BeyondTrust

Password Safe 22.2

User Guide

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

TC:8/11/2022

Table of Contents

Password Safe User Guide **4**
Select a Display Language 4
Log In to the Web Portal 4
Change Your Login Password 5
Reset a Forgotten Password 5
Navigate the Password Safe Web Portal **6**
Read the Accounts Grid 6
Use Quick Links 7
Request a Password from Password Safe **8**
Request a Password Release 8
Review a Password Request 8
Approve or Deny a Password Request 9
Retrieve a Password 9
Multi-System Checkout 9
Approve a Request for Multi-System Checkout 10
Use the OneClick Feature 10
Request SSH or RDP Sessions in Password Safe **11**
Request an RDP Session 11
SSH Direct Connect 11
RDP Direct Connect 12
Password Restrictions 13
Enforce Session End Time 13
Request Remote Proxy Session **14**
Password Safe Use Cases **16**
Request Access to a Linux Account - Password Retrieval 16
Request RDP Access to a Windows Account - Session Management 18
Request Access to a Microsoft SQL Account - Remote Applications 19
Use Team Passwords **22**
Create a Credential in Team Passwords 22
Manage Folders in Team Passwords 23
View and Copy a Credential in Team Passwords 24

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Edit and Delete a Credential in Team Passwords 25

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Password Safe User Guide

Password Safe includes a web-based interface for executing password requests and approvals. You can launch the Password Safe web portal by selecting **Password Safe** from the 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 U-Series Appliance and perform tasks. The specific tasks a user can perform are 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:** A pre-login banner might be configured on your system. You must click **OK** before you can enter your credentials.*

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Change Your Login Password

In the BeyondInsight Console, click the **Profile and preferences** button, and then click **Change Password**. Your password must be 6-117 characters in length.

> ***Note:*** *You cannot change your password if you are currently logging in with Active Directory or LDAP credentials, or if your account is currently logged out.*

Reset a Forgotten Password

If you forget your console password, click **Forgot Password** on the **Login** page. Enter your username and then click **Reset Password**.

You will receive an email from the console administrator. Click the reset link provided in the email.

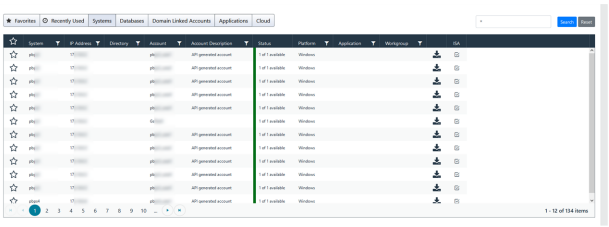
> ***Note:*** *You cannot reset your password if you are currently logging in with Active Directory or LDAP credentials, or if SMTP is improperly configured.*

> *For more information on configuring SMTP, please see Run the Configuration Wizard at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/install/install-software.htm#Run.*

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Navigate the Password Safe Web Portal

In the **Accounts** tab, click a tab to search for the account, system, or application you need to access.



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

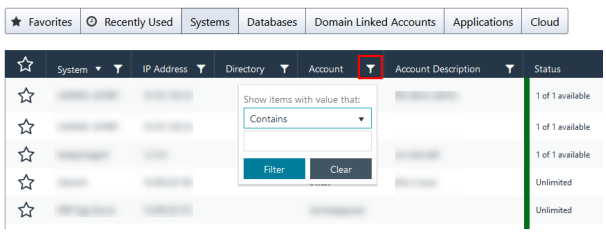
> ***Note:*** *When you first log in to the Password Safe web portal, no accounts are available in the* ***Favorites*** *tab.*

Read the Accounts Grid

You can rearrange the grid columns by clicking the title and dragging to the desired location. The following information is displayed in the grid:

Favorites	Click the star to add your most used accounts to your list of favorites. You can then select the **Favorites** tab to display only favorite accounts.
System	The system's name.
OneClick buttons	Click the OneClick buttons to access the OneClick feature. A grayed out button indicates that the account cannot be accessed using OneClick.
Directory	The directory name, if applicable.
Account	The username on the account.
Account Description	The description of the managed account provided when the account was set up.
Status	Indicates if the account is available. Green indicates the account is available. Red indicates it is unavailable.
Platform	The type of operating system.
Application	The application managed by Password Safe, if applicable.
Workgroup	The workgroup the account is tied to, if applicable.
Download RDP Direct Connect File buttons	Click the **Download RDP Direct Connect File** (down arrow) button to request an RDP Direct Connect session.

Each column title has its own search filter. From the dropdown, select **Contains**, **Starts With**, **Is Equal To**, or **Is Not Equal To**. Enter a search string, and then click **Filter**.



©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

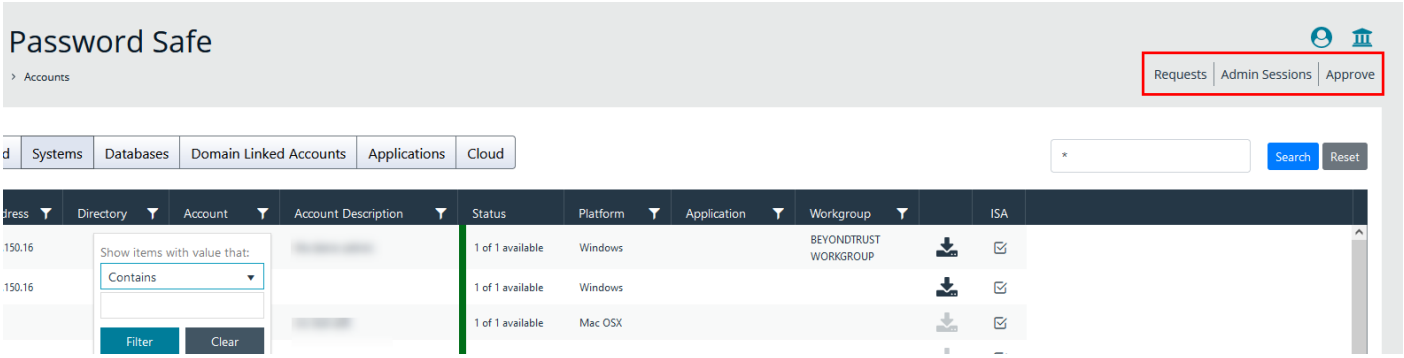
For more information, please see the following:

- *"Use the OneClick Feature" on page 10*
- *"SSH Direct Connect" on page 11*
- *"RDP Direct Connect" on page 12*

Use Quick Links

The Password Safe web portal uses quick links at the top of the page to navigate to different areas of the application.

The links displayed depend on your assigned Password Safe roles.



©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Request a Password from Password Safe

If you have a dual control configuration, the password release is a three-step process. Using dual control ensures the security of the system account password, provides accountability, and provides dual control over the managed accounts.

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 one of the following roles: **Requestor**, **Approver**, or **Requestor/Approver**.

Request a Password Release

1. Log in to the Password Safe web portal.
2. On the **Accounts** page, click the tab for the type of system or application you need to access.
3. Select the system from the list.
4. On the **Requests** page, set the following:
    - **Start Date:** Select the start date for the session that corresponds with the access policy.
    - **Start Time:** Select **Immediately** to release the password at the current time, or click the **Scheduling** button for a future release. For example, schedule a release to coincide with scheduled maintenance.
    - **Requested Duration:** Set the length of time that the password should be available.

      The default value is two hours. The maximum duration is 365 days. The default and maximum durations are set on the managed account.

    - **Access Request:** For the session type, select **Password**, **RDP Session**, **SSH**, or **Application Session**.
    - **Reason:** Enter a reason for the request. The maximum allowed length is 200 characters.
    - **Ticket System:** Select a ticket system from the list. Ticket systems can be used for cross-reference.
    - **Ticket Number:** Enter a ticket number.

***Note: Reason**, **Ticket System**, and **Ticket Number** fields may or may not be 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.*

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

Review a Password Request

You can review password requests on the **Requests** page. The list of requests available for review depends on your role. You can review the requests on systems where you are a requester.

1. On the **Requests** page, click the buttons to view all, active, and pending requests.
2. Use the filter setting available on each header to narrow the search. Enter filter criteria in the box.

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Approve or Deny a Password Request

When a password request for a system is properly submitted, the associated approvers for that system are notified by email of the pending request. Using the following procedure, an approver can approve or deny the password request:

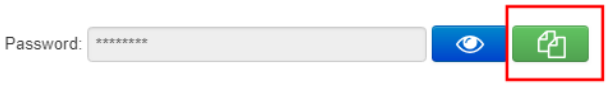
1. Log in to to the Password Safe Web Portal.
2. Select **Approve** and click **Pending**.
3. Click on a pending request.
4. Enter a comment for the approval.
5. Select **Approve** or **Deny**.

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

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. The password displays in a separate window. The visibility of the password may be limited, with a timer showing remaining time. The dialog box can be closed before the timeout.
3. To copy the password to the clipboard, click the **Copy** button.
4. Use the password to log in to the system within the password release time period.



Multi-System Checkout

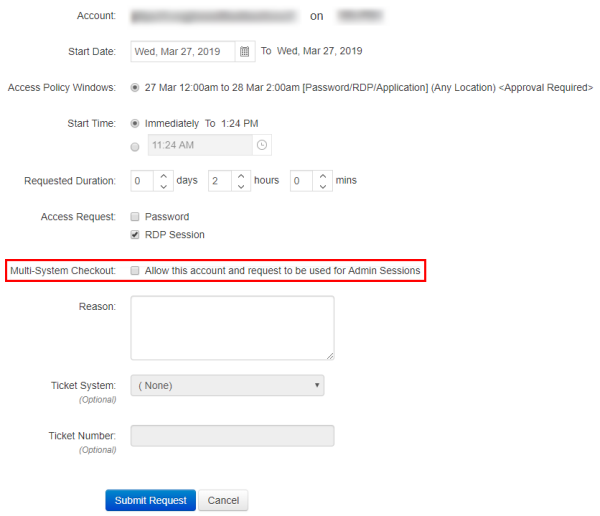
Managed systems can be linked to Active Directory accounts. You can submit a request to these Active Directory accounts and then access the managed systems linked to that account.

> ***Note:*** *Your Password Safe administrator must configure the correct permissions for the managed system to use this feature.*

1. Log in to the Password Safe web portal.
2. Click **Menu**, then select **Accounts**.
3. Click the **Domain Linked Accounts** tab for the system type you need to access.
4. Select the account from the list.

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

5. On the **Requests** page, set the following:



   - **Start Date:** Select the start date for the session that corresponds with the access policy.
   - **Start Time:** Select **Immediately** to release the password at the current time, , or use the scheduling option to schedule the password release for another time. For example, schedule a release to coincide with scheduled maintenance.
   - **Requested Duration:** Set the length of time the password should be available.

     The default value is two hours. The maximum duration is 365 days. The default and maximum durations are set on the managed account by your Password Safe administrator.

   - **Access Request:** Select the type of access: **Password**, **RDP Session**, **SSH**, or **Application Session**.

> ***Note:*** *The available options will vary depending on the account selected.*

   - **Multi-System Checkout:** Select this option to use this account and request for **Admin Sessions**. This option is displayed only if the requestor has permissions to use this feature.
   - **Reason:** Enter a reason for the request. By default, this field is required, but it can be disabled through BeyondInsight options. The maximum allowed length is 200 characters.
   - **Ticket System:** (optional) Select a ticket system from the list. Ticket systems can be used for cross-reference.
   - **Ticket Number:** (optional) Enter a ticket number.
6. Click **Submit Request**. An email is sent to the approver if email notification is configured.

Approve a Request for Multi-System Checkout

If the request is approved either automatically or by an approver, the account is available on the **Admin Sessions** page for the duration of the request for which it was approved.

1. On the **Admin Sessions** page, select an account from the **Available Accounts** list.
2. The **Asset/IP** list populates with managed systems that are tied to the account.
3. Select an asset from the **Asset** menu.
4. Once a request is approved, the requestor can then choose to open the session with any computer linked to the approved account regardless of whether or not it was included in the initial request.
5. Click **Connect** to start the RDP or SSH session.

Use the OneClick Feature

A requestor sees the **OneClick (thunderbolt)** button when they log in to Password Safe to make a request. When they open **OneClick**, any access policies that are configured with auto-approve are checked for availability. Clicking the button allows the requestor to choose the duration of the request and connect immediately, as long as they have entered a request which meets the criteria of the access policy. Comprehensive messages are displayed to the requestor if their requests do not meet the requirements configured in the access policy.

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Request SSH or RDP 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 SSH or RDP connection types.

Password Safe acts as a proxy, providing session management to target systems. No passwords are transmitted, allowing inherently secure session management.

Request an RDP Session

1. Log in to the Password Safe web portal.
2. On the **Accounts** page, click the tab for the type of system or application you need to access.
3. Select the account from the list.
4. On the **Requests** page, set the following:
    - **Start Date:** Select the start date for the session that corresponds with the access policy.
    - **Start Time:** Select **Immediately** to start the session at the current time, or click the **Scheduling** button for a future session.
    - **Requested Duration:** Set the length of time that the session should be available. The maximum duration is 365 days. The default and maximum durations are set on the managed account.
    - **Access Request:** Select the session type of **RDP Session**.
    - **RDP Admin Console:** If an administrator has enabled this option in the access policy, you can request a remote session in console mode (mstsc /admin). This can be useful if the number of remote sessions is maxed out on the host. An RDP console session allows you to connect without requiring other sessions to disconnect. Running a console session disables certain services and functionality, such as but not limited to:
        - Remote Desktop Services client access licensing
        - Time zone redirection
        - Remote Desktop Connection broker redirection
        - Remote Desktop easy print
    - **Reason:** Enter a reason for the request. By default, this field is required, but it can be disabled through BeyondInsight options. The maximum allowed length is 200 characters.
    - **Ticket System:** (optional) Select a ticket system and enter the ticket number. Ticket systems can be used for cross-reference.

> *For more information on **mstsc /admin**, please see mstsc at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/mstsc.*

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

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.

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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.

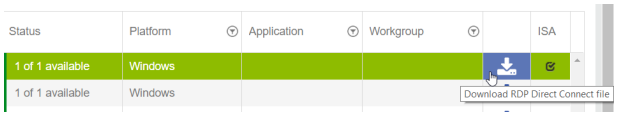
RDP Direct Connect

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

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 use RDP 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.

1. Log in to the Password Safe web portal.
2. On the **Accounts** page, click the tab for the type of system or application you need to access.
3. Find the account in the list.
4. Click the download arrow.
5. Run the file to establish a connection to the target system.
6. Enter your password that you use to authenticate into Password Safe



©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

> **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.*

Password Restrictions

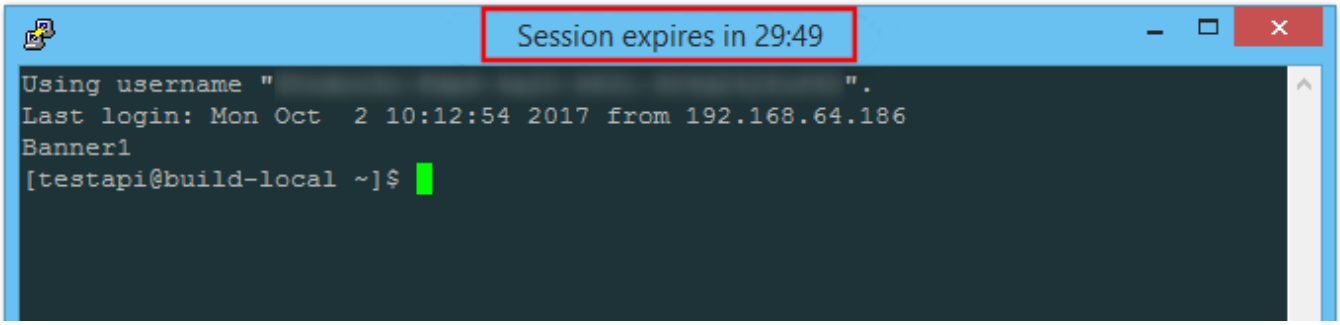
- On Windows 2008 and Windows 7, the password cannot exceed 81 characters. If a password is too long, the user cannot log in with the selected account.
- On Windows 2012, the password cannot exceed 127 characters. If a password is too long, the user cannot log in with the selected account.

Enforce Session End Time

When a Password Safe administrator creates an access policy, they assign a time frame that permits access to the asset. As part of that policy, the administrator can enforce the end of the session and close the session when the time expires. Sessions display a counter showing when the session will end.

RDP Session

SSH Session



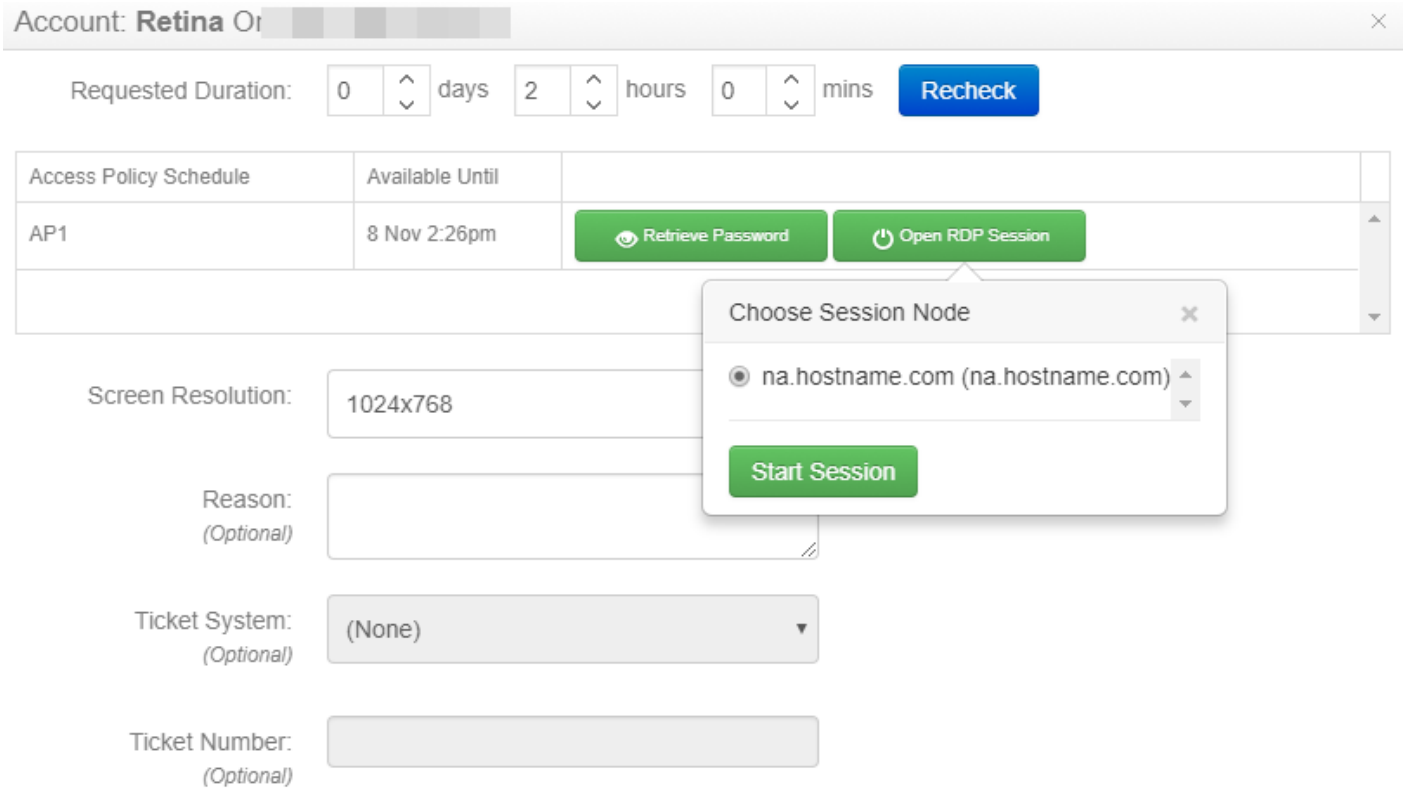
©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Request Remote Proxy Session

In larger environments, assets you need to access might not be in your region. If configured by your Password Safe administrator, you can select a node associated with another region to proxy these session types:

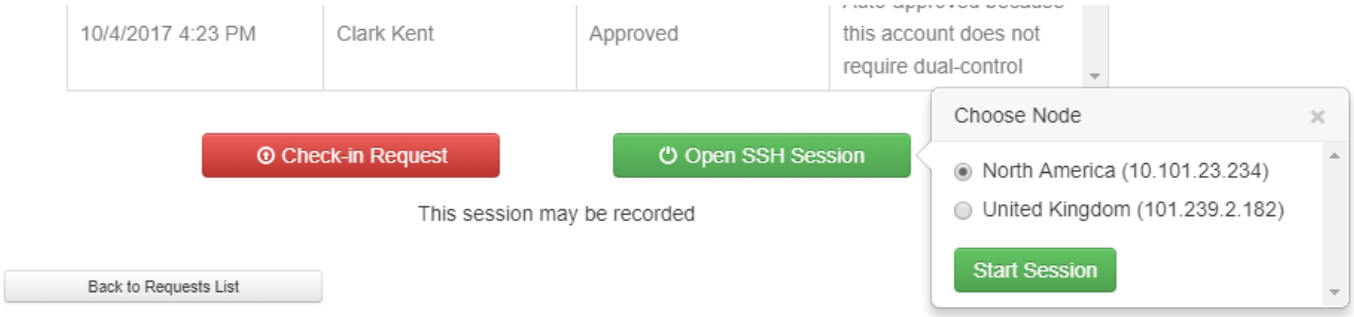
- Direct Connect sessions
- SSH sessions
- RDP sessions
- Admin sessions

When using OneClick to request a session, click **Open RDP Session**, and then select a node from the list:



©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

When requesting a session as a requestor, click **Open SSH Session**, and then select a node from the list:



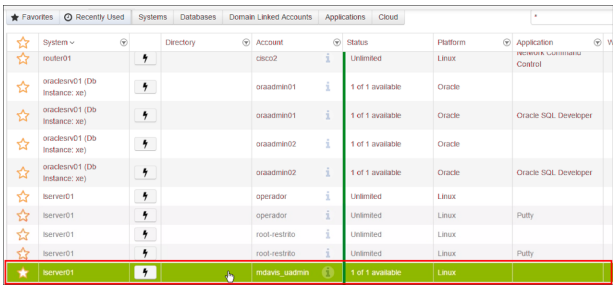
©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Password Safe Use Cases

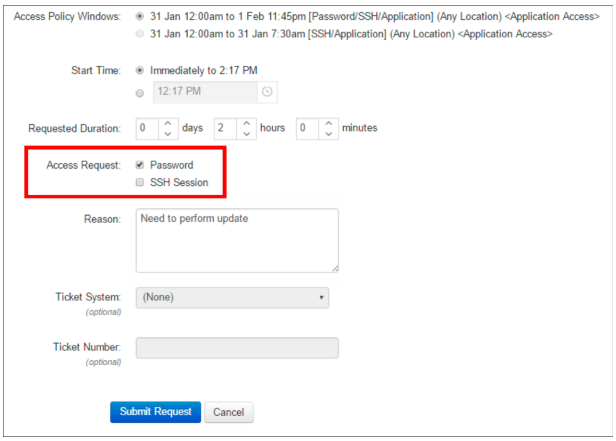
Request Access to a Linux Account - Password Retrieval

In this use case, you log in to the web portal and request access to a privileged account password. The system gives you access to the password after verifying in the policy that you are authorized and do not require approval. If you request the password again, the process repeats. However, you will see that every time, Password Safe gives you a different and unique password to allow proper usage tracking.

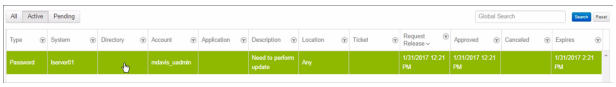
1. Log in to the web portal.
2. Scroll to the system **lserver01**, find the **mdavis_uadmin** account, and click to open.



3. Enter a date, time, and duration.
4. Select the **Password** check box and enter a reason for the request.
5. Click **Submit Request**.

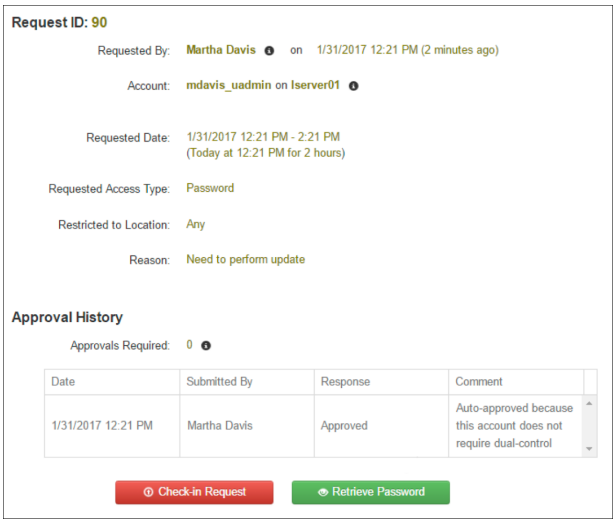


6. Depending on your access policy, the request may be auto-approved. If so, you should have an active request immediately available. Otherwise, wait for approval.
7. Select the active request.

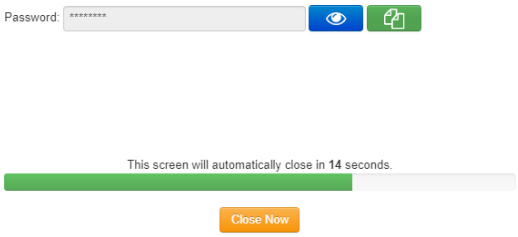


©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

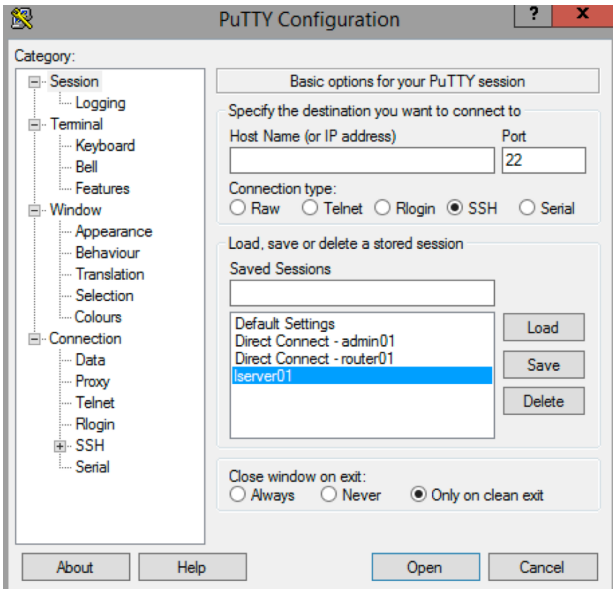
8. Click **Retrieve Password**.



9. Click the blue reveal password button to view the password, or click the green clipboard button to copy the password.



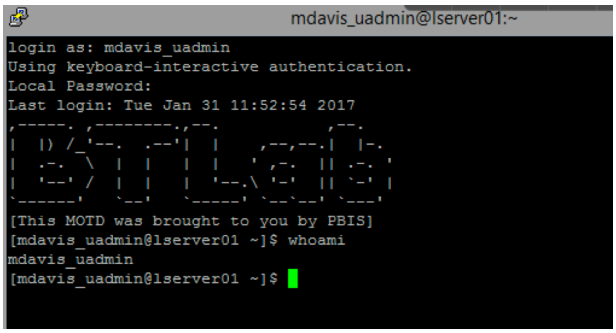
10. Open **PuTTY** on the BeyondInsight host, and open a connection to the **lserver01** host.



©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

11. Log in to **lserver01** as **mdavis_uadmin** and right-click to paste the password from the clipboard. You will be logged in directly.

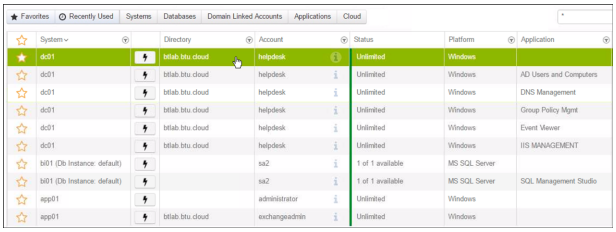
12. When finished, close the SSH session, and click the **Check-in Request** to release the **mdavis_uadmin** account.



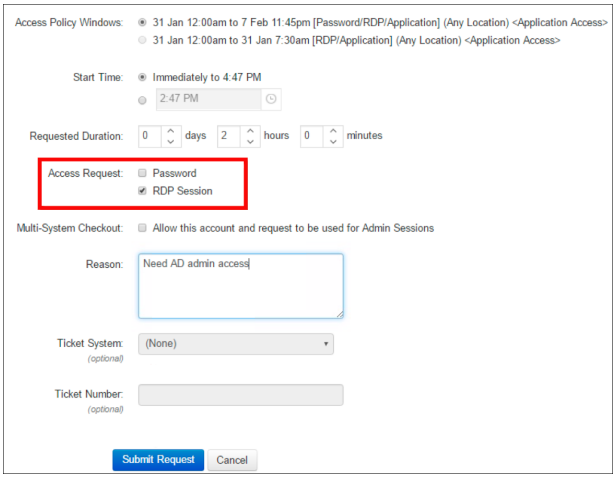
Request RDP Access to a Windows Account - Session Management

In this use case, you log in to the web portal and request access to a privileged account. You choose RDP to provide a proxy session, allowing you to access the account without requiring direct password retrieval.

1. Log in to the web portal.
2. Scroll to the system **dc01** and find the **helpdesk** account that does not have an application configured, then click to open.

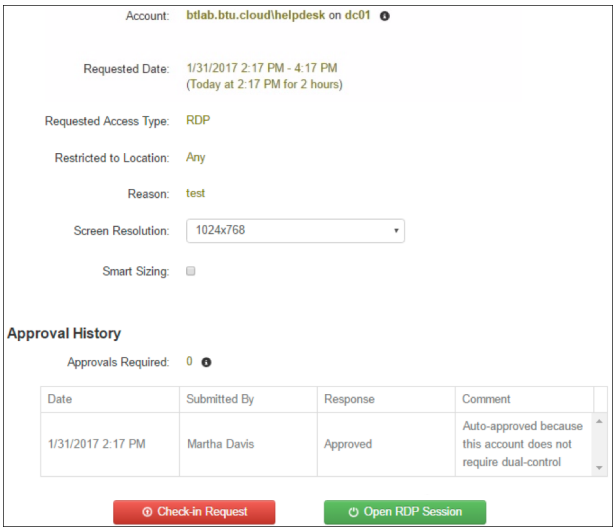


3. Enter a date, time, and duration.
4. Check the **RDP Session** box and enter a reason for the request.
5. Click **Submit Request**.
6. Depending on your access policy, the request may be auto-approved. If so, you should have an active request immediately available. Otherwise, wait for approval.
7. Select the active request.

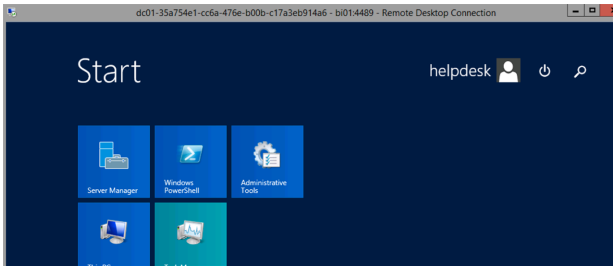


©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

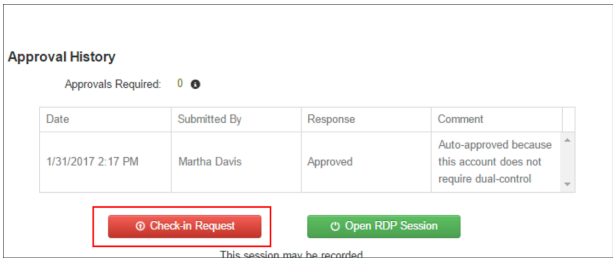
8. Select a **Screen Resolution**.
9. Click **Open RDP Session** to download an RDP connection file.



10. Run the file to directly access **dc01** as the helpdesk account, using Password Safe as a proxy.



11. When finished, close the RDP window and click **Check-in Request** to release the helpdesk account.

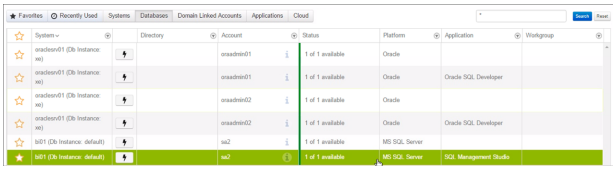


> ***Note:*** *The session terminates when you click on* ***Check-in Request****, even if you leave the RDP session open.*

Request Access to a Microsoft SQL Account - Remote Applications

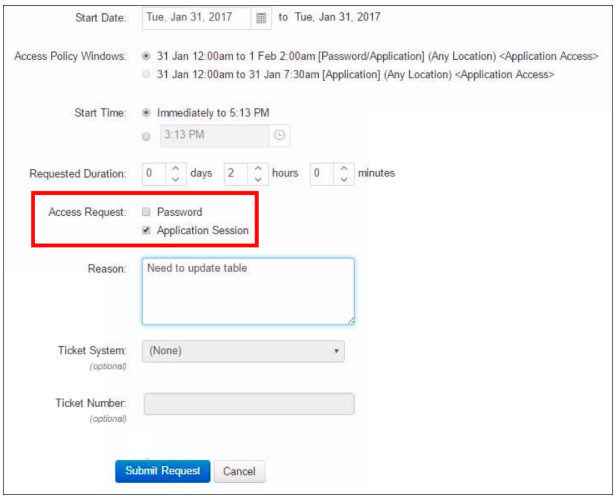
In this use case, you request access to a Microsoft SQL Server. However, you need the SQL Server privileged account just to access Microsoft SQL Server Management Studio. You do not need the password or a full RDP session.

1. Log in to the web portal.
2. Click the **Databases** tab.
3. Scroll to the system **bi01**, find the **sa2** account associated with **SQL Management Studio**, and click to open.

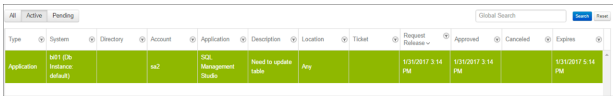


©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

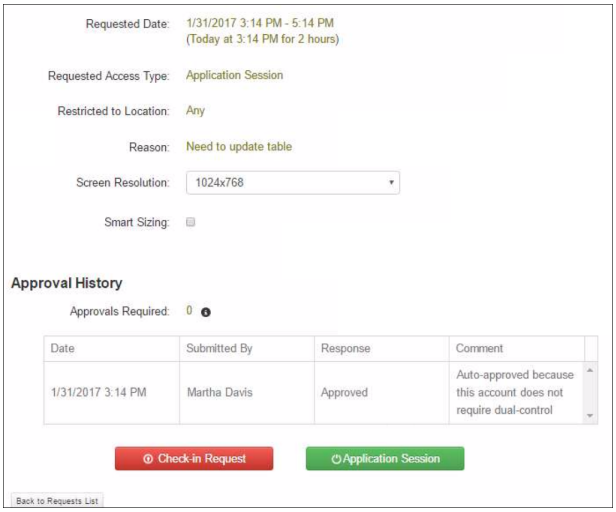
4. Enter a date, time, and duration.
5. Select the **Application Session** check box and enter a reason for the request.
6. Click **Submit Request**.



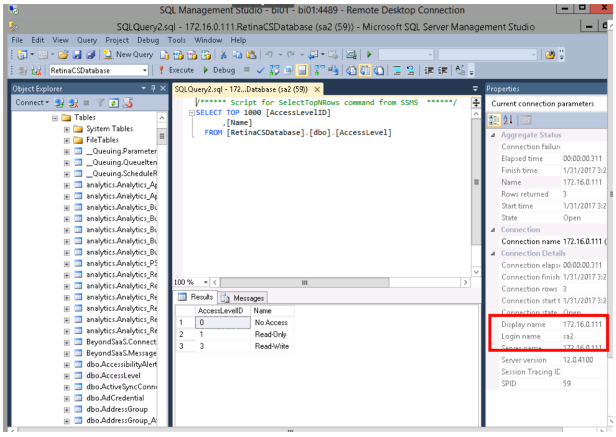
7. Depending on your access policy, the request may be auto-approved. If so, you should have an active request immediately available. Otherwise, wait for approval.
8. Select the active request.



9. Select a **Screen Resolution**.
10. Click **Application Session** to download an RDP connection file.



11. Run the file to connect to the **bi01** host, with your connection limited to using SQL Server Management Studio only.
12. When finished, close the application session, and click the **Check-in Request** to release the **sa2** account.



©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Tip: *Delegating access based on applications allows you to restrict what certain users can do in your environment. For instance, instead of granting a semi-skilled user a full session to a critical server, you may want to delegate access only to the applications they need to do their job. This helps to avoid incidents caused by someone restarting or deleting something in error.*

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

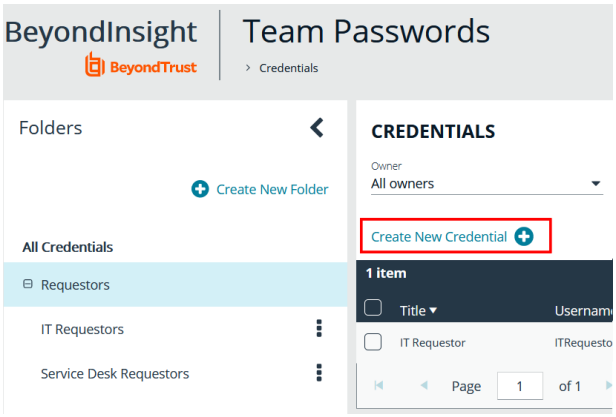
Use Team Passwords

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

Create a Credential in Team Passwords

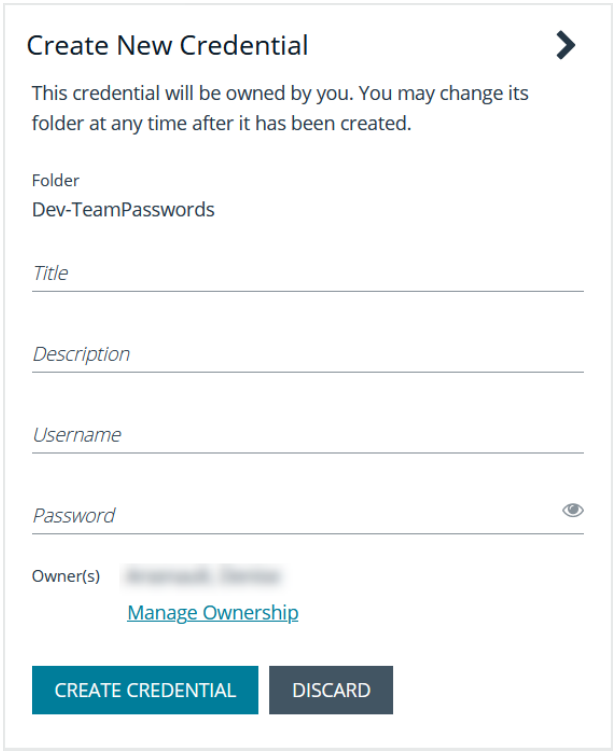
You can create credentials in the parent folder for any of your teams or in any of your team's subfolders. The user who creates the credential is its owner and may change its folder at any time after it has been created.

1. From the left navigation pane in the console, select **Team Passwords**.
2. From the **Folders** pane, select a folder, and then click **Create New Credential**.



©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

3. In the **Create New Credential** pane:
    - Enter a **Title**, **Description**, **Username**, and **Password**.
    - Click **Manage Ownership** if you wish to assign ownership to individual team members or to the entire team.
    - Click **Create Credential**.



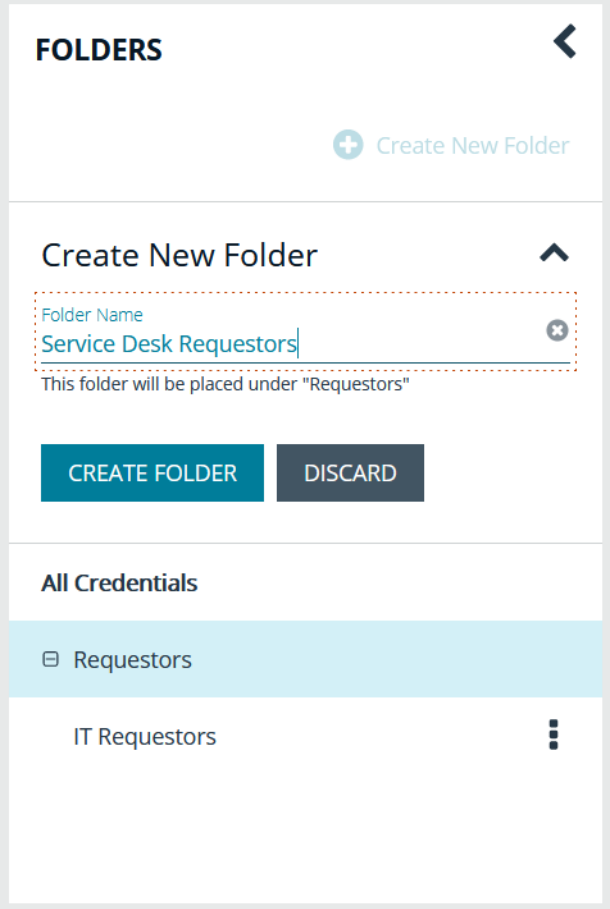
Manage Folders in Team Passwords

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

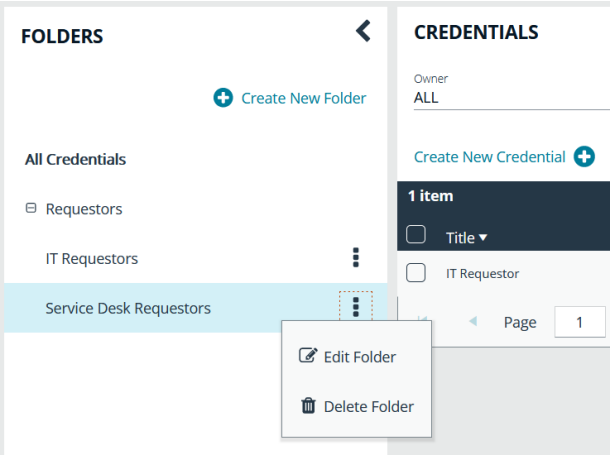
1. From the left navigation pane in the console, select **Team Passwords**.

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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



4. The new folder is listed under the folder you selected when creating it. To edit the folder name or to delete the folder, select the folder, click the vertical ellipsis, and then select **Edit Folder** or **Delete Folder**.



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

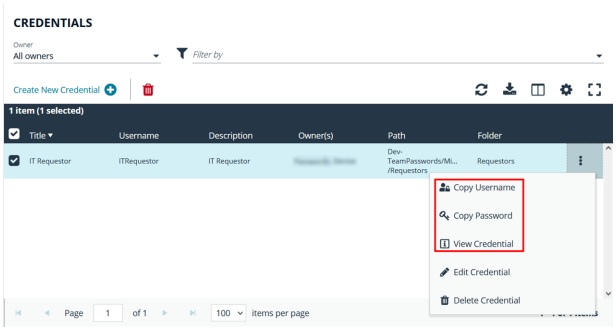
> *For more information on how to move a credential to a new subfolder, please see "Edit and Delete a Credential in Team Passwords" on page 25.*

View and Copy a Credential in Team Passwords

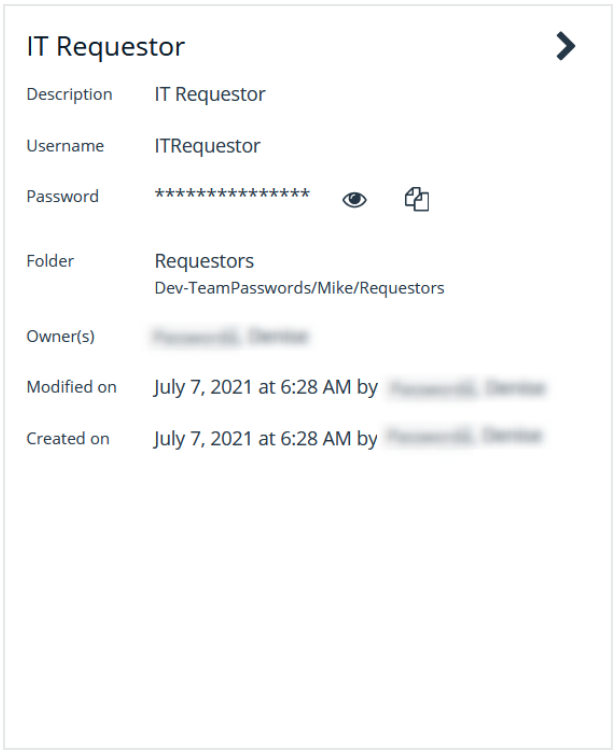
You can view details for your team's credentials, such as who owns the credential, when the credential was created and modified, and the folder path for the credential. You can also copy the username and password for a team credential so you may use it.

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

1. From the left navigation pane in the console, select **Team Passwords**.
2. From the **Folders** pane, select a folder, and then select a credential.
3. Click the vertical ellipsis for the credential.
4. To quickly copy the username and password, select those options from the dropdown menu.
5. To view the details for the credential, select **View Credential** from the dropdown menu.



6. To view the credential password, click the eye icon in the credential details pane.
7. To copy the credential password , click the copy icon in the credential details pane.



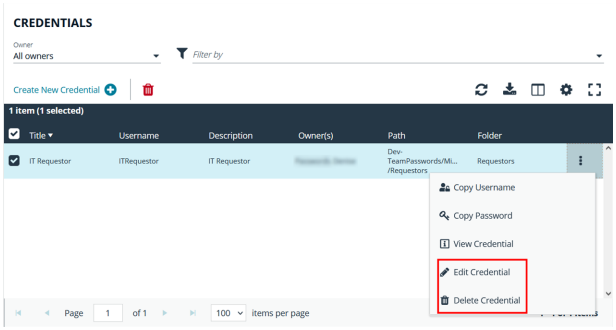
Edit and Delete a Credential in Team Passwords

Credential owners can edit the properties and manage ownership for credentials they own, as well as delete credentials they own. Password Safe Administrators can edit the properties, manage ownership, and delete all credentials in Team Passwords.

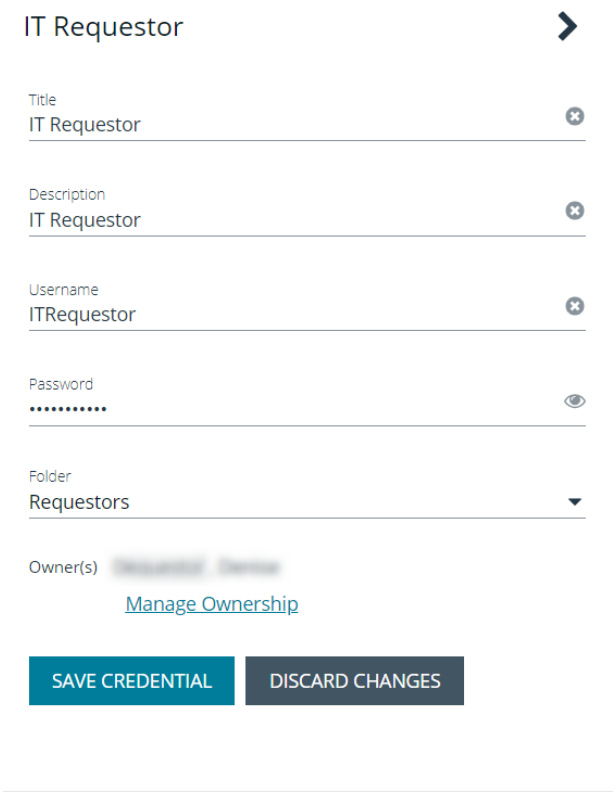
1. From the left navigation pane in the console, select **Team Passwords**.
2. From the **Folders** pane, select a folder, and then select a credential.
3. Click the vertical ellipsis for the credential.

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

4. To delete a credential, select **Delete Credential**, and then click **Delete** on the confirmation message.
5. To edit a credential, select **Edit Credential**.

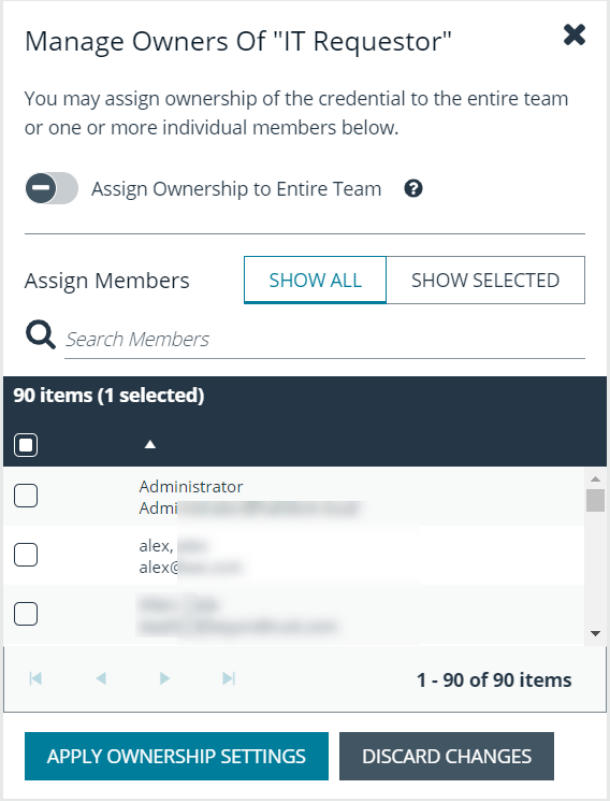


6. Modify the **Title**, **Description**, **Username**, **Password**, and **Folder** for the credential as required.
7. To manage the ownership of the credential, click **Manage Ownership**.



©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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



8. Click **Save Credential** once you have made your edits.

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.