BeyondTrust

Password Safe
User Guide 6.10

TC:2/7/2020

Table of Contents

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.

A Password Safe user is authorized to log into the Password Safe 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:

- English (US)
- German
- Spanish (LA)
- French (FR)
- French (CA)
- Korean
- Japanese
- Portuguese (BR)

You can select a language from the list on the **Login** page or by clicking the **Profile and preferences** button.

***Note:** By default, the **Language Settings** menu is not available. Your BeyondInsight administrator must enable it in the **Site Options**. If no languages are available, contact your BeyondInsight administrator.*

Log into 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, enter the RADIUS code and then click **Login**.
- **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.*

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.*

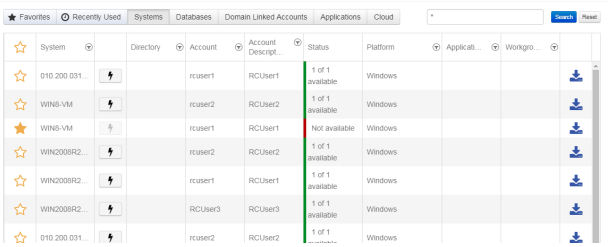
Reset a Forgotten Password

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.*

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 x 800 pixels.*

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

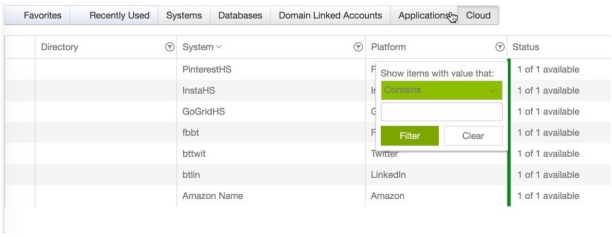
Read the Accounts Grid

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. For more information, please see "Use the OneClick Feature " on page 9
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. For more information, please see "SSH Direct Connect" on page 11, and "RDP Direct Connect" on page 11.

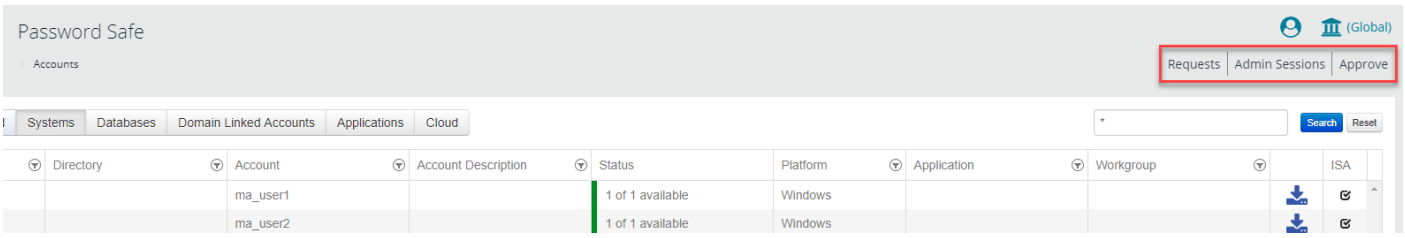
Each column title has its own search filter. From the dropdown, select **Contains**, **Starts With**, **Is Equal To**, or **Is Not Equal To**. Enter a search string, and then click **Filter**.



Use Quick Links

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

The links displayed depend on your assigned Password Safe roles.



Request a Password from Password Safe

If you are using 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 requestor requests a password release.
2. **Password approval:** An authorized approver reviews and approves the request for release.
3. **Password retrieval:** The authorized requestor 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. Click **Menu**, then select **Accounts**.
3. Click the tab for the account type you need to access.
4. Select the system from the list.
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 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. 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.

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 requestor.

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.

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 into 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 for a maximum of 20 seconds. The dialog box can be closed before the 20-second 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.

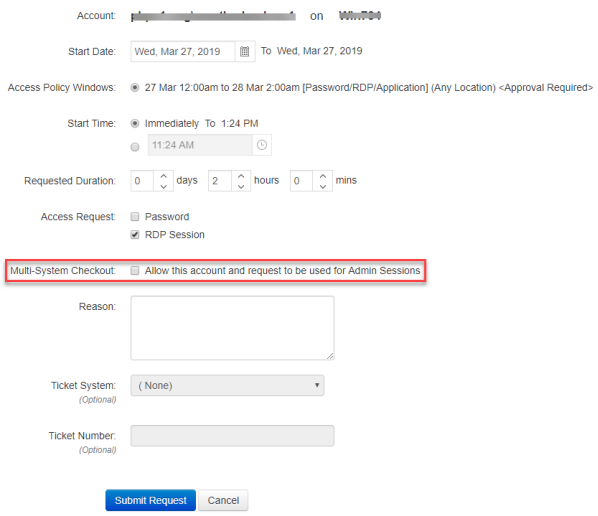
Multi-System Checkout

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.

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 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**.
   - **Multi-System Checkout:** Check this box to use this account and request for **Admin Sessions**. This check box will only be displayed on the request if the requestor has been assigned the **Write** permission for **Password Safe Admin Session** and the selected account is an active directory account.
   - **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 into 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.

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. Click **Menu**, then select **Accounts**.
3. Click the tab for the account type you need to access.
4. Select the account from the list.
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 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

      
      For more information, please see Microsoft documentation on using **mstsc /admin**.
    - **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.
6. Click **Submit Request**. An email is sent to the approver if email notification is configured.

SSH Direct Connect

SSH Direct Connect uses an SSH client to initiate a session to a target system. As the requestor, you can access the system without ever viewing the managed accounts credentials. To configure an application to connect to Password Safe, you must provide a connection string.

> ***Note:*** *Each application has its own unique string format.*

Once the application connects to Password Safe, you are prompted to enter your Password Safe login credentials. If successful, the connection is established.

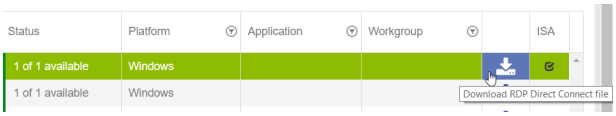
RDP Direct Connect

You can also use Direct Connect to initiate an RDP session. As the requestor, you can access the system without ever viewing the managed accounts 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. Click **Menu**, then select **Accounts**.
3. Click the tab for the account type you need to access.
4. Find the account in the list.
5. Click the download arrow.
6. Run the file to establish a connection to the target system.
7. Enter your password that you use to authenticate into Password Safe



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

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

Password Restrictions

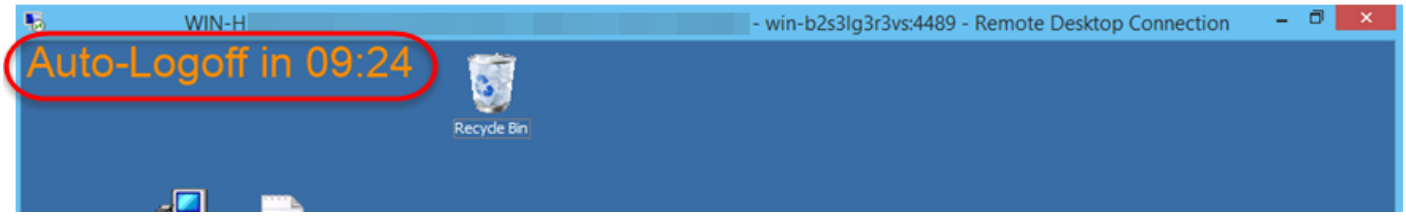
- On Windows 2008 and Windows 7, the password cannot exceed 81 characters. If a password is too long, the user cannot log in with the selected account.
- On Windows 2012, the password cannot exceed 127 characters. If a password is too long, the user cannot log in with the selected account.

Enforce Session End Time

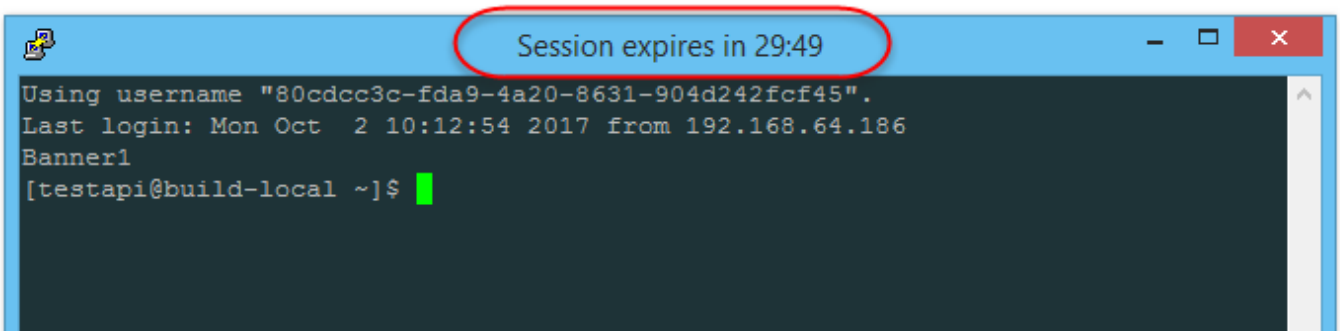
When a Password Safe administrator creates an access policy, they assign a time frame that permits access to the asset. As part of that policy, the administrator can enforce the end of the session and close the session when the time expires. Sessions display a

counter showing when the session will end.

RDP Session:



SSH Session:



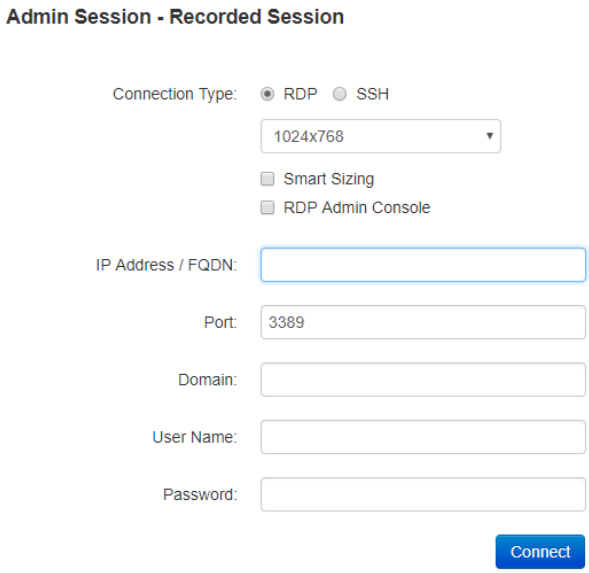
Admin Sessions

When an administrator logs into the Password Safe web portal, they can open the **Admin Sessions** page and log onto any machine for a session without a password request.

> ***Note:*** *The **Admin Sessions** page will always be available for administrators and ISA users. It can also be made available to any user if an administrator has granted permissions for the **Password Safe Admin Session** permission.*

1. Select the **Admin Session** page, and complete the fields provided.
2. Click **Connect** and instantly open the RDP or SSH Admin Session.

Tip: *The requestor can choose from a menu or manually enter the IP address of the computer they want to connect to. If* ***Multi-System Checkout*** *is configured for requestors, two additional fields display:* ***Available Accounts*** *and* ***Asset / IP****.*

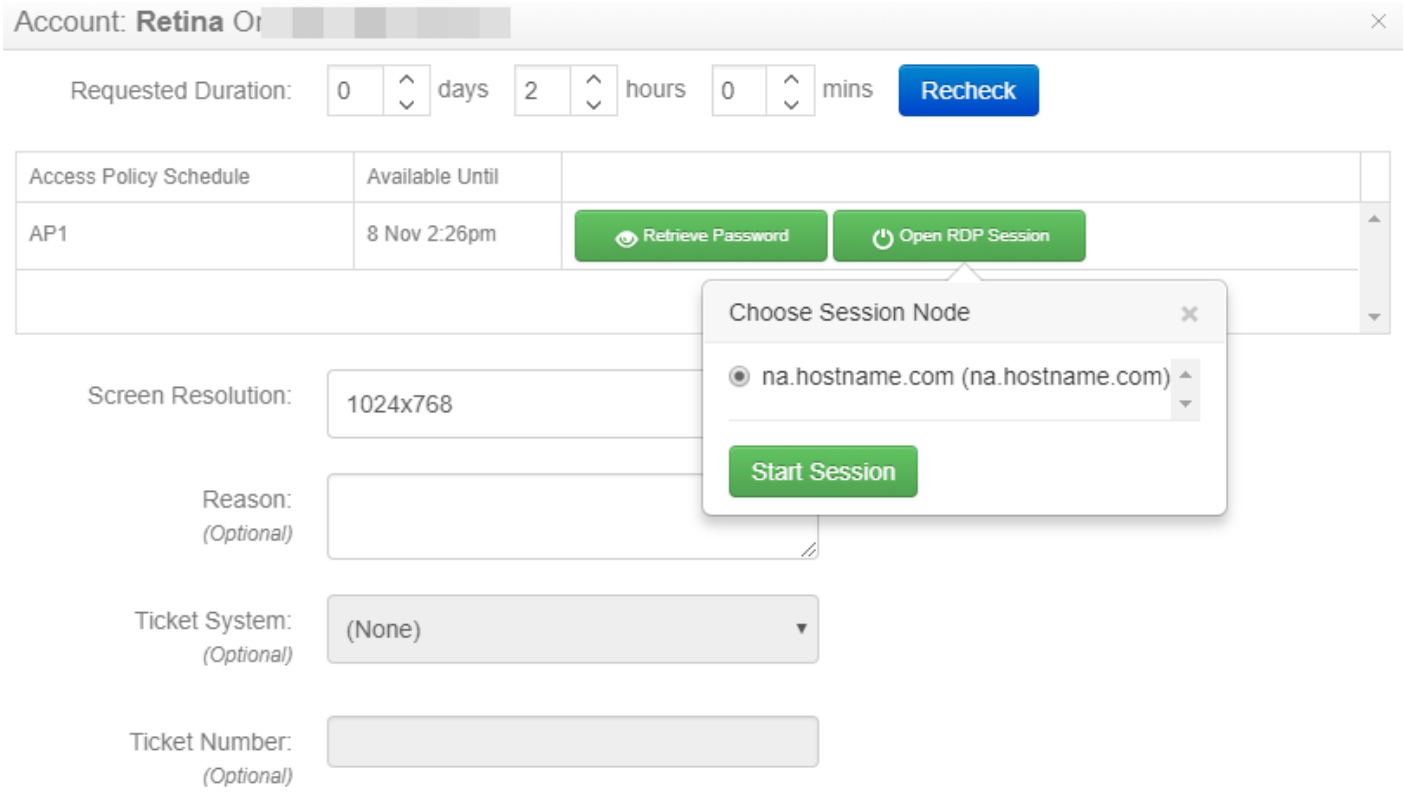


Request Remote Proxy Session

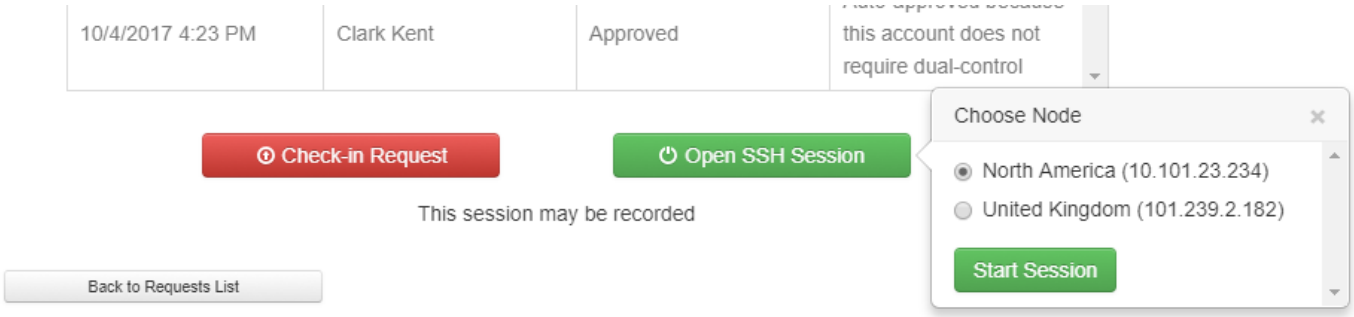
In larger environments, assets you need to access might not be in your region. If configured by your Password Safe administrator, you can select a node associated with another region to proxy these session types:

- 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:



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

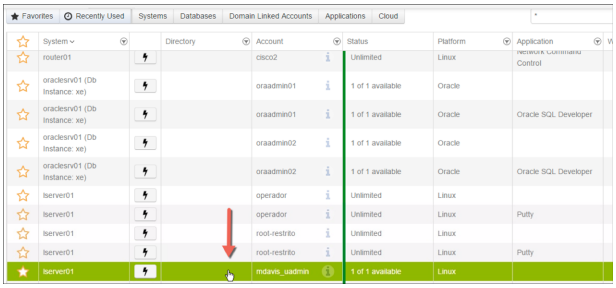


Password Safe Use Cases

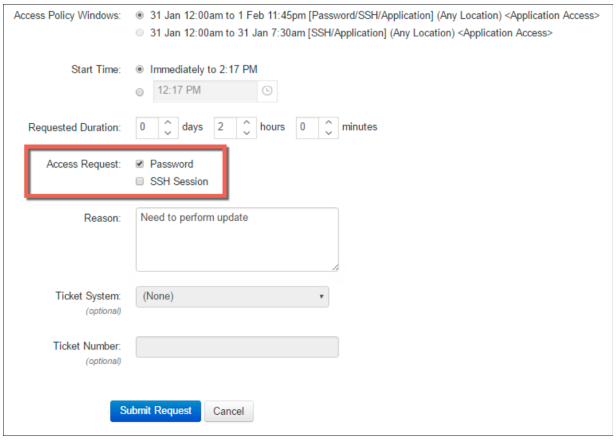
Request Access to a Linux Account - Password Retrieval

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.

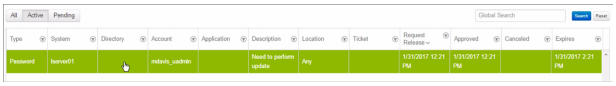
1. Log into the web portal.
2. Scroll to the system **lserver01**, find the **mdavis_uadmin** account, and click to open.



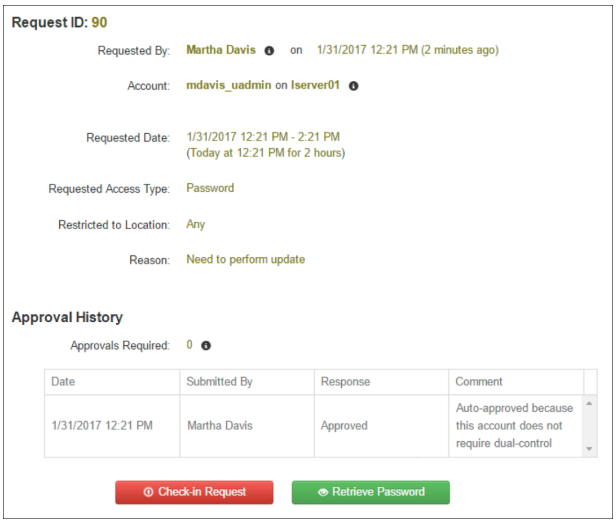
3. Enter a date, time, and duration.
4. Select the **Password** check box and enter a reason for the request.
5. Click **Submit Request**.



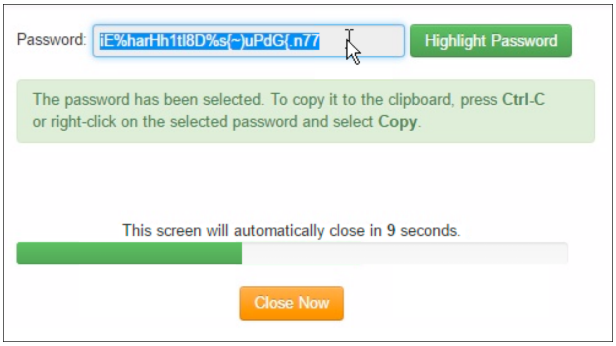
6. Depending on your access policy, the request may be auto-approved. If so, you should have an active request immediately available. Otherwise, wait for approval.
7. Select the active request.



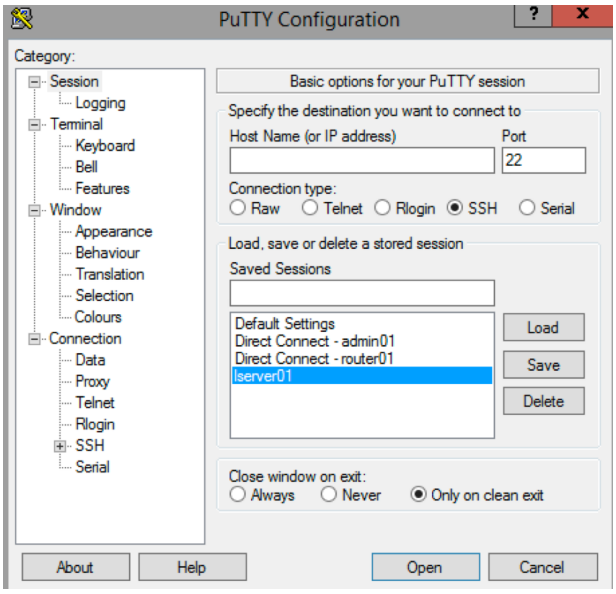
8. Click **Retrieve Password**.



9. Highlight the password, and copy it to the clipboard.

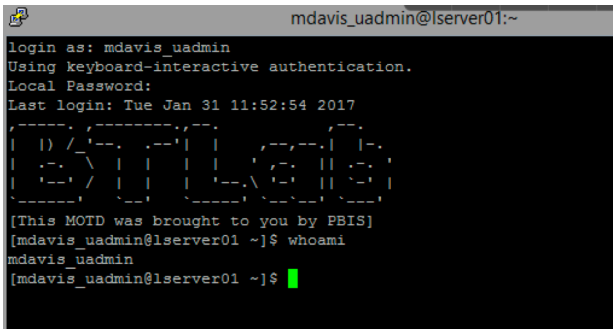


10. Open **PuTTY** on the BeyondInsight host, and open a connection to the **lserver01** host.



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

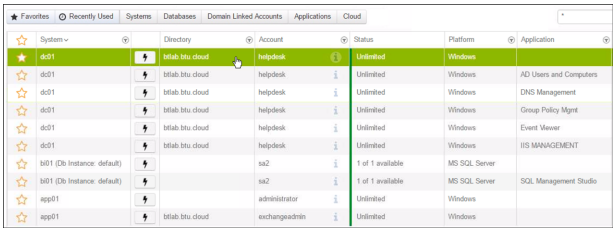
12. When finished, close the SSH session, and click the **Check-in Request** to release the **mdavis_uadmin** account.



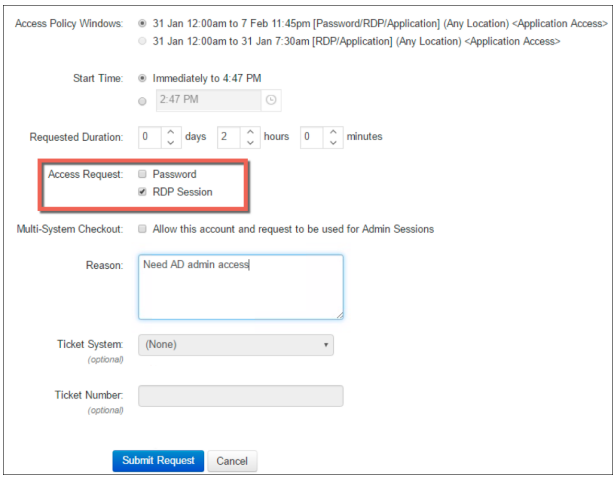
Request RDP Access to a Windows Account - Session Management

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.

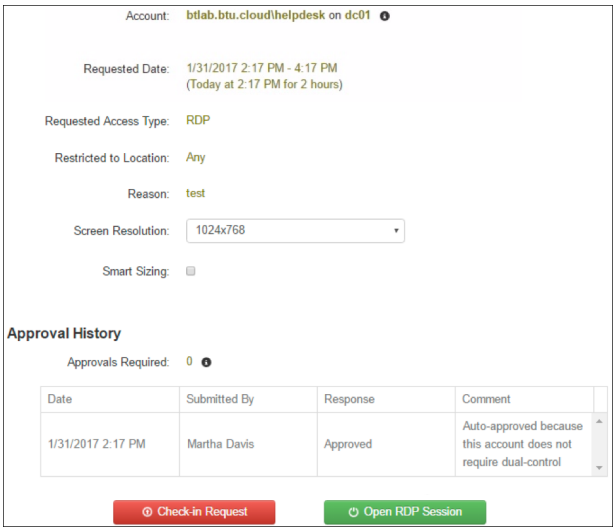
1. Log in to the web portal.
2. Scroll to the system **dc01** and find the **helpdesk** account that does not have an application configured, then click to open.



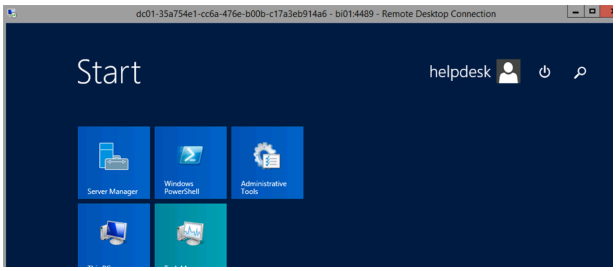
3. Enter a date, time, and duration.
4. Select the **RDP Session** check box and enter a reason for the request.
5. Click **Submit Request**.
6. Depending on your access policy, the request may be auto-approved. If so, you should have an active request immediately available. Otherwise, wait for approval.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



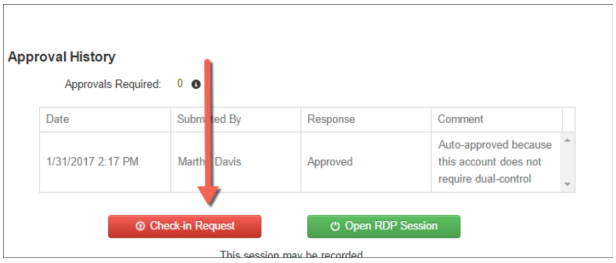
8. Select a **Screen Resolution**.
9. Click **Open RDP Session** to download an RDP connection file.



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



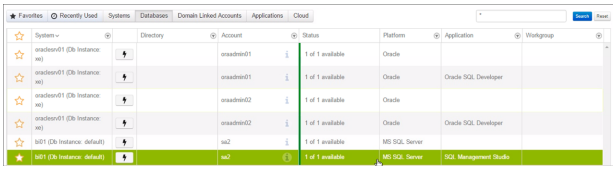
11. When finished, close the RDP window and click **Check-in Request** to release the helpdesk account.



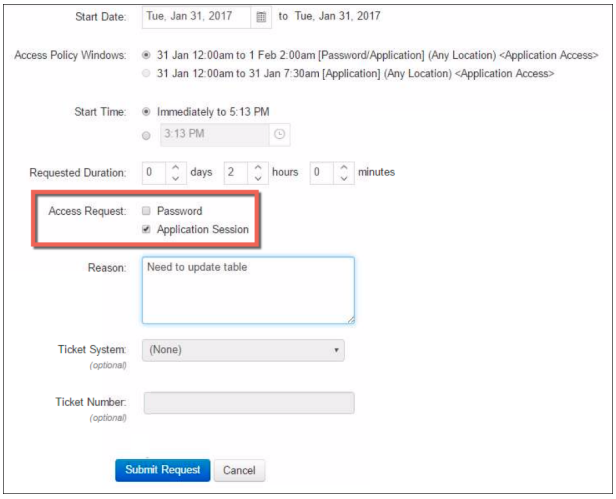
Request Access to a Microsoft SQL Account - Remote Applications

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.

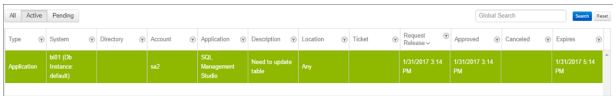
1. Log into the web portal.
2. Click the **Databases** tab.
3. Scroll to the system **bi01**, find the **sa2** account associated with **SQL Management Studio**, and click to open.

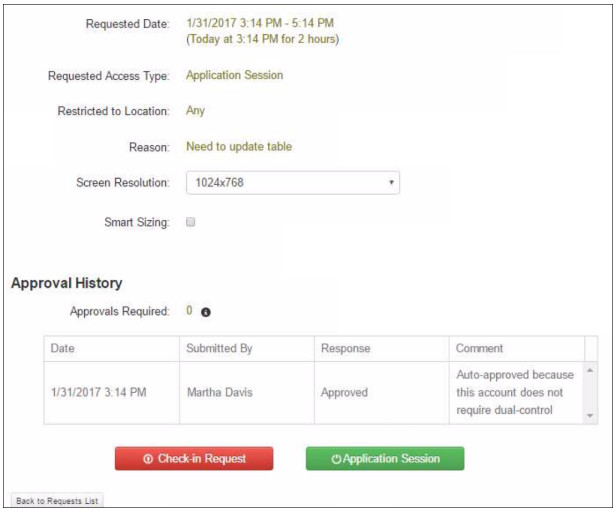


4. Enter a date, time, and duration.
5. Select the **Application Session** check box and enter a reason for the request.
6. Click **Submit Request**.



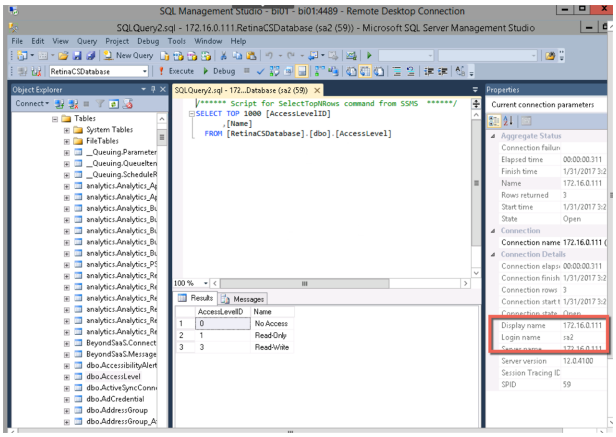
7. Depending on your access policy, the request may be auto-approved. If so, you should have an active request immediately available. Otherwise, wait for approval.
8. Select the active request.
9. Select a **Screen Resolution**.
10. Click **Application Session** to download an RDP connection file.





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.



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.*