BeyondTrust

Password Safe 24.1
User Guide

TC:4/16/2024

Table of Contents

Password Safe User Guide

Password Safe 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'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.

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.*

Select a Display Language

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

- English
- French
- German
- 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.

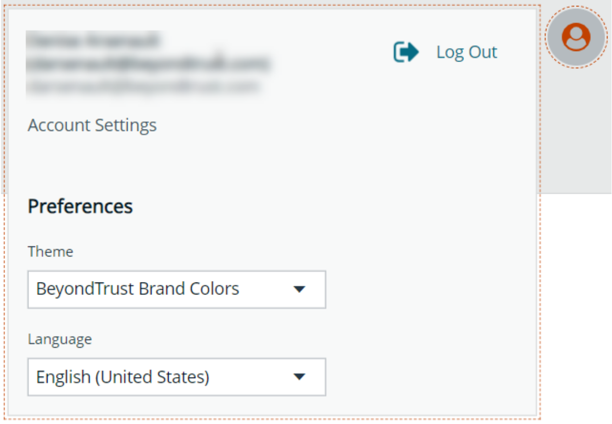
***Note:** If no languages are available, please contact your BeyondInsight administrator.*

Change and Reset Password Safe Login Password

Change Password and Two-Factor Authentication Settings

Users can maintain the security and control of their account and protect it against unauthorized access. 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**.

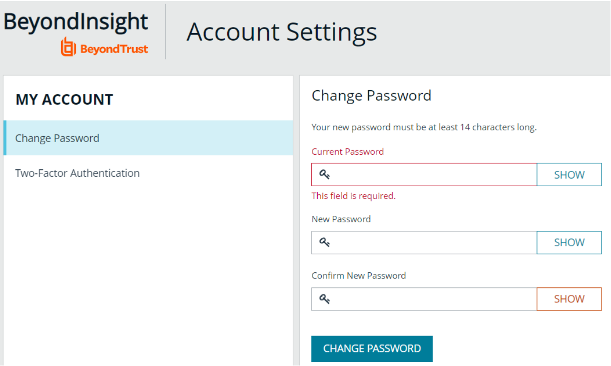


[redacted]

Theme: BeyondTrust Brand Colors

Language: English (United States)

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



Your new password must be at least 14 characters long.

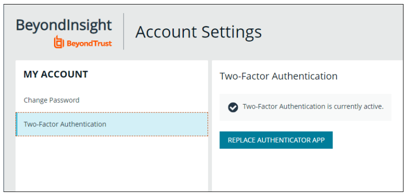
Current Password — SHOW

This field is required.

New Password — SHOW

Confirm New Password — SHOW

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.



BeyondInsight
BeyondTrust
Account Settings
MY ACCOUNT
Change Password
Two-Factor Authentication
Two-Factor Authentication

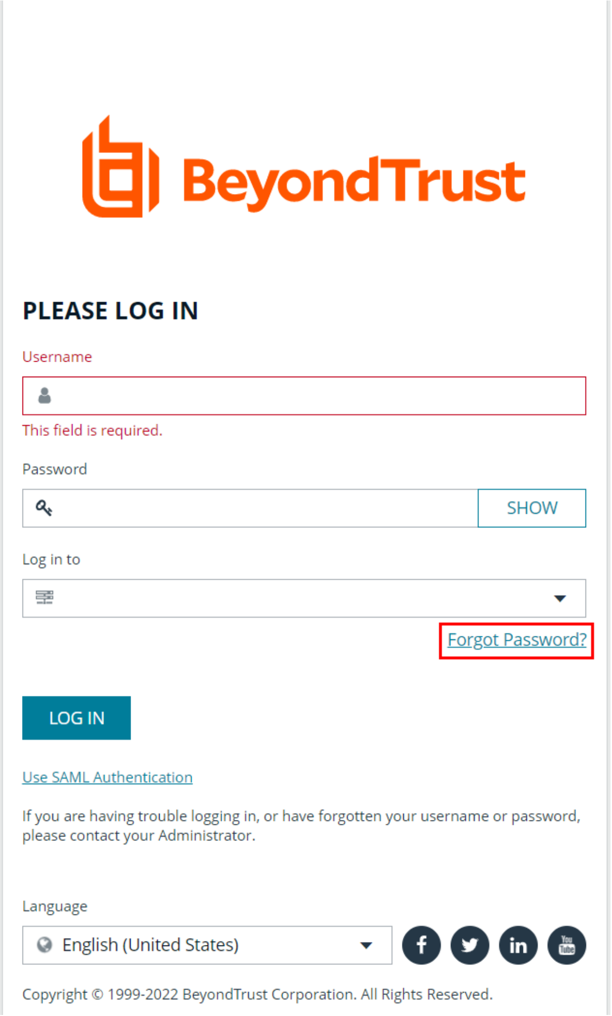
Two-Factor Authentication is currently active.

REPLACE AUTHENTICATOR APP

Reset Password

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

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



BeyondTrust

PLEASE LOG IN

Username

This field is required.

Password

SHOW

Log in to

Forgot Password?

LOG IN

Use SAML Authentication

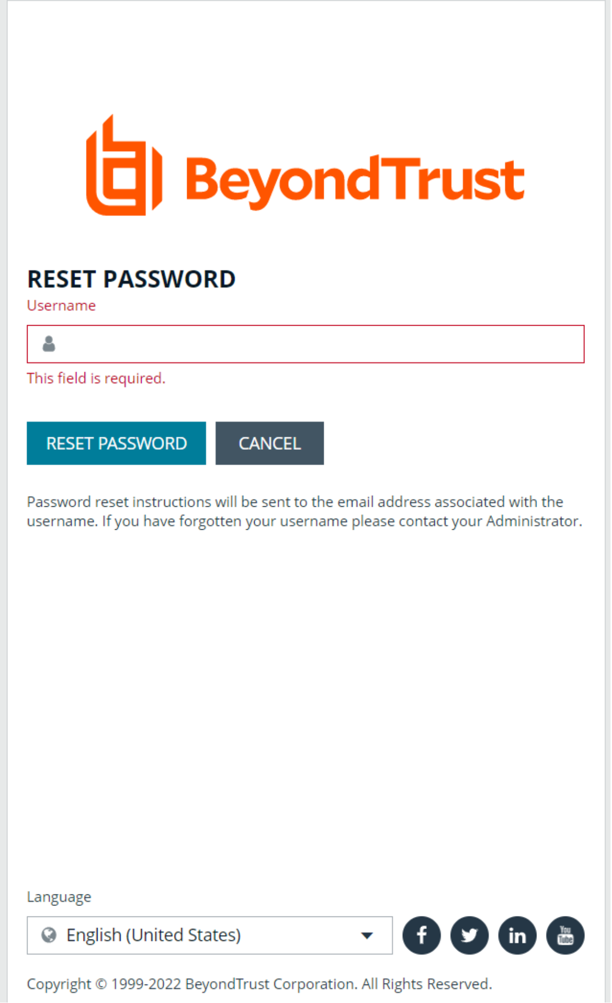
If you are having trouble logging in, or have forgotten your username or password, please contact your Administrator.

Language

English (United States)

Copyright © 1999-2022 BeyondTrust Corporation. All Rights Reserved.

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



RESET PASSWORD

Username

This field is required.

Password reset instructions will be sent to the email address associated with the username. If you have forgotten your username please contact your Administrator.

Language

English (United States)

Copyright © 1999-2022 BeyondTrust Corporation. All Rights Reserved.

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

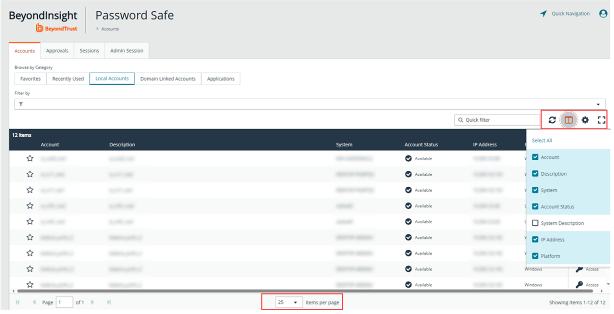
An overview of each tab is described in the sections below.

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.

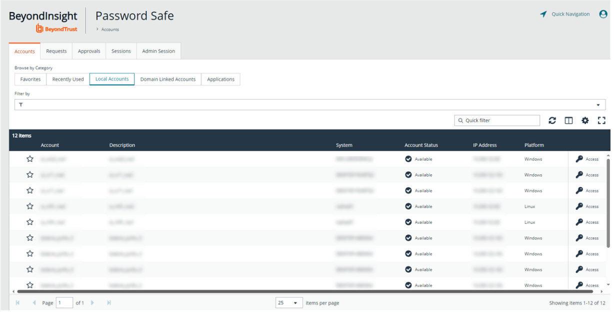
An option to change the number of displayed **Items per page** is located below the grid. The changes appear dynamically as they are selected.



Accounts Tab Overview

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:

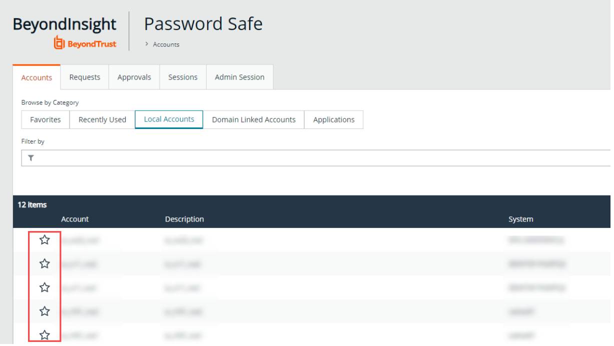
- Click the **Browse by Category** buttons: **Favorites**, **Recently Used**, **Local Accounts**, **Domain Linked Accounts**, and **Applications**, to filter the list by category.
- Select filter criteria from the **Filter by** dropdown to filter by selected account properties.
- Search for accounts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



> ***Note:** The **Status** column from the **Local Accounts** and **Domain Linked Accounts** grids was removed in Password Safe version 23.1. This column, now called **Account Status**, has been re-added in Password Safe version 23.3.*

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 next to the account to add it to the **Favorites** tab. Click **Refresh** above the grid to update the listed accounts.*

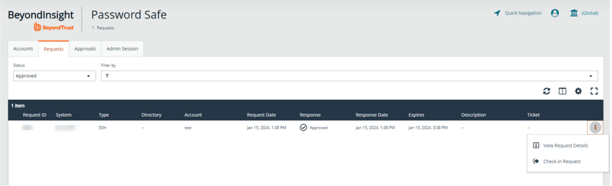


12 items

	Account	Description	System
☆	[redacted]	[redacted]	[redacted]
☆	[redacted]	[redacted]	[redacted]
☆	[redacted]	[redacted]	[redacted]
☆	[redacted]	[redacted]	[redacted]
☆	[redacted]	[redacted]	[redacted]

Requests Tab Overview

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**. You can also check-in a request by clicking on the vertical ellipsis for the request, and selecting **Check-in Request**.



Status: Approved

Filter by

1 Item

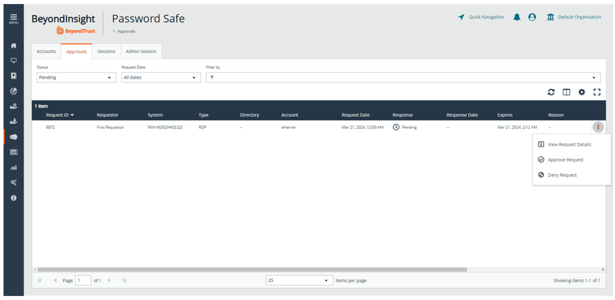
Request ID	System	Type	Directory	Account	Request Date	Response	Response Date	Expires	Description	Ticket
[redacted]	[redacted]	SSH	--	test	Jan 15, 2024, 1:38 PM	Approved	Jan 15, 2024, 1:38 PM	Jan 15, 2024, 3:38 PM	--	--

Approvals Tab Overview

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**.

To approve or deny a request from the **Approvals** grid, click the vertical ellipsis for the request, and then click **Approve Request** or **Deny Request**.



Status: Pending

Request Date: All dates

Filter by

1 Item

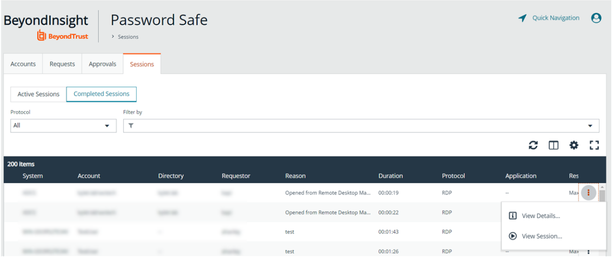
Request ID ▾	Requestor	System	Type	Directory	Account	Request Date	Response	Response Date	Expires	Reason
6872	First Requestor	WIN-MJ5S2HKQLQ2	RDP	--	sihanna	Mar 21, 2024, 12:00 AM	Pending	--	Mar 21, 2024, 2:12 AM	--

Page 1 of 1   25 items per page   Showing Items 1-1 of 1

Sessions Tab Overview

The **Sessions** tab is displayed 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.

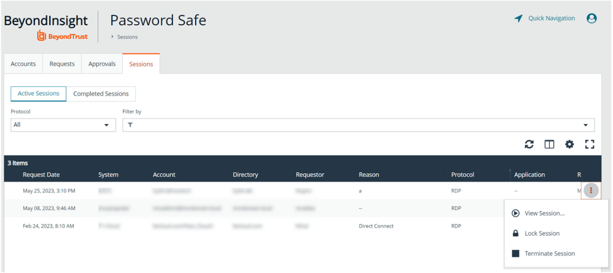


200 items

System	Account	Directory	Requestor	Reason	Duration	Protocol	Application	Res
[redacted]	[redacted]	[redacted]	[redacted]	Opened from Remote Desktop Ma...	00:00:19	RDP	--	Max
[redacted]	[redacted]	[redacted]	[redacted]	Opened from Remote Desktop Ma...	00:00:22	RDP		
[redacted]	[redacted]	--	[redacted]	test	00:01:43	RDP		
[redacted]	[redacted]	--	[redacted]	test	00:01:26	RDP	--	Max

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.*



3 items

Request Date	System	Account	Directory	Requestor	Reason	Protocol	Application	R
May 25, 2023, 3:10 PM	[redacted]	[redacted]	[redacted]	[redacted]	a	RDP	--	M
May 08, 2023, 9:46 AM	[redacted]	[redacted]	[redacted]	[redacted]	--	RDP		
Feb 24, 2023, 8:10 AM	[redacted]	[redacted]	[redacted]	[redacted]	Direct Connect	RDP		

Admin Session Tab Overview

The **Admin Sessions** tab is displayed only for users who have full control permissions to the **Password Safe Admin 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 requesting passwords and sessions, and managing sessions, please see the following:*
>
> - *"Request a Password from Password Safe" on page 11*
> - *"Request and Start Sessions in Password Safe" on page 15*
> - *"Approve or Deny Requests for Passwords and Sessions" on page 21*
> - *"Manage Active Sessions" on page 22*
> - *"View Recorded Sessions" on page 23*

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.

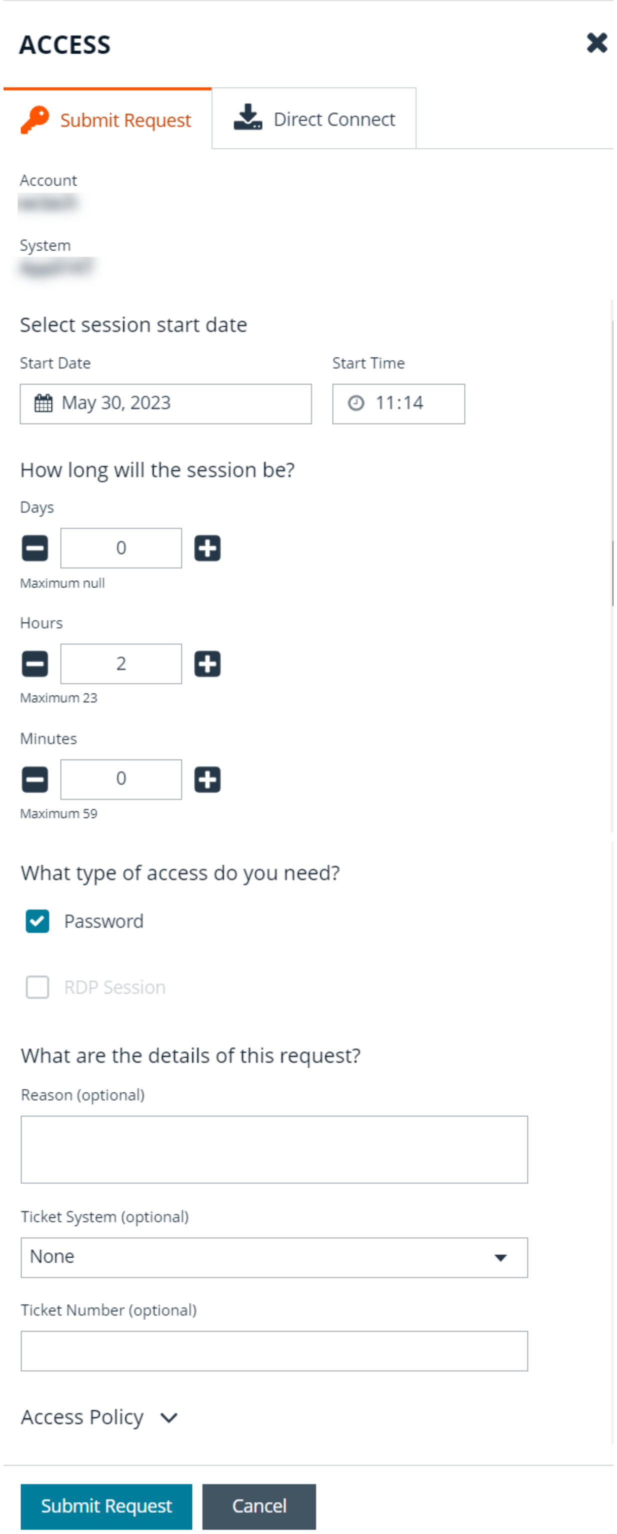
Request a Password Release

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 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 with a one-time use token, which expires after a period of time based on **Session Initialization** timeout settings.
4. Run the file to establish a connection to the target system.
5. Enter the password that you use to authenticate into Password Safe.
6. Click **Access** for the managed account for which you wish to request a password.

7. 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.*

8. 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.



ACCESS

Submit Request | Direct Connect

Account
[redacted]

System
[redacted]

Select session start date

Start Date: May 30, 2023
Start Time: 11:14

How long will the session be?

Days: 0
Maximum null

Hours: 2
Maximum 23

Minutes: 0
Maximum 59

What type of access do you need?

☑ Password

□ RDP Session

What are the details of this request?

Reason (optional):

Ticket System (optional): None

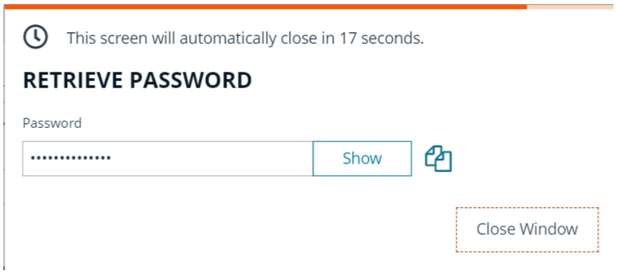
Ticket Number (optional):

Access Policy

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.



This screen will automatically close in 17 seconds.

RETRIEVE PASSWORD

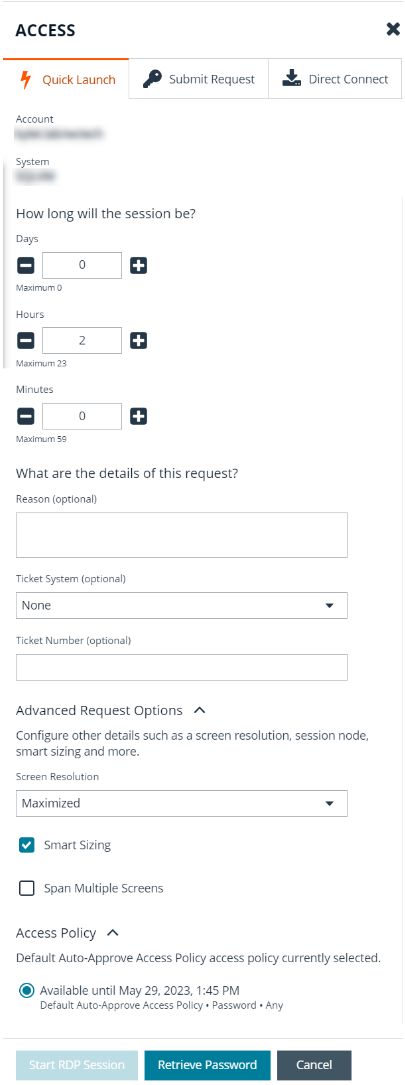
Password: ••••••••••••••

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.



Account
[redacted]

System
[redacted]

How long will the session be?

Days: 0 (Maximum 0)

Hours: 2 (Maximum 23)

Minutes: 0 (Maximum 59)

What are the details of this request?

Reason (optional)

Ticket System (optional): None

Ticket Number (optional)

Advanced Request Options

Configure other details such as a screen resolution, session node, smart sizing and more.

Screen Resolution: Maximized

☑ Smart Sizing

□ Span Multiple Screens

Access Policy

Default Auto-Approve Access Policy access policy currently selected.

● Available until May 29, 2023, 1:45 PM
Default Auto-Approve Access Policy • Password • Any

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 sections below detail how to request and start sessions in Password Safe.

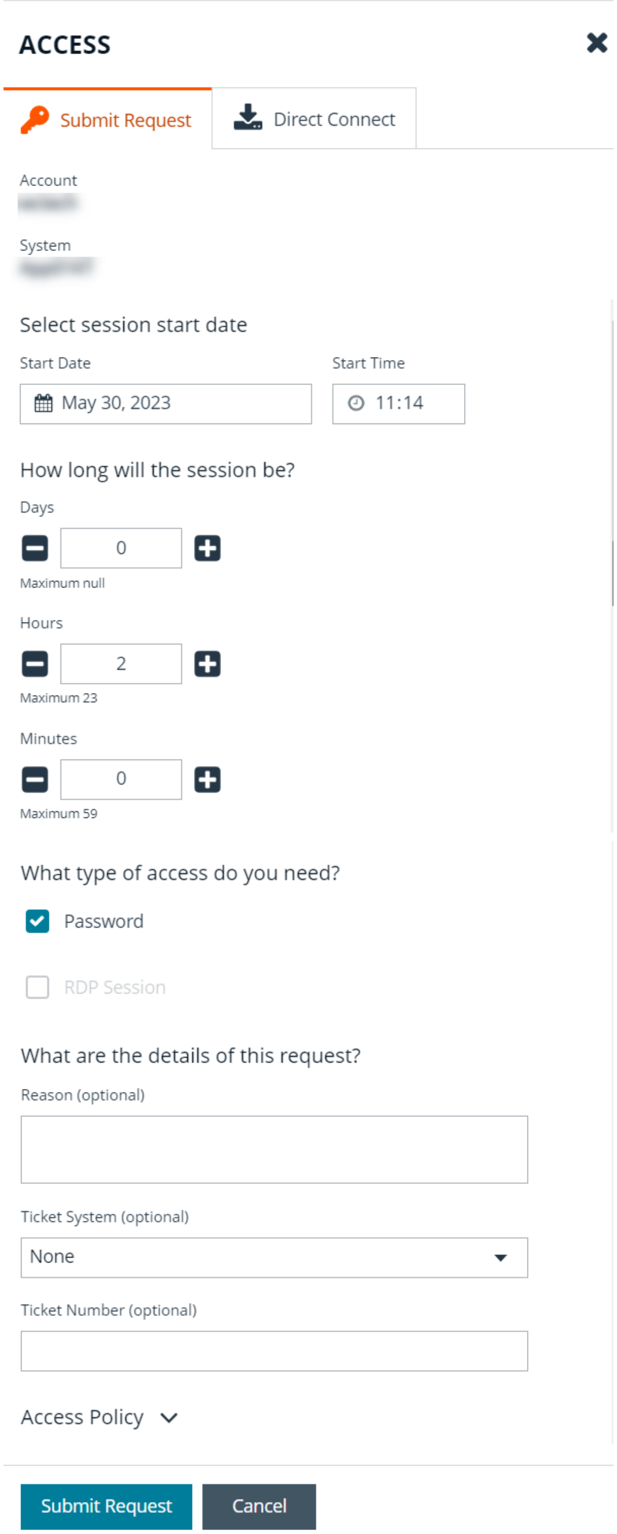
Request an RDP Session

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**.
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 with a one-time use token, which expires after a period of time based on **Session Initialization** timeout settings.
4. Run the file to establish a connection to the target system.
5. Enter the password that you use to authenticate into Password Safe.

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 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.*

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



ACCESS

Submit Request | Direct Connect

Account
[redacted]

System
[redacted]

Select session start date

Start Date: May 30, 2023
Start Time: 11:14

How long will the session be?

Days: 0
Maximum null

Hours: 2
Maximum 23

Minutes: 0
Maximum 59

What type of access do you need?

☑ Password

□ RDP Session

What are the details of this request?

Reason (optional):

Ticket System (optional): None

Ticket Number (optional):

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. 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 with a one-time use token, which expires after a period of time based on **Session Initialization** timeout settings.
4. Run the file to establish a connection to the target system.
5. Enter the password that you use to authenticate into Password Safe.
6. Find the account in the list.Click **Access** for the managed account for which you wish to request a session.
7. From the **Direct Connect** tab, click **Download RDP File**.
8. Run the file to establish a connection to the target system.
9. Enter the password that you use to authenticate into Password Safe.

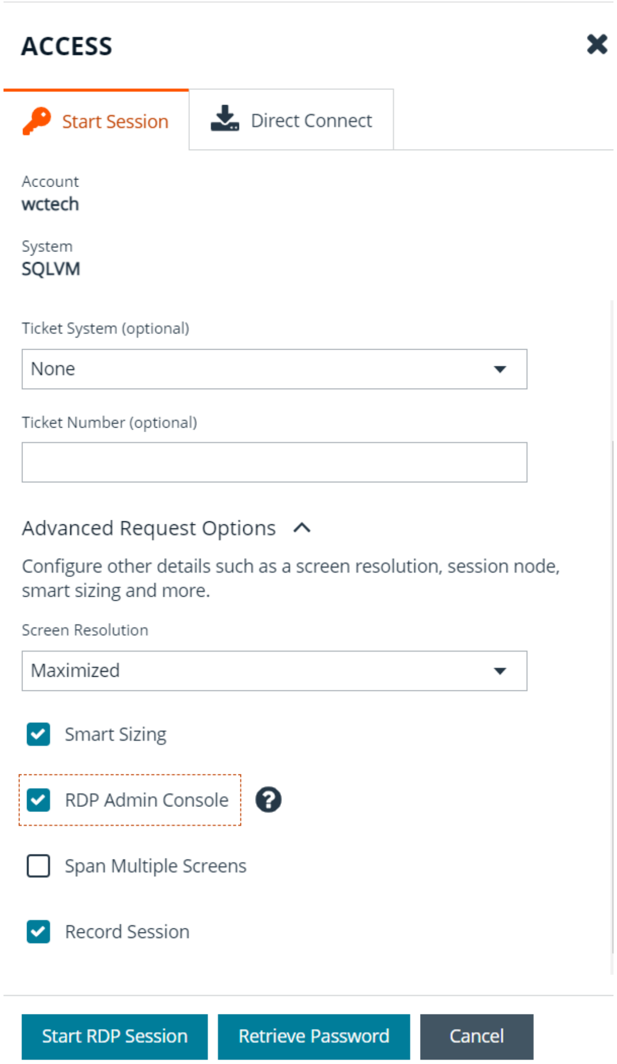
> ***Tip:*** *When using direct connect, enter the password, the defined delimiter, and then the 2FA. The password policy does not need to account for the delimiter.*

> ***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 with a one-time use token, which expires after a period of time based on **Session Initialization** timeout settings.
4. Run the file to establish a connection to the target system.
5. Enter the password that you use to authenticate into Password Safe.



Account
wctech

System
SQLVM

Ticket System (optional)
None

Ticket Number (optional)

Advanced Request Options

Configure other details such as a screen resolution, session node, smart sizing and more.

Screen Resolution
Maximized

☑ Smart Sizing

☑ RDP Admin Console

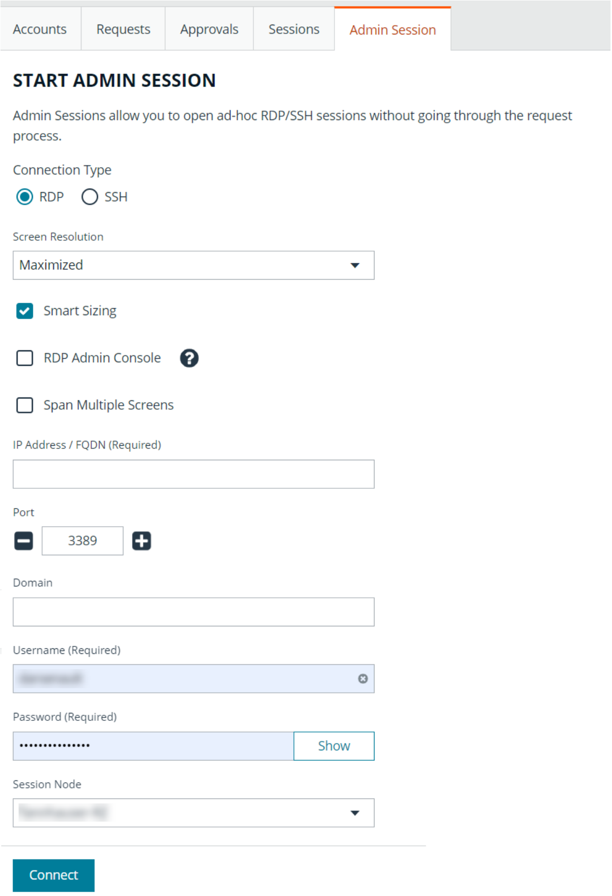
☐ Span Multiple Screens

☑ Record Session

Start an Admin Session

Users who have full control permissions for the **Password Safe Admin 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.

> ***Note:** Admin sessions are recorded by default. If your administrator has enabled the option, a **Record Session** check box displays on the form, giving you the option to record the session or not.*



START ADMIN SESSION

Admin Sessions allow you to open ad-hoc RDP/SSH sessions without going through the request process.

Connection Type
● RDP ○ SSH

Screen Resolution: Maximized

☑ Smart Sizing

□ RDP Admin Console

□ Span Multiple Screens

IP Address / FQDN (Required):

Port: 3389

Domain:

Username (Required): [redacted]

Password (Required): ••••••••••••••• Show

Session Node: [redacted]

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 the password 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:**

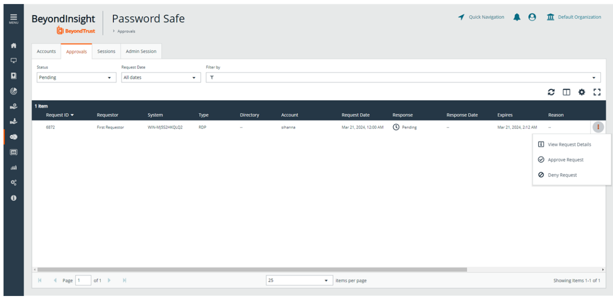
```
ssh -p 4422 <Requester>@<Account name>:<Application alias>@<System name>@<Password Safe>
```

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. Go to **Password Safe > Approvals**.
2. Click the vertical ellipsis to the right of the request and select **Approve Request** or **Deny Request**.



Status: Pending
Request Date: All dates
Filter by

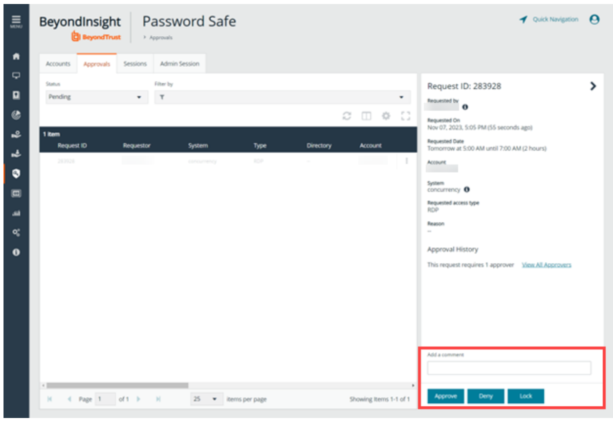
1 Item

Request ID	Requestor	System	Type	Directory	Account	Request Date	Response	Response Date	Expires	Reason
6872	First Requestor	WIN-MJ5S2HKQLQ2	RDP	--	sihanna	Mar 21, 2024, 12:00 AM	Pending	--	Mar 21, 2024, 2:12 AM	--

Page 1 of 1 · 25 items per page · Showing Items 1-1 of 1

To add a comment to the approval:

3. Click the vertical ellipsis to the right of the request and select **View Request Details**.
4. Enter a comment for the approval.
5. Click **Approve** or **Deny**.
6. To lock the request, even if it has previously been approved, click **Lock**. This prevents the requestor from triggering a new session from it.
   - The request can be unlocked to re-allow access.
   - Lock is unavailable if there is an active session running for that request.



Status: Pending
Filter by

1 Item

Request ID	Requestor	System	Type	Directory	Account
283928	[illegible]	concurrency	RDP	--	[illegible]

Page 1 of 1 · 25 items per page · Showing Items 1-1 of 1

Request ID: 283928
Requested by: [illegible]
Requested On: Nov 07, 2023, 5:05 PM (55 seconds ago)
Requested Date: Tomorrow at 5:00 AM until 7:00 AM (2 hours)
Account: [illegible]
System: concurrency
Requested access type: RDP
Reason: --
Approval History
This request requires 1 approver View All Approvers
Add a comment

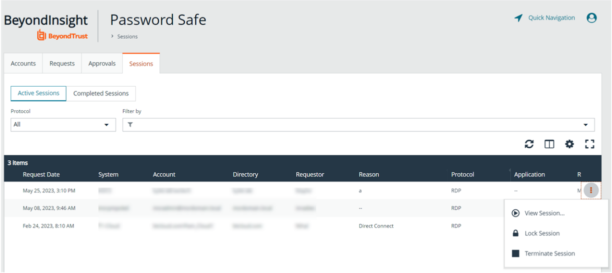
> ***Note:*** *An approver is asked to confirm any denied requests. Once a request is approved, the approver can still deny it if the situation warrants.*

Manage Active Sessions

Password Safe Administrators, ISA users, or users that have been granted permissions to the asset through a Smart Group that is assigned the **Active Session Reviewer** role can view and manage active sessions in real time. While viewing an active session you can lock, terminate, and cancel the session, as detailed in the steps below.

> ***Note:*** *Admin sessions are listed in the grid only for users who have read permissions to the* ***Password Safe Admin Session Reviewer*** *feature.*

1. From the left navigation, click **Menu**, and then under **Password Safe**, click **Active Sessions**.
2. Use the dropdowns above the grid to locate the session you wish to view or manage, and then click the vertical ellipsis for the session.
    - Click **Lock** to immediately lock the session.
    - Click **Terminate** to immediately disconnect the session.
    - Click **View Session** to view the active session.

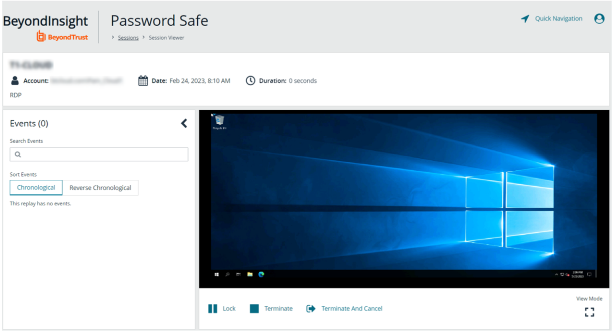


3 items

Request Date	System	Account	Directory	Requestor	Reason	Protocol	Application	R
May 25, 2023, 3:10 PM	[redacted]	[redacted]	[redacted]	[redacted]	a	RDP	--	M
May 08, 2023, 9:46 AM	[redacted]	[redacted]	[redacted]	[redacted]	--	RDP		
Feb 24, 2023, 8:10 AM	[redacted]	[redacted]	[redacted]	[redacted]	Direct Connect	RDP		

> ***Note:*** *Keystrokes, such as those used when the user opens a window, accesses an application, or clicks an option, are logged in the* ***Events*** *pane as they are executed. You can sort these chronologically but you cannot select them during an active session.*

3. While viewing an active session, use the controls below the session display window as follows:
    - Click **Lock** to immediately lock the session
    - Click **Terminate** to immediately disconnect the session.
    - Click **Terminate and Cancel** to immediately end a session and check in the request.



[redacted]

Account: [redacted]   Date: Feb 24, 2023, 8:10 AM   Duration: 0 seconds

RDP

This replay has no events.

> ***Note:*** *The* ***Terminate and Cancel*** *button is only present for sessions initiated by requestors. It is not available for sessions initiated by administrators or ISA users. It is also not available for Admin Sessions.*

> ***Note:*** *When a session is locked or terminated, the user receives a message indicating the session has been locked or terminated and to contact their administrator. Terminated sessions are removed from the* ***Active Sessions*** *grid, and can be viewed from the* ***Completed Sessions*** *grid.*

View Recorded Sessions

For auditing purposes, all RDP and SSH sessions in Password Safe can be recorded and accessible for viewing from the **Sessions > Completed Sessions** grid. Session recording is available for regular sessions, ISA sessions, and Admin sessions. The following users can view recorded sessions:

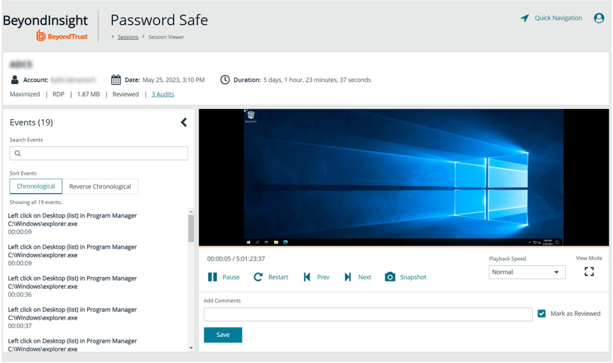
- Administrators
- Users with the Auditor role
- Users with the Recorded Session Reviewer role
- Users with the ISA role

To access and review completed sessions in Password Safe, follow these steps:

1. From the left navigation, click **Menu**, and then click **Completed Sessions** under **Password Safe**.
2. Use the **Protocol** and **Filter By** dropdowns above the grid to filter the list to assist with locating the desired session. Once you have located the session you wish to view, click the vertical ellipsis for it, and then select **View Session** .
    - Alternatively, you can select **View Details** and then click the **View Session** link from the **Session Details** pane.

> *Tip:* *If a session recording has been archived, the* ***View Session*** *option is not available. If available, select the* ***Restore Session*** *option to restore the recording. You can also restore the archived session from the session's details by selecting* ***View Details*** *and then clicking the* ***Restore*** *link.*

3. Once the session displays, click **Play** to review the recording. You can hover over any part of the video progress bar to reveal the time stamp and click anywhere on the bar to select an instance in the recorded session. Use the control buttons below the recording to pause and restart the recording.



[redacted]

Account: [redacted] Date: May 25, 2023, 3:10 PM Duration: 5 days, 1 hour, 23 minutes, 37 seconds

Maximized | RDP | 1.87 MB | Reviewed | 3 Audits

Showing all 19 events.

Left click on Desktop (list) in Program Manager
C:\Windows\explorer.exe
00:00:09

Left click on Desktop (list) in Program Manager
C:\Windows\explorer.exe
00:00:09

Left click on Desktop (list) in Program Manager
C:\Windows\explorer.exe
00:00:36

Left click on Desktop (list) in Program Manager
C:\Windows\explorer.exe
00:00:37

Left click on Desktop (list) in Program Manager
C:\Windows\explorer.exe

00:00:05 / 5:01:23:37

Playback Speed: Normal

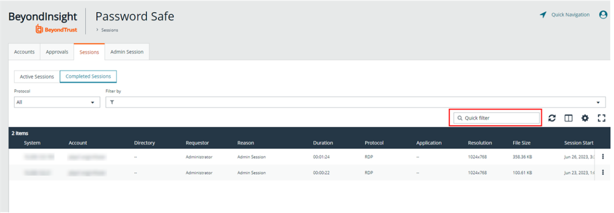
☑ Mark as Reviewed

> *Tip:* *Keystrokes that occurred within the session, such as the user opening a window, accessing an application, or clicking an option, are stored as events and listed in the* ***Events*** *pane to the left of the recorded session. You can click specific listed events or click the* ***Prev*** *and* ***Next*** *buttons below the recording to skip to those events within the recording.*
>
> *To take a screenshot of a session frame and export it as a JPEG file, click the* ***Snapshot*** *button. The file exports with a resolution of 1024 × 768. The JPEG file is automatically saved to the default download location specified in your browser settings.*

4. Add comments and check **Mark as Reviewed** for auditing purposes.
5. The number of audits is displayed as a link above the session recording. Click the link to view who viewed the session and when, as well as to see their comments.

Use Keystroke Search

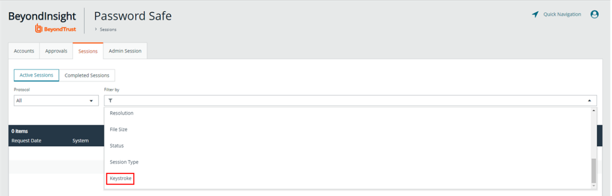
To find sessions in either **Active Sessions** or **Completed Sessions**, enter a word or phrase in the **Quick filter** field. The list of sessions is automatically filtered based on what is entered in the field.



2 items

System	Account	Directory	Requestor	Reason	Duration	Protocol	Application	Resolution	File Size	Session Start
[redacted]	[redacted]	--	Administrator	Admin Session	00:01:24	RDP	--	1024x768	358.36 KB	Jun 26, 2023, 3:
[redacted]	[redacted]	--	Administrator	Admin Session	00:00:22	RDP	--	1024x768	100.61 KB	Jun 23, 2023, 1:

To search for global keystrokes, select **Keystroke** from the **Filter by** dropdown list, and then enter a word or phrase in the **Keystroke** field.



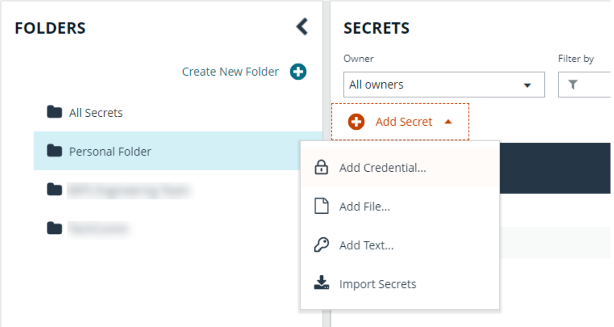
Use Secrets Safe

The Secrets Safe feature minimizes the risk of unauthorized access to secrets. It 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

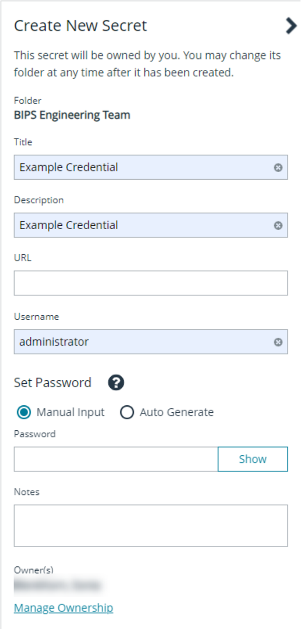
You can create secrets in the parent folder for any of your teams or in any of your team's subfolders. The user who creates the secret is its owner and may change its folder at any time after it has been created.

1. From the left menu, 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**, **Add Text**, or **Import Secrets**, 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**.



Create New Secret

This secret will be owned by you. You may change its folder at any time after it has been created.

Folder
BIPS Engineering Team

Title
Example Credential

Description
Example Credential

URL

Username
administrator

Set Password

● Manual Input ○ Auto Generate

Password

Notes

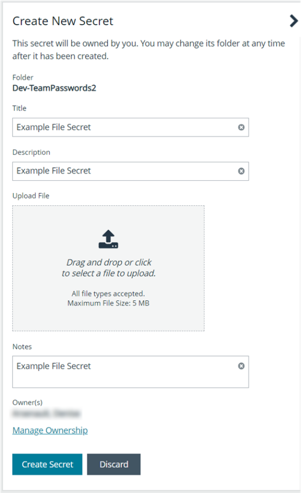
Owner(s)
[redacted]

Manage Ownership

> ***Note:** The **Manage Ownership** feature will not display if you create a secret within your personal folder.*

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**.



Create New Secret

This secret will be owned by you. You may change its folder at any time after it has been created.

Folder
Dev-TeamPasswords2

Title
Example File Secret

Description
Example File Secret

Upload File

Drag and drop or click to select a file to upload.

All file types accepted.
Maximum File Size: 5 MB

Notes
Example File Secret

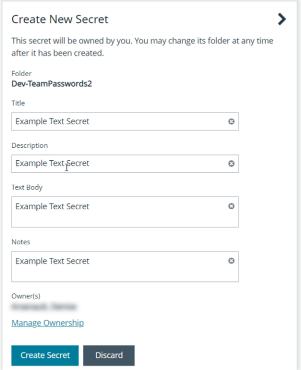
Owner(s)
[redacted]

Manage Ownership

> ***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**.



Create New Secret

This secret will be owned by you. You may change its folder at any time after it has been created.

Folder
Dev-TeamPasswords2

Title: Example Text Secret

Description: Example Text Secret

Text Body: Example Text Secret

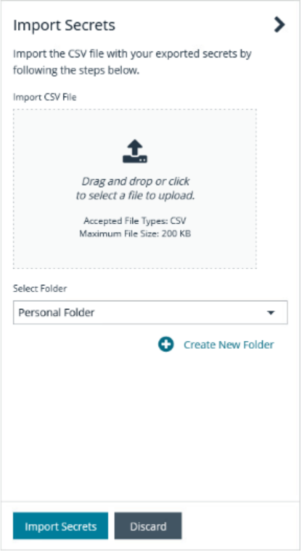
Notes: Example Text Secret

Owner(s)
[redacted]

Import Secrets

1. Drag the file into the **Import CSV File** box or click the box to select a file to upload.
2. Select a folder or create a new folder to save the imported secret to.
3. Click **Import Secrets**.

> ***Note:*** *File type must be CSV. Files must be 200KB or less.*



Import Secrets

Import the CSV file with your exported secrets by following the steps below.

Import CSV File

Drag and drop or click to select a file to upload.

Accepted File Types: CSV
Maximum File Size: 200 KB

Select Folder: Personal Folder

IMPORTANT!

- *Import Secret file type must be CSV*
- *Files must be 200KB or less.*
- *CSV files must contain the following:*
  - *CSV (comma is the only supported field separator)*
  - *Header row (the first row in the file is skipped and seconds are processed starting on line two)*

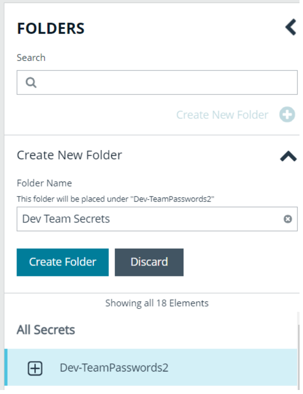
- *Eight columns are required (not all columns are used)*
  - *URL*
  - *Username*
  - *Password*
  - *TOTP <Not Used>*
  - *Extra <Not Used>*
  - *Name*
  - *Grouping <Not Used>*
  - *Fav <Not Used>*
- ***Example:** CSV File - url,username,password,totp,extra,name,grouping,fav*

URL	*Username*	*Password*	*TOTP*	*Extra*	*Name*	*Group*	*Favourite*
https://www.testsite00001.com	*TestUser01*	*password01*			*TestName001*		
https://www.testsite00002.com	*TestUser02*	*password02*			*TestName002*		

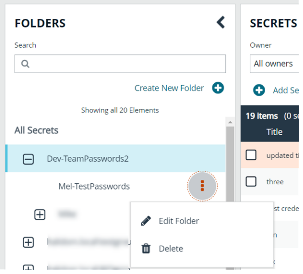
Manage Folders in Secrets Safe

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

1. From the left menu, 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**.



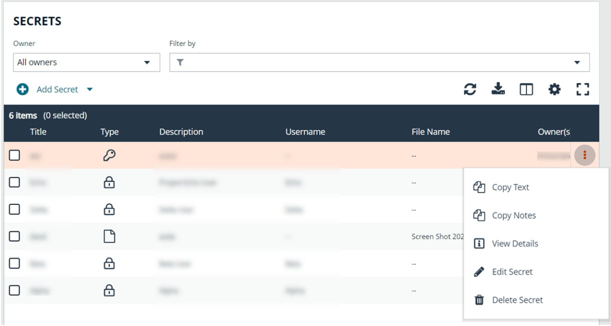
> ***Note:** You cannot edit the name of a parent folder or delete parent folders. Only subfolders may be deleted. Also, if you do not own all of the secrets in a subfolder, you are not able to delete it.*

> *For more information on how to move a credential to a new subfolder, please see "Edit and Delete a Secret in Secrets Safe" on page 29.*

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 secret so you can use it.

1. From the left menu, 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.



SECRETS

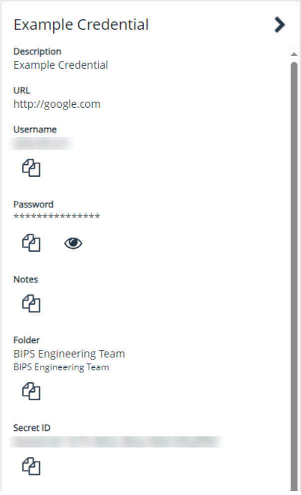
Owner: All owners

Filter by:

6 items (0 selected)

	Title	Type	Description	Username	File Name	Owner(s
□	[redacted]	🔑	[redacted]	[redacted]	--	[redacted]
□	[redacted]	🔒	[redacted]	[redacted]	--	
□	[redacted]	🔒	[redacted]	[redacted]	--	
□	[redacted]	📄	[redacted]	[redacted]	Screen Shot 202	
□	[redacted]	🔒	[redacted]	[redacted]	--	
□	[redacted]	🔒	[redacted]	[redacted]	--	

- While viewing the details for a credential secret type, you can:
    - Click the applicable copy icons to copy the username, password, notes, folder path, and secret ID.
    - 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.



Example Credential

Description
Example Credential

URL
http://google.com

Username
[redacted]

Password
****

Notes

Folder
BIPS Engineering Team
BIPS Engineering Team

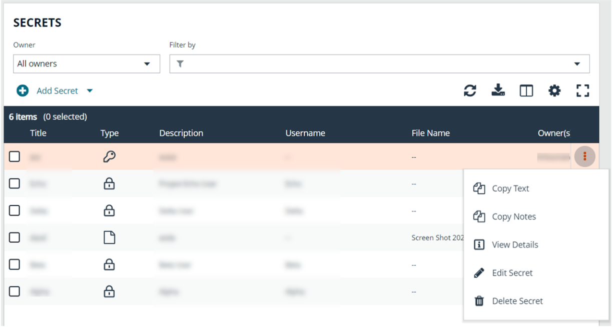
Secret ID
[redacted]

Edit and Delete a Secret in 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 menu, 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**.



SECRETS

Owner: All owners

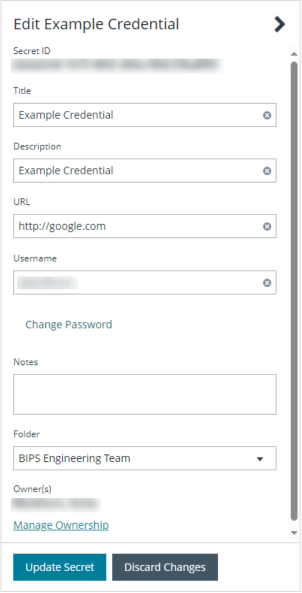
Filter by:

Add Secret

6 items (0 selected)

	Title	Type	Description	Username	File Name	Owner(s
□	[redacted]	🔑	[redacted]	[redacted]	--	[redacted]
□	[redacted]	🔒	[redacted]	[redacted]	--	
□	[redacted]	🔒	[redacted]	[redacted]	--	
□	[redacted]	📄	[redacted]	[redacted]	Screen Shot 202	
□	[redacted]	🔒	[redacted]	[redacted]	--	
□	[redacted]	🔒	[redacted]	[redacted]	--	

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



Edit Example Credential

Secret ID: [redacted]

Title: Example Credential

Description: Example Credential

URL: http://google.com

Username: [redacted]

Change Password

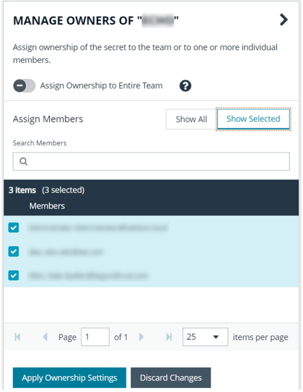
Notes:

Folder: BIPS Engineering Team

Owner(s): [redacted]

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**.



MANAGE OWNERS OF "[redacted]"

Assign ownership of the secret to the team or to one or more individual members.

○ Assign Ownership to Entire Team

Assign Members

Search Members

3 items (3 selected)

	Members
☑	[redacted]
☑	[redacted]
☑	[redacted]

Page 1 of 1 | 25 items per page

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

Workforce Passwords User Guide

As enterprise applications continue to expand, so do access credentials for employees. Rather than using insecure credential storage methods, such as storing credentials on a desktop, in Notepad, or in an email, you can leverage Workforce Passwords within Password Safe as a secure enterprise credential storage method.

Workforce Passwords provides a browser extension, available in Chrome, Edge, and Firefox, to seamlessly inject stored credentials for enterprise application URLs.

Once the extension is downloaded, you can access any credentials (with URLs) that are stored in Secrets Safe. You can manage your stored credentials by logging into Password Safe and also using the browser extension.

Workforce Passwords requires Password Safe 23.2 or a later release.

Manage Credentials and Folders in Secrets Safe

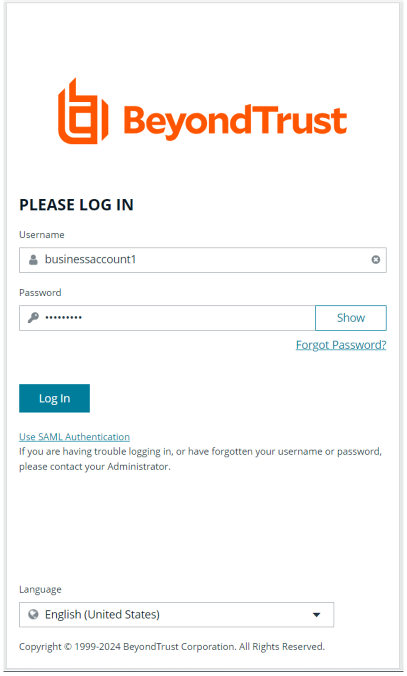
With Workforce Passwords, you have access to a **Personal Folder** located in Secrets Safe. Credentials within this folder are only accessible to you, the user who created them. Sub-folders can also be added within the **Personal Folder**. You can create multiple secrets within the **Personal Folder** or any of its sub-folders.

> ***Note:*** *Workforce Passwords should only be used for business credentials. Information stored in a personal folder is recoverable by an administrator of the site.*

Add a New Secret for Workforce Passwords

To add a new secret in Secrets Safe that can be accessed using Workforce Passwords:

1. Log in to Password Safe using the credentials and URL provided by your administrator.



PLEASE LOG IN

Username: businessaccount1

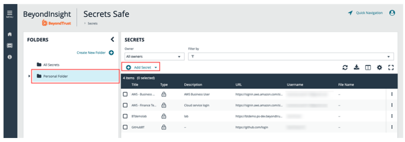
Password: •••••••••

If you are having trouble logging in, or have forgotten your username or password, please contact your Administrator.

Language: English (United States)

Copyright © 1999-2024 BeyondTrust Corporation. All Rights Reserved.

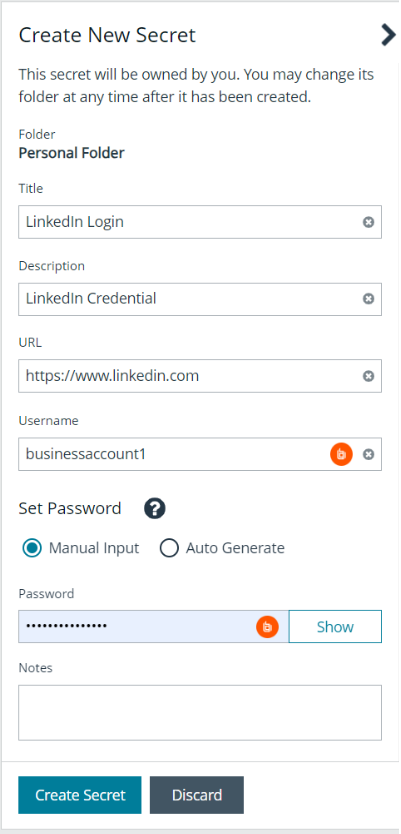
2. From the left menu, click **Secrets Safe**.
3. Under **Folders**, select the **Personal Folder** or a sub-folder in which to create the secret.



4 items (0 selected)

Title	Type	Description	URL	Username	File Name
AWS - Business ...		AWS Business User	https://signin.aws.amazon.com/si...	[redacted]	–
AWS - Finance Te...		Cloud service login	https://signin.aws.amazon.com/si...	[redacted]	–
BTdemolab		lab	https://btdemo.ps-dev.beyondtru...	[redacted]	–
GitHubBT		–	https://github.com/login	[redacted]	–

4. Under **Secrets**, click **Add Secret**, and then select one of the following:
   - **Add Credential**
   - **Add File**
   - **Add Text**
   - **Import Secrets**
5. For **Credential**, **File**, and **Text** secret types:
   - Enter the following information in the **Create New Secret** form:
     - **Title**: Title of the secret.
     - **Description**: Description of the credential to highlight the use and purpose.
     - **URL**: The web address of the site you want to log in to.
     - Any other required information.
   - Click **Create Secret** to save the secret in the folder selected.
6. For the **Import Secret** type:
   - Drag and drop the file into the **Import CSV File** box, or click in the box to select a file to upload.
   - Select a folder from the dropdown or create a new folder to save the secret to.
   - Click **Import Secrets**.



Create New Secret

This secret will be owned by you. You may change its folder at any time after it has been created.

Folder
Personal Folder

Title
LinkedIn Login

Description
LinkedIn Credential

URL
https://www.linkedin.com

Username
businessaccount1

Set Password

● Manual Input ○ Auto Generate

Password
•••••••••••••••

IMPORTANT!

- *Import Secret file type must be CSV*
- *Files must be 200KB or less.*
- *CSV files must contain the following:*
  - *CSV (comma is the only supported field separator)*
  - *Header row (the first row in the file is skipped and seconds are processed starting on line two)*

- *Eight columns are required (not all columns are used)*
  - *URL*
  - *Username*
  - *Password*
  - *TOTP <Not Used>*
  - *Extra <Not Used>*
  - *Name*
  - *Grouping <Not Used>*
  - *Fav <Not Used>*

- ***Example:*** *CSV File - url,username,password,totp,extra,name,grouping,fav*

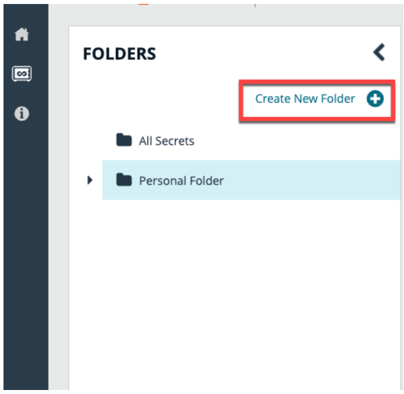
URL	*Username*	*Password*	*TOTP*	*Extra*	*Name*	*Group*	*Favourite*
https://www.testsite00001.com	*TestUser01*	*password01*			*TestName001*		
https://www.testsite00002.com	*TestUser02*	*password02*			*TestName002*		

Tip: *You can either manually input a password or select* ***Auto Generate*** *under* ***Set Password****. To leverage Password Safe policies for creating strong passwords, please see* *Create Password Policies* *at* *https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/create-password-policies.htm*.

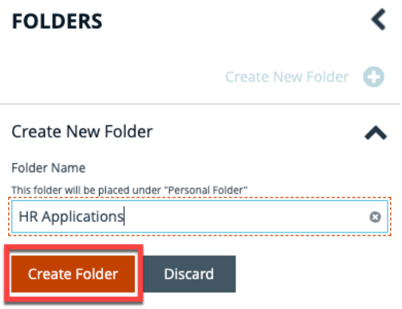
Add a Sub-folder

To add a sub-folder under the **Personal Folder**:

1. Under **Folders**, select your **Personal Folder**.
2. Click **Create New Folder**.



3. Give the folder a name, and then click **Create Folder**.



Once the folder is created, a notification displays with the message that your folder has been created. Navigate to your **Personal Folder** to see your newly created sub-folder.

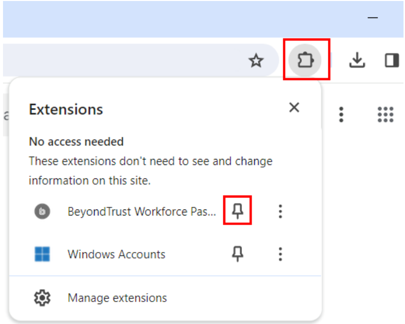
Setup Workforce Passwords Browser Extension

Add the Workforce Passwords Extension

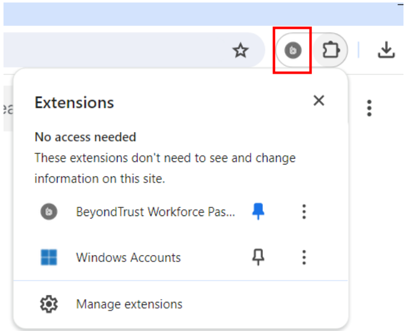
The Workforce Passwords Extension is available in the Chrome Web Store, the Microsoft Edge Add-ons Store, and the Firefox Browser Add-ons Store.

To download from the Chrome Web Store:

1. Navigate to the extension in the web store: Chrome Web Store at https://chrome.google.com/webstore/detail/beyondtrust-workforce-pas/lchpepnpfkooehfcdnlaklepfiedhipi.
2. Click the **Add to Chrome** button.
3. A pop up message asks if you want to **Add BeyondTrust Workforce Passwords?**. Click **Add extension**.
4. A pop up message displays confirming the extension has been added to Chrome.
5. To add the **BeyondTrust Workforce Passwords** icon to the toolbar:
   - Click the **Extensions** icon in the toolbar.
   - Click the **Pin** icon next to the **BeyondTrust Workforce Passwords** extension.


Extensions
No access needed
These extensions don't need to see and change information on this site.
BeyondTrust Workforce Pas...
Windows Accounts
Manage extensions

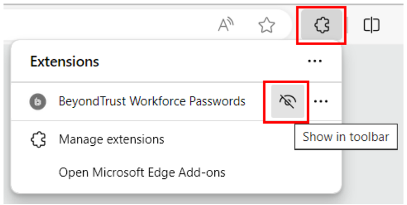
6. The **BeyondTrust Workforce Passwords** icon displays in the toolbar.



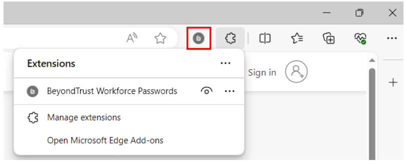
These extensions don't need to see and change information on this site.

To download from the Edge Add-ons Store:

1. Navigate to the extension in the add-ons store: Edge Add-ons at https://microsoftedge.microsoft.com/addons/detail/beyondtrust-workforce-pas/djojdgogandjnhpnmnpodfcgnbjmbich.
2. Click the **Get** button.
3. A pop up message asks if you want to **Add BeyondTrust Workforce Passwords to Microsoft Edge?**. Click **Add extension**.
4. A pop up message displays confirming the extension has been added to Edge.
5. To add the **BeyondTrust Workforce Passwords** icon to the toolbar:
   - Click the **Extensions** icon in the toolbar.
   - Click the **Show in toolbar** icon next to the **BeyondTrust Workforce Passwords** extension.



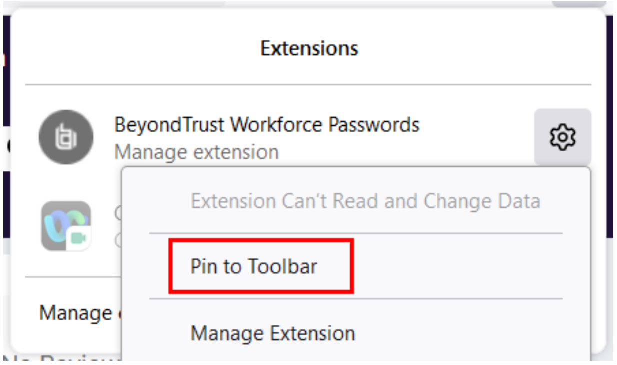
6. The **BeyondTrust Workforce Passwords** icon displays in the toolbar.



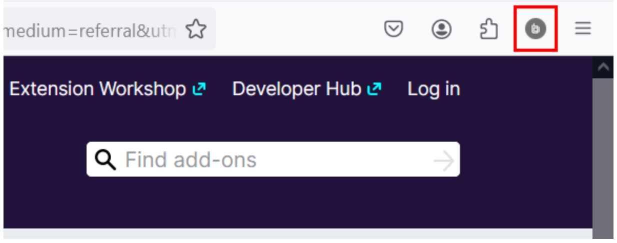
To download from the Firefox Add-ons Store:

1. Navigate to the extension in the Firefox Browser Add-ons Store at https://addons.mozilla.org/en-US/firefox/addon/beyondtrust-workforcepasswords/.
2. Click the **Add to Firefox** button.
3. A pop up message asks if you want to **Add BeyondTrust Workforce Passwords?**. Click **Add**.
4. A pop up message displays confirming the extension has been added. Click **Okay**.

5. To add the **BeyondTrust Workforce Passwords** icon to the toolbar:
    - Click the **Extensions** icon in the toolbar.
    - Click the gear box icon next to the **BeyondTrust Workforce Passwords** extension.
    - Select the **Pin to Toolbar** menu option.


Extensions
BeyondTrust Workforce Passwords
Manage extension
Extension Can't Read and Change Data
Pin to Toolbar
Manage Extension
Manage

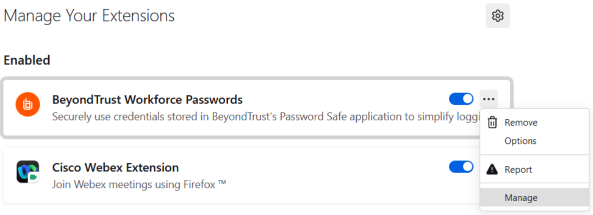
6. The **BeyondTrust Workforce Passwords** icon displays in the toolbar.



> ***Note:*** *For version 23.3.0.2 of the Workforce Passwords browser extension and for Firefox browsers only, you must enable the* ***Access your data for all websites*** *permission for the extension before logging in to it. The steps for enabling this permission are detailed below. In future releases of the browser extension, you'll receive a prompt to enable this permission, alleviating the need to manually set it.*

Enable the required permission for the extension as follows:

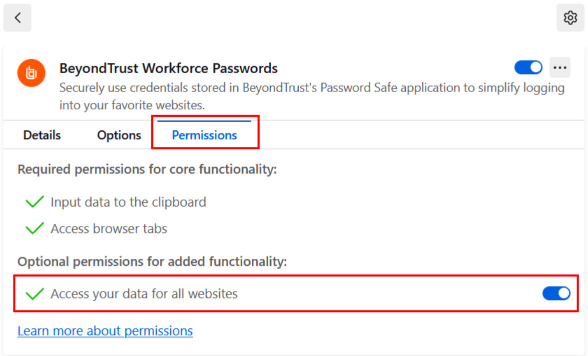
1. In your browser, click the **Extensions** icon in the toolbar, and then select **Manage extensions**.
2. Click the ellipsis button for the BeyondTrust Workforce Passwords extension.
3. Select **Manage** from the drop-down menu.



Securely use credentials stored in BeyondTrust's Password Safe application to simplify loggi

Join Webex meetings using Firefox ™

4. Click the **Permissions** tab.
5. Click the toggle to enable the **Access your data for all websites** permission.
6. Refresh the browser to log in to the Workforce Passwords extension.



Securely use credentials stored in BeyondTrust's Password Safe application to simplify logging into your favorite websites.

Required permissions for core functionality:

✓ Input data to the clipboard

✓ Access browser tabs

Optional permissions for added functionality:

✓ Access your data for all websites

Log In to the Browser Extension

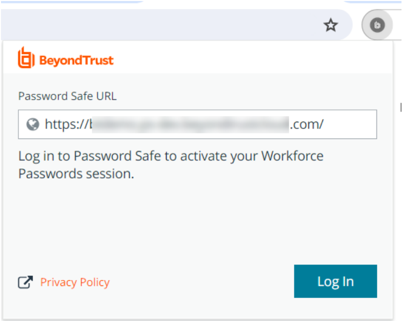
The following steps are based on the Chrome browser extension. Similar steps are used for the Edge and Firefox browser extensions.

You must authenticate through BeyondInsight to use Workforce Passwords. To do so, click the Workforce Passwords extension icon located in the toolbar, ensure you have input your Password Safe URL, and then use one of the following methods:

- Use the **Login** button to launch the BeyondInsight login screen and input your credentials.
- If an active authenticated BeyondInsight session is running that matches your Password Safe URL input, a **Use Active Session** button displays. Click the **Use Active Session** button to begin your Workforce Passwords session as that BeyondInsight user.

To log in to the Workforce Passwords browser extension:

1. In your browser, click the gray **BeyondTrust Workforce Passwords** icon in the toolbar.
2. If only a **Log In** button is available, enter the Password Safe URL and then click **Log In**.

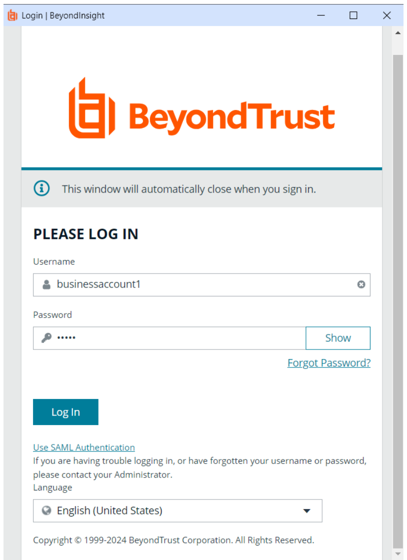


Password Safe URL

https://l[redacted].com/

Log in to Password Safe to activate your Workforce Passwords session.

3. The standard log in screen for BeyondInsight and Password Safe displays. Enter the credentials provided by your administrator and then click **Log In**.This authenticates you to the site where your Workforce Passwords secrets are stored.



This window will automatically close when you sign in.

PLEASE LOG IN

Username: businessaccount1

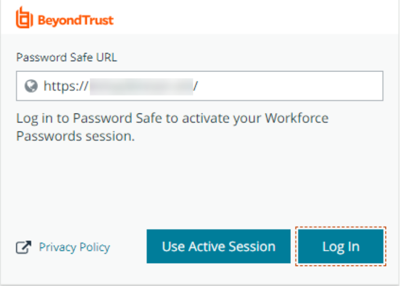
Password: •••••

If you are having trouble logging in, or have forgotten your username or password, please contact your Administrator.

Language: English (United States)

Copyright © 1999-2024 BeyondTrust Corporation. All Rights Reserved.

4. If the **Use Active Session** button is available, click it to use the credentials from that session to sign you in to Workforce Passwords. You can also use the **Login** button from this dialog to use different login credentials.



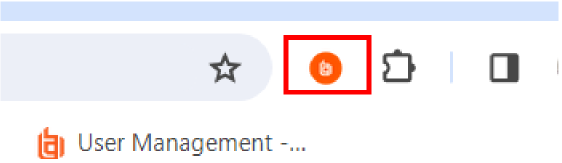
Password Safe URL

https://[redacted]/

Log in to Password Safe to activate your Workforce Passwords session.

> ***Note:*** *Ensure the Password Safe URL matches the SAML redirect URL; otherwise, the Workforce Passwords login does not work.*

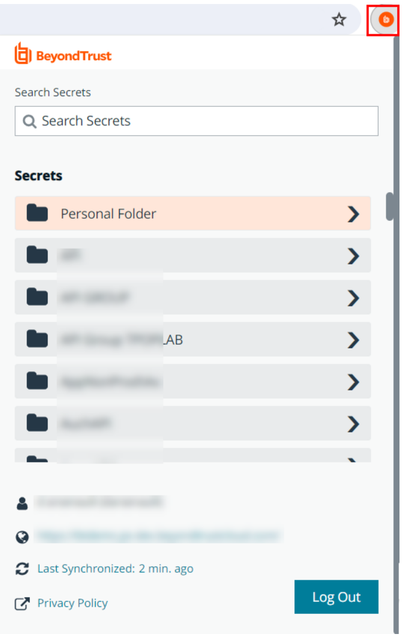
5. Upon successful log in, the Workforce Passwords browser extension icon in the toolbar changes from gray to orange.



Use the Browser Extension

Once the browser extension has been enabled and you have logged in to it, you can log into websites using your saved Workforce Passwords secrets.

1. Click the orange **BeyondTrust Workforce Passwords** icon in the toolbar.
2. Click the **Personal Folder**.



Search Secrets

Search Secrets

Secrets

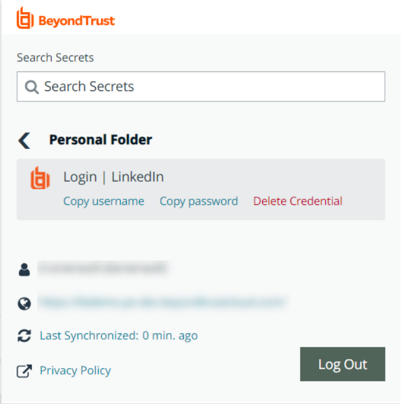
- Personal Folder
- [redacted]
- [redacted]
- [redacted]LAB
- [redacted]
- [redacted]

[redacted]

[redacted]

Last Synchronized: 2 min. ago

3. Click the link for the credentialed site you want to access. You can also search for a secret using the **Search Secret** field.



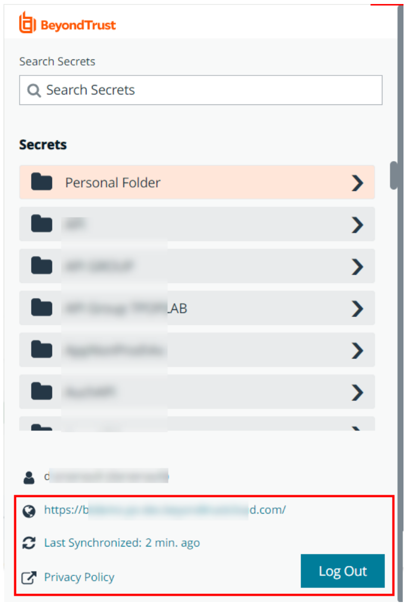
4. You are redirected to the URL saved to that credential.
   - If one secret is saved with that URL, credentials are auto-injected.
   - If more than one secret is saved with that URL, select the appropriate credentials in the log in screen.
   - You can also copy and paste usernames and passwords into the log in screen using the **Copy username** and **Copy password** links available when accessing the credentialed site in the browser extension pop-out dialog.
5. Once credentials are entered in the log in screen, click the **Log In** button to sign you in to your account associated with that URL.

Additional Options

At the bottom of the browser extension Secrets pop-out dialog, you can also:

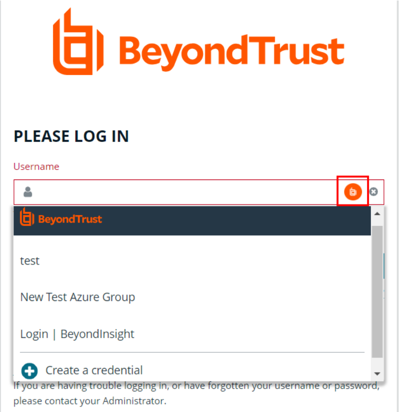
- Synchronize to the most recently saved credentials by clicking the **Last Synchronized <minutes> ago** link.
- Go to the most recently logged in instance of a session by clicking the instance link.
- Log out of the Workforce Passwords session.

> ***Note:*** *Automatic synchronization occurs only when logging in with the browser extension. If a new secret is created, trigger a manual sync by clicking the **Last Synchronized <minutes> ago** link. If the link is not working, ensure you are running the latest version of the internet browser. If yes, log out of the Workforce Passwords browser extension and log back in.*



Inline Log In

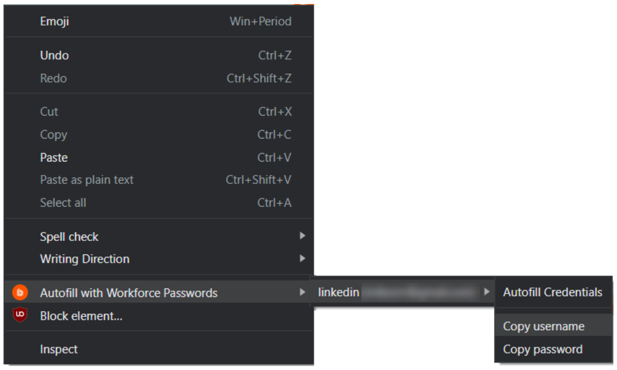
If you navigate to a website and have one or more valid credentials for that site, the orange BeyondTrust logo is embedded inline in the form field. Click the logo to bring up a list of available credentials to chose from. You also have the ability to create a new credential from here.



If you are having trouble logging in, or have forgotten your username or password, please contact your Administrator.

Click Form Field for Menu

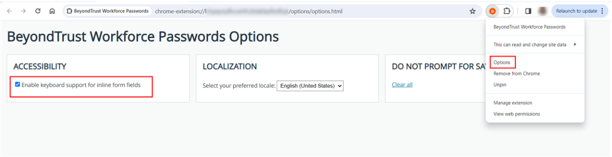
You can right-click on the form field to display a Workforce Passwords menu with different options, including **Autofill with Workforce Passwords**. From here you can autofill your credentials, or copy and paste username and password.



Enable Keyboard Accessibility

Keyboard accessibility is turned off by default. Enabling keyboard accessibility allows you to access the orange BeyondTrust logo located within form fields using your keyboard. To enable keyboard accessibility:

1. Right-click the **Workforce Passwords** icon in the toolbar.
2. Select **Options**. The **BeyondTrust Workforce Passwords Options** dialog displays.
3. Check **Enable keyboard support for inline form fields**.


BeyondTrust Workforce Passwords
chrome-extension://[redacted]/options/options.html
Relaunch to update
BeyondTrust Workforce Passwords Options
ACCESSIBILITY
LOCALIZATION
DO NOT PROMPT FOR SA
Clear all
BeyondTrust Workforce Passwords
This can read and change site data
Options
Remove from Chrome
Unpin
Manage extension
View web permissions

☑ Enable keyboard support for inline form fields

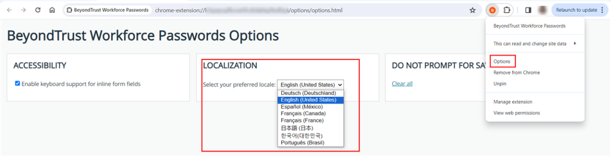
Select your preferred locale: English (United States)

Set Your Preferred Language

On launch, Workforce Passwords attempts to use the browser's chosen language. If that language is not supported, Workforce Passwords remains in English. You can change your preferred language in several different ways.

To see available languages and make a change, set your preferred locale, as follows:

1. Right-click the **Workforce Passwords** icon in the toolbar.
2. Select **Options**. The **BeyondTrust Workforce Passwords Options** dialog displays.
3. Under **Localization**, select your language from the dropdown.


BeyondTrust Workforce Passwords
chrome-extension://[redacted]/options/options.html
Relaunch to update

BeyondTrust Workforce Passwords Options

ACCESSIBILITY

☑ Enable keyboard support for inline form fields

LOCALIZATION

Select your preferred locale: English (United States)

Deutsch (Deutschland)
English (United States)
Español (México)
Français (Canada)
Français (France)
日本語 (日本)
한국어(대한민국)
Português (Brasil)

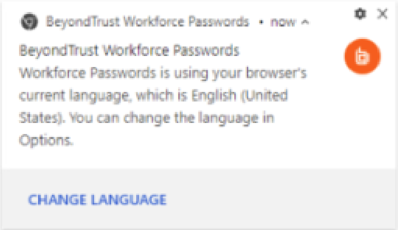
DO NOT PROMPT FOR SA

Clear all

BeyondTrust Workforce Passwords
This can read and change site data
Options
Remove from Chrome
Unpin
Manage extension
View web permissions

You can change your language in Chrome and Edge upon successful install of Workforce Passwords, as follows:

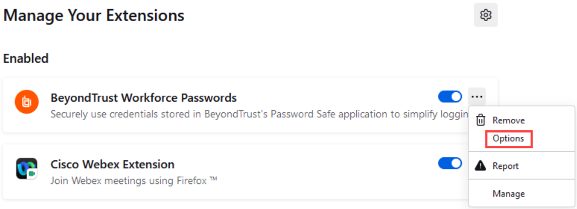
1. Click the **Extensions** icon in the browser toolbar.
2. Select **Manage Extensions**.
3. Click the **Change Language** button in the notification displayed on the bottom left of the screen.


BeyondTrust Workforce Passwords • now

BeyondTrust Workforce Passwords
Workforce Passwords is using your browser's current language, which is English (United States). You can change the language in Options.

You can change your language in Firefox upon successful install of Workforce Passwords, as follows:

1. Click the **Extensions** icon in the browser toolbar.
2. Select **Manage Extensions**.
3. Click the ellipsis to the right of the Workforce Passwords extension.
4. Select **Options**.


Manage Your Extensions

Enabled

BeyondTrust Workforce Passwords
Securely use credentials stored in BeyondTrust's Password Safe application to simplify loggin

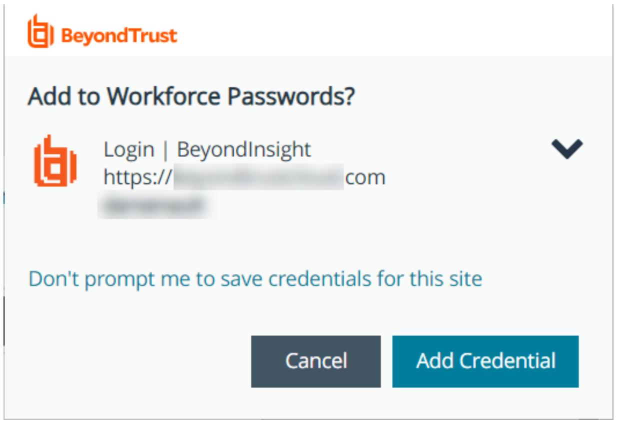
Cisco Webex Extension
Join Webex meetings using Firefox ™

Create, Update, or Delete Credentials Using the Browser Extension

Users with read/write access can create, update, or delete credentials using the Workforce Passwords Browser Extension.

Create Credential

If you enter credentials that aren't recognized by Workforce Passwords, you are prompted to either add the credential or cancel. Click on the down arrow to display all editable credential fields.



Add to Workforce Passwords?

Login | BeyondInsight
https://[redacted]com
[redacted]

Default values for these fields are pulled from the URL you want to log into. Editable fields are:

- **Title**
- **URL**

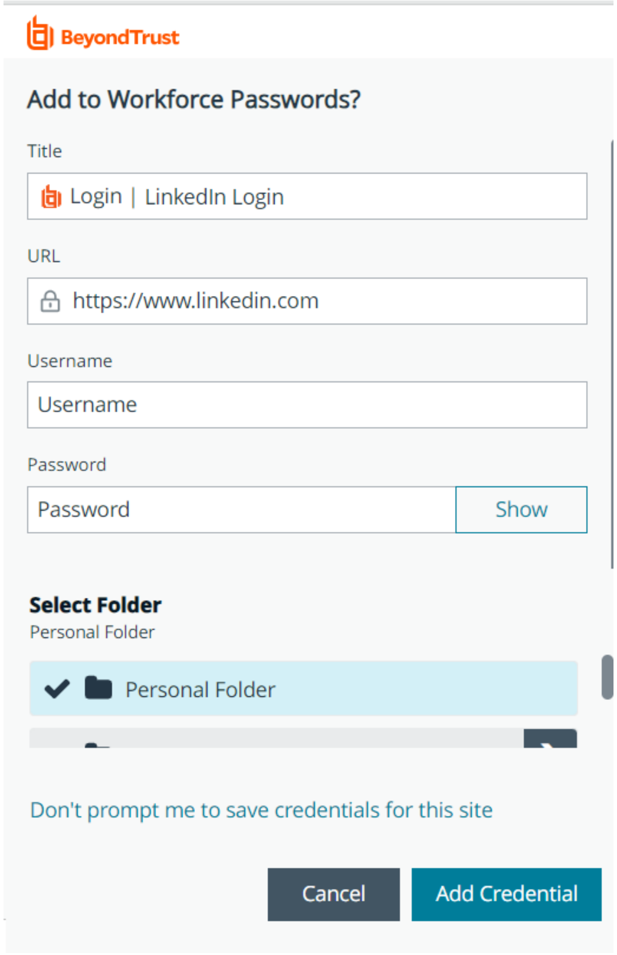
> ***Note:*** *A simple form of the URL for the site is stored by default. If the URL won't work without the parts that are trimmed off, the credential won't work by default. Edit the URL to include the full URL as required by the target site.*

- **Username**
- **Password**

You can also select which folder to save the credentials to. **Personal Folder** is selected by default.

Once all credential information has been added, click **Add Credential** to save it, or **Cancel** to ignore the updates.

When you return to that URL and click on the orange icon in the **Username** field, the new credentials are available.



Add to Workforce Passwords?

Title: Login | LinkedIn Login

URL: https://www.linkedin.com

Username: Username

Password: Password

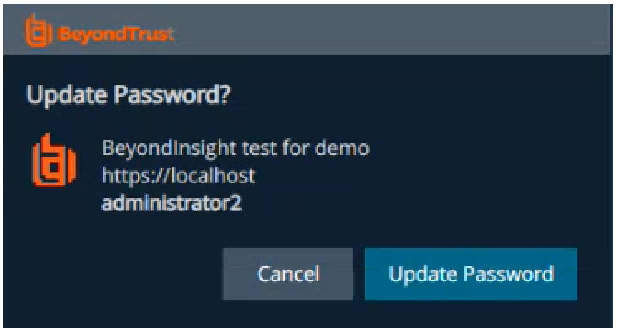
Select Folder
Personal Folder

✓ Personal Folder

> ***Tip:*** *Select* ***Don't prompt me to save credentials for this site*** *to disable the prompt asking to save credentials. You can reverse this action by clicking* ***Undo*** *on the dialog.*
>
> *To see a list of all sites with the save credentials prompt disabled, click on the orange icon next to the address bar and select* ***Options****. From here, you can remove that site from the list. It once again displays on the dialog.*

Update Credential

If you change a password for an already saved credential, you are prompted to update the password. Click **Update Password** or **Cancel** to cancel the update.



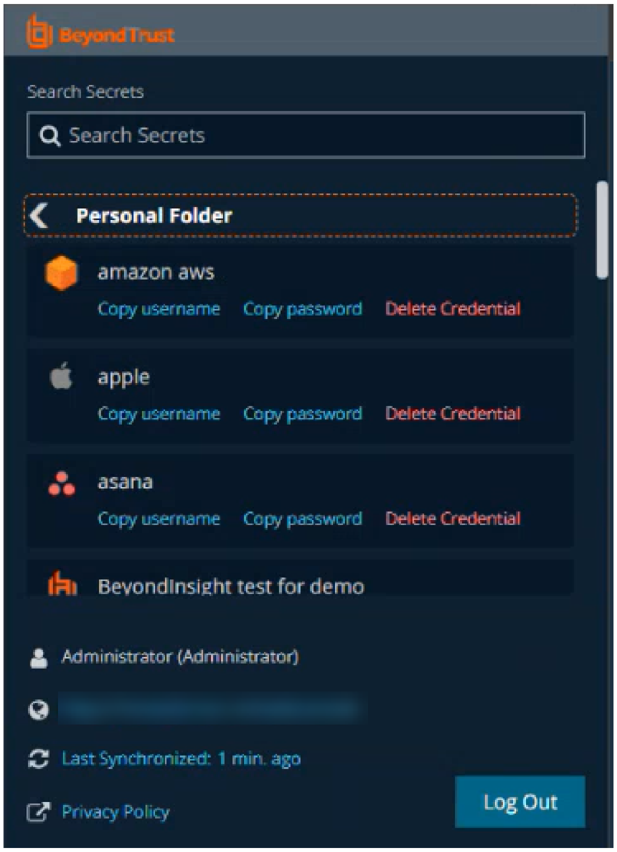
Update Password?

BeyondInsight test for demo
https://localhost
administrator2

Delete Credential

To delete credentials, click the orange icon in the toolbar, select the folder where the credentials are stored, select the credentials within that folder, and click **Delete Credential**. Confirm on the next dialog by clicking **Delete** or **Cancel**.

> ***Note:*** *Users with read-only access can delete credentials in their personal folder, but they cannot delete credentials from a shared folder if they are owned by another user.*



Search Secrets

Personal Folder

amazon aws

apple

asana

BeyondInsight test for demo

Administrator (Administrator)

[redacted]

Last Synchronized: 1 min. ago