password Safe" on page 14*
> - *"Approve or Deny Requests for Passwords and Sessions" on page 20*

Request a Password from Password Safe

Using a configuration that requires requests are approved by a designated approver, provides accountability and ensures the security of the system's account passwords by providing dual control over the managed accounts. A dual control configuration, requires the three following steps:

1. **Password request:** An authorized requester requests a password release.
2. **Password approval:** An authorized approver reviews and approves the request for release.
3. **Password retrieval:** The authorized requester retrieves the approved password.

To use a dual control setup, Password Safe users must be assigned the **Requestor** or **Approver** role, or both.

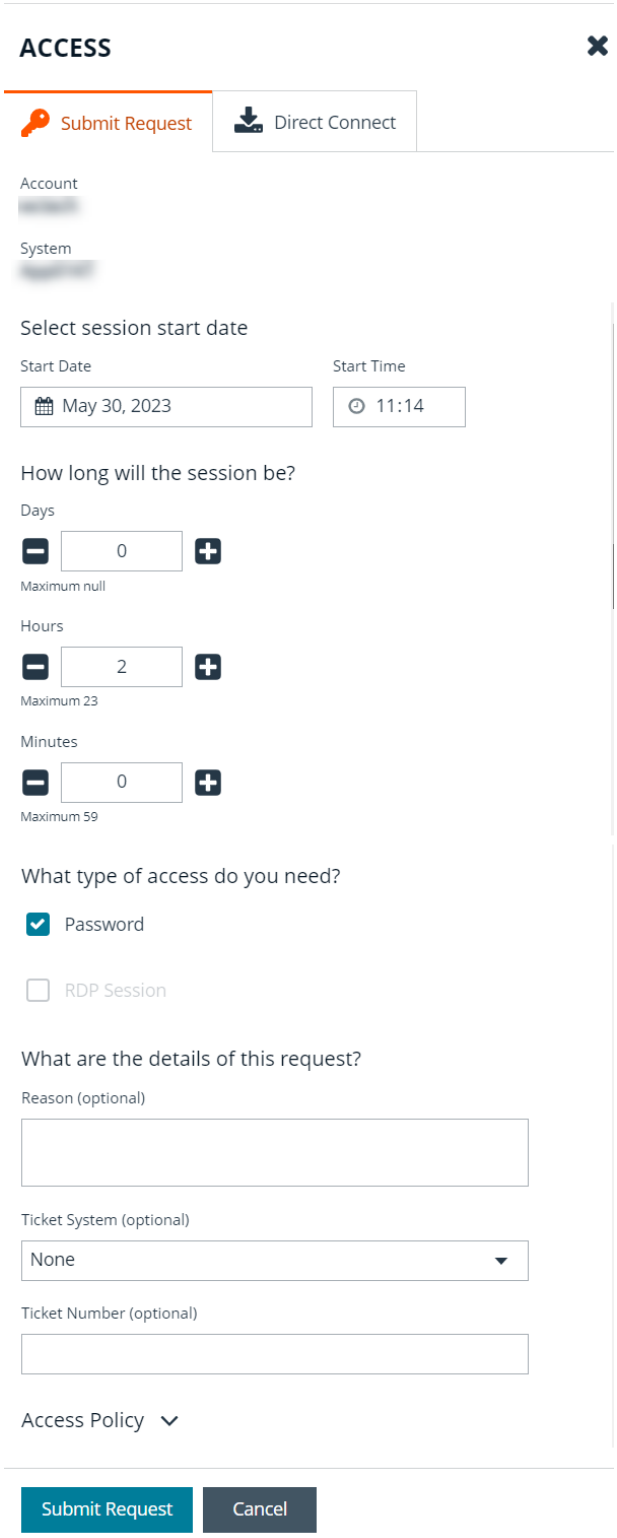
Request a Password Release

1. From the **Accounts** tab, load the accounts in the grid by clicking a category or using the filter options, and then click **Load All Accounts**.
2. Click **Access** for the managed account for which you wish to request a password.

3. From the **Submit Request** tab:
    - Set a start date and time for the password to be made available.
    - Set the length of time for the password to be available.
    - Check **Password** for the type of access you need.
    - Provide a reason for the request. The maximum allowed length is 200 characters.
    - Select a ticket system and provide a ticket number.

> ***Note: Reason**, **Ticket System**, and **Ticket Number** fields might be optional or required, depending upon options configured in the access policy by your Password Safe administrator. Also, if your Password Safe administrator has set a specific ticket system in the access policy, you cannot select a different ticket system with your request.*

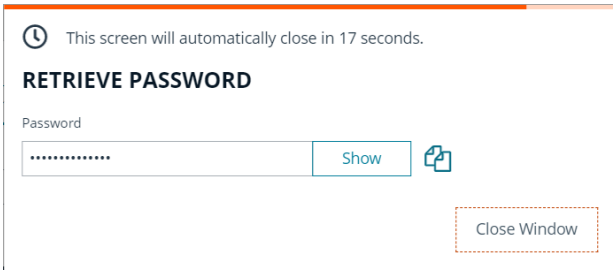
4. Click **Submit Request**. An email is sent to the approver if email notification is configured. You can view the status of your request from the **Requests** tab.



Retrieve a Password

Passwords approved for release can be displayed at any time (and as often as needed) during the release duration. After the password is approved, an email notification is sent to the requestor's email account. The requestor can then retrieve the password.

1. Click the link to see a window with the date and time the release was approved and any comments made by the approver.
2. Click **Retrieve Password** to display the system account password.
3. The password displays in a separate window. The visibility of the password might be limited, with a timer showing remaining time. Click **Close Window** to close the windows before the timeout.
4. To copy the password to the clipboard, click the **Copy** button.
5. Use the password to log in to the system within the password release time period.

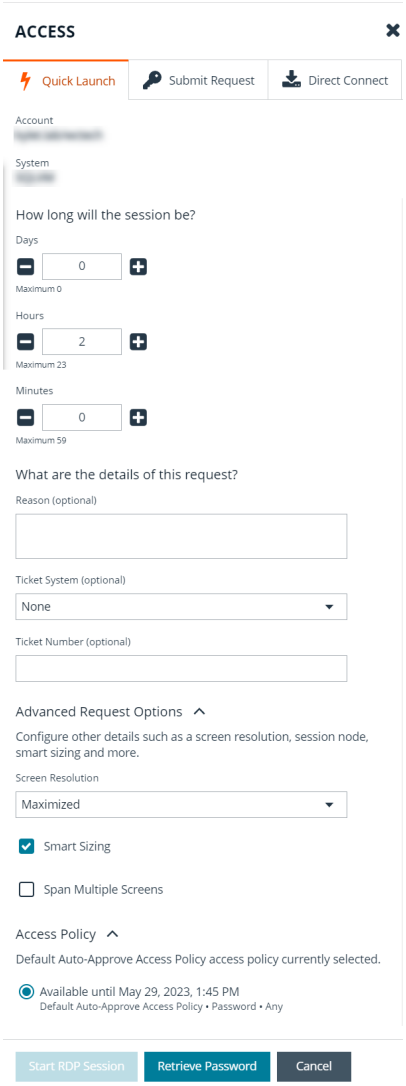


Retrieve a Password Using Quick Launch

If your access policy is configured for auto-approval for the managed system account you are accessing, **Quick Launch** is available, allowing you to quickly retrieve the password for the managed account, bypassing the approval process. To use Quick Launch:

1. From the **Accounts** tab, click **Access** for the managed account you wish to access.

2. From the **Quick Launch** tab, click **Retrieve Password**.
3. Click **Show** to display the password or click the **Copy** icon to copy it.



Request and Start Sessions in Password Safe

When configured by your Password Safe administrator, you can request access to a managed system using a remote session. Using the Password Safe request and approval system, you can request remote sessions that use RDP and SSH connection types.

Password Safe acts as a proxy, providing session management to target systems. No passwords are transmitted, allowing inherently secure session management. The below sections detail how to request and start sessions in Password Safe.

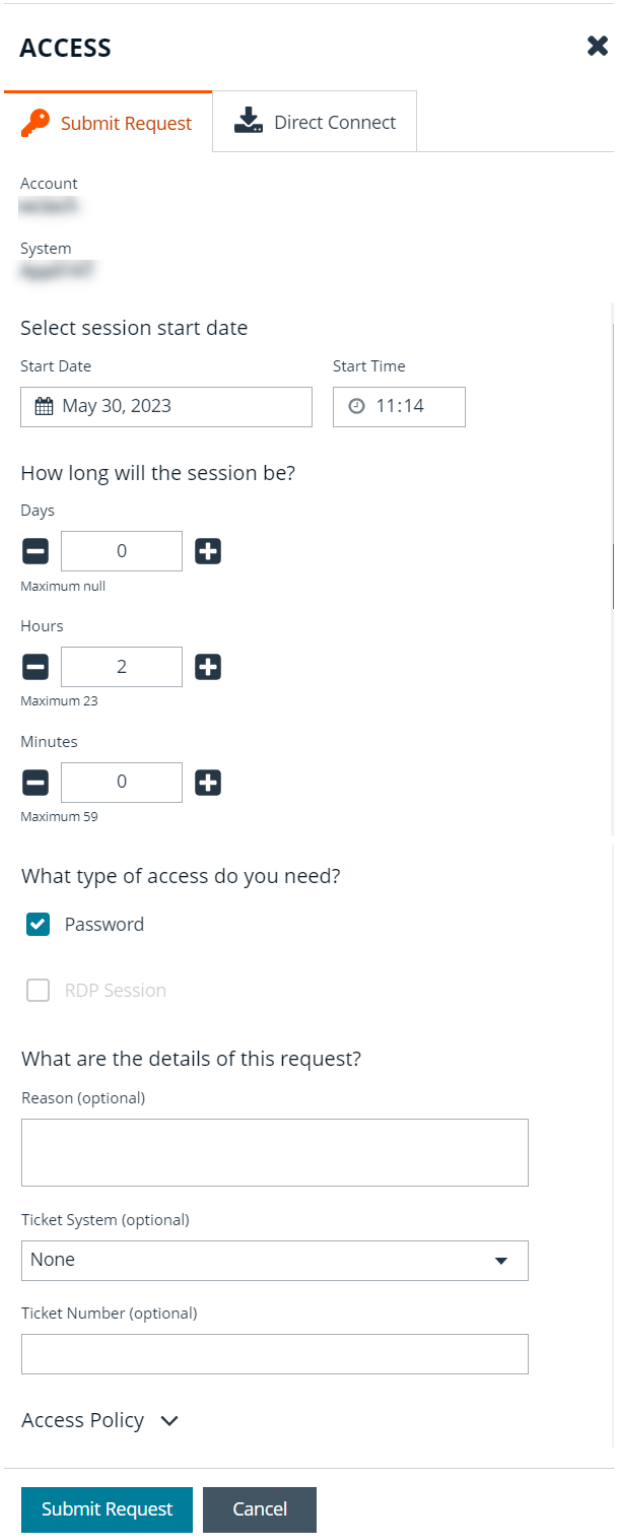
Request an RDP Session

1. From the **Accounts** tab, load the accounts in the grid by clicking a category or using the filter options, and then click **Load All Accounts**.

1. Click **Access** for the managed account for which you wish to request a session.
2. From the **Submit Request** tab:
    - Set a session start date and time that corresponds with the access policy and is outside of a scheduled maintenance window.
    - Set the length of time for the session.
    - Check **RDP Session** for the type of access you need.
    - Provide a reason for the request. The maximum allowed length is 200 characters.
    - Select a ticket system and provide a ticket number.

> ***Note: Reason**, **Ticket System**, and **Ticket Number** fields may be optional or required, depending upon options configured in the access policy by your Password Safe administrator. Also, if your Password Safe administrator has set a specific ticket system in the access policy, you cannot select a different ticket system with your request.*

3. Click **Submit Request**. An email is sent to the approver if email notification is configured.



Use Direct Connect for RDP Session

You can also use the **Direct Connect** feature to initiate an RDP session. As the requester, you can access the system without ever viewing the managed account's credentials.

To use Direct Connect, you must download the RDP file from the Password Safe web portal. This is a one-time download. Each account and system combination requires that you download the unique RDP file associated with it.

If the requestor is granted approval for RDP sessions, a message displays, stating, *Request requires approval. If the request is not approved within 5 minutes, this connection will close.* After five minutes, the RDP client disconnects, and you can send another connection request. When the request is approved, you are automatically connected.

To initiate a Direct Connect RDP session:

1. From the **Accounts** tab, load the accounts in the grid by clicking a category or using the filter options, and then click **Load All Accounts**.
2. Find the account in the list.Click **Access** for the managed account for which you wish to request a session.
3. From the **Direct Connect** tab, click **Download RDP File**.
4. Run the file to establish a connection to the target system.
5. Enter your password that you use to authenticate into Password Safe.

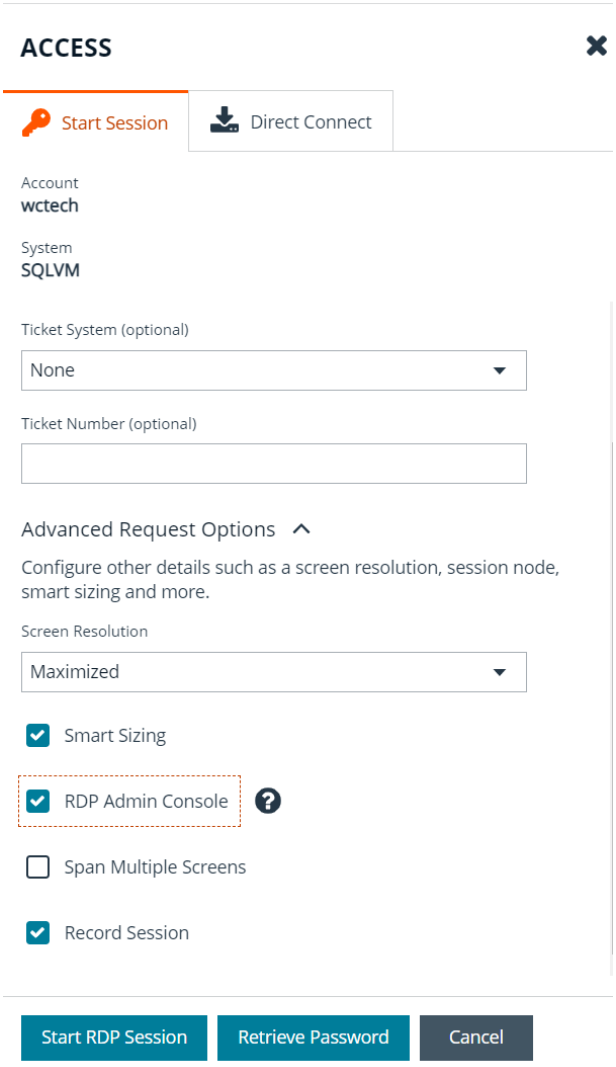
Note: *RDP Direct Connect supports only push two-factor authentication. An access-challenge response is not supported.*

Note: *LDAP users that use the mail account naming attribute cannot use RDP Direct Connect.*

Start an RDP Session Without Submitting a Request

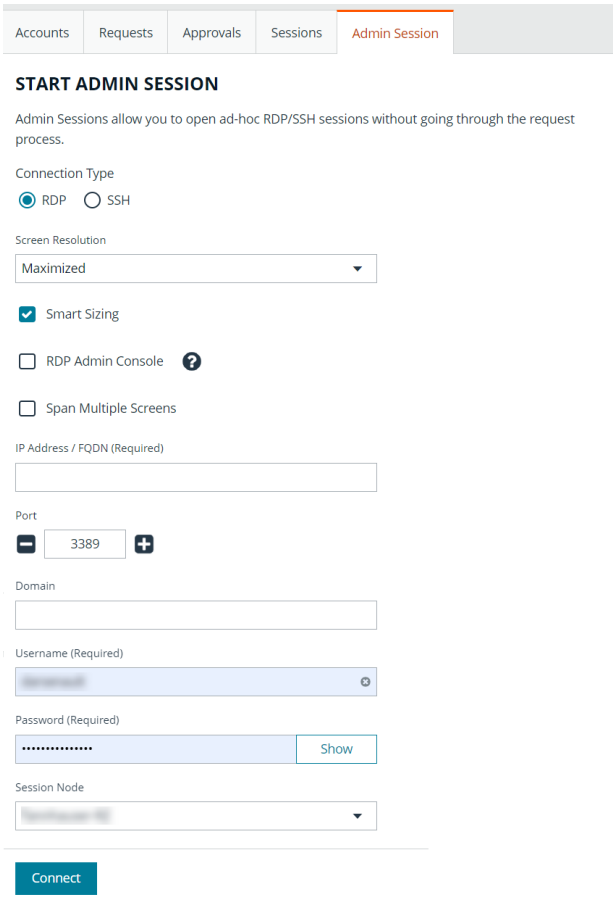
Users who have permissions to bypass the request and approval process for accessing the managed system and Password Safe administrators are able to start sessions and retrieve passwords immediately from the **Start Session** tab. The **Start Session** tab does not display for users who do not have permissions to bypass the request and approval process. To start the session:

1. From the **Accounts** tab, load the accounts in the grid by clicking a category or using the filter options, and then click **Load All Accounts**.
2. Click **Access** for the managed account for which you wish to request a session.
3. From the **Start Session** tab, select a ticket system and provide a ticket number, if required, check your desired options, and then click **Start RDP Session**. An RDP connection file downloads.
4. Run the file to establish a connection to the target system.
5. Enter your password that you use to authenticate into Password Safe.



Start an Admin Session

Users who have full control permissions for the **Password SafeAdmin Session** feature and Password Safe administrators can open ad-hoc RDP and SSH sessions without going through the request process, using an **Admin Session**. From **Admin Session** tab, you can start a session immediately by completing the form and clicking **Connect**. Admin sessions also allow you to select a node associated with another region to act as a proxy for the session. This is useful in larger environments when assets you need to access are in your region.



SSH Direct Connect

Using an SSH client, a user can use the Password Safe Request and Approval system for SSH remote connections. The requester's information, including the **Reason** and the **Request Duration**, are auto-populated with default Password Safe settings.

To access a managed account or application using Direct Connect, the requester has to connect to Password Safe's SSH Proxy using a custom SSH connection string with one of the following formats:

- **For UPN credentials:**

```
<Requester>+<Username@Domain>+<System Name>@<Password Safe>
```

- **For down-level logon names\non-domain credentials:**

```
<Requester>@<Domain\\Username>@<System Name>@<Password Safe>
```

You can override the default SSH port and enter port **4422**. The requester is then prompted to enter their password, which they use to authenticate with Password Safe.

- **For UPN credentials:**

```
ssh -p 4422 <Requester>+<Username@Domain>+<System Name>@<Password Safe>
```

- **For down-level logon names\non-domain credentials:**

```
ssh -p 4422 <Requester>@<Domain\\Username>@<System Name>@<Password Safe>
```

- **For an SSH application:**

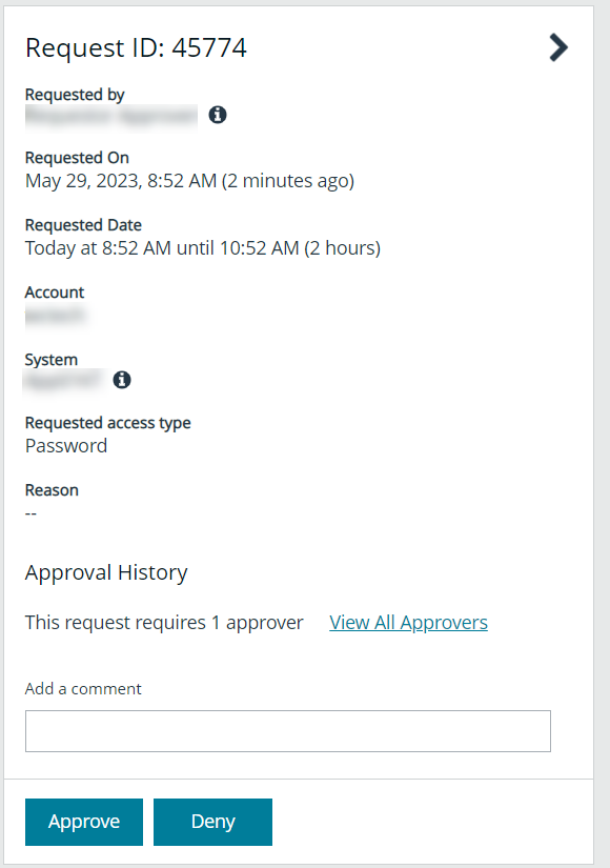
```
ssh -p 4422 <Requester>@<Account name>:<Application alias>@<System name>@<Password Safe>
```

Once the requester is authenticated, they are immediately connected to the desired machine.

Approve or Deny Requests for Passwords and Sessions

When a password request for a system is successfully submitted, the associated approvers for that system are notified by email of the pending request. If you have permissions to approve requests for password releases or sessions for managed systems, you can approve and deny requests from the **Approvals** tab, as follows:

1. Click the vertical ellipsis for the request and select **View Request Details**.
2. Enter a comment for the approval.
3. Click **Approve** or **Deny**.



Note: *An approver is asked to confirm any denied requests. Once a request is approved, the approver can still deny if the situation warrants.*

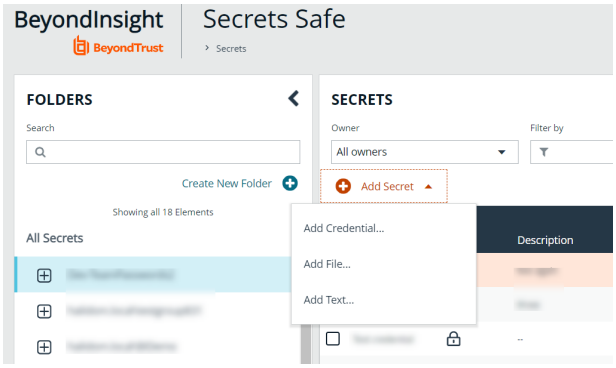
Use Secrets Safe

The Secrets Safe feature allows you to securely store secrets owned by developers and small groups in a controlled environment that you can audit. Secrets Safe supports 3 different types of secrets: credential, file, and text. Password Safe administrators can assign groups in BeyondInsight to teams, in which each team has its own isolated store where users can secure secrets used within that team. The creator of the secret becomes the owner and can assign ownership of the secret to the entire team or one or more individual members. Password Safe administrators and secret owners can manage secret ownership, edit secrets, and delete secrets, while team members may only view and retrieve secrets. Team members can create a folder structure to organize their secrets. Secrets can be found and accessed easily using search and filtering options.

Create a Secret in Secrets Safe

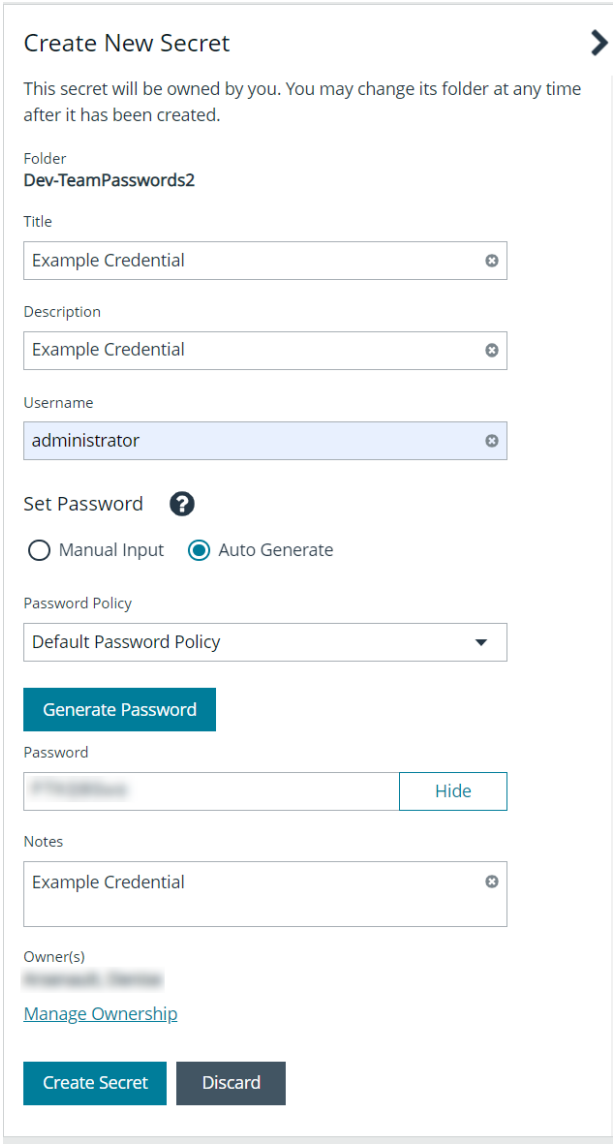
You can create secrets in the parent folder for any of your teams or in any of your team's subfolders. The user who creates the secret is its owner and may change its folder at any time after it has been created.

1. From the left navigation pane, click **Secrets Safe**.
2. From the **Folders** pane, select a folder, and then click **Add Secret** above the grid.
3. Select your secret type: **Add Credential**, **Add File**, or **Add Text**, and then fill out the form for each type as detailed in below steps.



Add Credential

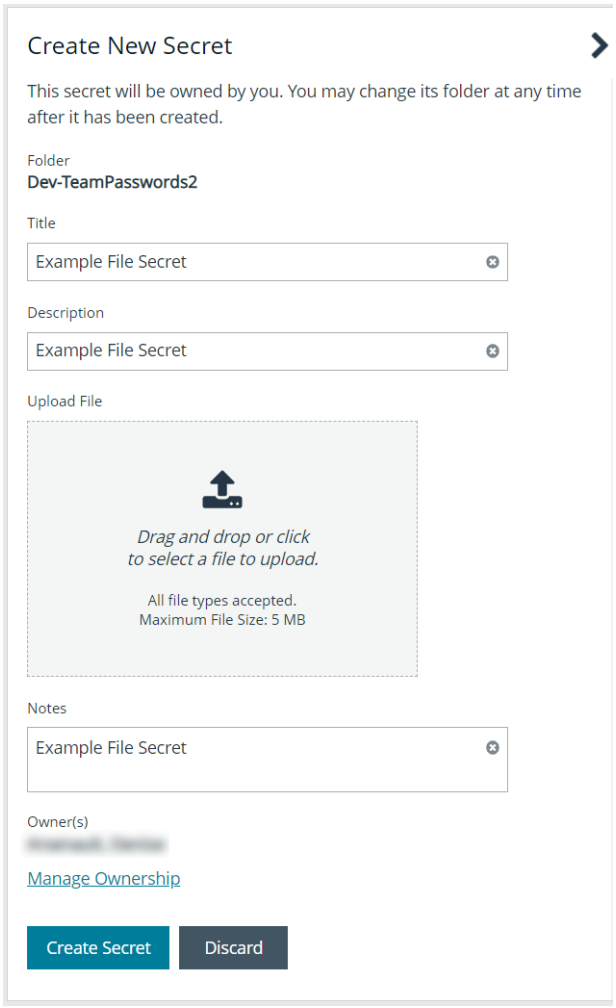
1. Enter a **Title**, **Description**, and **Username**.
2. Set the password:
   - Select **Manual Input** to manually enter a password.
   - Select **Auto Generate** and select a **Password Policy** from the list to have the password created based on the defined policy. Click **Generate Password**.
3. Add a note if you require additional information to display for this credential other than its description. You can add **Notes** as a column when viewing the list of credentials in the grid, and you can also filter the list by **Notes**.
4. Click **Manage Ownership** if you wish to assign ownership to individual team members or to the entire team.
5. Click **Create Secret**.



Add File

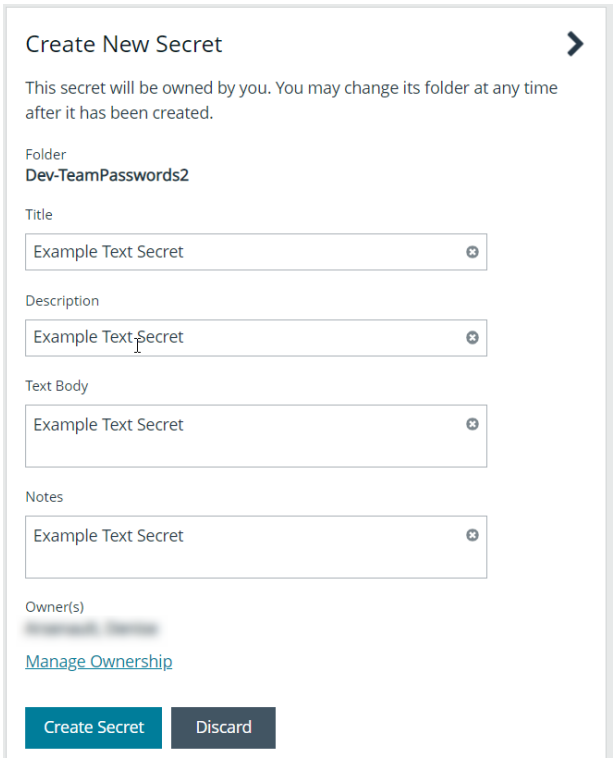
1. Enter a **Title** and **Description**.
2. Drag the file into the **Upload File** box or click the box to select a file to upload.
3. Click **Manage Ownership** if you wish to assign ownership to individual team members or to the entire team.
4. Click **Create Secret**.

> ***Note:*** *There are no restrictions on file type; however, files must be 5MB or less.*



Add Text

1. Enter a **Title** and **Description**.
2. Enter the body of the text.
3. Add a note if you require additional information to display for this credential other than its description. You can add **Notes** as a column when viewing the list of credentials in the grid, and you can also filter the list by **Notes**.
4. Click **Manage Ownership** if you wish to assign ownership to individual team members or to the entire team.
5. Click **Create Secret**.

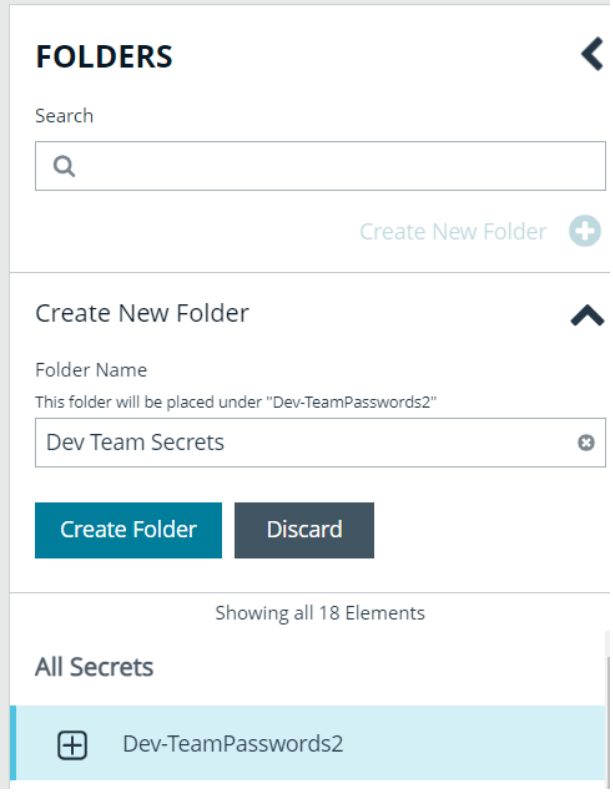


Manage Folders in Secrets Safe

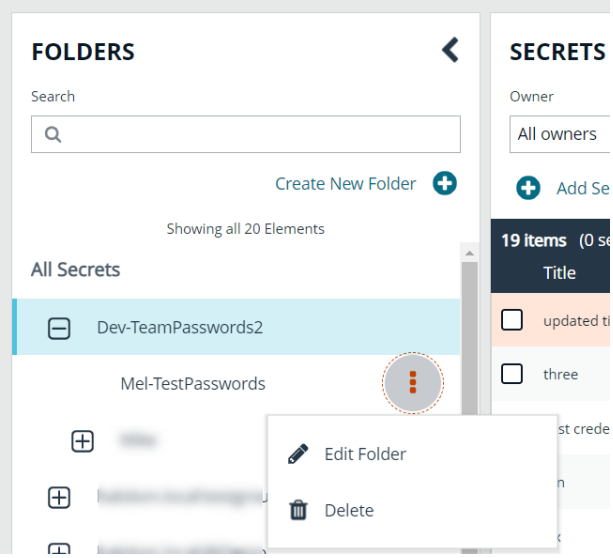
You can organize your team secrets into subfolders under the parent team folder to make locating a secret more efficient.

1. From the left navigation pane, click **Secrets Safe**.

2. To create a new folder, select the parent folder or one of its subfolders, and then click **Create New Folder**.
3. Enter a name for the folder, and then click **Create Folder**.



4. To edit a folder name or to delete a folder, expand the parent folder, click the vertical ellipsis for a subfolder, and then select **Edit Folder** or **Delete**.



> ***Note:*** *You cannot edit the name of a parent folder or delete parent folders. Only subfolders may be deleted. Also, if you do not own all of the secrets in a subfolder, you are not able to delete it.*

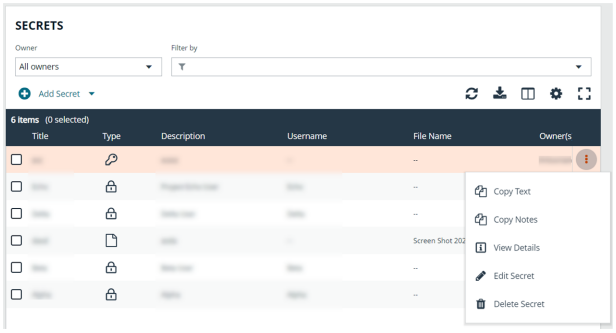
> *For more information on how to move a credential to a new subfolder, please see "Edit and Delete a Secret in Team Secrets Safe" on page 26.*

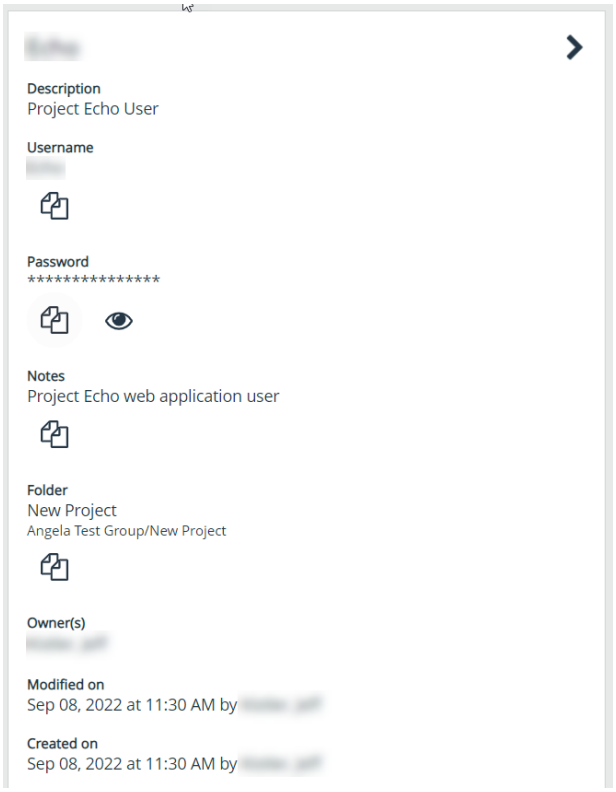
View and Copy a Secret in Secrets Safe

You can view details for your team's secrets, such as who owns the secret, when the secret was created and modified, and the folder path for the secret. You can also copy the username and password for a team secret so you may use it.

1. From the left navigation pane, click **Secrets Safe**.

2. From the **Folders** pane, select a folder.
3. From the **Secrets** grid, click the vertical ellipsis for the secret.
4. Each secret type, as indicated by its **Type** icon, has specific actions available from the options menu, as follows:
    - For credential secrets, you can **Copy Username**, **Copy Password**, and **Copy Notes**.
    - For file secrets, you can **Download File** and **Copy Notes**.
    - For text secrets, you can **Copy Text** and **Copy Notes**.
5. To view the details for any secret, select **View Details** from the menu.





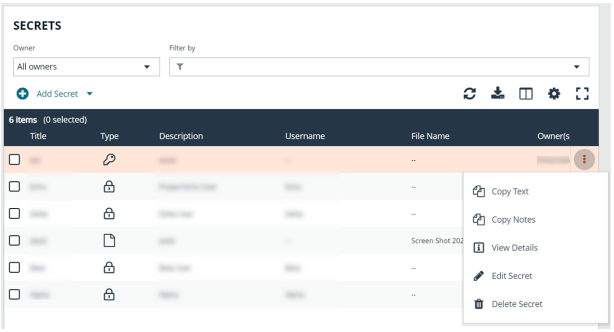
- While viewing the details for a credential secret type, you can:
    - Click the applicable copy icons to copy the username, password, notes, and folder path.
    - Click the eye icon to show the password.
- While viewing the details for a file secret type, you can:
    - Click the download icon to download the file.
    - Click the applicable copy icons to copy the notes and folder path.
- While viewing the details for a text secret type, you can:
    - Click the applicable copy icons to copy the text body, notes, and folder path.

Edit and Delete a Secret in Team Secrets Safe

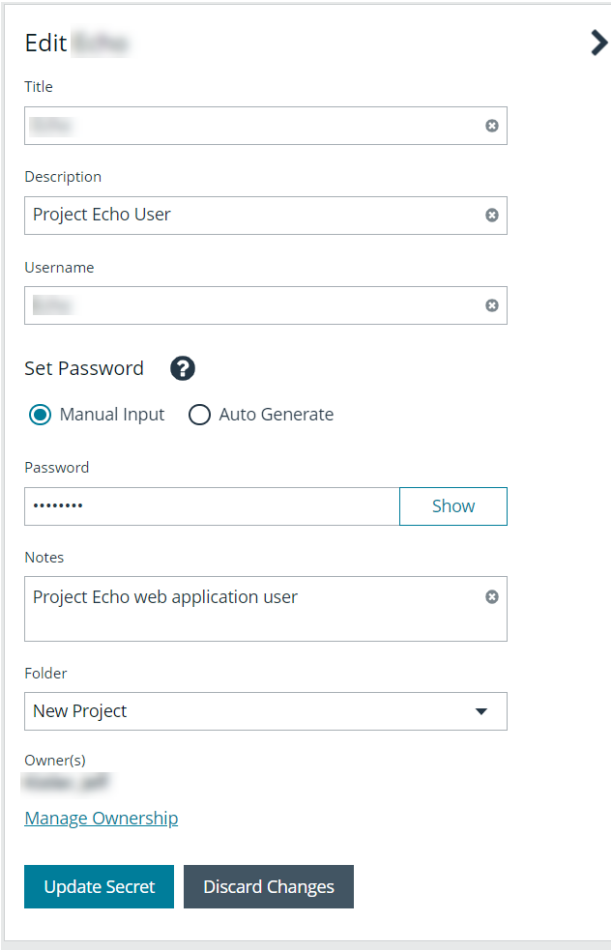
Secret owners can edit the properties and manage ownership for secrets they own, as well as delete secrets they own. Password Safe administrators can edit the properties, manage ownership, and delete all secrets in Secrets Safe.

1. From the left navigation pane, click **Secrets Safe**.
2. From the **Folders** pane, select a folder, and then select a secret.

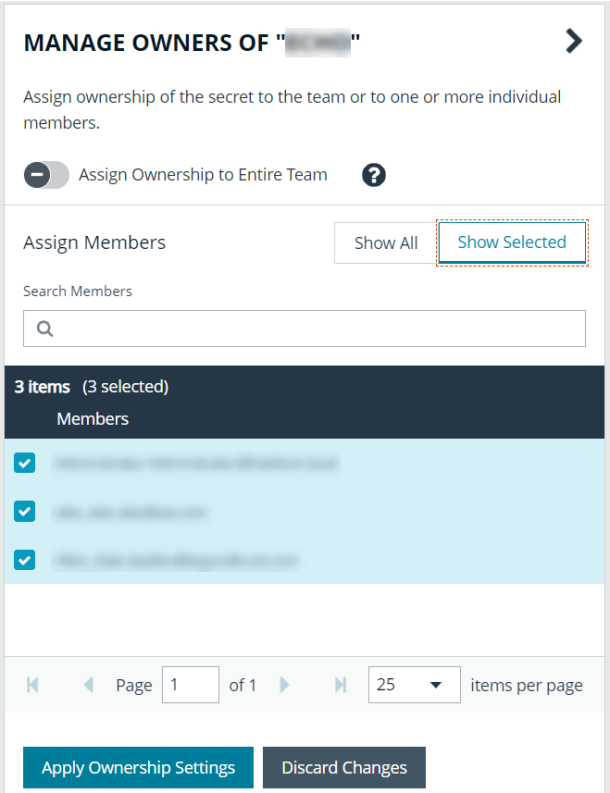
3. Click the vertical ellipsis for the secret.
4. To delete a secret, select **Delete Secret**, and then click **Delete** on the confirmation message.
5. To edit a secret, select **Edit Secret**.



6. Modify the properties for the secret as required. To manage the ownership of the secret, click **Manage Ownership**.



7. Enable the **Assign Ownership to Entire Team** option to assign all members of the team as owners of the secret. When new members are added to the team, they are automatically assigned as owners of the secret. Alternatively, select individual team members as owners.
8. Click **Apply Ownership Settings**.



9. Click **Update Secrets** once you have made your edits.