



BeyondTrust

Password Safe 24.1 Admin Guide

Table of Contents

Password Safe Administration Guide	8
Log In to the BeyondInsight Console	9
Log Out of the Console	10
Select a Display Language	10
Navigate the Console	12
Container Cards	12
Left Sidebar	12
Manage Toast Messages and Notifications in BeyondInsight	13
Add Assets to Password Safe	15
Workflow to Add Managed Systems and Accounts to Password Safe	15
Create a Functional Account	16
Override a Functional Account Password	16
Add a Managed System Manually	17
Add Managed Systems and Accounts Using Smart Rules	20
Add Active Directory Managed Accounts Using a Smart Rule	21
Add Endpoint Privilege Management for Windows Systems and Local Accounts into Password Safe	23
Configure Functional Account Requirements in Azure	26
Create Enterprise Application	26
Configure App Registration	26
BeyondTrust Password Safe Configuration	28
Work with Managed Systems	30
View Managed Systems Details	30
Import an SSH Server Key Using a Smart Rule	31
Manage the SSH Server Keys	31
Work with Managed Accounts	33
View Managed Accounts	33
View Managed Account Details	33
Delete Managed Accounts	34
Unlink Managed Accounts	34
Change Passwords for Managed Accounts	35

Configure Subscriber Accounts	36
Configure Password Reset for Managed Account Users	36
Use a Managed Account as a Discovery Scan Credential	37
Managed Account Aliasing	39
Disabled at Rest Managed Accounts	40
Enable the Disabled at Rest Setting	40
Verify Disabled at Rest Setting	41
Sample Disabled At Rest Workflow Description	41
Affected Settings	42
Disabled at Rest Managed Accounts	43
Enable the Disabled at Rest Setting	43
Verify Disabled at Rest Setting	44
Sample Disabled At Rest Workflow Description	44
Affected Settings	45
Work with Smart Rules	46
Predefined Smart Groups	46
Considerations When Designing Smart Rules	48
Smart Rule Processing	48
View and Select Smart Rules Processing Statistics	49
Use Dedicated Account Smart Rule	49
Use an Entra ID Smart Rule	54
Use Quick Groups	56
Edit Smart Rules	57
Delete Smart Rules	58
Audit Smart Rules	58
Configure Role Based Access	59
Group Features	59
Password Safe Roles	60
Create a Group and Assign Roles	62
Quarantine User Accounts	64
Configure API Access	65
Restrict Access to Password Safe Login Page	67
Configure Approvals	69

Use a Managed Account as a Credential	70
Configure LDAP Groups	71
Real Time Authorization	72
Configure Password Safe Access Policies	73
Create an Access Policy	73
Create a Connection Profile	76
Use a Predefined Connection Profile	77
Create Password Policies	78
View Recorded Sessions	80
Use Keystroke Search	81
Archive Recorded Sessions	81
Manage Active Sessions	82
Add Windows Components to Password Safe	83
Add a Directory	83
Add Directory Accounts	83
Add Propagation Actions to Managed Accounts	86
Configure Password Safe Global Settings	94
Sessions	94
Requests	95
Session Monitoring	96
Purging	97
Miscellaneous	97
Add Databases to Password Safe	99
Auto Discover and Manage Database Instances	99
Manually Add Database Instances	101
Manage Database Instance Accounts	102
Discover Accounts for SAP HANA Databases	104
Create a Functional Account for a SQL Server Database	105
SQL Server Instance Port Retrieval	106
Add a PostgreSQL Database Instance	107
Configure Settings on the Oracle Platform	109
Add Applications to Password Safe	114
Prerequisites	114

Add an Application	114
View Application Details	116
Use Encryption Module for RemoteApp	117
Associate the Application with a Managed Account	117
Set Up the Access Policy	117
Set Up Role-Based Access	118
Use the PS_Automate Utility	118
Use Autolt Passthrough	119
Add SAP as a Managed System	120
Configure API Registration	122
Add an API Key Policy API Registration	122
Add OAuth Authentication for API Access for Application Users	123
Add a Custom Platform or Application Platform	126
Create a New Platform	126
Configure the Options Tab	126
Configure the Steps Tab	127
Configure the Check/Change Password Tab	129
Create a New Application Platform	131
Export or Import a Custom Platform	135
Configure SSH and RDP Proxy Connections	137
Requirements for SSH	137
Host Key Algorithms	137
KEX Algorithms	137
MAC Algorithms	138
Ciphers	138
RSA Host Key Size	139
Auto-Launch PuTTY Registry File	139
Supported SSH Session Protocols	140
Multiple SSH Sessions	140
Enable Login Accounts for SSH Sessions	140
Use Direct Connect for SSH and RDP Session Requests	141
Configure RDP Sessions	143
SSH Client Check and Change Password Algorithms	146

The Following Algorithms Are Disabled by Default	146
Use the Following Registry Keys to Turn on the Algorithms	146
Configure Session Monitoring	147
Configure Listen Host and File Location	147
Configure Concurrent Sessions	147
Use Session Masking	148
Customize Session Images	148
Configure Recorded Sessions in a Multi-Node Environment	150
Configure Keystroke Logging	151
Enhanced Session Auditing	151
Configure Algorithms used by the Session Monitoring Proxy	154
Use DSS Authentication	155
Generate and Distribute the Key	155
Create a Functional Account with DSS Authentication	155
Create a Functional Account on the Unix or Linux Platform	156
Set DSS on the Managed Account	157
DSS Key Auto Management	158
Configure Password Safe Agents	160
Configure the Password Change Agent	160
Configure the Mail Agent	161
Configure the Password Test Agent	161
Configure Session Agents for Remote Proxy Sessions	162
Add Ticket Systems to the List on the Requests Page	164
Customize Email Notifications	165
Email Notifications Sent by Password Safe	165
Customize Mail Templates	167
Configure Workgroups for Multi-Node and Multi-Tenant Environments	168
Create a Password Safe Worker Node	168
Assign a Password Safe Worker Node to a Workgroup	168
Assign a Workgroup to a Managed Account	168
Assign Agents to Workgroups for Multi-Tenant Environments	169
Configure and Use Secrets Safe	171
Assign the Secrets Safe Feature to a Group	171

Create a Secret in Secrets Safe	171
Manage Folders in Secrets Safe	175
View and Copy a Secret in Secrets Safe	175
Edit and Delete a Secret in Secrets Safe	176
Password Safe PS_Automate Utility User Guide	178
Define Command Line Arguments in INI File	180
General Section	180
Credentials Section	181
TaskSequences Section	182
App Task Sequences	182
WebApp Task Sequences	184
Certificates	184
Web App Known Issues	184

Password Safe Administration Guide

Password Safe is your privileged access management solution to ensure your resources are protected from insider threats. It combines privileged password and session management to discover, manage, and audit all privileged credential activity.

Password Safe creates and secures privileged accounts through automated password management, encryption, secure storage of credentials, and a sealed operating system.

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.

Password Safe is supported on a hardened U-Series Appliance that creates and secures privileged accounts through automated password management, encryption, secure storage of credentials, and a sealed operating system.

More specifically, you can use Password Safe to accomplish the following:

1. Scan, identify, and profile all assets for automated Password Safe management, ensuring no credentials are left unmanaged.
2. Control privileged user accounts, applications, SSH keys, cloud admin accounts, RPA accounts, and more.
3. Use adaptive access control for automated evaluation of just-in-time context for authorization access requests.
4. Monitor and record live sessions in real time and pause or terminate suspicious sessions.
5. Enable a searchable audit trail for compliance and forensics, and achieve complete control and accountability over privileged accounts.
6. Restrict access to critical systems, including assets and applications, keeping them safe from potential inside threat risks.

Log In to the BeyondInsight Console

The admin credentials used to log in to the BeyondInsight console for the first time are configured during the installation process. Afterward, the credentials you use to log in to the console depend on the type of authentication configured for your BeyondInsight system. Logging into the console varies depending on the type of authentication configured for your system.

The following authentication types can be used:

- **BeyondInsight:** Create local users in BeyondInsight and add them to groups to assign permissions to features. Local users can log in to the console from the BeyondInsight login page.
- **Active Directory:** Add Active Directory users in BeyondInsight and add them to groups to assign permissions to features. Active Directory users can log in to the console from the BeyondInsight login page.
- **Microsoft Entra ID:** Add Entra ID users in BeyondInsight and add them to groups to assign permissions to features. Entra ID users can log in to the console from the BeyondInsight login page.



Note: To use Entra ID credentials for logging into BeyondInsight, the accounts must use SAML authentication. For more information on configuring Entra ID SAML with BeyondInsight, please see [Configure Microsoft Entra ID SAML with BeyondInsight SAML](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/security-provider.htm#configure-entra-id) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/security-provider.htm#configure-entra-id>.

- **LDAP:** Add LDAP users and add them to groups to assign permissions to features. LDAP users can log in to the console from the BeyondInsight login page.
- **Two-Factor Authentication:** Configure two-factor authentication with a RADIUS server or time-based one-time password (TOTP) authenticator app, and assign it to users in BeyondInsight. Users are prompted for their two-factor login options after providing their credentials on the BeyondInsight login page.
- **Smart Card:** Configure BeyondInsight to allow authentication using a smart card PIN. Users can bypass the BeyondInsight login page and navigate to the smart card site access URL provided by the administrator to use smart card authentication.
- **SAML Authentication:** Configure SAML identity providers in BeyondInsight to use authentication for web tools that support SAML 2.0 standard, such as PingID, Okta, and ADFS. Users can authenticate with the default SAML identity provider configured in BeyondInsight by clicking the **Use SAML Authentication** link on the BeyondInsight login page. To log in using a SAML identity provider other than the default provider, users can navigate to the SAML site access URL provided by the administrator.
- **Claims-Aware:** Configure a claims-aware website to bypass the current BeyondInsight login page and authenticate against any configured Federated Service that uses SAML to issue claims.



Note: When working in the console, the times displayed match the web browser on the local computer unless stated otherwise.

To log in:

1. Open a browser and enter the URL for your BeyondInsight / Password Safe instance:
https://<hostname>/WebConsole/index.html.
2. Enter your username and password. The default username is **Administrator**, and the password is the administrator password you set in the .
3. If applicable, select a domain or LDAP Server from the **Log in to** list.



Tip: The **Log in to list** is only displayed on the **Login** page when there are either AD or LDAP user groups created in the BeyondInsight console. The **Log in to list** is displayed by default, but may be disabled / enabled by an admin user by toggling the **Show list of domains/LDAP servers on login page** setting from **Configuration > System > Site Options** page.

4. Click **Log In**.
5. To log in using SAML Authentication, click the **Use SAML Authentication** link below the **Log In** button. You are redirected to the single sign-on access site for the default SAML identity provider configured by your administrator in BeyondInsight.



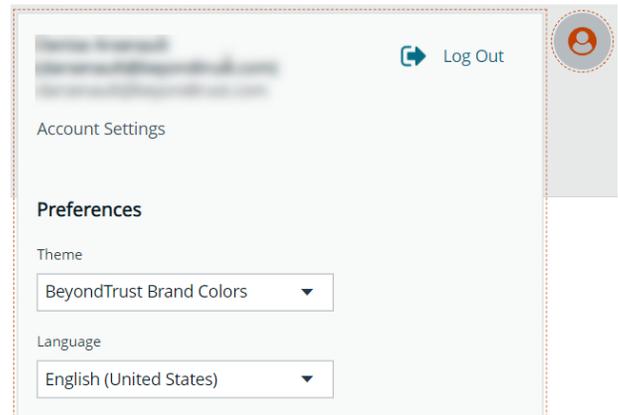
Note: If the initial login attempt fails, and two-factor authentication (2FA) is enabled, the user is taken to the 2FA page for security reasons.



For more information, please see the [BeyondInsight and Password Safe Authentication Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/index.htm>.

Log Out of the Console

To log out of the console, click **Profile and preferences** in the top-right corner, and then click **Log Out**.



Select a Display Language

BeyondInsight and Password Safe can be displayed in the following languages:

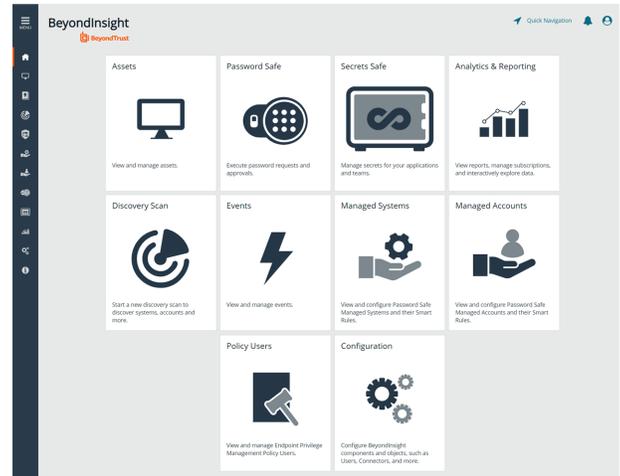
- English
- French
- German
- Japanese
- Korean
- Portuguese
- Spanish

If the **Show language picker** option is enabled in **Configuration > System > Site Options > Localization**, 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** dropdown.

Navigate the Console

Once logged into the BeyondInsight console, you are taken to the **Home** page, where the suite of features is easily accessible using any of the following methods:

- Click the container cards.
- Click the icons in the left sidebar.
- Click **Menu** in the left sidebar to expand it, and then click your desired feature.
- Click **Quick Navigation** in the top-right corner or press **CTRL+K** to access a list of the commonly used features and your favorites.
 - Locate your desired feature from the list by typing at least 3 characters.
 - Click the star next to any of the features in the list to add them to your favorites. Favorites are displayed at the top of the list.
 - Click the star next to any favorite to remove it as favorite.



Container Cards

You can quickly access the following functionality from the container cards:

- View and manage assets.
- Access Password Safe to execute password requests and approvals.
- Access Secrets Safe to view and manage team secrets.
- Access reports on collected data.
- Initiate a discovery scan to discover new systems and accounts.
- View and manage Endpoint Privilege Management events.
- View and edit managed systems.
- View and edit managed accounts.
- View and manage Endpoint Privilege Management policy users.
- Access configuration settings for BeyondInsight and Password Safe components and objects.

Left Sidebar

The following features are available from the left sidebar:

- **Dashboard (Preview):** Customize your dynamic dashboards using the **Dashboard Editor**.
- **Assets:** Display and manage all assets. Access the **Smart Rules** page to create and manage Smart Groups. Add assets to Password Safe management.
- **Smart Rules:** View and manage Smart Rules.
- **Discovery:** Run and schedule discovery scans, review active, completed, and scheduled scans, and view the list of discovery scanners.

- **Endpoint Privilege Management:** View and manage Endpoint Privilege Management events, policies, policy users, agents, file integrity monitoring, and session monitoring, if you have an Endpoint Privilege Management license.
- **Managed Systems:** View and configure properties for Password Safe managed systems, managed databases, managed directories, managed applications, and their associated Smart Rules.
- **Managed Accounts:** View and configure properties for Password Safe managed accounts and their associated Smart Rules.
- **BeyondInsight for Unix & Linux:** View and manage hosts, settings, logs, policies, license information, and jobs for BeyondInsight for Unix & Linux.
- **Password Safe:** Access the Password Safe web portal to request passwords and remote access sessions and to approve requests.
- **Privileged Remote Access:** View Privileged Remote Access session data in a dashboard, if you have a Privileged Remote Access license and have the integration with BeyondInsight configured.
- **Secrets Safe:** View and manage team secrets.
- **Analytics & Reporting:** Access reports on collected data.
- **Configuration:** Configure BeyondInsight and Password Safe components and objects, such as users and groups, authentication settings, connectors, and much more.
- **About:** Access helpful links and support tools, such as generating a support package and analysis to send to BeyondTrust Technical Support. View the current BeyondInsight version information, as well as the history of installed versions. View version information for currently installed plugins. View the maintenance expiry date and disable or enable the **Maintenance Expiry Warning Banner**.

Manage Toast Messages and Notifications in BeyondInsight

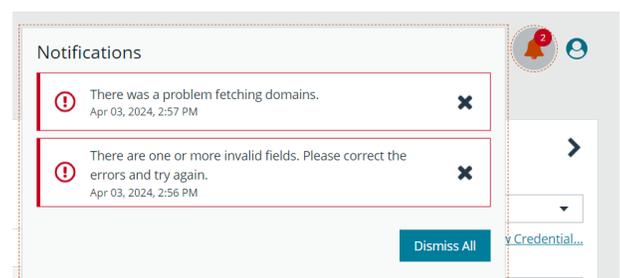
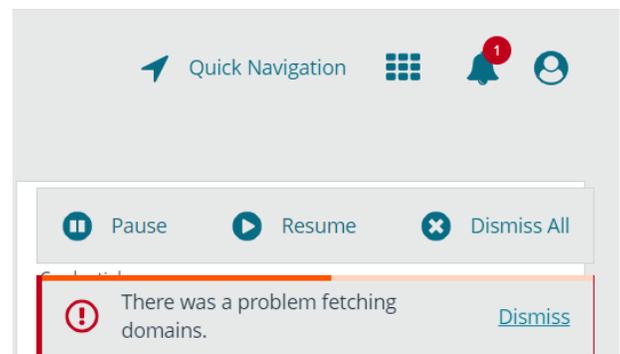
During your session, BeyondInsight displays toast messages to indicate successes, failures, warnings, and errors for actions you have taken. Toast messages auto-dismiss after 8 seconds based on a timer. There may be multiple messages displayed at once. A control bar displays above the message(s) that can be used to control the message timer. You can control the messages as follows:

- Click **Dismiss** directly in a message to dismiss that specific message immediately.
- Use the control bar above the message(s) to pause all timers, resume all timers, or dismiss all messages.

Toast messages that you haven't dismissed but instead have timed out can be reviewed in the Message Notification Center by clicking the **Notifications** (bell) icon in the top right of the console. This allows you to view more details for errors or warnings if they exist, and dismiss them.

More details about the Message Notification Center are as follows:

- Success messages are not sent to the notification center, whether or not they were dismissed.
- A max of 6 messages can be displayed at once and a scroll bar is provided to view more as needed.
- The notification center can show up to 100 of the most recent notifications, sorted from newest to oldest.
- Notifications that are older than 1 hour are not available.
- Once you log out of BeyondInsight, any notifications that existed in the notification center are cleared and are no longer available.





Note: A warning banner displays at the top of the screen if your maintenance contract for BeyondInsight is close to expiry or has expired. Click **More Details** to go to the **About** page, where you can disable and re-enable the warning.

A warning banner displays at the top of the screen if your installation includes any Discovery Agents earlier than version 20.1. These must be updated by the end of 2021. You can go to **Discovery > Discovery Scanners** to view all scanners in the system, and their version.

Click **Dismiss** to hide warning banners until your next login.

Add Assets to Password Safe

This chapter provides a high-level overview of adding systems and accounts to be managed by Password Safe. Once assets are managed by Password Safe, selected users can request access to them. For details on adding specific systems, please refer to the chapter for the particular system in this guide.

A system and the associated account can be added to Password Safe in any of the following ways:

- **Manually:** After an asset is added to the management console, you can add the asset to Password Safe.
- **Smart Rules:** You can create a Smart Rule with selected filter criteria, to match on the systems that you want to add to Password Safe.
- **Discovery Scanning:** You can run a Discovery Scan in BeyondInsight on a selected range of IP addresses.

Workflow to Add Managed Systems and Accounts to Password Safe

There are three ways to add systems and accounts to Password Safe:

- Add the asset manually.
- Run a Discovery Scan and then import the assets using an address group or directory query.
- Use API scripts.

The following is a high-level overview of the steps required to add systems and accounts to be managed in Password Safe.

1. **Add the functional account:** A functional account is one that can access the system with the privileges required to manage and change passwords for shared accounts on the system.
2. **Add the managed system:** A managed system is a computer or device where one or more account passwords are to be maintained by Password Safe. Managed systems can be Windows machines, Unix/Linux machines, network devices, databases, firewalls, routers, iLO machines, and LDAP or Active Directory domains.
3. **Add the managed account:** A managed account is an account on the managed system whose password is being stored and maintained through Password Safe. Typically, managed accounts are privileged accounts that can perform administrative tasks on the managed system.
4. **Configure managed system settings:** After a system is added to Password Safe, configure settings that apply to the managed system.
5. **Set up role based access:** Create user groups that permit users to:
 - Log in to the Password Safe web portal.
 - Assign Password Safe roles, such as **Requester** or **Approver**.
 - Create access policies to permit accounts to access the systems, applications, and sessions, and to request password releases.

Create a Functional Account

A functional account on a managed system is required to manage passwords for accounts on that managed system. The passwords for functional accounts **cannot** be retrieved through the Password Safe web portal.



IMPORTANT!

Do not set up a functional account as a managed account. Functional accounts have built-in management capabilities and passwords might fail to synchronize, causing issues.



Note: The settings vary, depending on the type and platform chosen.

1. In BeyondInsight, go to **Configuration > Privileged Access Management > Functional Accounts**.
2. Click **Create New Functional Account**.
3. Select a type from the list.
4. Select a platform from the list.



Note: The **DSS authentication** and **Automatic password management** settings are not supported if you are using the elevated credential **pbrun jumphost**.

5. Provide credentials and a description for the account.
6. Provide an alias. The **Alias** value is shown in the selectors throughout Password Safe where you must select a functional account to use.
7. Select a Workgroup, if applicable.
8. If desired, enable **Automatic Password Management**, and then select the password policy and change frequency. This option enables automatic password changes for each managed system that this functional account is associated with at the designated frequency.



Note: If the **Automatic Password Management** option is enabled, passwords are set immediately when a new functional account is added to Password Safe. They are changed during the next scheduled rotation.

9. Click **Create Functional Account**.

Override a Functional Account Password

Every managed system that uses a specific functional account has a unique password associated with that functional account. The password on the managed system might be out of sync with the password in Password Safe. You can override a functional account password from the **Functional Account** section in the **Advanced Details** of a managed system.

Add a Managed System Manually



Note: Settings vary depending on the platform type. When an account is manually added to a managed system, the default configuration of the account is set to what is configured on the managed system.

There are two ways to add a managed system to Password Safe manually:

- From the **Managed Systems** page, click **Create New Managed System**, and then complete the **Create New Managed System** form.
- From the **Assets** page, click the vertical ellipsis for an asset, then select **Add to Password Safe**, and then complete the **Create New Managed System** form.

Below are the fields and settings with their descriptions that are available when creating a new managed system. The available fields change depending on the **Entity Type** and **Platform** for the system.

Field / Setting	Description or Action
Entity Type	Type of system: Asset , Database , Directory , or Cloud .
Platform	The platform for the system based on the Entity Type .
Name	Unique name for the system.
Port	Default RDP port for new managed systems.
Instance Number (SAP only)	If you have added your System Application Products (SAP) environment to Password Safe management, provide the instance number.
Domain (Directory types only)	Name of the Domain where the directory resides.
Description	Description for the system.
DNS Name	DNS name for the system.
IP Address	IP address for the system.
Allow Managed System to be an Application Host (non-Windows systems only)	Toggle on or off to allow the system to be an application host.
NetBIOS Name (Windows, Active Directory, and LDAP systems only)	Unique NetBIOS name for the system.
Workgroup	Select a pre-defined workgroup from the list.
Port	Enter a port number.
Automatic Password Change Options	Toggle Enabled to automatically check and update managed account passwords at a set frequency or after password releases.
Password Policy	Select a Password Safe password policy or use the default policy. The policy provides the requirements used by Password Safe to create passwords, such as password length and permitted characters.
Change Agent (available only when Endpoint Privilege Management is installed)	Select Password Safe or Endpoint Privilege Management client from the list.

Field / Setting	Description or Action
Elevation	<p>Select an elevated account to run as: sudo, pmsrun, pbrun, pbrun jumppost.</p> <p>If you are using pbrun jumppost, enter the IP address for the Privilege Management for Unix & Linux policy server that you want to connect to.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: SSH Key Enforcement Mode is not available if you are using pbrun jumppost. </div>
Change Agent (available only when Endpoint Privilege Management is installed)	Select Password Safe or Endpoint Privilege Management Client from the list.
Functional Account	<p>Select a functional account from the list. If a functional account is not available, click the Create New Functional Account link. The link is located in two places, below the dropdown and within the dropdown list. This allows you to create a functional account without leaving the Managed Systems page.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: The Create New Functional Account link is available to users with the Password Safe Configuration Management feature permission. </div>
Use Login Account for SSH Sessions	<p>Create a login account to allow the user to open an SSH session in environments where remote shell access is not permitted, for instance the root account.</p> <p>Login Account: Select the account name.</p>
Account Name Format (For Windows, Linux, Oracle, MS SQL Server, and Active Directory only)	Select a format for the account name from the list: Domain\Account , UPN: accountName@domainName , or sAMAccountName: Account Name only .
Timeout	The timeout value determines the amount of time in seconds that a connection attempt to the managed system remains active before being aborted. In most cases, we recommend you use the default value (30 seconds). If there are problems with connection failures with the system, this value can be increased.
SSH Key Enforcement Mode	<p>Verifies SSH host keys from a known host. You can import SSH keys from a host using a Smart Rule.</p> <p>Auto Accept Initial Key: The first key imported is automatically accepted. Any new key imported after the initial key must be manually accepted.</p> <p>Manually Accept Keys: SSH connections to the host are permitted for accepted keys only. If a new key is detected from the host, the key is stored in the database and an email is sent to the Administrators user group. The key must then be accepted or denied.</p>
Default DSS Key Policy	If you are using DSS authentication for the system, select a key policy or use the default.
Release Duration	The duration that can be requested during the request process. The default value is 2 hours. When the Requested Duration (as entered by the user on the Requests page in the web portal) is exceeded, the session ends if the Force Termination option is enabled for the access policy.
Max Release Duration	The maximum length of time the requester is permitted to enter on the Requests page. Applies to password and session requests. The maximum length that can be set is 365 days.
Contact e-mail	Enter the email address where you want Password Safe system notifications to be sent.



For more information, please see the following:

i

- ["Add SAP as a Managed System" on page 120](#)
- ["Create Password Policies" on page 78](#)
- ["Enable Login Accounts for SSH Sessions" on page 140](#)
- ["Import an SSH Server Key Using a Smart Rule" on page 31](#)
- ["Manage the SSH Server Keys" on page 31](#)
- ["Set DSS on the Managed Account" on page 157](#)
- ["Configure Password Safe Access Policies" on page 73](#)

Add Managed Systems and Accounts Using Smart Rules

You can add assets to Password Safe using an asset-based Smart Rule.



Tip: Before proceeding, consider the selection criteria to use to add the assets. There are several options available, including **Operating System** and **Directory Query**.



Note: SSH key enforcement is not supported when using the **pbrun jumphost** elevated credential. The settings display as available after **pbrun jumphost** is selected. However, the settings will not work with the elevated credential.

1. From the left menu, click **Smart Rules**.
2. Leave **Asset** selected as the **Smart Rule type filter**.
3. Click **+ Create Smart Rule**.
4. Select a **Category** from the dropdown.
5. Enter a **Name** and **Description** for the Smart Rule.
6. Select a **Reprocessing Limit** from the dropdown to limit how often the Smart Rule processes. **Default** means the Smart Rule processes when necessary. This is the preferred setting for less intensive processing. For more intensive processing select another option to restrict the Smart Rule to run once per selection.



Note: A Smart Rule always processes when first saved or updated.

7. Set the **Selection Criteria** by selecting **ALL** or **ANY** from the **Include Items that match the following** dropdown and selecting the filter criteria from the list. **Address Group** is a very useful filter and more than once condition may be added.
8. In the **Actions** section, select **Manage Assets Using Password Safe** from the list.
9. Select the **Platform**, **Functional Account**, and **Account Name Format**. Other settings may be left as defaults or changed as required.



Note: These settings are the same settings available when adding the system manually by creating a new managed system.

10. In the **Actions** section, click **Add another action**.
11. Select **Show asset as Smart Group** from the list. This is helpful for grouping assets and accounts by their type.
12. Click **Create Smart Rule**.

Create New Asset Based Smart Rule

Selection Criteria ⊖

Include Items that match ALL of the following

Address Group ⊕

Linux Servers ⊖

Use to discover new assets during scans

[Add another condition](#) [Add a new group](#)

Actions ⊖

Manage Assets using Password Safe ⊕

Platform Windows ⊖

Change Agent Password Safe ⊖

Account Name Format Domain/Username ⊖

Functional Account UVM function account ⊖

Enable Automatic Password Management yes ⊖

Enable Accounts For AD Queries no ⊖

Password Rule Default Password Policy ⊖

Connection Timeout 30 ⊕

Port 3389 ⊕

Show asset as Smart Group ⊕

[Add another action](#)

[Create Smart Rule](#) [View Results](#) [Discard](#)



Tip: To view the contents of a Smart Rule when creating a new rule or editing an existing rule:

- Once the rule is saved, click **View Results**.
- You are taken to the associated grid, where the contents of the Smart Rule are listed.
- If the rule is actively processing, a banner displays letting you know that.



Note:

- **View Results** displays only if you have permissions to the grid corresponding to the Smart Rule, i.e.; Assets, Managed Accounts, Managed Systems.
- The Smart Rule must be saved with **Show <entity> as Smart Group** selected under **Actions** to view the results.



Tip: Because the Smart Rule must process to display the contents in the grid, we recommend viewing the results using only the **Show <entity> as Smart Group** action and before adding additional actions that may make changes to accounts and assets in your network.

Once you have confirmed the rule contains your desired items, you can then add additional actions to the Smart Rule.



For complete descriptions of fields and settings for the Smart Rule, please see ["Add a Managed System Manually" on page 17](#).

Add Active Directory Managed Accounts Using a Smart Rule

You can create a Smart Rule that discovers and adds Active Directory accounts to Password Safe, using the below procedure. The procedure also shows how to link domain accounts to the system.



Note: A directory query and a domain should be created prior to creating a Smart Rule.

1. From the left menu, select **Smart Rules**.
2. From the **Smart Rule type filter** list, select **Managed Account**.
3. Click **+ Create Smart Rule**.
4. Select the **Selection Criteria** as applicable:
 - **Asset Smart Group:** Select a Smart Group from the list.
 - **Child Smart Rule:** Select a Smart Rule you want to filter the child Smart Rules from.
 - **Dedicated Account:** Select an account filter from the list. Enter a keyword to search on.
 - **Directory Query:** Choose to **Include** or **Exclude accounts from Directory Query**.
 - Select a query from the list, or click **Create New Directory Query** to open the form and create a new query.
 - Provide the frequency for the query to run. Leave the entry as **0** for a one time run.
 - Enable the **Discover accounts for Password Safe Management** option to discover accounts when the Smart

- Rule processes.
 - Select a **Domain** from the list.
 - **Managed Account Fields:** This filter only applies to existing managed accounts.
 - Select a filter: **Account Name, Create Date, Description, Domain Name, Last Change Date** or **Last Change Result**.
 - Select an expression, and then enter a keyword to search on, for example, **WIN** for Windows.
 - **Managed System Fields:** The Smart Rule is filtered according to the managed system you select.
 - Select a filter: **System Name, Create Date, Last Update Date**.
 - Select an expression, and then enter a keyword to search on, for example, **WIN** for Windows.
 - **Platforms:** Select a platform or check **Select All**.
 - **User Account Attribute:** Select the attribute from the list, and then provide the filter condition and value for that attribute. For each attribute filter, select **Yes** for **Discover accounts for Password Safe Management**, and then select a Smart Group to search in.
 - **Privilege:** Select **is one of** or **is not one of**. Select **All** or one, or a combination of **Administrator, Guest, or User**.
 - **SID:** Select an expression, and then enter a keyword to search on.
 - **Account Name:** Select an expression, and then enter a keyword to search on.
 - **Password Age:** Select an expression, and then select age parameters to search on.
5. In the **Actions** section, select **Manage Account Settings** to add the accounts that match on the criteria to Password Safe. The settings are the same as when you add the accounts manually.
6. Additional properties can be set under **Actions**:
- **Assign preferred Domain Controller on each Active Directory account:** Select the **Active Directory domain** and **Domain Controller** from the lists.
 - **Assign workgroup on each account:** Used with agent workgroups in multi-active deployments, this action enables you to define groups of accounts that will be assigned to specific password change agents. Select a workgroup from the list, or select **Any**.
 - **Link domain accounts to Managed Systems:** When used with **Directory Accounts** filter criteria, this action creates a linked association between the directory accounts and the target asset Smart Groups for role-based access control.
 - **Link managed accounts to Remote Applications:** Assigns the application(s) to any managed accounts that match the **Session Criteria**.
 - **Map Dedicated Accounts To:** Use only when the **Dedicated Accounts** filter criteria is selected. This action identifies the group of user accounts that are used to match against the dedicated account mask condition.
 - **Send an email Alert:** Select to send an email alert when the Smart Rule processes. The email contains a summary of the results the managed accounts matched by the Smart Rule and any changes since its last execution.
 - **Set attributes on each account:** Select to assign an attribute to filter and sort managed accounts. When viewing the Smart Groups on the **Managed Accounts** page, the groups are organized based on the filters selected in the Smart Group. You can use the default attributes that are available or create an attribute on the **Configuration** page. When the Smart Rule runs, the attribute is applied to all managed accounts that match on the selected filter criteria.
7. Under **Actions**, click the link to **Add another action**, and then select **Show managed account as Smart Group**.
8. Click **Create Smart Rule**.

Add Endpoint Privilege Management for Windows Systems and Local Accounts into Password Safe

The integration between Password Safe and Endpoint Privilege Management for Windows (EPM) allows for agent-based local account password rotation and privileged account retrieval to *run as* actions for accounts on Windows systems where an EPM agent is running.

Prior to BeyondInsight 24.1, EPM agents could only use certificates to authenticate with BeyondInsight. You can download the certificate from **Configuration > System > Downloads > Download Client Certificate** in the BeyondInsight console. BeyondInsight configuration segments can be included in the EPM policy to enable policy management from one console and password policy from Password Safe.

Using BeyondInsight 24.1 or a later version, you can use installer activation keys to leverage OAuth authentication when configuring the integration between BeyondInsight and Endpoint Privilege Management (EPM) agents that support OAuth communications. Prior to this, the integration between EPM agents and BeyondInsight was certificate-based only. While certificate-based authentication is still available, the addition of OAuth authentication greatly simplifies the setup process.

In Endpoint Privilege Management for Windows, features to support Password Safe integration include:

- Off-network account management: The EPM agent contacts Password Safe for password tests or password changes.
- Allow as Password Safe user: You can run an application using managed account credentials sourced from Password Safe.

i For more information on configuring OAuth authentication for EPM agents, see [Configure OAuth Authentication for Agents Using Installer Activation Keys](#).

Discover Local Accounts on EPM Windows Systems

For 22.4 and later releases of Password Safe in conjunction with the Endpoint Privilege Management for Windows 22.9 EPM agent, discovery can be performed by the EPM agent on the EPM Windows system on a scheduled basis, eliminating the need to run a discovery scan in BeyondInsight. The EPM agent, running on a Windows system, publishes local user data to the **Assets** grid in BeyondInsight. You can then add the local accounts to Password Safe using a Smart Rule or add them manually.

For Password Safe releases prior to 22.4, you can add well-known local admin accounts into Password Safe using a Smart Rule, eliminating the need to run a discovery scan in BeyondInsight, as documented in the next [section](#).

i For more information on configuring the Endpoint Privilege Management for Windows integration with Password Safe, as well as discovering and onboarding accounts from EPM Windows systems, please see [Integrate Endpoint Privilege Management for Windows with Password Safe](https://www.beyondtrust.com/docs/privilege-management/integration/pmw-password-safe/password-safe-integration.htm) at <https://www.beyondtrust.com/docs/privilege-management/integration/pmw-password-safe/password-safe-integration.htm>.

Add Known Local Admin Managed Accounts Using a Smart Rule

It can be useful in some cases to onboard well-known local admin accounts, such as the Windows administrator or the Linux root account, from endpoints into Password Safe without the need to run a discovery scan against the endpoints. You can create a managed system Smart Rule that uses the **Create Managed Account on each system** action to accomplish this.

One scenario in which this is useful is when you have Endpoint Privilege Management (EPM) clients in your environment. You can create a managed system Smart Rule to add local accounts as managed accounts from the EPM client endpoints so that a password rotation event exists when the EPM agent requests it. Having these preconfigured managed accounts saves time by not having to configure and run a discovery scan after the EPM agent makes the request.

Create the Smart Rule as follows:

1. From the left menu, click **Smart Rules**.
2. From the **Smart Rule type filter** list, select **Managed System**.
3. Click **+ Create Smart Rule**.
4. From the **Category** dropdown, select **Managed Systems**.
5. Provide a name and description.
6. For the **Selection Criteria**, select **Asset Smart Group** and **Endpoint Privilege Management Clients** from the dropdowns.
7. For **Actions**, select **Show managed system as Smart Group** and **Create Managed Account on each system** from the dropdowns.
8. Leave the remaining settings for **Actions** as default or modify as required.



Note: *Administrator is the default account name, because that is standard for Windows systems. You can modify the name if you have configured something other than default standard local admin account name in your environment. You can also add multiple **Create Managed Account on each system** actions if you have additional local admin accounts you wish to manage with Password Safe.*

9. Click **Create Smart Rule**.

Create New Managed System Based Smart Rule

Details ▾

Category: Managed Systems

Name: Create EPM Admin Managed Accounts Active

Description:

Reprocessing limit: Default

Selection Criteria ▾

Include Items that match ALL of the following

- Asset Smart Group
- Endpoint Privilege Management Clients

[Add another condition](#) [Add a new group](#)

Actions ▾

- Show managed system as Smart Group
- Create Managed Account on each system

Account Name: Administrator

Password Rule: Default Password Policy

Enable Automatic Password Management: yes

Change Password Time: 23 30

Change Password Frequency: Every 30 Days

Default Release Duration: Days: 0 Hours: 2 Minutes: 0

Maximum Release Duration: Days: 0 Hours: 2 Minutes: 0

ISA Default Release Duration: Days: 0 Hours: 2 Minutes: 0

Max Concurrent Request: 1

Account Options: Change Password after Release, Check Password

Change Password on Mismatch

Email release notifications to:

Create Managed Account on each system

Account Name: btadmin

Password Rule: Default Password Policy

Enable Automatic Password Management: yes

Change Password Time: 23 30

Change Password Frequency: Every 30 Days

Default Release Duration: Days: 0 Hours: 2 Minutes: 0

Maximum Release Duration: Days: 0 Hours: 2 Minutes: 0

ISA Default Release Duration: Days: 0 Hours: 2 Minutes: 0

Max Concurrent Request: 1

Account Options: Change Password after Release, Check Password

Change Password on Mismatch

Email release notifications to:

[Add another action](#)

Create Smart Rule **View Results** **Discard**



Tip: To view the contents of a Smart Rule when creating a new rule or editing an existing rule:

- Once the rule is saved, click **View Results**.
- You are taken to the associated grid, where the contents of the Smart Rule are listed.
- If the rule is actively processing, a banner displays letting you know that.



Note:

- **View Results** displays only if you have permissions to the grid corresponding to the Smart Rule, i.e.; Assets, Managed Accounts, Managed Systems.
- The Smart Rule must be saved with **Show <entity> as Smart Group** selected under **Actions** to view the results.



Tip: Because the Smart Rule must process to display the contents in the grid, we recommend viewing the results using only the **Show <entity> as Smart Group** action and before adding additional actions that may make changes to accounts and assets in your network.

Once you have confirmed the rule contains your desired items, you can then add additional actions to the Smart Rule.



For more information, please see the following:

- ["Add a Managed System Manually" on page 17](#)
- ["Add Directory Accounts" on page 83](#)

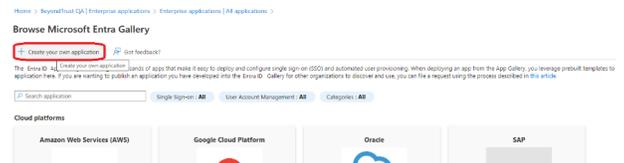
Configure Functional Account Requirements in Azure

Follow the steps below to set up Entra ID for use with BeyondTrustPassword Safe.

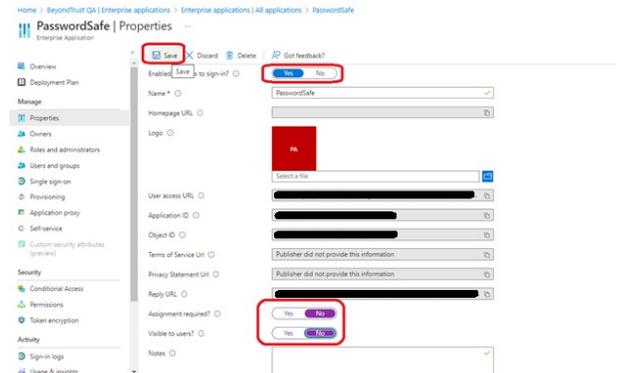
 **Note:** Accounts can be managed with or without multifactor authentication enabled in Azure.

Create Enterprise Application

1. In Microsoft Azure, go to **Enterprise Applications** and select **New application**.
2. Select **Create your own application**.

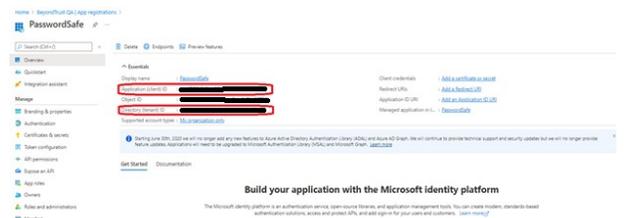


3. Name your application, select the application type (**App you're developing**) and click **Create**.
4. Update the name if necessary, select the **Supported Account Types (this directory only)** and click **Register**.
5. Under **Properties**, disable **Assignment required** and **Visible to users**, and click **Save**.

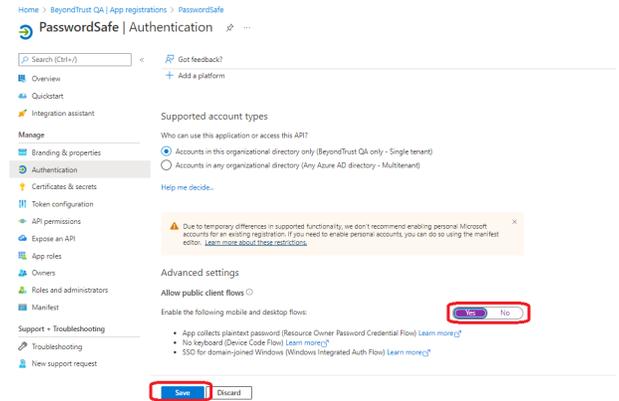


Configure App Registration

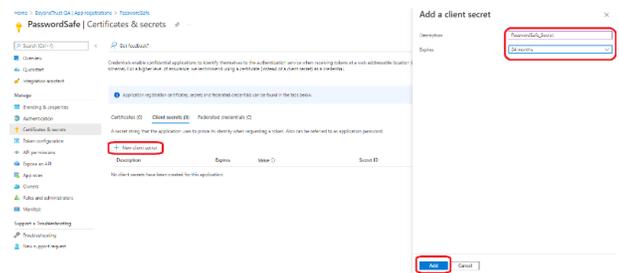
6. In **Overview** section, copy the **Application (Client) ID** and **Directory (Tenant) ID**. These are needed later to configure the Password Safe functional account.



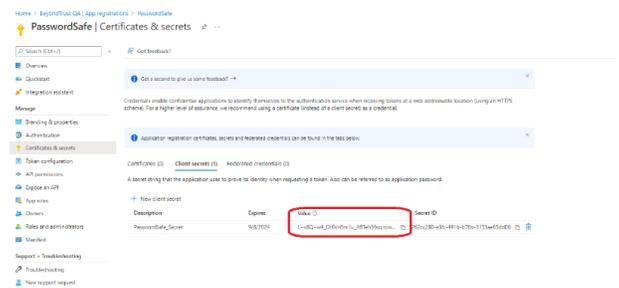
7. In the **Authentication** section, enable **Allow public client flows**, and click **Save**.



8. In the **Certificates and secrets** section, click **New client secret**. Enter the **Description**, an expiration date, and click **Add**.

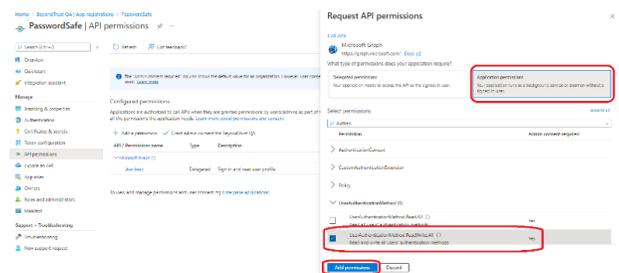


9. Copy the secret **Value**. This is needed later to configure the Password Safe functional account.



Note: The value is displayed only once, immediately after adding the new secret.

10. In the **API permissions** section, add **Microsoft Graph**, and select type **Application permissions**.

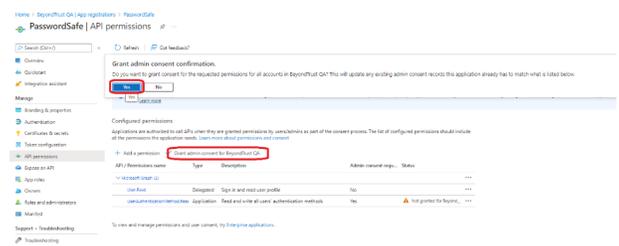


11. Add Microsoft Graph application permission **UserAuthenticationMethod.ReadWrite.All**, **Domain.Read.All**, **Group.Read.All**, and **User.EnableDisableAccount.All**.

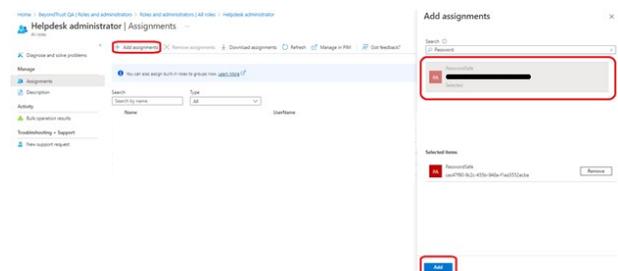
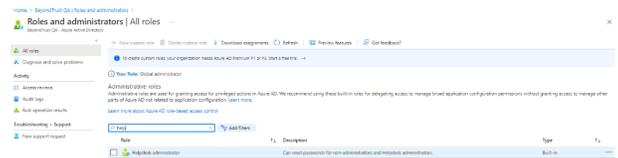
12. If **User.Read** is not already added, select **Delegated permissions** and add it.

13. Click **Add Permissions**.

14. Click **Grant admin consent** for for your organization, and click **Yes** on the confirmation message.



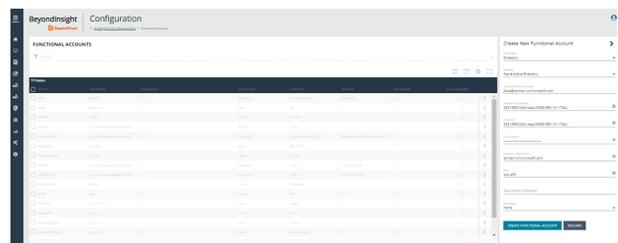
15. From the main menu, select **Roles and administrators**, then select the **Helpdesk administrator** role.
16. Click **Add assignments**, then assign the application to the **Helpdesk administrator** role.



This completes configuration in Microsoft Azure. The remaining steps are done in BeyondTrust Password Safe.

BeyondTrust Password Safe Configuration

17. Go to **Configuration > Privileged Access Management > Functional Accounts**.
18. Click **Create New Functional Account**.
19. For the **Entity Type**, select **Directory**.
20. For the **Platform**, select **Microsoft Entra ID**.
21. Enter the **Username** in UPN format.
22. Enter the previously saved values for the **Application (Client) ID**, **Tenant ID**, and **Client Secret**.
23. Set the **Alias**.
24. Click **Create Functional Account**.
25. Go to **Managed Systems**.
26. Click **Create New Managed System**.
27. For the **Entity Type**, select **Directory**.
28. For the **Platform**, select **Entra ID**.
29. Enter the **Domain**, select the **Functional Account** created above, and select the **Account Name Format**.
30. Click **Create Managed System**.



The Managed Account can be created manually or by using a Smart Rule.

31. Create the Managed Account manually.
 - Select the Managed System created above.
 - Click the vertical ellipsis at the right end of the row.
 - Select **Create New Managed Account**.
 - Enter the **Username** in UPN format, and enter **Objectid** for the **User** and **UPN**.

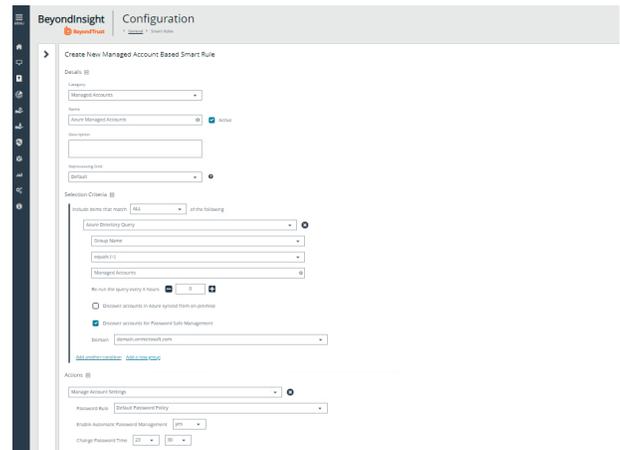


32. Create the Managed Account using a Smart Rule.

- Accounts can be onboarded by using **Group Name** or **UPN** (starts with/ends with) filters.



For more information on using Smart Rules, please see ["Work with Smart Rules"](#) on page 46.



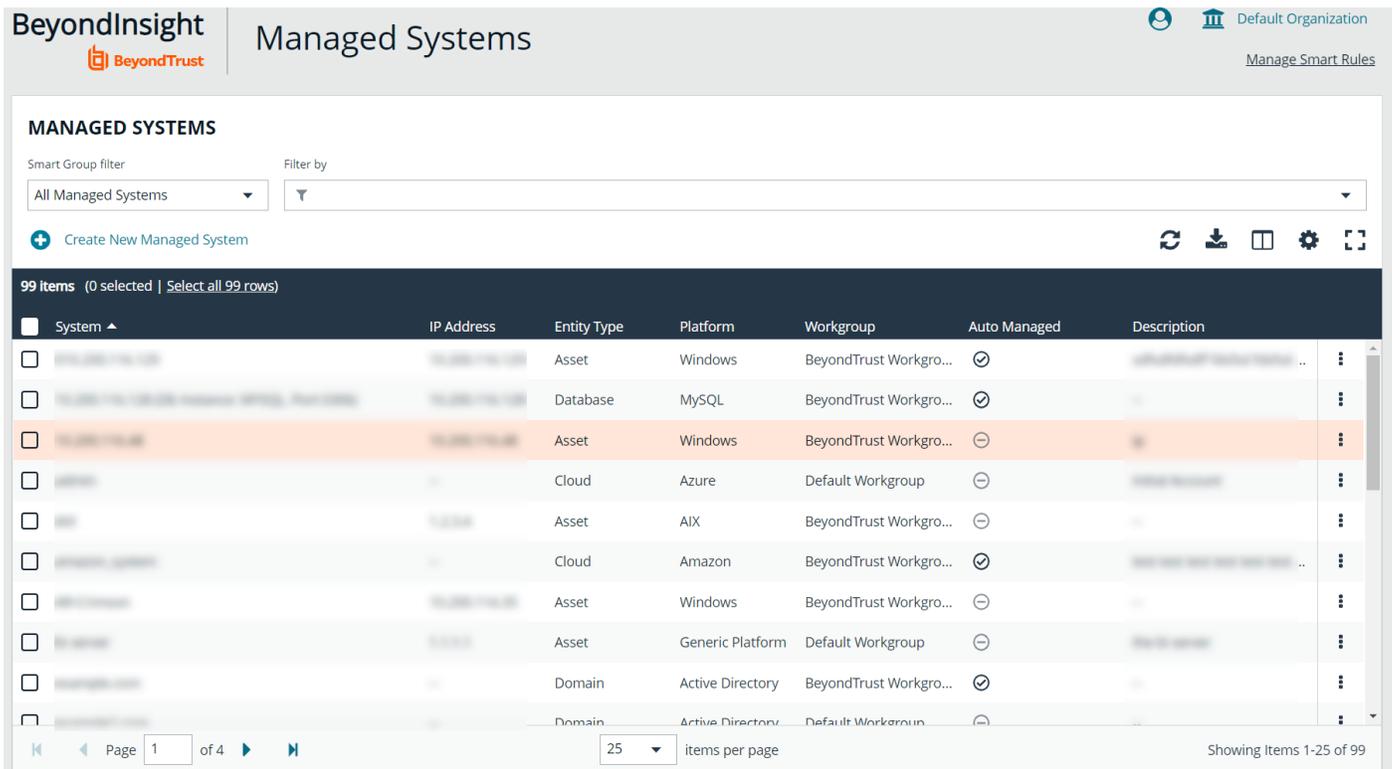
The screenshot shows the 'BeyondInsight Configuration' interface for creating a 'New Managed Account Based Smart Rule'. The page is divided into several sections:

- Details:** Includes fields for 'Group' (set to 'Managed Accounts'), 'Name' (set to 'Admin Managed Accounts'), 'Description', and 'Authentication' (set to 'Default').
- Selection Criteria:** Includes a dropdown for 'Include items that match' (set to 'All'), a 'Query' field (set to 'Group Name'), and a 'Managed Accounts' field (set to 'Managed Accounts'). It also has checkboxes for 'Run the query every 4 hours', 'Discover accounts in Active sync from on-premise', and 'Discover accounts for Password Safe Management'.
- Actions:** Includes a dropdown for 'Manage Account Settings', a 'Password Rule' dropdown (set to 'Default Password Policy'), and a 'Change Password Time' dropdown (set to 'On').

Work with Managed Systems

A managed system is any system being managed by Password Safe. A managed system can be an asset, database, directory, or cloud platform. By default, all managed systems are listed on the **Managed Systems** page, as the **Smart Group filter** is set to the built-in Smart Group **All Managed Systems**. You can filter the systems listed in the grid by selecting a different Smart Group from the **Smart Group filter** list.

Managed systems can be manually created from the **Managed Systems** page, as well as from the **Assets** page. Managed systems can also be added using Smart Rules.



BeyondInsight | **Managed Systems** | Default Organization | [Manage Smart Rules](#)

MANAGED SYSTEMS

Smart Group filter: All Managed Systems | Filter by: [dropdown]

+ Create New Managed System

99 items (0 selected | [Select all 99 rows](#))

System	IP Address	Entity Type	Platform	Workgroup	Auto Managed	Description
[checkbox] [System Name]	[IP Address]	Asset	Windows	BeyondTrust Workgro...	☑	[Description]
[checkbox] [System Name]	[IP Address]	Database	MySQL	BeyondTrust Workgro...	☑	[Description]
[checkbox] [System Name]	[IP Address]	Asset	Windows	BeyondTrust Workgro...	☐	[Description]
[checkbox] [System Name]	[IP Address]	Cloud	Azure	Default Workgroup	☐	[Description]
[checkbox] [System Name]	[IP Address]	Asset	AIX	BeyondTrust Workgro...	☐	[Description]
[checkbox] [System Name]	[IP Address]	Cloud	Amazon	BeyondTrust Workgro...	☑	[Description]
[checkbox] [System Name]	[IP Address]	Asset	Windows	BeyondTrust Workgro...	☐	[Description]
[checkbox] [System Name]	[IP Address]	Asset	Generic Platform	Default Workgroup	☐	[Description]
[checkbox] [System Name]	[IP Address]	Domain	Active Directory	BeyondTrust Workgro...	☑	[Description]
[checkbox] [System Name]	[IP Address]	Domain	Active Directory	Default Workgroup	☐	[Description]

Page 1 of 4 | 25 items per page | Showing Items 1-25 of 99



For more information on adding managed systems, please see the following:

- ["Add a Managed System Manually" on page 17](#)
- ["Add Managed Systems and Accounts Using Smart Rules" on page 20](#)

View Managed Systems Details

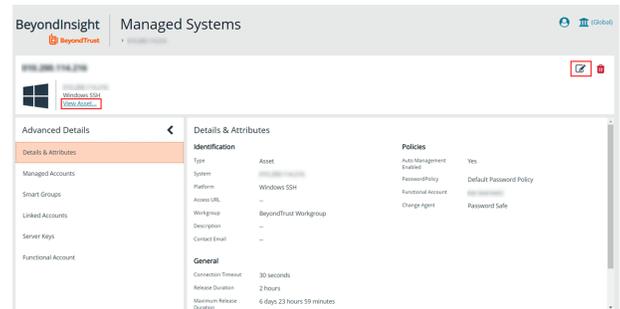
You can view details about the managed system, such as:

- Identifying details, attributes, and policies
- Managed accounts on the managed system
- Smart Groups associated with the managed system

- Accounts linked to managed accounts on the managed system
- Public keys related to the managed system
- Functional account for the managed system

View the details of a managed system as follows:

1. From the **Managed Systems** page, click the vertical ellipsis for the managed system.
2. Select **Go to Advanced Details**.
3. Click through the tabs in the **Advanced Details** pane to view details on each topic.

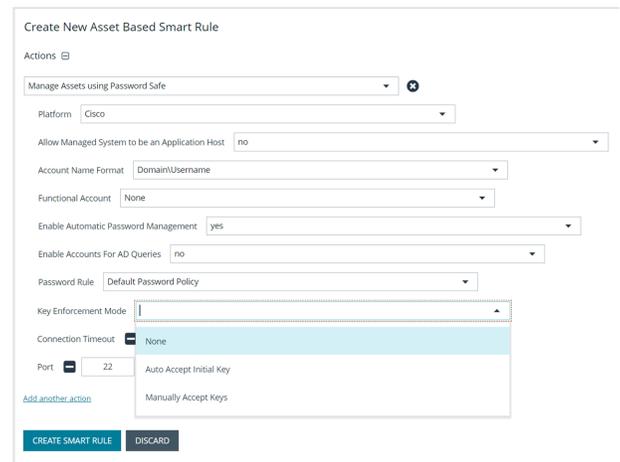


Note: For managed systems that are linked to assets, you can click the **View Asset** link in the upper left to view the details of the asset. Click **View Managed System** to return the **Advanced Details** for the managed system.

Import an SSH Server Key Using a Smart Rule

You can import SSH Server keys from a host and accept the key on the **Advanced Details** for a managed system. Supported key types are RSA, DSA, and ECDSA. From the **Smart Rules** page, create an asset-based Smart Rule using **Actions** settings such as the below:

1. Select **Manage Asset Using Password Safe** from the dropdown.
2. Select a **Platform** that supports server keys, such as **Cisco**.
3. Select the **Functional Account**.
4. For the **Key Enforcement Mode** option, choose either **Auto Accept Initial Key** or **Manually Accept Keys**.
5. Set the other settings as desired or leave as defaults.
6. Add another action to **Show Asset as Smart Group**.
7. Click **Create Smart Rule**.




Note: The settings here are the same as when adding a system on the **Create Managed Systems** page. For descriptions for all the settings, please see ["Add a Managed System Manually" on page 17](#).

Manage the SSH Server Keys

After the Smart Rule processes, hosts with SSH server keys are populated in the Smart Group you created.

An email notification is sent to the **Administrators** user group when a key is imported and the **Key Enforcement Mode** is set to **Manually Accepted Keys**. The email notifies the administrators that a fingerprint requires action, what asset the key is on, and also provides details about the fingerprint.

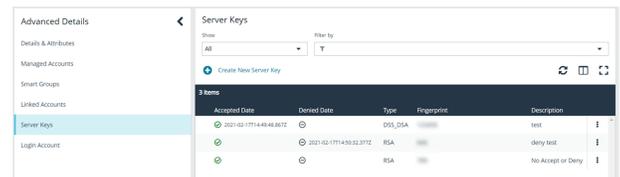
The **Fingerprint Verification** email template can be modified from **Configuration > Privileged Access Management > Mail Templates**.



For more information on modifying email templates, please see ["Customize Email Notifications" on page 165](#).

Accept or Deny a Key

1. From the **Managed Systems** page, click the vertical ellipsis for the managed system.
2. Select **Go to Advanced Details**.
3. Click the **Server Keys** tab.
4. Click the vertical ellipsis for the server key you wish to work with.
 - If auto approved, no further action is required.
 - If manually approved, click **Accept** or **Deny**.



Accepted Date	Denied Date	Type	Enforcement	Description
2021-02-10T14:48:48.812Z		DOS_DSA	Auto	Test
	2021-02-10T14:50:32.207Z	RSA	Manually	deny test
		RSA	Manually	No Accept or Deny

5. After a key is accepted, from the **Functional Accounts** tab, click the **Test Functional Account** button to verify the key with the functional account.

Add a Key Manually

1. From the **Managed Systems** page, click the vertical ellipsis for the managed system.
2. Select **Go to advanced details....**
3. Click the **Server Keys** tab.
4. Click **+ Create New Server Key** above the grid.
5. Click **Accept** or **Deny**.
6. Select a **Key Type** from the list and enter a **Fingerprint** and a **Description**.
7. Click **Create Key**.
8. After a key is added, from the **Functional Accounts** tab, click the **Test Functional Account** button to verify the key with the functional account.



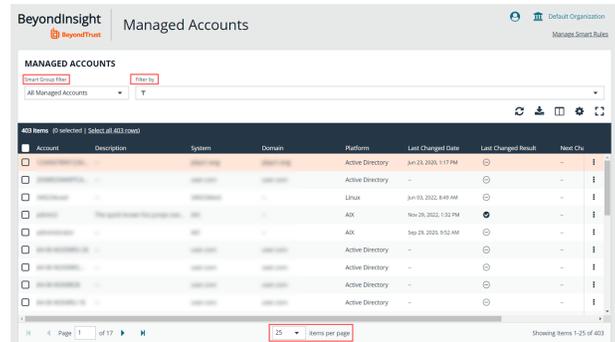
Note: The fingerprint must be unique. An error message is displayed if the key is already imported.

Work with Managed Accounts

Managed accounts are user accounts which are local or active directory accounts on the managed system.

View Managed Accounts

When viewing managed accounts, you can change the number of items displayed on the page using the **Items per page** dropdown at the bottom of the grid. You can use the filters above the grid to filter the list by smart group and the various attributes listed in the **Filter by** dropdown.



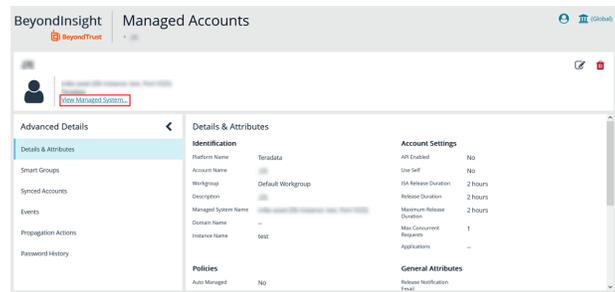
View Managed Account Details

After the account is added to Password Safe management, you can:

- Review the attributes and settings assigned to the account, such its identifying details, settings, and policies.
- View managed systems linked to the account.
- View Smart Groups associated with the account, as well as their last process date and processing status.
- See which accounts are synced to the managed account.
- View a list of password changes and the reason for each change.

To view details on a specific managed account:

1. From the **Managed Accounts** page, click the vertical ellipsis for the account.
2. Select **Go to Advanced Details**.
3. Managed account details, such as identification information, account settings, policies and attributes are displayed under **Details & Attributes** for quick access.
4. To see more granular details, click through the tabs in the **Advanced Details** pane to view details on each topic.



Tip: Click the **View Managed System** link above the grid to view the advanced details for the managed system associated with the managed account. To return to the advanced details for the managed account, click the **View Managed Account** link.

i For more information on propagation actions, please see "[Add Propagation Actions to Managed Accounts](#)" on page 86.

Delete Managed Accounts

Managed accounts can be deleted, except for synced accounts. A message is displayed if an account cannot be deleted.

1. From the menu, select **Managed Accounts**.
2. Select the account or multiple accounts you want to delete, and then click the **Delete** button above the grid.

MANAGED ACCOUNTS

Smart Group filter: All Managed Accounts (dropdown) | Filter by: [input]

Buttons: Add To Smart Group, Refresh, Sync, Delete

173 items (3 selected | [Select all 173 rows](#))

Account	Description	System
<input checked="" type="checkbox"/>	[blurred]	[blurred]
<input checked="" type="checkbox"/>	[blurred]	[blurred]
<input checked="" type="checkbox"/>	[blurred]	[blurred]

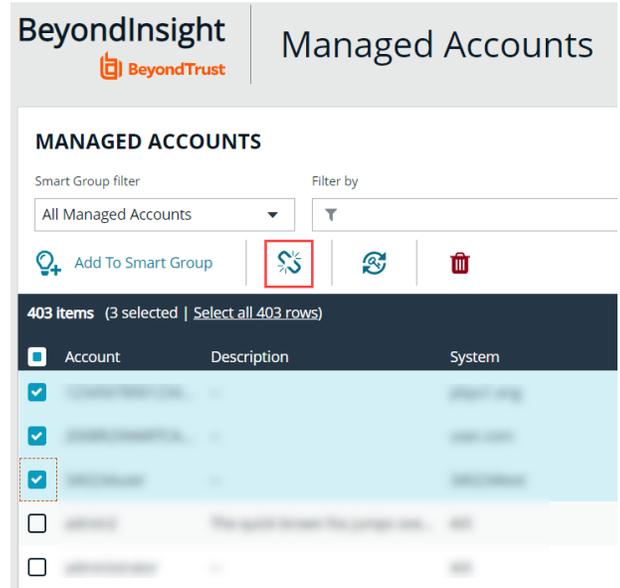
3. Click **Delete** on the confirmation message.

Unlink Managed Accounts

You can unlink managed accounts from managed systems; however, this applies to Active Directory accounts only. If accounts included in the unlink selection are not domain accounts, no action is taken on those accounts.

1. From the menu, select **Managed Accounts**.

2. Select the account or multiple accounts you want to unlink, and then click the **Unlink** button above the grid.

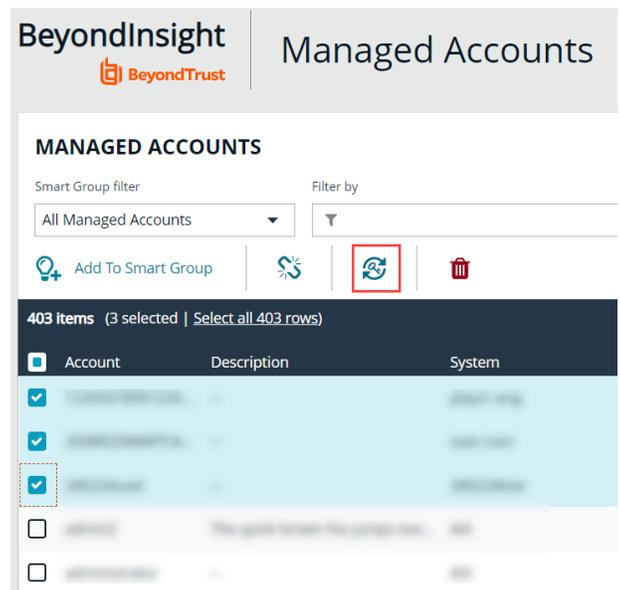


The screenshot shows the 'Managed Accounts' page in the BeyondTrust interface. At the top, there's a header with the BeyondTrust logo and the title 'Managed Accounts'. Below this, there's a section titled 'MANAGED ACCOUNTS' with a 'Smart Group filter' dropdown set to 'All Managed Accounts' and a 'Filter by' search box. A row of action buttons is visible: 'Add To Smart Group', 'Unlink' (highlighted with a red box), 'Refresh', and 'Delete'. Below the buttons, it says '403 items (3 selected | Select all 403 rows)'. A table with columns 'Account', 'Description', and 'System' is shown, with three rows selected (indicated by blue checkmarks in the first column).

3. Click **Unlink** on the confirmation message.

Change Passwords for Managed Accounts

1. From the menu, select **Managed Accounts**.
2. Select the account or multiple accounts for which you want to change the password, and then click the **Change Password** button above the grid.



This screenshot is identical to the one above, showing the 'Managed Accounts' page. In this instance, the 'Change Password' button (represented by a circular arrow icon) is highlighted with a red box, while the 'Unlink' button is not.

3. Click **Change Password** on the confirmation message.

Configure Subscriber Accounts

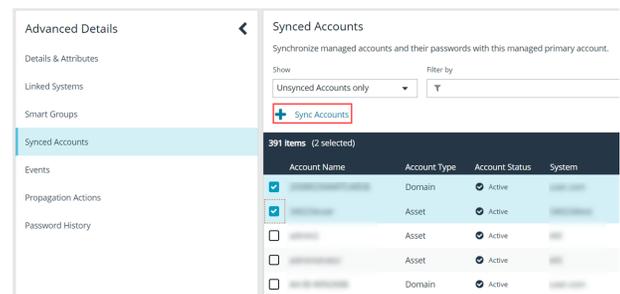
Any managed account can be synced to multiple accounts. These synced accounts become subscribers to the managed account. The managed account and all of its subscribers always share an identical password. When the password of the managed account or any of the subscriber accounts is changed, Password Safe automatically changes the password of the primary managed account and all of its subscribers to a new password.

Once an account is synchronized as a subscriber account, settings modifications are limited to:

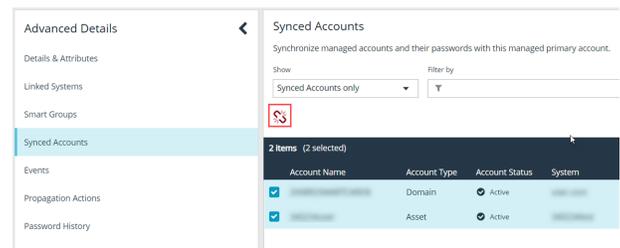
- Enable API
- Allow for scanning
- Application

To sync an account:

1. From the **Managed Accounts** page, click the vertical ellipsis button for the account.
2. Select **Go to Advanced Details**.
3. Under **Advanced Details**, click **Synced Accounts**.
4. Select the account or multiple accounts that you want to sync.
5. Click **Sync Accounts** above the grid.



6. To remove a synced account, select the account, and then click the **Unsync Accounts** button above the grid.



Configure Password Reset for Managed Account Users

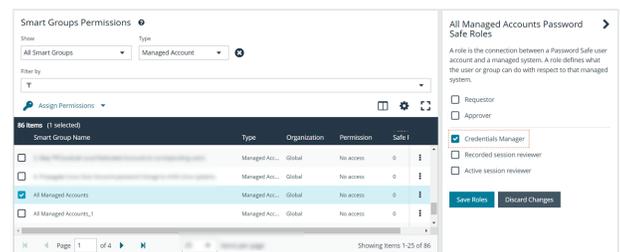
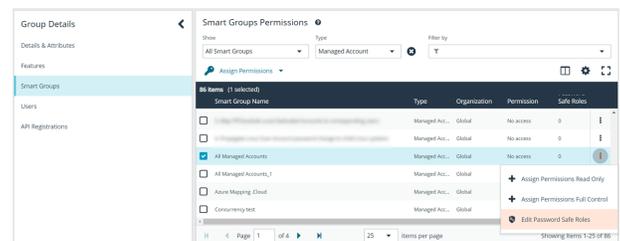
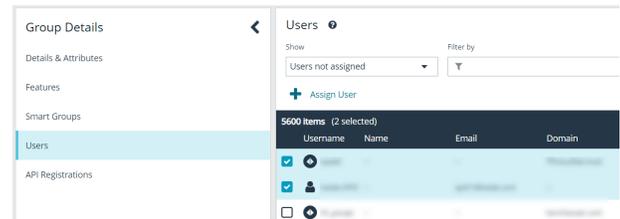
You can grant managed account users permission to reset the password on their own managed account, without granting them permission to reset passwords on other managed accounts. You can do this by creating a group, adding the managed account to the group, and then assigning permissions and the **Credential Manager** role to the group.

1. In the BeyondInsight console, go to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **Create New Group**.
3. Select **Create a New Group**.
4. Provide a name and description for the group, and then click **Create Group**.

5. From the **Group Details** pane, select **Users**.
6. Select users to add to the group, and then click **Assign User** above the grid.

7. From the **Group Details** pane, select **Features**.
8. Select the **Management Console Access** and **Password Safe Account Management** features, and then click **Assign Permissions**.
9. Select **Assign Permissions Read Only**. Do not grant **Full Control**.
10. From the **Group Details** pane, select **Smart Groups**.
11. Filter the list of Smart Groups by **Type > Managed Account**.
12. Select the Smart Group that contains the applicable managed accounts.
13. Click the vertical ellipsis button for the Smart Group, and then select **Edit Password Safe Roles**.

14. Select the **Credentials Manager** role, and then click **Save Roles**.



The managed account user can now log in to the console and reset the password for the managed account as follows:

1. Go to the **Managed Accounts** page.
2. Select the account.
3. Click the vertical ellipsis button for the account.
4. Select **Change Password**.

Use a Managed Account as a Discovery Scan Credential

A managed account can be used as a credential when configuring a Discovery Scan.



Note: Once the **Scanner** option is enabled, the key must be specified again if the account is edited. It may be the same key or a new one.

The following credential types are supported:

- Windows,
- SSH

- MySQL
- Microsoft SQL Server.

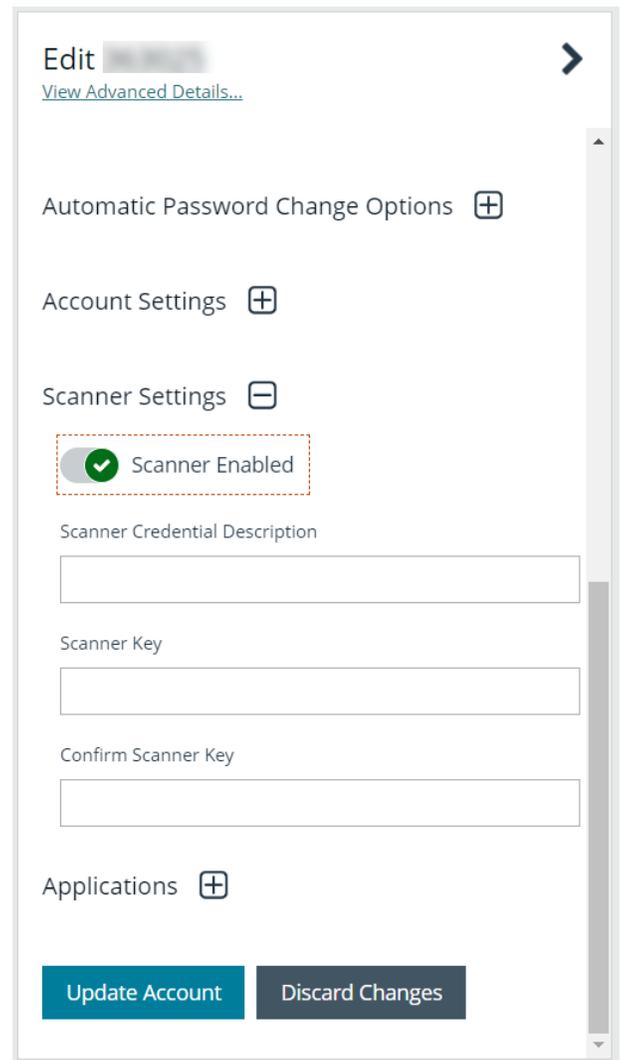
The following platforms are supported:

- Windows
- MySQL
- Microsoft SQL Server
- Active Directory
- Any platform with the **IsUnix** flag (AIX, HP UX, DRAC, etc.)

To add the managed account as a scan credential:

1. From the **Managed Accounts** page, click the vertical ellipsis button for the account.
2. Select **Edit Account**.
3. Expand **Scanner Settings**.
4. Click the toggle to enable the scanner.
5. For the **Scanner Credential Description**, enter a name for the account that can be selected as the credential when setting up the scan details. The name is displayed on the **Credentials Management** dialog box when setting up the scan.
6. Assign and confirm a key so that only users that know the key can use the credential for scanning.
7. Click **Update Account**.

i For more information on configuring credentials, please see [Add Credentials for Use in Scans](#) in the [BeyondInsight User Guide](#).



Edit [Account Name] ➔

[View Advanced Details...](#)

Automatic Password Change Options +

Account Settings +

Scanner Settings +

Scanner Enabled

Scanner Credential Description

Scanner Key

Confirm Scanner Key

Applications +

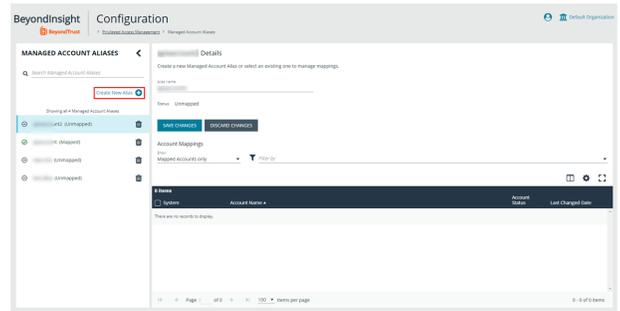
Update Account **Discard Changes**

Managed Account Aliasing

Aliases are accessible using the API only. Account mappings can be changed without affecting the alias name. At least one managed account is required to be mapped for the alias to be active; when an alias has two or more managed accounts mapped, it is considered to be highly available. An account can only be mapped to one alias. Managed account aliases can be accessed from **Configuration > Privileged Access Management > Managed Account Aliases**.

Create a New Alias

1. Navigate to **Configuration > Privileged Access Management > Managed Account Aliases**.
2. Click **Create New Alias +**.
3. Enter a name, and then click **Create Alias**.



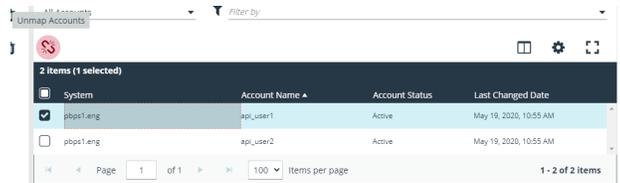
The new alias appears in the grid under **Account Mappings**, which displays all aliases ready to be mapped. New aliases show as **Unmapped** until they are associated with accounts.

Note: Each managed account can only be mapped to a single alias.

You can use the dropdown to select which accounts to display: **All Accounts**, **Mapped**, or **Unmapped Accounts** only.

The **Filter-by** allows you to filter accounts by **System**, **Account Name**, **Account Status**, or **Last Changed Date**.

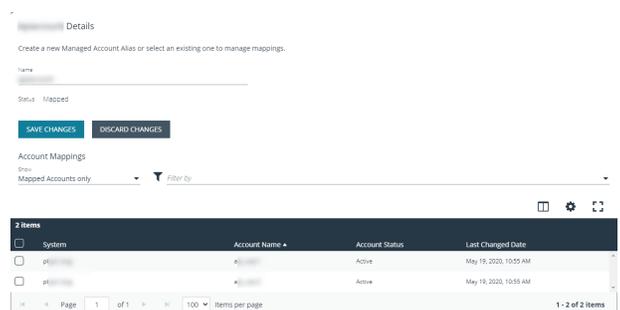
To unmap an account, select the account and click the broken link icon.



Mapped accounts have three status values:

- **Active:** The account credentials are current and can be requested.
- **Pending:** The account credentials are current but the password is queued to change.
- **Inactive:** The account password is changing.

The list of mapped accounts is rotated in a round-robin fashion, typically in order of last password change date. The preferred account, or the account whose status is active and has the oldest change date, is returned on the Alias API model.



Disabled at Rest Managed Accounts

Just-in-Time (JIT) is a critical aspect of controlling access to assets and identities within an organization. When flagged by a Password Safe administrator, Active Directory and Entra ID accounts can leverage JIT capabilities by disabling these accounts when checked in to Password Safe. When a requestor checks out an account, a workflow is initiated that re-enables the account for use. Once checked back in, the account is disabled again.

When enabling or disabling an account, Password Safe uses the **Preferred Domain Controller (DC)**, if set, for the managed account.



Note: The **Disabled at Rest** feature is only available for Active Directory (AD) and Entra ID accounts.



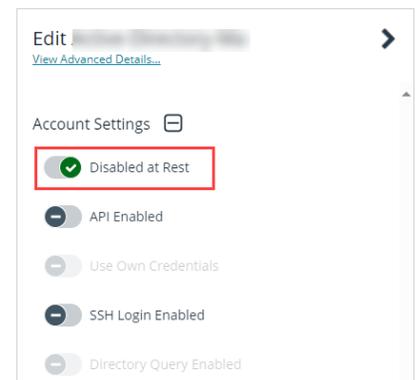
For more information, please see [Register and Configure an Application in Entra ID](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/azure-ad-app-registration.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/azure-ad-app-registration.htm>.

Enable the Disabled at Rest Setting

The **Disabled at Rest** setting can be activated by using a toggle switch, located in **Managed Accounts > Account Settings**, or by creating a Smart Rule.

Enable Disabled at Rest with Toggle Switch

1. From the left hand menu in the BeyondInsight console, click **Managed Accounts**.
2. Select a managed account and then click the vertical ellipsis to the right of the account.
3. From the menu, select **Edit Account**.
4. Under **Account Settings**, click the **Disabled at Rest** toggle switch to enable the setting.
5. Click **Update Account**.

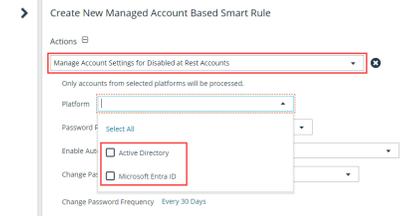


Create a Smart Rule for Disabled at Rest Accounts

In addition to setting the **Disabled at Rest** option in an individual managed account, you can also set the **Disabled at Rest** flag by creating a smart rule. The flag automatically turns on the **Disabled at Rest** setting for all matching accounts included in the smart rule, as follows:

1. From the left menu in the BeyondInsight console, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule Type Filter** dropdown.

3. Click **Create Smart Rule**.
4. Select **Managed Account Settings for Disabled at Rest Accounts** from the first dropdown under **Actions**.
5. Under **Platform**, select either **Active Directory** or **Microsoft Entra ID**.
6. Complete the smart rule, and then select **Create Smart Rule**.



IMPORTANT!

If the **Disabled At Rest** setting is set at the account level, it is overwritten by the **Manage Account Settings** action in a Smart Rule, which sets **Disabled at Rest** for all affected accounts to **No**. You must use the **Manage Account Settings for Disabled At Rest Accounts** action instead, which sets **Disabled at Rest** for all affected accounts to **Yes**.


Note:

- Concurrent accounts, those that are used by multiple users, are disabled only after the account is no longer in use by anyone.
- The **Disabled at Rest** feature is not supported with Password Cache. This service checks out the account it is configured for and keeps a cache locally. The cache is an active request, meaning the cached account is enabled, and it will stay enabled.

Verify Disabled at Rest Setting

Verify that the **Disabled at Rest** setting is enabled, as follows:

1. Click the vertical ellipsis to the right of the account that was updated.
2. From the menu, select **Go to Advanced Details**.
3. Under **Details & Attributes > Account Settings**, **Disabled at Rest** should be set to **Yes**.

Changes can also be viewed under **User Audits**, as follows:

1. Go to **Configuration > General > User Audits**.
2. Click the information icon to the right of the updated item. The **Edit Details** pane displays the action that was taken and the changes made.

Sample Disabled At Rest Workflow Description

Disabled accounts are temporarily enabled when a new Password Safe request is made. Using the **View Password** request as an example, view the workflow, as follows:

- Click the left menu in the BeyondInsight console and click **Password Safe**.
- Go to **Accounts > Directory Linked Accounts**.
- Click **Access** (key icon) to the right of the request.
- In the **Access** pane, under **Quick Launch**, set the time length of the session.

- Click **Retrieve Password**.
 - The account is now enabled.
 - It remains enabled for the duration of the session. If the user checks-in the request or the request expiry time is reached (whichever comes first), the account is queued to be disabled.



Note: When enabling the **Disable at Rest** feature on a managed account, the account is set to disabled in AD or Entra ID. If the account does not become disabled, a check out/check in may be required.

Affected Settings

When your account is set to **Disabled at Rest**, the following settings are not available:

- **Account Settings > Use Own Credentials.**
- **Account Settings > Directory Query Enabled**
- **Scanner Settings > Scanner Enabled**
- **Managed Account > Advanced Details > Propagation Actions**
- **Test Password** is not available in the ellipsis menu.



For more information about site replication considerations when leveraging the **Disable at Rest** feature, please refer to your Active Directory administrators.

Disabled at Rest Managed Accounts

Just-in-Time (JIT) is a critical aspect of controlling access to assets and identities within an organization. When flagged by a Password Safe administrator, Active Directory and Entra ID accounts can leverage JIT capabilities by disabling these accounts when checked in to Password Safe. When a requestor checks out an account, a workflow is initiated that re-enables the account for use. Once checked back in, the account is disabled again.

When enabling or disabling an account, Password Safe uses the **Preferred Domain Controller (DC)**, if set, for the managed account.



Note: The **Disabled at Rest** feature is only available for Active Directory (AD) and Entra ID accounts.



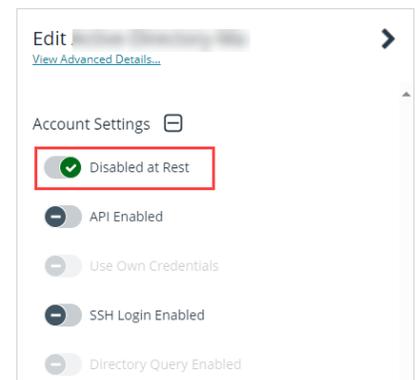
For more information, please see [Register and Configure an Application in Entra ID](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/azure-ad-app-registration.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/azure-ad-app-registration.htm>.

Enable the Disabled at Rest Setting

The **Disabled at Rest** setting can be activated by using a toggle switch, located in **Managed Accounts > Account Settings**, or by creating a Smart Rule.

Enable Disabled at Rest with Toggle Switch

1. From the left hand menu in the BeyondInsight console, click **Managed Accounts**.
2. Select a managed account and then click the vertical ellipsis to the right of the account.
3. From the menu, select **Edit Account**.
4. Under **Account Settings**, click the **Disabled at Rest** toggle switch to enable the setting.
5. Click **Update Account**.

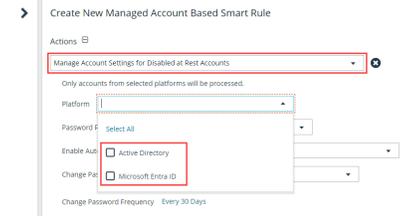


Create a Smart Rule for Disabled at Rest Accounts

In addition to setting the **Disabled at Rest** option in an individual managed account, you can also set the **Disabled at Rest** flag by creating a smart rule. The flag automatically turns on the **Disabled at Rest** setting for all matching accounts included in the smart rule, as follows:

1. From the left menu in the BeyondInsight console, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule Type Filter** dropdown.

3. Click **Create Smart Rule**.
4. Select **Managed Account Settings for Disabled at Rest Accounts** from the first dropdown under **Actions**.
5. Under **Platform**, select either **Active Directory** or **Microsoft Entra ID**.
6. Complete the smart rule, and then select **Create Smart Rule**.



IMPORTANT!

If the **Disabled At Rest** setting is set at the account level, it is overwritten by the **Manage Account Settings** action in a Smart Rule, which sets **Disabled at Rest** for all affected accounts to **No**. You must use the **Manage Account Settings for Disabled At Rest Accounts** action instead, which sets **Disabled at Rest** for all affected accounts to **Yes**.


Note:

- Concurrent accounts, those that are used by multiple users, are disabled only after the account is no longer in use by anyone.
- The **Disabled at Rest** feature is not supported with Password Cache. This service checks out the account it is configured for and keeps a cache locally. The cache is an active request, meaning the cached account is enabled, and it will stay enabled.

Verify Disabled at Rest Setting

Verify that the **Disabled at Rest** setting is enabled, as follows:

1. Click the vertical ellipsis to the right of the account that was updated.
2. From the menu, select **Go to Advanced Details**.
3. Under **Details & Attributes > Account Settings**, **Disabled at Rest** should be set to **Yes**.

Changes can also be viewed under **User Audits**, as follows:

1. Go to **Configuration > General > User Audits**.
2. Click the information icon to the right of the updated item. The **Edit Details** pane displays the action that was taken and the changes made.

Sample Disabled At Rest Workflow Description

Disabled accounts are temporarily enabled when a new Password Safe request is made. Using the **View Password** request as an example, view the workflow, as follows:

- Click the left menu in the BeyondInsight console and click **Password Safe**.
- Go to **Accounts > Directory Linked Accounts**.
- Click **Access** (key icon) to the right of the request.
- In the **Access** pane, under **Quick Launch**, set the time length of the session.

- Click **Retrieve Password**.
 - The account is now enabled.
 - It remains enabled for the duration of the session. If the user checks-in the request or the request expiry time is reached (whichever comes first), the account is queued to be disabled.



Note: When enabling the **Disable at Rest** feature on a managed account, the account is set to disabled in AD or Entra ID. If the account does not become disabled, a check out/check in may be required.

Affected Settings

When your account is set to **Disabled at Rest**, the following settings are not available:

- **Account Settings > Use Own Credentials.**
- **Account Settings > Directory Query Enabled**
- **Scanner Settings > Scanner Enabled**
- **Managed Account > Advanced Details > Propagation Actions**
- **Test Password** is not available in the ellipsis menu.



For more information about site replication considerations when leveraging the **Disable at Rest** feature, please refer to your Active Directory administrators.

Work with Smart Rules

You can use Smart Groups to add assets, systems, and accounts into Password Safe management. The Smart Rule filters that you configure for the Smart Groups determine the assets that are added as managed systems and managed accounts in Password Safe.

There are four types of Smart Rules available with a Password Safe license: **Asset**, **Managed Account**, **Managed System**, and **Policy User**.

You can use Smart Rules to add the following types of assets:

- Systems
- Network Devices
- Databases
- Local Linux and Windows accounts
- Active Directory accounts
- Dedicated accounts



Note: The settings in a Smart Rule override the settings configured on the managed system.



For more information on using Smart Rules, please see the [BeyondInsight User Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/smart-rules/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/smart-rules/index.htm>.

Predefined Smart Groups

By default there are Smart Groups already defined and created.

The following tables list Smart Groups useful in Password Safe environments.

Asset Based Smart Groups

Smart Group	Category	Definition
All Assets in Password Safe	Assets and Devices	All assets under Password Safe management.
Recent Assets not in Password Safe	Assets and Devices	All assets discovered in the last 30 days that have not yet been added to Password Safe.
Recent Non Windows Assets not in Password Safe	Assets and Devices	All non Windows assets discovered in the last 30 days that have not yet been added to Password Safe.
Recent Windows Servers not in Password Safe	Servers	Windows servers discovered in the last 30 days that have not yet been added to Password Safe.
Recent Virtual Servers not in Password Safe	Virtualized Devices	Virtualized server assets discovered in the last 30 days that have not yet been added to Password Safe.



Note: Virtual machine processing within Smart Rules has been deprecated as of BeyondInsight and Password Safe 24.1. For upgrades to the BeyondInsight and Password Safe 24.1 release, the **Virtualized Devices** category for Smart Rules still displays in the UI; however, any Smart Rules based on this category are marked as inactive. For upgrades to the 24.1 release, **Child Smart Rule** filters that use any of the following built-in rules are removed:

- Microsoft Hyper-V
- Parallels
- Recent Virtual Servers not in Password Safe
- Virtual Servers
- Virtual Workstations
- VMware vSphere
- Xen

Managed System Smart Rules

Smart Rule	Category	Definition
Database Managed Systems	Types	Database Managed Systems
Directory Managed Systems	Types	Directory Managed Systems
Cloud Managed Systems	Types	Cloud Managed Systems
Asset Managed Systems	Types	Asset Managed Systems
All Managed Systems associated with BeyondInsight Assets	Managed Systems	All Managed Systems associated with BeyondInsight Assets
All Managed Systems not associated with BeyondInsight Assets	Managed Systems	All Managed Systems not associated with BeyondInsight Assets
All Managed Systems	Managed Systems	All Managed Systems
Recently Added Managed Systems	Managed Systems	Managed Systems added less than 30 days ago

Managed Accounts Smart Groups

Smart Group	Definition
All Managed Accounts	All accounts managed by Password Safe.
Recently Added Managed Accounts	Filters on managed accounts added less than 30 days ago.
Database Managed Accounts	Filters on the database platform and includes SQL Server and Oracle platforms.
Hardware Device Managed Accounts	Filters on hardware devices including Dell DRAC and HP iLO platforms.
Linux Managed Accounts	Filters on the Linux platform.

Mac Managed Accounts	Filters on the macOS platform.
Unix Managed Accounts	Filters on the Unix platform.
Windows Managed Accounts	Filters on the Windows platform.

Considerations When Designing Smart Rules

- The filter criteria is processed hierarchically. When creating the filter structure, place the filters that reduce the largest number of entities at the top of the hierarchy.
- When adding Active Directory accounts using a directory query, ensure the query is as restrictive as possible. For example, configure the query on a smaller set of data in your environment.
- When adding assets to Password Safe, be cautious about creating more than one Smart Rule with the same systems or accounts. If the Smart Rules have different actions, they will start continually overwriting each other in an endless loop.
- There can be delays when a Smart Rule depends on external data source, such as LDAP, as processing can take longer. For example, a directory query that uses the discover accounts feature (managed account Smart Rule) or discover assets feature (asset-based Smart Rule).

Smart Rule Processing

A Smart Rule processes and updates information in Smart Groups when certain actions occur, such as the following:

- The Smart Rule is created, or edited and saved.
- A timer expires.
- You manually kick off the processing by selecting the Smart Rule from the grid on the **Smart Rules** page, and then click **Process**.



Note: The **Process** action from the grid on the **Smart Rules** page does not apply to managed account and managed system Quick Group Smart Rules, because these only run once upon creation and cannot be triggered to run again.

- A Smart Rule with Smart Rule children triggers the children to run before the parent completes.
- Managed account Smart Rules with selection criteria **Dedicated Account** process when a change to a mapped group is detected. This can occur in the following scenarios:
 - A new user logs on.
 - The group refreshes in Active Directory by an administrator viewing or editing the group in **Configuration > Role Based Access > User Management**.

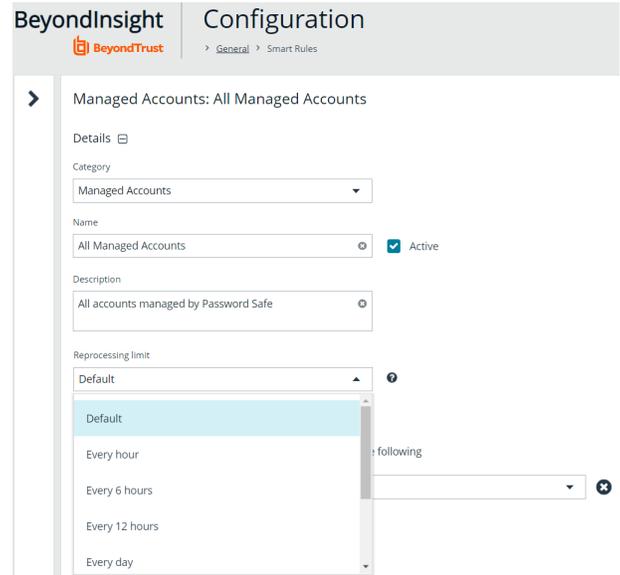
Change the Processing Frequency for a Smart Rule

By default, Smart Rules process when asset changes are detected. The assets in the Smart Rule are then dynamically updated. For Smart Rules that require more intensive processing, you might want Smart Rules to process less frequently.

To provide more restrictive processing, you can select alternate frequency settings to override the default processing. The Smart Rules process in the selected time frame (for example, the rule processes once a week).

When creating a new Smart Rule or updating an existing one, select your desired frequency from the **Reprocessing limit** list in the **Details** section.

 **Note:** A Smart Rule is always processed when first saved or updated.



View and Select Smart Rules Processing Statistics

The Smart Rules grid displays some processing statistics by default. Additional Smart Rules processing statistics, such as **Processed Date**, **Successful Attempts**, and **Failed Attempts** are available and can be displayed in the Smart Rules grid.

To add this information to the grid:

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Click the **Column chooser** icon in the upper right of the grid.
3. Click the desired column to add that information to the grid.
 - Check marks indicate columns currently displayed.
 - You can remove a displayed column by clicking the column name in the **Column chooser** list.
 - If there are more columns displayed than can fit in the width of the screen, a scroll bar appears at the bottom of the grid. It may be necessary to scroll sideways to view any additional columns.

Use Dedicated Account Smart Rule

A dedicated account Smart Rule allows you to dynamically map dedicated administrative accounts outside of BeyondInsight to users in a BeyondInsight group. This allows a lower privileged BeyondInsight user to access a higher privileged user's account temporarily while using Password Safe.

The below procedures provide instructions for configuring BeyondInsight users with the ability to access a dedicated directory account's credentials, using a query matching on directory attributes. Once configured, the users are able to request a password checkout for the dedicated account from the Password Safe portal. The user can then access resources using the dedicated account credentials.

You must configure the following in BeyondInsight:

- Create a directory query to retrieve the directory account as well as its attributes.
- Create a Smart Rule to run the directory query to find the account and its directory attributes, and add it as a managed account in Password Safe.
- Create a Smart Rule to map the dedicated account to a user group in BeyondInsight.
- Assign user group permissions to the two newly created Smart Rules.

Create the Directory Query

1. Navigate to **Configuration > Role Base Access > Directory Queries**.
2. Click **+ Create New Directory Query**, and complete form as follows:
 - **Directory Type:** Leave as **Active Directory**.
 - **Title:** Provide a meaningful name that allows for easy identification of the query.
 - **Credentials:** Select a credential that has permissions to query the directory user accounts.
 - **Query Target:** Provide the LDAP path to the target.
 - **Scope:** Leave as **This Object and All Child Objects**.
 - **Object Type:** Select **User Objects**.
 - **Dynamically refresh results each use:** Leave enabled.
 - **Basic Filter:** Provide the name of the dedicated account.
3. Click **Create Directory Query**.

New Directory Query

Directory Type
Active Directory

Title
Dedicated Account Directory Query

Credentials
Credential
Active Directory [Create New Credential...](#)

Query Target
Path
LDAP://exampledomain.local/CN=Users.DC [BROWSE](#)

Scope
This Object And All Child Objects

Object Type
Computer Objects

Dynamically refresh results each use.

BASIC FILTER

A "*" wildcard character may be used anywhere in the name and description to match multiple values.

Name
Denise.sa

Description

[TEST](#)

Query Test Results
Results limited to first 100 for preview

0 items		
Name	Type	Description
There are no records to display.		

[CREATE DIRECTORY QUERY](#) [DISCARD](#)

Create the Smart Rule to Run the Directory Query and Add Managed Account



Note: This example is specific to managed accounts. Similar instructions apply for the other rule or entity types

1. From the left menu, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule type** filter dropdown.
3. Click **+ Create Smart Rule**.
4. Configure the Smart Rule as follows:
 - **Category:** Select **Managed Accounts**.
 - **Name:** Provide a meaningful name that allows for easy identification of the Smart Rule.
 - **Selection Criteria:**
 - Select **Directory Query** from the dropdown.
 - Leave **Include accounts from Directory Query** selected.
 - Select the directory query created in above steps.
 - Leave **Discover accounts for Password Safe Management** enabled.
 - Select the **Domain** from the dropdown.
 - **Actions:**
 - Select **Manage Account Settings** from the dropdown and set its related options as desired.
 - Add another action and select **Show managed account as Smart Group** from the dropdown.
 - Add another action and select **Link domain accounts to Managed Systems** from the dropdown, and then select your desired **Asset or Managed System Smart Group** from the dropdown.
5. Click **Create Smart Rule**.

Create New Managed Account Based Smart Rule

Details ▾

Category: Managed Accounts ▾

Name: Dedicated Account Query Smart Rule Active

Description:

Reprocessing limit: Default ▾ ⓘ

Selection Criteria ▾

Include items that match ALL ▾ of the following

Directory Query ▾ ⊕

Include accounts from Directory Query ▾

Dedicated Account Directory Query ▾

Re-run the query every X hours: 0 ⊖ ⊕

Discover accounts for Password Safe Management

Domain: example.com ▾

[Add another condition](#) [Add a new group](#)

Actions ▾

Manage Account Settings ▾ ⊕

Password Rule: Default Password Policy ▾

Enable Automatic Password Management: no ▾

Default Release Duration: Days: 0 Hours: 2 Minutes: 0

Maximum Release Duration: Days: 0 Hours: 2 Minutes: 0

ISA Default Release Duration: Days: 0 Hours: 2 Minutes: 0

Max Concurrent Request: 1 ⊖ ⊕

Account Options:

Email release notifications to:

Show managed account as Smart Group ▾ ⊕

Link domain accounts to Managed Systems ▾ ⊕

Asset or Managed System Smart Group: Asset Managed Systems - (Managed System group) ▾

[Add another action](#)

Create Smart Rule **View Results** **Discard**



Tip: To view the contents of a Smart Rule when creating a new rule or editing an existing rule:

- Once the rule is saved, click **View Results**.
- You are taken to the associated grid, where the contents of the Smart Rule are listed.
- If the rule is actively processing, a banner displays letting you know that.


Note:

- **View Results** displays only if you have permissions to the grid corresponding to the Smart Rule, i.e.; Assets, Managed Accounts, Managed Systems.
- The Smart Rule must be saved with **Show <entity> as Smart Group** selected under **Actions** to view the results.



Tip: Because the Smart Rule must process to display the contents in the grid, we recommend viewing the results using only the **Show <entity> as Smart Group** action and before adding additional actions that may make changes to accounts and assets in your network.

Once you have confirmed the rule contains your desired items, you can then add additional actions to the Smart Rule.

Create the Smart Rule to Map the Dedicated Account to the User Group

1. From the left navigation pane, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule type** filter dropdown.
3. Click **+ Create Smart Rule**.
4. Configure the Smart Rule as follows:
 - **Category:** Select **Managed Accounts**.
 - **Name:** Provide a meaningful name that allows for easy identification of the Smart Rule.
 - **Selection Criteria:**
 - Select **Dedicated Account** from the dropdown.
 - Select **Directory Attribute Match** from the dropdown.
 - Select the directory attribute you wish to match.
 - **Actions:**
 - Select **Show managed account as Smart Group** from the dropdown.
 - Add another action and select **Map Dedicated Accounts to** from the dropdown.
 - Select the applicable **User Group** to map to.
5. Click **Create Smart Rule**.

Managed Accounts: Dedicated Account Mapping Smart Rule

Details

 Category
 Managed Accounts

 Name
 Dedicated Account Mapping Smart Rule Active

 Description

 Reprocessing limit
 Default

Selection Criteria

 Include items that match ALL of the following

- Dedicated Account
- Directory Attribute Match
- employeeNumber

[Add another condition](#) [Add a new group](#)

Actions

- Show managed account as Smart Group
- Map Dedicated Accounts To
- User Group: LowPriv

[Add another action](#)



Tip: To view the contents of a Smart Rule when creating a new rule or editing an existing rule:

- Once the rule is saved, click **View Results**.
- You are taken to the associated grid, where the contents of the Smart Rule are listed.
- If the rule is actively processing, a banner displays letting you know that.



Note:

- **View Results** displays only if you have permissions to the grid corresponding to the Smart Rule, i.e.: Assets, Managed Accounts, Managed Systems.
- The Smart Rule must be saved with **Show <entity> as Smart Group** selected under **Actions** to view the results.

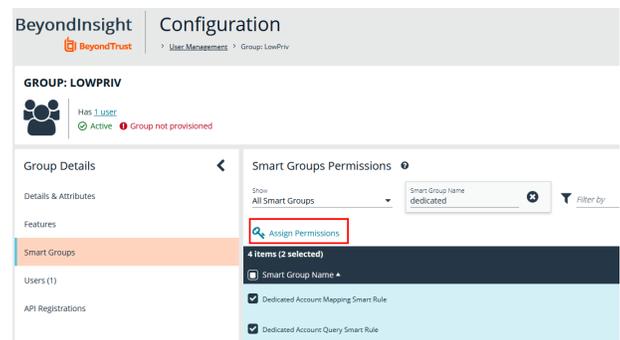


Tip: Because the Smart Rule must process to display the contents in the grid, we recommend viewing the results using only the **Show <entity> as Smart Group** action and before adding additional actions that may make changes to accounts and assets in your network.

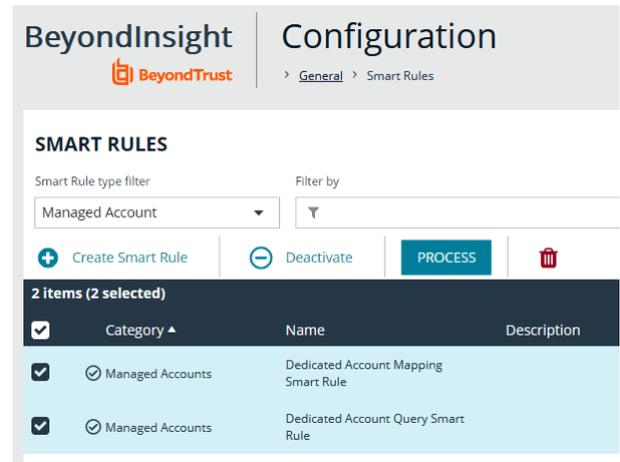
Once you have confirmed the rule contains your desired items, you can then add additional actions to the Smart Rule.

Assign User Group Permissions to the Smart Rules

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Locate the user group you had selected when creating the Smart Rule for dedicated account mapping.
3. Click the vertical ellipsis for the group, and then select **View Group Details**.
4. In the **Group Details** pane, click **Smart Groups**.
5. In the **Smart Group Permissions** pane, select the two dedicated account smart groups you created.
6. Click **Assign Permissions > Assign Permissions Read Only** above the grid.



From the **Smart Rules** page, process the two newly created smart groups. After processing, the dedicated account discovered by the directory query is listed on the **Managed Accounts** page. Users belonging to the group you chose to map the dedicated account to are indicated in the **Mapped to User** column. You might need to add this column to the grid using the **Column Chooser** button above the grid.



Use an Entra ID Smart Rule

An Entra ID Smart Rule enables Password Safe to automatically discover Entra ID accounts. This allows privileged accounts in Entra ID to be managed, including password rotation and check-in and check-out.

Follow the steps below to discover Entra ID accounts.

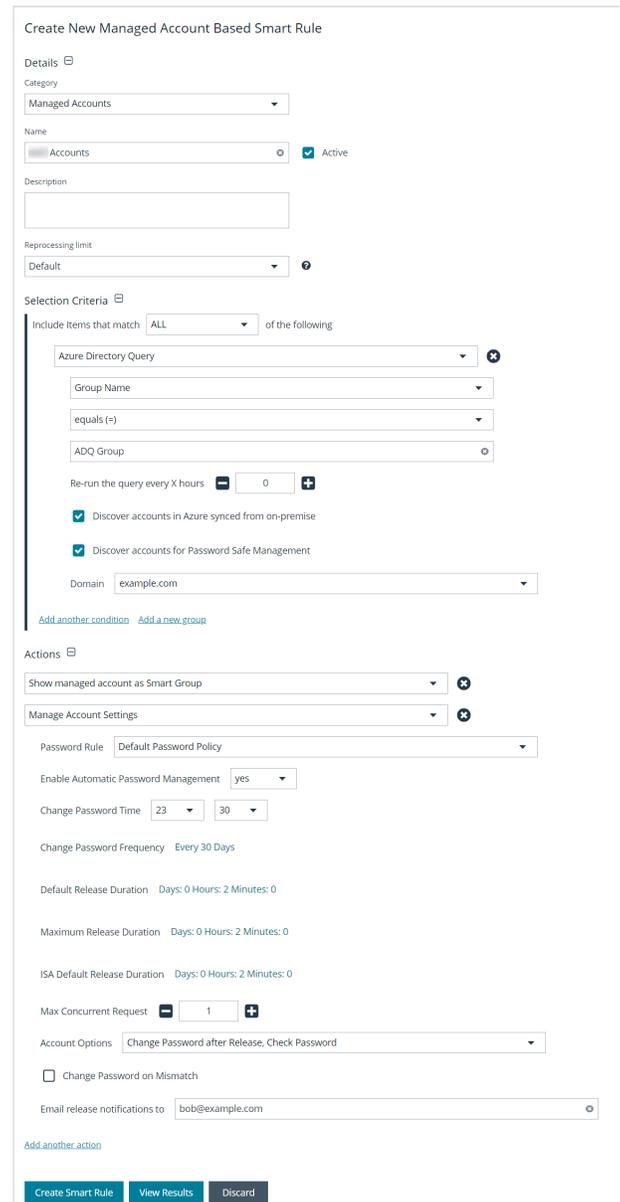
1. From the left menu, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule type filter** dropdown.
3. Click **+ Create Smart Rule**.

4. Configure the rule as follows:

- **Category:** Select **Managed Accounts**.
- **Name:** Provide a meaningful name and description that allows for easy identification of the Smart Rule.
- **Reprocessing Limit:** If desired, select a reprocessing limit.
- Under **Selection Criteria:**
 - Select **Azure Directory Query** from the dropdown. There are several filters, and options are dynamic, depending on other selections:
 - Include **ALL** or **ANY** of the selection criteria.
 - There are two matching options available for discovering Entra ID accounts: **Group Name** and **User Principle Name**. Use a **Group Name** match to discover all accounts that are a member of the specified group. Use a **User Principle Name** match to allow a partial name match.
 - If using a **Group Name**, **equals** is the only match option. Enter the **Group Name**.
 - If using a **User Principle Name**, select **starts with** or **ends with** and enter the name.
 - Set the value for how many hours for rerunning the query.
 - Check the **Discover accounts in Azure synced from on-premise** option to include Entra ID accounts synced from on-premises Entra ID, as well as Azure-only accounts.
 - Leave **Discover accounts for Password Safe Management** checked.
 - Select an Azure domain from the dropdown.
 - Add additional selection criteria and groups, as required.

5. Under **Actions**, select **Show managed account as Smart Group**, and then add other actions as required to manage settings or work with the managed account.

6. Click **Create Smart Rule**.




Tip: To view the contents of a Smart Rule when creating a new rule or editing an existing rule:

- Once the rule is saved, click **View Results**.
- You are taken to the associated grid, where the contents of the Smart Rule are listed.
- If the rule is actively processing, a banner displays letting you know that.


Note:

- **View Results** displays only if you have permissions to the grid corresponding to the Smart Rule, i.e.; Assets, Managed Accounts, Managed Systems.
- The Smart Rule must be saved with **Show <entity> as Smart Group** selected under **Actions** to view the results.



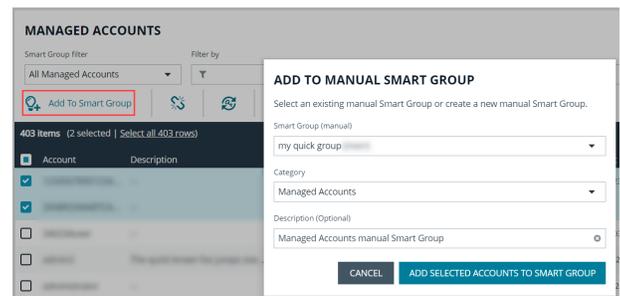
Tip: Because the Smart Rule must process to display the contents in the grid, we recommend viewing the results using only the **Show <entity> as Smart Group** action and before adding additional actions that may make changes to accounts and assets in your network.

Once you have confirmed the rule contains your desired items, you can then add additional actions to the Smart Rule.

Use Quick Groups

For a simpler way to organize managed accounts, you can group them using a Quick Group. The default processing time on a Quick Group is **Once**.

1. In the console, click **Managed Accounts**.
2. From the **Smart Group filter** dropdown, select an existing smart group in which the managed accounts are members.
3. Check the boxes for the managed accounts that you want to add to the Quick Group.
4. Click **Add to Smart Group** above the grid.
5. Select a group from the **Smart Group** dropdown or create a new one by typing in the name and clicking **Add as New Option**.
6. Select **Quick Groups** from the **Category** dropdown.
7. Leave the default description or enter a new one.
8. Click **Add Selected Accounts To Smart Group**.
9. Your new smart group is now available in the **Smart Group filter** dropdown.
10. To remove accounts from the Quick Group:
 - Select the group from the **Smart Group filter** dropdown.
 - Check the boxes for each account you wish to remove, and then click **Remove From Smart Group** above the grid.
 - To quickly locate Quick Groups from the **Smart Rules** page, select **Quick Groups** from the **Category** dropdown.
 - To change the name and description for a Quick Group, or to deactivate a Quick Group:
 - From the **Smart Rules** page, click the vertical ellipsis for the group, and then select **View Details**.
 - Make your changes, and then click **Save Changes**.



You can also quickly manually add managed systems to Smart Groups from the **Managed Systems** page.



Note: Managed systems do not have a Quick Group category; however, the concept and process is essentially the same as it is for managed accounts.

1. In the console, click **Managed Systems**.
2. From the **Smart Group filter** dropdown, select an existing Smart Group in which the managed systems are members.
3. Check the boxes for the managed systems that you want to add to the Quick Group.
4. Click **Add to Smart Group** above the grid.
5. Select a group from the **Smart Group** dropdown or create a new one by typing in the name and clicking **Add as New Option**.
6. Select a **Category** from the dropdown.
7. Leave the default description or enter a new one.
8. Click **Add Selected Systems To Smart Group**.
9. Your new smart group is now available in the **Smart Group filter** dropdown.

To remove a managed system from a Smart Group:

1. Select the Smart Group from the **Smart Group filter**.
2. Check the boxes for the managed systems that you want to remove from the group.
3. Click **Remove From Smart Group** above the grid.

To change the name and description for a managed system Quick Group, or to deactivate a Quick Group:

1. Navigate to the **Smart Rules** page.
2. Select **Managed System** from the **Smart Rule type filter**.
3. Locate the Quick Group you created.
4. Click the vertical ellipsis for the group, and then select **View Details**.
5. Make your changes, and then click **Save Changes**.



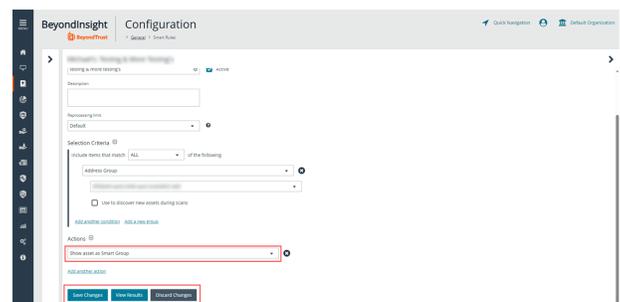
Note: You cannot add or modify filters or actions for Quick Groups.



For more information about Smart Rule processing, please see ["Change the Processing Frequency for a Smart Rule" on page 48](#).

Edit Smart Rules

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Click the vertical ellipsis to the right of the Smart Rule.
3. Select **Edit Smart Rule**.
4. Make the necessary changes and then click **Save Changes**.





Tip: To view the contents of a Smart Rule when creating a new rule or editing an existing rule:

- Once the rule is saved, click **View Results**.
- You are taken to the associated grid, where the contents of the Smart Rule are listed.
- If the rule is actively processing, a banner displays letting you know that.



Note:

- **View Results** displays only if you have permissions to the grid corresponding to the Smart Rule, i.e.; Assets, Managed Accounts, Managed Systems.
- The Smart Rule must be saved with **Show <entity> as Smart Group** selected under **Actions** to view the results.



Tip: Because the Smart Rule must process to display the contents in the grid, we recommend viewing the results using only the **Show <entity> as Smart Group** action and before adding additional actions that may make changes to accounts and assets in your network.

Once you have confirmed the rule contains your desired items, you can then add additional actions to the Smart Rule.

Delete Smart Rules

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select one or more Smart Rules.
3. Click the Trash Can icon above the grid. You can also click the vertical ellipsis to the right of a single Smart Rule and select **Delete**.



Note: Built in Smart Rules cannot be deleted. These are identified by the Lock icon.



Note: A Smart Rule that is used in another Smart Rule cannot be deleted or marked as inactive.

Audit Smart Rules

To audit new or edited Smart Rules:

1. Go to **Configuration > General > User Audits**.
2. Select **Section** from the **Filter by** dropdown.
3. Select **Smart Rule** from the **Section** dropdown.
4. Click the information icon to the right of the Smart Rule.
 - If a Smart Rule is added, the **Add Details** pane displays with all added information.
 - If a Smart Rule is edited, the **Edit Details** pane displays with all edited information.

Configure Role Based Access

Creating groups gives you great flexibility in delegating access to managed systems. Permissions provide access to BeyondInsight system components, while Password Safe roles determine the scope of access to managed systems.

- **Group permissions:** Permissions are assigned when you create a group. Permissions are system-wide and provide access to various components of the BeyondInsight infrastructure. There are permissions that are specific to accessing and using features of the Password Safe application.
- **Password Safe roles:** The roles define the actions that Password Safe users can take when using the Password Safe web portal for password releases or access to applications.

Group Features

The following table provides information on the Password Safe features that you can assign to your groups.

Feature	Full Control permission assigned
Password Safe Account Management	Grants permissions to the following features on the Managed Accounts page: <ul style="list-style-type: none"> • Bulk delete accounts • Add accounts to a Quick Group • Remove accounts from a Quick Group • Add, edit, and delete accounts
Password Safe Admin Session	Allows non-ISA users access to the Admin Session feature in Password Safe. Using an Admin Session allows administrators to open ad-hoc RDP / SSH sessions without going through the request process.
Password Safe Bulk Password Change	Use the bulk password change feature on the Managed Accounts page.
Password Safe Agent Management	Grant a user administrator permissions to the Configuration > Privileged Access Management Agents page.
Password Safe Configuration Management	Grant a user administrator permissions to the Configuration > Privileged Access Management page.
Password Safe Policy Management	Grant a user administrator permissions to the Configuration > Privileged Access Management Policies page.
Password Safe Role Management	Manage roles provided they have the following permissions: Password Safe Role Management and User Accounts Management .
Password Safe System Management	Users can manage systems on the Managed Systems page, including: <ul style="list-style-type: none"> • Create, change, and remove directory and cloud systems. • Link and unlink directory accounts to managed systems. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: Password Safe Account Management is needed with Password Safe System Management to manage Password Safe accounts. Full Control is required for both. </div>
Smart Rule Management - Managed Account	Users can create and edit Managed Account Smart Rules.

Smart Rule Management - Managed System	Users can create and edit Managed System Smart Rules.
Secrets Safe	Users can access the Secrets Safe feature.

In addition to Password Safe features permissions, users need the following general permissions:

Asset Management	Read, create, and delete assets and databases.
Management Console Access	Access to log on to the management console.

Password Safe Roles

In Password Safe, a role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system. Roles are assigned to Smart Groups, and the roles that you can assign depend on the Smart Group type, as follows:

- **Asset Smart Group:** The ISA and Auditor roles may be assigned.
- **Managed Account Smart Group:** The Requestor, Approver, Credentials Manager, Recorded Session Viewer, and Active Session Reviewer roles may be assigned.

Role	Description
Requester	<p>Allows users to submit a request to retrieve managed passwords or remote session connection files.</p> <p>When assigning the Requester role, you must select an access policy.</p>
Approver	<p>Allows users to approve requests for the release of managed passwords or remote session connection files.</p> <p>Typically, system administrators and network engineers are assigned to this role.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: <i>In peer approval environments, users may be both approvers and requestors. In this case, a user cannot approve their own requests when dual control is enforced.</i> </div>
Information Security Administrator (ISA)	<p>Allows users to setup managed systems and accounts.</p> <p>The ISA role provides the functionality required for security help desk personnel. User with the ISA role can delegate limited authority to those responsible for resource management.</p> <p>This role enables a user to bypass every workflow and security measure, like approval workflows or checked out accounts.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: <i>If another user has an account checked out and the password is known by this user, an ISA user can view the password. ISA users are not permitted to use the Admin Session feature.</i> </div>
Auditor	<p>Users with the Auditor role can:</p> <ul style="list-style-type: none"> • Run reports in BeyondInsight Analytics & Reporting • Replay recorded sessions in the Password Safe web portal <p>The Auditor role can be assigned with other roles.</p>
Credentials Manager	Allows users to set credentials using the PUT ManagedAccounts/{accountId}/Credentials API.

Recorded Session Reviewer	Allows users to view and take action on completed recorded Password Safe sessions, including: <ul style="list-style-type: none">• Add comments• Mark the session as reviewed• Archive sessions if configured on the U-Series Appliance
Active Session Reviewer	Allows users to view and take action on active Password Safe sessions, including: <ul style="list-style-type: none">• Lock session• Terminate the session• Cancel the request

On all systems where a user is granted the ISA role, the user can change the following system details:

- Grant users/groups roles to the managed system.
- Review password release and session requests.
- Add and change accounts on managed systems.
- Assign a system to a collection (provided the ISA role is granted to the user for both the system and the collection).
- Remove their ISA role from a system.

Create a Group and Assign Roles

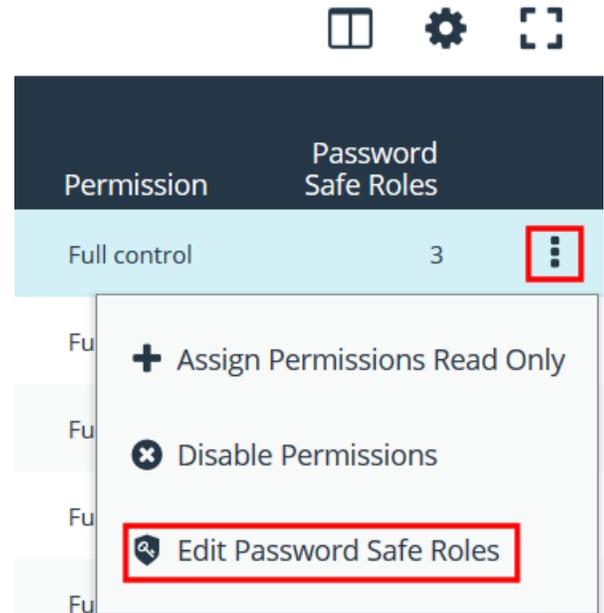


Note: You cannot assign roles to the *BeyondInsight* administrator.

Roles are only available to BeyondInsight features.

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **+ Create New Group**.
3. Select **Create a New Group**.
4. Enter a name and description for the group.
5. Click **Create Group**.
6. Assign users to the group:
 - Under **Group Details**, select **Users**.
 - From the **Show** dropdown list, select **Users not assigned**.
 - Filter the list of users displayed in the grid by **Type**, **Username**, **Name**, **Email**, and **Domain**, if desired.
 - Select the users you wish to add to the group, and then click **Assign User** above the grid.
 - Assign features permissions to the group:
 - Under **Group Details**, select **Features**.
 - Filter the list of features displayed in the grid using the **Show** and **Filter by** dropdown lists.
 - Select the features you wish to assign permissions to, and then click **Assign Permissions**.
 - Select **Assign Permissions Read Only** or **Assign Permissions Full Control**.
 - Assign Smart Groups permissions and roles to the group:
 - Under **Group Details**, select **Smart Groups**.
 - Filter the list of Smart Groups displayed in the grid using the **Show** and **Filter by** dropdown lists.
 - Select the Smart Group or groups you wish to assign permissions to, and then click **Assign Permissions**.
 - Select **Assign Permissions Read Only** or **Assign Permissions Full Control**.

- Select the Smart Group you wish to assign Password Safe roles to, and then click the vertical ellipsis button.
- Select **Edit Password Safe Roles**.



- Select the role(s). If selecting **Requestor**, also select an access policy from the dropdown.
- Click **Save Roles**.

Password Safe Roles

A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system.

Requestor

Access Policy for Requestor ▼

Approver

Credentials Manager

Recorded session reviewer

Active session reviewer

SAVE ROLES

DISCARD CHANGES

Quarantine User Accounts

You can turn on the quarantine feature as a preventative measure when suspicious activity is detected. When quarantine is turned on, the user account can no longer log in to the console or API, and any active sessions are terminated immediately.

The difference between account lockout and account quarantine is that account lockout cannot terminate sessions.

Turn on the setting at the user account level as follows:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Select the **Users** tab.
3. Click the vertical ellipsis for the user account.
4. Select **Edit User Details**.
5. Check the **Account Quarantined** option to enable it.
6. Click **Update User**.

Set the Refresh Interval on the Quarantine Cache

You can set the length of time that passes before the cache is updated with the user accounts from the database. The quarantine is only applied to the user account after the cache is updated.

The user can remain logged in and sessions remain active up until the refresh interval time passes (and the cache is updated with the quarantine status).

1. Go to **Configuration > System > Site Options**.
2. Under **Session**, enter the number of seconds that pass before the cache is updated with the most recently discovered quarantined user accounts.

The default value is **600** seconds (10 minutes). The maximum value is **1200** seconds (20 minutes).

3. Click **Update Session Options**.

Configure API Access

When using the Password Safe API, the group where the users are assigned must permit access to the API. Additionally, any managed accounts that must be accessible by the API must also be configured.

Configure Group with API Access

A BeyondInsight user has API access if at least one of the user groups they belong to has API access enabled.

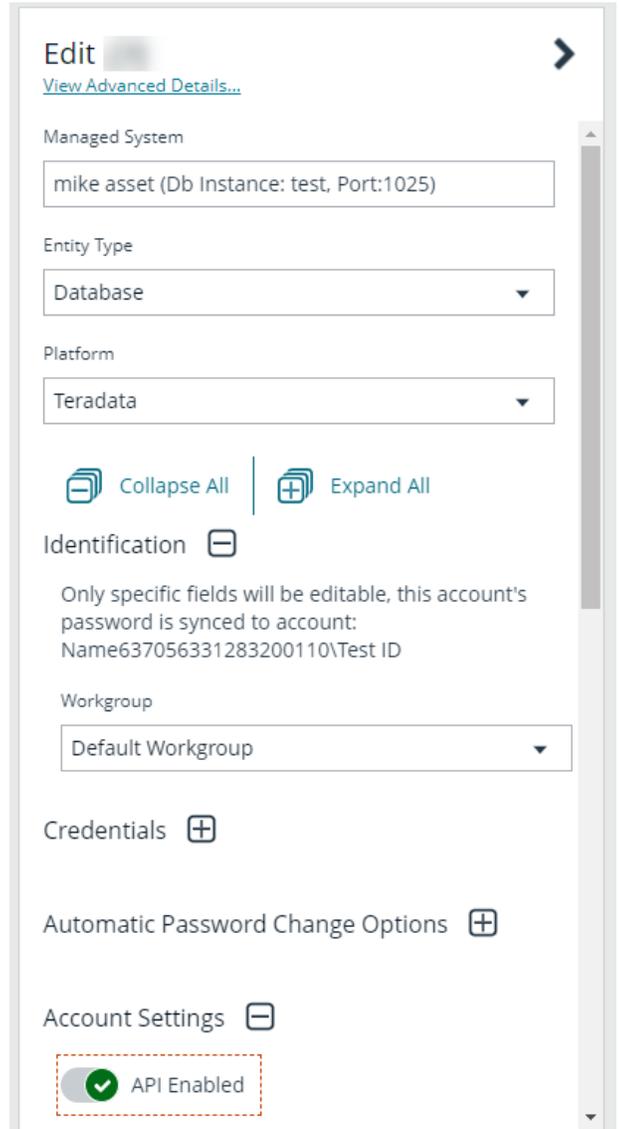
1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click the vertical ellipsis for the group.
3. Select **View Group Details**.
4. Under **Group Details**, select **API Registrations**.
5. Select the API registrations for the group.

Enable API Setting for Managed Account

You must turn on API access for a Password Safe managed account to be accessible to the API methods.

1. Navigate to the **Managed Accounts** page.
2. Click the vertical ellipsis for a managed account, and then select **Edit Account**.

3. Scroll down and expand **Account Settings**.
4. Click the toggle to turn on the **API Enabled** option.
5. Click **Update Account**.



Edit 

[View Advanced Details...](#)

Managed System
mike asset (Db Instance: test, Port:1025)

Entity Type
Database

Platform
Teradata

 Collapse All |  Expand All

Identification 

Only specific fields will be editable, this account's password is synced to account:
Name637056331283200110\Test ID

Workgroup
Default Workgroup

Credentials 

Automatic Password Change Options 

Account Settings 

API Enabled

Restrict Access to Password Safe Login Page

When using SAML, smart card, or claims-aware authentication to access the Password Safe web portal, you might not want users to log in directly to the web portal URL. You can disable direct access to the Password Safe web portal URL for Active Directory, LDAP, and local BeyondInsight users by enabling the **Disable Login Forms** setting. Users must then always provide the SAML, smart card, or claims-aware credentials before gaining access to the web portal.

The following procedure assumes the group and user are already created.

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Users** tab, click the vertical ellipsis for the user.
3. Select **Edit User Details**.

4. Check **Disable Login Forms** to enable it.

Edit User ➤

[View User Details...](#)

First Name

Last Name

Email

Username

Account Quarantined

Credential

[Create New Credential...](#)

Domain / Domain controller

Authentication Options ?

Override Smart Card User Principal Name

Disable Forms Login

Two-Factor Authentication

Configure Approvals

You can control the number of approvers required for a requester. You can also control the number of approvers required for each access type: **View Password**, **RDP**, and **SSH**. This is configured in an access policy, which can then be assigned to a group when assigning Password Safe roles to the group.



Note: Any of the approvers in the group can approve the request. If other subsequent approvers click the link, they will see that the request has already been approved. Other approvers can, however, override the approval and deny the request. If a request is denied by one approver, no approvers can subsequently override and approve. It is not possible to deny the request once the schedule window has actually begun.



For more information, please see:

- ["Create a Group and Assign Roles" on page 62](#)
- [Approve or Deny Requests for Passwords and Sessions in the Password Safe User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/documents/ps/ps-user.pdf](https://www.beyondtrust.com/docs/beyondinsight-password-safe/documents/ps/ps-user.pdf)

Use a Managed Account as a Credential

You can use a managed account for the credential when you are configuring queries and user groups for Active Directory and LDAP.



Note: You cannot delete a managed account if it is used as a credential for a user group. You can delete a managed account used as a credential for a directory query; however, the query will no longer run. You must select another credential for the query to run again.



For more information on managed account settings, please see ["Use a Managed Account as a Discovery Scan Credential" on page 37.](#)

Configure the Managed Account

Before you configure the query or group, the managed account must be in place and specific settings must be selected.

When you configure the managed account settings, be sure to select the **Allow this account to be used in BeyondInsight and Directory Queries** option.

If there are several managed accounts organized in a Smart Group, select **Enable Accounts for AD/LDAP queries** in the Smart Rule.



IMPORTANT!

Disable the **Change Password After Release** option on the managed account, because log files can grow significantly in a short time when using managed account credentials with a directory query.

Configure the Query

Active Directory and LDAP queries can use a managed account as a credential.

An Active Directory or LDAP group can use a managed account as the credential. When you create the group, the managed account is listed as a credential.



For more information on creating directory queries, please see [Create a Directory Query at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/tools/directory-query.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/tools/directory-query.htm).

Configure LDAP Groups

Before logging in to Password Safe using LDAP, you must configure an LDAP group.



For more information on creating and configuring LDAP groups, please see [Add an LDAP Directory Group](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/role-based-access/create-groups/ldap.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/role-based-access/create-groups/ldap.htm>.

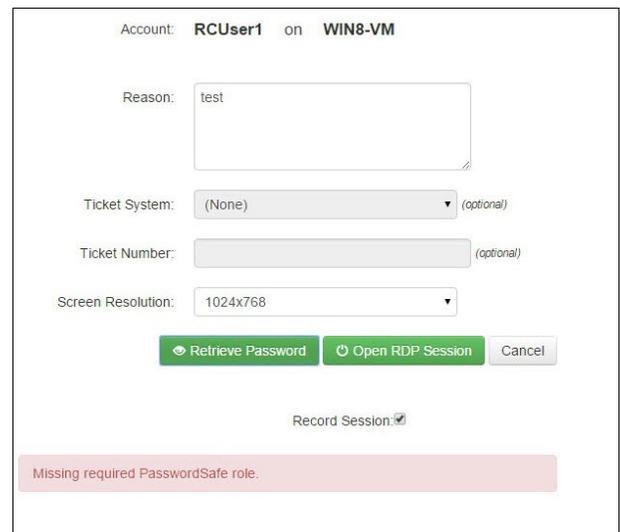
Real Time Authorization

Real Time Authorization allows administrators to remove users from groups while they are logged in with a directory account and use the registry key to perform an additional check to ensure that the user still has access to the password at the time they requested it. This puts the user through the log in process every time a password is requested.

Enable the following registry key to turn on this feature:

HKLM\SOFTWARE\BeyondTrust\PBPS\EnableCheckoutAuthorization

After the user is removed from the group, they receive the following error message when they request password access: *Missing required Password Safe role.*



Account: **RCUser1** on **WIN8-VM**

Reason:

Ticket System: (optional)

Ticket Number: (optional)

Screen Resolution:

Record Session:

Missing required PasswordSafe role.

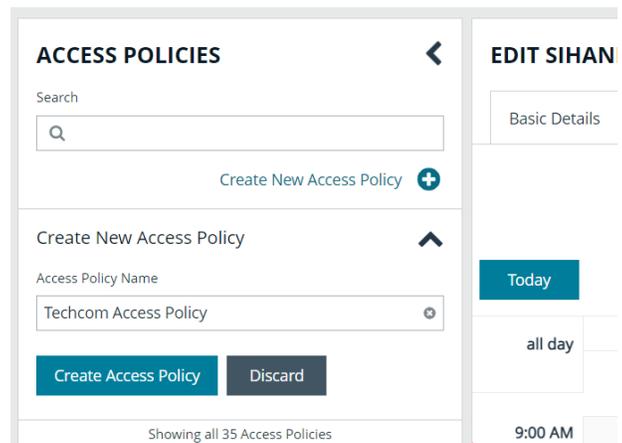
Configure Password Safe Access Policies

An access policy defines the time frame and frequency that users can request passwords, remote access sessions, or access applications under Password Safe management.

An access policy is selected when you are configuring the **Requester** role.

Create an Access Policy

1. Go to **Configuration > Privileged Access Management Policies > Access Policies**.
2. In the **Access Policies** pane, click **Create New Access Policy**.
3. Enter a name for the policy, and then click **Create Access Policy**.



4. On the **Basic Details** tab:
 - Enter a description for the policy.
 - Optionally, enable the **Email Notifications** option to send emails when a request is received for the policy.

 **Note:** Recipients may receive a large number of email notifications. Selective use of this option is strongly advised. Multiple addresses cannot be added at once. Each email address must be added one at a time by clicking **Add Another Email**.

5. Select the **Schedule** tab, and then click **Create Schedule**.
6. Configure the recurrence, time, and date settings for the policy. If you select a daily recurrence, you can optionally select **Allow multi-day check-outs of accounts**. This option allows the user continuous access to a granted request over a span of days.
7. Optionally, enable the **Enable Location Restrictions** option, and then select a location from the list.
8. If applicable, select an address from the **X-Forwarded-For** list. This field is an allowed value of **X-Forwarded-For header**, which was added by an F5 load balancer or proxy. It uses address groups to verify if the IP address is to be in that list. The URL and named host will be ignored. If the **X-Forwarded-For** field has a value of **Any**, then no X-Forwarded-For header is required or verified. In the case where it is configured, the X-Forwarded-For header is required and its value should be in the list of IPs in the address group.



Note: In the case of a new configuration, this error message can be found in the log:

```
CheckLocationAllowed: XForwardedForHeaderValue 1.1.1.1 is not registered/trusted. Add
this XForwardedForHeaderValue to the TestGroupName Address group
```

9. Select the type of access to permit: **View Password**, **RDP**, **SSH**, or **Application**.
10. For each type of access selected, configure the parameters as required. Descriptions for each parameter are as follows:

Approvers	Select the number of approvers required to permit access. Check Auto Approve if the requests do not require any approvers.
Allow API Rotation Override	Check this option for View Password access, to allow API callers such as Password Safe Cache to override the Change Password After Any Release managed account setting for view-type requests.
Record	Check the box to record the session.
Keystroke Logging	Keystrokes can be logged during RDP, SSH, and application sessions. Uncheck the boxes for each policy type to disable keystroke logging for that type.
Enhanced Session Auditing	Enhanced session auditing applies to RDP and application sessions and is on by default. Click the toggle to turn off enhanced session auditing.
Concurrent	Set the number of sessions permitted at a time. Check Unlimited to permit the user any number of connections to occur at the same time.
Log off on Disconnect	Check this box to automatically log off the user when the connection to the session disconnects or the session window closes. This option applies only to RDP and RDP application sessions, and is active only when Enhanced Session Auditing is enabled. <div data-bbox="836 1312 885 1375" data-label="Image"> </div> <div data-bbox="901 1327 1485 1421" data-label="Text"> <p>Note: If the session has been terminated by an Active Sessions reviewer, the logoff on disconnect occurs regardless of the access policy setting.</p> </div>
Force Termination	Check this box to close the session when the time period expires. When Log off on Disconnect is also selected, the user is logged off the session. This check box applies to RDP, SSH, and application sessions. When the Requested Duration (as entered by the user on the Requests page in the web portal) is exceeded, the session ends if the Force Termination box is checked for the access policy. The default and maximum release durations are configured on the Managed Accounts page and Managed System Settings page.

RDP Admin Console	<p>Select this option to show the RDP Admin Console check box on RDP-based requests. This option allows administration of a Remote Desktop Session host server in console mode (mstsc /admin). This can be useful if the number of remote sessions is maxed out on the host.</p> <p>Using the RDP Admin Console allows you to use a remote session without requiring other sessions to disconnect. Running a remote session using the RDP Admin Console disables certain services and functionality, such as, but not limited to:</p> <ul style="list-style-type: none"> • Remote Desktop Services client access licensing • Time zone redirection • Remote Desktop Connection Broker redirection • Remote Desktop Easy Print
Connection Profile	<p>Select a profile from the list or click Manage Connection Profiles to be taken to the Connection Profiles page to create a new profile.</p>

11. Under **Policy Options**:

- If you want users to provide a reason when making requests in Password Safe, click the toggle for the **Reason is required for new requests** option to enable it.
- If you want users to provide a ticket number for a ticketing system when making requests in Password Safe, click the toggle for the **Require a ticket system and a ticket number for requests** option to enable it.
 - Once enabled, select the **Ticket System** from the dropdown. If you leave the **Ticket System** as **User Selected**, the user can select any ticket system from the list when making their request. If you select a specific ticket system for this option, the user is unable to change the ticket system when making their request.

12. Click **Create Schedule**. If the access policy is not yet marked as available, you are prompted to activate it now.

13. Assign the access policy to a user group as follows:

- Select the **Assignees** tab.
- Click **Manage Assignees**. You are taken to the **User Management** page.
- Click the vertical ellipsis for a group, and then select **View Group Details**.
- From the **Group Details** pane, click **Smart Groups**.
- Click the vertical ellipsis for a managed account Smart Group, and then select **Edit Password Safe Roles**.
- Check **Requestor**, and then select the access policy you just created from the dropdown.
- Click **Save Roles**.

14. Confirm the group is now listed as an assignee on the **Assignees** tab for the access policy you just created.



For more information, please see the following:

- ["Configure Keystroke Logging" on page 151](#)
- ["Enhanced Session Auditing" on page 151](#)
- For configuring release durations, ["Add a Managed System Manually" on page 17](#)
- For information on how to use `mstsc /admin`, `mstsc` at <https://docs.microsoft.com/en-us/windows->



[server/administration/windows-commands/mstsc](#)

- ["Create a Connection Profile" on page 76](#)

Create a Connection Profile

Connection profiles allow administrators to create a deny list of keywords, host names, and IP addresses. Each deny listed item can be given a separate action which is triggered when requesters type a deny listed item in an active SSH session.

Administrators can choose to have Password Safe perform the following actions when a match occurs:

- **No Action:** Select to be alerted only if a match occurs.
- **Block:** Blocks the transmission of the command to the remote machine.
- **Lock:** Locks the session for the requester.
- **Block and Lock:** Performs both a block and lock as described above.
- **Terminate:** Ends the remote session.



Note: Connection policies apply to SSH and SSH application sessions.

1. Go to **Configuration > Privileged Access Management Policies > Connection Profiles**.
2. From the **Connection Profiles** pane, click **Create New Connection Profile**.
3. Enter a name for the profile, and then click **Create Connection Profile**.
4. Optionally, to send email notifications when a deny listed item is triggered, click **Email Notification Settings** to expand it and add an email recipient



Note: Recipients may receive a large number of email notifications. Selective use of this option is strongly advised.

5. Click **Save Changes**.
6. Click **Create Match Condition**.
7. To add a deny listed item, select one of the following from the **Match** dropdown: **Keyword**, **Hostname**, or **IP Address**.
8. Enter the match criteria in the **Value** box.
9. From the **Session Control** dropdown, select the action to take when the deny listed item is triggered.
10. Click **Create Condition**. Each deny listed item is displayed on a separate line.
11. Apply the connection profile to an access policy schedule, as follows:
 - Go to **Configuration > Privileged Access Management Policies > Access Policies**.
 - Select the policy.
 - From the **Edit Policy** pane, click the **Schedule** tab.
 - Double-click a schedule to open it, or create a new schedule.
 - Scroll down to the **Connection Profile** dropdown, and then select the newly created profile from the list.

Use a Predefined Connection Profile

The following predefined connection profiles are available for an access policy: **Lateral Movement** and **Suspicious Activity**.

The profiles are configured to match on keywords that might indicate suspicious behavior occurring on your network. If a match is detected on any of the keyword values then the session is blocked.

You can add or delete keywords in the predefined connection profiles.

Create Password Policies

Password Safe ships with a default password policy used to generate new passwords for auto managed accounts. You can change the settings for the default policy, such as password length and complexity, but you cannot delete the default password policy. You can also create new password policies.



Note: Ensure the policies you create in Password Safe align with password complexity and restrictions in place on the managed system; otherwise, Password Safe might create a password that does not comply with the rules in place on that managed system.

1. Go to **Configuration > Privileged Access Management Policies > Password Policies**.
2. Click **Create New Password Policy**.
3. Enter a name for the password policy, and then click **Create Password Policy**.
4. Optionally provide a description for the policy, and set the following parameters:
 - Check **Allow use for Secrets Safe** to allow the policy to be available for selection within team password credentials. The policy can be selected when a credential is using the **Auto Generate** option for setting the credential's password.
 - Use the **-** and **+** buttons to incrementally lower or raise the **Minimum length** and **Maximum length** of passwords for the selected policy. You can also manually enter the numbers in the text fields. Valid entries are **4 - 255** characters.
 - Select the **First Character Value**.
 - Alpha Characters Only
 - AlphaNumeric Permitted
 - Any Character Permitted
 - **Uppercase Characters:** Use the toggle button to permit or deny the use of uppercase characters in passwords. If uppercase characters are permitted:
 - Set the **Minimum number of required uppercase characters** using the **-** and **+** buttons or by entering a number in the text field.
 - Enter permissible characters in the **Allow only the following uppercase characters** field.
 - **Lowercase Characters:** Use the toggle button to permit or deny the use of lowercase characters in passwords. If lowercase characters are permitted:
 - Set the **Minimum number of required lowercase characters** using the **-** and **+** buttons or by entering a number in the text field.
 - Enter permissible characters in the **Allow only the following lowercase characters** field.
 - **Numeric Characters:** Use the toggle button to permit or deny the use of numeric characters in passwords. If numeric characters are permitted:
 - Set the **Minimum number of required numeric characters** using the **-** and **+** buttons or by entering a number in the text field.
 - Enter permissible characters in the **Allow only the following numeric characters** field.
 - **Non-Alphanumeric Characters:** Use the toggle button to permit or deny the use of non-alphanumeric characters in passwords. If non-alphanumeric characters are permitted:
 - Set the **Minimum number of required non-alphanumeric characters** using the **-** and **+** buttons or by entering a number in the text field.

Techcom Password Policy Details

Password Policy Name
7 characters remaining
Techcom Password Policy

Description (Optional)

Allow use for Secrets Safe

Minimum length
8

Maximum length
10

First Character Value
 Alpha Characters Only
 AlphaNumeric Permitted
 Any Character Permitted

Uppercase Characters
 Permit uppercase characters

Minimum number of required uppercase characters
2

Allow only the following uppercase characters
 ABCDEFGHIJKLMNOPQRSTUVWXYZ
[Reset to Default](#)

Non-Alphanumeric Characters
 Permit non-alphanumeric characters

Minimum number of required non-alphanumeric characters
1

Allow only the following non-alphanumeric characters
 -!@#%&*'()+-=?<>|[]_.,
[Reset to Default](#)

Update Password Policy **Discard Changes**

- Enter permissible characters in the **Allow only the following non-alphanumeric characters** field.
5. Click **Update Password Policy**.

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.



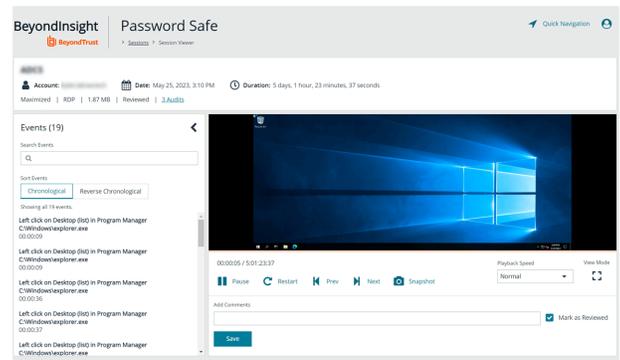
Tip: If a session recording has been archived, the **View Session** option is not available. If available, select the **Restore Session** option to restore the recording. You can also restore the archived session from the session's details by selecting **View Details** and then clicking the **Restore**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



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.

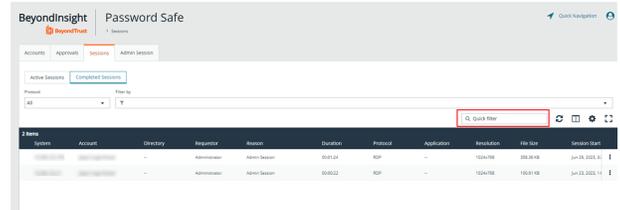
To take a screenshot of a session frame and export it as a JPEG file, click the **Snapshot** button. The file exports with a resolution of 1024 × 768. The JPEG file is automatically saved to the default download location specified in your browser settings.



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.



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

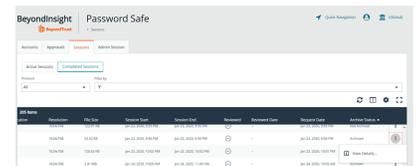


Archive Recorded Sessions

Administrators can configure auto-archiving of recorded sessions by enabling and configuring the **Session Monitoring Archive** feature on the U-Series Appliance. Session Monitoring Archive allows you to configure the transfer of session monitoring files from this appliance to an external data repository to prevent filling the local storage. You can set archiving rules to determine when the appliance must archive session monitoring recording file, based on a specific number of days the recording file was created and based on the number of MB remaining for storage space. When one condition is met, the archiving begins.

When session archiving is enabled, archived sessions are listed in the **Completed Sessions** grid. You can locate them by adding the **Archive Status** column using the **Column Chooser** button above the grid.

Click vertical ellipsis for the archived session, and then select **View Details** to view session details. If desired, you can restore the archived session by clicking **Restore** in the session's details.



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.

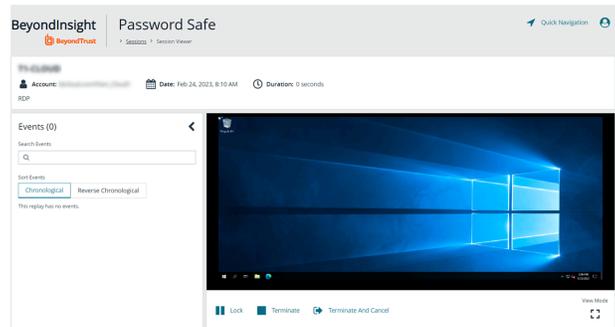
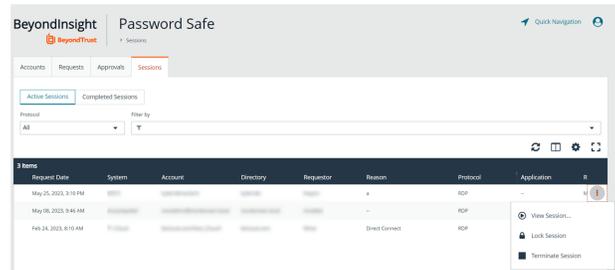
1. From the left navigation, click **Menu**, and then under **Password Safe**, click **Active Sessions**.
2. Use the dropdowns above the grid to locate the session you wish to view or manage, and then click the vertical ellipsis for the session.
 - Click **Lock** to immediately lock the session.
 - Click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

 **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.

 **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.



Add Windows Components to Password Safe

Password Safe can manage Active Directory and LDAP directories and directory accounts, as well as credentials used to run the following:

- Windows services
- Windows scheduled tasks
- IIS application pools
- COM+ and DCOM applications
- SCOM RunAs identities

Add a Directory

1. From the left menu, select **Managed Systems**.
2. Click **Create New Managed System**.
3. From the **Type** list, select **Directory**.
4. From the **Platform** list, select **Active Directory** or **LDAP**.
5. Configure the settings for the directory, and then click **Create Managed System**.



For more information on adding managed systems manually, please see ["Add a Managed System Manually" on page 17](#).

Add Directory Accounts

You can add directory accounts manually or by creating an Active Directory account with a Smart Group.

Add Directory Accounts Manually

1. On the **Managed Systems** page, select the managed system for the directory, and then click the vertical ellipsis button for the managed system.



Tip: Filter the list of managed systems in the grid by selecting **Directory Managed Systems** from **Smart Group filter** to quickly find your managed system.

2. Select **Create Managed Account**.
3. Configure the managed account settings as necessary, and then click **Create Account**.



Tip: When configuring the managed account settings for an Active Directory account, you can choose a domain controller to change or test a password. The domain controller on the managed account overrides a domain controller on the functional account selected.

i For more information on adding managed accounts manually, please see ["Add a Managed System Manually"](#) on page 17.

Discover Active Directory Accounts with an Active Directory Query

1. From the left menu, click **Smart Rules**.
2. From the **Smart Rule type filter** list, select **Managed Account**.
3. Click **+ Create Smart Rule**.
4. Select **Managed Accounts** from the **Category** list.
5. Provide a name and description for the Smart Rule.
6. Set the following **Selection Criteria**:
 - **Directory Query > Include accounts from Directory Query**.
 - Select the query from the list, or click **Create New Directory Query** to open the form and create the query.
 - Ensure the **Discover accounts for Password Safe Management** option is enabled.
 - Select a **Domain** from the list.
7. Set the following **Actions**:
 - **Show managed account as Smart Group**.
 - **Manage Account Settings**: Configure these settings as necessary, ensuring to select the following options from the **Account Options** dropdown:
 - **Change Password after Release**
 - **Check Password**
 - **Enable accounts for AD/LDAP queries**

! IMPORTANT!

By default, the Smart Rule auto manages the passwords for the directory accounts. If you do not want this, set **Enable Automatic Password Management** to **no**; otherwise, **ALL** accounts in the query will have passwords changed.

8. Click **Create Smart Rule**.

Create New Managed Account Based Smart Rule

Details ⊟

Category ⊟ Managed Accounts

Name ⊟ AD Query ⊞ Active

Description ⊟

Reprocessing limit ⊟ Default ⊞

Selection Criteria ⊟

Include Items that match ⊟ ALL ⊟ of the following

Directory Query ⊟ ⊞

Include accounts from Directory Query ⊟

AppSec OnBoarding ⊟

Re-run the query every X hours ⊞ 0 ⊞

Discover accounts for Password Safe Management

Domain ⊟ example.com ⊟

[Add another condition](#) [Add a new group](#)

Actions ⊟

Show managed account as Smart Group ⊟ ⊞

Manage Account Settings ⊟ ⊞

Password Rule ⊟ Default Password Policy ⊟

Enable Automatic Password Management ⊟ yes ⊟

Change Password Time ⊟ 23 ⊟ 30 ⊟

Change Password Frequency ⊟ Every 30 Days

Default Release Duration ⊟ Days: 0 Hours: 2 Minutes: 0

Maximum Release Duration ⊟ Days: 0 Hours: 2 Minutes: 0

ISA Default Release Duration ⊟ Days: 0 Hours: 2 Minutes: 0

Max Concurrent Request ⊞ 1 ⊞

Account Options ⊟ Change Password after Release, Check Password ⊟

Change Password on Mismatch

Email release notifications to ⊟

[Add another action](#)

Create Smart Rule View Results Discard



Tip: To view the contents of a Smart Rule when creating a new rule or editing an existing rule:

- Once the rule is saved, click **View Results**.
- You are taken to the associated grid, where the contents of the Smart Rule are listed.
- If the rule is actively processing, a banner displays letting you know that.



Note:

- **View Results** displays only if you have permissions to the grid corresponding to the Smart Rule, i.e.; Assets, Managed Accounts, Managed Systems.
- The Smart Rule must be saved with **Show <entity> as Smart Group** selected under **Actions** to view the results.



Tip: Because the Smart Rule must process to display the contents in the grid, we recommend viewing the results using only the **Show <entity> as Smart Group** action and before adding additional actions that may make changes to accounts and assets in your network.

Once you have confirmed the rule contains your desired items, you can then add additional actions to the Smart Rule.

9. To view the Active Directory accounts:

- Go the **Managed Accounts** page.
- Select the newly created Smart Group from the **Smart Group filter** list.

Link Active Directory Accounts to Managed System

You can link Active Directory accounts to managed systems on a specified domain.

1. From the left menu, click **Managed Systems**.
2. Select the managed system, and then click the vertical ellipsis button for the managed system.
3. Select **Go to Advanced Details**.
4. Under **Advanced Details**, click **Linked Accounts**.
5. Filter the list by **Not Linked**.
6. Select the accounts, and then click **Link Accounts** above the grid.

Create an Active Directory Functional Account

When creating an Active Directory managed account, the functional account requires a domain controller. Administrators can choose a targeted domain controller from the menu, or select **Any Domain Controller**, which allows Active Directory to choose.



Note: If a failure occurs when connecting to a target domain controller, Password Safe connects at the domain level.

Add Propagation Actions to Managed Accounts

Password Safe allows you to manage the credentials for Windows Services, Task Scheduler, IIS Application Pools, Windows Auto Logon, COM+ Applications, DCOM Applications, and SCOM RunAs Identities. These accounts can be added as managed accounts in Password Safe. When their passwords are changed by Password Safe, the credentials are updated in any systems associated with the managed account, if these options are assigned under **Advanced Details > Propagation Actions** on the managed account.



Note: The below information applies only for propagation actions that target Windows systems. It does not apply for Unix or Linux systems, or for SSH script actions.

For propagation actions that target Windows systems, Password Safe deploys a local agent to managed systems via the Password Safe Propagation Service to complete its tasks.

When a managed account password change occurs and Password Safe determines that a propagation action must occur, the Password Safe Propagation Service connects to the remote host using the Named Pipes (SMB) protocol over TCP port 445 (as well as UDP ports 137, 138, 139) to access the ADMIN\$ share and authenticates using the functional account specified in the managed system. This connection occurs directly from the appliance.

Once connected, the Password Safe Propagation Service creates a temporary folder on the ADMIN\$ share, `\\remotehost\admin$\RBExecService`, and deploys the `BTExecService.exe` local agent in this folder. The propagation service then completes all of the required propagation actions locally using the `BTExecService.exe`.

After all required propagation actions are complete, the propagation service deletes the `BTExecService.exe` agent, as well as the temporary folder on the ADMIN\$ share.

The following access is required for propagation actions to succeed:

- Functional account requires access to the ADMIN\$ share on the target managed system(s).
- The Microsoft .NET Framework must be at version 4.7.2 or above on the target managed system(s).
- The `\\remotehost\admin$\RBExecService` folder and `BTExecService.exe` agent must be exempt from any security or endpoint protection software on the target managed system(s).

The following network ports must be accessible between the Password Safe appliance and target managed system(s):

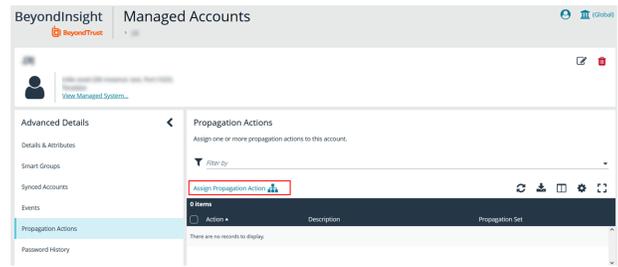
- 445 (TCP)
- 137 (UDP)
- 138 (UDP)
- 139 (UDP)

Assign Propagation Actions to Managed Accounts

You can manually assign propagation actions to a managed account as follows:

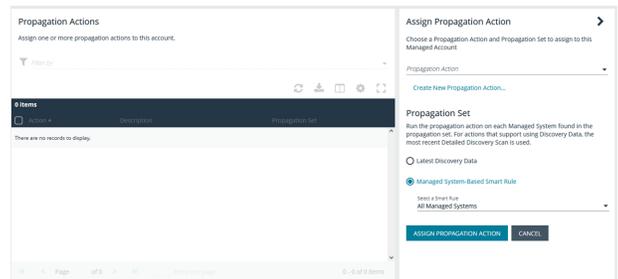
1. From the **Managed Accounts** page, click the vertical ellipsis for an account.
2. Select **Go to Advanced Details**.

- Under **Advanced Details**, click **Propagation Actions**.
- Click **Assign Propagation Action** above the grid.



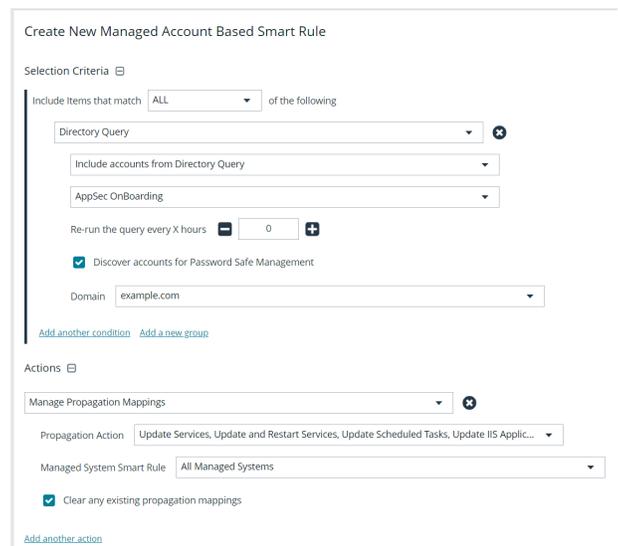
- Select a **Propagation Action** from the list.

 **Note:** To create a custom propagation action, click **Create New Propagation Action** below the dropdown and complete form. Please see ["Create Custom Propagation Action to Run a Script" on page 88](#) for more information.



- Select a **Propagation Set** to assign to this managed account. The **Propagation Action** runs on each managed system found in the **Propagation Set**.
 - Select **Latest Discovery Data** to use managed systems from the most recent detailed discovery scan.
 - Select a **Managed System-Based Smart Rule** from the list to use managed systems associated with a Smart Rule.

Propagation actions are also available when creating a managed account Smart Rule by selecting **Manage Propagation Mappings** under **Actions**, and then checking the applicable actions from the **Propagation Action** dropdown.



Available built-in Propagation Actions

- Update Services
- Update and Restart Services
- Update Scheduled Tasks
- Update IIS Application Pools

- Update and Restart IIS Application Pools
- Update Windows Auto Logon
- Update COM+ Applications
- Update DCOM Applications
- Update SCOM RunAs Identities

Create Custom Propagation Action to Run a Script

Password Safe also allows you to create new propagation actions to run PowerShell, Windows Command, and Unix Shell scripts as follows.



Note: Ensure you have deployed your script to your desired systems prior to creating a custom propagation action to run a script, as Password Safe does not deploy the script.

1. Navigate to **Configuration > Privileged Access Management > Propagation Actions**.
2. Click **+ Create Propagation Action**.
3. Complete the form by selecting the type of script to run, providing a name and description for the action, entering the full path (including script name) to the script you want to execute, and specifying the command line parameters. The following parameters can be used:

- **%u** managed account name
- **%p** managed account password
- **%h** script host name
- **%i** script host ip
- **%j** managed system name
- **%k** managed system ip



Note: The **%p** parameter must be in quotes to be passed correctly in the command line.

4. Click **Create Propagation Action**.

Create New Propagation Action

➔

Select an action to configure its options

Action Type
Run PowerShell Script

General Details

Run Update Script ✕

Action Description

Timeout (seconds)
− 120 +
Maximum 300

Shell Script Details

myscript.bat ✕ ?

%u %p %h %i ✕ ?

CREATE PROPAGATION ACTION
DISCARD

When a propagation action is triggered, the activity is logged as an event for the managed account. You can view events by viewing the advanced details for a managed account and clicking **Events** in the **Advanced Details** pane. Password changes as well as propagation actions that occurred for that account are listed in the **Events** grid.

Manage Windows Service Accounts



Note: When managing Windows services on managed systems in a clustered configuration, the Windows Services Cluster API is used. For successful update of clustered service credentials, all nodes of the cluster must be managed by Password Safe.

When a service is under Password Safe management, the following occurs when the managed account password changes:

- A service that is running restarts when the password is changed.
- A service that is stopped is not restarted when the password is changed.
- Dependent services may or may not restart based on the state of the primary service.

Before adding a service account to Password Safe management, we recommend you do the following:

- Verify machines are in the domain, if applicable.
- Verify assets are managed with a local administrator account if not in the domain, or with a domain administrator account if in the domain.

Complete the following procedures to prepare and add a service account to Password Safe management.

Prepare the Service

1. On the asset where the service resides, open the Windows Services snap-in and stop the service if running.
2. Right-click the service, and then select **Properties**.
3. Select the **Log on** tab and enter the local or active directory account and current credentials. If required, retrieve a password using the Password Safe administrator credentials.
4. Restart the service to verify it starts successfully.

Run a Scan on the Service Assets

1. In the BeyondInsight Console, click **Discovery Scan** to run a **Detailed Discovery Scan** against the target systems to add the systems as assets in BeyondInsight. The detailed scan collects data of the services for the targets.
2. Add the discovered assets to Password Safe management.
3. Verify the following:
 - From the **Assets** page:
 - Select the asset, and then click the vertical ellipsis button for the asset.
 - Select **Go to Advanced Details**.
 - Under **Scan Data**, click **Services**.
 - Confirm the services have been collected, their **Status** is **Running**, and the **Log On As** account name is correct.

- From the **Managed Systems** page:
 - Select the managed system, and then click the vertical ellipsis button for the system.
 - Select **Edit Managed System**.
 - Verify that **NetBIOS Name** is entered.
- 4. From the **Managed Accounts** page:
 - Select the managed account associated with the service, and then click the vertical ellipsis button for the managed account.
 - Select **Go to Advanced Details**.
 - Click **Propagation Actions** from the **Advanced Details** pane.
 - Click **Assign Propagation Action** and assign the **Update Services** or **Update and Restart Services** action for this account.
- 5. From the **Managed Accounts** page:
 - Select the managed account associated with the service, and then click the vertical ellipsis button for the managed account.
 - Select **Test Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.
 - Click the vertical ellipsis button for the managed account again.
 - Select **Change Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.
- 6. Restart the service to verify the password change. The password change is successful if the service restarts. Otherwise, the password change is not successful. Go through all the steps in this chapter to troubleshoot.

Manage Windows Scheduled Task Accounts

When a scheduled task is under Password Safe management, the following occurs when the managed account password changes:

- A scheduled task that is running stops when the password is changed.
- A scheduled task that is stopped will run again at its next scheduled interval time.

Before adding a scheduled task account to Password Safe management, be sure to:

- Start the Task Scheduler service on the target.
- Verify machines are in the domain, if applicable.
- Verify assets are managed with a local administrator account if not in the domain, or with a domain administrator account if in the domain.

Complete the following procedures to prepare and add scheduled task accounts to Password Safe management.

Prepare the Scheduled Tasks

1. On the asset where the scheduled task resides, open the **Task Scheduler** snap-in and end the task if running.
2. Right-click the scheduled task, and then select **Properties**.
3. On the **General** tab, click **Change User**, and enter the local or active directory account and current credentials. If required, retrieve

a password using the Password Safe administrator login.

4. Run the task to verify it runs successfully.

Run a Scan on the Scheduled Tasks Assets

1. In the BeyondInsight Console, click **Discovery Scan** to run a **Detailed Discovery Scan** against the target systems to add the systems as assets in BeyondInsight. The detailed scan collects data for the scheduled tasks for the targets.
2. Add the discovered assets to Password Safe management.
3. Verify the following:
 - From the **Assets** page:
 - Select the asset, and then click the vertical ellipsis button for the asset.
 - Select **Go to advanced details**.
 - Under **Scan Data**, click **Scheduled Tasks**.
 - Confirm the scheduled tasks were collected.
 - Click the **i** button for each scheduled each task and verify the **Run As** account name is correct.
 - From the **Managed Systems** page:
 - Select the managed system, and then click the vertical ellipsis button for the system.
 - Select **Edit Managed System**.
 - Verify that **NetBIOS Name** is entered.
4. From the **Managed Accounts** page:
 - Select the managed account associated with the scheduled task, and then click the vertical ellipsis button for the managed account.
 - Select **Go to Advanced Details**.
 - Click **Propagation Actions** from the **Advanced Details** pane.
 - Click **Assign Propagation Action** and assign the **Update Scheduled Tasks** action to this account.
5. From the **Managed Accounts** page:
 - Select the managed account associated with the scheduled task, and then click the vertical ellipsis button for the managed account.
 - Select **Test Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.
 - Click the vertical ellipsis button for the managed account again.
 - Select **Change Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.
6. Run the scheduled task to verify the password change. The password change is successful if the scheduled task starts. Otherwise, the password change is not successful. Go through all the steps in this chapter to troubleshoot.

Manage Windows IIS Application Pool Accounts

When an IIS application pool account is under Password Safe management, the following occurs when the managed account password changes:

- An IIS application pool that is running restarts when the password is changed.
- An IIS application pool that is stopped is not started when the password is changed.

Before adding an IIS application pool account to Password Safe management, be sure to:

- Start the IIS Admin Service on the target.
- Verify machines are in the domain, if applicable.
- Verify assets are managed with a local administrator account if not in the domain, or with a domain administrator account if in the domain.

Complete the following procedures to prepare and add IIS application pool accounts to Password Safe management.

Run a Scan on the IIS Application Pool Assets

1. In the BeyondInsight Console, click **Discovery Scan** to run a **Detailed Discovery Scan** against the target systems to add the systems as assets in BeyondInsight. The detailed scan collects data for the IIS application pools for the targets.
2. Add the discovered assets to Password Safe management.
3. Verify the following:
 - From the **Assets** page:
 - Select the asset, and then click the vertical ellipsis button for the asset.
 - Select **Go to advanced details**.
 - Under **Scan Data**, click **Application Pools**.
 - Confirm the IIS application pools have been collected, and that their **Identity** account name is correct.
 - From the **Managed Systems** page:
 - Select the managed system, and then click the vertical ellipsis button for the system.
 - Select **Edit Managed System**.
 - Verify that **NetBIOS Name** is entered.
4. From the **Managed Accounts** page:
 - Select the managed account associated with the IIS application pool, and then click the vertical ellipsis button for the managed account.
 - Select **Go to Advanced Details**.
 - Click **Propagation Actions** from the **Advanced Details** pane.
 - Click **Assign Propagation Action** and assign the **Update IIS Application Pools** or **Update and Restart IIS Application Pools** action to this account.
5. From the **Managed Accounts** page:
 - Select the managed account associated with the IIS application pool, and then click the vertical ellipsis button for the managed account.
 - Select **Test Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.
 - Click the vertical ellipsis button for the managed account again.
 - Select **Change Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.

Manage Windows Auto Logon, COM+ Application, DCOM Application, SCOM RunAs Identities Accounts

Complete the following procedures to prepare and add a service to Password Safe management.

Run a Scan on the Service Assets

1. In BeyondInsight, click **Discovery Scan** to run a **Detailed Discovery Scan** against the target systems to add the systems as assets in BeyondInsight. The detailed scan collects data of the services for the targets.
2. Add the discovered assets to Password Safe management.
3. From the **Managed Accounts** page:
 - Select the managed account associated with the service, and then click the vertical ellipsis button for the managed account.
 - Select **Go to Advanced Details**.
 - Click **Propagation Actions** from the **Advanced Details** pane.
 - Click **Assign Propagation Action** and assign the the appropriate Windows Auto Logon, COM+ Applications, DCOM Applications, and SCOM RunAs Identities propagation actions for this account.
4. From the **Managed Accounts** page:
 - Select the managed account associated with the service, and then click the vertical ellipsis button for the managed account.
 - Select **Test Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.
 - Click the vertical ellipsis button for the managed account again.
 - Select **Change Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.



Note: The functional account associated with the SCOM Managed System must be added to the Operations Manager Administrators profile in the SCOM Operations Manager Console.

Configure Password Safe Global Settings

1. In the BeyondInsight console, go to **Configuration > Privileged Access Management > Global Settings**.
2. Set the options in each of the sections below. Click the **Update** button for each section to apply changes made in that section.

Sessions

Setting	Description / Action
Connecting to systems using	Choose how you want to connect to systems. Select DNS Name or IP Address , or All if you want multiple connection options to be available.
Default RDP port for new Managed Systems	Change the default port for all RDP sessions.
Token timeout for remote session playback	Change the default timeout. The default is 30 seconds. The range is 10 - 60 seconds.
Session initialization timeout	Change the default session token value. The default is 60 seconds. The range is 5 - 600 seconds. Applies to SSH, RDP, and application sessions.
Default RDP screen resolution	Change the default screen resolution. Range is 640x480 - 1920x2058 pixels. An option is available to allow the client application to select screen resolution.
Allow multiple monitors in remote desktop sessions	Check this option to allow more than one monitor in a remote desktop session.
Enable smart sizing by default	Check this option to resize the RDP window to match the size of the user's screen.
Allow users to select a remote proxy	Check this option if you want users to be able to select specific BeyondInsight instances when making requests.
Make smart card device available in remote desktop sessions	When this option is checked, the user must log in to the session using smart card credentials when configured for the system. This setting applies to all RDP sessions and is disabled by default.
Hide record check box for ISA sessions	This option is checked by default. When this option is checked, ISA sessions are recorded and the Record Session check box is not available on ISA session requests. Uncheck this option if you want the Record Session check box available on the requests, giving the user the option to record the session.
Hide record check box for Admin Sessions	This option is checked by default. When this option is checked, Admin sessions are recorded and the Record Session check box is not available on the Start Admin Session form. Uncheck this option if you want the Record Session check box available on the form, giving the user the option to record the session.

Setting	Description / Action
Allow desktop background in remote desktop sessions	Controls whether the desktop background is displayed in the remote session. Can be disabled in scenarios of slower network connections.
Bypass SSH Connection Tests	<p>This option is disabled by default; therefore, Password Safe performs a quick connectivity test to the target system to validate it's online and available. Checking this option to bypass the SSH connectivity test can be useful in environments when systems may not always be online and available.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note: <i>Allowing the test to happen can result in a faster connectivity failure response back to the user (ie: a 5 sec test vs a 30 sec timeout for an SSH connection). If systems are consistently available, then the test can be bypassed to slightly reduce the initial connection time.</i></p> </div>

Requests

Setting	Description / Action
Require a ticket system and ticket number for ISA requests	Enable to have mandatory completion of the Ticket System and Ticket Number fields on all requests.
Display who has approved sessions	Enable this option on all requests.
Reason is required for new ISA requests	Enable this option on all requests.
Auto-select access policy for Quick Launch	Enable to automatically select the best access policy. When this option is selected, the access policy with the most available actions, or multiple access policies will be selected if each one has a different action. When this option is not selected, all the available access policy schedules will display when using Quick Launch .
Bypass SSH Landing Page for Quick Launch	Enable to save time for users when connecting using Quick Launch .
Bypass SSH Landing Page for regular or ISA requests	Enable to bypass the SSH landing page when running an SSH Session or SSH Application Session, and instead directly open PuTTY. This setting applies only to regular requests, ISA requests, and admin sessions. It does not apply to sessions initiated using Quick Launch .
Domain Account Concurrency Behavior	<p>This setting defines how the Concurrent setting in an access policy applies the checkout concurrency for a domain account.</p> <p>When Account is selected, Password Safe applies the checkout concurrency to how many concurrent sessions a domain account may have per environment.</p> <p>When Account and System is selected, Password Safe applies the checkout concurrency to how many concurrent sessions a domain account may have per system in an environment.</p>
View Password and SSH Session request display timeout (seconds)	Enter a number between 0 and 300 seconds, to set the maximum time for viewing a credential. The default is 120 seconds. Setting this number to 0 disables the timer, and the credential remains visible until the user closes the view or navigates away from the screen.

 For more information, please see "[Add Ticket Systems to the List on the Requests Page](#)" on page 164.

Session Monitoring

Setting	Description / Action
Keystroke logging for admin session (RDP)	Records keystrokes for recorded RDP admin sessions that can be viewed in the right pane when viewing a recorded session. This is enabled by default. Uncheck this option to disable keystroke recording for RDP admin sessions.
Keystroke logging for admin session (SSH)	Records keystrokes for recorded SSH admin sessions that can be viewed in the right pane when viewing a recorded session. This is enabled by default. Uncheck this option to disable keystroke recording for SSH admin sessions.
Keystroke logging for ISA (RDP)	Records keystrokes for recorded RDP ISA sessions that can be viewed in the right pane when viewing a recorded session. This is enabled by default. Uncheck this option to disable keystroke recording for RDP ISA sessions.
Keystroke logging for ISA (SSH)	Records keystrokes for recorded SSH ISA sessions that can be viewed in the right pane when viewing a recorded session. This is enabled by default. Uncheck this option to disable keystroke recording for SSH ISA sessions.
Keystroke logging for ISA (Application)	Records keystrokes for recorded ISA application sessions that can be viewed in the right pane when viewing a recorded session. This is enabled by default. Uncheck this option to disable keystroke recording for ISA application sessions.
Enhanced session auditing for ISA (RDP)	Enhanced session auditing captures and records all mouse activity in the Keystrokes menu of Recorded Sessions for RDP sessions. Enhanced session auditing is enabled by default. It uses the rules in the access policy for Admin Session multi-session checkouts. During a recorded RDP session, an agent called pbpsmon is installed on the host for the duration of the session. The agent monitors and audits Windows click events.
Enhanced session auditing for ISA (application)	Enhanced session auditing captures and records all mouse activity in the Keystrokes menu of Recorded Sessions for RDP application sessions. Enhanced session auditing is enabled by default. It uses the rules in the access policy for Admin Session multi-session checkouts. During a recorded RDP session, an agent called pbpsmon is installed on the host for the duration of the session. The agent monitors and audits Windows click events.

 **Note:** Session monitoring captures text that is copied in an RDP session window. The copied text is captured only the first time. Any subsequent copy tasks of the same text are not captured for the session.

 **Note:** To use enhanced session auditing, the functional account of the managed Windows host or Remote Desktop Services host must have administrative rights.

 For information on Session Monitoring options, please see "[Configure Session Monitoring](#)" on page 147.

Purging

Setting	Description / Action
Minimum retention for old password	Set the number of days to retain old passwords. The default is 30 days. The range is 1 - 360 days.
Number of old passwords to retain	Set the number of past passwords to retain. The default is 5 passwords. The range is 1 - 30 passwords. <div style="border: 1px solid black; padding: 5px; background-color: #e6f2ff;">  Note: Password Safe will retain, at minimum, a number of passwords equal to the total of the current password (1) plus the value for Past Passwords. Password Safe will delete all passwords that are older than the number of days equal to the value of Minimum Retention Days. </div>
Retention period for sent mail log	Set the number of days to store log entries for sent email. The default is 30 days. The range is 1 - 365 days.
Retention period for admin log	Set the number of days to store the administrator activity logs. The default is 90 days. The range is 30 - 365 days.
Retention period for password change log	Set the number of days to store password change logs. The default is 90 days. The range is 30 - 365 days.
Retention period for password test results	Set the number of days to store success and failure results for automated password tests. The default is 30 days. The range is 10 - 90 days.
Retention period for system event log	Set the number of days to store system event logs. The default is 365 days. The range is 5 - 1095 days.

Miscellaneous

Setting	Description / Action
Unlock accounts on password change	Enable for locked accounts to automatically unlock when their password has changed.
Enable Rebex debug logging	Enable Rebex debug logging to troubleshoot custom platform issues.
Jumphost connection format	Select Hostname or IP Address .
Enable automatic admin notifications for failed password events	Failed email notifications can be sent to multiple admin accounts. Disable to stop sending admin notification emails, or enable to start sending admin notification emails. This setting is disabled for new installations but enabled for existing installations.
Enable automatic notifications for failed propagation events	Notifications are sent to the email address assigned to the Managed System, Managed Account, or Active Directory managed system. Disable to stop sending propagation notification emails, or enable to start sending propagation notification emails. This setting is enabled by default for all new installations.



Tip: To access propagation and password events from the BeyondInsight console, click **Managed Accounts** in the left menu. Click the vertical ellipsis to the right of a managed account, and then select **Go to Advanced Details**. Under **Advanced Details**, click **Events**.

Changes made to **Global Settings** can be seen on the **User Audits** page:

1. Go to **Configuration > General > User Audits**.
2. Changes that were made to Password Safe **Global Settings** are indicated as **PMM Global Settings** in the **Section** column. Click the **i** button for the audit item to view more details about the action taken.

Showing all 2 User Audits    

Section	Username	IPAddress	
PMM Global Settings	Administrator		



Note: Network traffic can create delays in establishing the connection. Increase the token timeout if you are experiencing network timeouts. For more information on multi-node session playback, please see "[Configure Recorded Sessions in a Multi-Node Environment](#)" on page 150.

Add Databases to Password Safe

There are two ways to discover and manage database instances:

- Auto-discover using a scan template, and then auto-manage using a Smart Group. Use this method for SQL Server and Oracle.
- Manually add and manage databases. Use this method for MongoDB, MySQL, Sybase ASE, and Teradata.

Auto Discover and Manage Database Instances

The following scan types include database instance data in the scan results:

- **Detailed Discovery Scan:** This scan requires credentials and it deploys a scan agent to the scan targets. Besides systems, this scan provides associated information on services, scheduled tasks, users, and databases.
- **Advanced Discovery Scan:** This scan performs the same operations of the detailed scan, but provides information on all associated attributes.

After you run a scan, the assets are displayed on the **Assets** page. At this point, you can create a Smart Rule to manage the database instances.

1. From the left menu, click **Smart Rules**.
2. Click **+ Create Smart Rule**.

3. Select or create a new category and provide a name and description for the Smart Group.
4. For selection criteria, select **Address Group**, and then select the group that includes the database instances.
5. Add another condition, select **Host Database Instance**, and then select the database types.
6. For the actions, select **Show asset as Smart Group**.
7. Add more actions of **Manage Assets using Password Safe**, and then select the platforms, account name formats, functional accounts, and other desired settings, ensuring to use the default port numbers for the databases:
 - Oracle: **1521**
 - SQL Server: **1433**
8. Click **Create Smart Rule**.

 **Note:** An Oracle database can be part of a database cluster. If several nodes are found through discovery, only a single database managed system is created. Cluster fail over is supported.

 **Note:** The Smart Rule auto-excludes the functional account assigned for that system, as well as the **sa** account for MS SQL Server systems, from Password Safe onboarding. The **sa** account is excluded as a precaution against it being inadvertently onboarded by mistake. If you want Password Safe to manage the **sa** account, you can either manually create the managed account or use the **Create Managed Account on each system Smart Rule** action in a Managed System Based Smart Rule.

 **Tip:** To view the contents of a Smart Rule when creating a new rule or editing an existing rule:

- Once the rule is saved, click **View Results**.
- You are taken to the associated grid, where the contents of the Smart Rule are listed.
- If the rule is actively processing, a banner displays letting you know that.

Create New Asset Based Smart Rule

Details

Category: Servers

Name: MSSQL and Oracle Databases Active

Description: Discover MSSQL and Oracle Databases

Reprocessing limit: Default

Selection Criteria

Include items that match ALL of the following

- Address Group: address group
- Use to discover new assets during scans
- Host Database Instance: MS SQL Server, Oracle

[Add another condition](#) [Add a new group](#)

Actions

- Show asset as Smart Group
- Manage Assets using Password Safe
 - Platform: MS SQL Server
 - Account Name Format: Domain\Username
 - Functional Account: lwm db functional account
 - Enable Automatic Password Management: yes
 - Enable Accounts For AD Queries: no
 - Password Rule: Default Password Policy
 - Connection Timeout: 30
 - Port: 1433
- Manage Assets using Password Safe
 - Platform: Oracle
 - Change Agent: Password Safe
 - Account Name Format: Domain\Username
 - Functional Account: .local\administrator
 - Enable Automatic Password Management: yes
 - Enable Accounts For AD Queries: no
 - Password Rule: Default Password Policy
 - Elevation: None
 - Connection Timeout: 30
 - Port: 1521

[Add another action](#)

Create Smart Rule **View Results** **Discard**

**Note:**

- **View Results** displays only if you have permissions to the grid corresponding to the Smart Rule, i.e.; Assets, Managed Accounts, Managed Systems.
- The Smart Rule must be saved with **Show <entity> as Smart Group** selected under **Actions** to view the results.



Tip: Because the Smart Rule must process to display the contents in the grid, we recommend viewing the results using only the **Show <entity> as Smart Group** action and before adding additional actions that may make changes to accounts and assets in your network.

Once you have confirmed the rule contains your desired items, you can then add additional actions to the Smart Rule.

Manually Add Database Instances

You can manually add the following database instance types. When selecting the database platform, ensure the correct port number is displayed.

- Mongo: **27017**
- MS SQL Server: **1433**
- MySQL: **3306**
- Oracle: **1521**
- PostgreSQL: **5432**
- SAP HANA: **30015**
- Sybase ASE: **5000**
- Teradata: **1025**

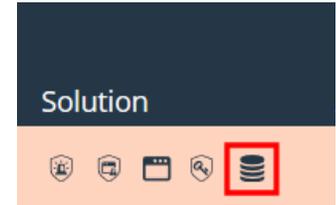
Manually Add Databases to Assets Managed by Password Safe

1. From the left menu, click **Assets**.
2. Click the vertical ellipsis button for the asset, and then select **Go to Advanced Details**.
3. Under **General Data**, click **Databases**.
4. Click **+ Add Database** above the grid.
5. Provide a name, select the platform, add a version, leave the default port, and then click **Save Database**.

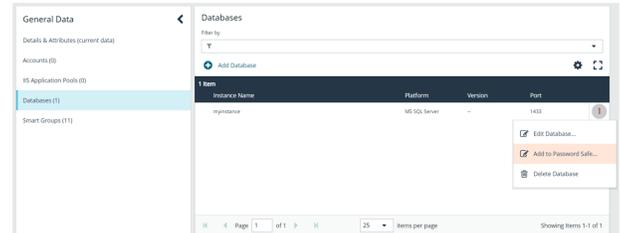
Manually Add Databases to Password Safe Management

1. From the left menu, click **Assets**.

- Assets that host database instances are indicated by a **Database Host** icon in the **Solution** column.



- Click the vertical ellipsis button for the desired asset, and then select **Go to Advanced Details**.
- Under **General Data**, click **Databases**.
- Click the vertical ellipsis button for the desired instance, and then select **Add to Password Safe**.
- On the **Create New Managed System** form, expand **Credentials** and select the functional account.
- Select other settings as desired, and then click **Create Managed System**.



Manage Database Instance Accounts

Once the database instances are managed, create a managed accounts Smart Rule to manage the database instance accounts. The steps are the same for both auto-discovered or manually added database instances.

- From the left menu, click **Smart Rules**.
- Select **Managed Account** from the **Smart Rule type filter** dropdown.
- Click **+ Create Smart Rule**.
- Select **Managed Accounts** from the **Category** dropdown.
- Provide a meaningful **Name** and **Description** for the Smart Rule.

6. Select the criteria to match on the database instance account name, filtering out any named functional accounts.
7. Select **Yes** from the **Discover accounts for Password Safe Management** list.
8. From the **Discover accounts from** list, select the smart group where the database instance resides.
9. In the **Actions** section, select **Show managed account as a Smart Group** from the list.
10. Select **Manage Account Settings** from the list.
11. Select a password rule, and either auto-manage the accounts or do not.
12. Click **Create Smart Rule**.

Create New Managed Account Based Smart Rule

Selection Criteria ⊞

Include items that match ALL of the following

User Account Attribute ⊞ ✕

Account Name ⊞

equals (+) ⊞

instance name ⊞

Discover accounts for Password Safe Management yes ⊞

Discover accounts from All Assets ⊞

Include disabled accounts no ⊞

User Account Attribute ⊞ ✕

Account Name ⊞

does not contain ⊞

and FAPasswordSafe ⊞

Discover accounts for Password Safe Management yes ⊞

Discover accounts from All Assets ⊞

Include disabled accounts no ⊞

[Add another condition](#) [Add a new group](#)

Actions ⊞

Show managed account as Smart Group ⊞ ✕

Manage Account Settings ⊞ ✕

Password Rule Default Password Policy ⊞

Enable Automatic Password Management yes ⊞

Change Password Time 23 ⊞ 30 ⊞

Change Password Frequency Every 30 Days

Default Release Duration Days: 0 Hours: 2 Minutes: 0

Maximum Release Duration Days: 0 Hours: 2 Minutes: 0

ISA Default Release Duration Days: 0 Hours: 2 Minutes: 0

Max Concurrent Request - 1 +

Account Options Change Password after Release, Check Password ⊞

Change Password on Mismatch

Email release notifications to

[Add another action](#)

[Create Smart Rule](#) [View Results](#) [Discard](#)



Tip: To view the contents of a Smart Rule when creating a new rule or editing an existing rule:

- Once the rule is saved, click **View Results**.
- You are taken to the associated grid, where the contents of the Smart Rule are listed.
- If the rule is actively processing, a banner displays letting you know that.



Note:

- **View Results** displays only if you have permissions to the grid corresponding to the Smart Rule, i.e.; Assets, Managed Accounts, Managed Systems.
- The Smart Rule must be saved with **Show <entity> as Smart Group** selected under **Actions** to view the results.



Tip: Because the Smart Rule must process to display the contents in the grid, we recommend viewing the results using only the **Show <entity> as Smart Group** action and before adding additional actions that may make changes to accounts and

assets in your network.



Once you have confirmed the rule contains your desired items, you can then add additional actions to the Smart Rule.



Note: When using MYSQL with multiple accounts with the same name, Password Safe can only support rotating the password on all instances of the username using a functional account.

Discover Accounts for SAP HANA Databases

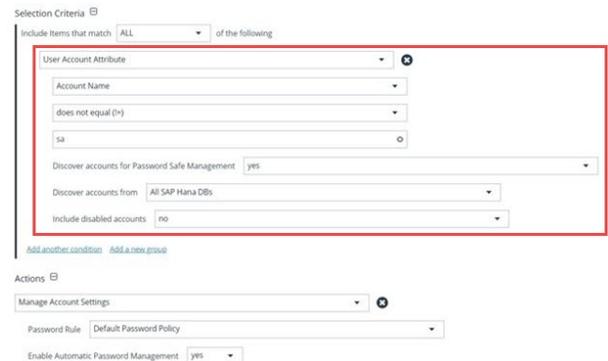
Most database platforms leverage the Discovery Scanner to discover the asset and then find the accounts in the database. SAP HANA, however, does not use the Discovery Scanner. With the SAP HANA database platform, you must manually create the asset and then leverage a managed account Smart Rule for account discovery.



For more information, please see [Add Assets to Password Safe](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/add-assets/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/add-assets/index.htm>.

When creating the managed account Smart Rule, select the following under **Selection Criteria**:

- **User Account Attribute** from the first dropdown list.
- **Account Name** from the second list.
- The appropriate operator from the third list, i.e. contains, equals (=), starts with, etc.
- Enter the appropriate value in the next field.
- **Yes** from the **Discover Accounts for Password Safe Management** dropdown list.
- **All SAP Hana DBs** from the **Discover accounts from** dropdown list.
- **no** from the **Include disabled accounts** dropdown list.
- An existing asset Smart Group that contains the SAP HANA asset (s) in your environment, from the **Discover Accounts From** dropdown list.



The screenshot shows the configuration interface for a Smart Rule. The **Selection Criteria** section is highlighted with a red box and contains the following settings:

- Include items that match: ALL of the following
- User Account Attribute: [Dropdown]
- Account Name: [Dropdown]
- Operator: does not equal (!=)
- Value: sa
- Discover accounts for Password Safe Management: yes
- Discover accounts from: All SAP Hana DBs
- Include disabled accounts: no

The **Actions** section below shows:

- Manage Account Settings: [Dropdown]
- Password Rule: Default Password Policy
- Enable Automatic Password Management: yes



For more information, please see [Work with Smart Rules](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/work-with-smart-rules.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/work-with-smart-rules.htm>.

Create a Functional Account for a SQL Server Database

When you are adding SQL Server as a managed system, you must first create a security login in SQL Server to use for the functional account.

Permissions and Roles in SQL Server

The following roles and permissions are required for the functional account:

- Server roles – public
- ALTER ANY LOGIN
- CONNECT SQL

Apply Permissions to a Functional Account:

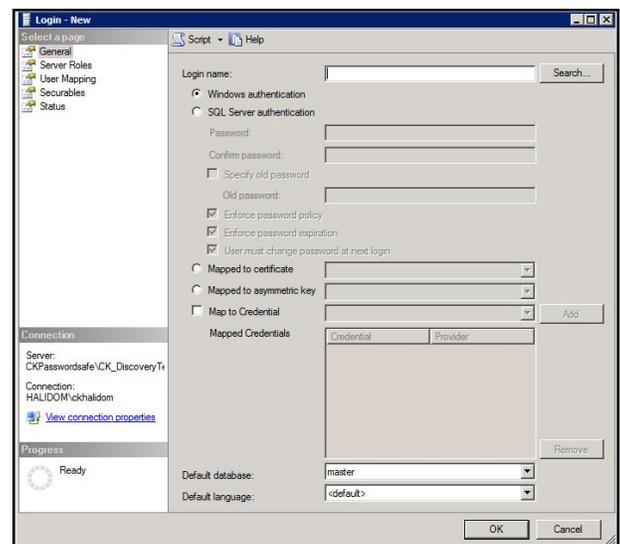
The following code samples show you how to apply the required permissions to the functional account.

```
GRANT CONNECT SQL TO [FunctionalAccountName];
```

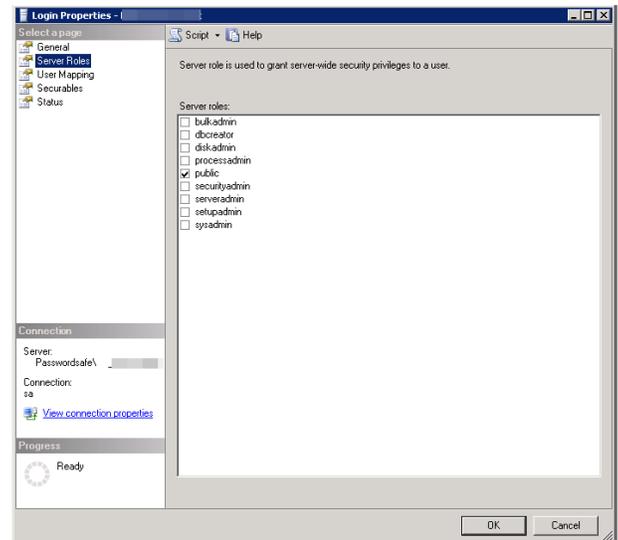
```
GRANT ALTER ANY LOGIN TO [FunctionalAccountName];
```

Create the Account in SQL Server

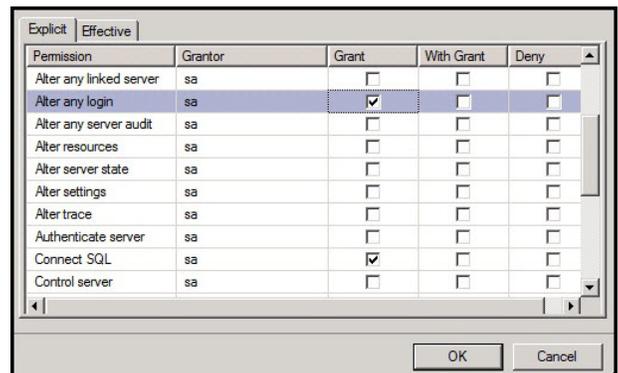
1. Connect to a database as the SQL Server **sa** on the asset you manage.
2. Expand **Security** and expand **Logins**.
3. Right-click **Logins** and select **New login**.
4. Enter a **Login name** and select **SQL Server Authorization**.
5. Enter and confirm a password.
6. Configure the user as desired and click **OK**.



7. To configure the user, right-click the user and select **Properties**.
8. Select **Server Roles** and ensure the public roles is selected.



9. Select **Securables** and click **Search**.
10. Select the server instance and click **OK**.
11. From the list of permissions, ensure the **Alter any login** and **Connect SQL** are selected for **Grantor sa**.
12. Click **OK**.



SQL Server Instance Port Retrieval

To configure a SQL Server database for Password Safe, you must retrieve the port number on the managed database instance using a query. The below query is required for database instances only. You do not need to provide a port number for the default instance.

1. Create an instance on SQL Server.
2. Once the instance is running, open the database and then select **New Query**.
3. Execute the following query as shown on separate lines:

```
GO
xp_readerrorlog 0, 1, N'Server is listening on'
GO
```

4. From the left menu in BeyondInsight, click **Assets**.
5. On the **Assets** page, find the asset where the SQL Server database is installed.

6. Click the vertical ellipsis for the asset, and then select **Go to Advanced Details**.
7. Under **General Data**, click **Databases**.
8. Click **+ Add Database** above the grid.
9. Enter a name for the instance.
10. Select **MS SQL Server** from the **Platform** dropdown.
11. Leave the default port or manually add the correct database port.
12. Click **Save Database**.
13. From the **Databases** grid, click the vertical ellipsis for the newly created database, and then select **Add to Password Safe**.
14. Select the details required for the managed system.
15. Click **Create Managed System**.

Add a PostgreSQL Database Instance

A PostgreSQL database instance must be added manually.

Before adding the instance to Password Safe management, you must create an account in PostgreSQL to use as the functional account in Password Safe.

Create Accounts in PostgreSQL



Note: The following instructions are for guidance only. For details on how to create an account, refer to the PostgreSQL documentation.

To create the account with appropriate level permissions:

1. Run **pgadmin** from the icon on the tray.
2. Right-click **Login/Group** roles, and then click **Create**.
3. Enter a name. This is the functional account.
4. On the **Privileges** tab, ensure the following permissions are in place for the functional account: **Login**, **Create role**, and **Inherit rights from parent roles**.
5. Right-click **Login/Group** roles, and then select **Create**.
6. Enter a name. This is the managed account.
7. On the **Privileges** tab, ensure the following permissions are in place for the managed account: **Login**, and **Inherit rights from parent roles**.

You must also know the database instance name and the port number. In **pgadmin**, click **Object**, select **Properties**, and then click the **Connection** tab.

Add the PostgreSQL Instance to Password Safe

1. Scan the asset where the PostgreSQL instance resides.
2. From the left menu in BeyondInsight, click **Assets**.
3. Click the vertical ellipsis button for the asset, and then select **Go to Advanced Details**.
4. Under **General Data**, click **Databases**.

5. Click the vertical ellipsis button for the desired instance, and then select **Add to Password Safe**.
6. Set the following:
 - **Instance Name:** Enter the instance name.
 - **Platform:** Select **PostgreSQL**.
 - **Version:** Enter the PostgreSQL version number. This is optional.
 - **Port:** The default port value is **5432**.
7. Click **Create Managed System**.

Configure Settings on the Oracle Platform

When adding Oracle as a managed system, follow these steps:

- Add the functional account to the console.
- Add the functional account to the Oracle user list in Oracle.
- Set the IP address for the host in Oracle Net Manager.

Add the Functional Account

1. Select **Configuration**.
2. Under **Privileged Access Management**, click **Functional Accounts**.
3. Click **Create Functional Account**.
4. Select **Database** from the **Type** dropdown list.
5. Select **Oracle** from the **Platform** list.
6. Select **SYSDBA** from the **Privilege** list, and then enter the username and password. The SYSDBA role is required if you use the SYS Oracle account as the functional account.
7. Continue to set the remaining options.



Note: When adding the Oracle platform as a managed system, be sure to select the SYSDBA functional account.



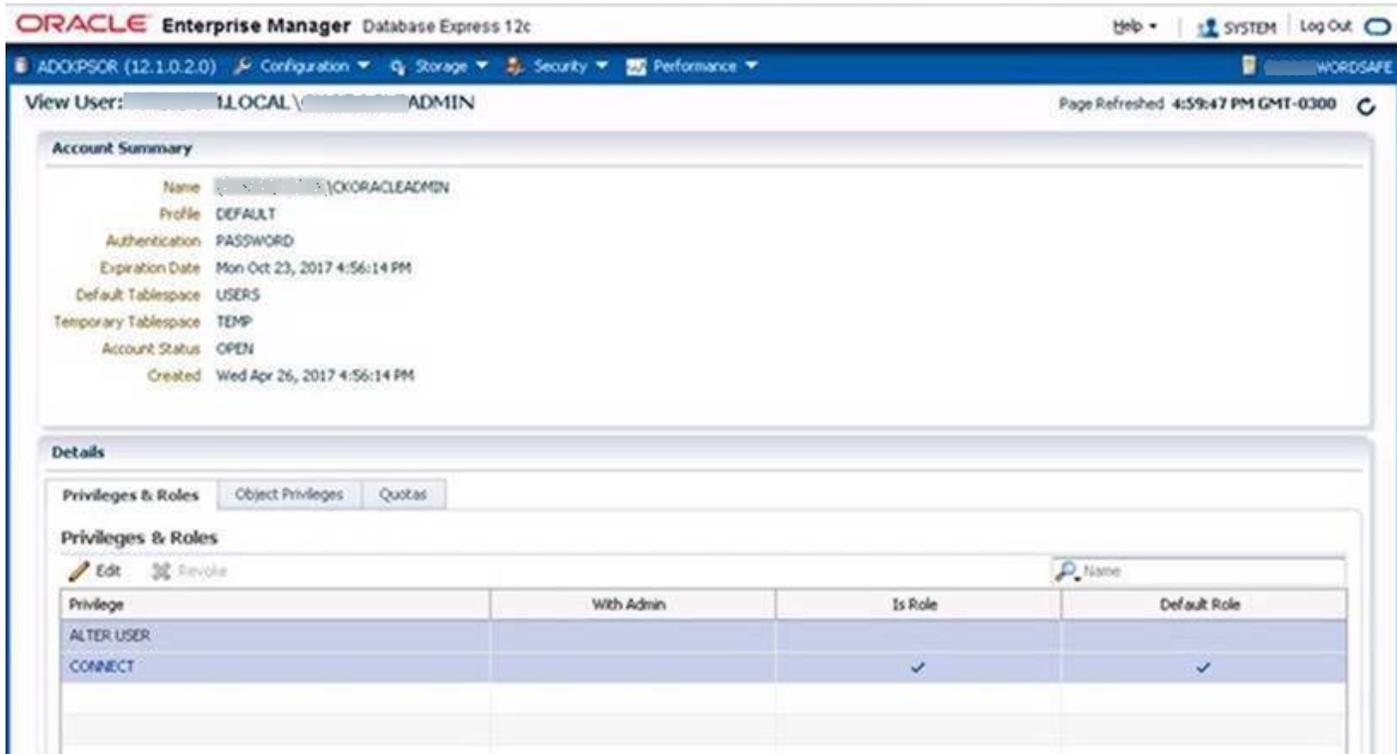
For more information, please see "[Create a Functional Account](#)" on page 16.

Set Permissions for the Functional Account in Oracle

In Oracle Enterprise Manager, the functional account (other than SYS) must be added to the Oracle user list.

The user account must be assigned the following **Privileges & Roles**:

- ALTER USER
- CONNECT
- SELECT ON DBA_USERS (Required for auto Discovery of Oracle instance managed accounts.)



Create the Functional Account in Oracle

To create a functional account in Oracle:

```
CREATE USER [FunctionalAccountName] IDENTIFIED BY password;
GRANT CONNECT TO [FunctionalAccountName];
```

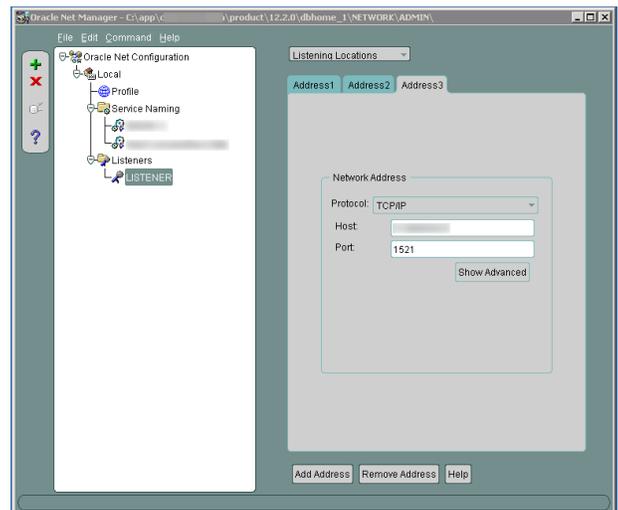
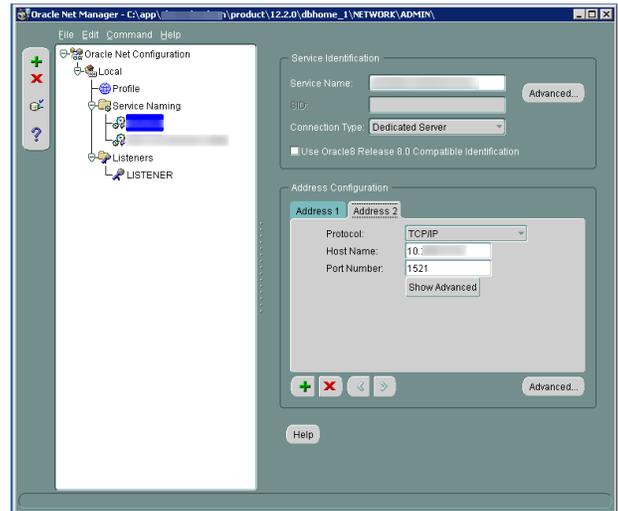
To grant permission to the functional account to change passwords on a managed account:

```
GRANT CONNECT TO [FunctionalAccountName];
GRANT ALTER USER TO [FunctionalAccountName];
GRANT SELECT ON DBA_USERS TO [FunctionalAccountName];
```

Configure the Host

On the Oracle platform, you must configure the following settings:

- In Oracle Net Manager, the host name IP address must be explicitly set as a listener.
- Also in Oracle Net Manager, set the service name as the host name IP address.



Use Encrypted Connections

Password Safe supports Oracle database connections that are configured to use encryption. Using encryption is optional.

The following encryption protocols are supported:

- AES128
- AES192
- AES256
- RC4_128, RC4_256, 3DES112
- 3DES168

Configure encryption using Oracle Net Manager.



Note: The following section is provided for guidance only. For more information, refer to Oracle product documentation.

On the **Profile** node, select **Network Security** and then set the following:

- On the **Integrity** tab, select:
 - **Server** from the **Integrity** menu
 - **required** from the **Checksum Level** menu
 - **SHA256** as the method
- On the **Encryption** tab, select:
 - **Server** from the **Encryption** menu
 - **required** from the **Encryption Type** menu
 - **AES256** as the method



Note: If you select **required** for **Checksum Level** and **Encryption Type**, you must enter an encryption seed in the **sqlnet.ora** file.

Oracle Internet Directories OID

OID Connect Descriptors (also known as TNS Connect Strings) define all parameters needed to connect to a specific Oracle database service, such as the instance name, DNS name, IP address, and port. You can leverage OID Connect Descriptors to add Oracle database systems to Password Safe.

When adding an Oracle database as a Managed System in Password Safe, select the appropriate database service and Password Safe reads the Connect Descriptor data when communicating with the Oracle database.

Create New Managed System
➤

Type
Database ▼

Platform
Oracle ▼

Collapse All |
 Expand All

Identification

Connection Type
Oracle Internet Directories ▼

OID Server
OID LDAP ▼

DB Service
TESTALIAS1 ▼

LOAD

Configure an Oracle Internet Directory

To use this functionality, you must configure an OID, as follows:

1. Go to **Configuration > Privileged Access Management > Oracle Internet Directories**.
2. Click **Create New Oracle Internet Directory +**.
3. Enter a name for the directory, a short description, and information for the LDAP server.
4. Check **Use SSL** if desired.
5. If you turn off **Use Anonymous**, enter a name and password.
6. Click **Create Directory** when done, or **Discard**, if you do not wish to keep it.
7. You can also click **Test Server** to test the connection.

Create New Oracle Internet Directory

Name

Description

LDAP Server

Use SSL

Context

Use Anonymous

Username

Password

Add Applications to Password Safe

Applications can be managed by Password Safe. Requesters can request access to an application and launch a session through the Password Safe web portal. This provides a secure and user-friendly way to manage application access, enhancing overall productivity and security for both requesters and administrators.

Application sessions can be recorded.

Prerequisites

- The application or script must be hosted in a published Remote Desktop Services (RDS) container on the RDS server, that the functional account and managed account can access.
- The host must be accessible on port 3389.
- The system where the application resides must already be added to Password Safe before you can add the application.

To add an application to Password Safe management, you must do the following:

- Set up the application details in Password Safe configuration.
- Associate the application with a managed account.
- Create an access policy that permits application access. Recording and keystroke logging can be turned on here.
- Create a user group that includes the Smart Group containing the managed accounts.
- Assign the **Requester** role to the Smart Group. This includes selecting the access policy.

Add an Application

Follow the steps below to add an application.



Note: Confirm the application or script to be configured in Password Safe is configured and hosted in a published RDS container on the RDS server prior to configuring it in Password Safe.

Please refer to this Microsoft article for more information: [Create a Remote Desktop Services collection for desktops and apps to run at](https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-create-collection)
<https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-create-collection>.

If you require assistance with this process, please contact your system or network administrators, or Microsoft Support if necessary.

1. Select **Configuration > Privileged Access Management > Applications**.
2. Click **Create New Application**.
3. Enter a **Name** (required) and **Version** (optional) for the application. We recommend using the name of the application for transparency.
4. Enter an **Alias** (required). By default, an alias combines the name and version, but can also be edited to display any desired alias.
5. Enter the path to the application in the **Application/Command** (required) field. For example, **C:\Program Files\Windows NT\Accessories\wordpad.exe**.



Tip: Use the **PS_Automate** utility to automate the launch and authentication to a web page or to a standard Windows GUI application, by seamlessly passing vaulted credentials to a remote application. Enter the variable **%PsAutomate%** in the **Application/Command** field to ensure the **PS_Automate** utility is used regardless of the location of the application.

6. Enter the arguments to pass to the application in the **Parameters** (optional) field.

Default placeholders are as follows:

- managed account name = **%u**
- managed account password = **%p**
- managed asset name = **%h**
- managed asset IP = **%i**
- database port = **%t**
- database instance or asset name = **%d**
- jump host dns = **%n**
- database dns = **%s**
- access URL = **%w**

Usage syntax for the **PS_Automate** utility is as follows:

- Web application: **ps_automate.exe [ini=path to inifile][TargetURL=url] [BrowserName=name of browser]**
 - Accepted values for **BrowserName** are: "chrome", "firefox", "msedge"
- Windows application: **ps_automate.exe [ini=path to inifile]**

7. Select an option under **Where do you need the application to run?**:
 - **On the current system** is the default and runs the application on the managed system that the account is currently on.
 - **On a different system** runs the application based on the selections in the **Functional Account** and **Managed System** dropdown lists, i.e. an RDS server or RDS farm.
 - Select a **Functional Account** to connect to the Password Safe managed system hosting the remote application.

Create New Application

Application Name

Application Name is required

Version (optional)

Alias

Application/Command

Parameters (optional)

View Default Parameters Placeholders ▼

Where do you need the application to run?

On the current system
Run the application on whichever managed system the account is currently on.

On a different system
Run the application on the following functional account and managed system

Functional Account

Managed System

Domain linked account behavior

No Association
This application will not be associated with any Linked Systems or Smart Groups

Associate with Linked Systems
The application will be associated with linked systems

Windows

Unix

Associate with Smart Group
The application will be associated with a Smart Group

Smart Group

Autolt Passthrough

Launch Application in RemoteApp mode

Active

- Select a **Managed System**. The managed system must have the application (such as **wordpad.exe**) configured. When starting an application session, an RDP session connects to this application server and starts the application.
8. Select an option under **Domain linked account behavior**:
 - **No Association**: The application is not associated with any Linked Systems or Smart Groups. This applies only when the application is assigned to a directory-type managed account, i.e. Active Directory, LDAP, etc.
 - **Associate with Linked Systems**: The application is associated with linked systems. Select one or both of the following system types:
 - **Windows**
 - If you associate the application with a linked Windows system, standard users see all Windows-based systems applied to the Domain Linked Account when they log in to Password Safe. This excludes Unix systems.
 - **Unix**
 - If you associate the application with a linked Unix system, standard users see all Unix-based systems applied to the Domain Linked Account. This excludes Windows systems.
 - If both options are selected, all systems associated to the Domain Linked Account are shown.
 - **Associate with Smart Group**: The application is associated with a managed system Smart Group. Select a Smart Group from the dropdown list. The application is only associated with linked systems that belong to the selected Smart Group and are linked to the account.
 9. Enable **Autolt Passthrough** to automatically pass the credentials for the application through an RDP virtual channel. Using **Autolt Passthrough** provides a secure way to access applications through a remote session. The user requesting the session is not required to enter the application credentials.
 10. Enable **Launch Application in RemoteApp mode** to initiate a remote app session rather than a full desktop session. This limits use to the specified app and the user is presented with an application window. This setting is defined per application.
 11. Select **Active** to make the application available for remote sessions.
 12. Click **Create Application**.

To edit an application:

1. Navigate to the application and then click the vertical ellipsis to the right of the application.
2. Select **Edit Application**.
3. Make the necessary changes and then click **Save Changes**.

To view advanced application details from the **Edit Application** pane, click **View Advanced Details**.



For more information, please see the following:

- On using the **PS_Automate Utility**, "[Use the PS_Automate Utility](#)" on page 118
- For the prerequisites for **Autolt Passthrough**, "[Use Autolt Passthrough](#)" on page 119

View Application Details

Once an application has been created, you can view advanced application details by following these steps:

1. Select **Configuration > Privileged Access Management > Applications**.
2. Click the vertical ellipsis to the right of the application.
3. Select **Go To Advanced Details**. Under **Advanced Details**, you can select:
 - **Details & Attributes** - This displays a read-only grid containing application information.
 - **Managed Accounts** - This displays a read-only grid listing managed accounts that are linked to the application.

You can edit application details or delete the application using the **Edit** and **Delete** icons, located in the upper-right of the **Advanced Details** page.

Use Encryption Module for RemoteApp

The Encrypted Module for RemoteApp is an application which is automatically enabled to hide sensitive information from the terminal service logs.

To use this encryption, the managed system must be configured with a functional account which is also an administrator on the server the user is connecting to.

Associate the Application with a Managed Account

Now that the application is configured, the application must be associated with a managed account.

1. In the console, click **Managed Accounts**.
2. On the **Managed Accounts** page, click the vertical ellipsis for the managed account, and then select **Edit Account**.
3. In the **Edit Managed Account** pane, scroll down to **Applications** and click **+** to expand the **Applications** section.
4. From the drop-down list, select the applications, and then click **Update Account**.



For more information about editing the managed account settings to select an application, please see ["Add a Managed System Manually" on page 17](#).

Set Up the Access Policy

You can create an access policy or use an existing policy. The access policy is part of the **Requester** role setup, described in the next section.



Note: Application access policies apply to all applications.

1. Select **Configuration > Privileged Access Management Policies > Access Policies**.
2. Create a new access policy and schedule or edit an existing access policy and schedule. Within the schedule settings, enable **Application**, under **Policy Types**, and save the access policy.



For more information on creating and editing access policies and schedules, please see ["Configure Password Safe Access Policies" on page 73](#).

Set Up Role-Based Access

Users who need to access an application must be managed accounts that are members of a group.



Note: Access to applications is also available to admins and ISA users, without the need to configure an access policy.

The **Requester** role and application access are assigned as part of creating the user group.

Use the PS_Automate Utility

Overview

The Password Safe **PS_Automate** utility helps to avoid the need to manually enter credentials when launching Windows GUI applications from Password Safe, saving time and increasing security.

The **PS_Automate** utility allows you to seamlessly pass vaulted credentials from Password Safe to a remote application using the pass through option (using token pass instead of credentials). This includes the ability to launch and authenticate to a web page or to a standard Windows GUI application.

To ensure a seamless experience, the utility supports Incognito mode for popular web browsers, such as Chrome, Firefox, and Microsoft Edge, with Edge being the default. By using an INI file, you can easily specify the input and operational behavior for the utility.

The **PS_Automate** utility, as well as INI files for Amazon Web Services, Azure, Office 365, and Google, are made available when enhanced session auditing is enabled in Password Safe. The files are deployed by the session proxy when a session is created in Password Safe.

The system where the **PS_Automate** utility is deployed must have internet access, in order to automatically download the latest version of the required browser drivers on first use:

- chromedriver.exe
- msedgedriver.exe
- geckodriver.exe

The utility uses the browser drivers, and the versions of the drivers must match the versions of the browsers used.



Note: **PS_Automate** is a utility for Windows only. It is not supported on macOS.

Usage

The usage syntax for the **PS_Automate** utility is as follows:

Web Applications

```
ps_automate.exe [ini=path to inifile][TargetURL=url] [BrowserName=name of browser]
```

Windows Applications

```
ps_automate.exe [ini=path to inifile]
```



Note: For testing purposes the utility also accepts username and password on the command line: **[username=username] [password=password]**. However, this is not recommended for production use, as command line parameters can be written to Windows logs, such as the event log.



Example:

```
ps_automate.exe ini="BIWebApp.ini"  
TargetURL="https://localhost/WebConsole/index.html#!/dashboard" BrowserName="chrome"
```

```
ps_automate.exe ini= "C:\automate\AWSWebApp.ini"  
TargetURL="https://534949981440.signin.aws.amazon.com/console/" BrowserName="firefox"
```

```
ps_automate.exe ini="MSWebApp.ini"  
TargetURL="https://login.microsoftonline.com"BrowserName="msedge"
```

```
ps_automate.exe ini="ssms_database.ini"
```



For more information on defining the command line arguments in the INI file used by **PS_Automate**, please see [Define Command Line Arguments in INI File](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/integrations/ps-automate/command-line-arguments.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/integrations/ps-automate/command-line-arguments.htm>.

Use Autolt Passthrough

The following prerequisites must be in place before you can use the Autolt Passthrough feature:

- The application must be launched through an Autolt script.
- The wrapper Autolt script must call the Password Safe Passthrough library through **pspassthru.dll** (provided as part of the Password Safe Resource Kit).



For more information about turning on the feature, please see ["Add an Application" on page 114](#).

Autolt Script Details

The Autolt example script uses the following functions:

- **pspassthru.dll**
- **ps_get_credentials**
- **DLLCall**: An Autolt function. The first argument takes in the location of the DLL file to call.



*Example: Here the **pspassthru.dll** is located in the same directory as the Autolt script.*

```
Func get_credentials($token)
    Local $aResult = DLLCall("pspassthru.dll", "str:cdecl", "pbps_get_
        credentials", "str", $token, "bool", 0)
    Local $credentials = StringSplit($aResult[0], " ")
    return $credentials
Endfunc
```

ps_get_credentials Function

```
char* ps_get_credentials(char* token, bool respond_with_json)
```

Parameters

char* token: A one-time use token provided by Password Safe as the last command line argument passed to the Autolt script.

bool respond_with_json: A flag to toggle the format of credentials. When this value is **True**, the credentials are in JSON format. Otherwise, they are in a white-space delimited list.

Return Value

The token is sent to Password Safe to be validated.

- If the token is valid for the current session and has not been used, the return value is a string with credentials in the desired format.
- If the token is invalid or has been used, the return value is NULL.

Tokens are validated and credentials are sent over an encrypted RDP virtual channel not visible to the end user.

Add SAP as a Managed System

You can add your SAP environment to Password Safe management.

Password Safe supports **SAP NetWeaver**.

Requirements

- **Instance Number**: When adding the system to Password Safe you must know the SAP instance number.
- **Client ID**: An ID that is unique to the SAP instance.



Note: The instance number and client ID are provided in an email when you purchase SAP.

- **SAP permissions:** The Password Safe functional account requires RFC privileges.

SAP RFC privileges are needed for password changes. RFC permissions assigned to the functional account permit the password change. However, the password cannot be tested.

If an account has RFC privileges, that account can change their password and others. It can also test its own password.

- The username and password in Password Safe must be the same as in SAP.

Set Up the Functional Account

The functional account requires the Client ID. All other settings are the typical functional account settings.



For more information on creating functional accounts, please see ["Create a Functional Account" on page 16](#).

Add SAP

You must add SAP manually. You cannot add SAP using a Smart Rule.

1. In the console, click **Assets**.
2. Select the asset where the SAP instance resides, and then select **Add to Password Safe**.
3. Select **SAP** from the **Platform** list.
4. Enter the instance number.
5. All other settings are the typical managed system settings.



For more information on adding Managed Systems, please see ["Add a Managed System Manually" on page 17](#).

Configure API Registration

Administrators can configure two types of API registrations in BeyondInsight, allowing you to integrate part of the BeyondInsight and Password Safe functionality into your applications. One method uses an API key and the second method uses an Open Authorization (OAuth) authentication access policy for application users. Setting up each type of registration is detailed in the sections below.

Add an API Key Policy API Registration

To create an API key policy API registration:

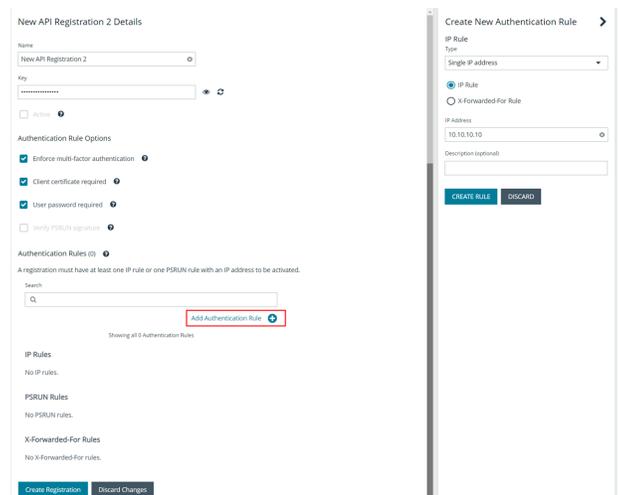
1. Go to **Configuration > General > API Registrations**.
2. Click **Create API Registration**.
3. Select **API Key Policy** from the dropdown list. The **Details** screen is displayed. Fill out the new API registration details, as detailed below:

- Select the **Authentication Rule Options** you wish to enable:
 - **Enforce multi-factor authentication:** This setting is enabled by default. When enabled, requires users to abide by multi-factor authentication settings configured for Password Safe. Disabling this setting bypasses multi-factor authentication when accessing user accounts through API. This allows applications integrated with Password Safe using an API key to abide by multi-factor authentication settings configured for the application, as opposed to using the Password Safe settings.
 - **Client Certificate Required:** When enabled, a client certificate is required with the web request, and if not enabled, client certificates are ignored and do not need to be present. A valid client certificate is any client certificate that is signed by a Certificate Authority trusted by the server on which BeyondInsight resides.
 - **User Password Required:** When enabled, an additional **Authorization** header value containing the RunAs user password is required with the web request. If not enabled, this header value does not need to be present and is ignored if provided.

Square brackets surround the password in the header. For example, the **Authorization** header might look like:

```
Authorization=PS-Auth key=c479a66f...c9484d; runas=doe-main\johndoe; pwd=[un1qu3];
```

- **Verify PSRUN Signature:** The PSRUN signature is an extra level of authentication. It's computed from the factors using a shared secret between the client and server. PSRUN sends the signature as part of the header during its API request. If enabled, the server recomputes the signature during factor validation and compares it against the one sent by the client. If the signatures match, the client's identity is considered verified. The signature effectively keeps the client in sync with the server. Changing the secret on the server requires the client to be rebuilt and guarantees that out-of-date clients cannot authenticate.



- An authentication rule must be included. Click **Add Authentication Rule**.
 - At least one IP rule or PSRUN rule is required, providing a valid source IP address (IPv4 or IPv6), an IP range, or CIDR from which requests can be sent for this API key (one IP address, IP range, or CIDR per line).
 - X-Forwarded-For rules can also be created, providing a valid source IP address (IPv4 or IPv6), an IP range, or CIDR from which requests can be sent for this API key. In a load-balanced scenario, IP authentication rules are used to validate the load balancer IPs, and the X-Forwarded-For header is used to validate the originating client IP. Existing rules cannot be changed from an IP rule to a X-Forwarded-For rule, or vice versa.
 - If an X-Forwarded-For rule is configured, it is required on the HTTP request (only a single header is allowed on the request). If the X-Forwarded-For header is missing, the request fails with a *401 Unauthorized* error.
 - Click **Create Rule**.
- 4. Click **Create Registration**.

BeyondInsight generates a unique identifier (API key) that the calling application provides in the **Authorization** header of the web request. The API key is masked and can be shown in plain text by clicking the **Show Key** icon next to the **Key** field. The API key can also be manually rotated, or changed, by clicking the circular arrow.



Note: Once the key has been changed, any script using the old key receives a "401 Unauthorized" error until the new key is used in its place. Read access and rotation of the key is audited.

Add OAuth Authentication for API Access for Application Users

OAuth is an open standard protocol that allows users to grant limited access to their resources on one website or application to another website or application without sharing their credentials, such as username or password. By enhancing Password Safe authentication to support OAuth, Password Safe application users can benefit from improved overall security and the ease of integration that this feature provides.

OAuth uses access tokens, which are short-lived secrets that grant access to specific resources or APIs on behalf of the application user. Users can revoke access to Password Safe for any connected application or service. This provides more robust control over access to sensitive information.

Application users are a user type that represent applications that interface with the public API. These users can't log in to the web console. They can only authenticate and interact with the public API and they can only authenticate using the OAuth client credential flow for the public API. When creating an application user you must provide an API registration of the type **API Access Policy**, which is specifically used for application users. This API registration is used for processing IP rules instead of the API Key Policy registrations typically assigned to user groups.

Configure API Access Policy Registration

The API Access Policy registration is used specifically for OAuth. To create this in the BeyondInsight console:

1. Go to **Configuration > General > API Registrations**.
2. Click **Create API Registration**.
3. Select **API Access Policy** from the dropdown list. The **Details** screen is displayed.
4. Fill out the new API registration details, including the **Access Token Duration**. This field determines how long the OAuth token stays active.
5. Click **Add Authentication Rule**, enter the required information, and then click **Create Rule**.

Add an Application User

Application users represent applications that interface with the BeyondInsight public API. Application users cannot log in to the BeyondInsight console. They can only authenticate and interact with the public API, using Client ID and Client Secret for credentials within the OAuth client credential flow.

An API Registration type of API Access Policy must be assigned to an application user, and is used for processing IP rules. To create an application user:

1. Go to **Configuration > Role Based Access > User Management > Users**.
2. Click **Create New User**.
3. Select **Add an Application User** from the dropdown list. The **Create New Application User** screen is displayed.
4. Add a username.
5. Under **API Access Policy**, select the policy.
6. Copy the information from the **Client ID** and **Client Secret** fields for later use.
7. Click **Create User**.
8. Assign the user to a group that has the required permissions to access BeyondInsight and Password Safe features.
 - Click the vertical ellipsis for the user, and then select **View User Details**.
 - From the **User Details** pane, click **Groups**.
 - Locate the group, select it, and click **Assign Group** above the grid.

Recycle the Client Secret for an Application User

When editing an application user, you have an option to recycle their secret. Once recycled, you can copy or view the new secret. When a secret is recycled and the user account is updated with this change, the previous client secret is no longer valid.

To recycle the secret for an application user:

1. Go to **Configuration > Role Based Access > User Management > Users**.
2. Locate the application user in the grid.
3. Click the ellipsis to the right of the user, and then select **Edit User Details**.
4. Click the **Recycle** icon to the right of the **Client Secret**.
5. Click **Recycle** on the confirmation message that displays.
6. Copy the new secret for later use.
7. Click **Update User**.

View and Update OAuth Secret Expiry

The user's secret will eventually expire. The **Users** grid has an **OAuth Secret Expiry** column, which you can use to view what is close to expiring. The default duration of a client secret is **365** days. You can adjust the lifetime of the secret from the **Authentication Options** configuration area in BeyondInsight. Updating this value only changes the secret expiry date for new application users and recycled client secrets. Older secrets cannot be updated.

To view the OAuth Secret Expiry for an application user:

1. Go to **Configuration > Role Based Access > User Management > Users**.
2. Locate the application user. The **OAuth Secret Expiry** column lists the date and time that a client secret for that user expires.

To update the duration for client secrets:

1. Go to **Configuration > Authentication Management > Authentication Options**.
2. Under **Application User Authentication Settings**, enter the new duration of the client secret in the **Client Secret Expiry** field.
3. Click **Update Application User Authentications Settings**.



For more information, see the following:

- *API Registrations using the **Auth/SignAppIn API** function, in the [BeyondInsight and Password Safe API Guide](#).*
- *Grant API access to BeyondInsight users in ["Configure API Access" on page 65](#)*
- *[Use Certificates with APIs](#), in the [BeyondInsight and Password Safe API Guide](#).*

Add a Custom Platform or Application Platform

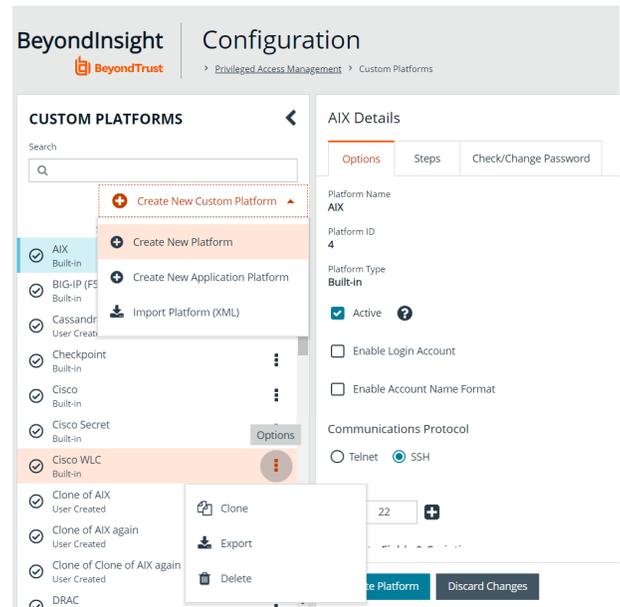
On the **Custom Platforms** page, you can add SSH and Telnet platforms, as well as SSH application platforms, tailored to your environment. Password Safe contains several built-in SSH and Telnet platforms designed for the most common configurations, such as Linux, Solaris, and Cisco. You can modify the details of built-in custom platforms to meet the needs of your environment. You can create new custom platforms for advanced configurations that are not supported by the built-in platforms, or for a platform that is currently not supported by Password Safe. You can also create new custom platforms by cloning a built-in or user-created custom platform.

All custom platforms work in the same way: by connecting to a remote SSH or Telnet server and waiting for a response. Once a response is received, a regular expression is evaluated against the response and the platform replies with a command that starts the process of changing a password on the relevant system.

Create a New Platform

1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management > Custom Platforms**.
2. In the **Custom Platforms** pane, click **Create New Custom Platform**, and then select **Create New Platform**.

Alternatively, click the vertical ellipsis button for a platform in the list, and then select **Clone** to clone an existing platform and modify its settings as desired.



3. Configure the settings on the **Options**, **Steps**, and **Check/Change Password** tabs as detailed in the following sections.

Configure the Options Tab

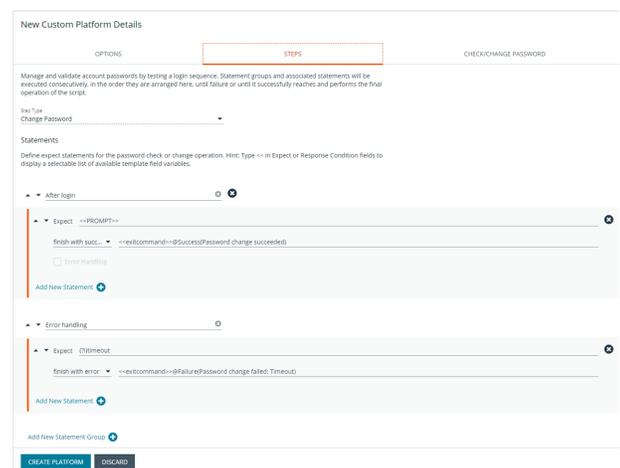
- **Platform Name:** Enter a name for the custom platform. The given name appears in the **Platform** lists throughout BeyondInsight and Password Safe and must be unique. Platform names cannot be changed after they have been created.
- **Platform ID** and **Platform Type** are assigned by the system and cannot be entered or edited.
- **Active:** Check this option to make the platform active in BeyondInsight and Password Safe.
- **Enable Login Account:** Check this option to display the **Use Login Account for SSH Sessions** option under the **Credentials** section in the settings for a managed system. Use this feature when an account other than the functional account is used to log in to the managed system.

- **Enable Account Name Format:** Check this option to display the **Account Name Format** dropdown under the **Credentials** section in the settings for a managed system.
- **Communications Protocol:** Indicate if the custom platform uses **Telnet** or **SSH**.
- **Port:** Use the default port of **22** for SSH or **23** for Telnet. Optionally, enter a port to test the settings.
- **Template Fields and Scripting:**
 - **Prompt regex:** Regular expression that evaluates to the shell prompt of the remote system; for example, `~]#`.
 - **Config prompt regex** and **Elevated prompt regex:** These two regular expressions are mainly meant for network appliances that have multiple prompts, depending on a mode.
 - **End of line:** The end of line field specifies how the platform indicates to the SSH or Telnet server that it is sending a command. The default is the carriage return character (`\r`).
 - **Exit Command:** Leave the default command as **exit**, or specify a new command for the platform to exit SSH or Telnet.
 - **Password command:** Enter the command to change the password.
- **Enable Account Elevation:** Check this option, if you want to select an **Elevation Command**.
- **Elevation Command:** Select an elevation command from the list to enable the option to elevate the functional account permissions on a managed system. The following elevation command types are supported:
 - **sudo**
 - **pbrun**
 - **pmsrun**
 - **pbrun jumphost**
- **Enable Jump Host:** If you use the elevation command **pbrun jumphost**, you can configure the Privilege Management for Unix & Linux policy server host name to connect to. Check this option to enable the jump host, and then enter the policy server host name details when configuring the **Check Password** options on the **Check/Change Password** tab.
- **Enable Cisco Enable Password:** Check this option to display the **Change Enable Password** option on the **Functional Account** tab under **Advanced Details** for a Cisco managed system.

Configure the Steps Tab

From the **Steps** tab, define the responses that you expect from the server and the replies the platform sends. The options include two groups: **After Login** and **Error Handling**.

1. On the **Steps** tab, select the **Step Type** from the list. The template for expect statements changes depending on which of the following types is chosen:
 - **Change Password:** Manually changes the password for the custom platform.
 - **Check Password:** Tests the password by attempting a logon.
 - **Replace Public Key:** Runs a script to replace the public key.
2. Use the default statement group to start the custom platform. Additional statements and statement groups can be created as required.
 - To create a new statement, click **Add New Statement +** at the bottom of an existing statement group.



- To delete a statement, click the **X** at the right end of the **Expect** statement line.
 - To create a new statement group, click **Add New Statement Group +** at the bottom of the last statement group.
 - To delete a statement group, click the **X** and the right end of the statement group name.
 - To edit the name of the statement group, hover the cursor over the group name, click in the field, and then enter the name.
3. Enter an **Expect** statement. There are two ways to populate the **Expect** field:
 - Type text or a regular expression in the field.
 - Use a template field variable: Click in the field, enter **<<**, and then select a template from the list.
 4. Enter a **Response** statement. There are two ways to populate the **Response** field:
 - Type text or a regular expression in the field.
 - Use a template field variable. Click in the field, enter **<<**, and then select a template from the list.
 5. The **Response** type can be changed by selecting an option from the **Send Response** dropdown list. If **goto** is selected you need to select a statement group from the resulting list.
 6. **Error Handling** is enabled by default. Uncheck this option if error handling is not required. If error handling is required, ensure an error message is entered in the **Expect** statement for **Error handling**.
 7. The order of statement processing can be changed by clicking the Up or Down icons at the left of each **Expect** statement.

The following is an explanation of the functionality for each setting on the **Steps** tab, using a Linux platform as an example:

- **Error Handling:** The error handling check ensures that when the statement comes in, all of the statements in the error handling section are evaluated first, before **Enter your reason for login**. For example, when the platform connects to the remote SSH server, the SSH server replies with:

```
Welcome to Linux Mint
* Documentation: http://www.linuxmint.com
Last login: Mon Apr 13 10:45:51 2015 from dev-machine
Enter your reason for login:
```

The platform tries try to find a match, in the following order:

```
- BADCOMMAND
- Usage:
- BAD PASSWORD
- Enter your reason for login:
```

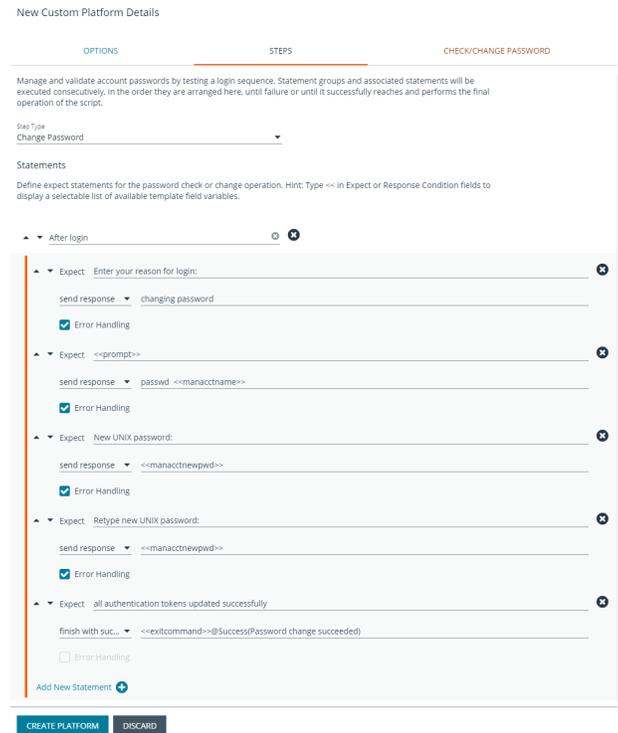
If a match is found for **Enter your reason login**, the platform replies with **changing password**. The platform expects the SSH server to send back the shell prompt and the platform replies with **passwd <<manacctname>>**.

When the platform communicates with the remote server, it replaces the tags with data. In the image shown, **<<manacctname>>** is replaced by the managed account associated with the platform. These are template field variables that are inserted into the **Expect** box and **Response** box. If you have a prompt defined in the options tab as **~] \$**, the platform converts the tag **<<prompt>>** to this value when it evaluates the regular expressions.

- **Expect Statement:** We recommend that you include the prompt in the regex of the **Expect** field to ensure the platform waits until all the data from the previous command is read from the target system before proceeding to the next statement.

The final **Expect** statement says expect **all authentication tokens updated successfully** and the response statement is **finish with success**. When you create a custom platform, you must be able to detect when a password has been successfully changed on the remote server. When you have detected this event, you must set the **Action** dropdown to finish with success.

- **Goto statements:** The flow jumps to the group specified by the **goto** statement. Flow does not return to the original group. If a group is to be used as a goto, it should be designed such that the intended task of the platform is completed there.



Configure the Check/Change Password Tab

Once you complete the fields on the **Check/Change Password** tab, Password Safe runs the credentials. Log in to the host using the managed account name and follow through the configurations provided on the **Steps** tab.

1. Select the **Host** from the dropdown.
2. If you use the elevated credential **pbrun jumphost**, enter the IP address for the PBUL policy server in the **Jumphost** field.



Note: Ensure the **Enable Jump Host** box is checked on the **Options** tab. Otherwise, the **Jumphost** field is not displayed on the **Check/Change Password** tab.

3. Use the default port for SSH or Telnet. Optionally, enter a port to test the settings.
4. Provide the details for the **Functional Account Credentials**.
5. In the **Elevation Command** field, enter an elevated account such as sudo or sudoer to elevate the functional account permissions.
6. Provide **Managed Account Credentials** and a new password.
7. Click **Change Password** or **Check Password**, as applicable.
8. When the test returns a successful connection, go to the **Options** tab, check the **Active** box, and then click **Create Platform**.

OPTIONS
STEPS
CHECK/CHANGE PASSWORD

Enter Functional Account or Managed Account details to perform a password check or change test operation.

Step Type
Change Password Manage Steps...

Host

Jumphost

Port

Asset Name

Functional Account Credentials

Functional Account Name

Functional Account Password

Functional Account "Enable" Password (Optional)

Functional Account "Configure" Password (Optional)

Elevation Command (Optional)

Managed Account Credentials

Use Managed Account to Change Password (Disabled)

Managed Account Name (Optional)

Managed Account New Password

Managed Account Old Password

Timeout after: seconds

Change Password Results
Results for a password check or change operation will appear below when complete.

Create a New Application Platform

Custom application platforms leverage the custom platform functionality, with the added capability of providing an intermediary target (application host) for the custom platform using a script-based approach to managing accounts on application servers specific or customized to your environment.



Note: Custom application platforms only support SSH; Telnet is not supported.

Prior to creating a new application platform, you must configure a managed system to be an application host by enabling the **Allow Managed System to be an Application Host** setting in its properties. The application host is the managed system where the scripts for the application are run.



Note: Once a managed system is configured as an application host, other managed systems can be configured to use it, as indicated by the **Associated Managed Systems** indicator. You cannot disable the **Allow Managed System to be an Application Host** setting if other managed systems are currently configured to use this application host.

Create New Managed System ➤

Entity Type
Asset

Platform
AIX

 Collapse All |  Expand All

Identification 

Name

Port
- 22 +

Description

DNS Name

IP Address

Allow Managed System to be an Application Host (yes)

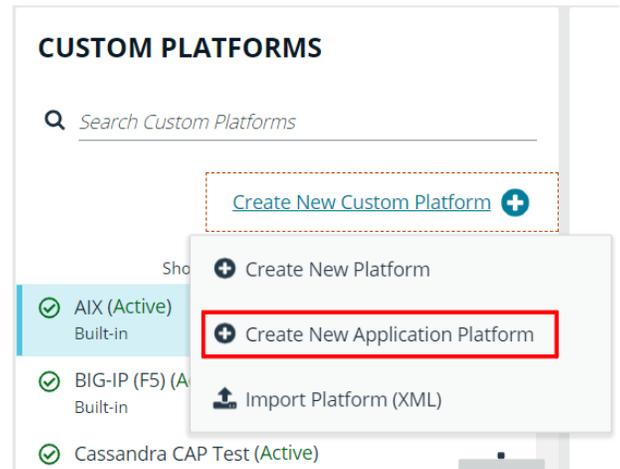
Associated Managed Systems: 0

Workgroup

To create the new application platform, follow the following steps:

1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management > Custom Platforms**.

- In the **Custom Platforms** pane, click **Create New Custom Platform**, and then select **Create New Application Platform**.



- Configure the settings on the **Options**, **Steps**, and **Check/Change Password** tabs as detailed in the following sections.

Configure the Options Tab

- Platform Name:** Enter a name for the custom platform. The given name appears in the **Platform** lists throughout BeyondInsight and Password Safe and must be unique. Platform names cannot be changed after they have been created.
- Platform ID** and **Platform Type** are assigned by the system and cannot be entered or edited.
- Active:** Check this option to make the platform active in BeyondInsight and Password Safe.
- Enable Login Account:** Check this option to display the **Use Login Account for SSH Sessions** option under the **Credentials** section in the settings for a managed system. Use this feature when an account other than the functional account is used to log in to the managed system.
- Enable Account Name Format:** Check this option to display the **Account Name Format** dropdown under the **Credentials** section in the settings for a managed system.
- Enable Account Elevation:** Check this option if you want to select an **Elevation Command**.
- Elevation Command:** Select an elevation command from the list to enable the option to elevate the functional account permissions on a managed system. The following elevation command types are supported:
 - sudo
 - pbrun
 - pmrun
 - pbrun jumphost

New Custom Application Platform Details

OPTIONS

Platform Name
New Custom Application Platform ✕

Platform names cannot be changed after they have been created.

Platform ID --

Platform Type User Created

Active ?

Enable Login Account

Enable Account Name Format

Enable Account Elevation

Elevation Command
sudo ▼

CREATE PLATFORM
DISCARD

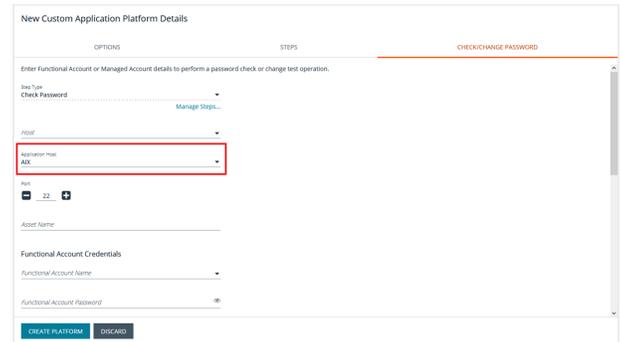
Configure the StepsTab

The **Steps** tab is configured in the same way as it is for all custom platforms. However, for application platforms there are 6 additional fields available for **Expect** statements, as follows:

- **Address**
- **App Host Functional Account Keypass**
- **App Host Functional Account Key**
- **App Host Functional Account Name**
- **App Host Functional Account Password**
- **Port**

Configure the Check/Change Password Tab

The **Check/Change Password** tab is configured in the same way as it is for all custom platforms; however, you must also select an **Application Host**.



The screenshot shows the 'New Custom Application Platform Details' form with three tabs: 'OPTIONS', 'STEPS', and 'CHECK/CHANGE PASSWORD'. The 'CHECK/CHANGE PASSWORD' tab is active. The form contains the following fields and sections:

- Enter Functional Account or Managed Account details to perform a password check or change test operation.**
- App Tab:** Check Password (dropdown menu)
- Host:** (dropdown menu)
- Application Host:** (dropdown menu, highlighted with a red box)
- App:** (dropdown menu)
- Asset Name:** (text input field)
- Functional Account Credentials:**
 - Functional Account Name:** (dropdown menu)
 - Functional Account Password:** (password input field)
- Buttons:** CREATE PLATFORM, DISCARD

Once your custom application platform has been created, you can configure a managed system to use it by selecting it from the **Platform** dropdown. Also select the **Application Host** for this managed system. When Password Safe rotates or checks a password for an account that exists on this managed system, it connects to the application host and then runs the steps as defined on the **Steps** tab for this custom application platform instance.

Create New Managed System ➤

Entity Type
Asset

Platform
New Custom Application Platform

 Collapse All |  Expand All

Identification 

Name

Port
 22 

Description

DNS Name

IP Address

Application Host
AIX

Workgroup

Automatic Password Change Options 

Export or Import a Custom Platform

Export a Custom Platform

Exporting a custom platform can assist you with troubleshooting.

1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management > Custom Platforms**.
2. Click the **Actions** (vertical ellipsis) button for the platform you wish to export, and then select **Export**.
3. Save the XML file.

Import a Custom Platform or Application Platform

1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management > Custom Platforms**.
2. In the **Custom Platforms** pane, click **Create New Custom Platform**.
3. Select **Import Platform (XML)**.
4. Locate and select the exported platform file. If the platform currently exists, it modifies the existing platform. If the platform does not currently exist, a new custom platform is added.



Example: Linux Platform

In this short synopsis of the Linux platform, you can see how it works by expecting data and responding to the data based on the evaluation of regular expressions. It examines the output of each command to determine if an error occurred or if it can continue sending replies to the server.

1. Platform establishes a connection to the remote SSH server with the provided credentials.
2. SSH server replies with:

```
Welcome to Linux Mint
* Documentation: http://www.linuxmint.com
Last login: Mon Apr 13 10:45:51 2015 from dev-machine
dev@dev-machine ~ ]#
```

3. The platform evaluates a regular expression, looking for the shell prompt "**~]#**", and replies with the **passwd** command for the specified managed account.

```
passwd managedaccount complexpassword
```

4. If the arguments passed to the **passwd** command are valid, the server replies with:

```
Enter new Unix Password:
```

5. The platform waits for the server's response and evaluates a regular expression, looking for **Enter new Unix Password**.
6. If the response is not **Enter new Unix Password**, the platform waits for other possible responses such as **User does not**



exist.

7. If the regular expression evaluates to **true**, the platform exits with an error.
8. If the regular expression **Enter new Unix Password** evaluates to **true**, the platform replies with the new password.

Configure SSH and RDP Proxy Connections

In the Password Safe web portal, requesters can request access to use SSH or RDP remote connections. To permit remote connections, you must configure an access policy.

The following section provides additional information on setting up SSH or RDP connections.

i For more information, please see "[Configure Password Safe Access Policies](#)" on page 73.

Requirements for SSH

- You must install PuTTY to enable SSH functionality. Go to www.putty.org to download the software.
- If you use a Windows 8 or Windows Server 2012 VMWare virtual machine, VMWare Tools installs itself as a URL Handler for SSH and stops the sample registry script from working. You must remove the registry variable:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMwareHostOpen\Capabilities\UrlAssociations]"ssh"="VMwareHostOpen.AssocUrl"
```

Host Key Algorithms

Below is a list of host key algorithms enabled for use by Password Safe's SSH client and server. Supported algorithms in default order of preference are:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519
- rsa-sha2-512
- rsa-sha2-256
- ssh-rsa (disabled by default)
- ssh-dss (disabled by default)

Use the following registry key to change the available client host key algorithms:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\client_host_key_algorithms (REG_MULTI_SZ)
```

Use the following registry key to change the available server host key algorithms:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\host_key_algorithms (REG_MULTI_SZ)
```

KEX Algorithms

Below is a list of key exchange (KEX) algorithms enabled for use by Password Safe's SSH client and server. Supported algorithms in default order of preference are:

- curve25519-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group14-sha256
- diffie-hellman-group14-sha1 (disabled by default for incoming client connections only)
- diffie-hellman-group-exchange-sha1 (disabled by default)
- diffie-hellman-group1-sha1 (disabled by default)

Use the following registry key to change the available key exchange algorithms for the client side of Password Safe's SSH proxy (between the proxy and the managed systems):

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\kex_algorithms (REG_MULTI_SZ)

Use the following registry key to change the available key exchange algorithms for the server side of Password Safe's SSH proxy (between the user's SSH client and the proxy):

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\client_kex_algorithms (REG_MULTI_SZ)

MAC Algorithms

Below is a list of message authentication code (MAC) algorithms enabled for use by Password Safe's SSH client and server. Supported algorithms in default order of preference are:

- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1
- hmac-sha1-96 (disabled by default)
- hmac-md5 (disabled by default; not supported in FIPS mode)

Use the following registry key to change the available mac client host key algorithms:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\client_macs (REG_MULTI_SZ)

Use the following registry key to change the available mac server host key algorithms:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\macs (REG_MULTI_SZ)

When Password Safe is running in FIPS mode, every supported MAC algorithm is enabled by default.

Ciphers

Below is a list of ciphers enabled for use by Password Safe's SSH client and server. Supported ciphers in default order of preference are:

- aes256-ctr
- aes192-ctr
- aes128-ctr
- aes256-cbc (disabled by default)
- aes192-cbc (disabled by default)
- aes128-cbc (disabled by default)
- blowfish-cbc (disabled by default; not supported in FIPS mode)
- 3des-cbc (disabled by default)

Use the following registry key to change the available client cipher algorithms:

HKEY_LOCAL_MACHINE\SOFTWARE Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\client_ciphers (REG_MULTI_SZ)

Use the following registry key to change the server cipher algorithms:

HKEY_LOCAL_MACHINE\SOFTWARE Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\ciphers (REG_MULTI_SZ)

When Password Safe is running in FIPS mode, every supported cipher is enabled by default.

RSA Host Key Size

You can configure the size (in bits) of the RSA private host key generated and used by Password Safe's SSH server.

Use the following registry key to change the host key size:

HKEY_LOCAL_MACHINE\SOFTWARE Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\rsa_host_key_size (REG_DWORD)

Valid values are: **2048 (default)**, **3072**, and **4096**.

Auto-Launch PuTTY Registry File

To launch the SSH client automatically, the SSH protocol must be associated with an application. To register an application, such as PuTTY, which is used in the example below, change the references to PuTTY to point to the application.

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\ssh]
@="URL:Secure Shell Protocol"
"URL Protocol"=""
[HKEY_CLASSES_ROOT\ssh\DefaultIcon]
@="%%ProgramFiles%\PuTTY\putty.exe"
[HKEY_CLASSES_ROOT\ssh\shell]
[HKEY_CLASSES_ROOT\ssh\shell\open]
[HKEY_CLASSES_ROOT\ssh\shell\open\command]
@="cmd /V:ON /s /c @echo off && set url=%1 && for /f \"tokens=1,2,3 delims=:/ \" %a in
(!url!) do set protocol=%a&set host=%b&set port=%c && start \"%\
%%ProgramFiles%\PuTTY\putty.exe\" -P !port! !host!"
```

Supported SSH Session Protocols

You can use the following protocols with an SSH session: X11, SCP, and SFTP. You also have options to allow local and remote port forwarding.



Note: When transferring files using SCP, there may be some incompatibilities with specific clients (e.g. WinSCP). We recommend using SFTP or a different client.

Use the Registry Editor to turn these settings on. These settings are all type DWORD with toggle values of either **0** (no) or **1** (yes).

- **X11:**

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\allow_x11 = 1 (DWORD)

- **SCP:**

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\allow_scp

- **SFTP:**

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\allow_sftp

- **Local Port Forwarding:** Whether or not to allow local port forwarding requests from the user's SSH client through to the managed system (default: 0)

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\allow_local_port_forwarding

- **Remote Port Forwarding:** Whether or not to allow remote port forwarding requests from the user's SSH client through to the managed system (default: 0).

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\allow_remote_port_forwarding



For more information, please see [Issues with WinSCP Using SCP Mode](https://beyondtrustcorp.service-now.com) at <https://beyondtrustcorp.service-now.com>.

Multiple SSH Sessions

To avoid a potential security risk, more than one SSH session is not permitted through a single SSH connection.

You can turn on the following registry key to permit more than one session on a connection:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\allow_multiplex = 1

Enable Login Accounts for SSH Sessions

Creating a login account allows the user to open an SSH session in environments where remote shell access is not permitted, for instance, the root account. A login account will be used to establish the initial shell connection and then switch the session to the managed account.



Note: The functional account used should be a low privilege user and not the same elevated functional account that has elevated privileges to change passwords.

This feature supports the following platforms: **AIX**, **HPUX**, **Linux**, and **Solaris**.

Enable Login Accounts Manually

To manually enable login accounts, you must enable the function on both the managed system and the managed account you want to use for the SSH session.

1. From the **Managed Systems** page, create a new managed system, or select one from the grid.
2. From the menu actions, select **Edit Managed System**.
3. Within the **Credentials** section, toggle the **User Login Account for SSH Sessions** option to **yes**.
4. Select your account from the **Login Account** dropdown.
5. Click **Update Managed System** and dismiss the configuration slide-out.
6. From the **Managed System** menu, select **Go to advance details**.
7. Select the **Managed Accounts** tab.
8. Select the managed account you wish to edit.
9. Within the **Credentials** section, toggle the **Login Account for SSH Sessions** option to **yes**.
10. Click **Update Account**.

Enable Login Accounts with a Smart Rule

For organizations managing many assets and accounts, administrators can enable login accounts with a Smart Rule as follows:

1. Create a Smart Rule to manage the assets to use to access the SSH session.
2. Select the action **Manage Assets using Password Safe**.
3. Select the platform and the functional account.
4. From the **Enable Login Account for SSH Session** list, select **yes**.
5. Select a login account.
6. Create a Smart Rule to manage the managed accounts to allow users to log in for an SSH session.
7. In the **Actions** section, select **Managed Account Settings**.
8. Scroll to **Account Options** and select **Enable Login Account for SSH Sessions**.

Use Direct Connect for SSH and RDP Session Requests

You can use Direct Connect for remote session requests for SSH and RDP sessions. Direct Connect requests access to a managed account on behalf of the requester. The requester accesses the system without ever viewing the managed account's credentials.

If the requester is not granted auto-approval for a session, the user receives a message stating *Request requires approval. If the request is not approved within 5 minutes this connection will close*. After 5 minutes the client disconnects and the user can send another connection request. When the request is approved, the user is automatically connected.

When there is an existing request for the system and account, the request is reused and the session created.

SSH Session Requests

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

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

- **For UPN credentials:**

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

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

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

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

- **For UPN credentials:**

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

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

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

- **For an SSH application:**

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

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

RDP Session Requests



Note: RDP Direct Connect supports push two-factor authentication. An access-challenge response is not supported. LDAP users that use the mail account naming attribute cannot use RDP Direct Connect.

To request an RDP session using Direct Connect:

1. Click the arrow to download the RDP Direct Connect file from Password Safe.

This is a one-time download. Each account and system combination requires that the user download the unique RDP file associated with it.

Status	Platform	Application	Workgroup	ISA
1 of 1 available	Windows			
1 of 1 available	Windows			

Download RDP Direct Connect file

2. Run the file to establish a connection to the targeted system.
3. The requester is then prompted to enter the password they use to authenticate with Password Safe.

Direct Connect Delimiters

You can customize the character delimiters accepted in a Direct Connect connection string (in addition to + and @) by setting the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\direct_connect\delimiters (REG_SZ)

Additionally, you can enable support for a dynamic delimiter. When this is enabled, any connection string that starts and ends with the same non-alphanumeric character is split on that character.



Example: '/' used as the delimiter:

```
ssh -p 4422 /requestor/maccount/msystem/@bihost
```

To enable dynamic delimiters (default is off), set the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\direct_connect\dynamic_delimiter = 1 (REG_DWORD)

Use Two-Factor Authentication Token

RDP and SSH Direct Connect sessions support using a two-factor authentication token.

- **RDP session:** A delimiter (,) must be entered after you enter the password. For example: **password, token**

The delimiter can be changed using the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\rdp_proxy\2fa_delimiter

The delimiter must be excluded from user login passwords.

- **SSH session:** You are prompted to enter a token after you enter the password.

Configure RDP Sessions

Certificate Authentication

To ensure secure communications, an RDP session uses the same certificate as the certificate created for the web portal. The certificate supports SSL/TLS authentication types.

Create a Certificate and Add to the BeyondInsight Server

To avoid certificate error messages when initiating an RDP session, create a certificate signed by a valid Certificate Authority (CA) for the BeyondInsight server. Add that certificate and the certificate chain to the BeyondInsight server certificate stores. Use the high-level steps below as guidance:

Create the Certificate Request

1. On the BeyondInsight server, open IIS Manager.
2. On the local host node, select **Server Certificates**, and then select **Create Certificate Request**.
3. Go through the **Request Certificate** wizard. On the **Cryptographic Service Provider Properties** page, select a bit length of **2048**.



Note: The **Common Name** equals the server name or the IP address, depending on the URL you are using for the BeyondInsight log in page.

For example, server name might be an IP address, the server short name, or a fully qualified domain name:

https:\\<server name>\webconsole

common name = <servername>

4. Enter a file name for the certificate request and set the location to the desktop.

Sign the Certificate

The procedure for signing the certificate varies, depending on your company's CA implementation.

1. Go to your Certificate Authority website.
2. On the **Certificate Request** or **Renewal Request** page, copy the text from the certificate request file.
3. Be sure to select **Web Server** as the **Certificate Template** type.
4. After you click **Submit**, download the certificate and certificate chain to your desktop.
5. Copy the files to the BeyondInsight server desktop. This will be the server certificate.
6. Open IIS Manager on the BeyondInsight server, and click **Complete Certificate Request**.
7. On the **Specify Certificate Authority Response** page, find the file on your desktop, enter a friendly name, and use the default **Personal** certificate store.

Bind the Server Certificate to the Default Web Site in IIS

1. Right-click **Default Web Site**, and then select **Edit Bindings**.
2. Select **https on port 443**, and then click **Edit**.
3. From the **SSL certificate** list, select the server certificate created earlier, and then click **OK**.

Add Certificate Chain

1. On the BeyondInsight server, open **mmc** and add the **Certificates** snap-in.
2. Expand **Trusted Root Certification Authorities**.
3. Right-click **Certificates** then select **All Tasks > Import**.
4. Go through the **Certificate Import** wizard to import the certificate chain file (created earlier).
5. Select the appropriate file extension. Be sure to store the certificate in **Trusted Root Certification Authorities**.

Enable Smart Sizing

When in an RDP session, the user can choose to smart size the client window so that no scroll bars display.

You can enable **Smart Sizing** on the **Session Monitoring Configuration** page by checking the box.

Turn Off Font Smoothing

Font smoothing is turned on by default. To turn off font smoothing, change the following registry key value from **0** to **1**

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\rdp_proxy\disable_font_smoothing = 1 (DWORD)

Configure RDP Port for Connection to Target System

Administrators can set an RDP connection port for a specific Windows managed system on a per-system basis. One or more RDP ports can be configured. Administrators can also use a Smart Rule to target a set of managed systems with the new RDP connection port.

- To set the RDP port for a managed system, go to **Configuration > Privileged Access Management > Global Settings > Sessions**, and then enter the **Default RDP port for new Managed Systems**.
- To edit an RDP port, go to **Managed Systems** and then click the ellipsis to the right of the Windows managed system. Select **Edit Managed System**. Under **Identification**, edit the port.
- To set an RDP port using a Smart Rule, go to **Smart Rules**. Select **Asset** under the **Smart Rule type filter**. Click **Create Smart Rule**. Under **Actions**, select **Windows** as the **Platform**, and then set the port.
- To set more than one port, go to **Smart Rules**. Select **Managed System** under the **Smart Rule type filter**. Click **Create Smart Rule**. Under **Actions**, select **Set port on each system**, and then enter the port. Click **Add another action** for each additional port.

Configure Session Proxy Ports

Ports can be configured using the **BeyondInsight** configuration tool. In the configuration tool, scroll to the Password Safe section to set all port values.

The default inbound port connections to the Password Safe proxy:

- RDP: **4489**
- SSH: **4422**
- Session Monitoring Listen Host: **127.0.0.1**
- Session Monitoring Listen Port: **4488**
- Session Monitoring RDP Listen Post: **4489**
- Session Monitoring SSH Listen Post: **4422**

Session Countdown Duration

You can configure the maximum amount of time for which the session countdown timer is displayed by setting the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\rdp_proxy\countdown_duration
(DWORD value in seconds, default is 1800)

SSH Client Check and Change Password Algorithms

When Password Safe checks and changes passwords, it uses the below list of algorithms to connect and communicate.

Authentication Methods	Password, Public key, Keyboard interactive
Encryption Algorithms	AES, Triple DES, Blowfish, blowfish-ctr, blowfish-cbc,
Encryption Modes	CBC, CTR
Host Key Algorithms	RSA, DSS, ecdsa-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, ssh-ed25519
Key Exchange Algorithms	curve25519-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1 (disabled by default), diffie-hellman-group-exchange-sha1 (disabled by default), diffie-hellman-group1-sha1 (disabled by default)
MAC Algorithms	MD5, SHA-1, SHA-2, HMAC-MD5, HMAC-MD5-96, HMAC-SHA1-96
Symmetric Key Algorithms	arcfour256, arcfour128, arcfour

The Following Algorithms Are Disabled by Default

diffie-hellman-group1-sha1	arcfour256	HMAC-SHA1-96
diffie-hellman-group-exchange-sha1	arcfour128	aes256-cbc
blowfish-ctr	arcfour	aes192-cbc
blowfish-cbc	HMAC-MD5	aes128-cbc
3des-cbc	HMAC-MD5-96	

Use the Following Registry Keys to Turn on the Algorithms

- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Eye\RetinaCS\SshKeyExchangeAlgorithms (DWORD) = 1023** (enables all key exchange)
- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Eye\RetinaCS\SshEncryptionAlgorithms (DWORD) = 31** (sets all encryption algorithms)
- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Eye\RetinaCS\MacAlgorithms (DWORD) = 15** (sets all MAC algorithms)



Note: These values are in decimal.

Weak RSA server host keys shorter than 1024 bits are rejected by default. Use the following registry key to change this setting:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Eye\RetinaCS\SshMinimumRsaKeySize (DWORD) = 1024 (size of key and bits)

Configure Session Monitoring

Session monitoring records the actions of a user while they access your password-protected managed systems. The actions are recorded in real time with the ability to bypass inactivity in the session. This allows you to view only the actions of the user.

You configure session monitoring when you add or edit a managed system.

There are additional settings you must configure, such as concurrent sessions and screen resolution.

Configure Listen Host and File Location

Using the BeyondInsight Configuration tool, you can set the listen host and file location for monitored sessions.

1. Open the BeyondInsight Configuration tool.
2. Go to the **Password Safe** section.
3. Enter the IP address for the listen host.
4. Set the location for the session monitoring file. The default location is in the installation directory: `\\data\sessionmonitoring`.

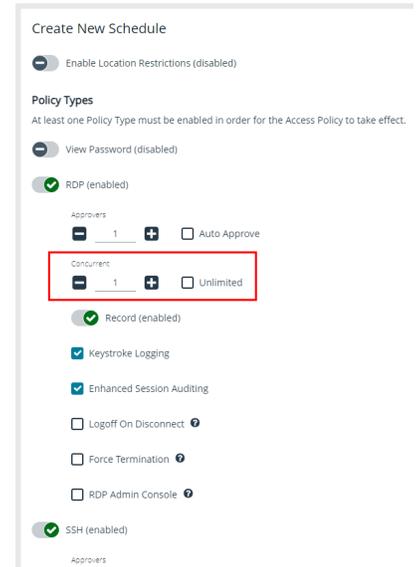
Configure Concurrent Sessions

Remote sessions can be limited to a set number of concurrent sessions.

The option to increase or limit the number of sessions a user can open at one time is configured from the schedule settings within an Access Policy.

To modify the number of concurrent sessions:

1. Navigate to **Configuration > Privilege Access Management Policies > Access Policies**.
2. Select an Access Policy or create a new one.
3. From the **Schedule** tab, select an existing schedule or click **Create New Schedule** to create a new one.
4. Scroll down to **Policy Types** and select **RDP** or **SSH**.
5. Set the number for the **Concurrent** option.
6. Click **Update Schedule** or **Create Schedule** to save the schedule.



Create New Schedule

Enable Location Restrictions (disabled)

Policy Types
At least one Policy Type must be enabled in order for the Access Policy to take effect.

View Password (disabled)

RDP (enabled)

Approvers
 1 Auto Approve

Concurrent
 1 Unlimited

Record (enabled)

Keystroke Logging

Enhanced Session Auditing

Logoff On Disconnect ⓘ

Force Termination ⓘ

RDP Admin Console ⓘ

SSH (enabled)

Approvers

If a user tries to open more sessions than allowed, a message displays on the **Requests** page.

i For more information, please see "[Configure Password Safe Access Policies](#)" on page 73.

Approval History

 Approvals Required: 0 

Date	Submitted By	Response	Comment
7/5/2016 10:36 AM	John Doe	Approved	Auto-approved because this account does not require dual-control

⊖ Check-in Request
⊖ Open SSH Session

This session may be recorded

Cannot create a new session. The limit for concurrent sessions has been reached.

Back to Requests List

Use Session Masking

Passwords can be hidden from session replays by applying a mask. When session masks are active, an SSH session recording at that time checks the keystrokes against the mask. Any matches are replaced. When the keystroke session is replayed, the viewer sees asterisks instead of the password. More than one mask can be active at a time.

Masks can be created, changed, and deleted. These actions are captured in user auditing.

1. Navigate to **Configuration > Privileged Access Management > Session Masks**.
2. To create a mask:
 - Click **Create New Mask** above the grid.
 - Enter a name for the mask and provide the mask pattern.
 - Leave the **Active** option checked.
 - Click **Create Session Mask**.
3. To edit a mask:
 - Locate the mask in the grid and click the vertical ellipsis button for it.
 - Select **Edit Session Mask**.
 - Edit the name and pattern for the mask as desired.
 - Check or uncheck the **Active** option as appropriate.
 - Click **Update Session Mask**.
4. To delete a mask, click the vertical ellipsis button for the mask, and then select **Delete**.

Customize Session Images

As a Password Safe administrator, you can add corporate logos to replace default brand splash, replay, and lock images. You can also specify an image that displays when an RDP session is being monitored and recorded in Password Safe.


IMPORTANT!

You must clear the browser cache to see new images after they have been updated. Also, it is a good practice to back up image files to a safe location because they will be overwritten on the next upgrade and must be replaced after the upgrade completes to restore the customization.

Specify a Custom Splash Image

To customize the splash image:

1. Place the customized **splash.png** file in this directory: **/eEye Digital Security/Retina CS/ Website/images**.



Note: Size must be 1024 × 768px

2. Rename the original **splash.png** file or move it to another location.
3. In the **[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\rdp_proxy]** registry key, add a string value of **splash_png** with a value of the path to the customized splash image.

Specify Custom Replay Images

To customize **Admin > Replay** logos, modify the following files:

- **C:\Program Files (x86)\eEye Digital Security\Retina CS\website\images\rdp-placeholder.jpg**



Note: Size must be 147 × 125px

- **C:\Program Files (x86)\eEye Digital Security\Retina CS\website\images\rdp-placeholder-lg.jpg**



Note: Size must be 1024 × 768px

- **C:\Program Files (x86)\eEye Digital Security\Retina CS\website\images\ssh_placeholder.jpg**



Note: Size must be 137 × 125px

Specify a Custom Lock Image

To customize the lock image that appears to the end user when an administrator locks an active session:

1. Place the customized **lock.png** file in this directory: **/eEye Digital Security/Retina CS/ Website/images**.



Note: Size must be 1024 × 768px

2. Rename the original **lock.png** file or move it to another location.
3. In the **[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\rdp_proxy\lock]** registry key, add a string value of **png** with a value of the path to the customized lock image.



Note: By default, the lock image is centered on the screen. To specify alternative x- and y-coordinates, create DWORD registry values named **x** and **y** under the **lock** registry key.

Specify a Monitoring Image

To specify an image to display when an RDP session is being monitored in Password Safe:

1. Name the image file **monitor.png** and place it in the **/eEye Digital Security/Retina CS/Website/images** directory.
2. Create the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\BeyondTrust\PBPS\SessionManager\rdp_proxy\monitor
```

3. Under this key, create a string value named **png** and set it to the path of **monitor.png**.

By default, the monitoring image is centered on the screen. To specify alternative **x**- and **y**- coordinates, create DWORD registry values named **x** and **y** under the **monitor** registry key.



Note: The monitoring image is removed 15 seconds after the session stops being monitored.

Specify a Recording Image

To specify an image to display when an RDP session is being recorded in Password Safe:

1. Name the image file **record.png** and place it in the **/eEye Digital Security/Retina CS/Website/images** directory.
2. Create the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\BeyondTrust\PBPS\SessionManager\rdp_proxy\record
```

3. Under this key, create a string value named **png** and set it to the path of **record.png**.

By default, the recording image is centered on the screen. To specify alternative **x**- and **y**- coordinates, create DWORD registry values named **x** and **y** under the **record** registry key.

Configure Recorded Sessions in a Multi-Node Environment

In a multi-node environment, sessions can be viewed from any node in the environment, regardless of the node where it was created.

SSL certificates are used to ensure secure communication between the nodes. You must create a certificate using a certificate authority (CA) and import the certificate on each of the nodes.

When setting up the certificate, the Password Safe agent host name (or host name override) must match the **Issued to** details on the certificate properties in the **Certificates** snap-in.



Note: The CA certificates that issue the SSL certificates (the **Issued by** on the certificate properties) must be trusted by all nodes in the environment.

To confirm the host name matches the **Issued to** field:

1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management Agents > Session Agents**.
2. Select the agent from the list, and view the host name indicated in the **Host Name Override** box.
3. Open the Windows Certificates snap-in, and then double-click the certificate.
4. Confirm the name of the certificate in one of the following places:
 - On the **General** tab, confirm the host name is the same name as in the **Issued to** field.
 - On the **Details** tab, scroll to the **Subject** field and confirm the **CN=<name>** matches on the agent host name.

Configure Keystroke Logging

Password Safe records keystrokes for all recorded sessions. Keystroke logging is enabled by default. When you open a recorded session, the pane on the right displays keystrokes. You can select a keystroke entry to view where that keystroke occurred. You can also filter keystroke entries by date, time, or keystroke in the **Search** box.

Turn Off Keystroke Logging

You can turn off keystroke logging for ISA users and admin sessions as follows:

1. Navigate to **Configuration > Privileged Access Management > Global Settings**.
2. Under the **Session Monitoring** settings, clear the applicable keystroke logging options.
3. Click **Update Session Monitoring Settings**.

Keystroke logging can be enabled for all other users when setting the scheduling options for an access policy.



For more information, please see ["Configure Password Safe Access Policies" on page 73](#).

Enhanced Session Auditing

Enhanced session auditing captures and records all mouse activity in the **Keystrokes** menu of **Recorded Sessions** for RDP and RDP application sessions. Enhanced session auditing is enabled by default. It uses the rules in the access policy for Admin Session multi-session checkouts. During a recorded RDP session, an agent called **pbpsmon** is installed on the host for the duration of the session. The agent monitors and audits Windows click events.



Note: Session monitoring captures text that is copied in an RDP session window. The copied text is captured only the first time. Any subsequent copy tasks of the same text are not captured for the session.



Note: To use enhanced session auditing, the functional account of the managed Windows host or Remote Desktop Services host must have administrative rights.

Turn Off Enhanced Session Auditing ISA Users

1. Navigate to **Configuration > Privileged Access Management > Global Settings**.
2. Under the **Session Monitoring** settings, clear the applicable enhanced session auditing options.

3. Click **Update Session Monitoring Settings**.

You can turn off enhanced session auditing for admin sessions and all other non-ISA users, when setting the scheduling options for an access policy.

Troubleshoot Enhanced Session Auditing

The following files are deployed as part of enhanced session auditing:

- **pbpsdeploy** (Password Safe Deployment Agent service)
- **pbpsmon**
- **pbpslaunch**
- **pbpsmon** and **pbpslaunch** (These are contained in a cab file that is copied to the Windows directory and extracted to **C:\pbps**.)

pbpsdeploy

The **pbpsdeploy.exe** file resides in the Windows directory (**C:\Windows**).

- Access to **ADMIN\$** is required to copy **pbpsdeploy.exe** from Password Safe to the target server.
- Confirm the service is displayed in the **Services** snap-in after deployment.
- The output from the deployment service should be in the pbsm logs.



Example:

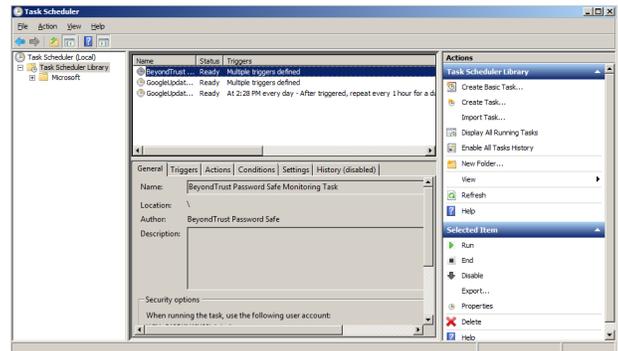
```
2017/03/07 15:47:12.186 2292 6548 INFO: Pushing pbpsdeploy service to 10.200.28.39 as
user backupadmin
2017/03/07 15:47:13.528 2292 6548 INFO: Starting pbpsdeploy service on 10.200.28.39 as
user backupadmin
2017/03/07 15:47:13.593 2292 6548 INFO: Copied pbpsmon.cab

2017/03/07 15:47:13.716 2292 6548 INFO: pbpsmon install:
Using binary directory C:\Windows\
Created directory C:\pbps
Extracting File "pbpsmon.exe" (Size: 15872 bytes) -> "C:\pbps\pbpsmon.exe"
Extracting File "pbpslaunch.exe" (Size: 145408 bytes) -> "C:\pbps\pbpslaunch.exe"
Extracting File "msvcp120.dll" (Size: 455328 bytes) -> "C:\pbps\msvcp120.dll"
Extracting File "msvcr120.dll" (Size: 970912 bytes) -> "C:\pbps\msvcr120.dll"
Extracting File "vccorlib120.dll" (Size: 247984 bytes) -> "C:\pbps\vccorlib120.dll"
Extracting File "libeay32.dll" (Size: 1359872 bytes) -> "C:\pbps\libeay32.dll"
Extracting File "ssleay32.dll" (Size: 252928 bytes) -> "C:\pbps\ssleay32.dll"
Creating registry keys
Registry keys successfully created
Creating task
Task successfully created
```

pbpsmon

Verify the following setup has been performed by the deployment service:

- In Task Scheduler, confirm the following task is created: **BeyondTrust Password Safe Monitoring Task**, or **BeyondTrust Password Safe Disposable Monitoring Task**. The task name depends on how enhanced session monitoring was installed.

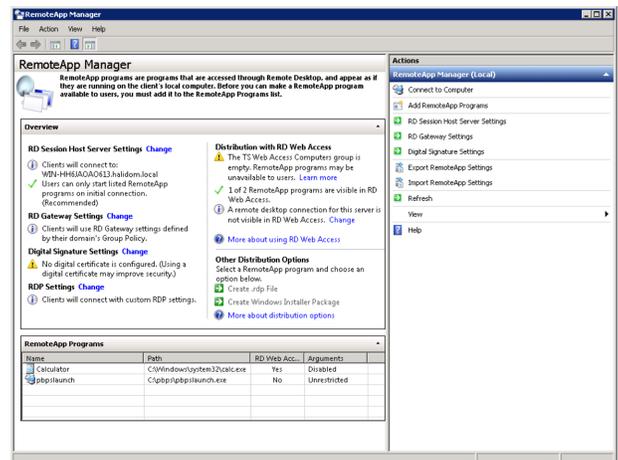


- In regedit, the following registry key is created, which creates the disconnect event:
HKLM\System\CurrentControlSet\Control\Terminal Server\Addins\PBPSMON

pbpslaunch

Verify the following setup has been performed by the deployment service:

- In regedit, the following registry key is created:
HKLM\Software\Microsoft\Windows NT\CurrentVersion\TerminalServer\TSAppAllowList\Applications\pbpslaunch
- A **pbpslaunch** entry exists in RemoteApp Manager.



- Locate the log statement *Accepting RDP Channel <name>*. There should be one for **pbpsmon**, and if it is an application session, one for **pbpslaunch**.



Example:

```
2017/03/07 15:47:14.659 3672 4788 INFO: Accepting RDP Channel PBPSMON
```

- The Event Viewer on the target server includes setup and cleanup results of **pbpsmon** and **pbpslaunch** sent to **pbsmd**.
 - Open **Event Viewer**.
 - Expand **Windows Logs**.

3. Click **Application**.
4. Filter the application log on **Source = pbpsdeploy**.



Note: You can prevent the session monitoring service from deploying **pbpsmon** and **pbpslaunch** on the managed system by setting the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\rdp_proxy\use_
pbpsdeploy = 0 (REG_DWORD)
```

Configure Algorithms used by the Session Monitoring Proxy

The encryption algorithms (ciphers), host key algorithms, key exchange (kex) algorithms, and MAC algorithms that may be used by Password Safe between the user's SSH client and the SSH proxy are configurable using the following registry keys:

- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\host_key_algorithms**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\kex_algorithms**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\macs**

The encryption algorithms (ciphers), host key algorithms, key exchange (kex) algorithms, and MAC algorithms that may be used by Password Safe between the SSH proxy and the managed system are configurable using the following registry keys:

- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\client_ciphers**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\client_host_key_algorithms**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\client_kex_algorithms**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\SessionManager\ssh_proxy\client_macs**

Each of these keys, if defined, must hold a multi-string value (REG_MULTI_SZ), with one algorithm name per line.

For example, ciphers might be:

- aes128-ctr
- aes192-ctr
- aes256-ctr

This restricts the available encryption algorithms to those named.

Use DSS Authentication

Applying DSS authentication on a managed system is a secure alternative to using password authentication. DSS authentication is set on the functional account and managed account properties.

DSS authentication is supported on the following systems: Linux, AIX, HP-iLO, HP-UX, DRAC, MAC OSX, Solaris, Juniper, and RACF.

 **Note:** Password Safe accepts SSH keys in the OpenSSH format. This includes support for newer key types typically used in that format, such as Ed25519.

Generate and Distribute the Key

You can generate keys using **puttygen.exe** on Windows systems and **ssh-keygen** on Unix-based systems. Consult the system documentation for other platforms.

 **Example:** How to generate a 2048-bit RSA key pair with **ssh-keygen**. The user account used to perform the scan is **admin**.

```
# ssh-keygen -t rsa -m PEM
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
/home/admin/.ssh/retina_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/admin/.ssh/retina_rsa.
Your public key has been saved in /home/admin/.ssh/retina_rsa.pub.
The key fingerprint is:
7f:5f:e3:44:2e:74:3c:c2:25:2b:82:7c:f8:0e:2a:da
```

/home/admin/.ssh/retina_rsa contains the RSA authentication identity of the user and should be securely transferred to the system running your scanner.

The file **/home/admin/.ssh/retina_rsa.pub** contains the RSA public key used for authentication. The contents of this file should be added to the file **~/.ssh/authorized_keys** on all machines that the user wishes to scan using public key authentication.

Create a Functional Account with DSS Authentication

Before you can create the account you must generate a private key. Copying or importing a key is part of setting the functional account properties with DSS authentication.

1. In BeyondInsight, go to **Configuration > Privileged Access Management > Functional Accounts**.
2. Click **Create New Functional Account**.
3. For the **Type**, select **Asset**.
4. Select a platform.
5. Select the elevation if desired.
6. Enter the username and password.
7. From the **Authentication Type** list, select **DSS**.

8. Upload the DSS key file.
9. Provide an alias and description, and then click **Save New Account**.

 For more information, please see "[Generate and Distribute the Key](#)" on page 155.

Create a Functional Account on the Unix or Linux Platform

Create an account on the Unix or Linux platform with a name like **functional_account**.

Ensure that the **su** command is available on the platform.

To assign necessary privileges to the functional account, invoke the command **sudo visudo** in the terminal and place the following lines under the root **ALL=(ALL) ALL** line:



Note: Be sure to add sudo elevation to the functional account on the managed system. These commands are adjusted to reflect password changes and DSS key changes and are OS-specific.

MAC OSX

```
functional_account ALL=(ALL) NOPASSWD: /usr/bin/grep, /usr/bin/sed, /usr/bin/tee, /usr/bin/passwd
```

UBUNTU/REDHAT

```
functional_account ALL=(ALL) NOPASSWD: /usr/bin/grep, /usr/bin/sed, /usr/bin/tee, /usr/bin/passwd
```

SOLARIS

```
functional_account ALL=(ALL) NOPASSWD: /usr/bin/grep, /usr/bin/cp, /usr/bin/tee, /usr/bin/sed,  
/usr/bin/passwd, /usr/bin/rm
```

HPUX

```
functional_account ALL=(ALL) NOPASSWD: /usr/bin/grep, /usr/bin/cp, /usr/bin/sed, /usr/bin/tee,  
/usr/bin/passwd, /usr/bin/rm
```

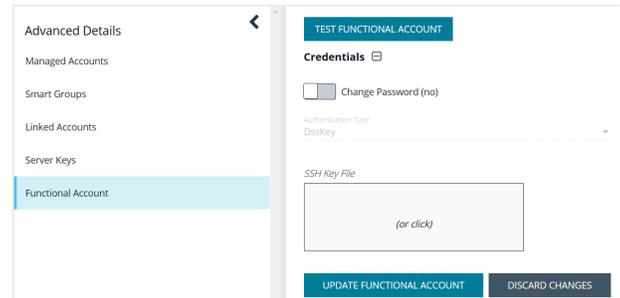
AIX

```
functional_account ALL=(ALL) NOPASSWD: /usr/bin/grep, /usr/bin/pwdadm, /usr/bin/tee,  
/usr/bin/passwd, /usr/bin/sed, /usr/bin/cp, /usr/bin/rm
```

Test the Functional Account

The key can be tested from the managed system.

1. From the menu, select **Managed Systems**.
2. Select the managed system, and then click the **More Options** button.
3. Select **Go to advanced details**.
4. Select **Functional Accounts**.
5. Click **Test Functional Account**.



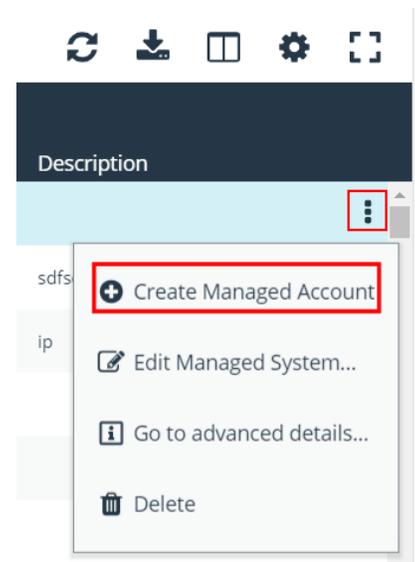
Set DSS on the Managed Account

An alternate and secure way to set up a managed account is with DSS authentication.

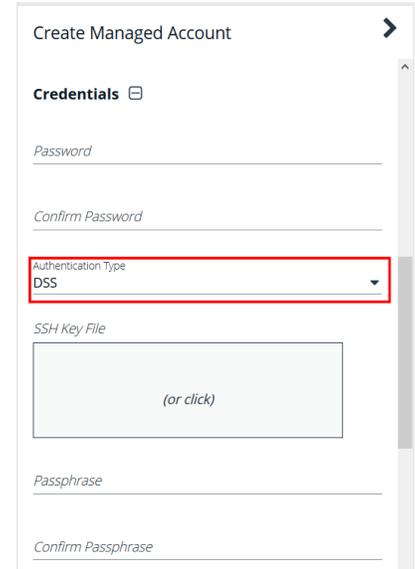
Before you can create the account, you must generate a private key. Copying or importing a key is part of setting the managed account properties with DSS authentication.

To create a managed account with DSS authentication:

1. From the menu, select **Managed Systems**.
2. Select the managed system, and then click the **More Options** button.
3. Select **Create Managed Account**.



4. From the **Authentication Type** list, select **DSS**.



The screenshot shows a 'Create Managed Account' form. Under the 'Credentials' section, there are fields for 'Password' and 'Confirm Password'. Below these is a dropdown menu for 'Authentication Type' which is highlighted with a red box and shows 'DSS' selected. Further down, there is an 'SSH Key File' section with a button that says '(or click)'. At the bottom, there are fields for 'Passphrase' and 'Confirm Passphrase'.

5. Configure all other settings as required, and then click **Create Account**.

i For more information, please see the following:

- ["Generate and Distribute the Key" on page 155](#)
- ["Work with Managed Accounts" on page 33](#)

DSS Key Auto Management

A DSS key policy is set on a managed system that supports DSS authentication.

The **Auto-Managed DSS key** option enables DSS key auto-management to take place when the password for the account is changed, either manually or scheduled. It follows the same schedule as password changing.

Generating a new DSS public/private key pair results in the removal of the old public key (if there is one) from the **authorized_keys** file and appends the new public key.

i For more information, please see ["Create a DSS Key Policy" on page 159](#).

Get the Public Key

1. Go to the **Managed Accounts** page.

2. Select the account and then click the **More Options** button.
3. Select **Public Key**.



Note: If a public key has been supplied, a popup displays the current public key.

Create a DSS Key Policy

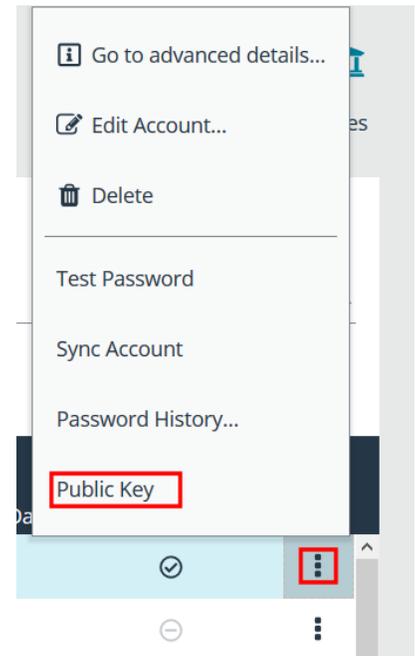
Password Safe ships with a default DSS key policy:

- Type: RSA
- Bit size: 2048
- Encryption: Auto Managed Passphrase is Default Password Policy

You can change the settings for the default policy but you cannot delete the policy.

Optionally, you can create additional policies.

1. Select **Configuration > Privileged Access Management > DSS Key Policies**.
2. Click **Create DSS Policy**.
3. Provide a name and description.
4. Select a Key Type: **RSA** or **DSA**.
5. Enable encryption.
6. Select a password policy.
7. Click **Create DSS Key Policy**.



Configure Password Safe Agents

Configure the Password Change Agent

Password Safe automatic password changes are controlled by the change agent that runs as a service on the U-Series Appliance. When the change agent runs, it checks the configuration to determine operational parameters of the U-Series Appliance. Logs provide a record of the change agent activities and messages, and indicate success or failure.

The following overview explains how the change agent runs:

1. The change agent retrieves a process batch from the database. A process batch consists of one or more managed accounts that have been flagged for a password change.
2. The passwords are changed on the managed accounts, and the change is recorded.
3. The change agent waits a set period of time for a response from the change job and moves to the next process batch in the database batch.

Recommendations

To maximize efficiency, we recommend a small batch size (such as 5) and a short cycle time (such as 60 seconds). If a password change fails, the change agent reprocesses it according to the retry value in the change agent settings.

1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management Agents > Password Change Agent**.
2. Set the following:
 - **Enable Password Change Agent:** Leave enabled to activate the agent when Password Safe starts.
 - **Active Change Tasks:** The number of accounts to change.
 - **Check the change queue every (seconds):** The frequency at which Password Safe cycles the password change queue.
 - **Retry failed changes after (minutes):** The amount of time before a failed password change is tried again.
 - **Maximum retries:** The maximum number of times an attempt is made to change the password after a failed password change attempt occurs.
 - **Unlimited Retries:** Enable to allow retries when a password change attempt fails.
3. Click **Save Configuration**.

PASSWORD CHANGE AGENT

Enable Password Change Agent

Active Change Tasks

−

+

Check the change queue every (seconds)

−

+

Retry failed changes after (minutes)

−

+

Maximum retries

−

+

Unlimited Retries

Configure the Mail Agent

Password Safe uses email to provide notification between approvers and requesters, error alerting, and general information delivery.

1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management Agents > Mail Agent**.

2. Set the following:

- **Enable Mail Agent (Running):** Enable to activate the mail agent when Password Safe starts.
- **Send mail every x minutes:** The number of minutes that pass before emails are sent.
- **Delete messages after x failed attempts:** The number of times the mail agent attempts to send an email.

3. Click **Save Configuration**.

MAIL AGENT

Mail agent notification test emails will be sent to admin@beyondtrust.com.

Enable Mail Agent (Running)

SEND TEST EMAIL



Send mail every minutes

Delete messages after failed attempts

SAVE CONFIGURATION

DISCARD CHANGES

Configure the Password Test Agent

The password test agent allows you to manually test all managed accounts and functional accounts. The test ensures that there is an open connection between the assets and Password Safe. BeyondInsight sends a notification email.

1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management Agents > Password Test Agent**.

2. Check the **Enable Password Test Agent** box.
3. Set the schedule, and then click **Save Configuration**.

PASSWORD TEST AGENT

Enable Password Test Agent

Active Test Tasks

- 26 +

Schedule Interval

Daily ▼

Start Time

2:13 A.M. 🕒

SAVE CONFIGURATION
DISCARD CHANGES

Configure Session Agents for Remote Proxy Sessions

In a distributed environment where there is more than one BeyondInsight instance installed, a Password Safe user can request a session to a remote instance. In this scenario, the user can request passwords and sessions for a remote instance by selecting a node on the **Requests** page in the Password Safe web portal.

BeyondInsight uses session agents to provide automatic heartbeat statuses to the primary BeyondInsight server. On startup the agent is set to **Active**, and on shutdown the agent is set to **Inactive**. The agent provides a status every five minutes. The Password Safe web portal displays only the active agents as nodes.

Configure a Display Name for a Session Agent

The display name is what appears as the name of the node in the Password Safe web portal. Configure the display name as follows:

1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management Agents > Session Agents**.
2. The **Session Agents** pane lists the active and inactive agents. Select an agent, and then enter the **Display Name** in the **Details** pane for that agent.
3. If the DNS name for the remote server is different from the primary BeyondInsight server, you can define a custom host name in the **Host Name Override** box. This ensures your connection to the host is valid and secure if using a custom certificate.
4. In the **Display Name** box, enter the node name that you want to display in the Password Safe web portal.
5. Click **Save Configuration**.


BeyondInsight

Configuration
Privileged Access Management > Session Agents

SESSION AGENTS

Search Session Agents

Showing all 2 Session Agents

- 🟢 Session Agent (Active)
- 🟢 Session Agent

Details

Host Name

ID

First Heartbeat Oct 01, 2019, 11:14 AM

Last Heartbeat Jul 24, 2020, 5:09 PM 🔄

State Active

Display Name

Host Name Override 🕒

SAVE CONFIGURATION
DISCARD CHANGES

Enable the Node Selector in Password Safe

If you want users to access specific BeyondInsight instances in the Password Safe web portal, then you must turn on the applicable **Sessions** setting in **Global Settings** configuration.

1. In the BeyondInsight console, go to **Configuration > Privileged Access Management > Global Settings**.
2. Under **Sessions** settings, click the toggle to enable the **Allow users to select a remote proxy when creating sessions** option.
3. Click **Update Sessions Settings**.

SESSIONS

Connect to systems using

DNS Name

IP Address

All

RDP session default port

Between 0 and 65535

Token timeout for remote session playback (seconds)

Between 10 and 60

Session initialization timeout (seconds)

Between 5 and 600 seconds

Default RDP screen resolution

1024x768

Enable smart sizing

Allow users to select a remote proxy when creating sessions

Make smart card device available in remote desktop sessions

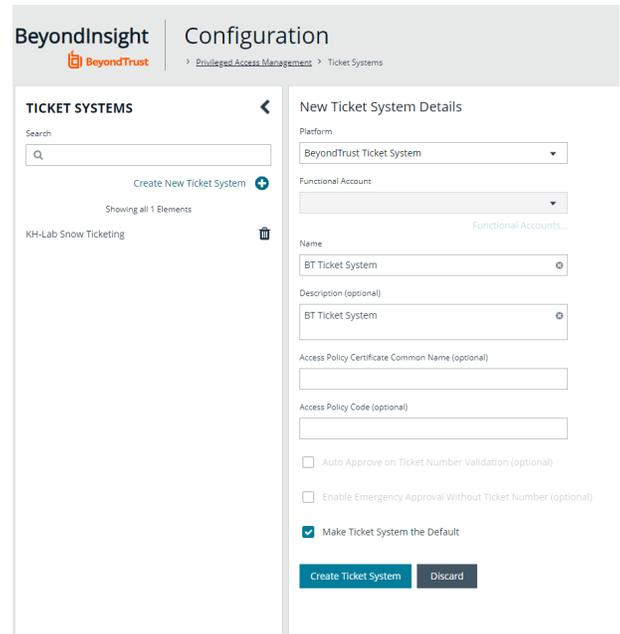
Hide record checkbox for ISA sessions

Add Ticket Systems to the List on the Requests Page

Password Safe can be configured to allow references to ticketing systems in the password release requests. This provides a method to include information that can be cross-referenced to an existing ticket or change control system for auditing purposes, or to be used in the approval process.

You can create a list of ticket system labels to populate the **Ticket System** list on a request.

1. In BeyondInsight, go to **Configuration > Privileged Access Management > Ticket Systems**.
2. From the **Ticket Systems** pane, click **Create New Ticket System**.
3. Select **BeyondTrust Ticket System** from the **Platform** list.
4. Enter a name and description.
5. Click **Create Ticket System**.



The screenshot shows the 'Configuration' page in BeyondInsight, specifically the 'Ticket Systems' section. On the left, there is a 'TICKET SYSTEMS' pane with a search bar and a 'Create New Ticket System' button. Below it, a list shows 'KH-Lab Snow Ticketing'. The main area is titled 'New Ticket System Details' and contains the following fields and options:

- Platform:** A dropdown menu with 'BeyondTrust Ticket System' selected.
- Functional Account:** A dropdown menu with 'Functional Accounts...' as a placeholder.
- Name:** A text input field containing 'BT Ticket System'.
- Description (optional):** A text input field containing 'BT Ticket System'.
- Access Policy Certificate Common Name (optional):** An empty text input field.
- Access Policy Code (optional):** An empty text input field.
- Auto Approve on Ticket Number Validation (optional)
- Enable Emergency Approval Without Ticket Number (optional)
- Make Ticket System the Default

At the bottom of the form are two buttons: 'Create Ticket System' (in blue) and 'Discard' (in grey).

i For information on integrating third party ticket systems, such as BMC Remedy, CA Service Desk, Jira, and ServiceNow with BeyondInsight and Password Safe, please see the following:

- [BeyondTrust BeyondInsight Guides](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm>
- [BeyondTrust Password Safe Guides](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/index.htm>

Customize Email Notifications

Email notifications are used to alert users on particular Password Safe actions, such as connection profile alerts, release requests, and password check failures.

Email Notifications Sent by Password Safe

The below table lists the email notifications that are sent to Password Safe users. It includes the event type that occurs to initiate the email notification and the account types that receive the email.

Local Accounts (Includes Non-Domain Asset and Database Managed Systems)

Event	Account	Not configurable	Configurable by template settings
Release Request	Managed	NA	<ul style="list-style-type: none"> Account's Approver Requester (CC) Asset's ISA
Request Response	Managed	NA	<ul style="list-style-type: none"> Account's Approver (CC) Requester Asset's ISA
Password Change Failure	Managed	<ul style="list-style-type: none"> Managed System's ISA Built-in Administrators group members Managed System contact person (Managed Systems settings UI) 	NA
	Functional	<ul style="list-style-type: none"> Managed System's ISA Built-in Administrators group members Managed System contact person (Managed Systems settings UI) 	NA
Password Check Failure	Managed	<ul style="list-style-type: none"> Managed System's ISA Built-in Administrators group members Managed System contact person (Managed Systems settings UI) 	NA
	Functional	<ul style="list-style-type: none"> Managed System's ISA Built-in Administrators group members Managed System contact person (Managed Systems settings UI) 	NA
Propagation Event Failure	Managed	<ul style="list-style-type: none"> Managed System contact person (Managed Systems settings UI) 	NA

Privileged Password Release	Managed	<ul style="list-style-type: none"> Managed Account Release Notification Recipients (Managed Accounts settings UI) 	NA
Non-Managed Release Expiration	Managed	<ul style="list-style-type: none"> Managed Account Release Notification Recipients (Managed Accounts settings UI) 	NA

Domain Accounts

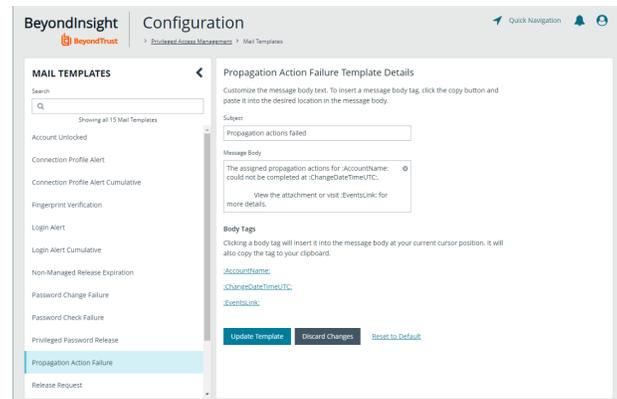
Event	Account	Not configurable	Configurable by template settings
Release Request	Managed	NA	<ul style="list-style-type: none"> Account's Approver Requester (CC) Domain Management permission (with Read/Write)
Request Response	Managed	NA	<ul style="list-style-type: none"> Account's Approver (CC) Requester Domain Management permission (with Read/Write)
Password Change Failure	Managed	<ul style="list-style-type: none"> Domain Management permission (with Read/Write) Built-in Administrators group members Managed System contact person (Managed Systems settings UI) 	NA
	Functional	<ul style="list-style-type: none"> Domain Management permission (with Read/Write) Built-in Administrators group members Managed System contact person (Managed Systems settings UI) 	NA
Password Check Failure	Managed	<ul style="list-style-type: none"> Domain Management permission (with Read/Write) Built-in Administrators group members Managed System contact person (Managed Systems settings UI) 	NA
	Functional	<ul style="list-style-type: none"> Domain Management permission (with Read/Write) Built-in Administrators group members Managed System contact person (Managed Systems settings UI) 	NA
Propagation Event Failure	Managed	<ul style="list-style-type: none"> Managed System contact person (Managed Systems settings UI) 	NA

Privileged Password Release	Managed	<ul style="list-style-type: none"> Managed Account Release Notification Recipients (Managed Accounts settings UI) 	NA
Non-Managed Release Expiration	Managed	<ul style="list-style-type: none"> Managed Account Release Notification Recipients (Managed Accounts settings UI) 	NA

Customize Mail Templates

The subject line and message body for a template can be customized in Password Safe configuration.

- In the BeyondInsight console, go to **Configuration > Privileged Access Management > Mail Templates**.
- Select a mail template type from the list.
- Type the subject line text.
- In the **Message Body** field, add the text for the email:
 - Copy a tag from the **Body Tags** section to a location in the message body.
 - When working within cumulative alert emails, ensure you add any additional body tags within the **<ROW></ROW>** elements.
 - To include hyperlinks that link directly to the approval and denial pages for a file or password request, use the **:approvalink:** and **:denylink:** message body tags.
- Click **Save Template**.



 **Note:** Only one **<ROW></ROW>** tag can be added to the mail template. If you wish to add more tags, they must be added to the row already present within the template. For example:

```
<ROW>:AlertTimeUTC: | :AlertTimeClient: | :ComputerName: | :AccountName: |
:AccountDomain: | :DNSName: | :IPAddress: | :EventCode: | :EventReferenceId: |
:SubjectSID:</ROW>
```

Configure Workgroups for Multi-Node and Multi-Tenant Environments

Password Safe allows you to assign worker nodes to workgroups to give the user more granularity on password changes. Password Safe uses workgroup assignments at the managed account level to allow Password Safe worker nodes to process password changes, password tests, and account notifications for their designated workgroup.

If a worker node is not assigned to a workgroup, the worker node functions on a global level and can change any account that does not have a designated workgroup assigned.

Create a Password Safe Worker Node

This is an automated self registered process, so it is not possible to add worker nodes manually. When any node in an active active configuration is running Password Safe, v6.0 or higher, the worker node registers with the BeyondInsight database.

You can view registered Password Safe worker nodes from **Configuration > Privileged Access Management > Worker Nodes**.

Assign a Password Safe Worker Node to a Workgroup

1. Select **Configuration > Privileged Access Management Agents > Worker Nodes**.
2. Select a worker node from the list on the left. The following options display:
 - **Organizations:** Use the dropdown list to select the organization.
 - **Unassigned:** The node is not assigned.
 - **Assign to existing workgroup:** If selected, use the dropdown list to select the workgroup you want.
3. Click **Save Worker Node** when done.

Assign a Workgroup to a Managed Account

You can assign a workgroup to a particular managed account by editing the managed account or by using a Smart Rule.

To assign a workgroup to particular managed account, go the **Managed Accounts** page and select the account to edit. On the **Edit Managed Account** page, select a workgroup from the dropdown list.



Note: If you set the workgroup value to **None**, the account can be changed by any Password Safe agent.

To assign a workgroup using a Smart Rule, go the **Smart Rules** page, and create or a edit an existing rule. Under **Actions**, select **Assign workgroup on each account**.

Create New Managed Account Based Smart Rule

Name
 Active

Description

Reprocessing limit

Selection Criteria

Include items that match of the following

-
-
-
-
- and
-

[Add another condition](#) [Add a new group](#)

Actions

-
-

[Add another action](#)

Assign Agents to Workgroups for Multi-Tenant Environments

After your BeyondInsight environment is configured with multiple organizations, the Password Safe worker nodes must be assigned to a workgroup. Multiple worker nodes can be assigned to one workgroup. This distributes the workload and allows Password Safe to scale if needed for the organization.

In a multi-tenant environment, each organization requires at least one worker node. You can only assign a worker node to one organization. Assigning a worker node to more than one organization is not a supported implementation.



Note: Any managed accounts that are in a workgroup that is not assigned to a worker node will not be processed.



Note: Every time a worker node is reassigned to a workgroup, the Password Safe omnIService must be restarted.

After the worker nodes are assigned, managed accounts can be reassigned to a different workgroup, if required. Managed accounts can be assigned to workgroups manually by editing the Managed Account or by creating a Smart Rule to bulk assign accounts to a new workgroup.



For more information, please see the following:

- i**
- For more information on assigning managed accounts to workgroups, "[Assign a Workgroup to a Managed Account](#)" on [page 168](#)
 - For more information on how to configure a multi-tenant environment, the [The BeyondInsight User Guide](#) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/multi-tenant.htm>

Synced Accounts in a Multi-Tenant Environment

When viewing synced accounts on a managed account in a multi-tenant environment, only synced accounts in that organization are displayed.

Configure and 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.

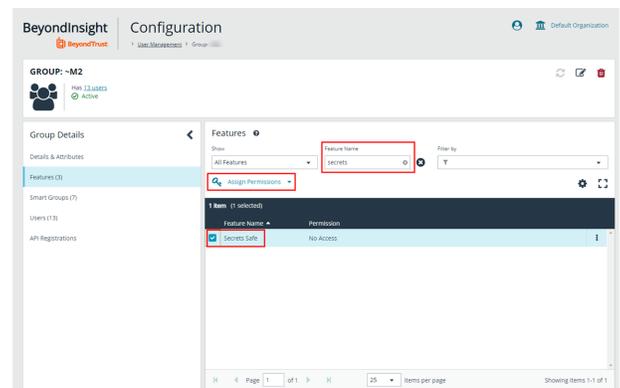
Assign the Secrets Safe Feature to a Group

Access to **Secrets Safe** is granted to users by assigning permissions for the **Secrets Safe** feature to a group in which the users are members.

1. In **BeyondInsight**, go to **Configuration > Role Based Access > User Management**.
2. Click the vertical ellipsis for the group you want to assign the **Secrets Safe** feature to, and then select **View Group Details**.
3. From the **Group Details** pane, select **Features**.
4. From the **Features** pane, select the **Secrets Safe** feature.



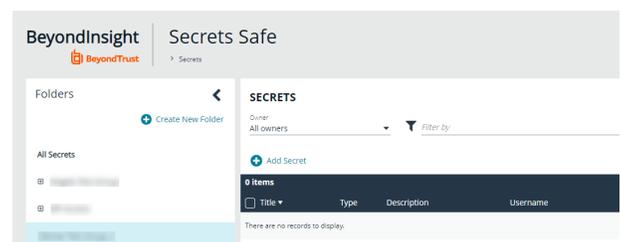
Tip: You can filter the list of features by **All Features** or **Disabled Features**, and **Feature Name** to quickly locate the **Secrets Safe** feature.



5. Click **Assign Permissions**, and then select **Assign Permissions Read Only**.
6. Users who are members of the group are granted access to the **Secrets Safe** page, where the group is listed as a parent level folder representing the team.



Note: The **Secrets Safe** feature cannot be removed from a group if secrets are still contained within the team.

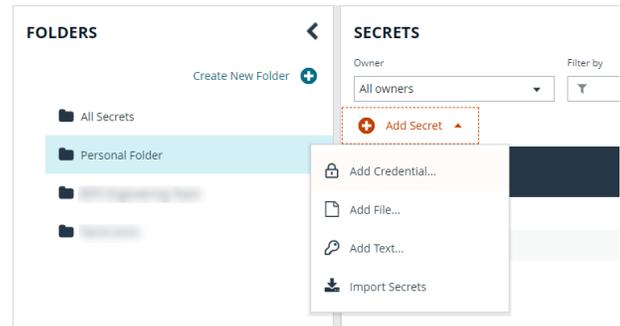


Create a Secret in Secrets Safe

Users can create secrets in the parent folder for any of their teams or in any of their team's subfolders. The user who creates the secret is its owner by default but may change ownership at time of creating the secret or after the secret has been created. Owners may change the folder for secrets after they have been created.

1. From the left menu, click **Secrets Safe**.

- From the **Folders** pane, select a folder, and then click **Add Secret** above the grid.
- 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

- Enter a **Title**, **Description**, and **Username**.
- 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**.
- 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**.
- Click **Manage Ownership** if you wish to assign ownership to individual team members or to the entire team.
- 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

Description

URL

Username

Set Password ?

Manual Input
 Auto Generate

Password
 Show

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**.



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

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

Description

Upload File



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

All file types accepted.
Maximum File Size: 5 MB

Notes

Ownership
[Manage Ownership](#)

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

Description

Text Body

Notes

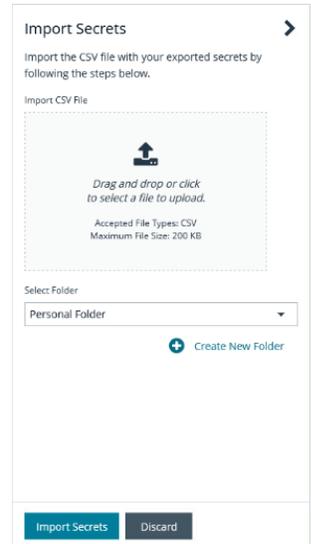
Ownership
[Manage Ownership](#)

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

Create New Folder

Import Secrets Discard



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>*

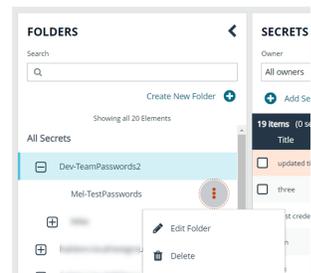
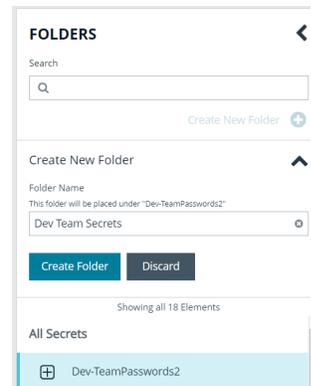
- **Example: CSV File - url,username,password,totp,extra,name,grouping,fav**

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

Users can organize their team secrets into subfolders under the parent team 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 secret to a new subfolder, please see ["Edit and Delete a Secret in Secrets Safe" on page 176](#).

View and Copy a Secret in Secrets Safe

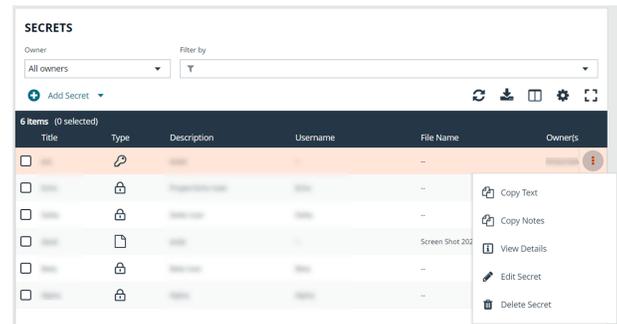
Users can view details for their team's secrets, such as who owns the secret, when the secret was created and modified, and the folder path for the secret. Users can also copy the username and password for a team secret so they may use it.

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.

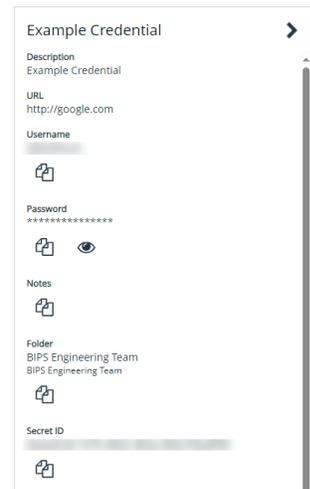
4. Each secret type, as indicated by its **Type** icon, has specific actions available from the options menu, as follows:

- 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.



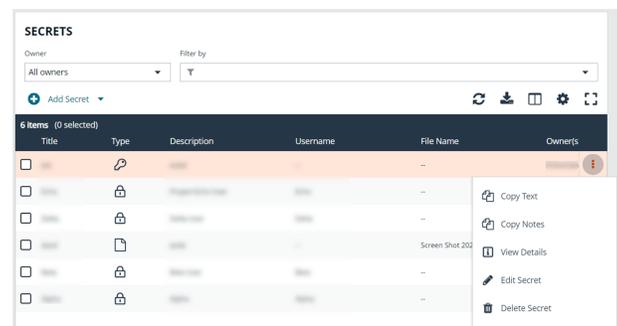
- While viewing the details for a credential secret type, you can:
 - Click the applicable copy icons to copy the username, password, notes, folder path, and secret ID.
 - Click the eye icon to show the password.
- While viewing the details for a file secret type, you can:
 - Click the download icon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



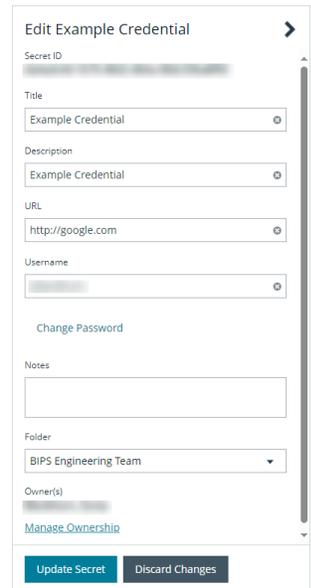
Edit and Delete a Secret in Secrets Safe

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.

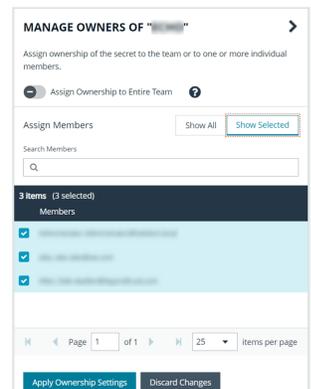
1. From the left menu, click **Secrets Safe**.
2. From the **Folders** pane, select a folder, and then select a secret.
3. Click the vertical ellipsis for the secret.
4. To delete a secret, select **Delete Secret**, and then click **Delete** on the confirmation message.
5. To edit a secret, select **Edit Secret**.



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



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



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

Password Safe PS_Automate Utility User Guide

Overview

The Password Safe **PS_Automate** utility helps to avoid the need to manually enter credentials when launching Windows GUI applications from Password Safe, saving time and increasing security.

The **PS_Automate** utility allows you to seamlessly pass vaulted credentials from Password Safe to a remote application using the pass through option (using token pass instead of credentials). This includes the ability to launch and authenticate to a web page or to a standard Windows GUI application.

To ensure a seamless experience, the utility supports Incognito mode for popular web browsers, such as Chrome, Firefox, and Microsoft Edge, with Edge being the default. By using an INI file, you can easily specify the input and operational behavior for the utility.

The **PS_Automate** utility, as well as INI files for Amazon Web Services, Azure, Office 365, and Google, are made available when enhanced session auditing is enabled in Password Safe. The files are deployed by the session proxy when a session is created in Password Safe.

The system where the **PS_Automate** utility is deployed must have internet access, in order to automatically download the latest version of the required browser drivers on first use:

- chromedriver.exe
- msedgedriver.exe
- geckodriver.exe

The utility uses the browser drivers, and the versions of the drivers must match the versions of the browsers used.



Note: *PS_Automate* is a utility for Windows only. It is not supported on macOS.

Usage

The usage syntax for the **PS_Automate** utility is as follows:

Web Applications

```
ps_automate.exe [ini=path to inifile][TargetURL=url] [BrowserName=name of browser]
```

Windows Applications

```
ps_automate.exe [ini=path to inifile]
```



Note: For testing purposes the utility also accepts username and password on the command line: **[username=username] [password=password]**. However, this is not recommended for production use, as command line parameters can be written to Windows logs, such as the event log.

**Example:**

```
ps_automate.exe ini="BIWebApp.ini"  
TargetURL="https://localhost/WebConsole/index.html#!/dashboard" BrowserName="chrome"
```

```
ps_automate.exe ini= "C:\automate\AWSWebApp.ini"  
TargetURL="https://534949981440.signin.aws.amazon.com/console/" BrowserName="firefox"
```

```
ps_automate.exe ini="MSWebApp.ini"  
TargetURL="https://login.microsoftonline.com" BrowserName="msedge"
```

```
ps_automate.exe ini="ssms_database.ini"
```

Define Command Line Arguments in INI File

INI files are commonly used configuration files for storing settings and preferences for applications. The **PS_Automate** utility uses INI files to specify its own settings and parameters. It is generally provided as a command line parameter, for example, **ini=login.ini**. If no file is specified, the utility looks for an INI file in the same source directory with the same name as the utility, i.e. **ps_automate.ini**.

When command line arguments are provided, they can technically be listed in any order as each is prefixed with the argument name, i.e. **argument=value**.

The following common predefined INI files are included with the deployment of the **PS_Automate** utility.

- **AWSWebApp.ini** for Amazon Web Services logins
- **BIWebApp.ini** for BeyondInsight logins
- **GoogleWebApp.ini** for Google URL logins
- **MSWebApp.ini** for Microsoft URL Logins
- **ssms_database.ini** for SQL Server Management Studio v18 logins

The INI file is in standard INI format consisting of one or more sections with each section containing one or more key/value pairs. Each of the sections and their key/value pairs are described below.

General Section

The **[General]** section defines the main settings for the application. Each setting and its accepted values are listed below.

Setting	Definition
BrowserName	Value: String (default is msedge) Required: No Description: Specifies the browser to launch for web app login (Edge, Chrome, Firefox). The browser can be specified in the INI file or overwritten by command line parameters.
TargetURL	Value: String Required: Yes Description: Specifies the web app URL. The URL can be specified in the INI file or overwritten by command line parameters.
EnableLogging	Value: Integer <ul style="list-style-type: none"> • 0 No logging (default) • 1 Error level • 2 Warning level • 3 Info level • 4 Debug level (Used for troubleshooting issues. A new console window is launched.) Required: No Description: Specifies if logging should be enabled.
LogMethod	Value: Integer <ul style="list-style-type: none"> • 1 Log to file (default) • 2 Log to debug window • 3 Log to both Required: No Description: Specifies what log method to use.

LogPath	<p>Value: Valid file path Required: No Description: Specifies the path to create log files. Defaults to script path.</p>
FixupPassword	<p>Value: Boolean (1* 0) Required: No Description: Specifies a different method of parsing out the password parameter. This allows a wider array of complex passwords to be used, such as space and quotes. Defaults to true.</p>
RunApp	<p>Value: Any valid Windows executable. May include custom command line values. Required: Only when TargetURL is not used. Description: This is the initial application launched by the utility. The RunApp may also contain values based from the command line.</p>
FileChangeDir	<p>Value: Any valid Windows directory. May NOT include custom command line values. Required: No Description: This is the initial working directory for the app in RunApp. Some apps require a custom WorkingDir value.</p>
AppWindowTitle	<p>Value: Any valid Windows title name. Required: No Description: This is the window the utility initially connects to for targeting commands. We recommend providing this value; otherwise, the currently active window is targeted, which may lead to undesirable results.</p>
WindowTitleMatchMode	<p>Value: Integer (-1*, -2, -3, -4, 1, 2, 3) Required: No Description: This is the method used to match the AppWindowTitle with the actual window text. The default is a case-insensitive search from the start of the window text.</p> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p> For more information, please see Windows Titles and Text at https://www.autoitscript.com/autoit3/docs/intro/windowsadvanced.htm.</p> </div>
IgnoreCerts	<p>Value: Integer (1* 0) Required: No Description: Enabling this option causes the Certificate warning screen to be automatically bypassed (accepted). This option only works on localhost for Chrome and Edge. Firefox does not have a localhost limitation.</p> <div style="border: 1px solid blue; padding: 5px; margin-top: 10px; background-color: #e6f2ff;"> <p> Note: This setting is for testing purposes only as bypassing certificates is NOT secure.</p> </div>
GlobalSequenceDelay	<p>Value: Integer in milliseconds (default is 250) Required: No Description: How much time to wait in between each TaskSequence.</p>
KioskMode	<p>Value: Integer (0 1) (default is 0) Required: No Description: Set to 1 to enable Kiosk mode in the browser. Application runs in full screen without any browser user interface such as toolbars and menus.</p>

Credentials Section

The **[Credentials]** section is an optional section used for hard coding the **username** and **password** values into the INI file. When this section is provided, both keys are required and override any command line values provided.



Note: This section is used for testing. We recommend you secure any INI files containing credentials.

Setting	Definition
UserName	Value: Valid username Required: Yes Description: The username to provide to the security dialog. Specified as %username% to the provided task.
Password	Value: Valid password. Required: Yes Description: The password to provide to the security dialog. Specified as %password% to the provided task.

TaskSequences Section

The **[TaskSequenceX]** sections of the INI file define the tasks to take once the **RunApp** or **TargetURL** has been accessed.

Place each **[TaskSequenceX]** in its own section in the INI file in sequential order and ideally order them numerically as per the following example:

```
[TaskSequence1]
task=value
...
[TaskSequence2]
task=value
...
[TaskSequence3]
...
```

Each **[TaskSequenceX]** can perform one or more tasks. Generally, a specific task sequence consists of providing information to target the appropriate dialog box/control and then send text or a command to it, for example **click**. Most pages generally require a minimum of two task sequences, one to populate the username and one to populate the password. Since tasks can be combined within the **[TaskSequenceX]**, the submission (posting) of these values can be tasks of the same **[TaskSequenceX]**.

Sometimes additional task sequences must be performed before or after supplying credentials. However, it is possible to automate many actions with a single task sequence through the use of **SendKeys** for Windows applications only.

App and WebApp task sequences and their values are listed below. All tasks within a task sequence are optional, though some depend on others or are mutually exclusive.

Each task can be defined only once within each **[TaskSequenceX]**.

App Task Sequences

App task sequences begin after being initiated by a **RunApp**.

The standard function of a sequence is to enter a string of data (**SendKeys**) into a particular control (**AppWindowControlID**) on a window. If a control is provided to the sequence, the utility attempts to attach to the control, focus it, and send it directly to the control. This is a very accurate way of targeting commands. If no control is provided (or one can't be found), the commands can still be issued to the active window/control.

In addition to the tasks from the generic task sequences, the following tasks are applicable for the **RunApp** (App) task sequences.

Setting	Definition
SequenceDelay	<p>Value: Integer in milliseconds (default is 0)</p> <p>Description: How much time to wait at the beginning of each task sequence. This is in addition to any value provided in GlobalSequenceDelay.</p>
SendKeys	<p>Value: Any valid string of characters</p> <p>Description: A sequence of characters to send to the focused control/field. The utility supports the special characters defined by AutoIt({TAB}, {ENTER}, etc.) when using the default mode of SendKeysRaw.</p> <div style="border: 1px solid orange; padding: 10px; margin-top: 10px;"> <p>i For more information on the special keys, please see the following:</p> <ul style="list-style-type: none"> • Send Command at https://www.autoitscript.com/autoit3/docs/functions/Send.htm • Send Keys Command at https://www.autoitscript.com/autoit3/docs/appendix/SendKeys.htm </div>
SendKeysDelay	<p>Value: Integer in milliseconds (default is 5)</p> <p>Description: This is the amount of time the utility waits in between each key stroke sent by SendKeys. It may be necessary to increase this delay if the interface cannot respond quickly enough to the send keys.</p>
SendKeysRaw	<p>Value: Boolean (1* 0)</p> <p>Description: Changes the interpretation of the SendKey sequence to be raw (literal). It will not interpret any of the special characters as defined by the AutoIt Send command. Due to the complexity of the characters often involved, we recommend setting this when using SendKeys to send passwords .</p>
AppWindowTitle	<p>Value: Any valid Windows title name.</p> <p>Required: No</p> <p>Description: This is almost identical to the AppWindowTitle specified in the generic task sequences. However, this is used to target to a new window that may be open during the authentication attempt. This value only needs to be provided if a new window requires focus. For instance, clicking on a login button may present a security warning or legal disclaimer in a new window which requires targeting. While it is not always required to target the new window directly, it can improve accuracy.</p>
WindowTitleMatchMode	<p>Value: Integer (-1*, -2, -3, -4, 1, 2, 3)</p> <p>Required: No</p> <p>Description: This is identical to the WindowTitleMatchMode specified in the generic task sequences; however, it targets the AppWindowTitle App task sequence.</p>
AppWindowControlID	<p>Value: Any valid window control ID name.</p> <p>Description: When provided, the utility targets the control directly. Valid control names are found with the AutoIt Windows Info utility and can be provided in a variety of formats.</p> <div style="border: 1px solid orange; padding: 10px; margin-top: 10px;"> <p>i For more information, please see ControlCommand at https://www.autoitscript.com/autoit3/docs/functions/ControlCommand.htm.</p> </div>
AppWindowControlClick	<p>Value: Boolean (1* 0)</p> <p>Description: Sends a standard left click event to the control defined in AppWindowControlID. Often, SendKeys can be used to simply send an {ENTER} command to a focused control, but in some circumstances, it may be necessary to send a click directly.</p>

WebApp Task Sequences

The web application depends on a **TargetURL** from the **General** section. Task sequences use **Xpath** to find and click the web page element.

The standard function of a web application task sequence is to enter an **Xpath** string for the element you want to interact with, as well as a value for the element.

The webapp tasks rely on browser drivers to accomplish their tasks. The utility automatically downloads the browser driver to the same location as the utility. The browser version (major.minor.build) must match the driver version or the utility may fail to launch the browser. For example, **chromeDriver 100.0.4896** will work with Chrome browser **100.0.4896.x**.

Ensure the functional account used for the RDS Session has network permissions that allow the **PS_Automate** to access the internet. For example, add the functional account to GPO, thereby allowing the functional account to use the proxy.

In addition to the tasks from the **General** section, the following tasks are applicable for the **WebApp TaskSequences** section.

Setting	Definition
XPathElement	Value: Xpath string for the element Description: Goes to the element specified.
XPathValue	Value: Xpath string for the element value. Description: Enters the text specified into the element.
XPathAction	Value: String value click , clear . Description: Clicks on the element specified by XPathElement .

Certificates

For keeping sensitive web traffic information secure, certificates are used. The **PS_Automate** utility has the ability to **IgnoreCerts**, which are provided for internal self hosted websites and for testing only.

Chrome and Edge browsers can ignore certificates for **localhost** only. The Firefox browser does not have this limitation.

Web App Known Issues

1. When multiple RDP sessions are launched for the same machine at the same time, the end user may experience a delay with the automated logon for one of the sessions. One session blocks while the other loads. Once the session successfully loads (maximum wait time 30 seconds), the other session is able to successfully load its browser and begin the automated login.
2. Manually clicking, opening new browser windows, or creating tabs on the launching of the automated browser can cause the automated login to fail.
3. Issues automatically updating the Firefox driver (geckodriver) to the latest version. If PS_Automate fails to launch the Firefox browser, one possible cause is that the driver version is out of date. PS_Automate attempts to update the driver; however, there is a known issue where geckodriver updates may fail. In that case download the geckodriver, from <https://github.com/mozilla/geckodriver/> and place it in the same directory as **ps_automate.exe**.