Password Safe 22.3

Admin Guide

TC:12/1/2022

Table of Contents

Password Safe Administration Guide 7
Log In to the BeyondInsight Console 8
Log Out of the Console 9
Select a Display Language 9
Navigate the Console 10
Add Assets to Password Safe 11
Workflow to Add Managed Systems and Accounts to Password Safe 11
Create a Functional Account 12
Override a Functional Account Password 12
Add a Managed System Manually 13
Add Managed Systems and Accounts Using Smart Rules 16
Add Active Directory Managed Accounts Using a Smart Rule 17
Add Known Local Admin Managed Accounts Using a Smart Rule 18
Configure Functional Account Requirements in Azure 21
Create Enterprise Application 21
Configure App Registration 22
BeyondTrust Password Safe Configuration 24
Work with Managed Systems 25
View Managed Systems Details 25
Import an SSH Server Key Using a Smart Rule 26
Manage the SSH Server Keys 26
Work with Managed Accounts 28
View Managed Accounts 28
View Managed Account Details 28
Delete Managed Accounts 29
Unlink Managed Accounts 29
Change Passwords for Managed Accounts 30
Configure Subscriber Accounts 30
Configure Password Reset for Managed Account Users 31
Use a Managed Account as a Discovery Scan Credential 32
Managed Account Aliasing 33

Work with Smart Rules 35
Predefined Smart Groups 35
Considerations When Designing Smart Rules 36
Smart Rule Processing 37
View and Select Smart Rules Processing Statistics 38
Use Dedicated Account Smart Rule 38
Use an Azure AD Smart Rule 42
Use Quick Groups 43
Configure Role Based Access 46
Group Features 46
Password Safe Roles 47
Create a Group and Assign Roles 49
Quarantine User Accounts 51
Configure API Access 52
Restrict Access to Password Safe Login Page 54
Configure Approvals 55
Use a Managed Account as a Credential 56
Configure LDAP Groups 57
Real Time Authorization 58
Configure Password Safe Access Policies 59
Create an Access Policy 59
Create a Connection Profile 63
Use a Predefined Connection Profile 65
Create Password Policies 66
Manage Recorded Sessions 68
View Recorded Sessions 68
Use Keystroke Search 68
Export a Session Frame 69
Archive Recorded Sessions 69
View and Restore Archived Sessions 69
Manage Active Sessions 71
View Active Sessions 71
Lock an Active Session 71

Terminate an Active Session 72
Terminate and Cancel an Active Session 72
View Keystrokes in Active Sessions 72
Add Windows Components to Password Safe 73
Add a Directory 73
Add Directory Accounts 73
Add Propagation Actions to Managed Accounts 75
Configure Password Safe Global Settings 83
Sessions 83
Requests 83
Session Monitoring 84
Purging 84
Miscellaneous 85
Add Databases to Password Safe 86
Auto Discover and Manage Database Instances 86
Manually Add Database Instances 87
Manage Database Instance Accounts 89
Create a Functional Account for a SQL Server Database 91
SQL Server Instance Port Retrieval 92
Add a PostgreSQL Database Instance 93
Configure Settings on the Oracle Platform 95
Add Applications to Password Safe 100
Add an Application 100
Use Encryption Module for RemoteApp 101
Associate the Application with a Managed Account 102
Set Up the Access Policy 102
Set Up Role-Based Access 102
Use the PS_Automate Utility 103
Use AutoIt Passthrough 104
Add SAP as a Managed System 105
Configure API Registration 107
Add a Custom Platform or Application Platform 109
Create a New Platform 109

Configure the Options Tab 110
Configure the Steps Tab 112
Configure the Check/Change Password Tab 113
Create a New Application Platform 115
Export or Import a Custom Platform 119
Configure SSH and RDP Connections 121
Requirements for SSH 121
Supported SSH Client Algorithms 121
Auto-Launch PuTTY Registry File 123
Supported SSH Session Protocols 124
Multiple SSH Sessions 124
Enable Login Accounts for SSH Sessions 124
Use Direct Connect for SSH and RDP Session Requests 125
Configure RDP Sessions 127
Configure Session Monitoring 130
Configure Listen Host and File Location 130
Configure Concurrent Sessions 130
Use Session Masking 131
Customize Session Images 131
Configure Recorded Sessions in a Multi-Node Environment 133
Configure Keystroke Logging 134
Enhanced Session Auditing 134
Configure Algorithms used by the Session Monitoring Proxy 137
Use DSS Authentication 138
Generate and Distribute the Key 138
Create a Functional Account with DSS Authentication 138
Create a Functional Account on the Unix or Linux Platform 139
Set DSS on the Managed Account 140
DSS Key Auto Management 141
Configure Password Safe Agents 143
Configure the Password Change Agent 143
Configure the Mail Agent 144
Configure the Password Test Agent 144

Configure Session Agents for Remote Proxy Sessions 145

Add Ticket Systems to the List on the Requests Page 147

Customize Email Notifications 148

Email Notifications Sent by Password Safe 148

Customize Mail Templates 150

Configure Workgroups for Multi-Node and Multi-Tenant Environments 151

Create a Password Safe Worker Node 151

Assign a Password Safe Worker Node to a Workgroup 151

Assign a Workgroup to a Managed Account 151

Assign Agents to Workgroups for Multi-Tenant Environments 153

Configure and Use Team Passwords 155

Assign a Group to a Team in Team Passwords 155

Create a Credential in Team Passwords 155

Manage Folders in Team Passwords 157

View and Copy a Credential in Team Passwords 158

Edit and Delete a Credential in Team Passwords 159

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 username used to sign into the BeyondInsight console for the first time is 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.
- **Azure Active Directory:** Add Azure Active Directory users in BeyondInsight and add them to groups to assign permissions to features. Azure Active Directory users can log in to the console from the BeyondInsight login page.
- **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 navigate to the SAML site access URL provided by your administrator to use SAML authentication.
- **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 Active Directory 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.*

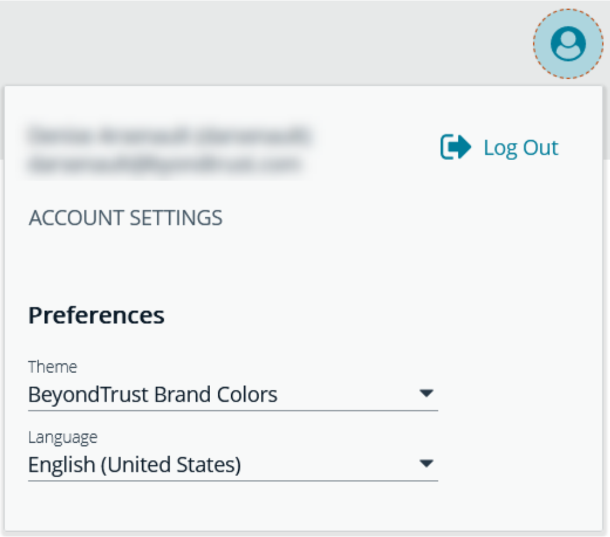
4. Click **Log In**.

***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 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.**



Theme
BeyondTrust Brand Colors

Language
English (United States)

Select a Display Language

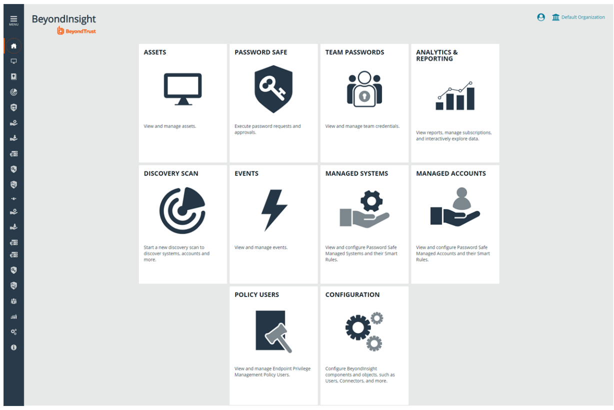
BeyondInsight and Password Safe can be displayed in the following languages:

- Dutch
- English
- French
- 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** list.

Navigate the Console

Once logged into the BeyondInsight Console, you are taken to the **Home** page, where the BeyondInsight suite of features is easily accessible by clicking the container cards or by clicking **Menu** in the left navigation menu.



ASSETS: View and manage assets.

PASSWORD SAFE: Execute password requests and approvals.

TEAM PASSWORDS: View and manage team credentials.

ANALYTICS & REPORTING: View reports, manage subscriptions, and interactively explore data.

DISCOVERY SCAN: Start a new discovery scan to discover systems, accounts and more.

EVENTS: View and manage events.

MANAGED SYSTEMS: View and configure Password Safe Managed Systems and their Smart Rules.

MANAGED ACCOUNTS: View and configure Password Safe Managed Accounts and their Smart Rules.

POLICY USERS: View and manage Endpoint Privilege Management Policy Users.

CONFIGURATION: Configure BeyondInsight components and objects, such as Users, Connectors, and more.

Available features include:

- **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 mange 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.
- **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.
- **Password Safe:** Access the Password Safe web portal to request passwords and remote access sessions and to approve requests.
- **Team Passwords:** View and manage team credentials.
- **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**.

> ***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 the BeyondInsight Console, go to **Configuration > Privileged Access Management > Functional Accounts**.
2. Click **Create 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.
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	Select an elevated account to run as: **sudo**, **pmrun**, **pbrun**, **pbrun jumphost**. If you are using **pbrun jumpost**, enter the IP address for the Privilege Management for Unix & Linux policy server that you want to connect to. *Note: **SSH Key Enforcement Mode** is not available if you are using **pbrun jumphost**.*
Change Agent (available only when Endpoint Privilege Management is installed)	Select **Password Safe** or **Endpoint Privilege Management Client** from the list.
Functional Account	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. *Note: The **Create New Functional Account** link is only available to users with administrative privileges.*
Use Login Account for SSH Sessions	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. **Login Account:** Select the account name.
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	Verifies SSH host keys from a known host. You can import SSH keys from a host using a Smart Rule. **Auto Accept Initial Key:** The first key imported is automatically accepted. Any new key imported after the initial key must be manually accepted. **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.
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:

- *"Add SAP as a Managed System" on page 105*
- *"Create Password Policies" on page 66*
- *"Enable Login Accounts for SSH Sessions" on page 124*
- *"Import an SSH Server Key Using a Smart Rule" on page 26*
- *"Manage the SSH Server Keys" on page 26*
- *"Set DSS on the Managed Account" on page 140*
- *"Configure Password Safe Access Policies" on page 59*

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.*

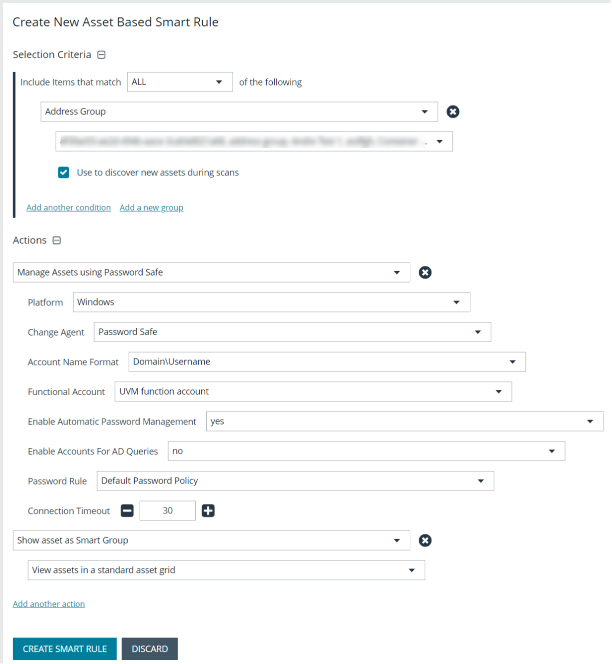
1. From the left navigation pane, click **Smart Rules**.
2. Select **Asset** from the **Smart Rule Type filter** dropdown list.
3. Click **Create Smart Rule +**.
4. Select a **Category** from the dropdown list.
5. Enter a **Name** and **Description** for the Smart Rule.
6. Select a **Reprocessing Limit** from the dropdown list 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

[redacted]

☑ Use to discover new assets during scans

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

Show asset as Smart Group

View assets in a standard asset grid

For complete descriptions of fields and settings for the Smart Rule, please see "Add a Managed System Manually" on page 13.

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 navigation, 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.
        - 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.
   - **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.

10. Under **Actions**, click the link to **Add another action**, and then select **Show managed account as Smart Group**.
11. Click **Create Smart Rule**.

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.

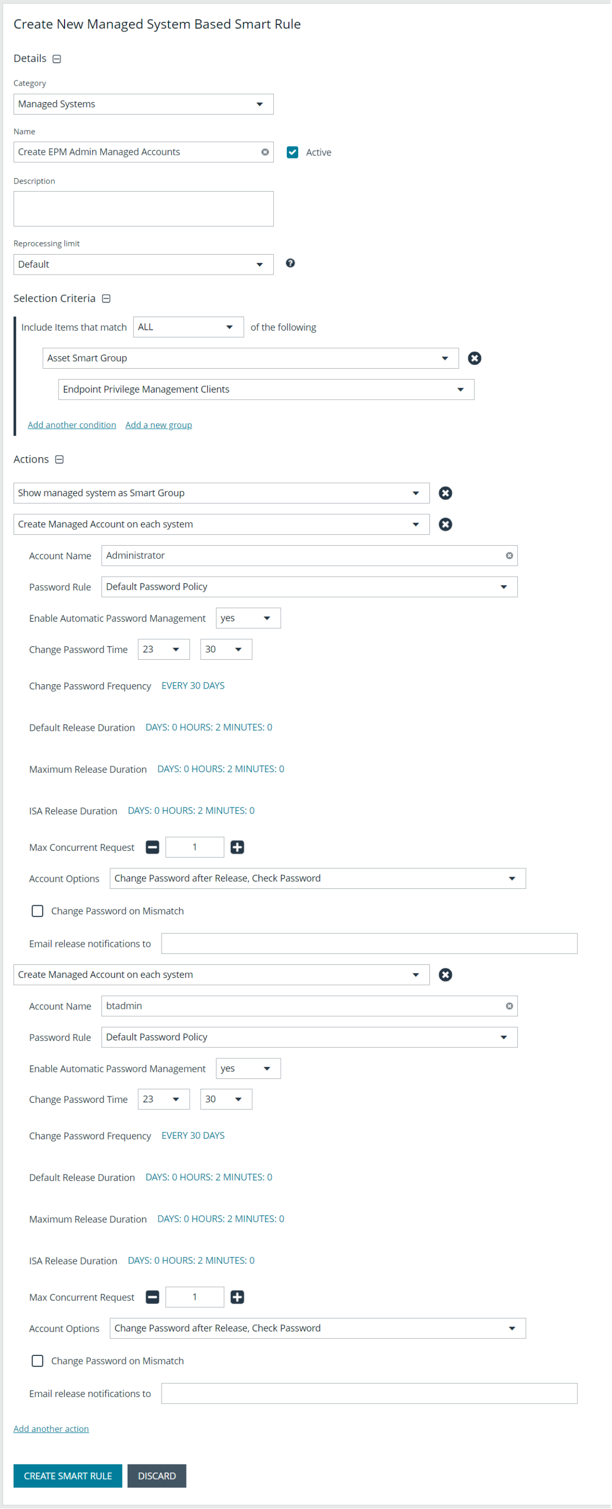
One scenario in which this is useful is when you have Endpoint Privilege Management (EPM) clients in your environment. You can create a managed system Smart Rule to add local accounts as managed accounts from the EPM client endpoints so that a password rotation event exists when the EPM agent requests 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 navigation 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 menu, 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 dropdown menus.
7. For **Actions**, select **Show managed system as a Smart Group** and **Create Managed Account on each system** from the dropdown menus.
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

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 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 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:

> *For more information, please see the following:*

- *"Add a Managed System Manually" on page 13*
- *"Add Directory Accounts" on page 73*

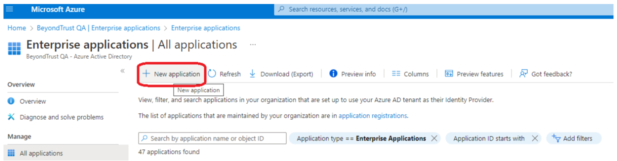
Configure Functional Account Requirements in Azure

Follow the steps below to set up Azure Active Directory 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**.



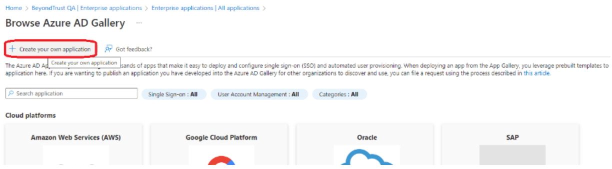
Microsoft Azure
Search resources, services, and docs (G+/)
Home > BeyondTrust QA | Enterprise applications > Enterprise applications
Enterprise applications | All applications
BeyondTrust QA - Azure Active Directory
New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?
Overview
Overview
Diagnose and solve problems
Manage
All applications
Search by application name or object ID
Application type == Enterprise Applications
Application ID starts with
Add filters

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

47 applications found

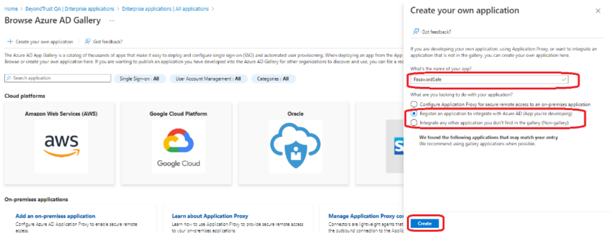
2. Select **Create your own application**.



Home > BeyondTrust QA | Enterprise applications > Enterprise applications | All applications >
Browse Azure AD Gallery
Create your own application
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
Google Cloud Platform
Oracle
SAP

The Azure AD Ap[...]sands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to application here. If you are wanting to publish an application you have developed into the Azure AD Gallery for other organizations to discover and use, you can file a request using the process described in this article.

3. Name your application, select the application type (**App you're developing**) and click **Create**.



Home > BeyondTrust QA | Enterprise applications > Enterprise applications | All applications >
Browse Azure AD Gallery
Create your own application
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
aws
Google Cloud Platform
Google Cloud
Oracle
On-premises applications
Add an on-premises application
Learn about Application Proxy
Manage Application Proxy co
Create your own application
Got feedback?
Create

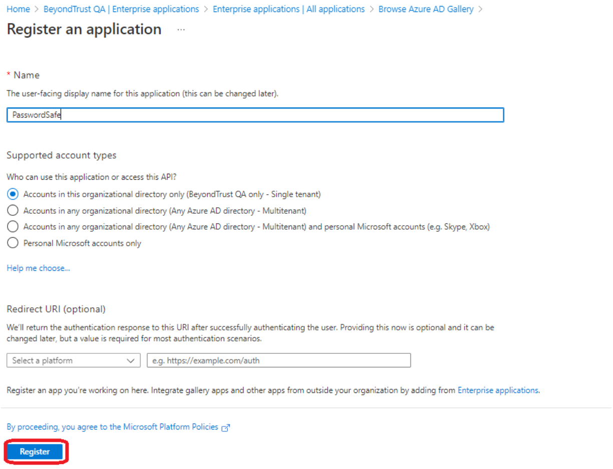
If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?
PasswordSafe

What are you looking to do with your application?
○ Configure Application Proxy for secure remote access to an on-premises application
● Register an application to integrate with Azure AD (App you're developing)
○ Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry
We recommend using gallery applications when possible.

4. Update the name if necessary, select the **Supported Account Types** (**this directory only**) and click **Register**.



Home > BeyondTrust QA | Enterprise applications > Enterprise applications | All applications > Browse Azure AD Gallery >
Register an application
Help me choose...
Select a platform
e.g. https://example.com/auth
Register

* Name

The user-facing display name for this application (this can be changed later).

PasswordSafe

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (BeyondTrust QA only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

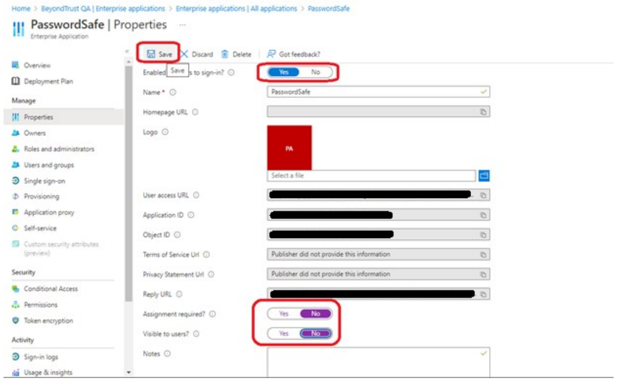
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

5. Under **Properties**, disable **Assignment required** and **Visible to users**, and click **Save**.



Home > BeyondTrust QA | Enterprise applications > Enterprise applications | All applications > PasswordSafe

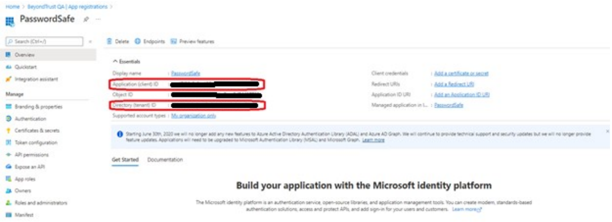
PasswordSafe | Properties

Enterprise Application

- Enabled for users to sign-in? [✓ Yes] No
- Name * : PasswordSafe
- Homepage URL :
- Logo : PA — Select a file
- User access URL : [redacted]
- Application ID : [redacted]
- Object ID : [redacted]
- Terms of Service Url : Publisher did not provide this information
- Privacy Statement Url : Publisher did not provide this information
- Reply URL : [redacted]
- Assignment required? Yes [✓ No]
- Visible to users? Yes [✓ No]
- Notes :

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.



Home > BeyondTrust QA | App registrations >

PasswordSafe

Essentials

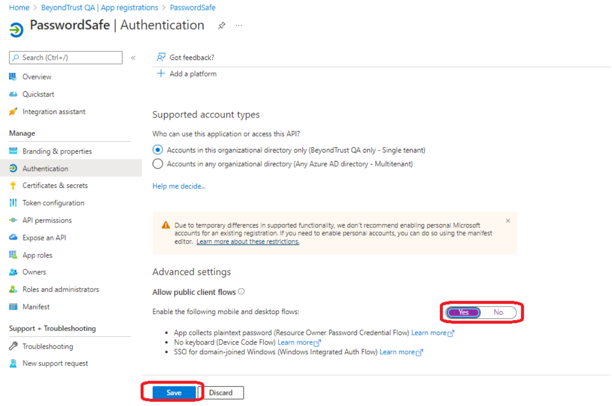
- Display name : PasswordSafe
- Application (client) ID : [redacted]
- Object ID : [redacted]
- Directory (tenant) ID : [redacted]
- Supported account types : My organization only
- Client credentials : Add a certificate or secret
- Redirect URIs : Add a Redirect URI
- Application ID URI : Add an Application ID URI
- Managed application in l... : PasswordSafe

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

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



Home > BeyondTrust QA | App registrations > PasswordSafe

PasswordSafe | Authentication

Supported account types

Who can use this application or access this API?

- ● Accounts in this organizational directory only (BeyondTrust QA only - Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

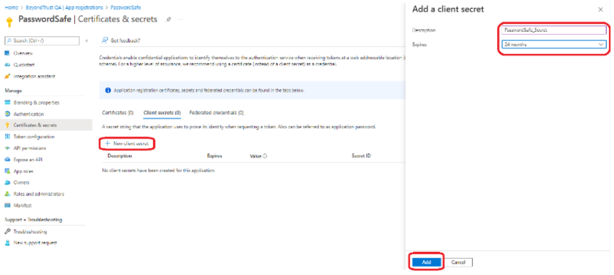
Advanced settings

Allow public client flows

Enable the following mobile and desktop flows: [✓ Yes] No

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

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



Home > BeyondTrust QA | App registrations > PasswordSafe

PasswordSafe | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) | Client secrets (0) | Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

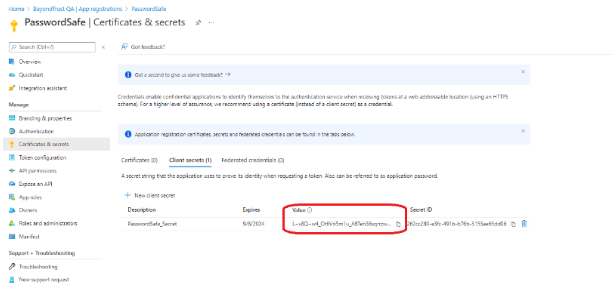
Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

Add a client secret

- Description : PasswordSafe_Secret
- Expires : 24 months

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.*



Got a second to give us some feedback? →

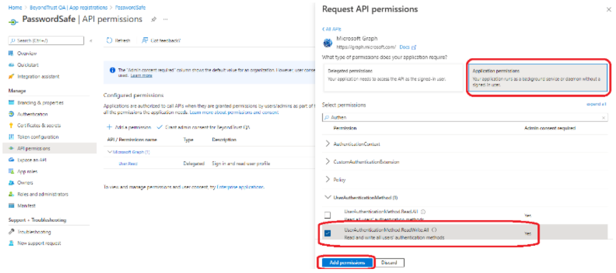
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
PasswordSafe_Secret	9/8/2024	L~v8Q~w4_Ct6Vri5m1u_A8Teh36sqrzw...	262cc280-e3fc-491b-b76b-3153ae65dd06

10. In the **API permissions** section, add **Microsoft Graph**, and select type **Application permissions**.
11. Add Microsoft Graph application permission **User.AuthenticationMethod.ReadWrite.All**, **Domain.Read.All**, and **Group.Read.All**.
12. If **User.Read** is not already added, select **Delegated permissions** and add it.
13. Click **Add Permissions**.



The "Admin consent required" column shows the default value for an organization. However, user conse... used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of t... all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

To view and manage permissions and user consent, try Enterprise applications.

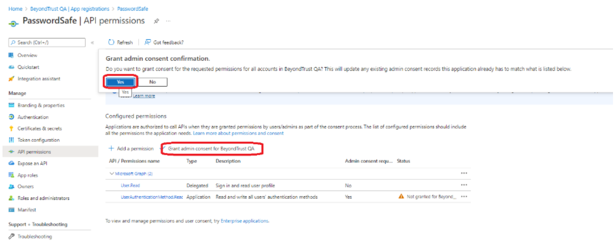
What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

	Permission	Admin consent required
	> AuthenticationContext	
	> CustomAuthenticationExtension	
	> Policy	
	∨ UserAuthenticationMethod (1)	
☐	UserAuthenticationMethod.Read.All Read all users' authentication methods	Yes
☑	UserAuthenticationMethod.ReadWrite.All Read and write all users' authentication methods	Yes

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



Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in BeyondTrust QA? This will update any existing admin consent records this application already has to match what is listed below.

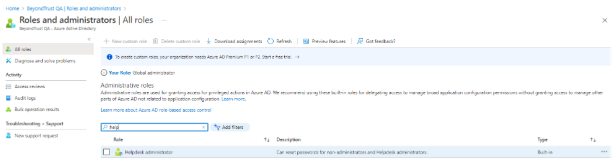
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
User.Read	Delegated	Sign in and read user profile	No	
UserAuthenticationMethod.Reac	Application	Read and write all users' authentication methods	Yes	⚠ Not granted for Beyond...

To view and manage permissions and user consent, try Enterprise applications.

15. From the main menu, select **Roles and administrators**, then select the **Helpdesk administrator** role.



To create custom roles, your organization needs Azure AD Premium P1 or P2. Start a free trial. →

Your Role: Global administrator

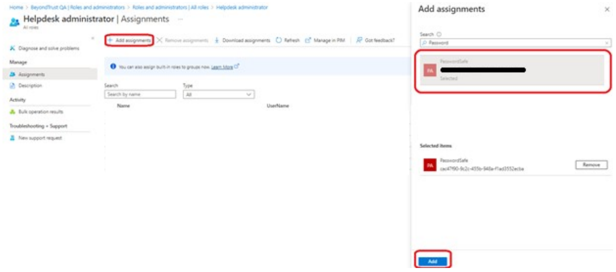
Administrative roles

Administrative roles are used for granting access for privileged actions in Azure AD. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Azure AD not related to application configuration. Learn more.

Learn more about Azure AD role-based access control

	Role	Description	Type
☐	Helpdesk administrator	Can reset passwords for non-administrators and Helpdesk administrators.	Built-in

16. Click **Add assignments**, then assign the application to the **Helpdesk administrator** role.



You can also assign built-in roles to groups now. Learn More

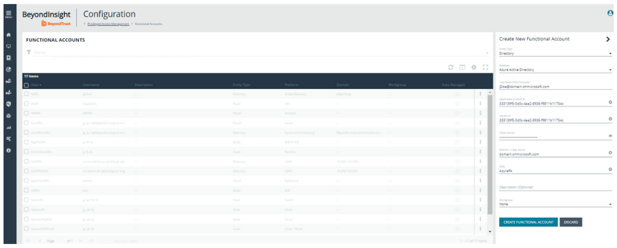
[redacted]

PasswordSafe
cad4790-9c2c-455b-948a-f1ad3552ecba

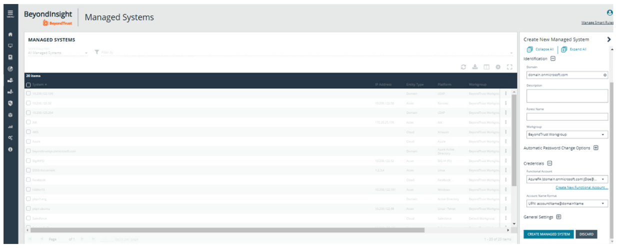
This completes configuration in Microsoft Azure. The remaining steps are done in BeyondTrust Password Safe.

BeyondTrust Password Safe Configuration

17. Go to **Configuration > Privileged Account Management > Functional Accounts**.
18. Click **Create New Functional Account**.
19. For the **Entity Type**, select **Directory**.
20. For the **Platform**, select **Azure Active Directory**,
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**.

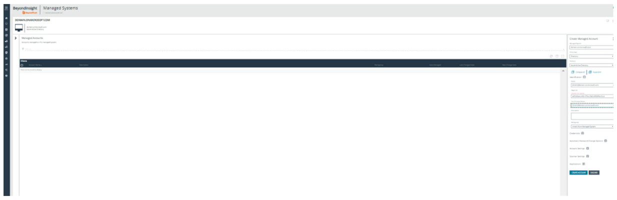


25. Go to **Managed Systems**.
26. Click **Create New Managed System**.
27. For the **Entity Type**, select **Directory**.
28. For the **Platform**, select **Azure Active Directory**,
29. Enter the **Domain**, select the **Functional Account** created above, and select the **Account Name Format**.
30. Click **Create Managed System**.

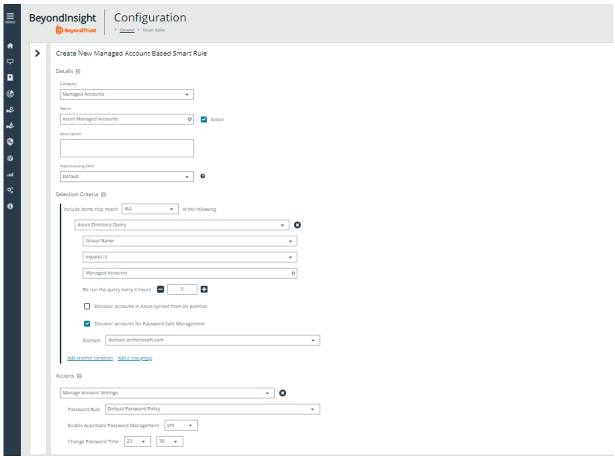


The Managed Account can be created manually or by using a Smart Rule.

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.



Create New Managed Account Based Smart Rule

Details

Category: Managed Accounts

Name: Azure Managed Accounts ☑ Active

Description:

Reprocessing limit: Default

Selection Criteria

Include Items that match ALL of the following

Azure Directory Query

Group Name

equals (=)

Managed Accounts

Re-run the query every X hours 0

☐ Discover accounts in Azure synced from on-premise

☑ Discover accounts for Password Safe Management

Domain: domain.onmicrosoft.com

Add another condition Add a new group

Actions

Manage Account Settings

Password Rule: Default Password Policy

Enable Automatic Password Management: yes

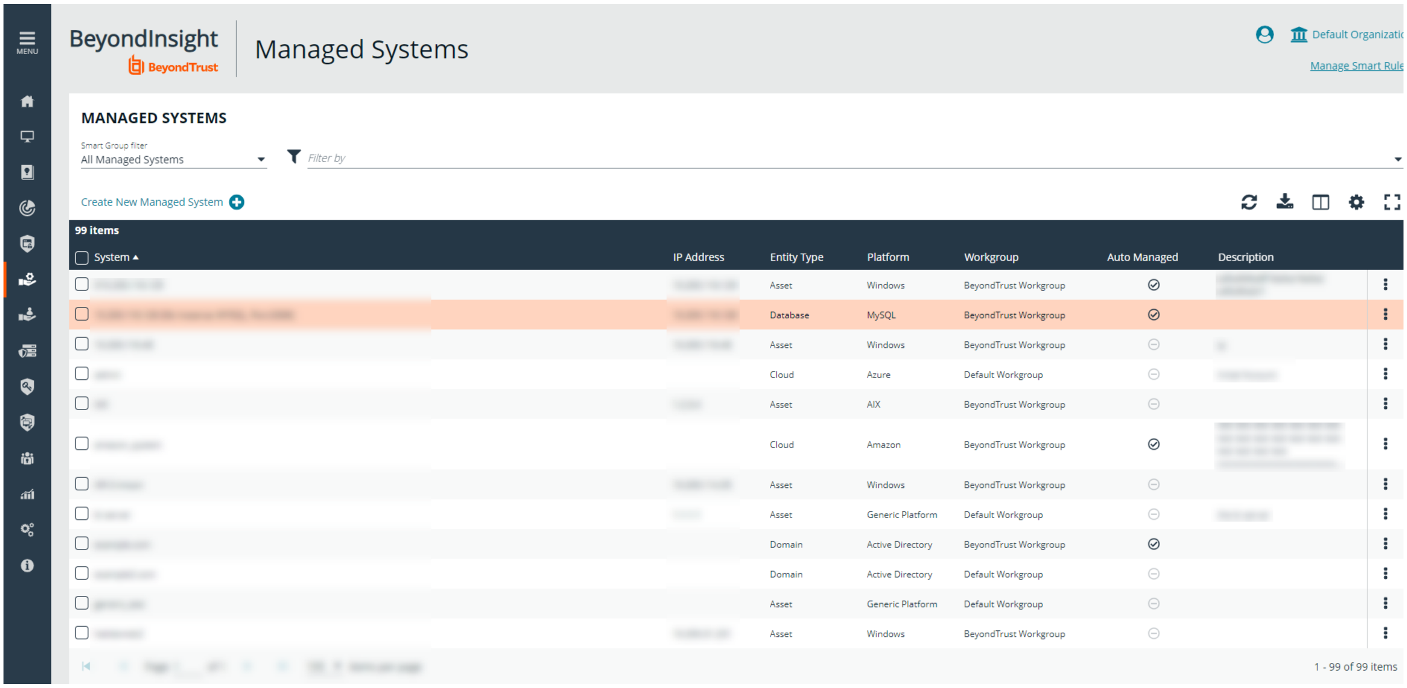
Change Password Time: 23 30

> *For more information on using Smart Rules, please see "Work with Smart Rules" on page 35.*

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.



MANAGED SYSTEMS

Smart Group filter: All Managed Systems

Filter by

Create New Managed System

99 items

System ▲	IP Address	Entity Type	Platform	Workgroup	Auto Managed	Description
[redacted]	[redacted]	Asset	Windows	BeyondTrust Workgroup	✓	[redacted]
[redacted]	[redacted]	Database	MySQL	BeyondTrust Workgroup	✓	
[redacted]	[redacted]	Asset	Windows	BeyondTrust Workgroup	⊖	[redacted]
[redacted]		Cloud	Azure	Default Workgroup	⊖	[redacted]
[redacted]	[redacted]	Asset	AIX	BeyondTrust Workgroup	⊖	
[redacted]		Cloud	Amazon	BeyondTrust Workgroup	✓	[redacted]
[redacted]	[redacted]	Asset	Windows	BeyondTrust Workgroup	⊖	
[redacted]	[redacted]	Asset	Generic Platform	Default Workgroup	⊖	[redacted]
[redacted]		Domain	Active Directory	BeyondTrust Workgroup	✓	
[redacted]		Domain	Active Directory	Default Workgroup	⊖	
[redacted]		Asset	Generic Platform	Default Workgroup	⊖	
[redacted]	[redacted]	Asset	Windows	BeyondTrust Workgroup	⊖	

[redacted] 1 - 99 of 99 items

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

- *"Add a Managed System Manually" on page 13*
- *"Add Managed Systems and Accounts Using Smart Rules" on page 16*

View Managed Systems Details

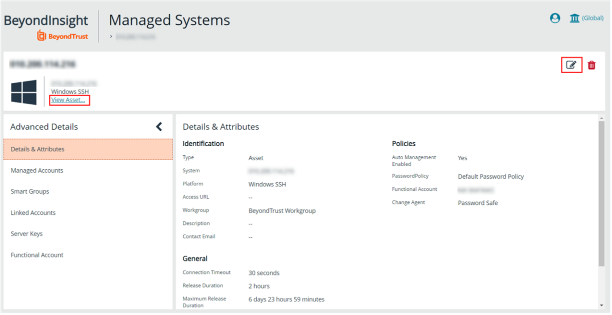
You can view details about the managed system, such as:

- 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.*



[redacted]

[redacted]
Windows SSH
View Asset...

Advanced Details
- Details & Attributes
- Managed Accounts
- Smart Groups
- Linked Accounts
- Server Keys
- Functional Account

Details & Attributes

Identification

Type	Asset
System	[redacted]
Platform	Windows SSH
Access URL	--
Workgroup	BeyondTrust Workgroup
Description	--
Contact Email	--

Policies

Auto Management Enabled	Yes
PasswordPolicy	Default Password Policy
Functional Account	[redacted]
Change Agent	Password Safe

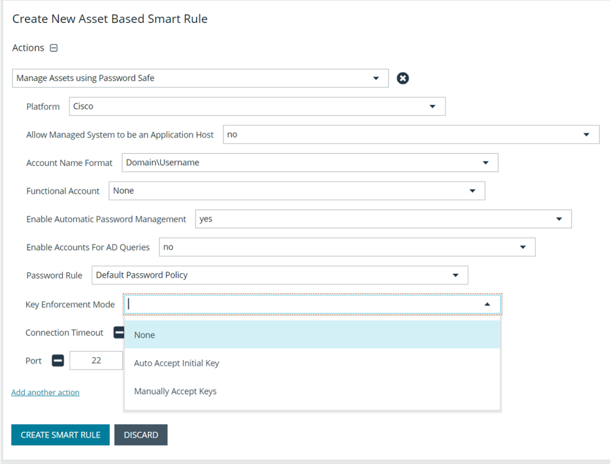
General

Connection Timeout	30 seconds
Release Duration	2 hours
Maximum Release Duration	6 days 23 hours 59 minutes

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**.


Create New Asset Based Smart Rule

Actions ⊟

Manage Assets using Password Safe

Platform	Cisco
Allow Managed System to be an Application Host	no
Account Name Format	Domain\Username
Functional Account	None
Enable Automatic Password Management	yes
Enable Accounts For AD Queries	no
Password Rule	Default Password Policy
Key Enforcement Mode	
Connection Timeout	
Port	22

> ***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 13.*

Manage the SSH Server Keys

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

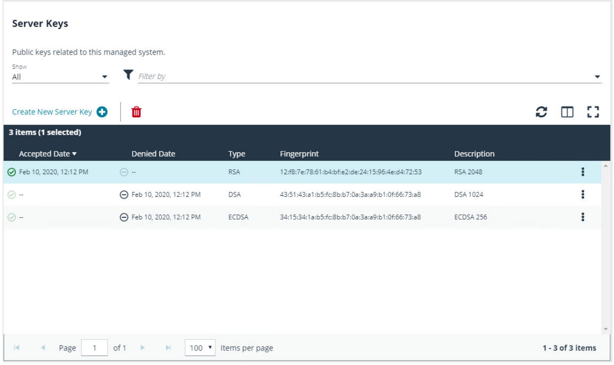
An email notification is sent to the **Administrators** user group when a key is imported and the **Key Enforcement Mode** is set to **Manually Accepted Keys**. The email notifies the administrators that a fingerprint requires action, what asset the key is on, and also provides details about the fingerprint.

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 148.

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**.



Server Keys

Public keys related to this managed system.

Show: All

3 items (1 selected)

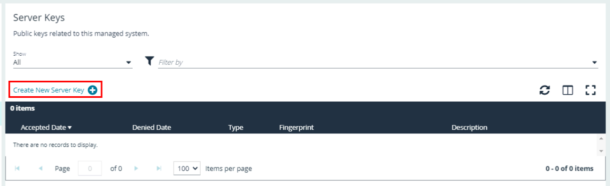
Accepted Date ▾	Denied Date	Type	Fingerprint	Description
✓ Feb 10, 2020, 12:12 PM	⊖ --	RSA	12:f8:7e:78:61:b4:bf:e2:de:24:15:96:4e:d4:72:53	RSA 2048
✓ --	⊖ Feb 10, 2020, 12:12 PM	DSA	43:51:43:a1:b5:fc:8b:b7:0a:3a:a9:b1:0f:66:73:a8	DSA 1024
✓ --	⊖ Feb 10, 2020, 12:12 PM	ECDSA	34:15:34:1a:b5:fc:8b:b7:0a:3a:a9:b1:0f:66:73:a8	ECDSA 256

1 - 3 of 3 items

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**.
5. Select a key type and enter a **Fingerprint** and a **Description**.
6. Click **Create Key**.



Server Keys

Public keys related to this managed system.

Show: All

0 items

Accepted Date ▾	Denied Date	Type	Fingerprint	Description

There are no records to display.

0 - 0 of 0 items

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

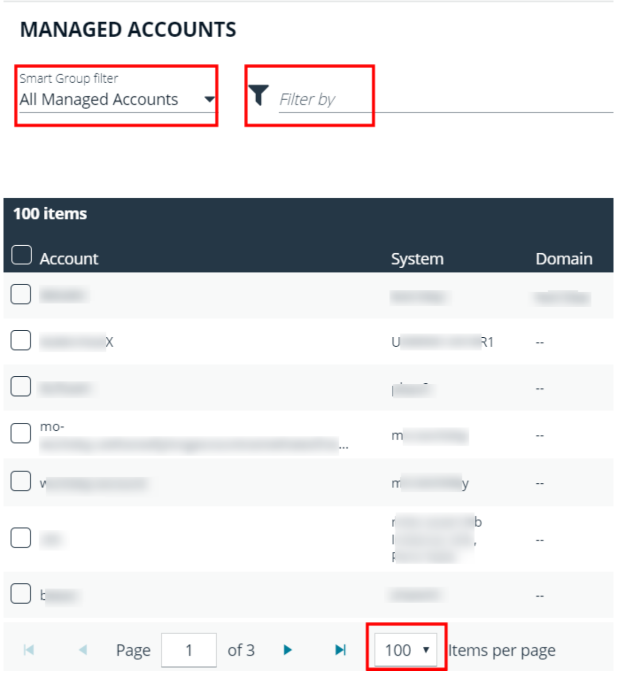
***Note:** The fingerprint must be unique. An error message is displayed if the key is already imported.*

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, the first 100 accounts are displayed in the grid. 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 **Smart Group filter** to filter the list by Smart Group and you can also filter the list by various attributes using the **Filter by** list.



MANAGED ACCOUNTS

Smart Group filter: All Managed Accounts

Filter by

100 items

□ Account	System	Domain
□ [redacted]	[redacted]	[redacted]
□ [redacted]	[redacted]	--
□ [redacted]	[redacted]	--
□ [redacted]	[redacted]	--
□ [redacted]	[redacted]	--
□ [redacted]	[redacted]	--
□ [redacted]	[redacted]	--

Page 1 of 3 · 100 ▾ Items per page

View Managed Account Details

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

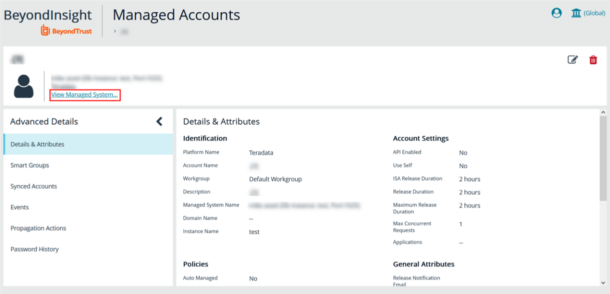
- Review the attributes and settings assigned to the account, such its identifying details, settings, and policies.
- View managed systems linked to the account.
- View Smart Groups associated with the account, as well as their last process date and processing status.
- See which accounts are synced 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 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.*



Details & Attributes

Identification

Platform Name	Teradata
Account Name	[redacted]
Workgroup	Default Workgroup
Description	[redacted]
Managed System Name	[redacted]
Domain Name	--
Instance Name	test

Account Settings

API Enabled	No
Use Self	No
ISA Release Duration	2 hours
Release Duration	2 hours
Maximum Release Duration	2 hours
Max Concurrent Requests	1
Applications	--

Policies

Auto Managed	No

General Attributes

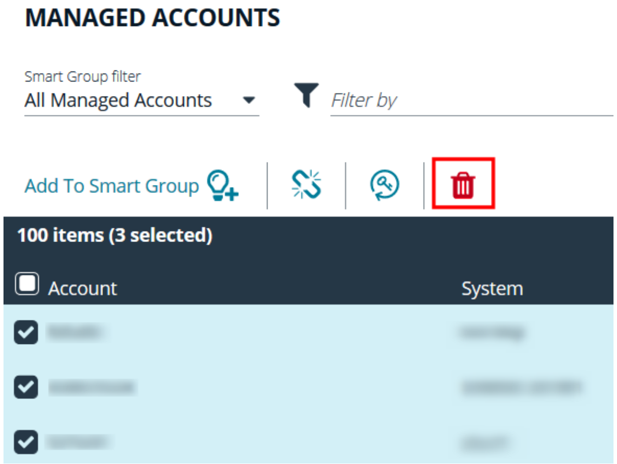
Release Notification Email

> *For more information on propagation actions, please see "Add Propagation Actions to Managed Accounts" on page 75.*

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.



100 items (3 selected)

□ Account	System
☑ [redacted]	[redacted]
☑ [redacted]	[redacted]
☑ [redacted]	[redacted]

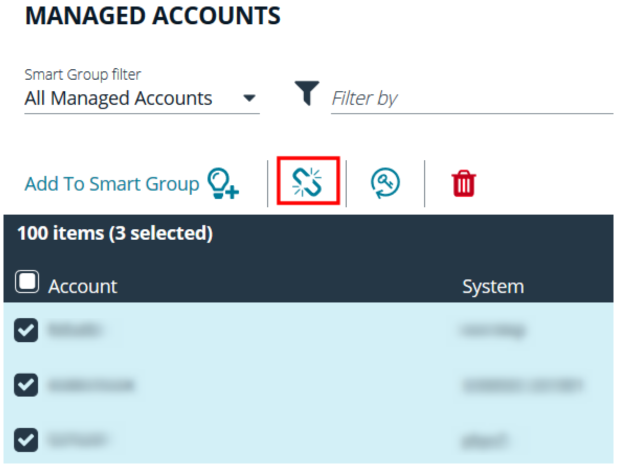
3. Click **Delete** on the confirmation message.

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**.

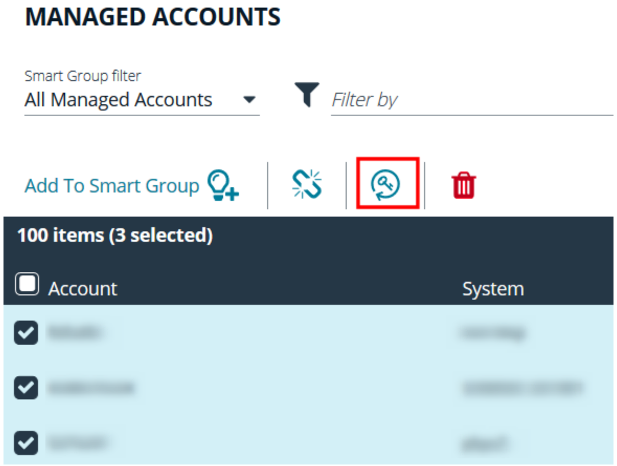
2. Select the account or multiple accounts you want to unlink, and then click the **Unlink** button above the grid.



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.



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.

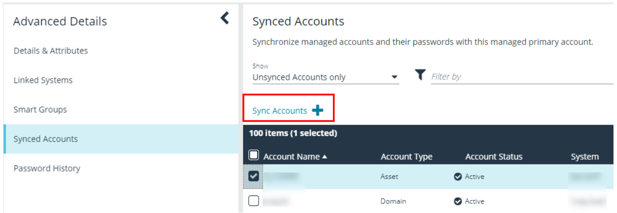
Once an account is synchronized as a subscriber account, settings modifications are limited to:

- Enable API
- Allow for scanning

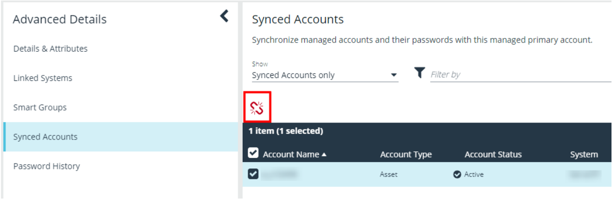
- Application

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 +**.



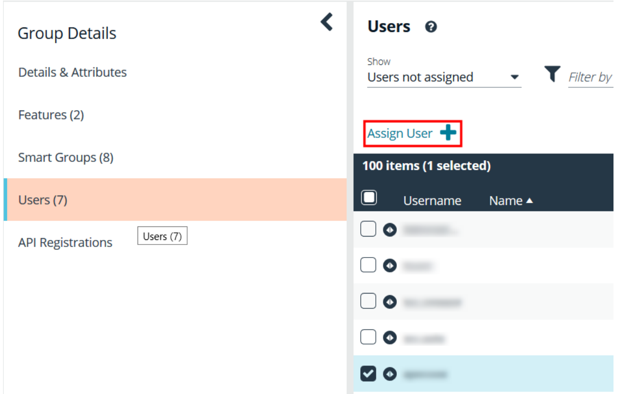
6. To remove a synced account, select the account, and then click the **Unsync Accounts** button above the grid.



Configure Password Reset for Managed Account Users

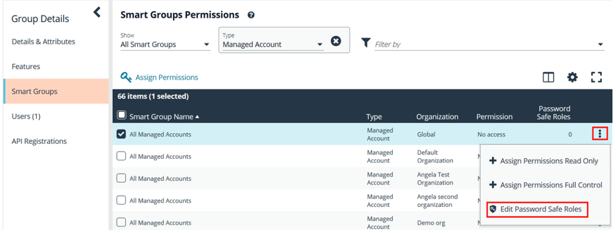
You can grant managed account users permission to reset the password on their own managed account, without granting them permission to reset passwords on other managed accounts. You can do this by creating a group, adding the managed account to the group, and then assigning permissions and the **Credential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

1. In the BeyondInsight Console, go to **Configuration > Role Based Access > User Management**.
2. Under **Groups**, 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**, and then assign users to the group.



6. From the **Group Details** pane, select **Features**.
7. Select the **Management Console Access** and **Password Safe Account Management** features, and then click **Assign Permissions**.
8. Select **Assign Permissions Read Only**. Do not grant **Full Control**.

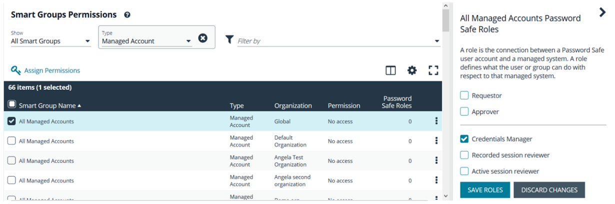
9. From the **Group Details** pane, select **Smart Groups**.
10. Filter the list of Smart Groups by **Type > Managed Account**.
11. Select the Smart Group that contains the applicable managed accounts.
12. Click the vertical ellipsis button for the Smart Group, and then select **Edit Password Safe Roles**.



66 items (1 selected)

Smart Group Name	Type	Organization	Permission	Password Safe Roles
☑ All Managed Accounts	Managed Account	Global	No access	0
□ All Managed Accounts	Managed Account	Default Organization		
□ All Managed Accounts	Managed Account	Angela Test Organization		
□ All Managed Accounts	Managed Account	Angela second organization		
□ All Managed Accounts	Managed Account	Demo org		

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



66 items (1 selected)

Smart Group Name	Type	Organization	Permission	Password Safe Roles
☑ All Managed Accounts	Managed Account	Global	No access	0
□ All Managed Accounts	Managed Account	Default Organization	No access	0
□ All Managed Accounts	Managed Account	Angela Test Organization	No access	0
□ All Managed Accounts	Managed Account	Angela second organization	No access	0

All Managed Accounts 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
□ Approver
☑ Credentials Manager
□ Recorded session reviewer
□ Active session reviewer

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.

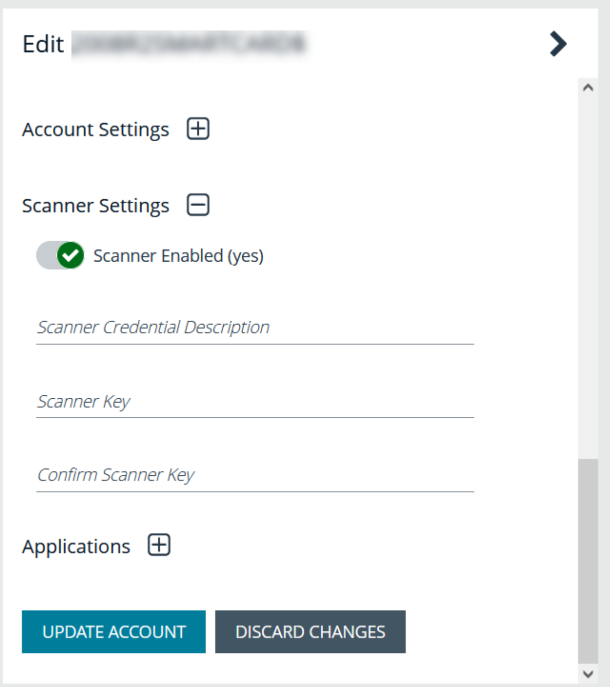
The following platforms are supported:

- 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**.



Edit [redacted]

Account Settings ⊞

Scanner Settings ⊟

Scanner Enabled (yes)

Scanner Credential Description

Scanner Key

Confirm Scanner Key

Applications ⊞

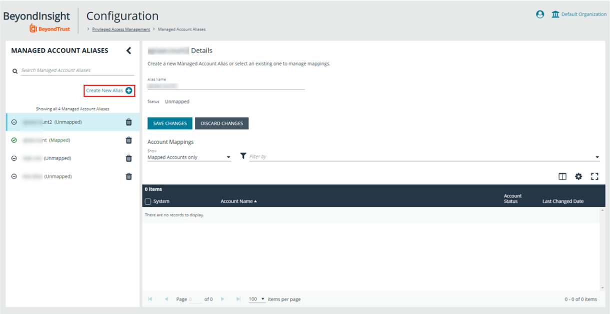
UPDATE ACCOUNT DISCARD CHANGES

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**.



BeyondInsight | Configuration

> Privileged Access Management > Managed Account Aliases

Default Organization

MANAGED ACCOUNT ALIASES

Search Managed Account Aliases

Create New Alias ⊕

Showing all 4 Managed Account Aliases

⊖ [redacted]unt2 (Unmapped)

✓ [redacted]nt (Mapped)

⊖ [redacted] (Unmapped)

⊖ [redacted] (Unmapped)

[redacted] Details

Create a new Managed Account Alias or select an existing one to manage mappings.

Alias Name [redacted]

Status Unmapped

SAVE CHANGES DISCARD CHANGES

Account Mappings

Show: Mapped Accounts only

Filter by

0 items

☐ System	Account Name ▲	Account Status	Last Changed Date

There are no records to display.

Page of 0 100 items per page 0 - 0 of 0 items

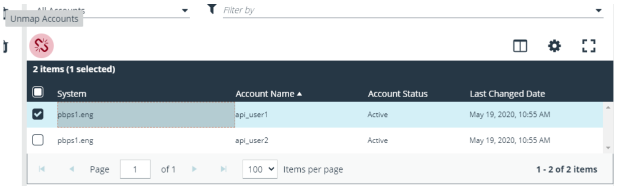
The new alias appears in the grid under **Account Mappings**, which displays all aliases ready to be mapped. New aliases show as **Unmapped** until they are associated with accounts.

> ***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.



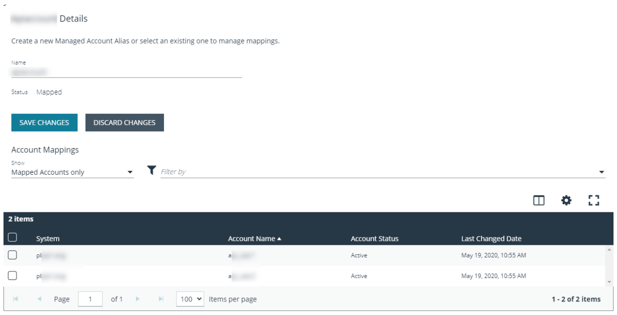
2 items (1 selected)

	System	Account Name ▲	Account Status	Last Changed Date
☑	pbps1.eng	api_user1	Active	May 19, 2020, 10:55 AM
□	pbps1.eng	api_user2	Active	May 19, 2020, 10:55 AM

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.



[redacted] Details

Create a new Managed Account Alias or select an existing one to manage mappings.

Name: [redacted]

Status: Mapped

Account Mappings

Show: Mapped Accounts only

2 items

	System	Account Name ▲	Account Status	Last Changed Date
□	pl[redacted]	a[redacted]	Active	May 19, 2020, 10:55 AM
□	pl[redacted]	a[redacted]	Active	May 19, 2020, 10:55 AM

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 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.

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 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 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**.

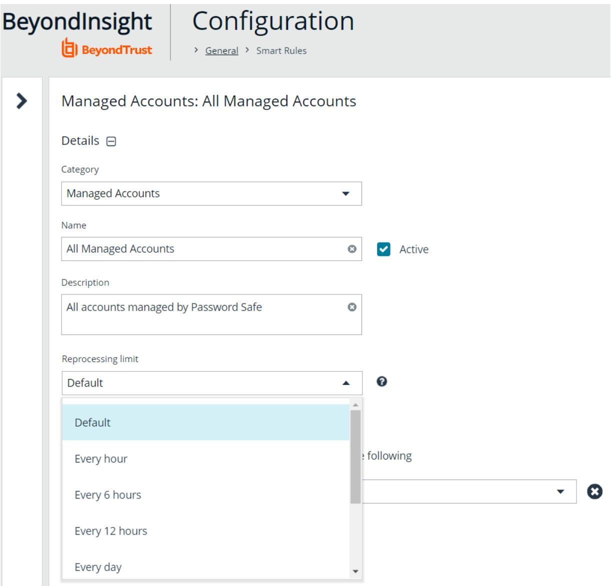
Change the Processing Frequency for a Smart Rule

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.*



Managed Accounts: All Managed Accounts

Details

Category: Managed Accounts

Name: All Managed Accounts ☑ Active

Description: All accounts managed by Password Safe

Reprocessing limit: Default

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 the BeyondInsight Console, 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.

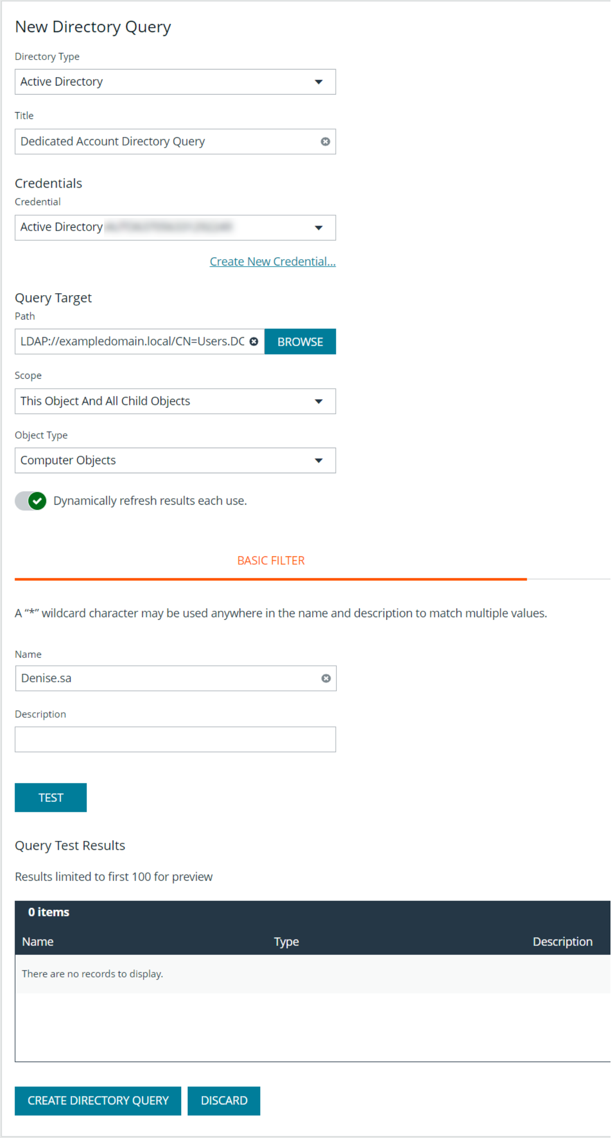
The below procedures provide instructions for configuring BeyondInsight users with the ability to access a dedicated directory account's credentials, using a query matching on directory attributes. Once configured, the users are able to request a password checkout for the dedicated account from the Password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

Query Target

Path: LDAP://exampledomain.local/CN=Users.DC

Scope: This Object And All Child Objects

Object Type: Computer Objects

Dynamically refresh results each use.

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

Name: Denise.sa

Description:

Query Test Results

Results limited to first 100 for preview

0 items

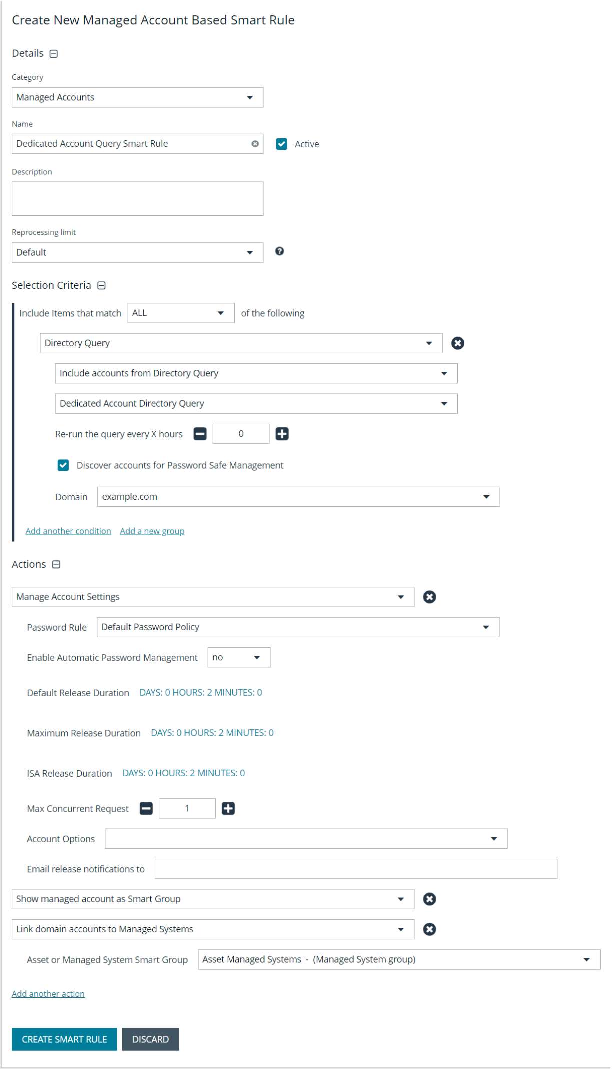
Name	Type	Description
There are no records to display.		

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

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 **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**.



Category: Managed Accounts

Name: Dedicated Account Query Smart Rule ☑ Active

Description:

Reprocessing limit: Default

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

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 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

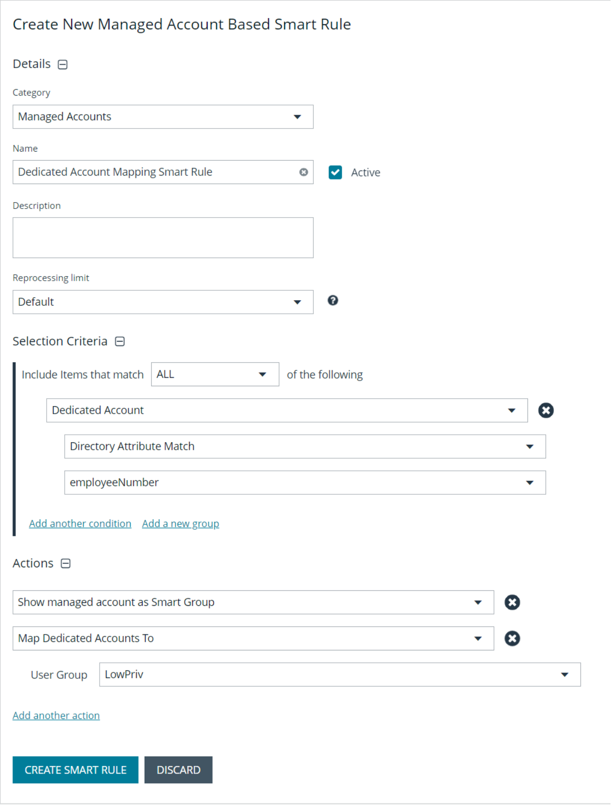
Asset or Managed System Smart Group: Asset Managed Systems - (Managed System group)

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**.



Create New Managed Account Based 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

Actions ⊟

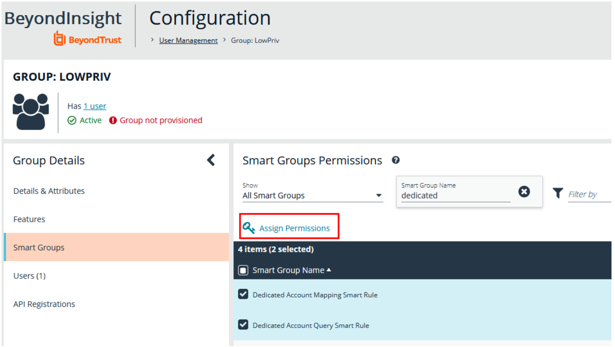
Show managed account as Smart Group

Map Dedicated Accounts To

User Group: LowPriv

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.



Configuration

› User Management › Group: LowPriv

GROUP: LOWPRIV

Has 1 user

Active · Group not provisioned

Smart Groups Permissions

Show: All Smart Groups

Smart Group Name: dedicated

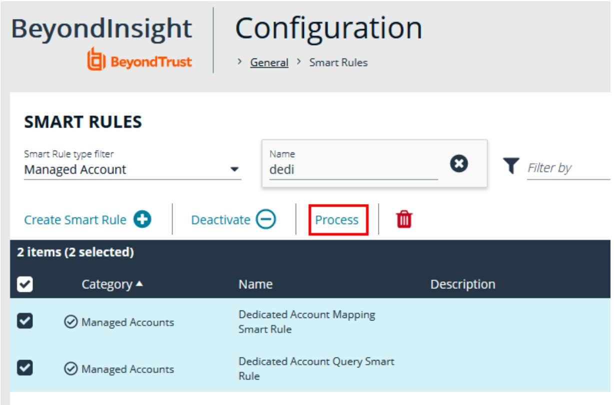
4 items (2 selected)

□ Smart Group Name ▲

☑ Dedicated Account Mapping Smart Rule

☑ Dedicated Account Query Smart Rule

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.



Smart Rule type filter: Managed Account

Name: dedi

2 items (2 selected)

☑	Category ▴	Name	Description
☑	Managed Accounts	Dedicated Account Mapping Smart Rule	
☑	Managed Accounts	Dedicated Account Query Smart Rule	

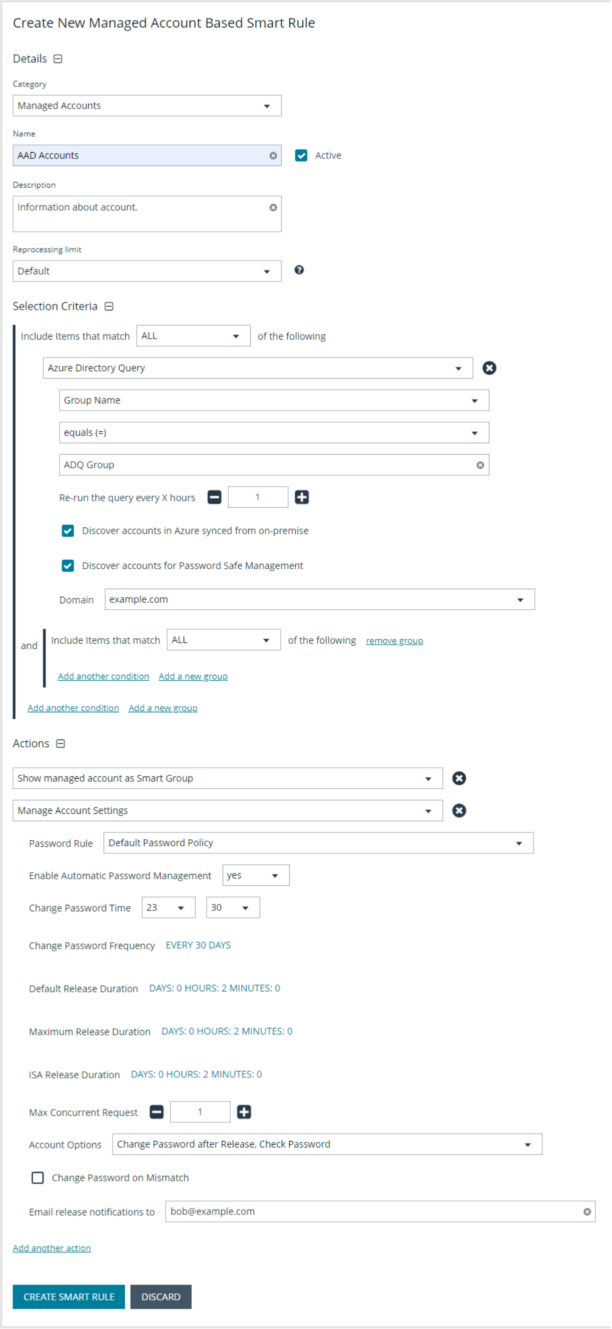
Use an Azure AD Smart Rule

An Azure Active Directory Smart Rule enables Password Safe to automatically discover Azure AD credentials. This allows privileged accounts in an Azure Active Directory to be managed, including password rotation and check-in and check-out.

Follow the steps below to discover Azure Active Directory Credentials.

1. On the left navigation pane, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule type filter** dropdown.
3. Click **Create Smart Rule +** and configure the role on the new screen.

4. **Category**: Select **Managed Accounts**.
5. **Name**: Provide a meaningful name and description that allows for easy identification of the Smart Rule.
6. **Reprocessing Limit**: If desired, select a reprocessing limit.
7. Under **Selection Criteria**, select **Azure Directory Query** from the dropdown.
8. There are several filters, and options are dynamic, depending on other selections.
    - Include **ALL** or **ANY** of the selection criteria.
    - Use a **Group Name** or a **User Principle Name**.
    - 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.
9. Set the value for how many hours for rerunning the query.
10. Check the **Discover accounts in Azure synced from on-premise** option to include AAD accounts synced from on-premises Azure AD, as well as Azure-only accounts.
11. **Discover accounts for Password Safe Management** is checked by default.
12. Select an Azure domain.
13. You can add additional selection criteria and groups.
14. Under **Actions**, select **Show managed account as Smart Group**.
15. Add other actions as required to manage settings or work with the managed account.
16. Click **Create Smart Rule**.



Create New Managed Account Based Smart Rule

Details ⊟

Category: Managed Accounts

Name: AAD Accounts ☑ Active

Description: Information about account.

Reprocessing limit: Default

Selection Criteria ⊟

Include Items that match ALL of the following

Azure Directory Query

Group Name

equals (=)

ADQ Group

Re-run the query every X hours 1

☑ Discover accounts in Azure synced from on-premise

☑ Discover accounts for Password Safe Management

Domain: example.com

and Include Items that match ALL of the following remove group

Add another condition Add a new group

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 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: bob@example.com

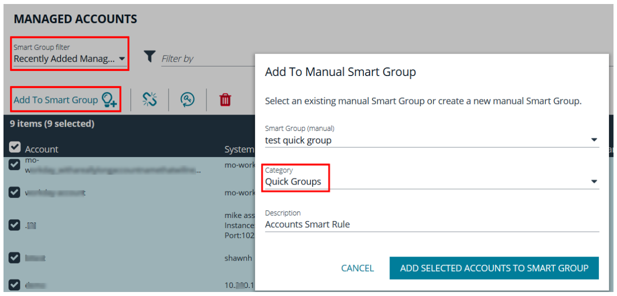
Add another action

CREATE SMART RULE DISCARD

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**.



MANAGED ACCOUNTS

Smart Group filter: Recently Added Manag...

9 items (9 selected)

Add To Manual Smart Group

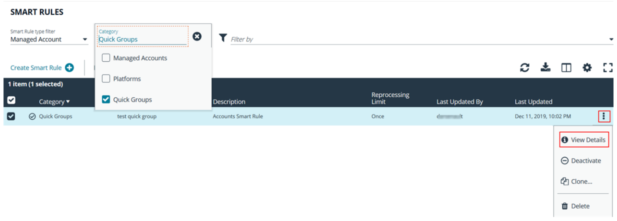
Select an existing manual Smart Group or create a new manual Smart Group.

Smart Group (manual): test quick group

Category: Quick Groups

Description: Accounts Smart Rule

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 **Quick Groups** from the **Category** dropdown, and then select a Quick Group from the **Smart Group** dropdown or create a new one.
6. Click **Add Selected Accounts To Smart Group**.
7. Your new Smart Group is now available in the **Smart Group filter** dropdown.
8. 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.



SMART RULES

Smart Rule type filter: Managed Account

Category: Quick Groups

□ Managed Accounts
□ Platforms
☑ Quick Groups

1 item (1 selected)

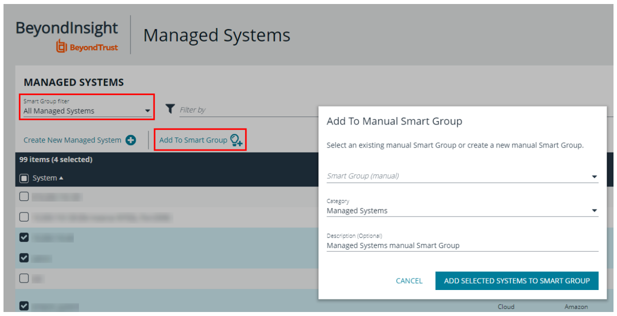
Category		Description	Reprocessing Limit	Last Updated By	Last Updated
Quick Groups	test quick group	Accounts Smart Rule	Once		Dec 11, 2019, 10:02 PM

9. To quickly locate Quick Groups from the **Smart Rules** page, select **Quick Groups** from the **Category** dropdown .
10. 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**.

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

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.*



BeyondInsight | Managed Systems

MANAGED SYSTEMS

Smart Group filter: All Managed Systems

99 items (4 selected)

Add To Manual Smart Group

Select an existing manual Smart Group or create a new manual Smart Group.

Smart Group (manual)

Category: Managed Systems

Description (Optional): Managed Systems manual Smart Group

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 **Category** from the dropdown, and then select a group from the **Smart Group** list or create a new one.
6. Click **Add Selected Systems To Smart Group**.
7. 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 37.

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: • 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 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: • Create, change, and remove directory and cloud systems. • Link and unlink directory accounts to managed systems. *Note: **Password Safe Account Management** is needed with **Password Safe System Management** to manage Password Safe accounts. **Full Control** is required for both.*
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.
Team Passwords	Users can access the Team Passwords 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.

Role	Description
Requester	Users can submit a request to retrieve a managed password or file. When assigning the Requester role, you must select an access policy.
Approver	Users can approve requests for the release of managed passwords or files. Typically, system administrators and network engineers are assigned to this role.
Requester/Approver	With this cross-functional role, a user can submit or approve requests for password or file releases. However, an approver cannot approve their request when dual control is enforced. This role is typically used in a peer approval environment.
Information Security Administrator	This role is responsible for setting up managed systems and accounts. The ISA role provides the functionality required for security help desk personnel. The ISA role can delegate limited authority to those responsible for resource management. The role enables a user to bypass every workflow and security measure, like approval workflows or checked out accounts. So even if another user already checked out an account and the password is known by this user, an ISA user can look at the password.
Auditor	Users can: • Log on and run reports in BeyondInsight Analytics & Reporting • View Replay Sessions in the web portal The Auditor role can be assigned with other roles.
No Roles	Assign this role to remove any previously assigned roles to a user group.
Credentials Manager	Users can set credentials using the **PUT ManagedAccounts/{accountId}/Credentials** API.
Recorded Session Reviewer	Users can view and take action on recorded Password Safe sessions, including: • Add comments • Mark the session as reviewed • Archive sessions if configured on the U-Series Appliance
Active Session Reviewer	Users can view and take action on active Password Safe sessions, including: • 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 release 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.

The roles that you can assign vary depending on the Smart Rule type.

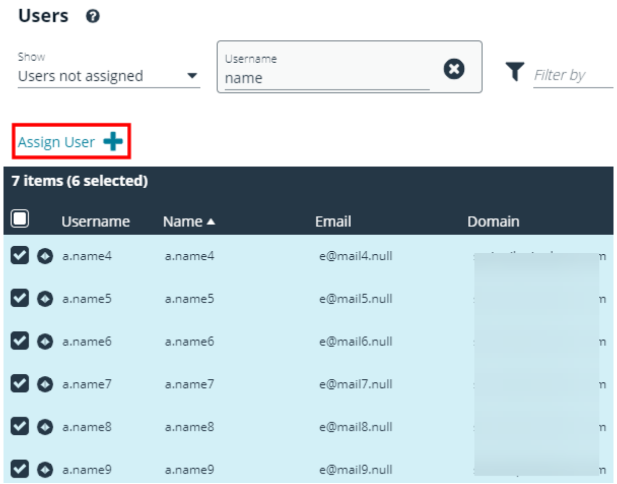
- **Asset Based Smart Rule:** Roles only include the ISA role and Auditor role.
- **Managed Accounts Based Smart Rule:** Roles include most roles.

Create a Group and Assign Roles

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

Roles are only available to BeyondInsight features.

1. From the left navigation pane in the console, select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Click **Create New Group**.
4. Select **Create a New Group**.
5. Enter a name and description for the group.
6. Click **Create Group**.
7. 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**.



Users

Show: Users not assigned

Username: name

Filter by

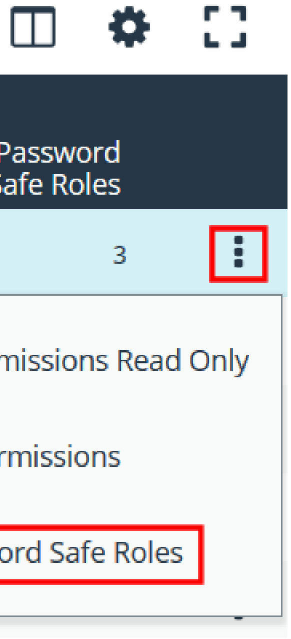
Assign User

7 items (6 selected)

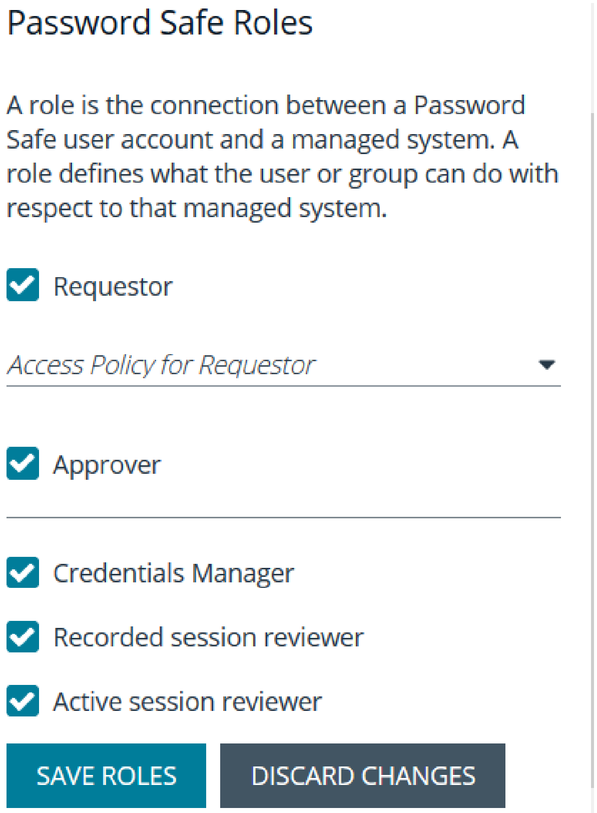
□	Username	Name ▲	Email	Domain
☑	a.name4	a.name4	e@mail4.null	[redacted]
☑	a.name5	a.name5	e@mail5.null	[redacted]
☑	a.name6	a.name6	e@mail6.null	[redacted]
☑	a.name7	a.name7	e@mail7.null	[redacted]
☑	a.name8	a.name8	e@mail8.null	[redacted]
☑	a.name9	a.name9	e@mail9.null	[redacted]

8. 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**.
9. 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 **More Options** button.
- Select **Edit Password Safe Roles**.



- Select the role(s). If selecting **Requestor**, also select an Access Policy from the dropdown list.
- 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

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.

The setting is turned on at the user account level as follows:

1. From the left navigation pane in the console, select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Under **Users**, select the user account.
4. Click the **More Options** button, and then select **Edit User Details**.
5. Enable the **Account Quarantined** option.
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. From the left navigation in the console, select **Configuration**.
2. Under **System**, click **Site Options**.
3. 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).

4. 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.

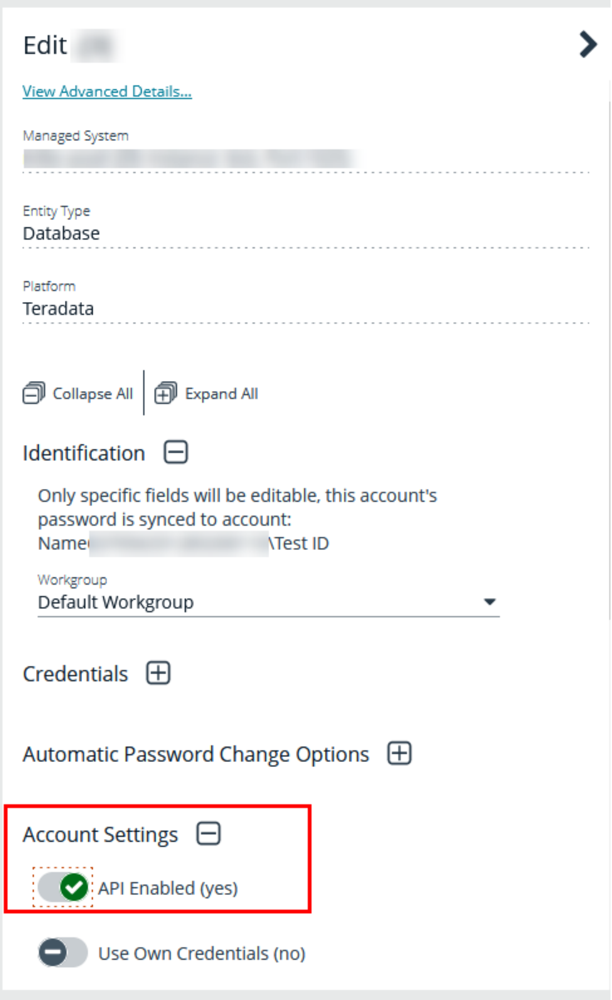
1. From the left navigation pane in the console, select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Select the group, and then click the **More Options** button.
4. Select **View Group Details**.
5. Under **Group Details**, select **API Registrations**.
6. Select 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. Select **Managed Accounts**.
2. Click the vertical ellipsis button for a managed account, and then select **Edit Account**.

3. Expand **Account Settings**, and then click the toggle to set the **API Enabled** option to **yes**.
4. Click **Update Account**.



Edit [redacted]

View Advanced Details...

Managed System
[redacted]

Entity Type
Database

Platform
Teradata

Identification

Only specific fields will be editable, this account's password is synced to account:
Name[redacted]\Test ID

Workgroup
Default Workgroup

Credentials

Automatic Password Change Options

Account Settings

API Enabled (yes)

Use Own Credentials (no)

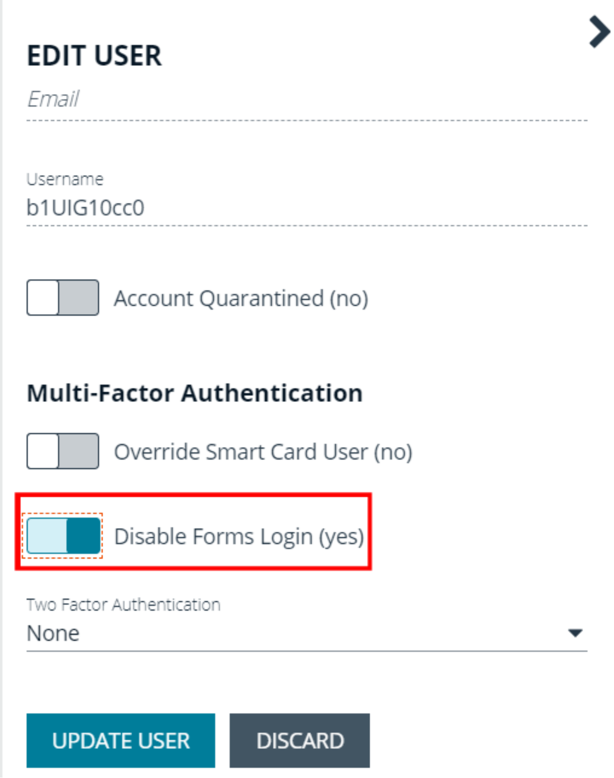
Restrict Access to Password Safe Login Page

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. Users must then always provide the SAML, smart card, or claims-aware credentials before gaining access to the web portal.

The setting can be applied to Active Directory, LDAP, and local BeyondInsight users.

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

1. From the left navigation pane in the console, select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Click **Users** to display the list of users in the grid.
4. Select a user, and then click the **More Options** button.
5. Select **Edit User Details**.
6. Click the toggle to change the **Disable Login Forms** option to **yes**.



EDIT USER

Email

Username: b1UIG10cc0

Account Quarantined (no)

Multi-Factor Authentication

Override Smart Card User (no)

Disable Forms Login (yes)

Two Factor Authentication: None

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 49.*

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 32.

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.

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 at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/role-based-access/create-groups/ldap.htm.

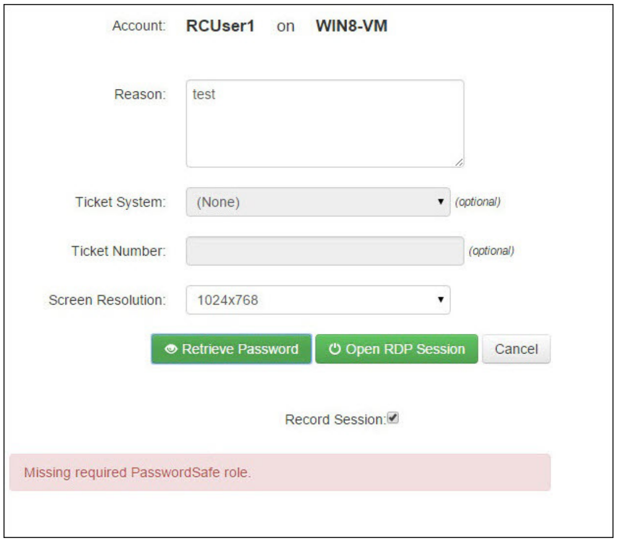
Real Time Authorization

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: test

Ticket System: (None) (optional)

Ticket Number: (optional)

Screen Resolution: 1024x768

Record Session: ☑

Missing required PasswordSafe role.

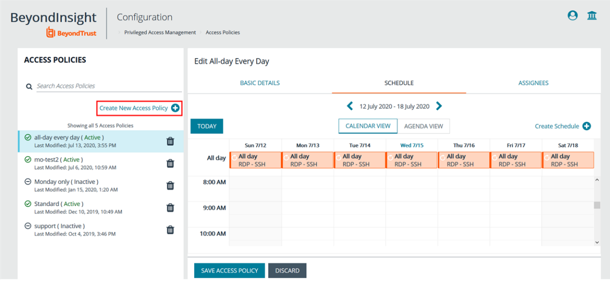
Configure Password Safe Access Policies

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

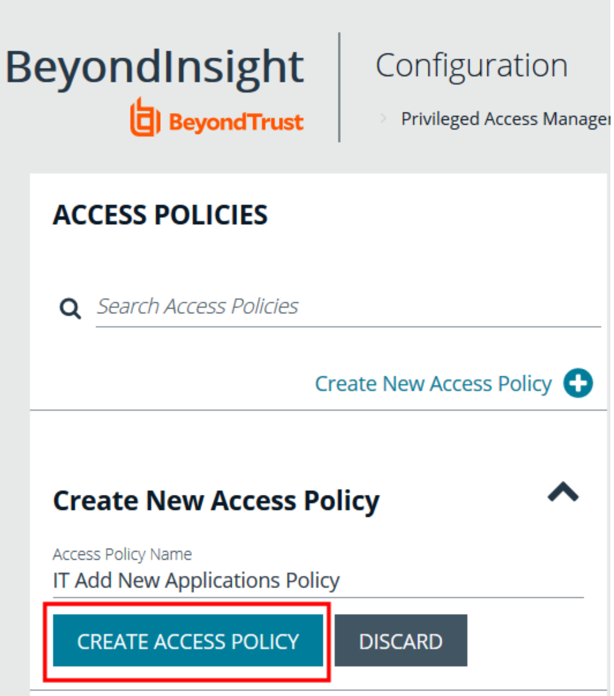
An access policy is selected when you are configuring the **Requester** role.

Create an Access Policy

1. In the console, navigate 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**.

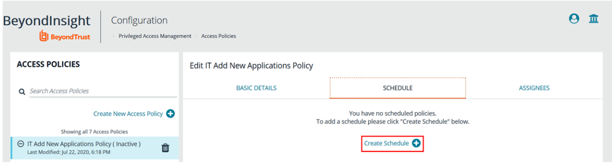


Access Policy Name
IT Add New Applications Policy

4. On the **Basic Details** tab:
   - Enter a description for the policy.
   - Enable the **Email Notifications** option to send emails when a request is received for the policy.
   - Enter an email address, and then click **Add**.

> ***Note:*** *Multiple addresses cannot be added at once. Each email address must be added one at time.*

5. Select the **Schedule** tab, and then click **Create Schedule**.


BeyondInsight
BeyondTrust
Configuration
Privileged Access Management
Access Policies
ACCESS POLICIES
Search Access Policies
Create New Access Policy
Showing all 7 Access Policies
IT Add New Applications Policy (Inactive)
Last Modified: Jul 22, 2020, 6:18 PM
Edit IT Add New Applications Policy
BASIC DETAILS
SCHEDULE
ASSIGNEES
Create Schedule

You have no scheduled policies.
To add a schedule please click "Create Schedule" below.

6. Configure the following scheduling parameters:
    - **Time Range:** Select the time of day when the policy can be accessed.
    - **Date Range:** Select a data range.
    - **Recurrence:** Select the frequency that the access is available. If you select **Daily**, and then select **Every Day**, you can optionally select **Allows multi-day check-outs of accounts**. This option allows the user continuous access to a granted request over a span of days.
7. Select the **Enable Location Restrictions** option if applicable, 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.

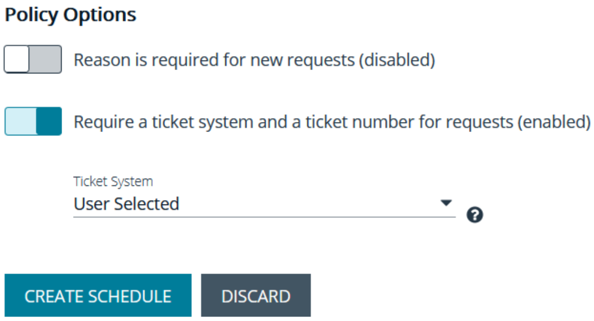
> ***Note:*** *In the case of a new configuration, this error message can be found in the log:*
>
> ```
> CheckLocationAllowed: XForwardedForHeaderValue 1.1.1.1 is not registered/trusted.  Add
> this XForwardedForHeaderValue to the TestGroupName Address group
> ```

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. ***Note:*** *If the session has been terminated by an Active Sessions reviewer, the logoff on disconnect occurs regardless of the access policy setting.*
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	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. 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: • Remote Desktop Services client access licensing • Time zone redirection • Remote Desktop Connection Broker redirection • Remote Desktop Easy Print
Connection Profile	Select a profile from the list or click **Manage Connection Profiles** to be taken to the **Connection Profiles** page to create a new profile.

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.



Policy Options

Reason is required for new requests (disabled)

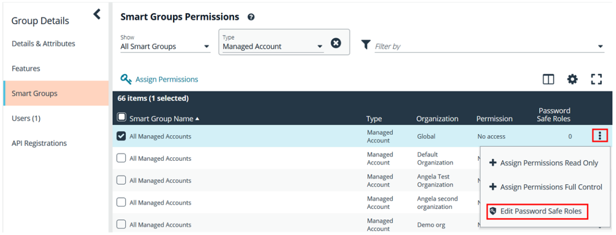
Require a ticket system and a ticket number for requests (enabled)

Ticket System: User Selected

12. Click **Create Schedule**. If the Access Policy is not yet marked as available, you are prompted to activate it now.
13. Click **Save Access Policy**.

The access policy can now be assigned to a group as follows:

1. Select the **Assignees** tab for your newly created access policy.
2. Click **Manage Assignees**. You are taken to the **User Management** page.
3. Select the **More Options** icon for a group, and then select **View Group Details**.
4. Under **Group Details**, select **Smart Groups**.
5. Select the **More Options** icon for a smart group, and then select **Edit Password Safe Roles**.



Smart Groups Permissions

Show: All Smart Groups

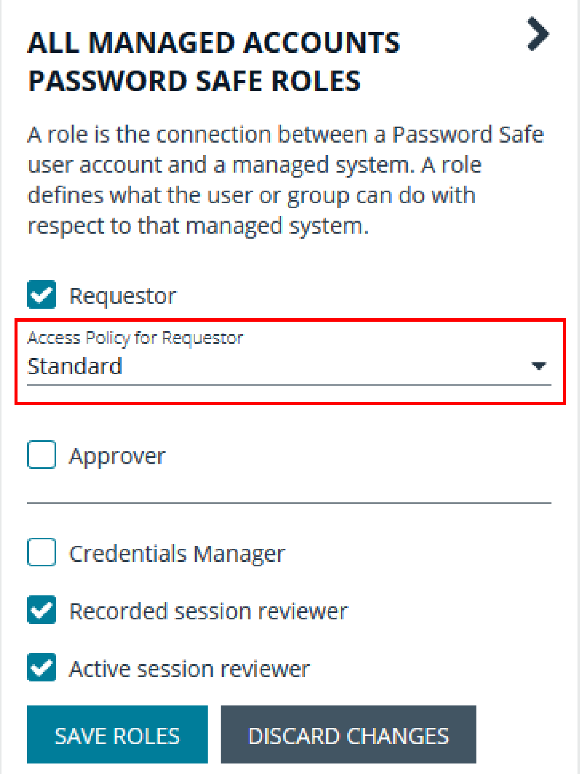
Type: Managed Account

Filter by

66 items (1 selected)

	Smart Group Name ▲	Type	Organization	Permission	Password Safe Roles
☑	All Managed Accounts	Managed Account	Global	No access	0
□	All Managed Accounts	Managed Account	Default Organization	N	
□	All Managed Accounts	Managed Account	Angela Test Organization	N	
□	All Managed Accounts	Managed Account	Angela second organization	N	
□	All Managed Accounts	Managed Account	Demo org	N	

6. Select the access policy from the **Access Policy for Requestor** dropdown.
7. Click **Save Roles**. The group is now listed as an assignee on the **Assignees** tab.



ALL MANAGED ACCOUNTS 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: Standard

□ Approver

□ Credentials Manager

☑ Recorded session reviewer

☑ Active session reviewer

For more information, please see the following:

- *"Configure Keystroke Logging" on page 134*
- *"Enhanced Session Auditing" on page 134*
- *For configuring release durations, "Add a Managed System Manually" on page 13*
- *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 63*

Create a Connection Profile

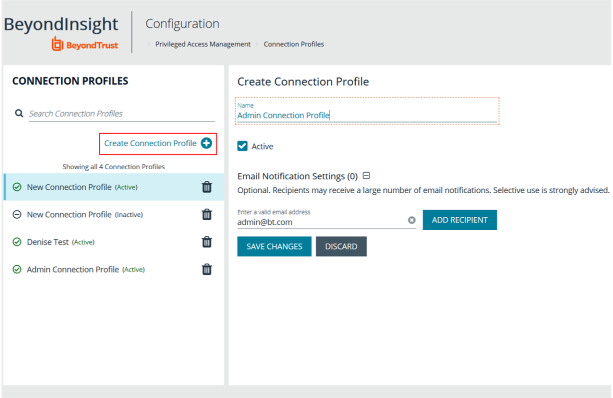
Connection profiles allow administrators to create a deny list of keywords, host names, and IP addresses. Each deny listed item can be given a separate action which is triggered when requesters type a deny listed item in an active SSH session.

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

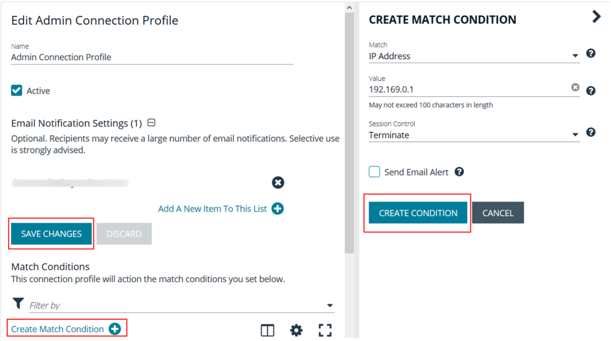
- **No Action:** Select to be alerted only if a match occurs.
- **Block:** Blocks the transmission of the command to the remote machine.
- **Lock:** Locks the session for the requester.
- **Block and Lock:** Performs both a block and lock as described above.
- **Terminate:** Ends the remote session.

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

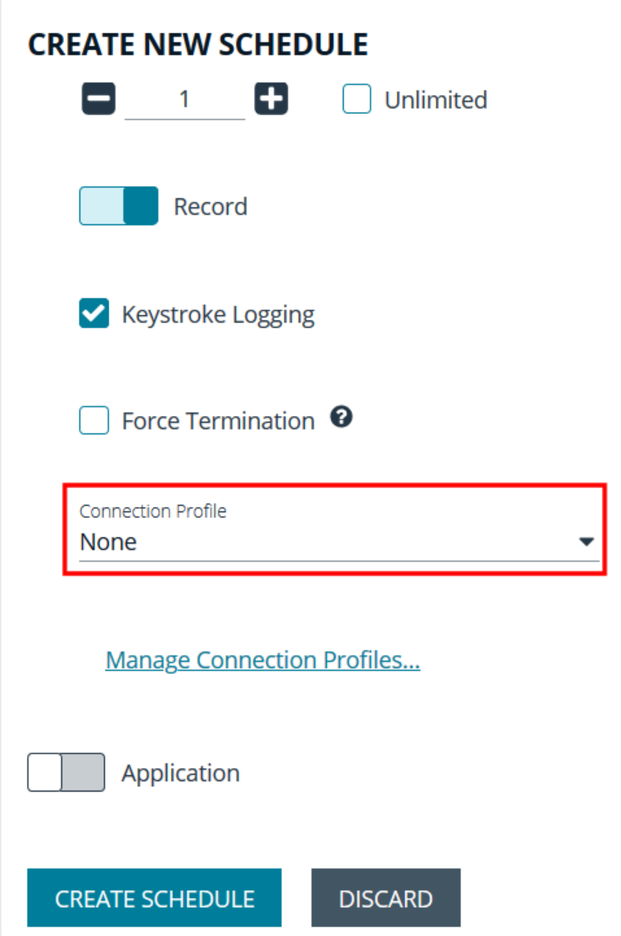
1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management Policies > Connection Profiles**.
2. In the **Connection Profiles** pane, click **Create Connection Profile**.
3. In the **Create Connection Profile** pane:
   - Enter a name for the profile.
   - Under **Email Notification Settings**, enter an email address and then click **Add Recipient** to send email notifications when a deny listed item is triggered.
4. Click **Save Changes**.


BeyondInsight
BeyondTrust
Configuration
Privileged Access Management
Connection Profiles
CONNECTION PROFILES
Search Connection Profiles
Create Connection Profile
Showing all 4 Connection Profiles
New Connection Profile (Active)
New Connection Profile (Inactive)
Denise Test (Active)
Admin Connection Profile (Active)
Create Connection Profile
Name
Admin Connection Profile
Active
Email Notification Settings (0)
Optional. Recipients may receive a large number of email notifications. Selective use is strongly advised.
Enter a valid email address
admin@bt.com
ADD RECIPIENT
SAVE CHANGES
DISCARD

5. Click **Create Match Condition**.
6. To add a deny listed item, select one of the following from the **Match** dropdown: **Keyword**, **Hostname**, or **IP Address**.
7. Enter the match criteria in the **Value** box.
8. From the **Session Control** dropdown, select the action to take when the deny listed item is triggered.
9. Click **Create Condition**. Each deny listed item is displayed on a separate line.
10. Click **Save Changes**.


Edit Admin Connection Profile
Name
Admin Connection Profile
Active
Email Notification Settings (1)
Optional. Recipients may receive a large number of email notifications. Selective use is strongly advised.
Add A New Item To This List
SAVE CHANGES
DISCARD
Match Conditions
This connection profile will action the match conditions you set below.
Filter by
Create Match Condition
CREATE MATCH CONDITION
Match
IP Address
Value
192.169.0.1
May not exceed 100 characters in length
Session Control
Terminate
Send Email Alert
CREATE CONDITION
CANCEL

11. After you save the connection profile, it must be applied on the access policy schedule. Select the access policy, and then double-click the blue shaded area of the scheduling grid. Select the connection profile from the menu.



CREATE NEW SCHEDULE

Use a Predefined Connection Profile

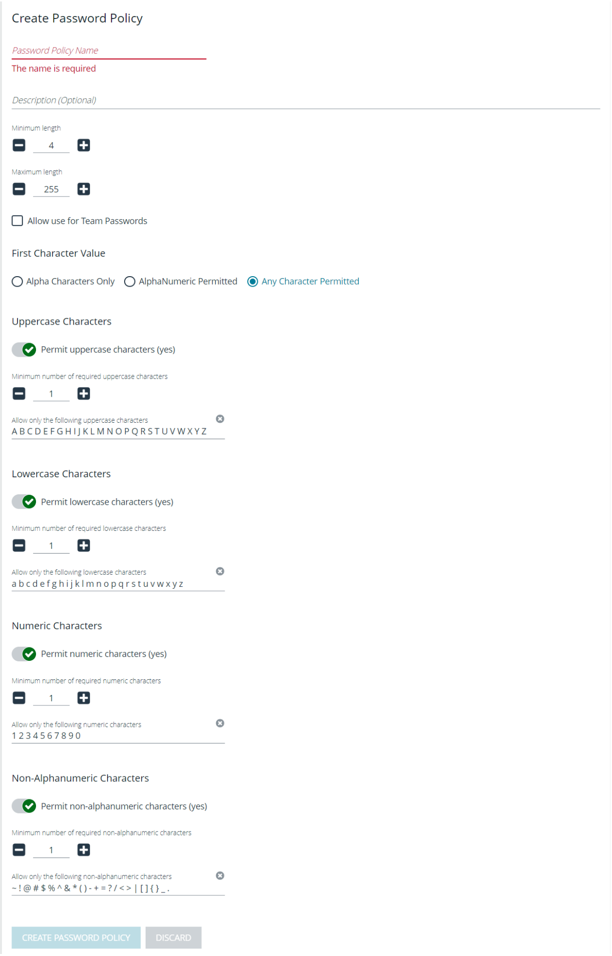
The following predefined connection profiles are available for an access policy: **Lateral Movement** and **Suspicious Activity**.

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.



Create Password Policy

Password Policy Name
The name is required

Description (Optional)

Minimum length
4

Maximum length
255

□ Allow use for Team Passwords

First Character Value

○ Alpha Characters Only ○ AlphaNumeric Permitted ● Any Character Permitted

Uppercase Characters

✓ Permit uppercase characters (yes)

Minimum number of required uppercase characters
1

Allow only the following uppercase characters
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Lowercase Characters

✓ Permit lowercase characters (yes)

Minimum number of required lowercase characters
1

Allow only the following lowercase characters
a b c d e f g h i j k l m n o p q r s t u v w x y z

Numeric Characters

✓ Permit numeric characters (yes)

Minimum number of required numeric characters
1

Allow only the following numeric characters
1 2 3 4 5 6 7 8 9 0

Non-Alphanumeric Characters

✓ Permit non-alphanumeric characters (yes)

Minimum number of required non-alphanumeric characters
1

Allow only the following non-alphanumeric characters
~ ! @ # $ % ^ & * ( ) - + = ? / < > | [ ] { } _ .

> ***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. In the BeyondInsight Console, go to **Configuration > Privileged Access Management Policies > Password Policies**.
2. Click **Create Password Policy**.
3. Enter a **Password Policy Name** and **Description**.
4. Set the following parameters for your policy:
    - **Minimum and Maximum Characters:** 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.
    - Check **Allow use for Team Passwords** 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.
    - Select the **First Character Value**.
    - **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.
    - Enter permissible characters in the **Allow only the following non-alphanumeric characters** field.

5. Click **Create Password Policy** when done.

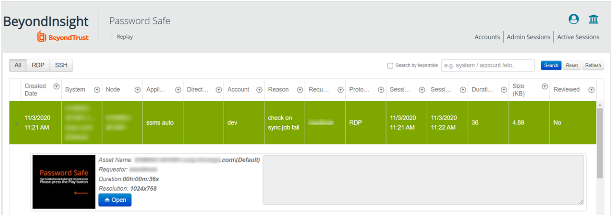
Manage Recorded Sessions

View Recorded 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

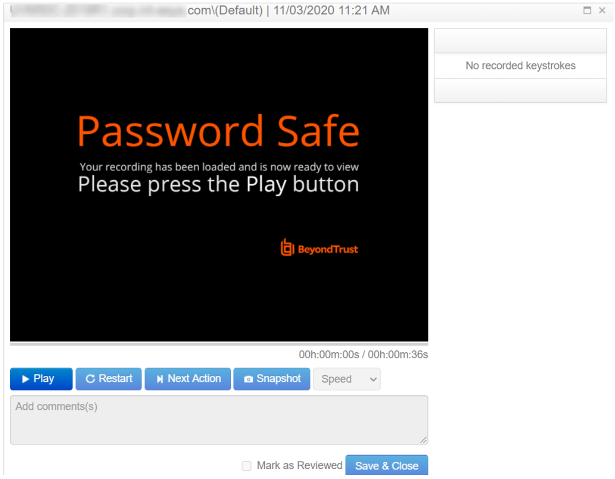
1. From the left navigation, click **Menu**, and then click **Replay** under **Password Safe**.
2. Click **All**, **RDP**, or **SSH** to find the recording.
3. Select a recorded session.
4. A thumbnail is displayed with session details. Click **Open**.



Created Date	System	Node	Appli...	Direct...	Account	Reason	Requ...	Proto...	Sessi...	Sessi...	Durati...	Size (KB)	Reviewed
11/3/2020 11:21 AM	[redacted]	[redacted]	ssms auto		dev	check on sync job fail	[redacted]	RDP	11/3/2020 11:21 AM	11/3/2020 11:22 AM	36	4.89	No

Asset Name: [redacted]*.com\(Default)*
Requestor: [redacted]
*Duration:**00h:00m:36s***
Resolution: ***1024x768***

5. 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.
6. Check **Mark as Reviewed** for easy tracking of reviewed sessions.
7. Add comments as needed, and then click **Save & Close**. The comments are displayed with the session thumbnail.


[redacted].com\(Default) | 11/03/2020 11:21 AM

No recorded keystrokes

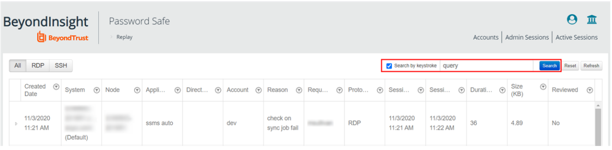
Password Safe
Your recording has been loaded and is now ready to view
Please press the Play button

00h:00m:00s / 00h:00m:36s

Use Keystroke Search

To find sessions containing keystrokes:

1. Check **Search by keystrokes** , and then enter a word or phrase in the field provided.
2. Click **Search**. If the word or phrase was logged, the sessions containing those keystrokes are displayed.



Created Date	System	Node	Appli...	Direct...	Account	Reason	Requ...	Proto...	Sessi...	Sessi...	Durati...	Size (KB)	Reviewed
11/3/2020 11:21 AM	[redacted] (Default)	[redacted]	ssms auto		dev	check on sync job fail	[redacted]	RDP	11/3/2020 11:21 AM	11/3/2020 11:22 AM	36	4.89	No

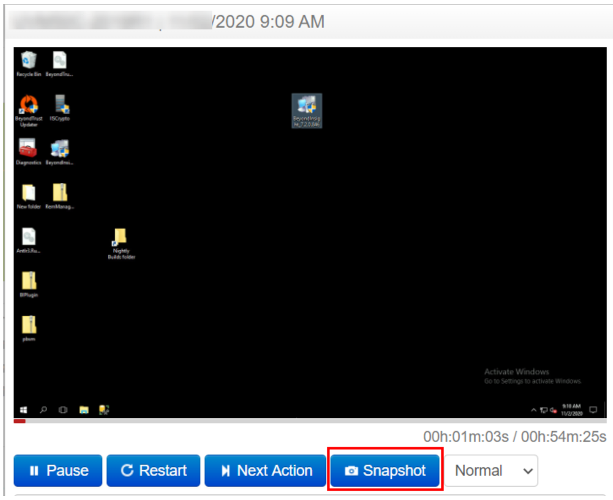
Export a Session Frame

You can select a screenshot from a recorded session and export to a JPEG file. The file exports to a resolution of 1024 × 768. This feature is available only for recorded RDP and SSH sessions. Snapshots can be taken while the recording is paused or in play mode.

Click the **Snapshot** button.

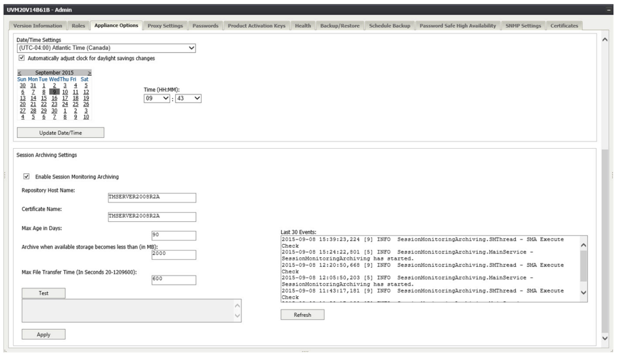
The JPEG file is automatically saved to your default download location specified in your browser settings.

A notification is displayed when the export is complete.



Archive Recorded Sessions

You can archive recorded sessions. Archive settings are configured on the U-Series Appliance.



Date/Time Settings: (UTC-04:00) Atlantic Time (Canada)

☑ Automatically adjust clock for daylight savings changes

Time (HH:MM): 09 : 43

Session Archiving Settings

☑ Enable Session Monitoring Archiving

Repository Host Name: TMSERVER2008R2A

Certificate Name: TMSERVER2008R2A

Max Age in Days: 90

Archive when available storage becomes less than (in MB): 2000

Max File Transfer Time (In Seconds 20-1209600): 600

Last 30 Events:

```
2015-09-08 15:39:23,224 [9] INFO  SessionMonitoringArchiving.SMThread - SMA Execute
Check
2015-09-08 15:24:22,801 [5] INFO  SessionMonitoringArchiving.MainService -
SessionMonitoringArchiving has started.
2015-09-08 12:20:50,668 [9] INFO  SessionMonitoringArchiving.SMThread - SMA Execute
Check
2015-09-08 12:05:50,203 [5] INFO  SessionMonitoringArchiving.MainService -
SessionMonitoringArchiving has started.
2015-09-08 11:43:17,181 [9] INFO  SessionMonitoringArchiving.SMThread - SMA Execute
Check
```

Note: *Parameters can be configured to allow auto-archiving of any recorded sessions older than a specific number of days.*

For more information, refer to the U-Series Appliance User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/administration/index.htm.

View and Restore Archived Sessions

Once a session has been recorded, you can retrieve it from the **Replay Sessions** window.

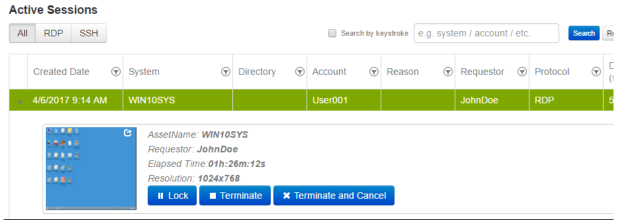
1. Open the session by clicking **Open**.
2. Once the viewer opens, click **Archive Session**.
3. Select the archived session.
4. Click **Restore Session** to restore the session.

Manage Active Sessions

View Active Sessions

You can view a session in real time. Administrators, ISA users, or users that have been granted permissions to the asset through a Smart Rule that has the **Active Session Reviewer** role, can view **Active Sessions** in real time.

1. Log in to the web portal.
2. Click **Menu**, and then click **Active Sessions**.
3. Select a session.
4. Click the thumbnail to open the session in a larger window.



Active Sessions

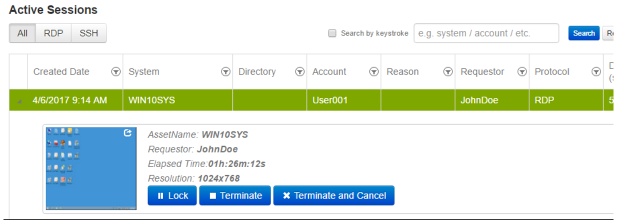
	Created Date	System	Directory	Account	Reason	Requestor	Protocol
	4/6/2017 9:14 AM	WIN10SYS		User001		JohnDoe	RDP

AssetName: ***WIN10SYS***
Requestor: ***JohnDoe***
*Elapsed Time:**01h:26m:12s***
Resolution: ***1024x768***

Lock an Active Session

1. Log in to the web portal.
2. Click **Menu**, and then select **Active Sessions**.
3. Select a session.
4. Click the **Lock** button to lock the user session, preventing further interaction with their session.

   The message displayed to the user is different for RDP and SSH sessions. See the output below.

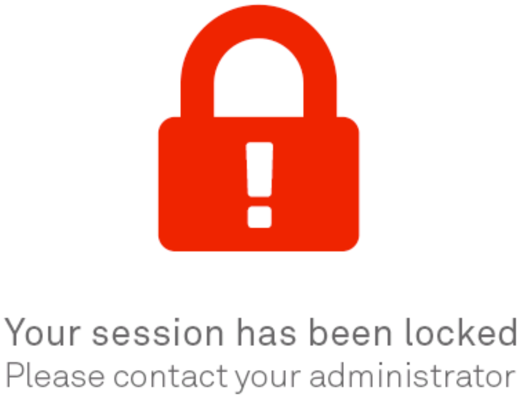


Active Sessions

	Created Date	System	Directory	Account	Reason	Requestor	Protocol
	4/6/2017 9:14 AM	WIN10SYS		User001		JohnDoe	RDP

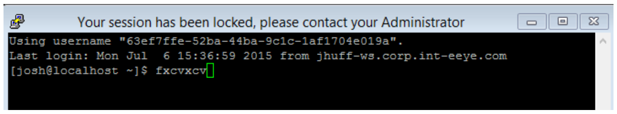
AssetName: ***WIN10SYS***
Requestor: ***JohnDoe***
*Elapsed Time:**01h:26m:12s***
Resolution: ***1024x768***

RDP Message: *Your session has been locked. Please contact your administrator.*



Your session has been locked
Please contact your administrator

SSH Message: *Your session has been locked, please contact your Administrator.*



Your session has been locked, please contact your Administrator

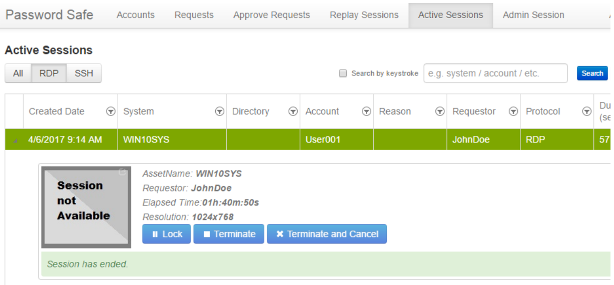
```
Using username "63ef7ffe-52ba-44ba-9c1c-1af1704e019a".
Last login: Mon Jul  6 15:36:59 2015 from jhuff-ws.corp.int-eeye.com
[josh@localhost ~]$ fxcvxcv
```

5. Click the **Unlock** button to unlock the session.

> ***Tip:*** *Alternatively, a session can be locked and unlocked when viewing the session in the session player window, by clicking the* ***Lock*** *and* ***Unlock*** *buttons.*

Terminate an Active Session

1. Log in to the web portal.
2. Click **Menu**, and then select **Active Sessions**.
3. Select a session.
4. Click the **Terminate** button to immediately end a session.



Created Date	System	Directory	Account	Reason	Requestor	Protocol	Du (se
4/6/2017 9:14 AM	WIN10SYS		User001		JohnDoe	RDP	57

AssetName: **WIN10SYS**
Requestor: **JohnDoe**
Elapsed Time:**01h:40m:50s**
Resolution: **1024x768**

Session has ended.

> ***Tip:*** *Alternatively, a session can be terminated when viewing the session in the session player window, by clicking the* ***Terminate*** *button.*

> ***Note:*** *When terminating a session, it automatically closes and is removed from the* ***Active Sessions*** *table. The session is then available to view in* ***Replay Sessions****.*

Terminate and Cancel an Active Session

1. Log in to the web portal.
2. Click **Menu**, and then select **Active Sessions**.
3. Click the **Terminate and Cancel** button to immediately end a session and check in the request.

Alternatively, a session can be terminated and canceled when viewing the session in the session player window, by clicking the **Terminate and Cancel** button. The **Terminate and Cancel** button is only present for sessions initiated by regular users. It is not avaialble for sessions initiated by administrators or ISA users. It is also not available in Admin Sessions.

View Keystrokes in Active Sessions

Keystrokes are logged and viewable during active sessions as they are executed. Administrators can sort these keystrokes as they populate by selecting the **Oldest to Newest** or **Newest to Oldest** sorting options within the **Keystroke** menu.

> ***Note:*** *Logged keystrokes* ***cannot*** *be selected during active sessions.*

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 13.*

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.*

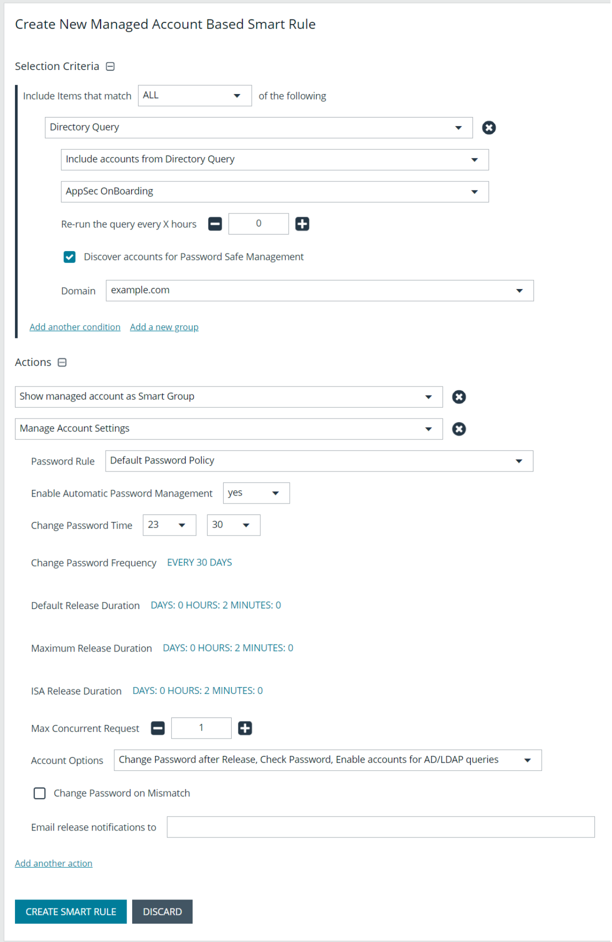
For more information on adding managed accounts manually, please see "Add a Managed System Manually" on page 13.

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 to create the query in real time.
   - 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.*



Create New Managed Account Based Smart Rule

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

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 Release Duration: DAYS: 0 HOURS: 2 MINUTES: 0

Max Concurrent Request: 1

Account Options: Change Password after Release, Check Password, Enable accounts for AD/LDAP queries

☐ Change Password on Mismatch

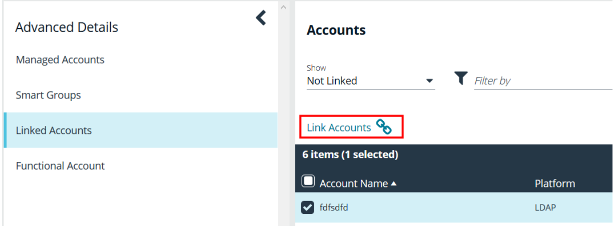
Email release notifications to

8. Click **Create Smart Rule**.
9. To view the Active Directory accounts, go the **Managed Accounts** page, and then 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.



Show: Not Linked

6 items (1 selected)

☐ Account Name ▲	Platform
☑ fdfsdfd	LDAP

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.

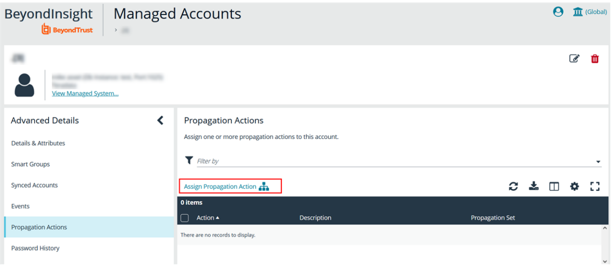
> ***Note:*** *If a failure occurs when connecting to a target domain controller, Password Safe connects at the domain level.*

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.

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



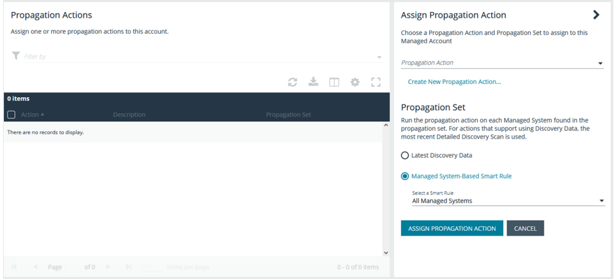
Assign one or more propagation actions to this account.

0 items

☐ Action ▲	Description	Propagation Set
There are no records to display.		

5. 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 76 for more information.*



Assign one or more propagation actions to this account.

0 items

☐ Action ▲	Description	Propagation Set
There are no records to display.		

Choose a Propagation Action and Propagation Set to assign to this Managed Account

Run the propagation action on each Managed System found in the propagation set. For actions that support using Discovery Data, the most recent Detailed Discovery Scan is used.

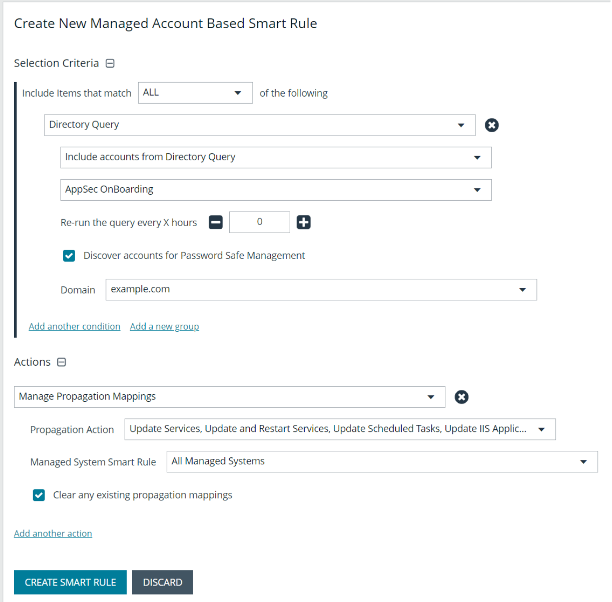
○ Latest Discovery Data

● Managed System-Based Smart Rule

Select a Smart Rule: All Managed Systems

6. 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.



Create New Managed Account Based Smart Rule

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

Actions ⊟

Manage Propagation Mappings

Propagation Action: Update Services, Update and Restart Services, Update Scheduled Tasks, Update IIS Applic...

Managed System Smart Rule: All Managed Systems

☑ Clear any existing propagation mappings

Available built-in Propagation Actions

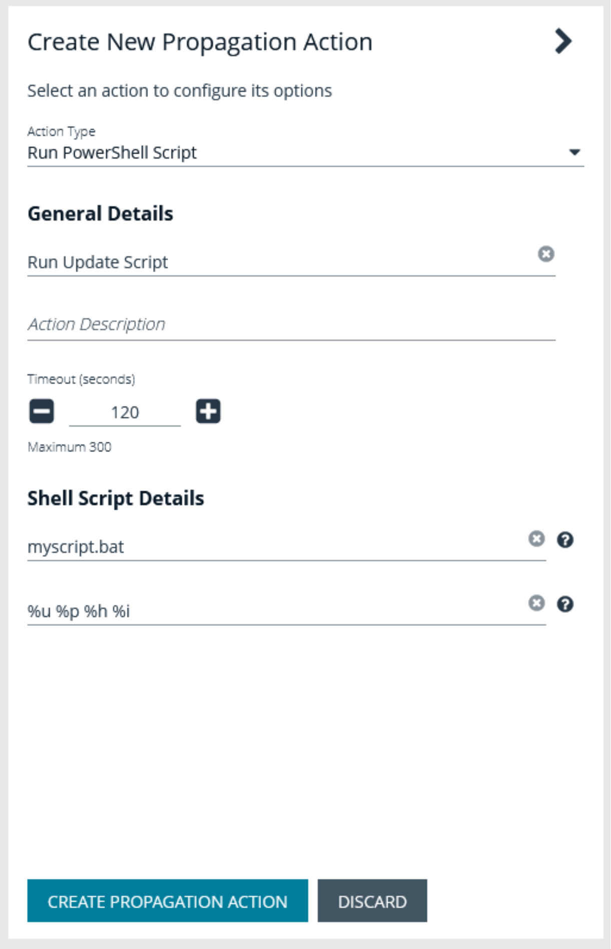
- Update Services
- Update and Restart Services
- Update Scheduled Tasks
- Update IIS Application Pools
- Update and Restart IIS Application Pools
- Update Windows Auto Logon
- Update COM+ Applications
- Update DCOM Applications
- Update SCOM RunAs Identities

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
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

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 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. 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.
RDP session default port	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 **30** 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.
Enable smart sizing	Enable to resize the RDP window to match the size of the user's screen.
Allow users to select a remote proxy	Enable 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 enabled, 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 turned off by default. This is an advanced feature. Please contact BeyondTrust Technical Support for assistance with using this feature.
Hide record checkbox for ISA sessions	Enable if you do not want the **Record Session** check box to be available on requests.

For more information, please see "Configure Session Monitoring" on page 130.

Requests

Setting	Description / Action
Require a ticket system and ticket number for 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 requests	Enable this option on all requests.

Auto-select access policy for OneClick	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 in **OneClick**.
Bypass SSH Landing Page for OneClick	Enable to save time for users when connecting using **OneClick**.
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 **OneClick**.
Domain Account Concurrency Behavior	This setting defines how the **Concurrent** setting in an access policy applies the checkout concurrency for a domain account. When **Account** is selected, Password Safe applies the checkout concurrency to how many concurrent sessions a domain account may have per environment. 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.
Password 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 147.

Session Monitoring

For information on Session Monitoring options, please see "Configure Session Monitoring" on page 130.

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. ***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**.*
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.

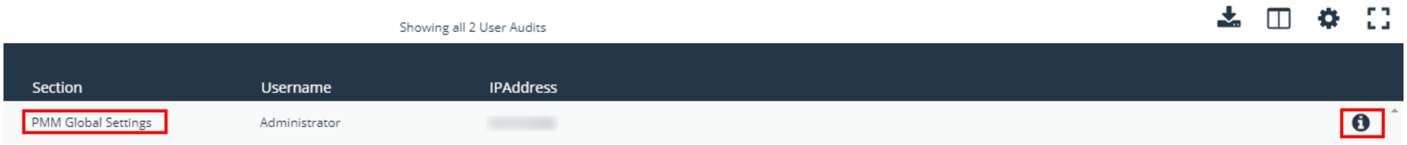
Retention period for password change log	Set the number of days to store password change logs. The default is **90** days. The range is **30 - 365** days.
Retention period for password test results	Set the number of days to store success and failure results for automated password tests. The default is **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 connect 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.

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	[redacted]

> ***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 133.*

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

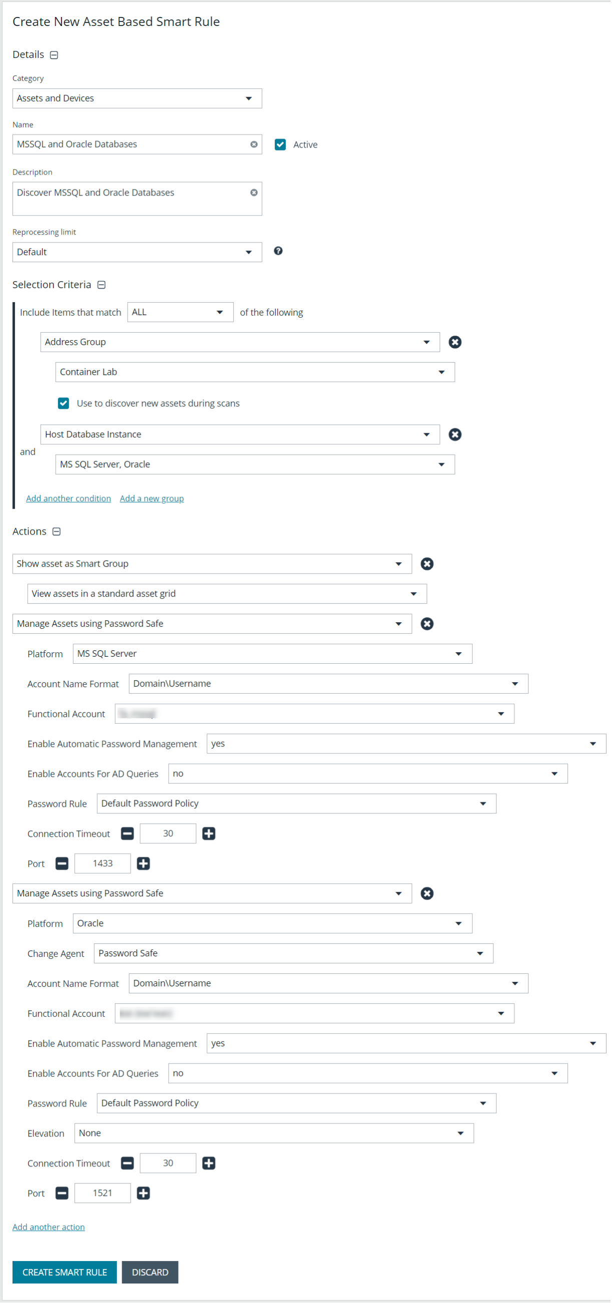
The following scan types include database instance data in the scan results:

- **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. Select **Configuration > General > 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**.



Create New Asset Based Smart Rule

Details ⊟

Category: Assets and Devices

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

Container Lab

☑ Use to discover new assets during scans

and

Host Database Instance

MS SQL Server, Oracle

Add another condition Add a new group

Actions ⊟

Show asset as Smart Group

View assets in a standard asset grid

Manage Assets using Password Safe

Platform: MS SQL Server

Account Name Format: Domain\Username

Functional Account: [redacted]

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: [redacted]

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

> ***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.*

Manually Add Database Instances

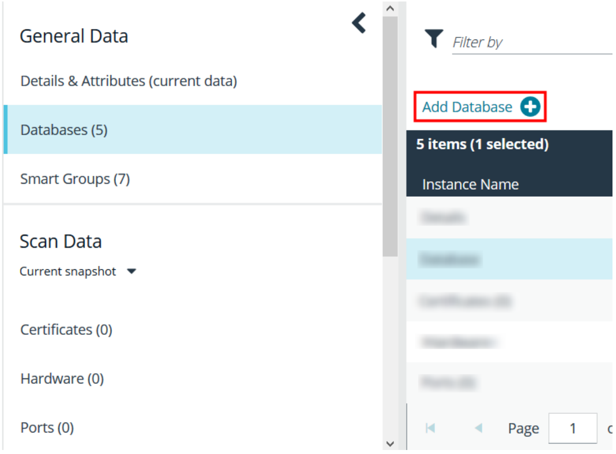
You can manually add the following database instance types. When selecting the database platform, ensure the correct port number is displayed.

- Mongo: **27017**
- SQL Server: **1433**

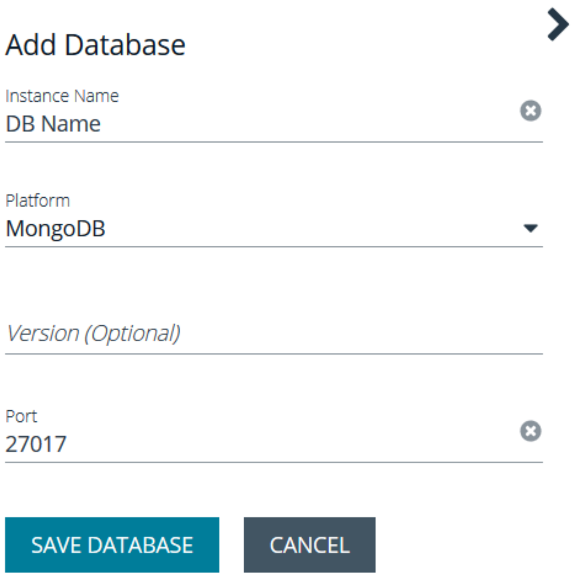
- MySQL: **3306**
- Oracle: **1521**
- PostgreSQL: **5432**
- Sybase ASE: **5000**
- Teradata: **1025**

Manually Add Databases to Assets Managed by Password Safe

1. From the menu, select **Assets**.
2. Select the desired asset, and then click the **More Option** button, and select **Go to advanced details**.
3. Under **General Data**, select **Databases**.
4. Click **Add Databases**.



5. Provide a name, select the platform, add a version, leave the default port, and then click **Save Database**.



Add Database

Instance Name: DB Name

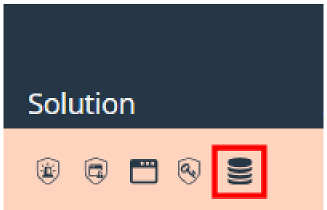
Platform: MongoDB

Version (Optional)

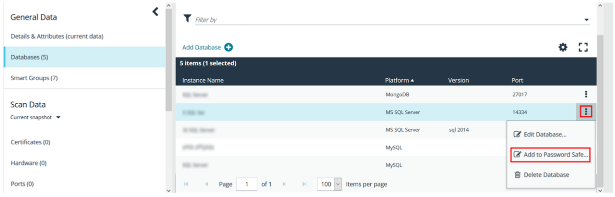
Port: 27017

Manually Add Databases to Password Safe Management

1. From the menu, select **Assets**.
2. Assets that host database instances are indicated by a **Database Host** icon in the **Solution** column.



3. Select the desired asset, click the **More Option** button, and then select **Go to advanced details**.
4. Under **General Data**, select **Databases**.
5. For the desired instance, click the **More Options** icon, and then select **Add to Password Safe**.
6. Select the functional account and other desired settings, and then click **Create Managed System**.



5 items (1 selected)

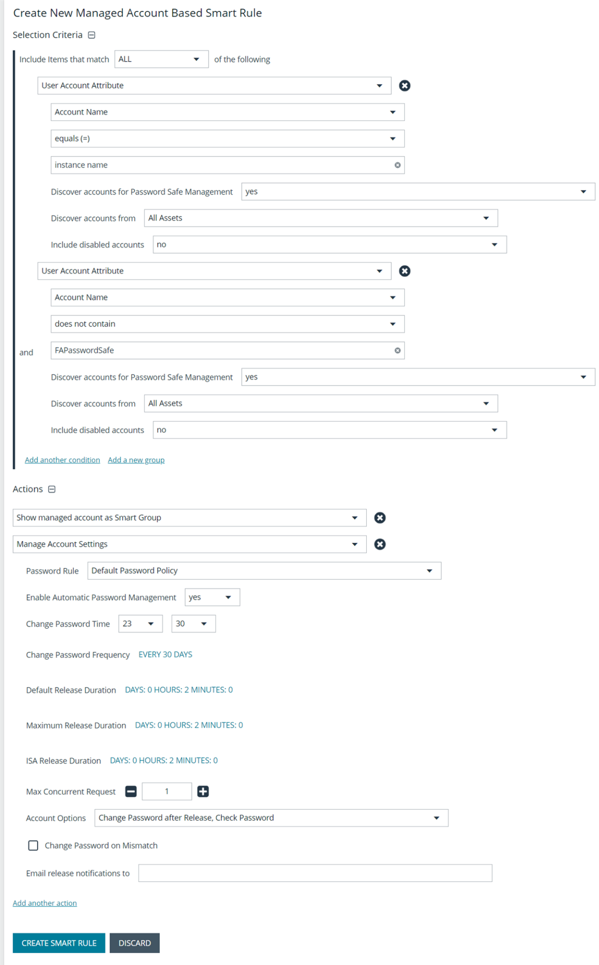
Instance Name	Platform ▲	Version	Port
[redacted]	MongoDB		27017
[redacted]	MS SQL Server		14334
[redacted]	MS SQL Server	sql 2014	
[redacted]	MySQL		
[redacted]	MySQL		

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.

1. From the menu, select **Smart Rules**.
2. Click **Create Smart Rule**.
3. Select **Managed Accounts** from the **Category** dropdown.
4. Provide a meaningful **Name** and **Description** for the Smart Rule.

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

and

User Account Attribute
Account Name
does not contain
FAPasswordSafe
Discover accounts for Password Safe Management: yes
Discover accounts from: All Assets
Include disabled accounts: no

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 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:

> ***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.*

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:

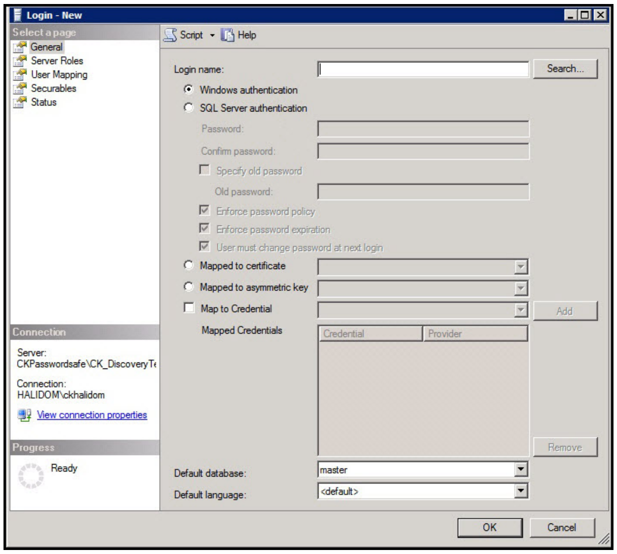
The following code samples show you how to apply the required permissions to the functional account.

```
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**.



Login name:

● Windows authentication

○ SQL Server authentication

Password:

Confirm password:

□ Specify old password

Old password:

☑ Enforce password policy

☑ Enforce password expiration

☑ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Credential	Provider

Default database: master

Default language: <default>

Connection

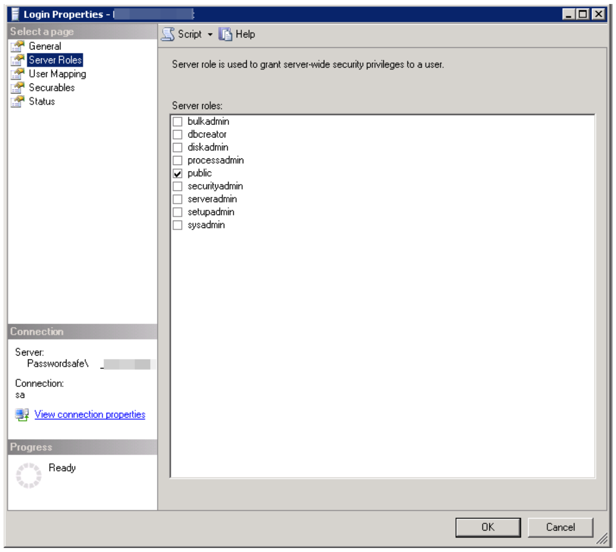
Server:
CKPasswordsafe\CK_DiscoveryTe

Connection:
HALIDOM\ckhalidom

Progress

Ready

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



Login Properties - [redacted]

Server role is used to grant server-wide security privileges to a user.

Server roles:

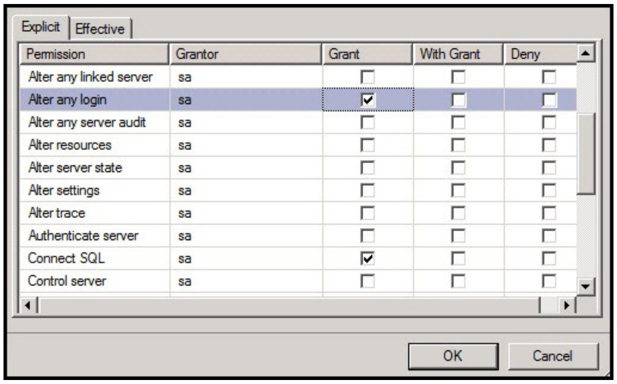
- ☐ bulkadmin
- ☐ dbcreator
- ☐ diskadmin
- ☐ processadmin
- ☑ public
- ☐ securityadmin
- ☐ serveradmin
- ☐ setupadmin
- ☐ sysadmin

Connection

Server:
Passwordsafe\ [redacted]

Connection:
sa

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**.



Permission	Grantor	Grant	With Grant	Deny
Alter any linked server	sa	☐	☐	☐
Alter any login	sa	☑	☐	☐
Alter any server audit	sa	☐	☐	☐
Alter resources	sa	☐	☐	☐
Alter server state	sa	☐	☐	☐
Alter settings	sa	☐	☐	☐
Alter trace	sa	☐	☐	☐
Authenticate server	sa	☐	☐	☐
Connect SQL	sa	☑	☐	☐
Control server	sa	☐	☐	☐

SQL Server Instance Port Retrieval

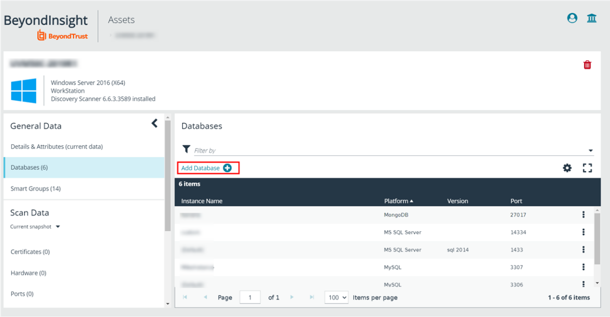
To configure a SQL Server database for Password Safe, you must retrieve the port number on the managed database instance using a query. The below query is required for database instances only. You do not need to provide a port number for the default instance.

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. Within BeyondInsight on the **Assets** page, find the asset where the SQL Server database is installed.
5. Within the asset's menu actions, select **Go to advanced details**.

6. Select the **Database** tab.
7. Click **Add Database**. Leave the default port or manually add the correct database port.
8. Click **Save Database**.



BeyondInsight | Assets > [redacted]

[redacted]

Windows Server 2016 (X64)
WorkStation
Discovery Scanner 6.6.3.3589 installed

General Data
- Details & Attributes (current data)
- Databases (6)
- Smart Groups (14)

Scan Data
- Current snapshot
- Certificates (0)
- Hardware (0)
- Ports (0)

Databases

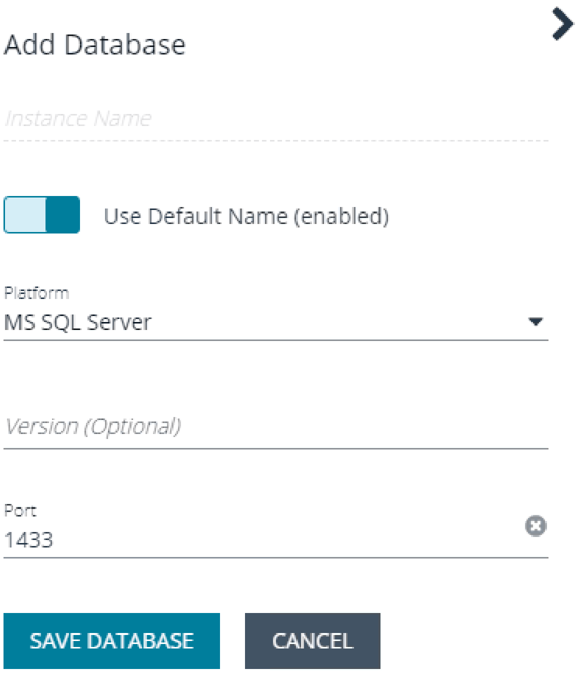
Filter by

Add Database

6 items

Instance Name	Platform	Version	Port
[redacted]	MongoDB		27017
[redacted]	MS SQL Server		14334
[redacted]	MS SQL Server	sql 2014	1433
[redacted]	MySQL		3307
[redacted]	MySQL		3306

Page 1 of 1 | 100 Items per page | 1 - 6 of 6 items



Add Database

Instance Name

Use Default Name (enabled)

Platform: MS SQL Server

Version (Optional)

Port: 1433

9. In the **Database** grid, select the newly created database from above.
10. From the **Database** menu actions, select **Add to Password Safe**.
11. Fill out the details required for the managed system.
12. Click the **Create Managed System** button.

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. Go to the **Assets** page.
3. Select the desired asset, click the **More Option** button, and then select **Go to advanced details**.
4. Under **General Data**, select **Databases**.
5. For the desired instance, click the **More Options** icon, 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.*

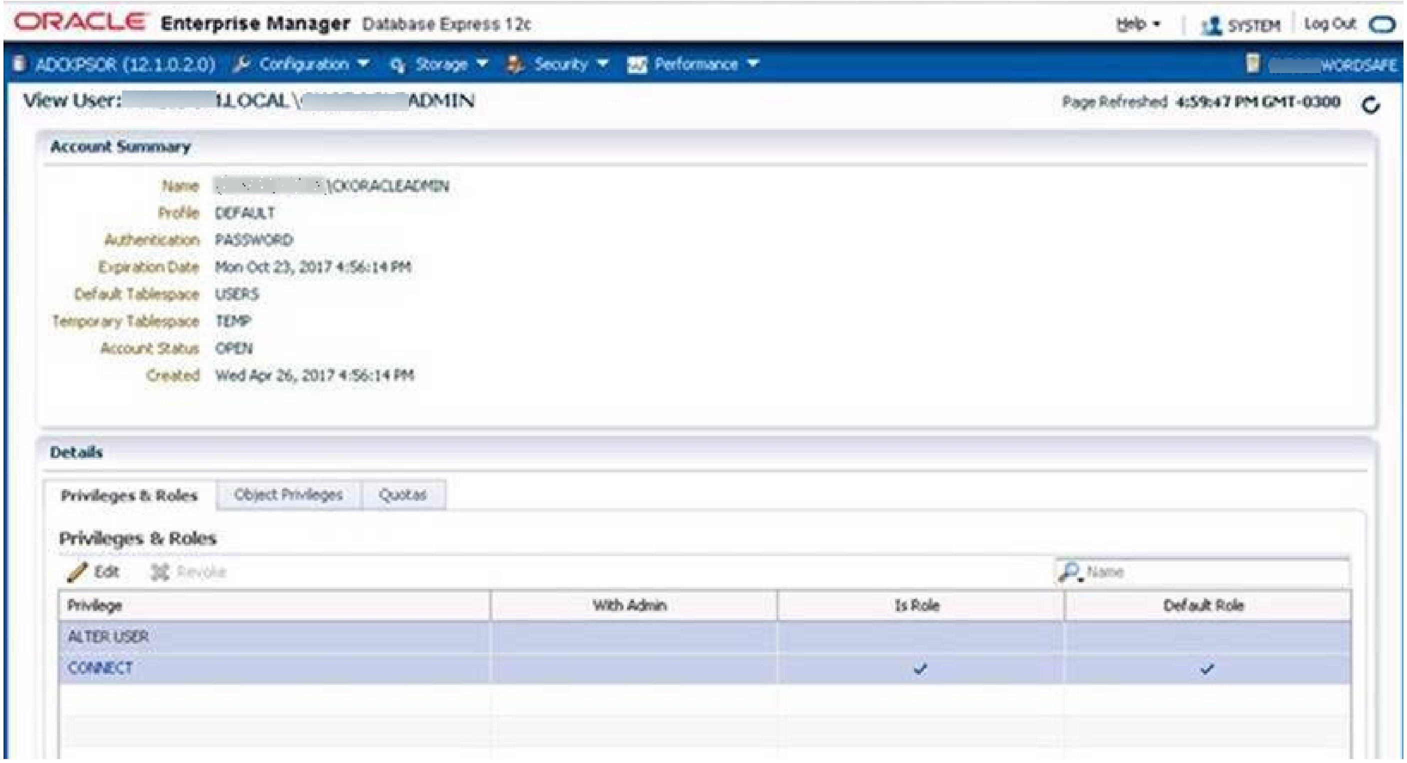
> *For more information, please see "Create a Functional Account" on page 12.*

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.)



View User: [redacted]1LOCAL\[redacted]ADMIN

Page Refreshed 4:59:47 PM GMT-0300

Account Summary

Name [redacted]\CKORACLEADMIN
Profile DEFAULT
Authentication PASSWORD
Expiration Date Mon Oct 23, 2017 4:56:14 PM
Default Tablespace USERS
Temporary Tablespace TEMP
Account Status OPEN
Created Wed Apr 26, 2017 4:56:14 PM

Details

Privileges & Roles

Privilege	With Admin	Is Role	Default Role
ALTER USER			
CONNECT		✓	✓

Create the Functional Account in Oracle

To create a functional account in Oracle:

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

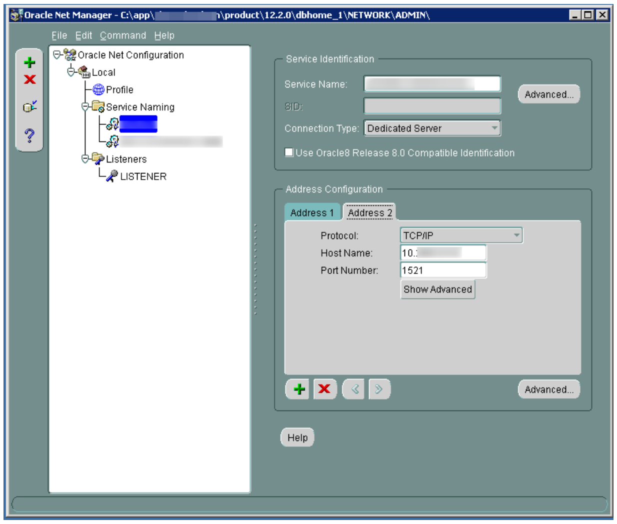
To grant permission to the functional account to change passwords on a managed account:

```
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.



Service Name: [redacted]

SID:

Connection Type: Dedicated Server

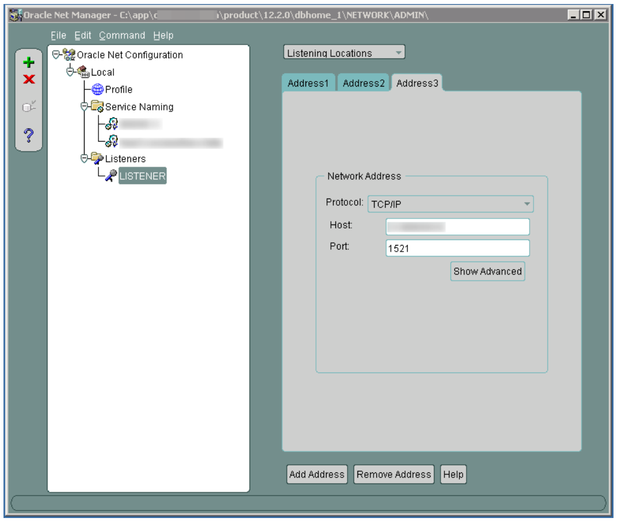
☐ Use Oracle8 Release 8.0 Compatible Identification

Protocol: TCP/IP

Host Name: 10.[redacted]

Port Number: 1521

- Also in Oracle Net Manager, set the service name as the host name IP address.



Listening Locations

Protocol: TCP/IP

Host: [redacted]

Port: 1521

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:

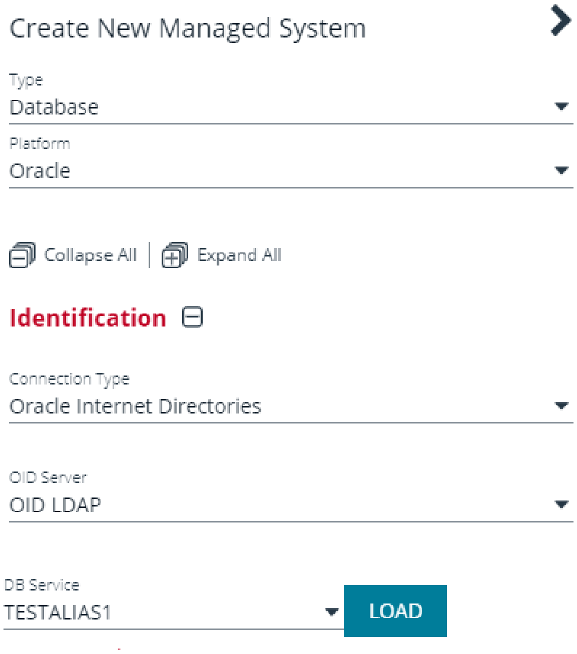
- On the **Integrity** tab, select:
  - **Server** from the **Integrity** menu
  - **required** from the **Checksum Level** menu
  - **SHA256** as the method
- On the **Encryption** tab, select:
  - **Server** from the **Encryption** menu
  - **required** from the **Encryption Type** menu
  - **AES256**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

Identification

Connection Type: Oracle Internet Directories

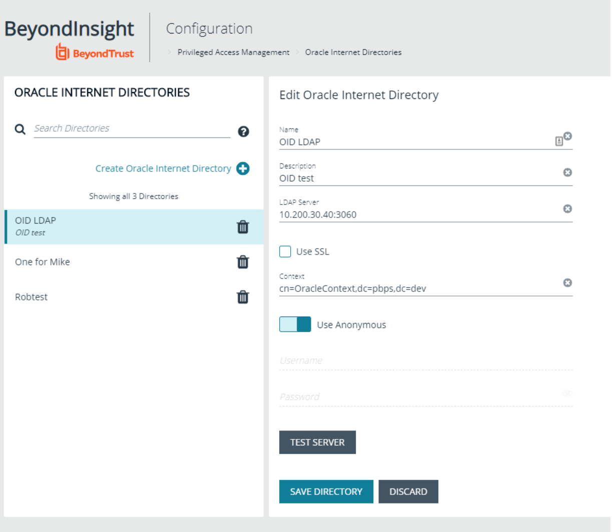
OID Server: OID LDAP

DB Service: TESTALIAS1

Configure an Oracle Internet Directory

To use this functionality, you need first to configure an OID.

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


BeyondInsight | Configuration
Privileged Access Management > Oracle Internet Directories

ORACLE INTERNET DIRECTORIES

Showing all 3 Directories

- OID LDAP — *OID test*
- One for Mike
- Robtest

Edit Oracle Internet Directory

Name: OID LDAP

Description: OID test

LDAP Server: 10.200.30.40:3060

☐ Use SSL

Context: cn=OracleContext,dc=pbps,dc=dev

Use Anonymous

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.

Application sessions can be recorded.

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 managed accounts. Assign the **Requester** role (or **Requester/Approver** role) that includes selecting the access policy.

Add an Application

Follow the steps below to add an application.

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 a **Functional Account** (optional) from the list to connect to the Password Safe managed system hosting the remote application.
8. Check the appropriate boxes to **Associate with linked systems**. Administrators can associate the application with a linked Windows system or a linked Linux or Unix system.
   - By default, the boxes are not checked, which is the most restrictive state. A standard user in Password Safe sees one row with an application to the same functional account and managed system.
   - 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 Linux and Unix systems.
   - If you associate the application with a linked Linux or Unix system, standard users see all Linux and 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.

> ***Note:*** *When configuring access to a Linux system, **sudo** can be used to configure authentication. The administrator can include a functional account, but this is not required.*

9. Select a **Managed System** from the list. 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.

> ***Note:*** *A **Managed System** is required if a **Functional Account** is selected.*

10. Enable **AutoIt Passthrough** to automatically pass the credentials for the application through an RDP virtual channel. Using **AutoIt 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.
11. 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.
12. Select **Active** to make the application available for remote sessions.
13. Click **Create Application**.

> *For more information, please see the following:*
>
> - *On using the **PS_Automate** Utility, "Use the PS_Automate Utility" on page 103*
> - *For the prerequisites for **AutoIt Passthrough**, "Use AutoIt Passthrough" on page 104*

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, select the managed account, and then click the **More Options** icon, and select **Edit Account**.
3. In the **Edit Managed Account** pane, scroll down to **Applications** and click **+** to expand the **Applications** section.
4. From the dropdown 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 13.

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: *The Application Access Policy applies 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 59.

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 **PS_Automate** utility allows you to automate the launch and authentication of various Windows GUI applications from Password Safe. You can use the utility to launch and authenticate to a web page or to a standard Windows GUI application.

The utility allows Password Safe to seamlessly pass vaulted credentials from Password Safe to a remote application using the pass through option (using token pass instead of credentials).

PS_Automate supports Incognito mode for Chrome, Firefox, and Microsoft Edge, with Microsoft Edge being the default browser when a browser name is not specified or supported.

The utility uses an INI file for all input and operational behavior. By using multiple INI files, the same utility can automate behavior to a wide range of authentication scenarios.

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.

> ***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 excepts 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 at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/integrations/ps-automate/command-line-arguments.htm.*

Use AutoIt Passthrough

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

- The application must be launched through an AutoIt script.
- The wrapper AutoIt 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 100.

AutoIt Script Details

The AutoIt example script uses the following functions:

- **pspassthru.dll**
- **ps_get_credentials**
- **DLLCall**: An AutoIt 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 AutoIt 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 AutoIt 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.

> ℹ *For more information on creating functional accounts, please see "Create a Functional Account" on page 12.*

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.

> ℹ *For more information on adding Managed Systems, please see "Add a Managed System Manually" on page 13.*

Configure API Registration

BeyondInsight provides a way to integrate part of the BeyondInsight and Password Safe functionality into your applications, using an API key. The **API Registrations** page is only available to Password Safe administrators.

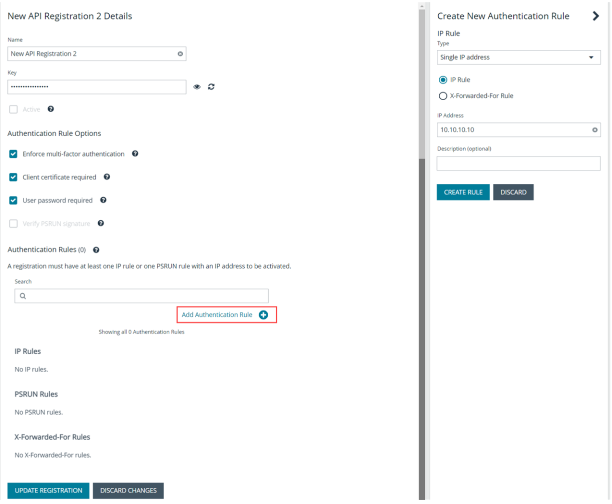
To create an API Registration:

1. In the BeyondInsight Console, navigate to **Configuration > General > API Registrations**.
2. Click **Create New API Registration**.
3. Enter a name for the new registration, and then click **Create API Regisration**.

   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.*

4. From the registration's **Details** pane, select the **Authentication Rule Options** you wish to enable and add an authentication rule:



New API Registration 2 Details

Name: New API Registration 2

Key: ················

☐ Active

Authentication Rule Options

☑ Enforce multi-factor authentication

☑ Client certificate required

☑ User password required

☐ Verify PSRUN signature

Authentication Rules (0)

A registration must have at least one IP rule or one PSRUN rule with an IP address to be activated.

Search

Add Authentication Rule

Showing all 0 Authentication Rules

IP Rules

No IP rules.

PSRUN Rules

No PSRUN rules.

X-Forwarded-For Rules

No X-Forwarded-For rules.

UPDATE REGISTRATION | DISCARD CHANGES

Create New Authentication Rule

IP Rule

Type: Single IP address

● IP Rule

○ X-Forwarded-For Rule

IP Address: 10.10.10.10

Description (optional):

CREATE RULE | DISCARD

   - **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.

- 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**.

5. Click **Update Registration**.

For more information, please see the following:

- *On API Registrations using the **Auth/SignAppIn API** function, the BeyondInsight and Password Safe API Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/api/authentication.htm*
- *On how to grant API access to BeyondInsight users, "Configure Role Based Access" on page 46*

Add a Custom Platform or Application Platform

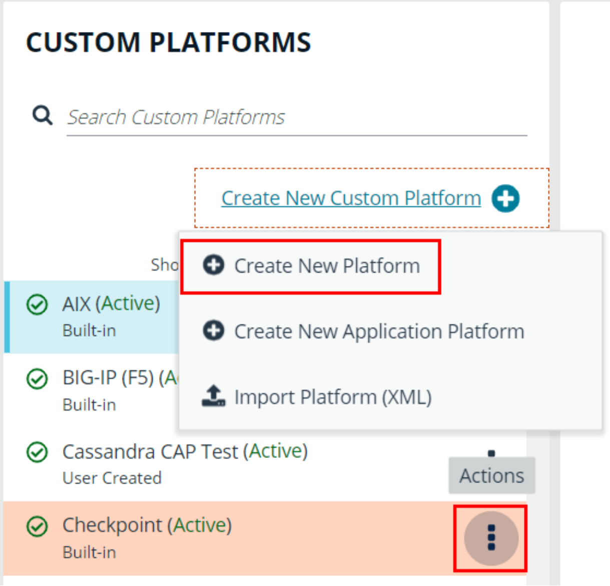
On the **Custom Platforms** page, you can add SSH and Telnet platforms, as well as SSH application platforms, tailored to your environment. Password Safe contains several built-in SSH and Telnet platforms designed for the most common configurations, such as Linux, Solaris, and Cisco. You can modify the 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**.

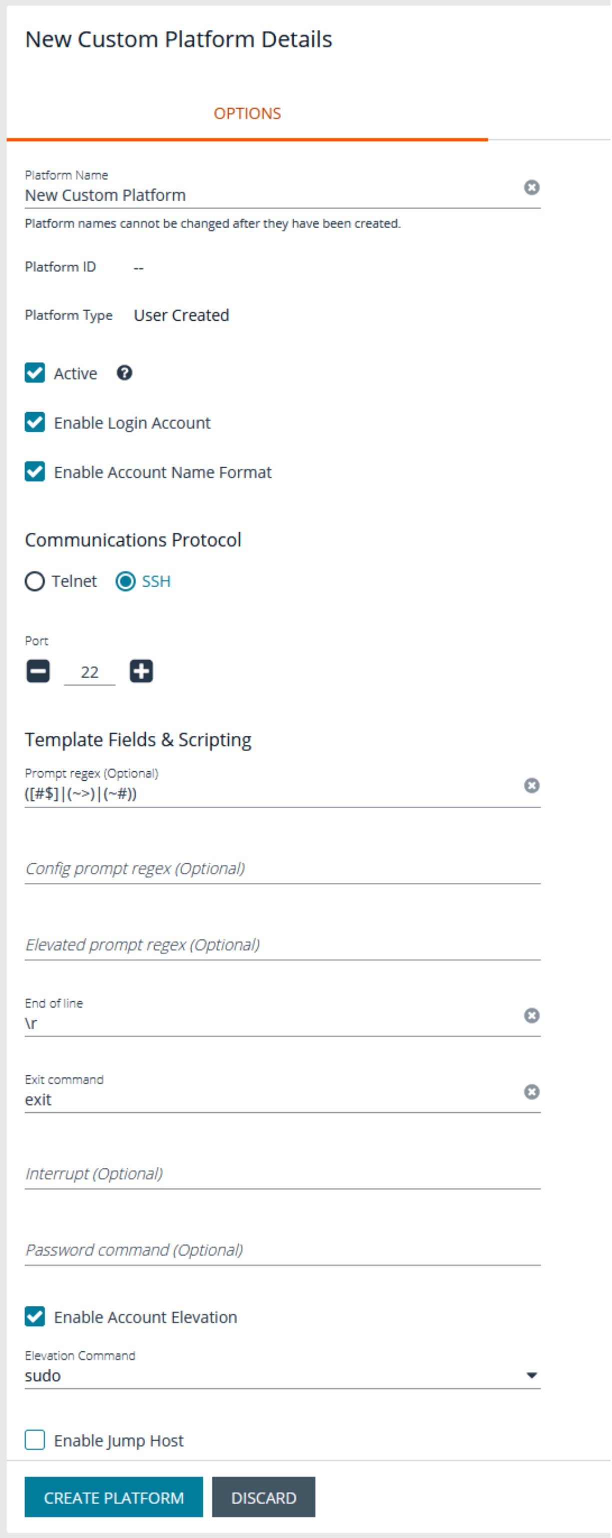
   Alternatively, click the **Actions** (vertical ellipsis) button for a platform in the list, and then select **Clone** to clone an existing platform and modify its settings as desired.



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**
    - **pmrun**
    - **pbrun jumphost**



New Custom Platform Details

Platform Name
New Custom 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

Communications Protocol

○ Telnet ● SSH

Port
22

Template Fields & Scripting

Prompt regex (Optional)
([#$]|(~>)|(~#))

Config prompt regex (Optional)

Elevated prompt regex (Optional)

End of line
\r

Exit command
exit

Interrupt (Optional)

Password command (Optional)

☑ Enable Account Elevation

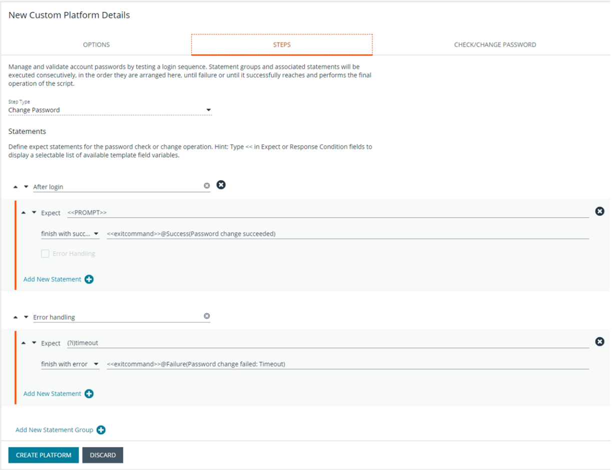
Elevation Command
sudo

☐ Enable Jump Host

- **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**.



New Custom Platform Details

Manage and validate account passwords by testing a login sequence. Statement groups and associated statements will be executed consecutively, in the order they are arranged here, until failure or until it successfully reaches and performs the final operation of the script.

Step Type
Change Password

Statements

Define expect statements for the password check or change operation. Hint: Type << in Expect or Response Condition fields to display a selectable list of available template field variables.

After login

Expect <<PROMPT>>

finish with succ... <<exitcommand>>@Success(Password change succeeded)

□ Error Handling

Error handling

Expect (?i)timeout

finish with error <<exitcommand>>@Failure(Password change failed: Timeout)

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.

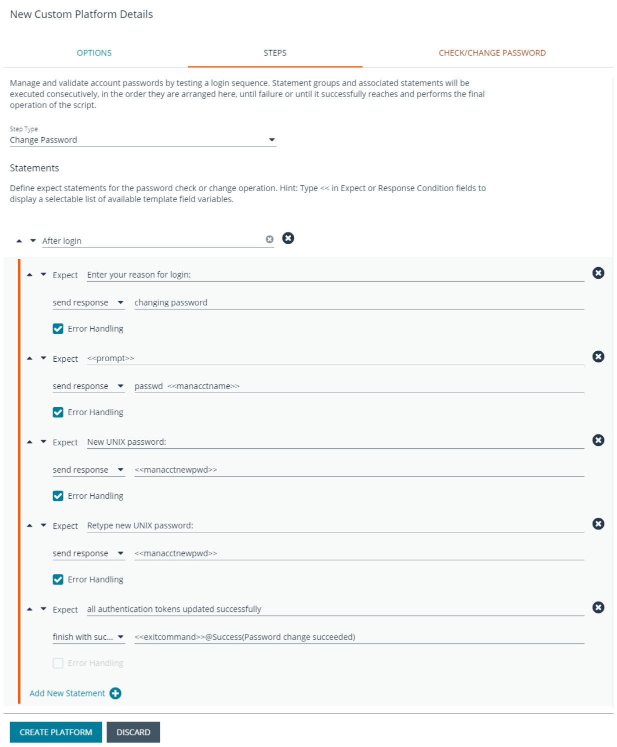
The following is an explanation of the functionality for each setting on the **Steps** tab, using a Linux platform as an example:

- **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:
```



New Custom Platform Details

Manage and validate account passwords by testing a login sequence. Statement groups and associated statements will be executed consecutively, in the order they are arranged here, until failure or until it successfully reaches and performs the final operation of the script.

Step Type: Change Password

Statements

Define expect statements for the password check or change operation. Hint: Type << in Expect or Response Condition fields to display a selectable list of available template field variables.

After login

Expect: Enter your reason for login:
send response: changing password
☑ Error Handling

Expect: <<prompt>>
send response: passwd <<manacctname>>
☑ Error Handling

Expect: New UNIX password:
send response: <<manacctnewpwd>>
☑ Error Handling

Expect: Retype new UNIX password:
send response: <<manacctnewpwd>>
☑ Error Handling

Expect: all authentication tokens updated successfully
finish with suc...: <<exitcommand>>@Success(Password change succeeded)
☐ Error Handling

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 proceding 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.

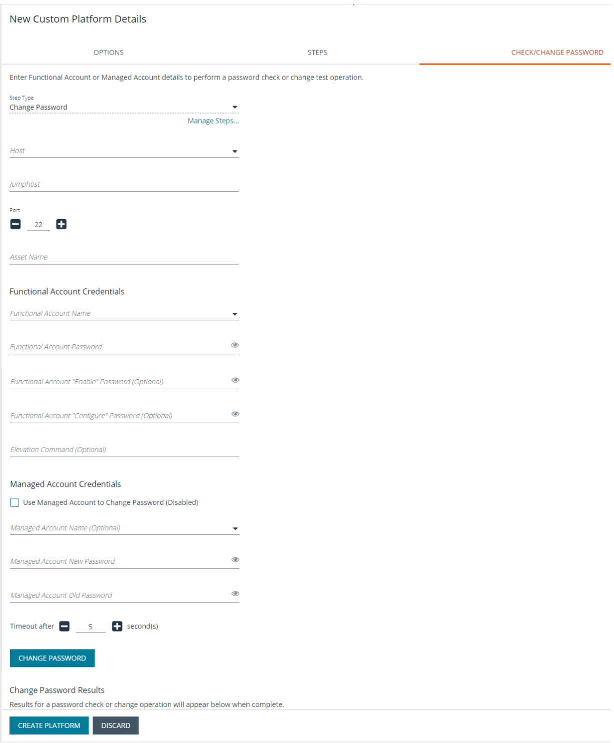
Configure the Check/Change Password Tab

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**.



New Custom Platform Details

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

Step Type: Change Password

Port: 22

□ Use Managed Account to Change Password (Disabled)

Timeout after 5 second(s)

Change Password Results

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

OPTIONS
STEPS
CHECK/CHANGE PASSWORD
Manage Steps...
Host
Jumphost
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
Managed Account Name (Optional)
Managed Account New Password
Managed Account Old Password
CHANGE PASSWORD
CREATE PLATFORM
DISCARD

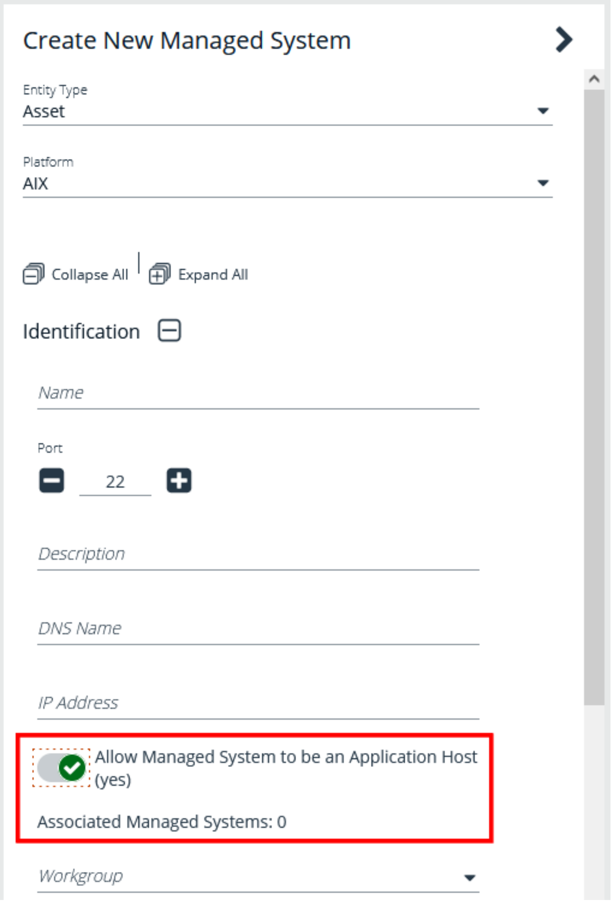
Create a New Application Platform

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

Port: 22

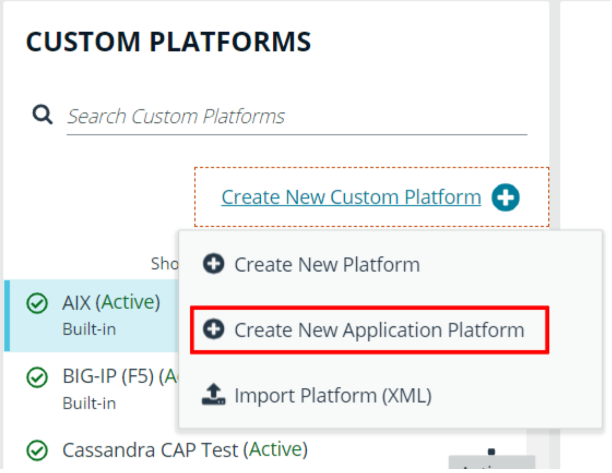
Allow Managed System to be an Application Host (yes)

Associated Managed Systems: 0

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

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

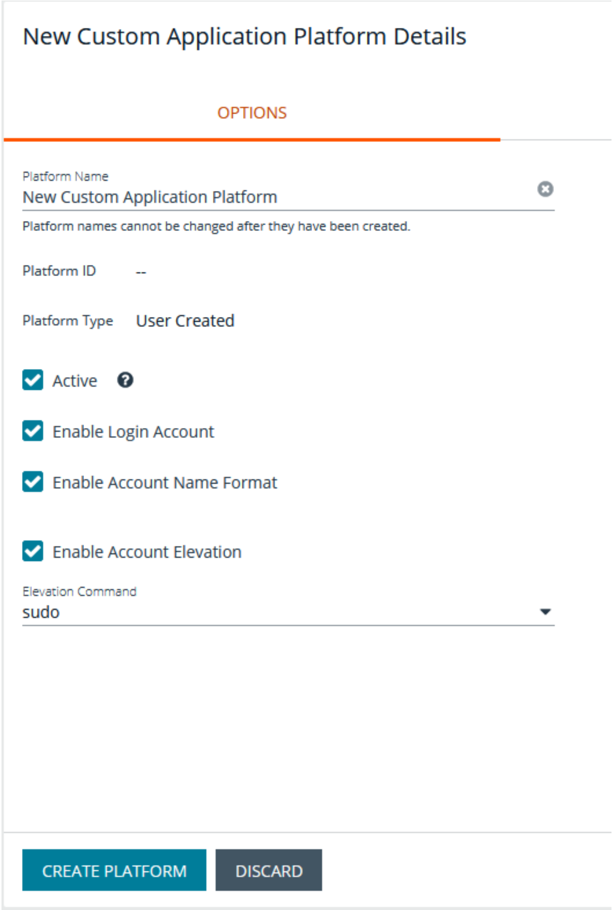
2. In the **Custom Platforms** pane, click **Create New Custom Platform**, and then select **Create New Application Platform**.



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.
- **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

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

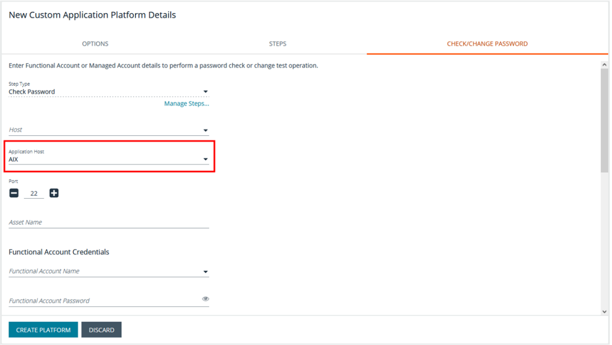
Configure the StepsTab

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**.



New Custom Application Platform Details

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

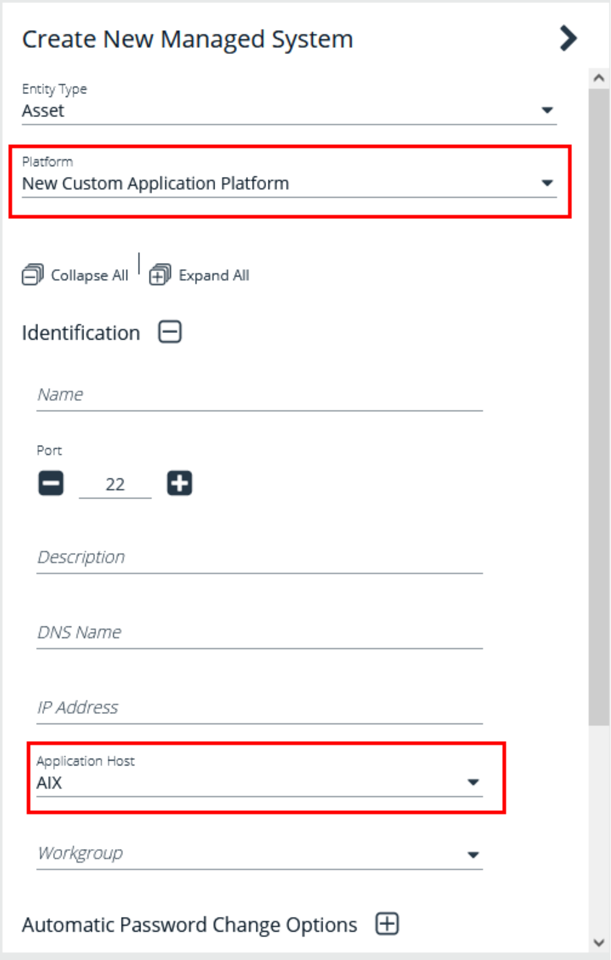
Step Type: Check Password

Application Host: AIX

Port: 22

Functional Account Credentials

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 manged 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

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 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.

For more information, please see "Configure Password Safe Access Policies" on page 59.

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"

Supported SSH Client 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-ct, 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\eEye\RetinaCS\SshKeyExchangeAlgorithms (DWORD) = 1023** (enables all key exchange)
- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\eEye\RetinaCS\SshEncryptionAlgorithms (DWORD) = 31** (sets all encryption algorithms)
- **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\eEye\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\eEye\RetinaCS\SshMinimumRsaKeySize (DWORD) = 1024 (size of key and bits)

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)
- 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 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\kex_algorithms (REG_MULTI_SZ)

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\client_kex_algorithms (REG_MULTI_SZ)

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 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.

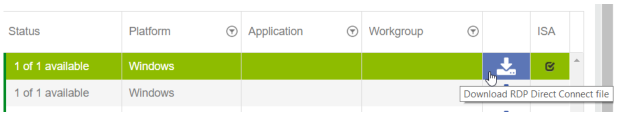
RDP Session Requests

> ***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 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)

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**.

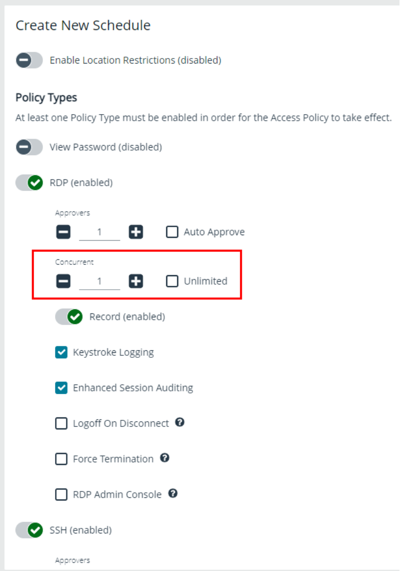
Configure Concurrent Sessions

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

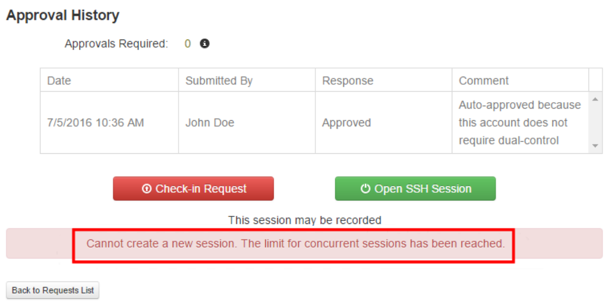
□ RDP Admin Console

SSH (enabled)

Approvers

If a user tries to open more sessions than allowed, a message displays on the **Requests** page.

> *For more information, please see "Configure Password Safe Access Policies" on page 59.*



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

This session may be recorded

Cannot create a new session. The limit for concurrent sessions has been reached.

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 lick 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.*

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs
131
©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.
TC: 12/1/2022

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.

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\SOFTWARE\Wow6432Node\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\SOFTWARE\Wow6432Node\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 59.*

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.*

To use enhanced session auditing, the functional account of the managed Windows host or Remote Desktop Services host needs 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:

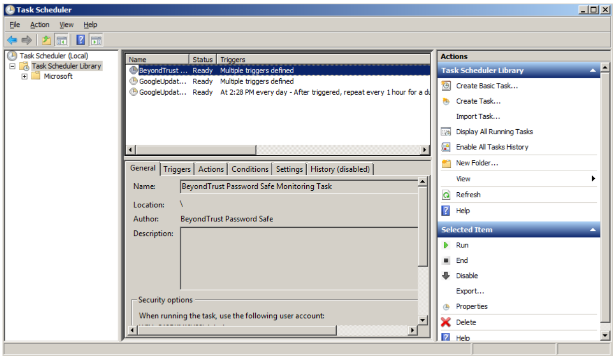
```
2017/03/07 15:47:12.186 2292 6548 INFO: Pushing pbpsdeploy service to 10.200.28.39 as
user backupadmin
2017/03/07 15:47:13.528 2292 6548 INFO: Starting pbpsdeploy service on 10.200.28.39 as
user backupadmin
2017/03/07 15:47:13.593 2292 6548 INFO: Copied pbpsmon.cab

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**.



Name	Status	Triggers
BeyondTrust ...	Ready	Multiple triggers defined
GoogleUpdat...	Ready	Multiple triggers defined
GoogleUpdat...	Ready	At 2:28 PM every day - After triggered, repeat every 1 hour for a d

Name: BeyondTrust Password Safe Monitoring Task
Location: \
Author: BeyondTrust Password Safe
Description:
Security options
When running the task, use the following user account:

- In regedit, the following registry key is created, which creates the disconnect event:

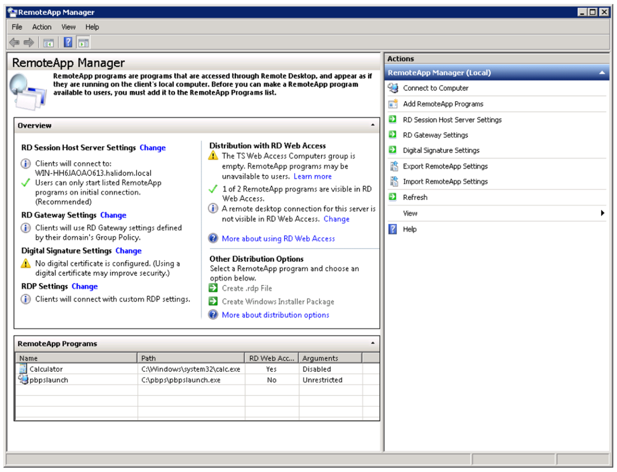
  HKLM\System\CurrentControlSet\Control\Terminal Server\Addins\PBPSMON

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.



RemoteApp Manager

RemoteApp programs are programs that are accessed through Remote Desktop, and appear as if they are running on the client's local computer. Before you can make a RemoteApp program available to users, you must add it to the RemoteApp Programs list.

RD Session Host Server Settings Change
Clients will connect to: WIN-HH6JAOAO613.halidom.local
Users can only start listed RemoteApp programs on initial connection. (Recommended)
RD Gateway Settings Change
Clients will use RD Gateway settings defined by their domain's Group Policy.
Digital Signature Settings Change
No digital certificate is configured. (Using a digital certificate may improve security.)
RDP Settings Change
Clients will connect with custom RDP settings.

Distribution with RD Web Access
The TS Web Access Computers group is empty. RemoteApp programs may be unavailable to users. Learn more
1 of 2 RemoteApp programs are visible in RD Web Access.
A remote desktop connection for this server is not visible in RD Web Access. Change
More about using RD Web Access

Other Distribution Options
Select a RemoteApp program and choose an option below.
Create .rdp File
Create Windows Installer Package
More about distribution options

Name	Path	RD Web Acc...	Arguments
Calculator	C:\Windows\system32\calc.exe	Yes	Disabled
pbpslaunch	C:\pbps\pbpslaunch.exe	No	Unrestricted

- 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**.
  1. Open **Event Viewer**.
  2. 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 the BeyondInsight Console, go to **Configuration > Privileged Access Management > Functional Accounts**.
2. Click **Create 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 138.*

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**.

The command applies to Password Safe v6.4.4 or later.

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, /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
```

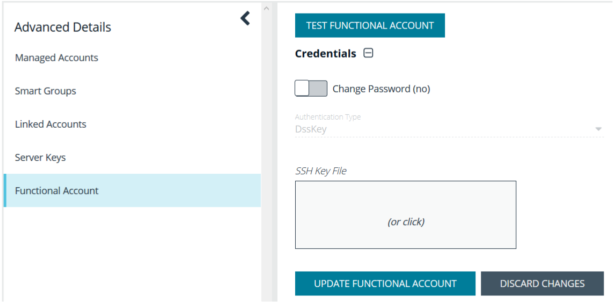
AIX

```
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**.



Change Password (no)

Authentication Type
DssKey

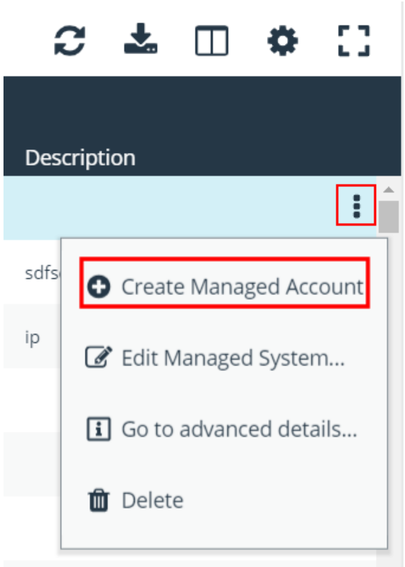
Set DSS on the Managed Account

An alternate and secure way to set up a managed account is with DSS authentication.

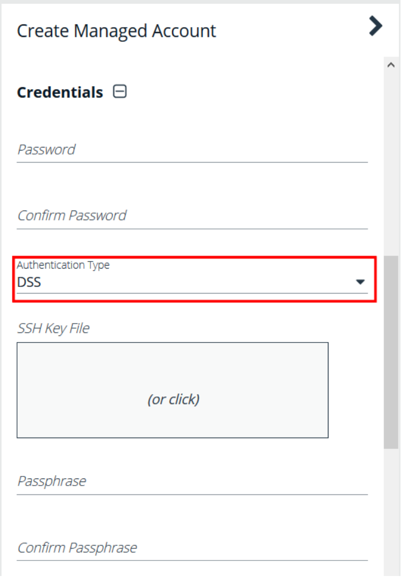
Before you can create the account, you must generate a private key. Copying or importing a key is part of setting the managed account properties with DSS authentication.

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**.



Create Managed Account

Credentials

Password

Confirm Password

Authentication Type: DSS

SSH Key File

(or click)

Passphrase

Confirm Passphrase

5. Configure all other settings as required, and then click **Create Account**.

For more information, please see the following:

- *"Generate and Distribute the Key" on page 138*
- *"Work with Managed Accounts" on page 28*

DSS Key Auto Management

A DSS key policy is set on a managed system that supports DSS authentication.

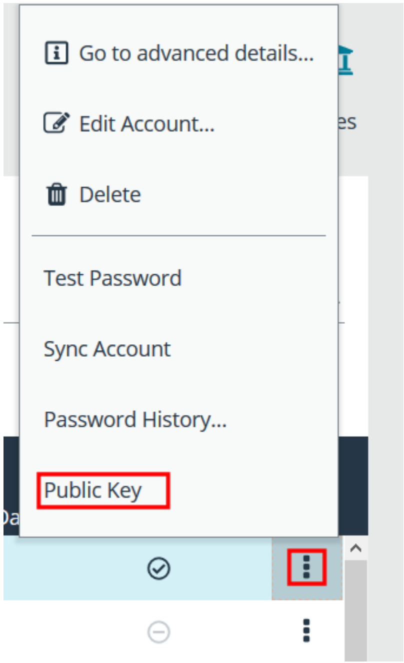
The **Auto-Managed DSS key** option enables DSS key auto-management to take place when the password for the account is changed, either manually or scheduled. It follows the same schedule as password changing.

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.

For more information, please see "Create a DSS Key Policy" on page 142.

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.

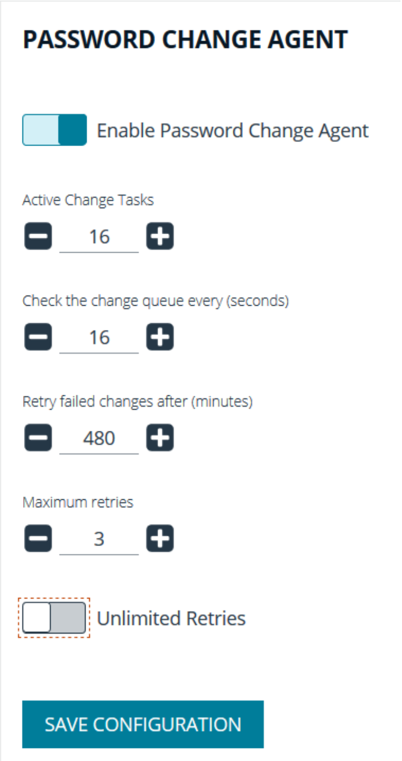
The following overview explains how the change agent runs:

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: 16

Check the change queue every (seconds): 16

Retry failed changes after (minutes): 480

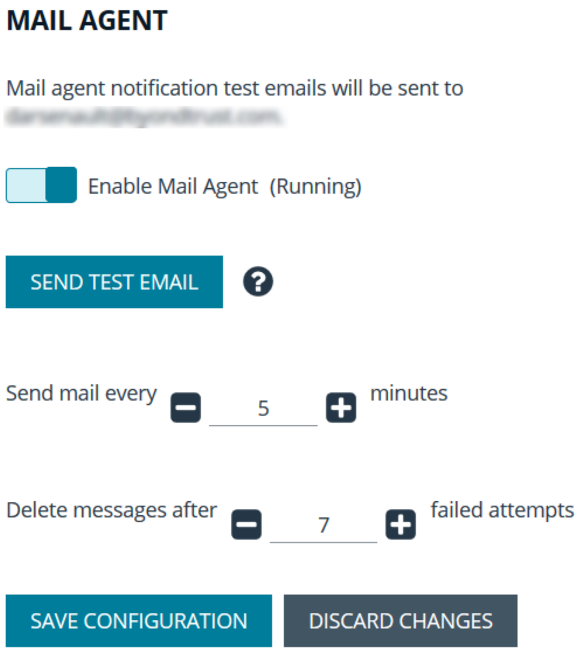
Maximum retries: 3

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 [redacted]

Enable Mail Agent (Running)

Send mail every 5 minutes

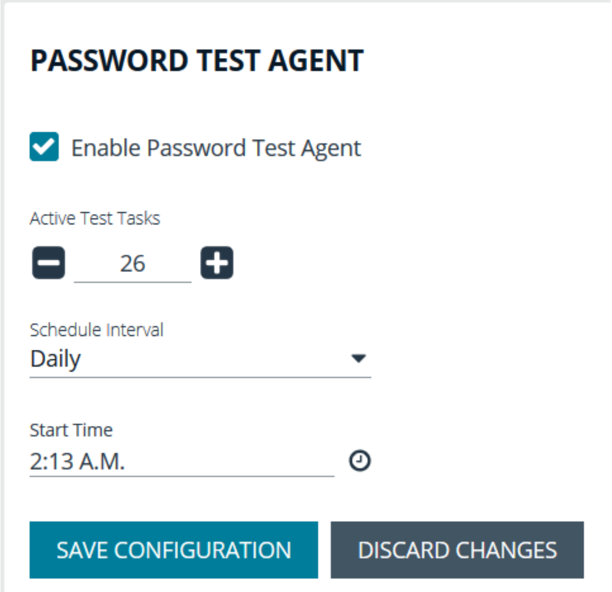
Delete messages after 7 failed attempts

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.

Configure Session Agents for Remote Proxy Sessions

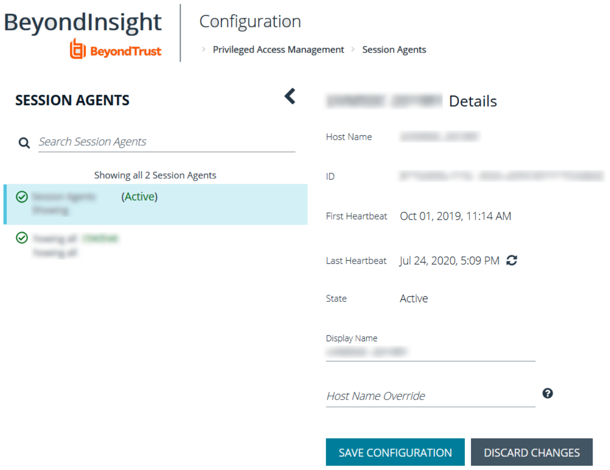
In a distributed environment where there is more than one BeyondInsight instance installed, a Password Safe user can request a session to a remote instance. In this scenario, the user can request passwords and sessions for a remote instance by selecting a node on the **Requests** page in the Password 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**.



Showing all 2 Session Agents

(Active)

Details

Host Name

ID

First Heartbeat: Oct 01, 2019, 11:14 AM

Last Heartbeat: Jul 24, 2020, 5:09 PM

State: Active

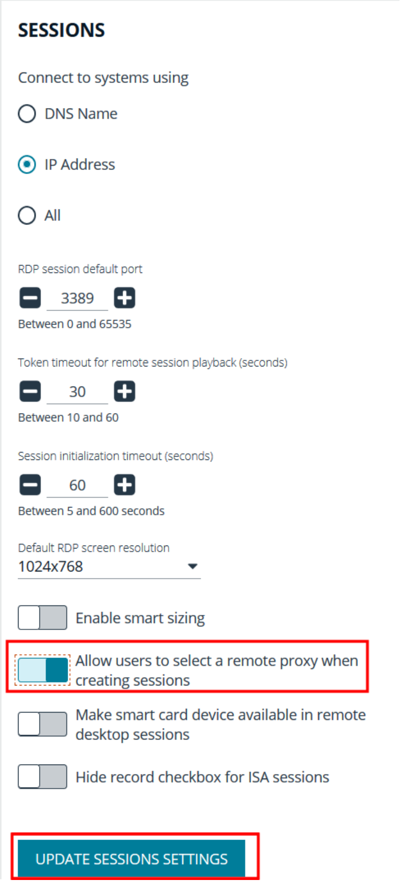
Display Name

Host Name Override

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: 3389
Between 0 and 65535

Token timeout for remote session playback (seconds): 30
Between 10 and 60

Session initialization timeout (seconds): 60
Between 5 and 600 seconds

Default RDP screen resolution: 1024x768

Enable smart sizing: off

Allow users to select a remote proxy when creating sessions: on

Make smart card device available in remote desktop sessions: off

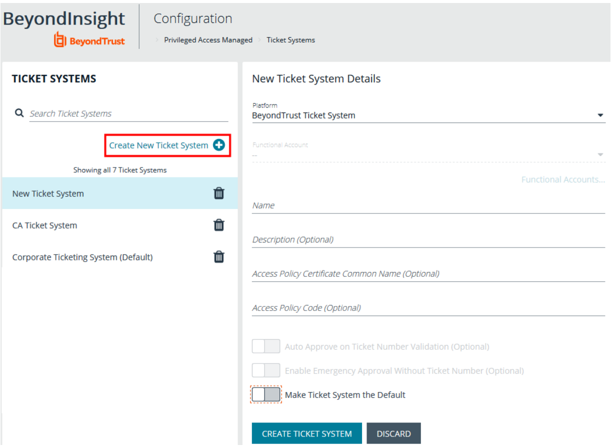
Hide record checkbox for ISA sessions: off

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 the BeyondInsight Console, go to **Configuration > Privileged Access Management > Ticket Systems**.
2. In the **Ticket Systems** pane, click **Create New Ticket System**.
4. Select **BeyondTrust Ticket System** from the **Platform** list.
5. Enter a name and description.
6. Click **Save Ticket System**.


BeyondInsight
BeyondTrust
Configuration
Privileged Access Managed
Ticket Systems
TICKET SYSTEMS
Search Ticket Systems
Create New Ticket System
Showing all 7 Ticket Systems
New Ticket System
CA Ticket System
Corporate Ticketing System (Default)
New Ticket System Details
Platform
BeyondTrust Ticket System
Functional Account
--
Functional Accounts...
Name
Description (Optional)
Access Policy Certificate Common Name (Optional)
Access Policy Code (Optional)
Auto Approve on Ticket Number Validation (Optional)
Enable Emergency Approval Without Ticket Number (Optional)
Make Ticket System the Default
CREATE TICKET SYSTEM
DISCARD

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 at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm*
- *BeyondTrust Password Safe Guides 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	• Account's Approver • Requester (CC) • Asset's ISA
Request Response	Managed	NA	• Account's Approver (CC) • Requester • Asset's ISA
Password Change Failure	Managed	• Managed System's ISA • Built-in BeyondInsight Administrator • Managed System contact person (Managed Systems settings UI)	NA
	Functional	• Managed System's ISA • Built-in BeyondInsight Administrator • Managed System contact person (Managed Systems settings UI)	NA
Password Check Failure	Managed	• Managed System's ISA • Built-in BeyondInsight Administrator • Managed System contact person (Managed Systems settings UI)	NA
	Functional	• Managed System's ISA • Built-in BeyondInsight Administrator • Managed System contact person (Managed Systems settings UI)	NA

Privileged Password Release	Managed	- Managed Account Release Notification Recipients (Managed Accounts settings UI)	NA
Non-Managed Release Expiration	Managed	- Managed Account Release Notification Recipients (Managed Accounts settings UI)	NA

Domain Accounts

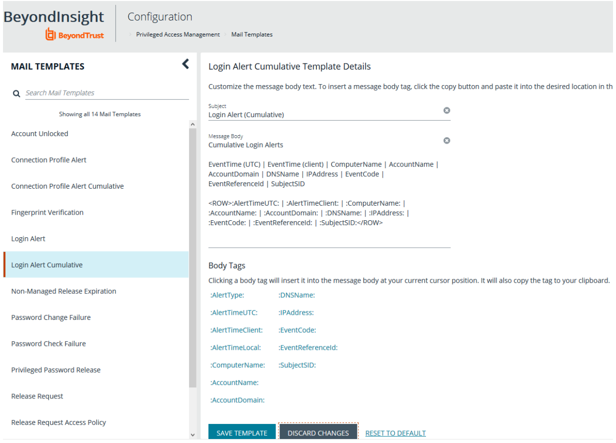
Event	Account	Not configurable	Configurable by template settings
Release Request	Managed	NA	- Account's Approver - Requester (CC) - Domain Management permission (with Read/Write)
Request Response	Managed	NA	- Account's Approver (CC) - Requester - Domain Management permission (with Read/Write)
Password Change Failure	Managed	- Domain Management permission (with Read/Write) - Built-in BeyondInsightAdministrator - Managed System contact person (Managed Systems settings UI)	NA
	Functional	- Domain Management permission (with Read/Write) - Built-in BeyondInsight Administrator - Managed System contact person (Managed Systems settings UI)	NA
Password Check Failure	Managed	- Domain Management permission (with Read/Write) - Built-in BeyondInsightAdministrator - Managed System contact person (Managed Systems settings UI)	NA
	Functional	- Domain Management permission (with Read/Write) - Built-in BeyondInsight Administrator - Managed System contact person (Managed Systems settings UI)	NA

Privileged Password Release	Managed	• Managed Account Release Notification Recipients (Managed Accounts settings UI)	NA
Non-Managed Release Expiration	Managed	• 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.

1. In the BeyondInsight Console, go to **Configuration > Privileged Access Management > Mail Templates**.
2. Select a mail template type from the list.
3. Type the subject line text.
4. 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 **:approvallink:** and **:denylink:** message body tags.
5. Click **Save Template**.



Login Alert Cumulative Template Details

Customize the message body text. To insert a message body tag, click the copy button and paste it into the desired location in th

Subject
Login Alert (Cumulative)

Message Body
Cumulative Login Alerts

EventTime (UTC) | EventTime (client) | ComputerName | AccountName | AccountDomain | DNSName | IPAddress | EventCode | EventReferenceId | SubjectSID

<ROW>:AlertTimeUTC: | :AlertTimeClient: | :ComputerName: | :AccountName: | :AccountDomain: | :DNSName: | :IPAddress: | :EventCode: | :EventReferenceId: | :SubjectSID:</ROW>

Body Tags

Clicking a body tag will insert it into the message body at your current cursor position. It will also copy the tag to your clipboard.

:AlertType:	:DNSName:
:AlertTimeUTC:	:IPAddress:
:AlertTimeClient:	:EventCode:
:AlertTimeLocal:	:EventReferenceId:
:ComputerName:	:SubjectSID:
:AccountName:	
:AccountDomain:	

***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.

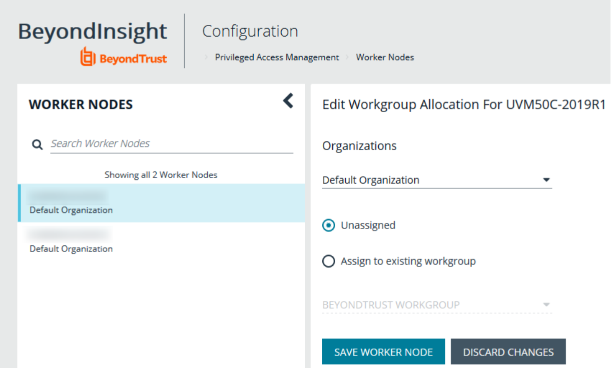
Create a Password Safe Worker Node

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 dropsdown list to select the workgroup you want.
3. Click **Save Worker Node** when done.



Showing all 2 Worker Nodes

[redacted]
Default Organization

[redacted]
Default Organization

Edit Workgroup Allocation For UVM50C-2019R1

Organizations: Default Organization

● Unassigned

○ Assign to existing workgroup

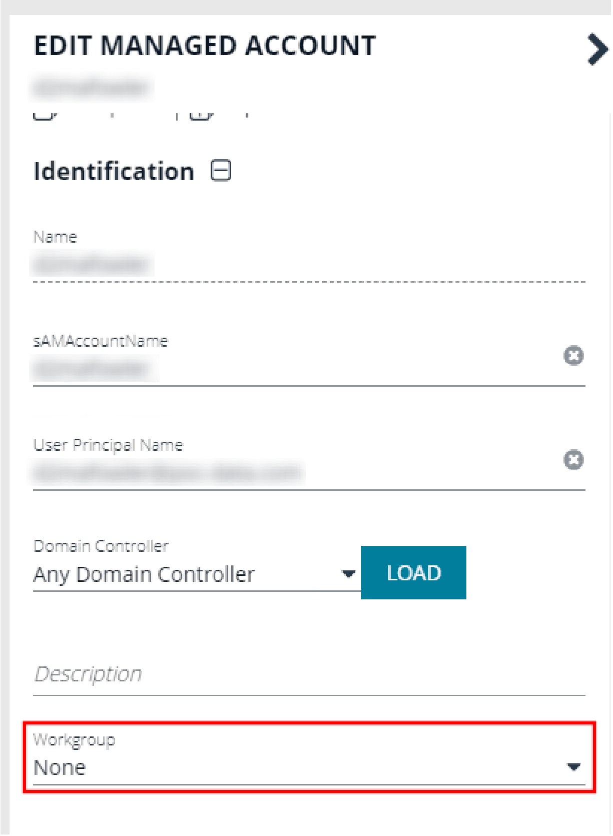
BEYONDTRUST WORKGROUP

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.*



EDIT MANAGED ACCOUNT

Identification

Name

sAMAccountName

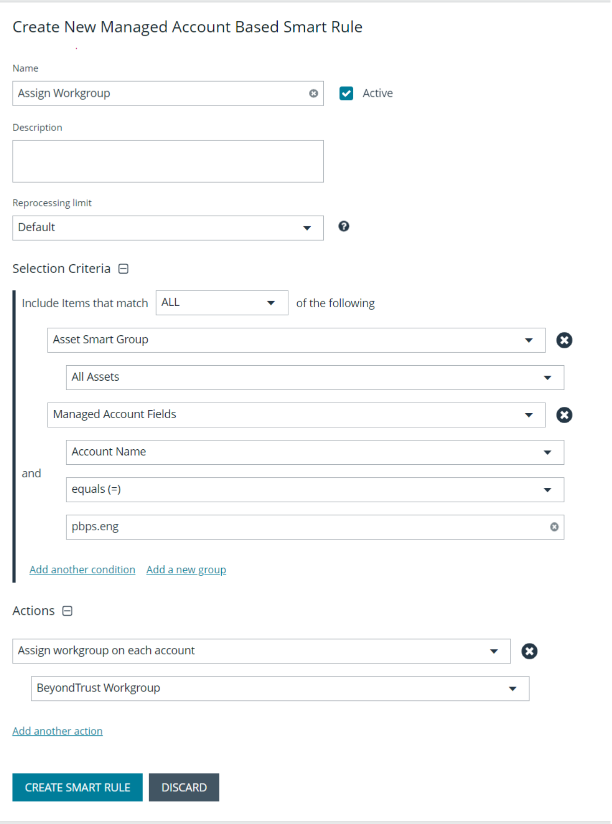
User Principal Name

Domain Controller: Any Domain Controller

Description

Workgroup: None

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: Assign Workgroup ☑ Active

Description:

Reprocessing limit: Default

Selection Criteria

Include Items that match ALL of the following

Asset Smart Group: All Assets

and

Managed Account Fields: Account Name, equals (=), pbps.eng

Actions

Assign workgroup on each account: BeyondTrust Workgroup

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:

- *For more information on assigning managed accounts to workgroups, "Assign a Workgroup to a Managed Account" on page 151*
- *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.

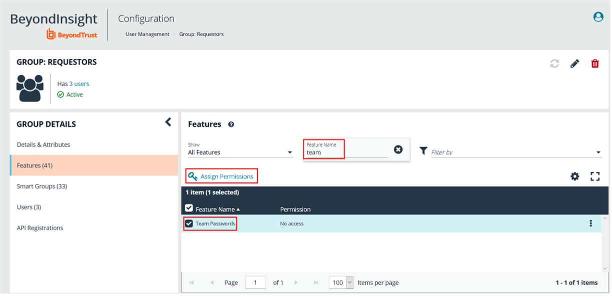
Configure and Use Team Passwords

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

Assign a Group to a Team in Team Passwords

Access to **Team Passwords** is granted to users by assigning permissions for the **Team Passwords** feature to a group in which the users are members.

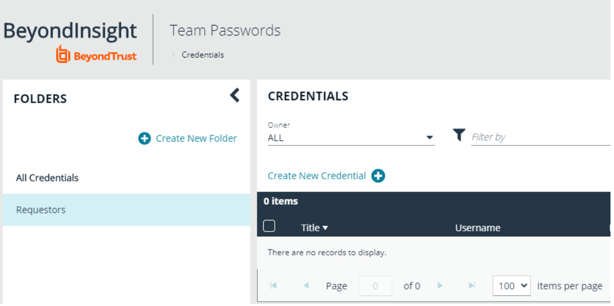
1. In the BeyondInsight Console, go to **Configuration > Role Based Access > User Management**.
2. Click the vertical ellipsis for the group you want to assign the **Team Passwords** feature to, and then select **View Group Details**.
3. From the **Group Details** pane, select **Features**.
4. From the **Features** pane, select the **Team Passwords** feature.



Feature Name	Permission
☑ Team Passwords	No access

> *Tip: You can filter the list of features by **All Features** or **Disabled Features**, and **Feature Name** to quickly locate the **Team Passwords** feature.*

5. Click **Assign Permissions**, and then select **Assign Permissions Read Only**.
6. User who are members of the group are granted access to the **Team Passwords** page, where the group is listed as a parent level folder representing the team.



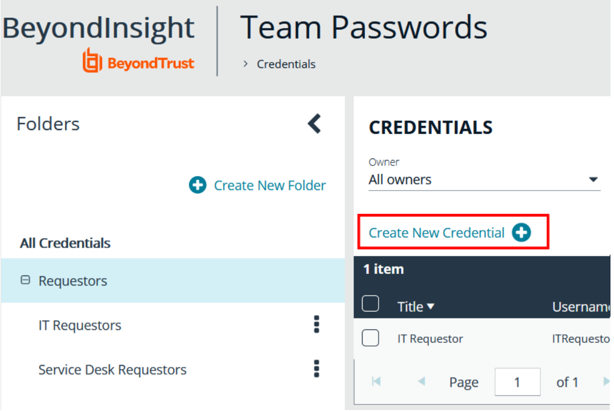
> ***Note:** Removing the **Team Passwords** feature from the group removes all folders and credentials in the team.*

Create a Credential in Team Passwords

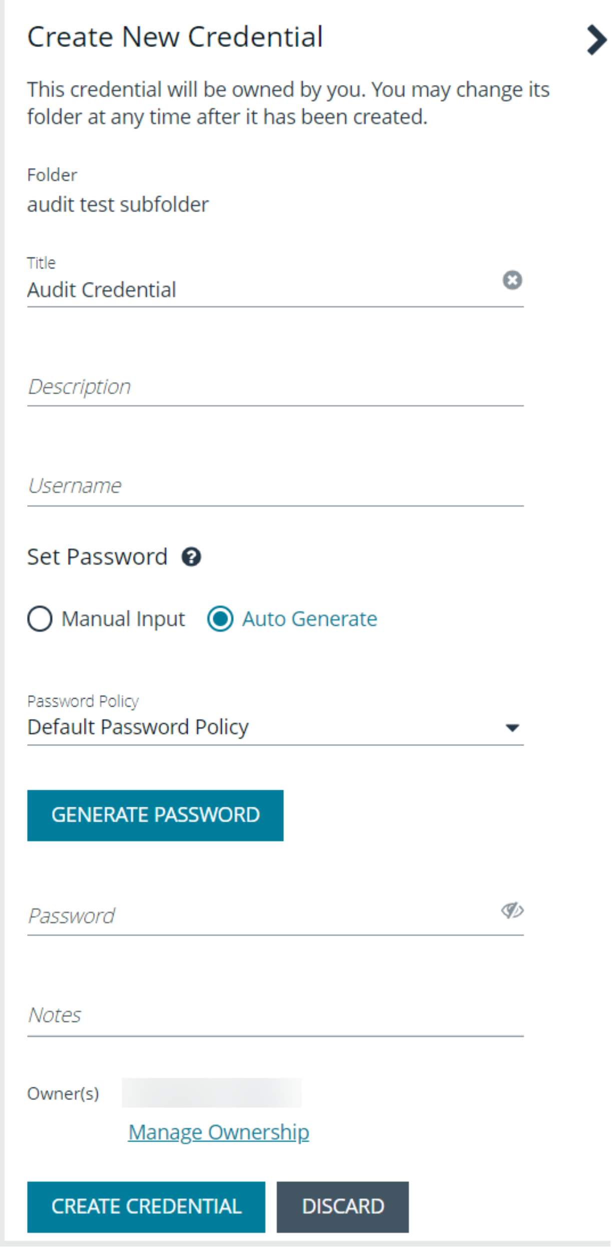
Users can create credentials in the parent folder for any of their teams or in any of their team's subfolders. The user who creates the credential is its owner by default but may change ownership at time of creating the credential or after the credential has been created. Owners may change the folder for credentials after they have been created.

1. On the left navigation pane in the console click **Team Passwords**.

2. From the **Folders** pane, select a folder, and then click **Create New Credential**.



3. If Add Credential is selected, in the **Create New Secret** pane:
   - 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 Credential**.



Create New Credential

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

Folder: audit test subfolder

Title: Audit Credential

Description

Username

Set Password

○ Manual Input ● Auto Generate

Password Policy: Default Password Policy

Password

Notes

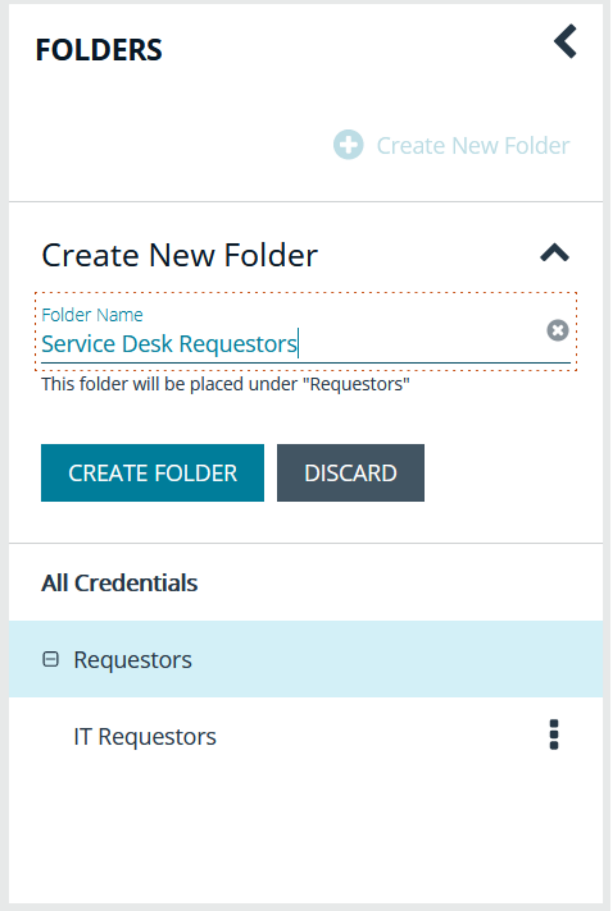
Owner(s)

Manage Folders in Team Passwords

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

1. On the left navigation pane in the console click **Team Passwords**.

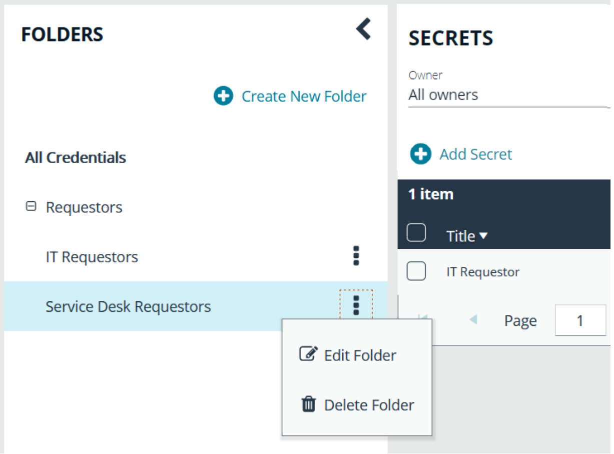
2. To create a new folder, select the parent folder for the team or one of its existing subfolders, and then click **Create New Folder**.
3. Enter a name for the folder, and then click **Create Folder**.



Folder Name: Service Desk Requestors

This folder will be placed under "Requestors"

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



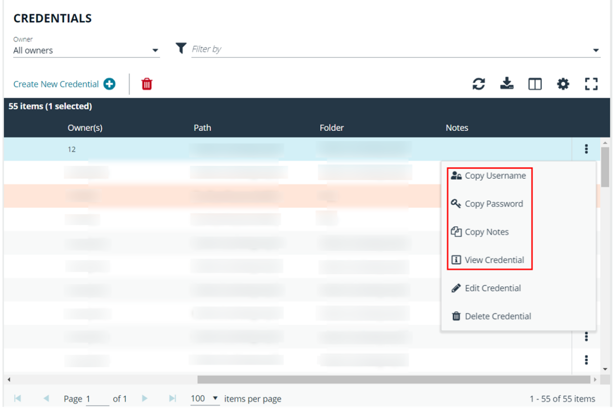
> ***Note:*** *You cannot delete parent team folders. Only subfolders may be deleted. Also, if you do not own all of the credentials in a subfolder, you are not able to delete it.*

> *For more information on how to move a credential to a new subfolder, please see "Edit and Delete a Credential in Team Passwords" on page 159.*

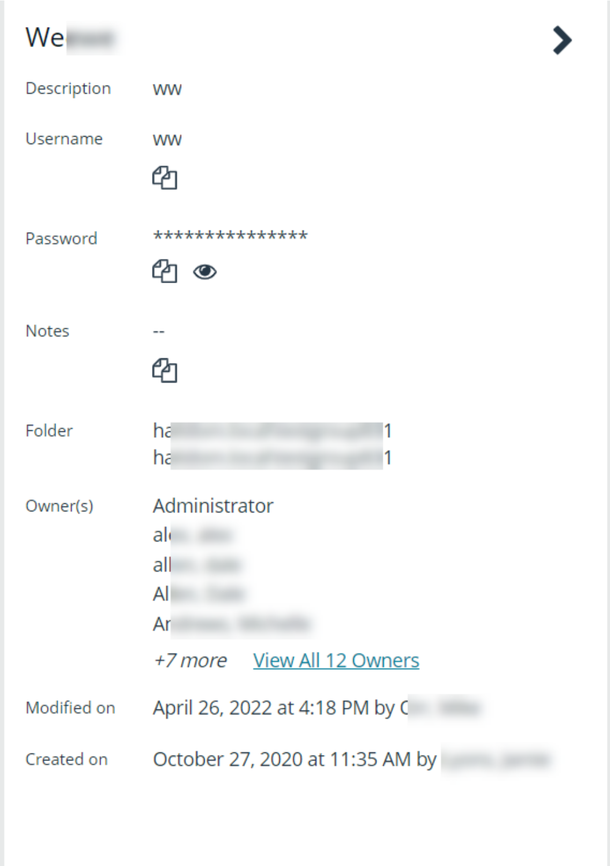
View and Copy a Credential in Team Passwords

Users can view details for their team's secrets, such as who owns the secret, when the secretwas 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. On the left navigation pane in the console click **Team Passwords**.
2. From the **Folders** pane, select a folder, and then select a credential.
3. Click the vertical ellipsis for the credential.
4. To quickly copy the username, password, and notes, select those options from the dropdown menu.
5. To view the details for the credential, select **View Credential** from the dropdown menu.



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



We[redacted]

Description ww

Username ww

Password ***************

Notes --

Folder ha[redacted]1
ha[redacted]1

Owner(s) Administrator
al[redacted]
all[redacted]
Al[redacted]
Ar[redacted]
+7 more View All 12 Owners

Modified on April 26, 2022 at 4:18 PM by C[redacted]

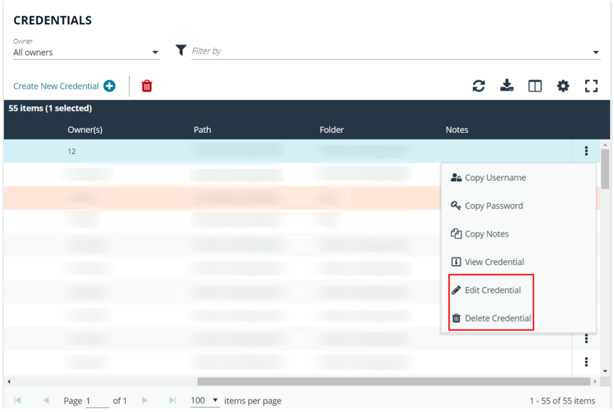
Created on October 27, 2020 at 11:35 AM by [redacted]

Edit and Delete a Credential in Team Passwords

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

1. On the left navigation pane in the console click **Team Passwords**.

2. From the **Folders** pane, select a folder, and then select a credential.
3. Click the vertical ellipsis for the credential.
4. To delete a credential, select **Delete Credential**, and then click **Delete** on the confirmation message.
5. To edit a credential, select **Edit Credential**.



CREDENTIALS

Owner: All owners

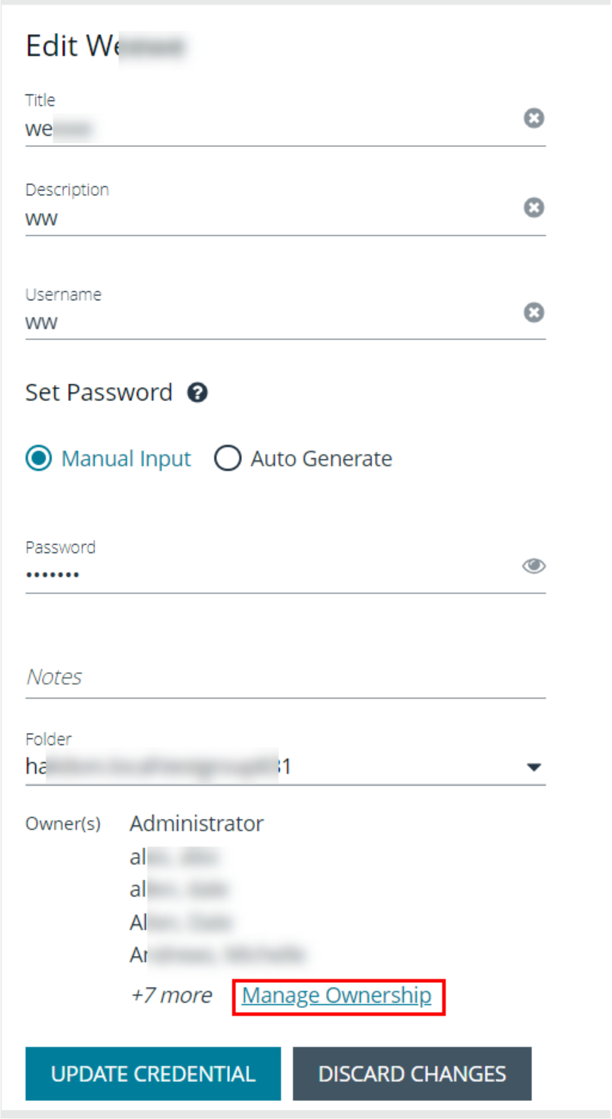
Filter by

55 items (1 selected)

Owner(s)	Path	Folder	Notes
12			

Page 1 of 1 | 100 items per page | 1 - 55 of 55 items

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



Edit We[redacted]

Title: we[redacted]

Description: ww

Username: ww

Set Password

● Manual Input ○ Auto Generate

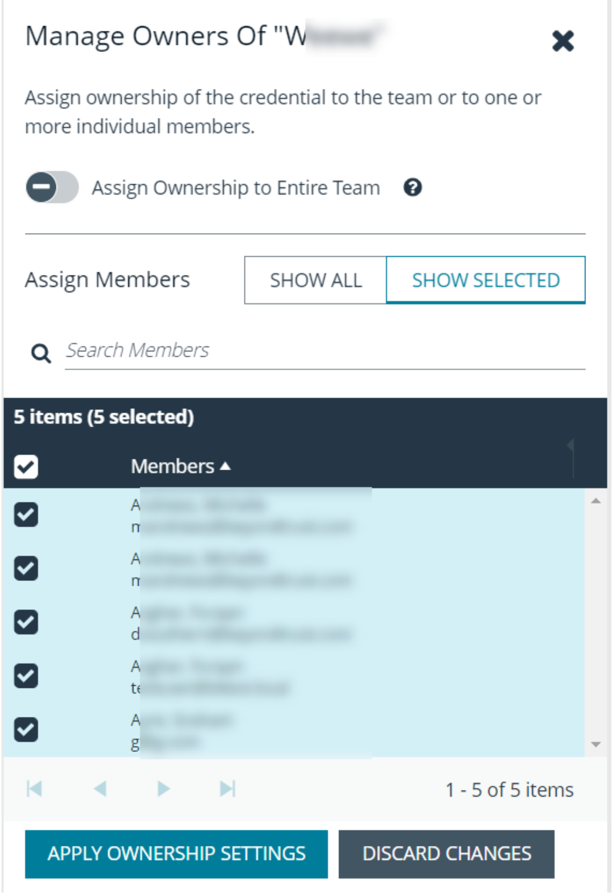
Password: •••••••

Notes

Folder: ha[redacted]1

Owner(s): Administrator
al[redacted]
al[redacted]
Al[redacted]
Ar[redacted]
+7 more

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



Manage Owners Of "W

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

Assign Ownership to Entire Team

5 items (5 selected)

☑	Members ▲
☑	A m
☑	A m
☑	A d
☑	A te
☑	A g

1 - 5 of 5 items

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