BeyondTrust

Password Safe
Admin Guide 7.0

TC:9/24/2020

Table of Contents

Password Safe Administration Guide

Password Safe is your privileged access management solution to ensure your resources are protected from insider threats.

Using Password Safe, you can restrict access to critical systems, including assets and applications, keeping them safe from potential inside threat risks.

Password Safe is supported on a Unified Vulnerability Management (UVM) hardened appliance that creates and secures privileged accounts through automated password management, encryption, secure storage of credentials, and a sealed operating system.

Log into 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 into the console depend on the type of authentication configured for your BeyondInsight system.

Note: *This section describes authentication types that are available to users of BeyondInsight. Configuration of security providers is beyond the scope of this document.*

The following authentication types can be used:

- **Password Safe Authentication**
- **Active Directory:** Create a BeyondInsight group and add Active Directory users as members.
- **LDAP:** Create a BeyondInsight group and add LDAP users as members.
- **Smart Card:** Configure Password Safe to allow authentication using a Smart Card PIN.
- **RADIUS:** Configure multi-factor authentication with a RADIUS server.
- **Third Party Authentication:** Configure Password Safe to use authentication for web tools which support SAML 2.0 standard such as PingID, Okta and ADFS.

1. Open a browser and enter **https://<*servername*>**. You are redirected to the web console.
2. Enter your username and password and then click **Log In**. The default username is Administrator, and the password is the password you set for Administrator in the configuration wizard.

Note: *You may need to accept a pre-login message, if one has been configured on your system.*

For more information on configuring authentication using BeyondInsight groups, Smart Card, RADIUS, and third party SAML 2.0 web tools, please refer to the BeyondInsight and Password Safe Authentication Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-ps-authentication.pdf.

Select a Display Language

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

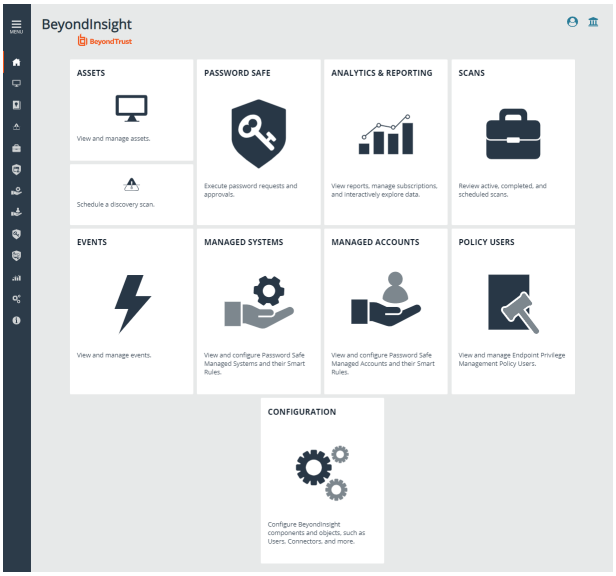
- English
- Dutch
- Spanish
- French
- Korean
- Japanese
- Portuguese

You can select a language from the list on the **Log In** page or by clicking the **Profile and preferences** icon.

> ***Note:*** *The* ***Language Settings*** *menu is not available by default. A BeyondInsight Administrator must enable it in* ***Site Options****.*

Navigate the Console

Once logged into the BeyondInsight console, your suite of features are easily accessible by clicking the container cards or by clicking **Menu** in the left navigation. Your available features vary depending on your license and the permissions assigned to your console account.



Features available on the home page may include:

- **Assets:** Display and manage all assets. Access the Smart Rules page to create and manage smart groups. Add assets to Password Safe management.
- **Scan:** Schedule discovery scans.
- **Password Safe:** Access the Password Safe web portal to request passwords and remote access sessions and approve requests.
- **Analytics and Reporting:** Access reporting features to run analytics on collected data.
- **Scans**: Review active, completed, and scheduled scans.
- **Events:** View and manage Endpoint Privilege Management events.
- **Managed Accounts:** View and configure properties for Password Safe managed accounts and their associated Smart Rules.
- **Managed Systems:** View and configure properties for Password Safe managed systems, managed databases, managed directories, managed applications, and their associated Smart Rules.
- **Policy Users:** View Endpoint Privilege Management policy users and assign policies to policy users.
- **Configuration:** Configure BeyondInsight and Password Safe components and objects, such as users and groups, authentication settings, connectors, and much more.

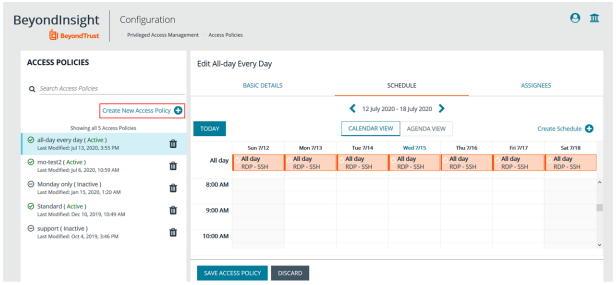
Configure Password Safe Access Policies

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

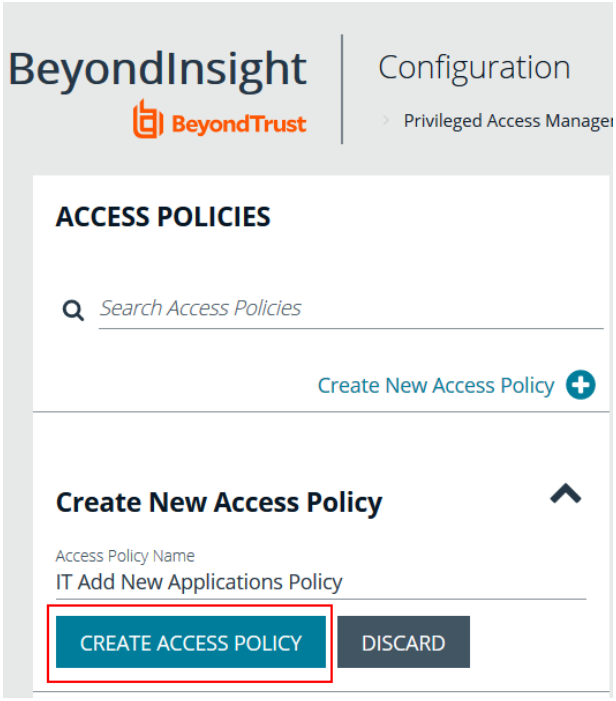
An access policy is selected when you are configuring the **Requester** role.

Create an Access Policy

1. Select **Configuration > Privileged Access Management Policies > Access Policies**.
2. In the **Access Policies** pane, click **Create New Access Policy**.



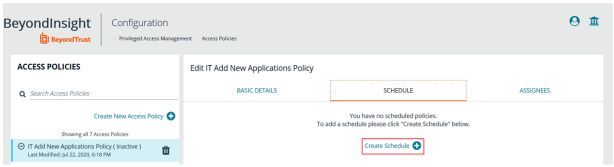
3. Enter a name for the policy, and then click **Create Access Policy**.



4. On the **Basic Details** tab:
   - Enter a description for the policy.
   - 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**.



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 that you are permitting: **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. Uncheck the box to turn off enhanced logging.

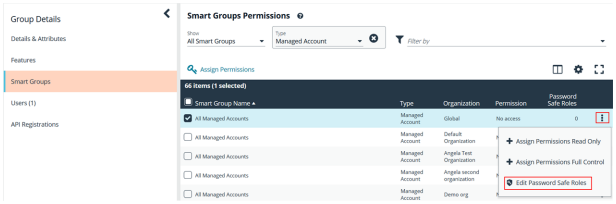
Concurrent	Set the number of sessions permitted at a time. Check **Unlimited** to permit the user any number of connections to occur at the same time.
Log off on Disconnect	Check this box to automatically log off the user when the connection to the session disconnects or the session window closes. This option applies only to RDP and RDP application sessions.
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. Click **Create Schedule**.
12. Select the **Basic Details** tab, and then check the **Available for Use** option to activate the access policy.
13. Click **Save Access Policy**.

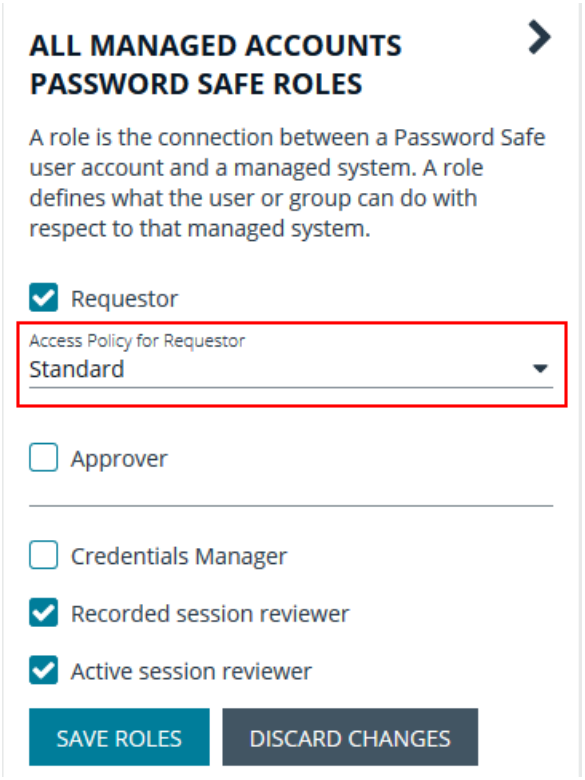
The access policy can now be assigned to a group as follows:

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**.



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.



For more information, please see the following:

- "Configure Keystroke Logging" on page 60
- "Enhanced Session Auditing" on page 61
- For configuring release durations, "Add a Managed System Manually" on page 31
- 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 12

Create a Connection Profile

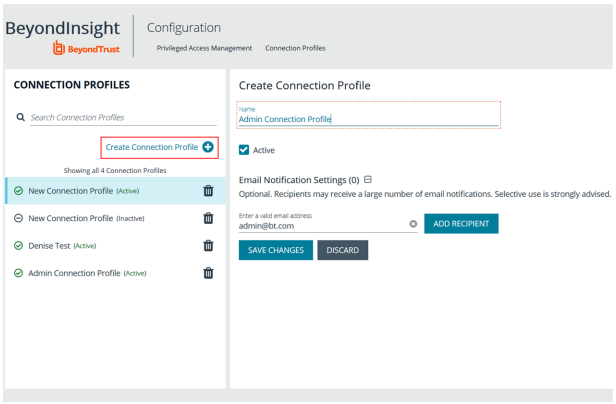
Connection profiles allow administrators to create a blacklist of keywords, host names, and IP addresses. Each blacklisted item can be given a separate action which is triggered when requesters type a blacklisted item in an active SSH session.

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

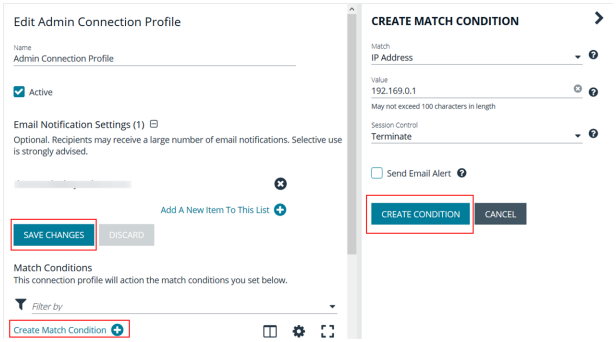
- **No Action:** Select to be alerted only if a match occurs.
- **Block:** Blocks the transmission of the command to the remote machine.
- **Lock:** Locks the session for the requester.
- **Block and Lock:** Performs both a block and lock as described above.
- **Terminate:** Ends the remote session.

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

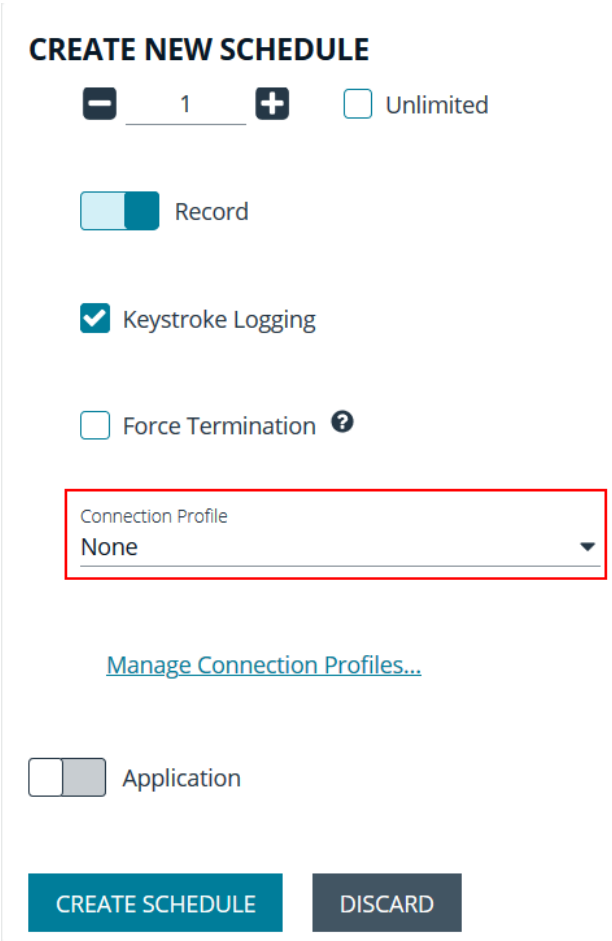
1. In the BeyondInsight console go to **Configuration > Privileged Access Management Policies > Connection Profiles**.
2. In the **Connection Profiles** pane, click **Create Connection Profile**.
3. In the **Create Connection Profile** pane:
    - Enter a name for the profile.
    - Under **Email Notification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



5. Click **Create Match Condtion**.
6. To add a blacklisted 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 blacklisted item is triggered.
9. Click **Create Condition**. Each blacklisted item is displayed on a separate line.
10. Click **Save Changes**.



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.



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.

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 appliance. When the change agent runs, it checks the configuration to determine operational parameters of the appliance. Logs provide a record of the change agent activities and messages, and indicate success or failure.

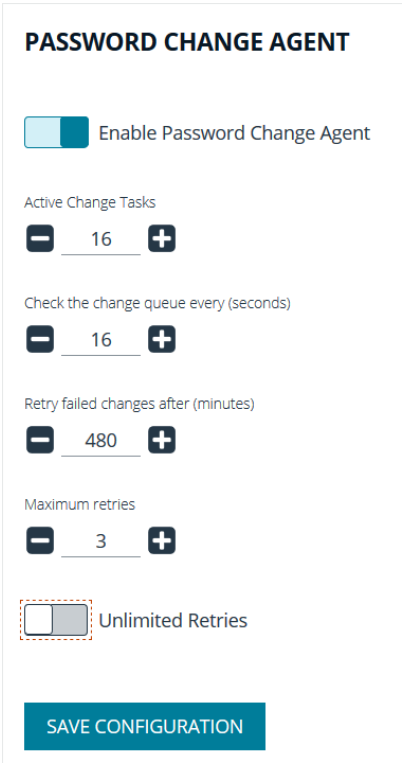
The following overview explains how the change agent runs:

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.

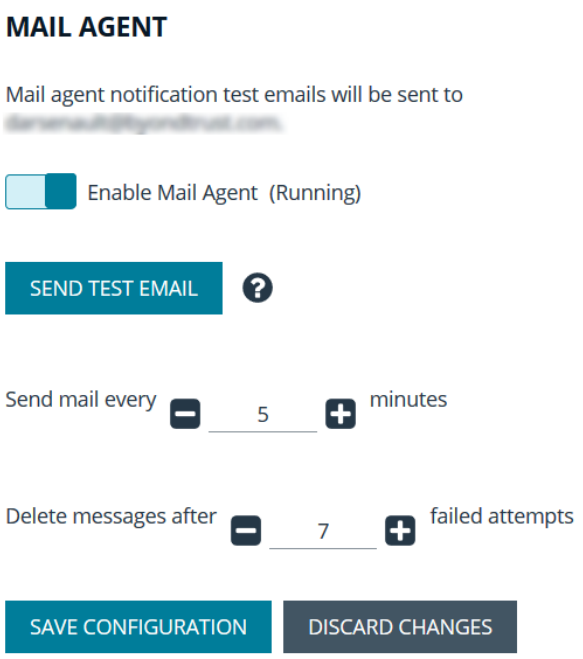
1. In the BeyondInsight console, go to **Configuration > Privileged Access Management Agents > Password Change Agent**.
2. Set the following:
    - **Enable Password Change Agent:** Leave enabled to activate the agent when Password Safe starts.
    - **Active Change Tasks:** The number of accounts to 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**.



Configure the Mail Agent

Password Safe uses email to provide notification between approvers and requesters, error alerting, and general information delivery.

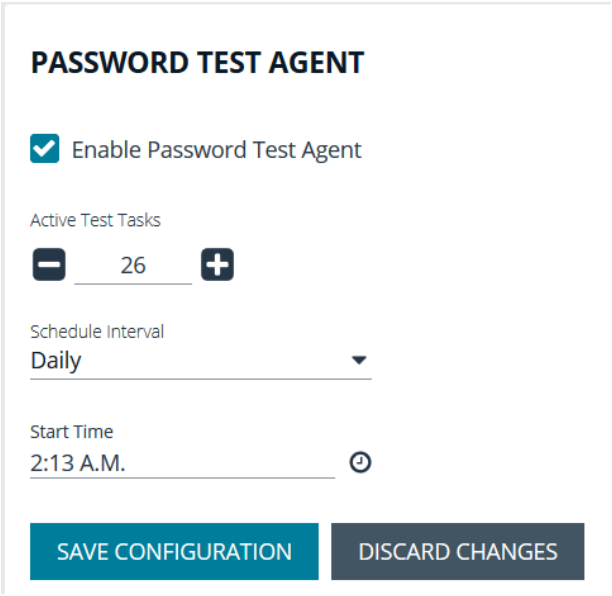
1. In the BeyondInsight console, go to **Configuration > Privileged Access Management Agents > Mail Agent**.
2. Set the following:
   - **Enable Mail Agent (Running):** Enable to activate the mail agent when Password Safe starts.
   - **Send mail every x minutes:** The number of minutes that pass before 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**.



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**.



Configure Session Agents for Remote Proxy Sessions

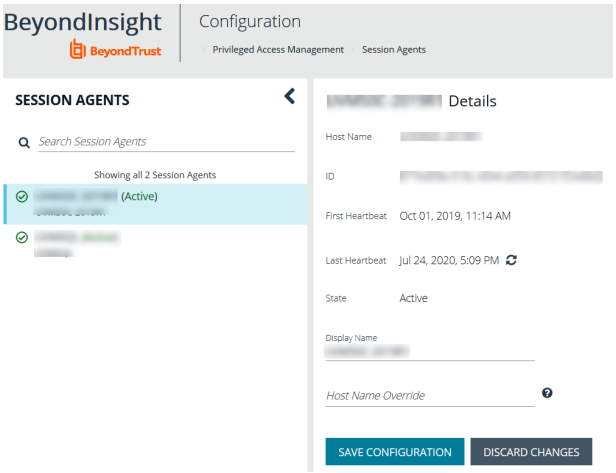
In a distributed environment where there is more than one BeyondInsight instance installed, a Password Safe user can request a session to a remote instance. In this scenario, the user can request passwords and sessions for a remote instance by selecting a node on the **Requests** page in the Password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

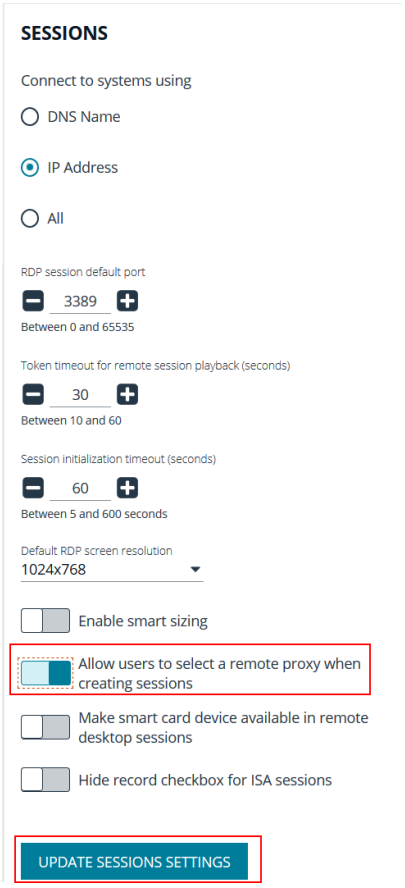
1. In the BeyondInsight console, go to **Configuration > Privileged Access Management Agents > Session Agents**.
2. The **Session Agents** pane lists the active and inactive agents. Select an agent, and then enter the **Display Name** in the **Details** pane for that agent.
3. If the DNS name for the 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**.



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**.



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	Allows you to 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	Allows you to change the default port for all RDP sessions.
Token timeout for remote session playback	Allows you to change the default timeout. The default is **30** seconds. The range is **10 - 60** seconds.
Session initialization timeout	Allows you the 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	Allows you to 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 uses 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 57.

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**.

For more information, please see "Add Ticket Systems to the List on the Requests Page" on page 21.

Session Monitoring

For information on Session Monitoring options, please see "Add Ticket Systems to the List on the Requests Page" on page 21

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**.

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.

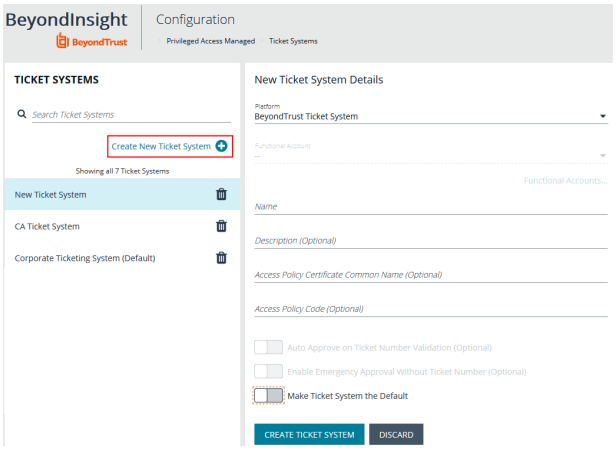
Network traffic can create delays in establishing the connection. Increase the token timeout if you are experiencing network timeouts. For more information on multi-node session playback, please see "Configure Session Monitoring" on page 57.

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**.



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

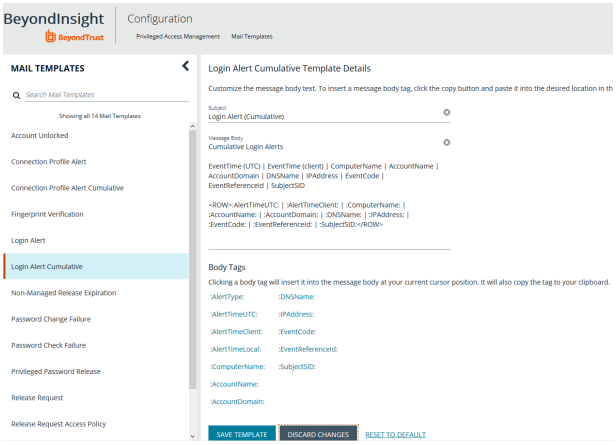
Event	Account	Not configurable	Configurable by template settings
Release Request	Managed	NA	• Account's Approver • Requester (CC) • Domain Management permission (with Read/Write)
Request Response	Managed	NA	• Account's Approver (CC) • Requester • Domain Management permission (with Read/Write)
Password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

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

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**.



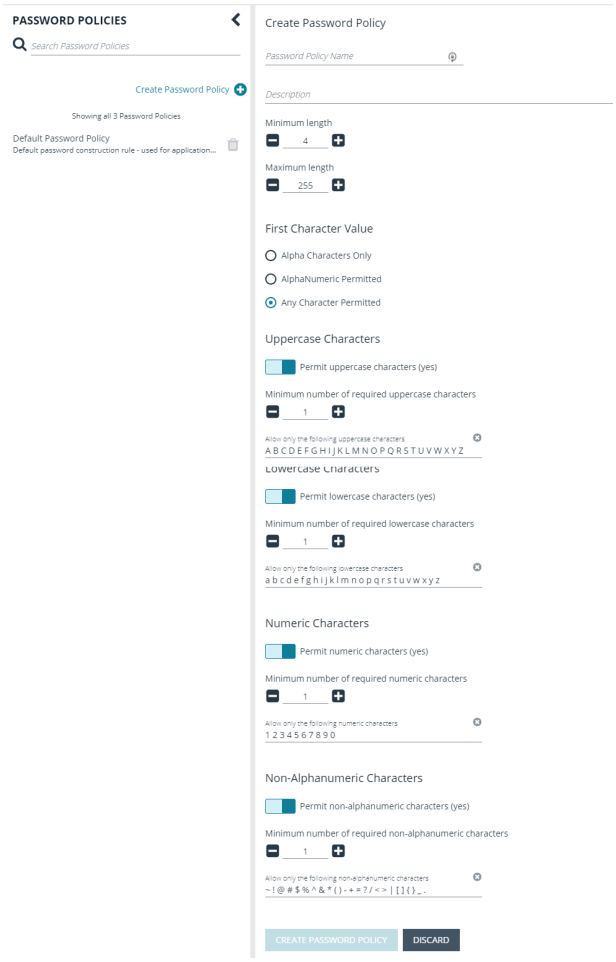
***Note:** Only one **<ROW></ROW>** tag can be added to the mail template. If you wish to add more tags, they must be added to the row already present within the template. For example:*

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

Create Password Policies

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

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



1. 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.
    - 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.

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.

For more detailed information on API Registrations using the **Auth/SignAppIn API** function, please see the BeyondInsight and Password Safe API Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/ps/ps-api.pdf.

To create an API Registration:

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

   BeyondInsight will generate 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 will receive a "401 Unauthorized" error until the new key is used in its place. Read access and rotation of the key is audited.*

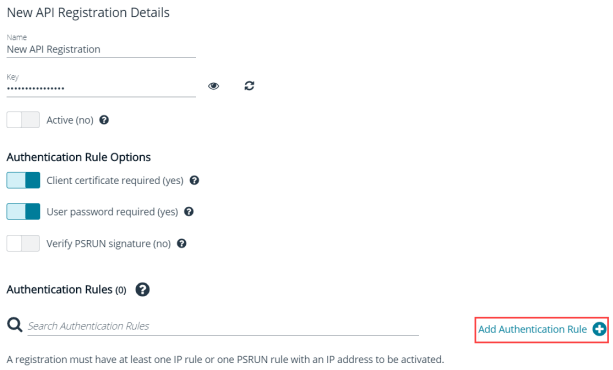
4. To configure the new registration or modify an existing one, select the registration and then set the **Authentication Rule Options** in the registration's **Details** pane.
   - **Client Certificate Required:** If enabled, a client certificate is required with the web request, and if not enabled, 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:** If 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];
     ```

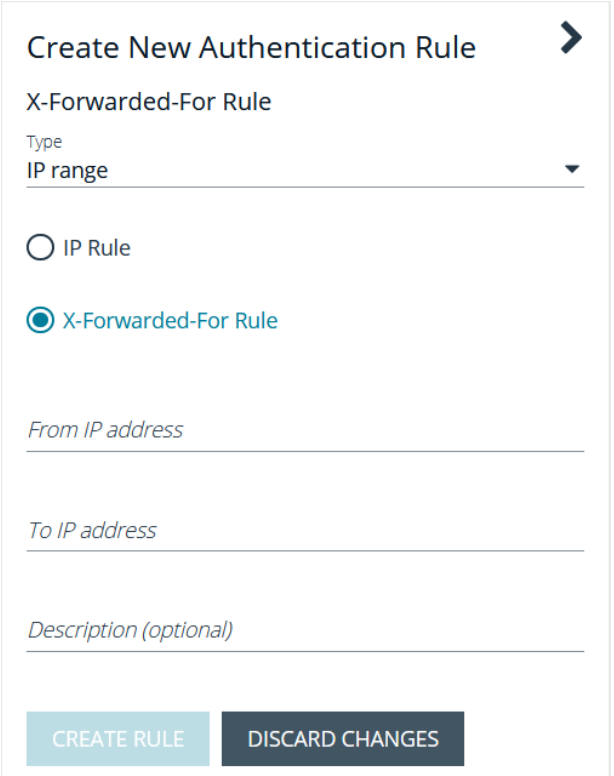
   - **Verify PSRUN Signature:** The PSRUN signature is an extra level of authentication. It's computed from the factors using a shared secret between the client and server. PSRUN sends the signature as part of the header during its API request. If enabled, the server recomputes the signature during factor 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.

5. From the registration's **Details** pane, 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 will fail with a *401 Unauthorized* error.



6. In the **Create New Authenticaton Rule** pane, click **Create Rule**.
7. In the **Details** pane, click **Save Changes**.

For information on how to grant API access to BeyondInsight users, please see "Role Based Access" on page 117.

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 the console.
- **Discovery Scanning:** Using BeyondTrust Network Security Scanning, you can run a discovery scan on a selected range of IP addresses.

Workflow to Add Managed Systems and Accounts to Password Safe

The following is a high-level overview on the steps required to add systems and accounts as 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.
2. **Add the managed system:** A managed system is a computer where one or more account passwords are to be maintained by Password Safe. Managed systems can be Windows machines, Unix/Linux machines, databases, firewalls, routers, iLO machines, and LDAP/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 into 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.

IMPORTANT!

Do not set up a functional account as a managed account. Functional accounts have built-in management capabilities and passwords could 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:*** *The passwords for functional accounts **cannot** be retrieved through the Password Safe web portal.*

9. Click **Save New 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.

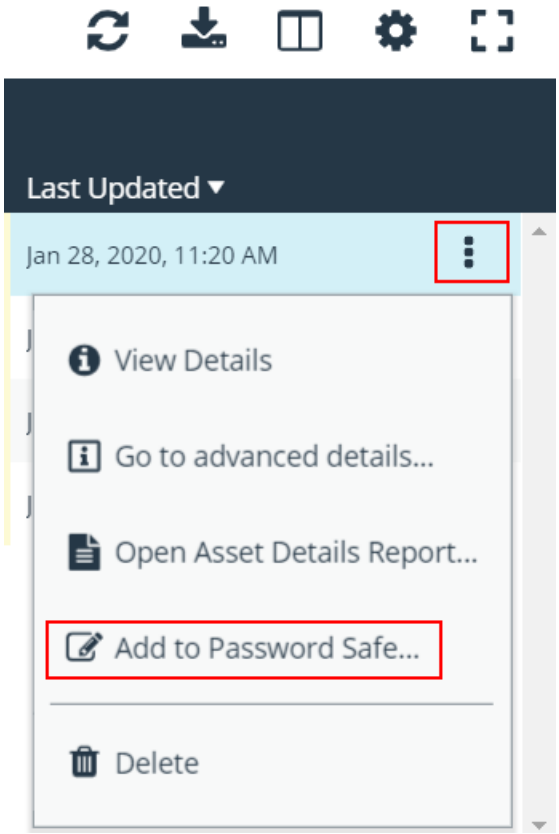
Add a Managed System Manually

> ***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 manually. From the **Managed System** grid, click **Create New Managed System**.

Alternatively, link the managed system to an asset:

1. On the **Assets** page, select the system you want to manage, and then click the vertical ellipsis at the right end of the line.
2. Select **Add to Password Safe** from the menu.



3. On the **Create New Managed System** form, set the system settings. The settings will vary based on the platform selected. The settings are described in the below table.
4. Click **Create Managed System**.

Setting	Description or Action
Platform	Select a platform type from the list.
Name	Enter a unique name for the system.
Instance Number (SAP only)	If you have added your SAP (System Application Products) environment to Password Safe management, provide the instance number. For more information, please see "Add SAP as a Managed System" on page 80.
Description	Enter a description for the system.
DNS Name	Enter the DNS name for the system.
Workgroup	Select the system workgroup from the dropdown list.
Port	Enter a port number.
NetBIOS (Windows and Active Directory managed systems only)	Enter a unique name for the system.

Enable Automatic Password Management	Toggle to automatically check and update managed account passwords at a set frequency or after password releases.
Default 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 For more information, please see "Create Password Policies" on page 26 .
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**.*
Functional Account	Select a functional account from the list.
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. For more information, please see "Enable Login Accounts for SSH Sessions" on page 87. **Login Account:** Select the account name.
Account Name Format	Select an account name format from the list: **sAMAccountName**, **UPN** or **domain\account**. For more information, please see "Set the Account Name Format within the Managed Assets using Password Safe Action" on page 40.
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, it is recommended to 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. For more information, please see "Import an SSH Server Key Using a Smart Rule" on page 40. **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. For more information, please see "Manage the SSH Server Keys" on page 41.

Default DSS Key Policy	If you are using DSS authentication for the system, select a key policy or use the default. For more information, please see "Set DSS on the Managed Account" on page 54.
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. For more information on force termination, please see "Create an Access Policy" on page 9.
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 Password Safe system notifications will be sent.

Add a Managed Account Manually

You can add an account after the system is added to Password Safe management.

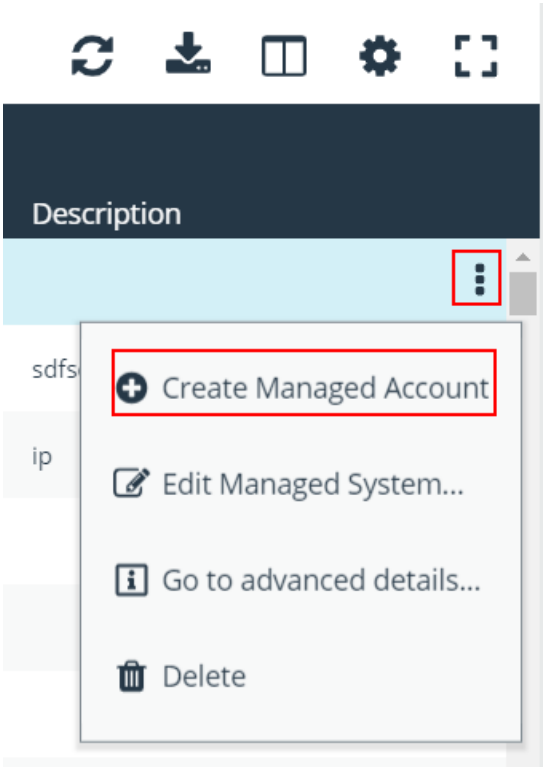
Note: *If the platform you are adding is Unix or Linux, additional settings are available.*

*The **DSS authentication** and **Use this account's current password to change the password** settings are **not** supported if you are using the elevated credential **pbrun jumphost**:*

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

2. Select a managed system, and then click the vertical ellipsis at the right end of the line.
3. Select **Create Managed Account**.

> ***Note:*** *This option is also available in the* ***Managed Accounts*** *section of* ***Advanced Details*** *of a managed system.*



4. Fill in the account settings, and then click **Create Account**. The settings are described in the below table.

Setting	Description or Action
Manage System, **Type**, **Platform**	Automatically populated from the managed system.
Name, **Description**	Provide a name and description for the managed account.
Workgroup	Select a workgroup from the list. Workgroups are used to assign a Password Safe worker node a specific area of responsibility. Password changes are then managed at the workgroup level. For more information, please see "Configure Workgroups for Multi-Node and Multi-Tenant Environments" on page 127.
Password, **Confirm password**	Enter the credentials for the managed account.

Automatic Password Change Options	Enable to automatically check and update managed account passwords at a set frequency or after password releases. The following settings must be configured: **Password Policy:** Select a password policy. A password policy provides complexity restrictions when a password is created for the managed account. For more information, please see "Create Password Policies" on page 26. **Change Password Frequency**, **Change Password Staring From:** Set password change frequency and scheduling. The password change frequency can be set to a maximum of every 999 days. **Check Password:** When selected, compares the password that is stored in Password Safe with the password on the managed system. **Reset Password on Mismatch:** Use with **Check Password**. The password on the managed account is reset if a mismatch is detected. If this option is not enabled, and a mismatch is detected, a notification email is sent to the system contact email address (if set up on the managed system). **Change Password After Release:** Select this option to require the password be changed after every release. **ISA Release Duration:** Select the duration for password releases to ISA users, up to a maximum of 365 days. This is the amount of time that transpires between the initial ISA user password retrieval and the automatic reset of the password (if enabled).
API Enabled	Select this option if the managed account will be accessed by the Password Safe API methods.
Use Own Credentials	Password Safe uses the current password on the managed account to log on to the managed system to change the password. Enable this option to use the managed account rather than the functional account to change the password.
Release Notification Email	When there is a password release request, an email is sent to the email account provided here.
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** box is checked for the access policy. For more information on force termination, please see "Create an Access Policy" on page 9.
Max Release Duration	The maximum length of time that 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.

Max Concurrent Requests	Select the maximum number of concurrent password requests for the managed account. When configuring a managed account you can set the number of password requests that can be made by the requester at one time. Enter **0** for unlimited concurrent requests. The default value is **1**. The following platforms support concurrent password requests: Windows, Unix, Database, and Cloud.
Scan Credential Description, **Scanner Key**, **Confirm Scanner Key**	A managed account can be used as a credential when configuring a network security scan. For more information, please see "Managed Accounts" on page 43.
Applications	Select the application that the managed account can access. For more information, please see "Add Applications to Password Safe" on page 76.

Settings Specific to Unix, Linux, macOS

Setting	Description or Action
Authentication Type	Select **Password** or **DSS**. If you want to use DSS authentication, please see "Set DSS on the Managed Account" on page 54.
Allow Fallback to Password	The **Authentication Type** of **DSS** needs to be selected for this option to be active. The password on the managed account is then used if the DSS key method fails.
Login Account for SSH Sessions	This option must be enabled on the managed system for this option to be available for the managed account. This option will allow the system to log into the SSH session by bypassing the functional account.

Add Managed Systems Using a Smart Rule

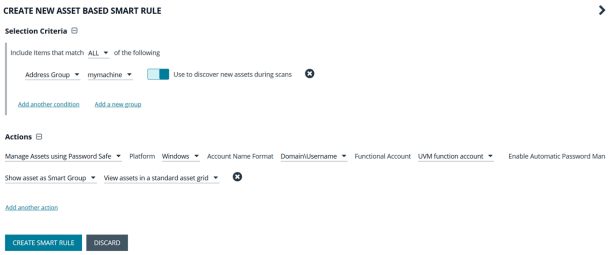
You can add assets to Password Safe using an asset based smart rule.

***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. In the console, click **Configuration**.
2. Under **General**, select **Smart Rules**.
3. From the **Smart Rule Type filter** dropdown list, select **Asset**.

4. Click **Create Smart Rule +**.
5. Select a **Category** from the dropdown list.
6. Enter a **Name** and **Description** for the smart rule.
7. Select a **Reprocessing Limit** from the dropdown list.
8. Set one or more **Selection Criteria**.
9. Select the filter criteria. Address groups are very useful here.
10. In the **Actions** section, select **Manage Assets Using Password Safe** from the list.
11. Select the platform, functional account, and other settings. The settings are the same as when you add the system manually.



> For complete descriptions, please see "Add a Managed System Manually" on page 31.

12. In the **Actions** section, click **Add Another Action**.
13. Select **Show asset as Smart Group** from the list. This is helpful for grouping assets and accounts by regions.
14. Click **Create Smart Rule**.

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. In the console, click **Configuration**.
2. Under **General**, select **Smart Rules**.
3. From the **Smart Rule type filter** list, select **Managed Account**.
4. Click **Create Smart Rule**.
5. Select the filter criteria:
    - **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 Directory Query from the menu or create one.
        - Enter the frequency that the query runs. Leave the entry as **0** for a one time run.
        - Check the box to discover accounts when the smart rule processes.
        - Select a domain.
    - **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 will be 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 **User Account Attribute**, and then select an attribute filter:
  - **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.

***Note:** For every filter, select **Yes** to discover accounts, and then select a smart group to search in.*

6. Select **Discover accounts for Password Management**.

***Note:** This option is available only for **Directory Query** and **User Account Attribute** filters.*

7. 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.

For complete descriptions, please see "Add a Managed Account Manually" on page 34.

8. Additional properties can be set under **Actions**:

- **Assign workgroup on each account:** Used with agent workgroups in multi-active deployments, this action allows 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 will be 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 will contain a summary of the results the managed accounts matched by the smart rule and any changes since its last execution.
- **Set attribute 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. Select **Show managed account as Smart Group**.
11. Click **Create Smart Rule**.

Work with Managed Systems

A managed system is any system that is managed by Password Safe. All managed systems can be viewed on the **Managed Systems** page, by selecting the built-in smart group **All Managed Systems** from the **Smart Group** menu in the console.

Set the Account Name Format within the Managed Assets using Password Safe Action

You can set the user account format when adding the following platforms as a managed system:

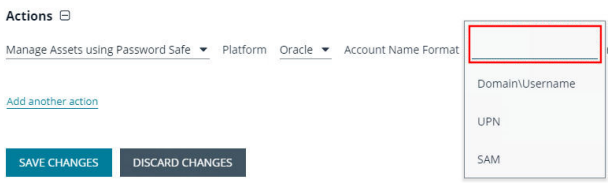
- Windows
- Linux
- Oracle
- MS SQL Server
- Active Directory

The following format types are supported:

- **Domain\Account name:** Enter the domain and user account name
- **UPN:** Uses the format **xxx@DomainName**
- **sAMAccountName:** Uses the Active Directory **sAMAccountName**

When you add managed systems using an asset-based smart group, the **Account Name Format** setting is available when a supported platform is selected.

If the smart group already exists, you must remove the managed assets using Password Safe, then add the assets again before you will see the **Account Name Format** setting.



Import an SSH Server Key Using a Smart Rule

You can import SSH Server keys from a host and accept the key on the **Managed System Advance Details** page.

Supported key types are RSA, DSA, and ECDSA.

1. Navigate to the **Configuration > General > Smart Rules** page.
2. Within the smart rule filter, select **Asset**, and then click **Create New Smart Rule**.
3. Enter a name, description, and category.
4. Create the filter settings. For example, select an address group that includes the IP addresses for the hosts.
5. In the **Perform Actions** section, select **Manage Asset Using Password Safe**.

> 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 31.

6. Select a key enforcement mode: **Auto Accept Initial Key** or **Manually Accept Keys**.
7. Click **+** to add another action, and then select **Show Asset as Smart Group**.
8. Click **Save**.

Manage the SSH Server Keys

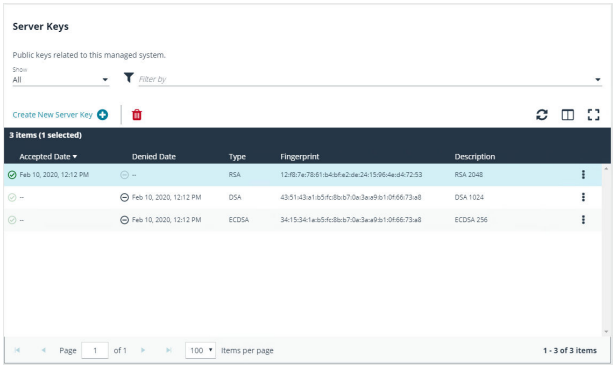
After the smart rule processes, hosts with SSH server keys are populated in the smart group you created.

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 on the **Configuration** page. Please see "Customize Mail Templates" on page 25.

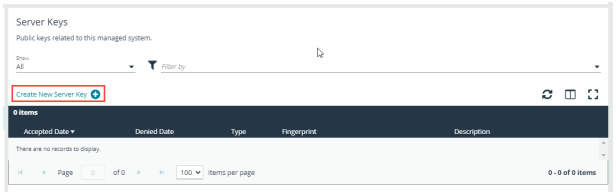
Accept or Deny a Key:

1. In the BeyondInsight console, go to the **Managed Systems** page.
2. Select the managed system from the grid, and then click the vertical ellipsis at the right end of the line.
3. Select **Go to advanced details...**.
4. Select the **Server Keys** tab.
5. Within the **Server Keys** table, select the server key you wish to work with.
6. From the Server Keys action (vertical ellipsis):
    - If auto approved, no further action is required.
    - If manually approved, click **Accept** or **Deny**.
7. 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. In the BeyondInsight console, go to the **Managed Systems** page.
2. Select the managed system from the grid, and then click the vertical ellipsis at the right end of the line.
3. Select **Go to advanced details...**
4. Select the **Server Keys** tab.
5. From the **Server Keys** table, click the **Create New Server Key** button.
6. Select a key type. Enter a **Fingerprint** and a **Description**.
7. Click the **Create Key** button.
8. After a key is added, from the **Functional Accounts** tab, click the **Test Functional Account** button to verify the key with the functional account.



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

View the BeyondInsight Details of an Asset-Linked Managed System

You can view the Asset details, such as hardware, ports, processes, scheduled tasks, and smart groups associated with the asset.

1. In the BeyondInsight console, go to the **Assets** page.
2. Select an asset from the grid.
3. Click the vertical ellipsis at the right end of the line.
4. Select **Go to advanced details...**
5. Click through the tabs to view more details on each topic.

View the Standalone Managed Systems Details

You can view the managed system details, such as managed accounts, smart groups, linked accounts, server keys, functional accounts, and login accounts associated with the managed system.

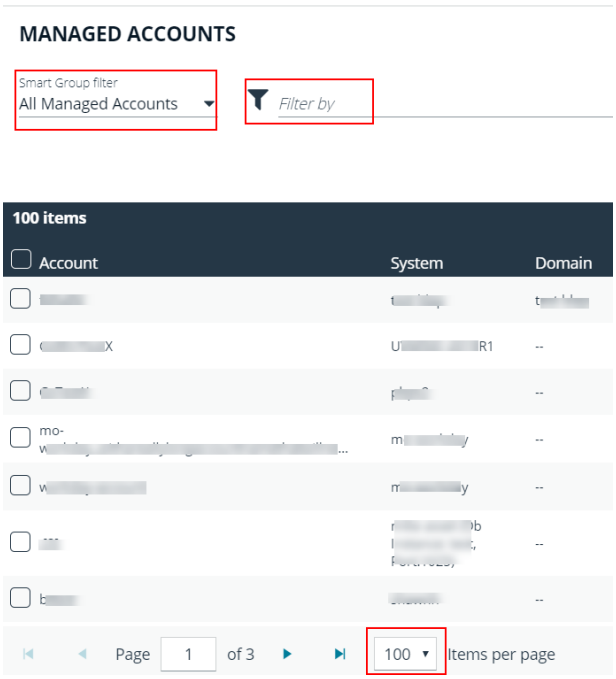
1. In the BeyondInsight console, go to the **Managed Systems** page.
2. Select a managed system from the grid.
3. Click the vertical ellipsis at the right end of the line.
4. Select **Go to advanced details...**
5. Click through the tabs to view more details on each topic.

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.



View Managed Account Details

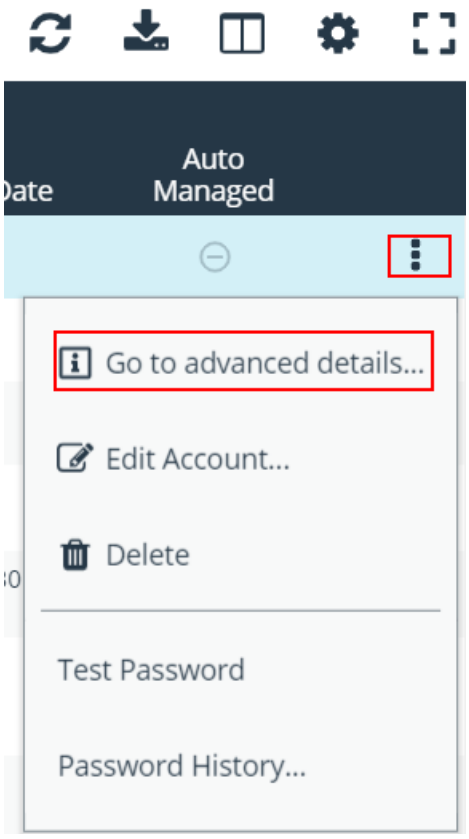
After the account is added to Password Safe management, you can:

- Review the settings assigned to the account.
- View a list of password changes and the reason for the change.
- See which accounts are synced to the managed account.
- View smart groups associated with the account, along with their last process date and processing status.

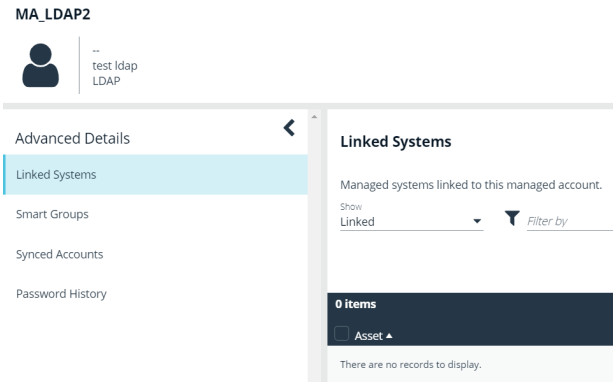
To view details on a managed account:

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

2. Select a managed account, and then click the **More Options** button.
3. Select **Go to advanced details** from the list.



4. Select each item under **Advanced Details** to view more information about managed systems linked to the account, smart groups, synced accounts, and password history for the managed account.

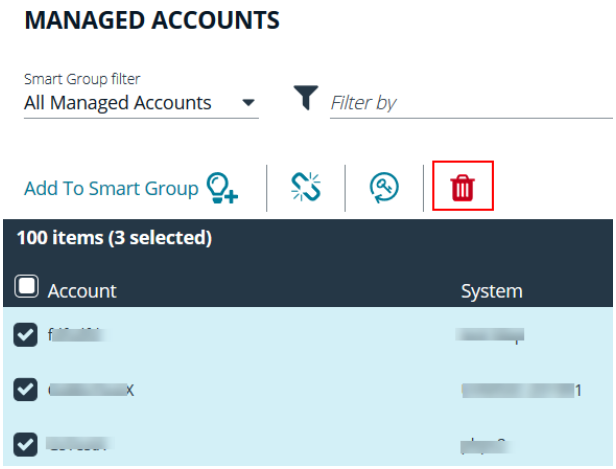


Delete Managed Accounts

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.

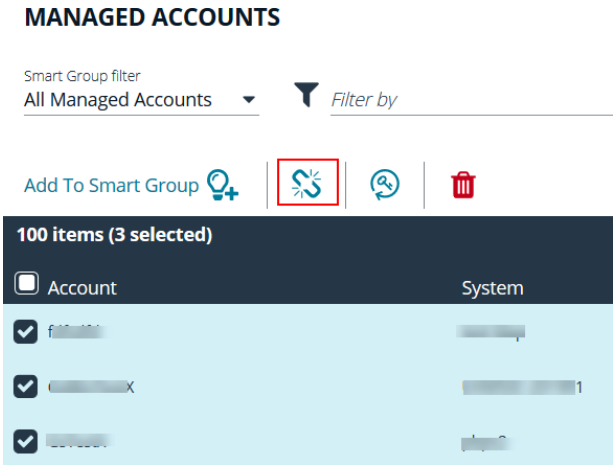


3. Click **Delete** on the confirmation message.

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.

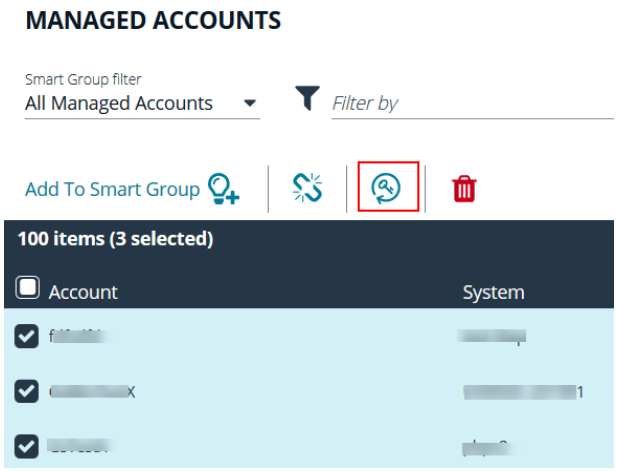


3. Click **Unlink** on the confirmation message.

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 will 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 master account and all of its subscribers to a new password.

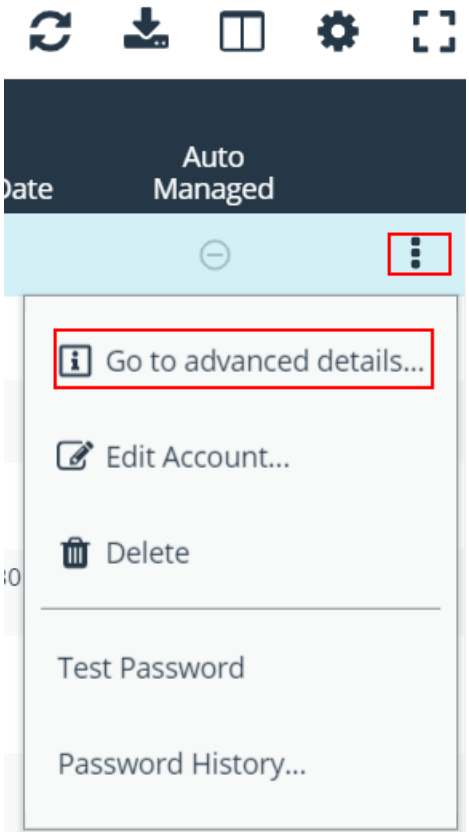
Once an account is synchronized as a subscriber account, settings modifications are limited to:

- Enable API
- Allow for use by Network Security Scanner
- Application

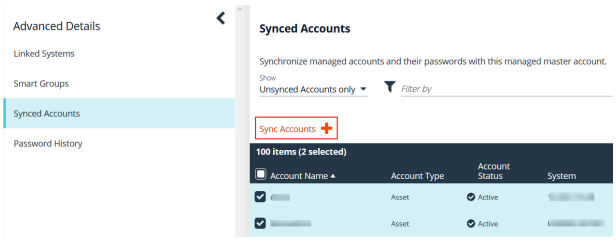
To sync an account:

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

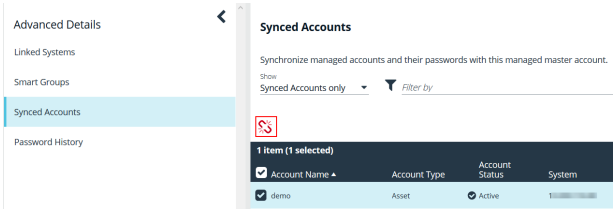
2. Select a managed account, and then click the **More Options** button.
3. Select **Go to advanced details**.



4. Under **Advanced Details**, select **Synced Accounts**.
5. Select the account or multiple accounts that you want to sync.
6. Click **Sync Accounts**.



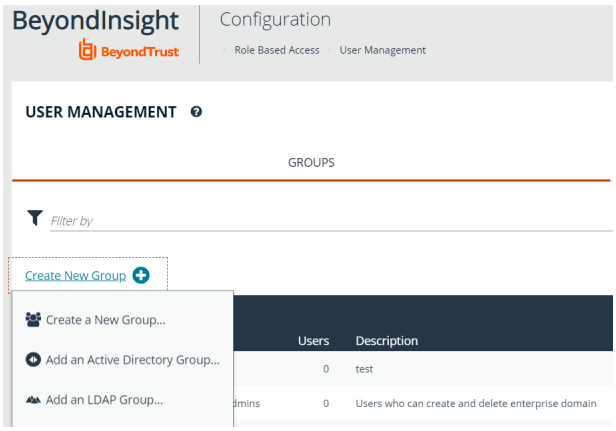
7. To remove a synced account, select the account, and then click the **Unsync Accounts** button above the grid.



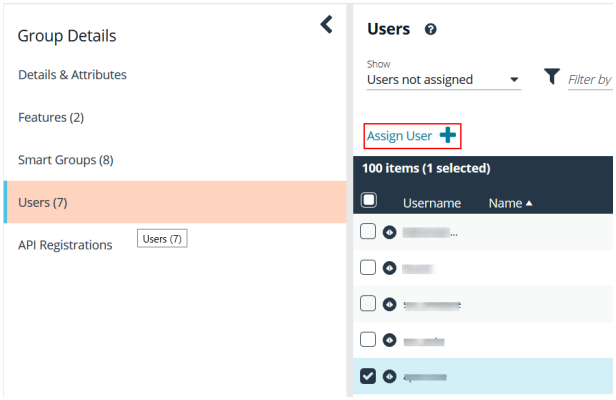
Configure Password Reset for Managed Account Users

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.

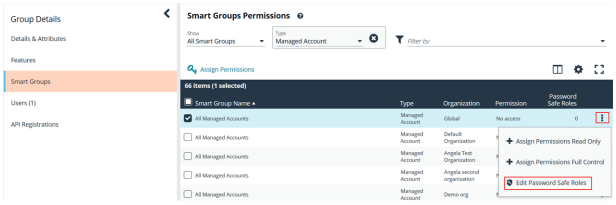
1. In the BeyondInsight console, go to **Configuration > Role Based Access > User Management**.
2. Under **Groups**, click **Create New Group**.

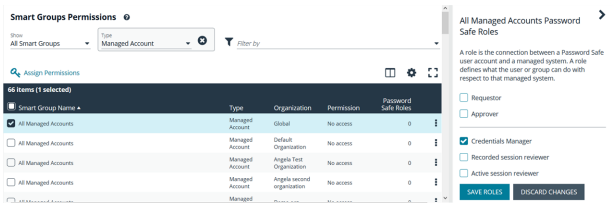


3. Select **Create a New Group**.
4. Provide a name and description for the group, and then click **Create Group**.
5. From the **Group Details** pane, select **Users**, and then assign users to the group.



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 **More Options** button, and then select **Edit Password Safe Roles**.
13. Select the **Credentials Manager** role, and then click **Save Roles**.





The managed account user can now log into 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 **More Options** button.
4. Select **Change Password**.

Use a Managed Account as a Network Scan Credential

A managed account can be used as a credential when configuring a network security scan.

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

The following credential types are supported:

- Windows,
- SSH
- MySQL
- Microsoft SQL Server.

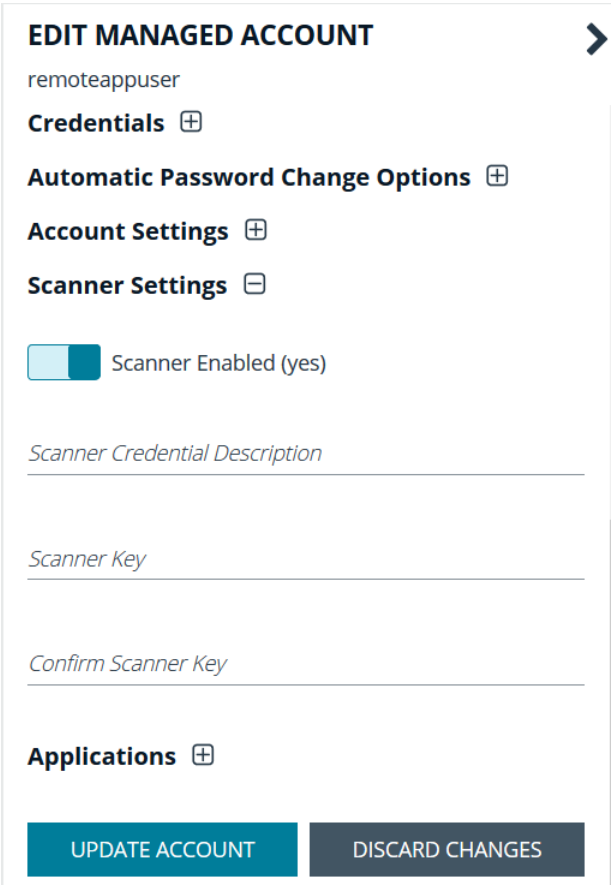
The following platforms are supported:

- 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. Go to the **Managed Accounts** page.
2. Select the managed account, and then click the **More Options** button.
3. Select **Edit Account**.

4. Expand **Scanner Settings**.
5. Click the slider to enable the scanner.
6. 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.
7. Assign and confirm a key so that only users that know the key can use the credential for scanning.
8. Click **Update Account**.

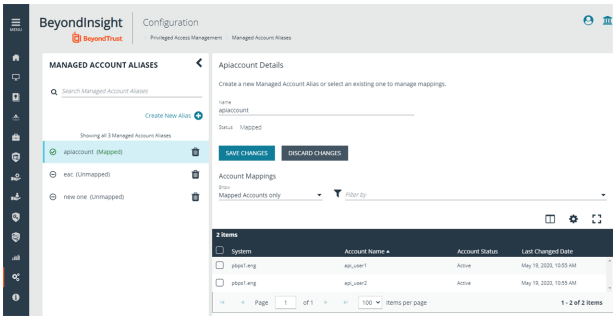


Managed Account Aliasing

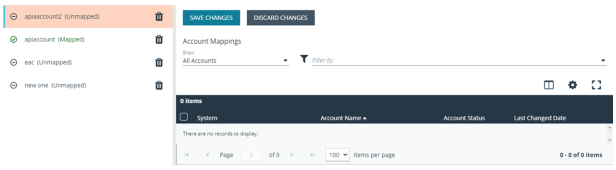
Aliases are accessible using the API only. Account mappings can be changed without affecting the alias name. At least one managed account is required to be mapped for the alias to be active; when an alias has two or more managed accounts mapped, it is considered to be highly available. An account can 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. In the BeyondInsight console, go to **Configuration > Managed Account Aliases**.
2. Click **Create New Alias**.
3. Enter a name, and then click **Create Alias**.



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

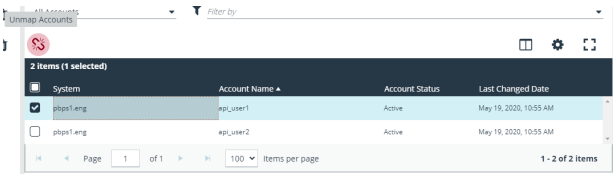


> ***Note:*** *Each managed account can only be mapped to a single alias.*

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

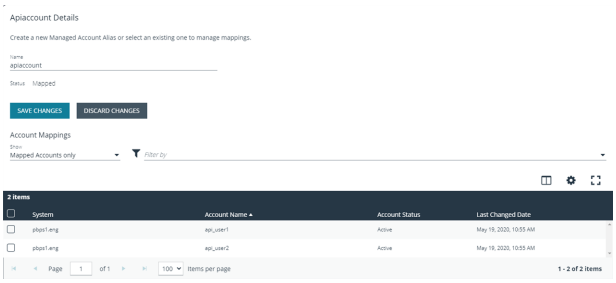
The **Filter-by** allows you to filter accounts by **System**, **Account Name**, **Account Status**, or **Last Changed Date**.

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



Mapped accounts have three status values:

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



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

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, RACF.

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.

The following example shows how to generate a 2048-bit RSA key pair with ssh-keygen. The user account that will be 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.

For more information, please see "Generate and Distribute the Key" on page 52.

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**.

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

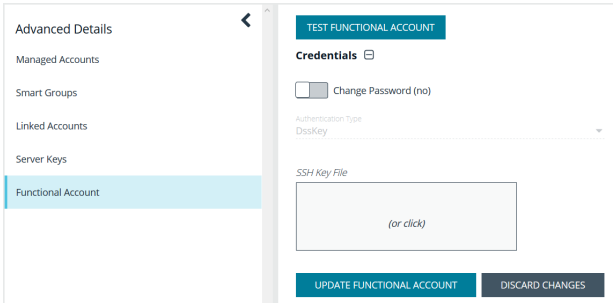
```
functional_account ALL=(ALL) NOPASSWD: /usr/bin/grep, /usr/bin/pwdadm, /usr/bin/tee,
/usr/bin/passwd, /usr/bin/sed, /usr/bin/cp, /usr/bin/rm
```

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**.



Set DSS on the Managed Account

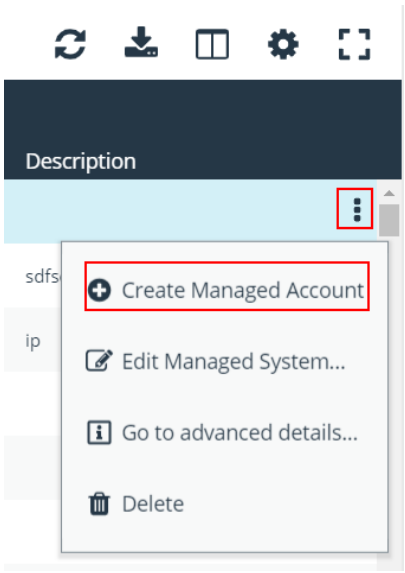
An alternate and secure way to set up a managed account is with DSS authentication.

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.

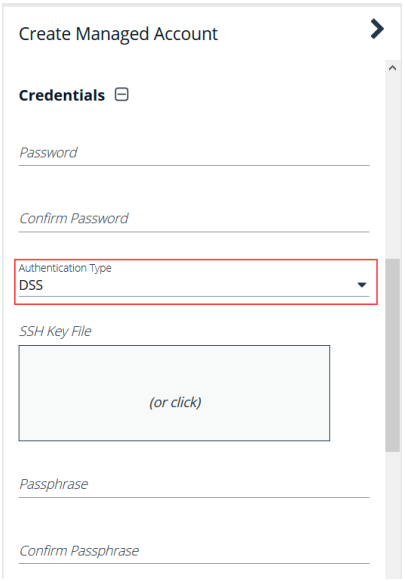
For more information, please see "Generate and Distribute the Key" on page 52.

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**.



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

For more information on configuring managed accounts, please see "Managed Accounts" on page 43

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.

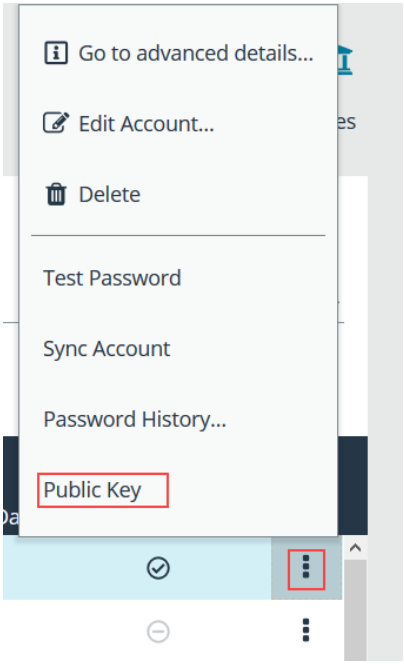
Generating a new DSS public/private key pair will remove the old public key (if there is one) from the **authorized_keys** file and append the new public key.

For more information, please see "Create a DSS Key Policy" on page 56.

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 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 that you need to configure, such as listen host and screen resolution.

Configure Listen Host and File Location

Using the BeyondInsight Configuration tool, you can set the listen host and file location for the monitored sessions.

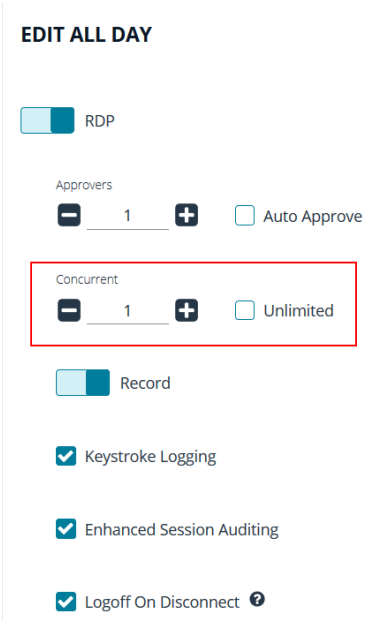
1. Open the BeyondInsight Configuration tool.
2. Go to the **Password Safe** section.
3. Enter the IP address for the listen host.
4. Set the location for the session monitoring file. The default location is in the installation directory **\data\sessionmonitoring**.

Configure Concurrent Sessions

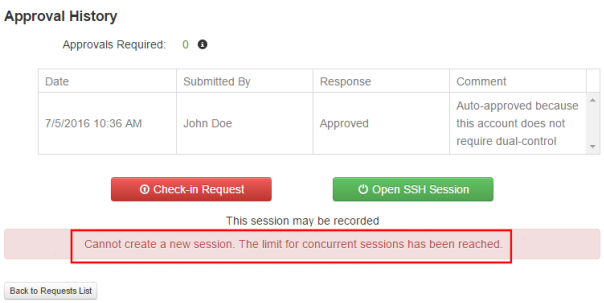
Remote sessions can be limited to a set number of concurrent sessions.

The option to increase or limit the number of sessions a user can open at one time is configured in access policies, when setting the schedule.

For more information, please see "Create an Access Policy" on page 9.



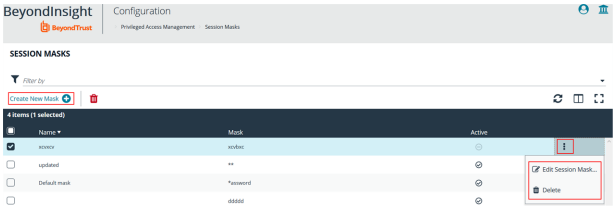
If a user tries to open more sessions than allowed, a message is displayed on the **Requests** page.



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 will check the keystrokes against the mask. Any matches are replaced. When the keystroke session is replayed, the viewer sees the 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. In the BeyondInsight console, go to **Configuration > Privileged Access Management > Session Masks**.
2. To create a mask:
    - Click **Create New Mask**.
    - Enter a name for the mask and the mask pattern.
    - Check the **Active** option.
    - Click **Create Session Mask**.
3. To edit a mask:
    - Click the **More Options** icon for the mask, and then select **Edit Session Mask**.
    - Edit the name for the mask or the mask itself.
    - Check or uncheck the **Active** option as appropriate.
    - Click **Update Session Mask**.
4. To delete a mask, click the **More Options** icon 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.

IMPORTANT!

You must clear the browser cache to see new images after they have been updated. Also, all image files should be backed up in a safe location because they will be overwritten on the next upgrade and must be replaced after the upgrade completes to restore the customization.

Customize 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 x 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.

Customize Replay Images

To customize the **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 x 125px*

- **C:\Program Files (x86)\eEye Digital Security\Retina CS\website\images\rdp-placeholder-lg.jpg**

  Note: *Size must be 1024 x 768px*

- **C:\Program Files (x86)\eEye Digital Security\Retina CS\website\images\ssh_placeholder.jpg**

  Note: *Size must be 137 x 125px*

Customize 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 x 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.

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 it was created on.

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

From the **Global Settings > Session Monitoring** configuration, you can turn off keystroke logging for ISA users and admin sessions.

Keystroke logging can be enabled for all other users when setting the scheduling options for an access policy.

1. In the BeyondInsight console go 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**.

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. In the BeyondInsight console, go 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:

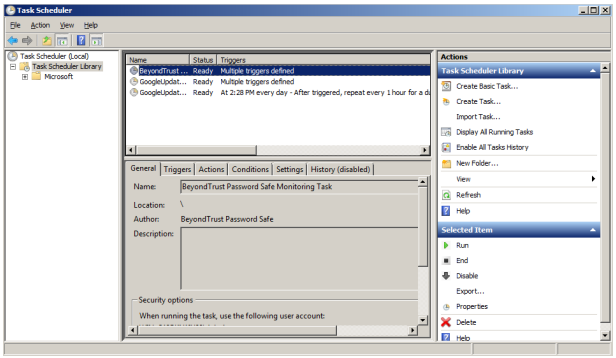
```
2017/03/07 15:47:12.186 2292 6548 INFO: Pushing pbpsdeploy service to 10.200.28.39 as user
backupadmin
2017/03/07 15:47:13.528 2292 6548 INFO: Starting pbpsdeploy service on 10.200.28.39 as user
backupadmin
2017/03/07 15:47:13.593 2292 6548 INFO: Copied pbpsmon.cab

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**.



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

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

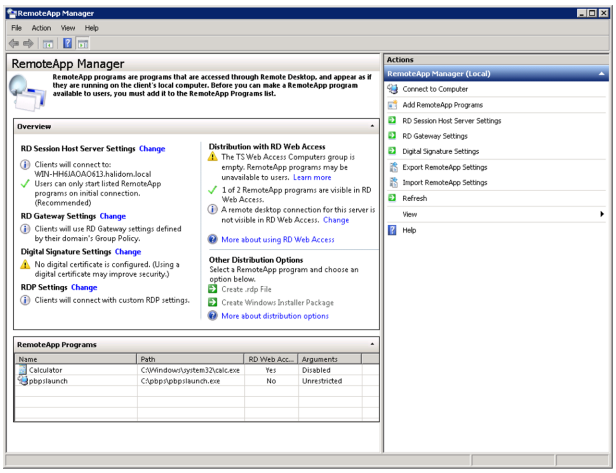
pbpslaunch

Verify the following setup has been performed by the deployment service:

- In regedit, the following registry key is created:

  HKLM\Software\Microsoft\Windows NT\CurrentVersion\TerminalServer\TSAppAllowList\Applications\pbpslaunch

- A **pbpslaunch** entry exists in RemoteApp Manager.



- Locate thelog 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 disable* ***pbpsmon*** *and* ***pbpslaunch*** *by adding the following registry value on the UVM and restarting the* ***Session Monitoring*** *service.*
>
> ```
> HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\rdp_proxy\disable_deploy = 1
> ```

Configure Algorithms used by the Session Monitoring Proxy

The set of encryption algorithms and MAC algorithms that may be used by Password Safe is configurable using registry keys:

- **HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/BeyondTrust/PBPS/SessionManager/ssh_proxy/ciphers**
- **HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/BeyondTrust/PBPS/SessionManager/ssh_proxy/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. The restriction applies both to the algorithms used between the client and Password Safe, and to the algorithms used between Password Safe and the managed system.

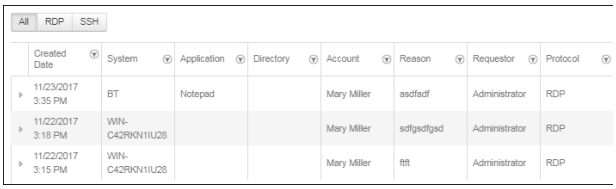
Manage Recorded Sessions

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. In the console, click **Menu**, and then click **Replay** under **Password Safe**.
2. Click **All**, **RDP**, or **SSH** to find the recording.
3. Select a recorded session. A thumbnail is displayed with session details.
4. Click **Open**, then **Play**, to review the recording. The recorded session opens in a new window with standard video viewing options.



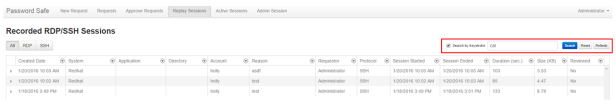
   You can hover over any part of the video progress bar to reveal the time stamp and click anywhere on the bar to select an instance in the recorded session.

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

Use Keystroke Search

To find sessions containing keystrokes:

1. Select the **Search by keystrokes** check box and 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.



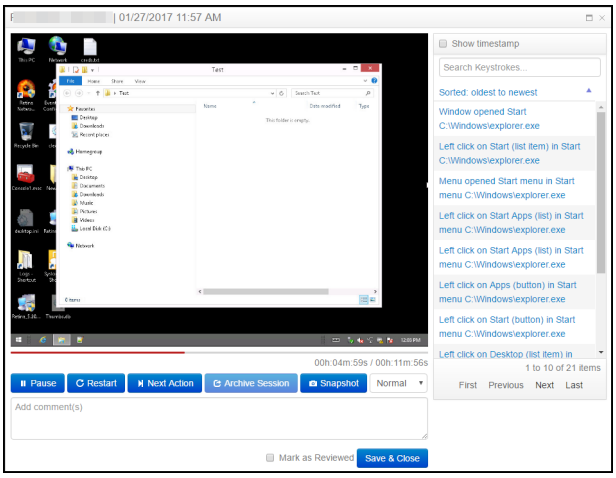
Export a Session Frame

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

Click the **Snapshot** button.

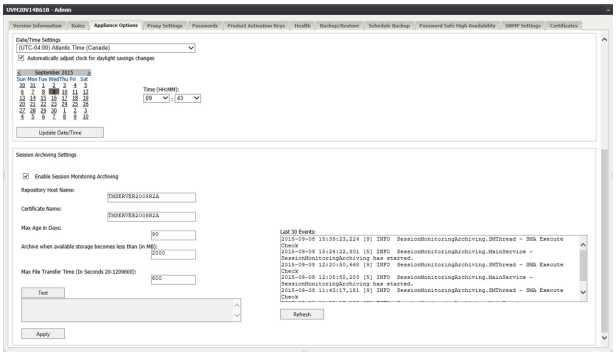
The JPEG file is automatically saved to your default download location specified in your browser settings.

A notification is displayed when the export is complete.



Archive Recorded Sessions

You can archive recorded sessions. Archive settings are configured on the UVM appliance.



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

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

View and Restore Archived Sessions

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

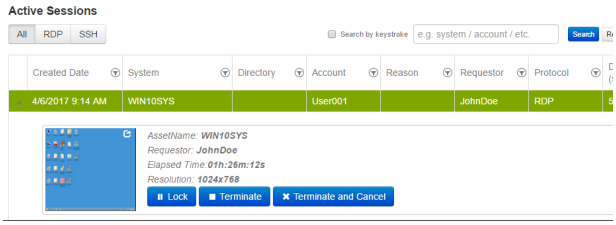
1. Open the session by clicking **Open**.
2. Once the viewer opens, click **Archive Session**.
3. Select the archived session.
4. Click **Restore Session** to restore the session.

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.

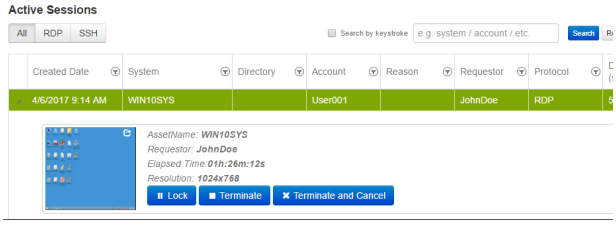
1. Log into the web portal.
2. Click **Menu** and then click **Active Sessions**.
3. Select a session.
4. Click the thumbnail to open the session in a larger window.



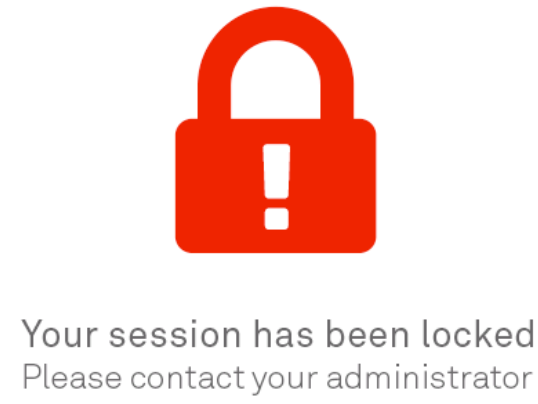
Lock an Active Session

1. Log into 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.

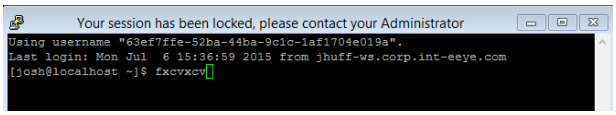
   The message displayed to the user is different for RDP and SSH sessions. See the examples below.



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



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

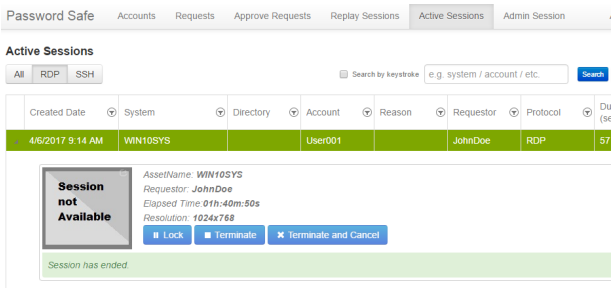


5. Click the **Unlock** button to unlock the session.

***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 into 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.



***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 will automatically close and be removed from the **Active Sessions** table. The session will then be available to view in **Replay Sessions**.*

Terminate and Cancel an Active Session

1. Log into 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, Windows Service accounts, Scheduled Task accounts, and IIS Application Pools accounts.

Add a Directory

1. From the 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 31

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 **More Options** button.

***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**.

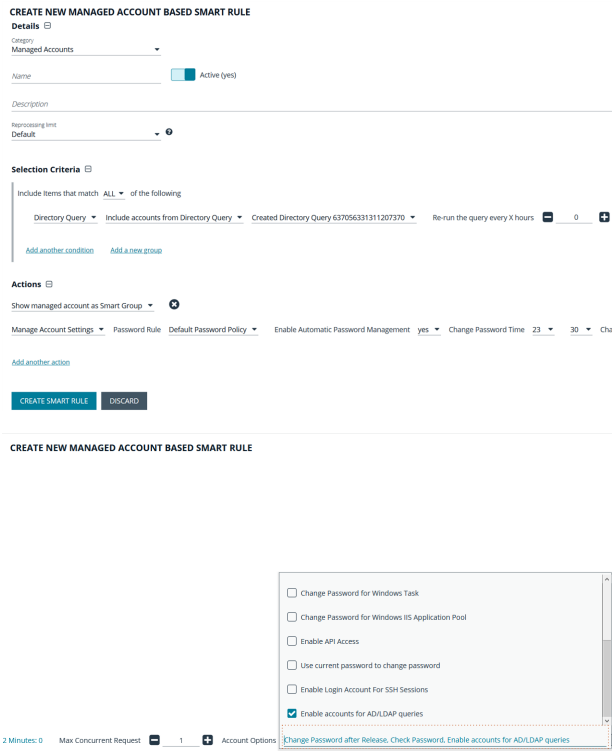
***Tip:** When configuring the managed account settings for an Active Directory account, you can choose a Domain Controller to change or test a password. The Domain Controller on the managed account will override a Domain Controller on the functional account selected.*

For more information on adding managed accounts manually, please see "Add a Managed Account Manually" on page 34

Discover Active Directory Accounts with an Active Directory Query

1. From the menu, select **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule type filter** list.
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



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 will auto manage the directory account passwords. If this is not desired, set **Enable Automatic Password Management** to **No**; otherwise, ALL accounts in the query will have passwords changed.*

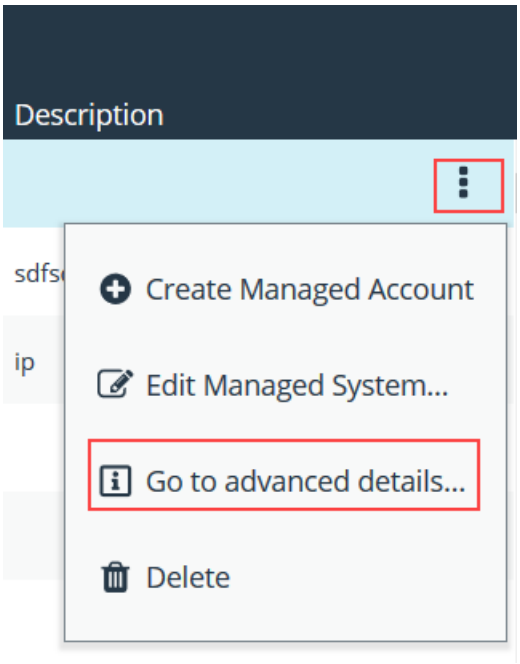
8. Click **Create Smart Rule**.
9. To view the Active Directory accounts, go the **Managed Accounts** page, and then select the newly created smart group from the **Smart Group filter** list.

Link Active Directory Accounts to Managed System

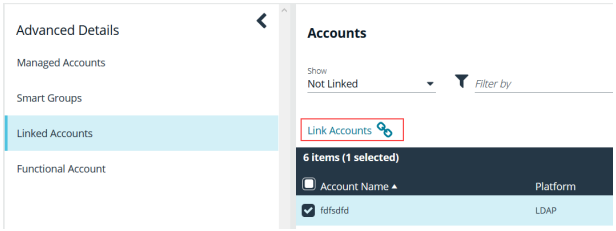
You can link Active Directory accounts to managed systems on a specified domain.

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

2. Select the managed system, and then click the **More Options** icon.
3. Select **Go to advanced details**.



4. Under **Advanced Details**, select **Linked Accounts**.
5. Filter the list by **Not Linked**.
6. Select the accounts, and then click **Link Accounts**.



Create an Active Directory Functional Account

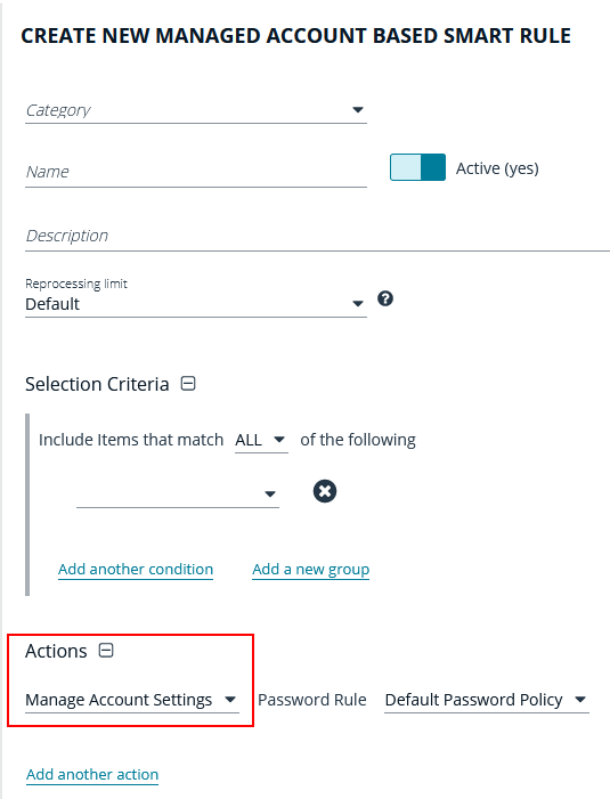
When creating an Active Directory managed account, the functional account requires a domain controller. Administrators can choose a targeted domain controller from the menu, or select **Any Domain Controller**, which allows Active Directory to choose.

Note: *If a failure occurs when connecting to a target Domain Controller, Password Safe will connect at the domain level.*

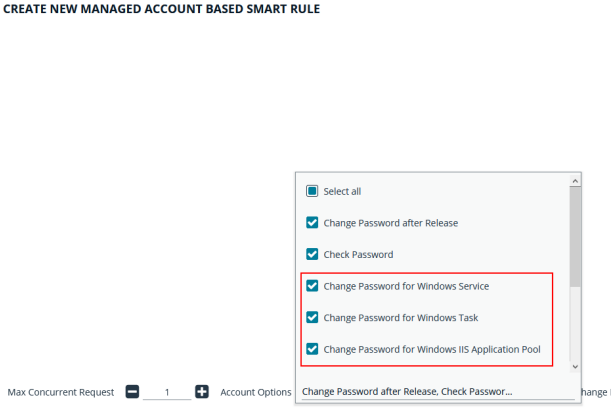
Add Windows Service, Task Scheduler, and IIS Application Pool Accounts to Password Safe Management

Password Safe allows you to manage the credentials that are used for services, scheduled tasks, and IIS application pools in Windows. Accounts that are used to run services, scheduled tasks, and IIS application pools can be added as managed accounts in Password Safe. When their passwords are changed by Password Safe, the credentials are updated in any services, scheduled tasks, and IIS application pools that are associated with the managed account, if these options are enabled under **Account Settings** on the managed account.

These options are also available when creating a managed account smart rule by selecting **Manage Account Settings** under **Actions**, and then checking the appropriate **Account Options**:



- **Change Password for Windows Service**
- **Change Password for Windows Task**
- **Change Password for Windows IIS Application Pool**



Manage Windows Service Accounts

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, be sure to:

- Start the remote registry service on the target.
- Start the UPnP (Universal Plug and Play) Device Host service on the target.
- Start the SDPP (Service Directory Placement Protocol) Discovery 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 a service account to Password Safe management.

Prepare the Service

1. On the asset where the service reside, 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 login.
4. Restart the service to verify it starts successfully.

Run a Scan on the Service Assets

1. In the BeyondInsight console, click **Scan** to run a **Detailed Discovery Scan** against the target systems to add the systems as assets in BeyondInsight. The detailed scan will collect data for the services for the targets.
2. Add the discovered assets to Password Safe management.
3. Verify the following:
    - From the **Assets** page, click the **More Options** icon for the asset, and then select **Open Asset Details Report** to confirm the services were collected, the log service status is **running**, and the login account name is correct.
    - From the **Managed Systems** page, click the **More Options** icon for the asset, and then select **Edit Managed System** and verify that **NetBIOS Name** is entered. It must be a fully qualified domain name (FQDN) if a domain account is used.
4. From the **Managed Accounts** page, click the **More Options** icon for the managed account associated with the service, and then select **Edit Account**. Under **Account Settings**, ensure the **Change Services** and **Restart Services** options are enabled.
5. Click **Update Account**.
6. From the **Managed Accounts** page, click the **More Options** icon for the managed account associated with the service, and then select **Test Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.
7. From the **Managed Accounts** page, click the **More Options** icon for the managed account associated with the service, and then select **Change Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.
8. 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.
- Start the UPnP (Universal Plug and Play) Device Host service on the target.
- Start the SDPP (Service Directory Placement Protocol) Discovery 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 **Scan** to run a **Detailed Discovery Scan** against the target systems to add the systems as assets in BeyondInsight. The detailed scan will collect data for the scheduled tasks for the targets.
2. Add the discovered assets to Password Safe management.
3. Verfiy the following:
    - From the **Assets** page, click the **More Options** icon for the asset, and then select **Open Asset Details Report** to confirm the scheduled tasks were collected and the login account name is correct.
    - From the **Managed Systems** page, click the **More Options** icon for the asset, and then select **Edit Managed System** and verify that **NetBIOS Name** is entered. It must be a fully qualified domain name (FQDN) if a domain account is used.
4. From the **Managed Accounts** page, click the **More Options** icon for the managed account associated with the scheduled task, and then select **Edit Account**. Under **Account Settings**, ensure the **Change Scheduled Tasks (yes)** option is enabled.
5. Click **Update Account**.
6. From the **Managed Accounts** page, click the **More Options** icon for the managed account associated with the scheduled task, and then select **Test Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.
7. 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:

- A IIS application pool that is running restarts when the password is changed.
- A 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.
- Start the UPnP (Universal Plug and Play) Device Host service on the target.
- Start the SDPP (Service Directory Placement Protocol) Discovery 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 **Scan** to run a **Detailed Discovery Scan** against the target systems to add the systems as assets in BeyondInsight. The detailed scan will collect 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, click the **More Options** icon for the asset, and then select **Open Asset Details Report** to confirm the IIS application pools were collected and the login account name is correct.
    - From the **Managed Systems** page, click the **More Options** icon for the asset, and then select **Edit Managed System** and verify that **NetBIOS Name** is entered. It must be a fully qualified domain name (FQDN) if a domain account is used.
4. From the **Managed Accounts** page, click the **More Options** icon for the managed account associated with the IIS application pool, and then select **Edit Account**. Under **Account Settings**, ensure the **Change IIS Application Pools (yes)** option is enabled.
5. Click **Update Account**.
6. From the **Managed Accounts** page, click the **More Options** icon for the managed account associated with the IIS application pool, and then select **Test Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.
7. From the **Managed Accounts** page, click the **More Options** icon for the managed account associated with the IIS application pool, and then select **Change Password**. A slide-out status message with the results of the change attempt is displayed at the bottom of the page.

Add Applications to Password Safe

Applications can be managed by Password Safe. Requesters can then request access to the 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 Application**.
3. Enter a name for the application. It is recommended to use the name of the application for transparency.

   The following are optional categorization fields:

   - **Version**
   - **Publisher**
   - **Type**
   - **Parameters:** The arguments to pass to the application. 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**
   - **Functional Account:** Select a functional account from the menu. The functional account must already be created.
   - **Managed System:** The managed system must have the application (such as **wordpad.exe**) configured. When starting an application session, an RDP session connects to this application server and starts the application.
   - **AutoIt Passthrough:** Check this box 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.

   The following fields are required:

- **Alias:** Combines the name and version entered by default, but can also be edited to display any desired alias.
- **Application/Command:** The path to the application. For example, **C:\Program Files\Windows NT\Accessories\wordpad.exe**.

> ***Note:*** *If **Functional Account** is set, then **Managed System** is required.*

4. Administrators can associate the application with a linked Windows system or a linked Linux or Unix system. By default, the boxes are not checked; this 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.
    - **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.
    - **Associate the Application with a linked Linux/Unix system:** Standard users see all Linux and Unix-based systems applied with the Domain Linked Account. This excludes Windows systems.
    - If both options are enabled, 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.*

5. Select **Active** to make the application available for remote sessions.
6. Click **Create Application**.

> There are prerequisites that must be met before you can use **AutoIt Passthrough**. For more information, please see "Use AutoIt Passthrough" on page 79.

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**.

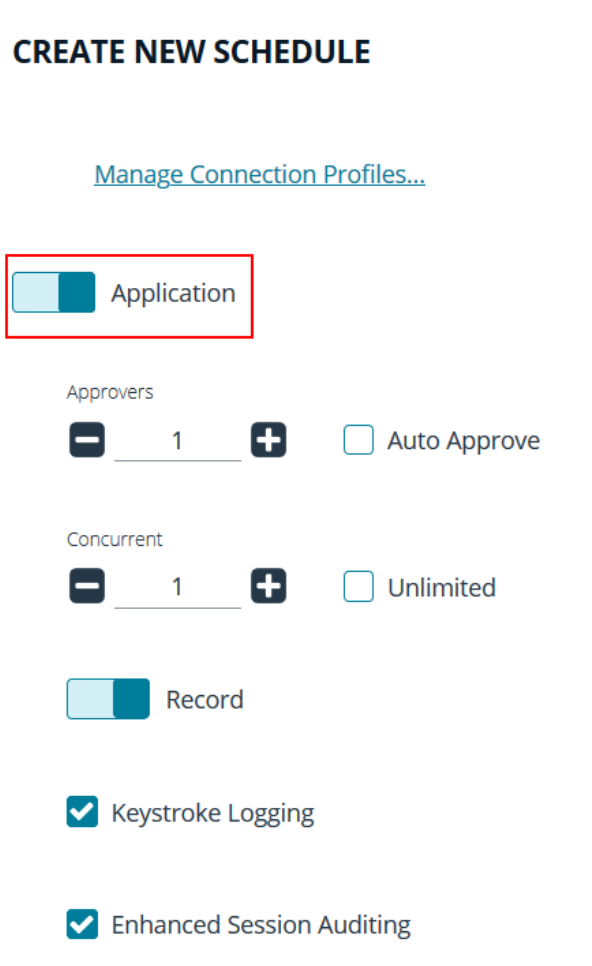
You can select the application by editing the managed account. For more information about managed accounts settings, please see "Add a Managed Account Manually" on page 34.

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 and enable the **Application** policy type for the schedule, 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 9.

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 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 thePassword Safe Passthrough library through **pbpspassthru.dll** (provided as part of the Password Safe Resource Kit).

> For information about turning on the feature, please see "Add an Application" on page 76.

AutoIt Script Details

The AutoIt example script uses the following functions:

- **pbpspassthru.dll**
- **pbps_get_credentials**
- **DLLCall**: An AutoIt function. The first argument takes in the location of the dll to call. In the example, the **pbpspassthru.dll** is located in the same directory as the AutoIt script.

Example:

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

pbps_get_credentials Function

```
char* pbps_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 need to know the SAP instance number.
- **Client ID:** An ID that is unique to that 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.

Please see "Create a Functional Account" on page 30.

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.

Please see "Add a Managed System Manually" on page 31.

Change Passwords for SAP Managed Accounts

The password for managed accounts can be changed only once a day. The current password is required to change the password.

If you try to change the password more than once a day, a message is displayed indicating that the password cannot be changed.

Add a Cloud Application

Applications can be configured for cloud applications. Requesters can request access to specific cloud sites and launch a session through the Password Safe web portal. The sessions can be recorded and monitored live or watched at a later date.

> ***Note:*** *Before configuring a cloud account, you must set up a functional account.*
>
> *Additionally, Microsoft 365 requires that both* ***Microsoft Online Service Sign-in Assistant for IT Professionals RTW*** *and* ***Azure Active Directory Module for Windows PowerShell*** *be downloaded and installed before managing an* ***Microsoft 365 Account*** *in Password Safe.*
>
> *To install the* ***Azure Active Directory Module for Windows PowerShell*** *see Connect with the Microsoft Azure Active Directory Module for Windows PowerShell at https://docs.microsoft.com/en-us/microsoft-365/enterprise/connect-to-microsoft-365-powershell?view=o365-worldwide#connect-with-the-microsoft-azure-active-directory-module-for-windows-powershell and note the following:*
>
> *Step 1.2,* ***Install-Module MSOnline****, requires a TLS 1.2 connection. To enable this, in the Admin PowerShell session first run this Powershell command:*
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```
>
> *Then install the module:* ***AzureAD****.*

The following cloud applications are supported:

Amazon Web Service	Azure
Box	Dropbox
Facebook	GoGrid
Google	Instagram
LinkedIn	Microsoft 365
Pinterest	Rackspace
Salesforce	Twitter
Workday	XING

To configure a cloud application:

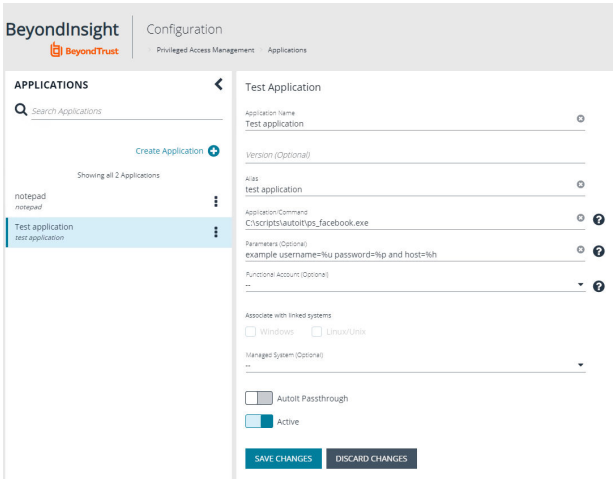
1. Select **Configuration**.
2. Under **Privileged Access Management**, click **Applications**.

3. On the **Applications** page, click **Create Application**.
4. Enter a name for the application. We recommend using the name of the application for transparency. The following are optional categorization fields: **Version**, **Publisher**, and **Type**.
5. The following fields are required:

   - **Alias:** Combines the name and version entered by default but can also be edited to display any desired alias.
   - **Application/Command:** The path to the application, such as **c:\Users\Administrator\Desktop\autoit\ps_facebook.exe**.

   The following are not required:

   - **Command Line Parameters:** The arguments to pass to the application.
   - **Functional Account:** Select a functional account. The functional account must already be created. A functional account is required for Azure, Microsoft 365, Amazon, and Workday cloud accounts, though it is not enforced.
   - **Managed System:** Required if a functional account is set.



Once a cloud application is configured, accounts must be added manually on the **Managed Accounts** page, though it is not enforced.

Note: *The Workday cloud application requires that you download and install the* ***GeoTrustGlobal_CA.er*** *certificate before you can configure the cloud in BeyondInsight.*

For more information, please see the following:

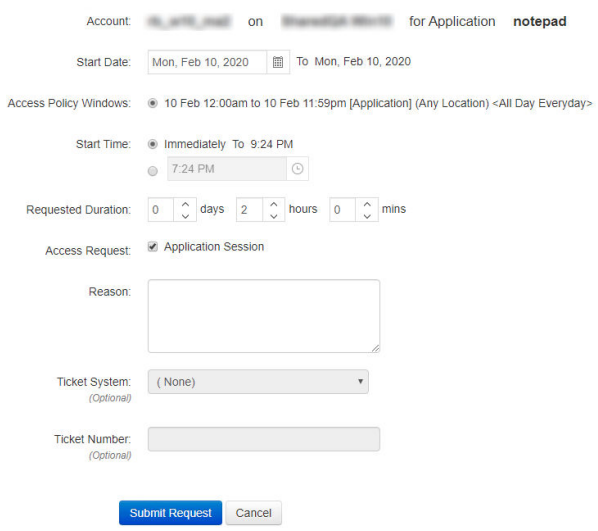
- For information on adding accounts manually, "Associate the Application with a Managed Account" on page 77
- For information on the Managed Systems page, "Work with Managed Systems" on page 40

Request an Application Session

Applications, including databases and cloud, are available in the web portal after the initial setup.

1. In the console, click **Menu** and then select **Password Safe > Accounts**.
2. Click a tab to display available applications: **Applications**, **Databases**, and **Cloud**.

3. On the grid, click the application that you want to access.
4. Enter a reason, if required.
5. Select the other parameters, if required.
6. Click **Application Session**.



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.

For more information, please see "Create an Access Policy" on page 9.

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

Requirements for SSH

- You must install PuTTY to enable SSH functionality. Go to **www.putty.org** and 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, ecdsa-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1
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	diffie-hellman-group-exchange-sha1	
blowfish-ctr	blowfish-cbc	3des-cbc
arcfour256	arcfour128	arcfour
HMAC-MD5	HMAC-MD5-96	HMAC-SHA1-96
aes256-cbc	aes192-cbc	aes128-cbc

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 now 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)

Client Host Key Algorithms

Below is a list of host key algorithms enabled for use by Password Safe's SSH client. 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
- 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)

Server Host Key Algorithms

Below is a list of host key algorithms enabled for use by Password Safe's SSH 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
- ssh-dss (disabled by default)

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 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-group14-sha1
- 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\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
(x86)%%\\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.

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 - no)
  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 - no).
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Beyondtrust\PBPS\SessionManager\ssh_proxy\allow_remote_port_forwarding

Multiple SSH Sessions

To avoid a potential security risk, more than one SSH session is not permitted through one 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 which will be used 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 which will 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 using Direct Connect, the requester has to connect to Password Safe's SSH Proxy using a custom SSH connection string with 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 will then be 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>
```

Once the requester is authenticated, they will be immediately connected to the desired machine.

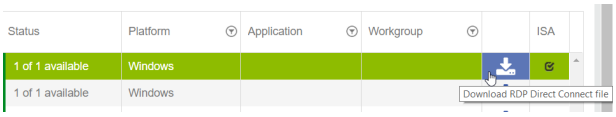
RDP Session Requests

> ***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.



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:

HKLM\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 will be split on that character.

For example: **ssh -p 4422 /requestor/maccount/msystem/@bihost**

In this case, '**/**' will be used as the delimiter.

To enable dynamic delimiters (default is off), set the following registry key:

HKLM\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 could 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 selecting the check 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.

These ports are configurable under **Global Settings**. The default inbound port connections to the Password Safe proxy:

- RDP: **3389**
- SSH: **4422**

Session Countdown Duration

You can configure the maximum amount of time for which the session countdown timer will be 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)

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.

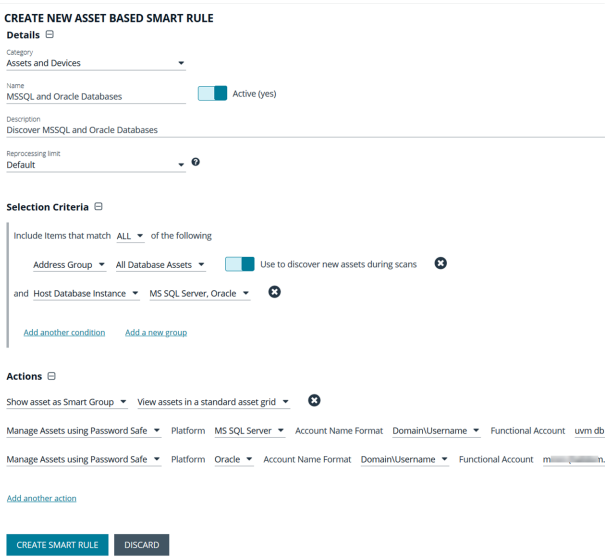
Auto Discover and Manage Database Instances

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

- All Audit Scan
- Asset Report Scan

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**.



Manually Add Database Instances

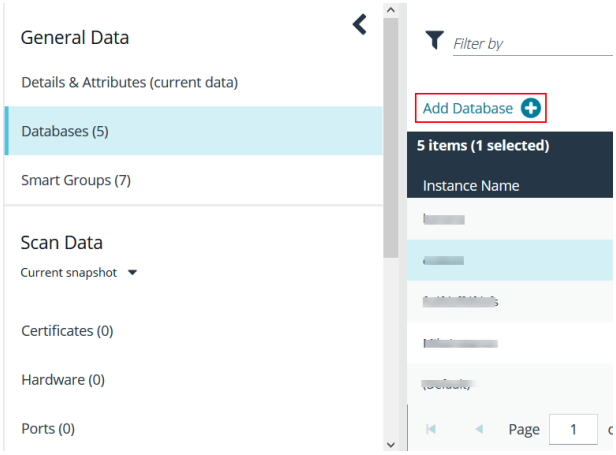
You can manually add the following database instance types. When selecting the database platform, ensure the correct port number is displayed.

- Mongo: **27017**
- SQL Server: **1433**
- MySQL: **3306**
- Oracle: **1521**
- PostgreSQL: **5432**

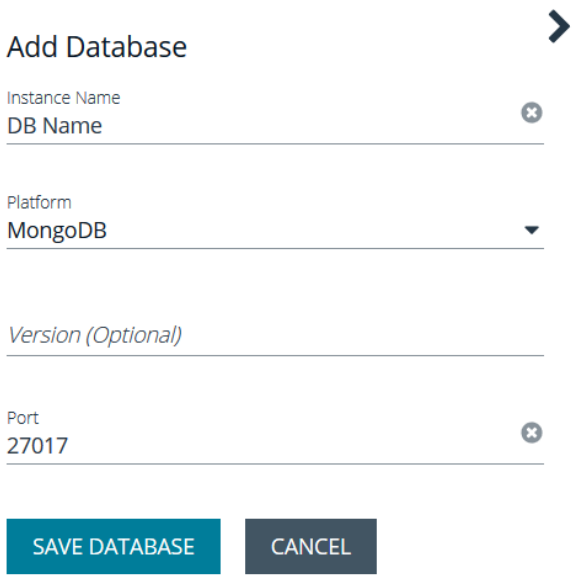
- Sybase ASE: **5000**
- Teradata: **1025**

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**.



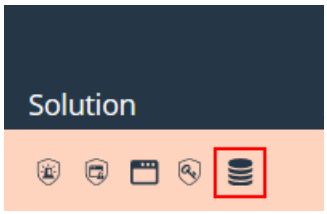
5. Provide a name, select the platform, add a version, leave the default port, and then click **Save Database**.



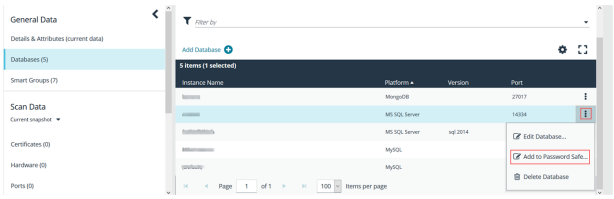
Manually Add Databases to Password Safe Management

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, and then click the **More Option** button, 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**.

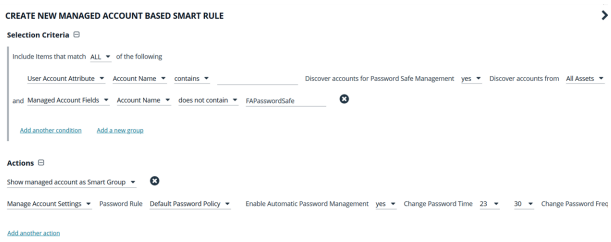


6. Select the functional account and other desired settings, and then click **Create Managed System**.

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. Create a managed account based smart rule, and select the criteria that will match on the database instance account name.
2. Select **Yes** from the **Discover accounts for Password Safe Management** list.
3. From the **Discover accounts from** list, select the address group where the database instance resides.



> ***Note:*** *If you have named functional accounts (which are not defaults), you should remove them from management by using managed account field filters, as shown in the screen shot.*

4. In the **Actions** section, select **Show managed account as a Smart Group** from the list.
5. Select **Manage Account Settings** from the list.
6. Select a password rule, and either Auto-Manage the Accounts or not.
7. Click **Create Smart Rule**.

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

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 that you will 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:

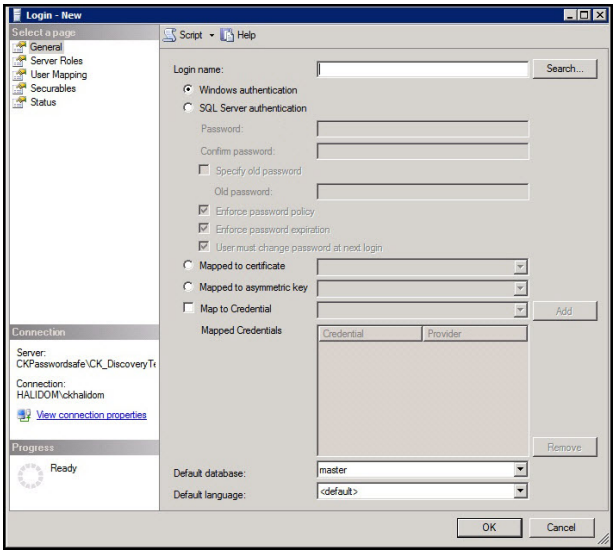
The following code samples show you how to apply the required permissions to the functional account.

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

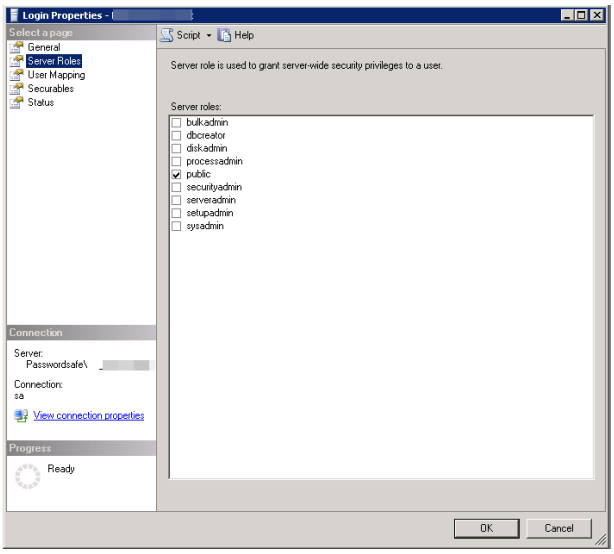
```
GRANT ALTER ANY LOGIN TO [FunctionalAccountName];
```

Create the Account in SQL Server

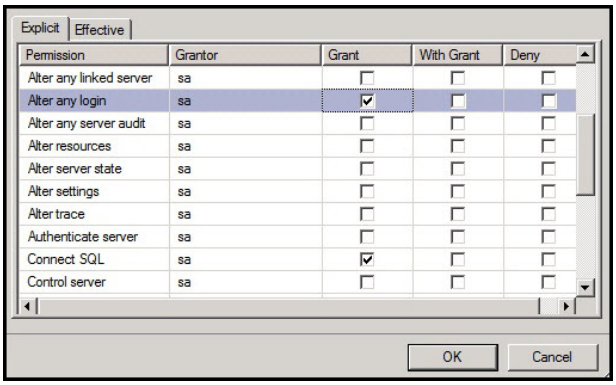
1. Connect to a database as the SQL Server **sa** on the asset you have managed.
2. Expand **Security** and then expand **Logins**.
3. Right-click **Logins** and then select **New login**.
4. Enter a **Login name** and then select **SQL Server Authorization**.
5. Enter and confirm a password.
6. Configure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



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



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



SQL Server Instance Port Retrieval

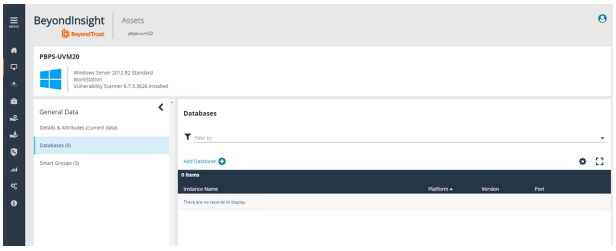
To configure a SQL Server database for Password Safe, you need to retrieve the port number on the managed database instance using a query. The below query is required for database instances only. You do not need to provide a port number for the default instance.

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:

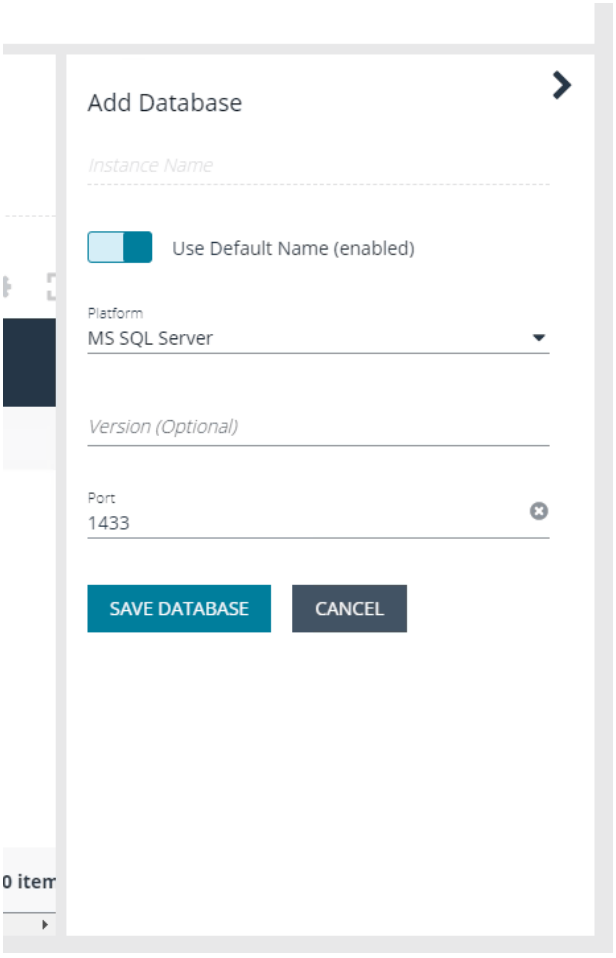
```
GO
xp_readerrorlog 0, 1, N'Server is listening on'
GO
```

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 advance 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**.



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. Create 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 that will be used as the functional account in Password Safe.

Create Accounts in PostgreSQL

> The following instructions are for guidance only. For more information about 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 select **Create**.
3. Enter a name. This will be 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 will be 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 also need to know the database instance name and the port number. In **pgadmin**, click **Object** , select **Properties**, and then select 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, and then click the **More Option** button, 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:** 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.

For more information, please see "Create a Functional Account" on page 30.

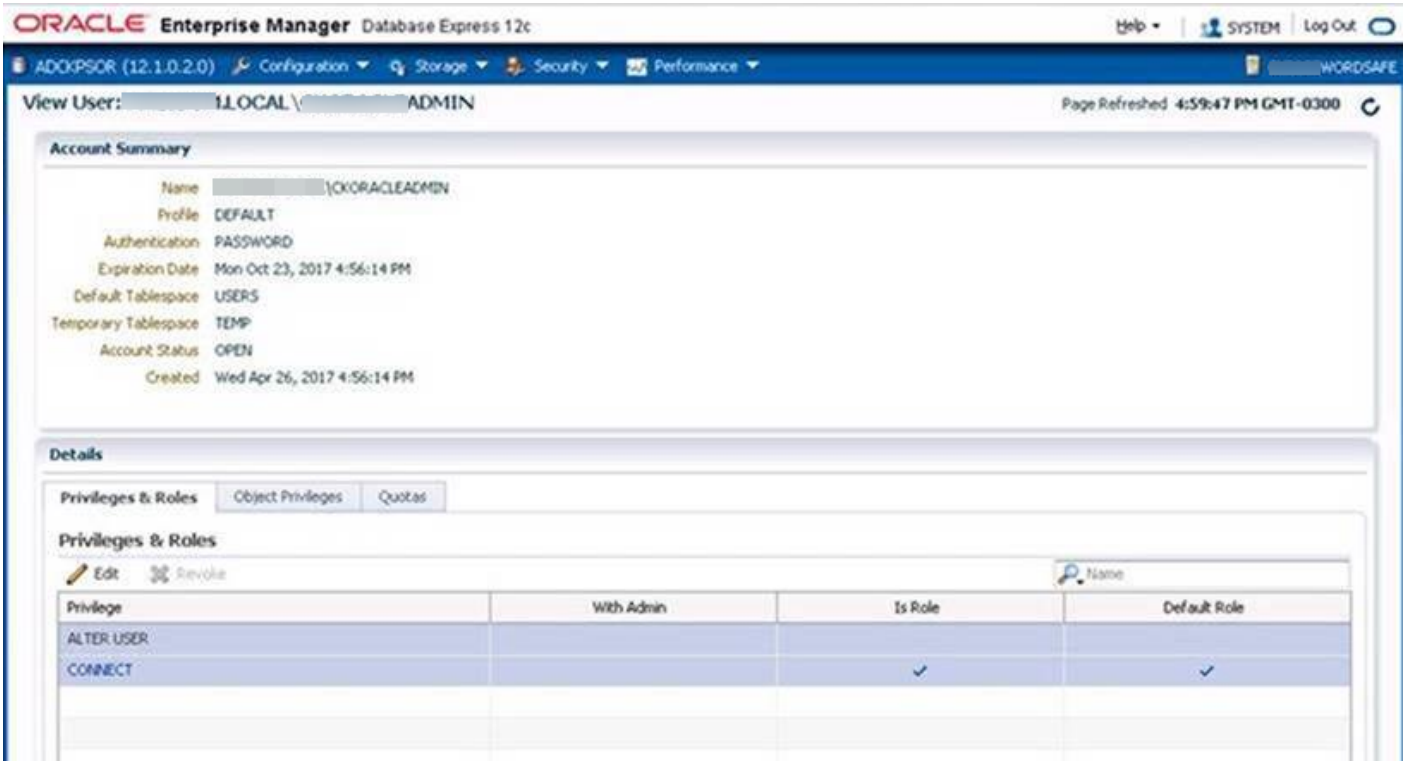
Note: *When adding the Oracle platform as a managed system, be sure to select the SYSDBA functional account.*

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 autodiscovery of Oracle instance managed accounts.)



Create the Functional Account in Oracle

To create a functional account in Oracle:

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

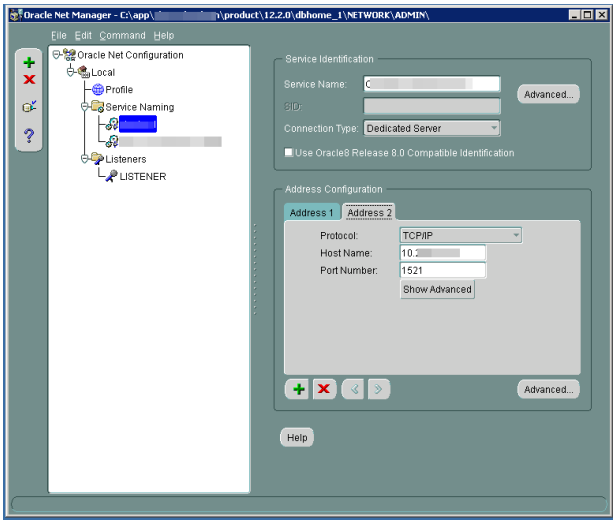
To grant permission to the functional account to change passwords on a managed account:

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

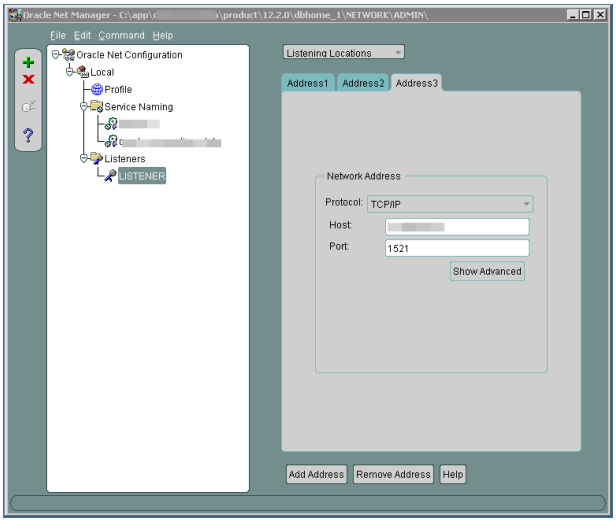
Configure the Host

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

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



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



Use Encrypted Connections

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

The following encryption protocols are supported:

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

Configure encryption using Oracle Net Manager.

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:

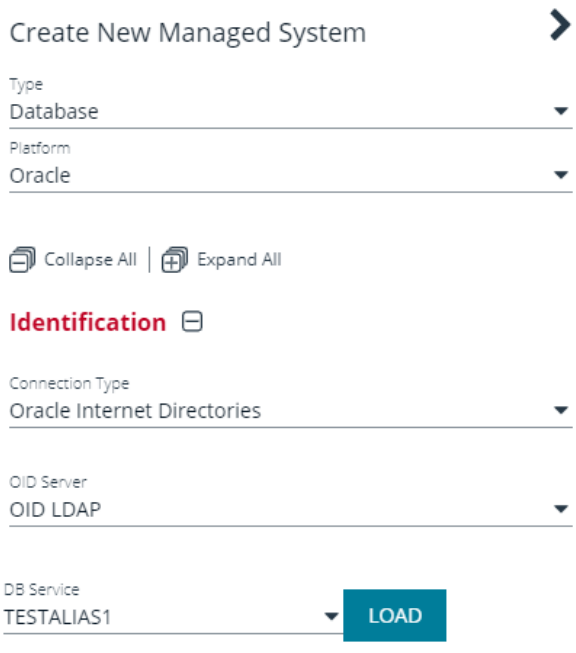
- On the **Integrity** tab, select:
  - **Server** from the Integrity menu
  - **required** from the Checksum Level menu
  - **SHA256** as the method
- On the **Encryption** tab, select:
  - **Server** from the Encryption menu
  - **required** from the Encryption Type menu
  - **AES256** as the method

***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.

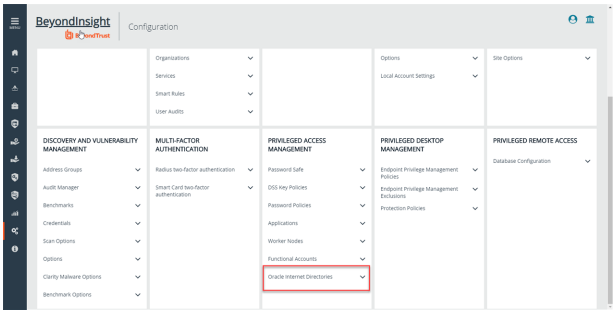
When adding an Oracle database as a Managed System in Password Safe, select the appropriate database service and Password Safe will read the Connect Descriptor data when communicating with the Oracle database.



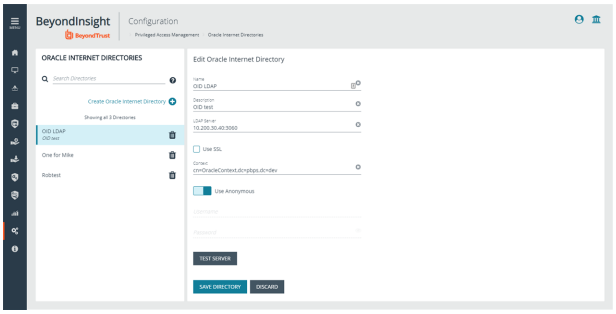
Configure an Oracle Internet Directory

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.



Add a Custom Platform

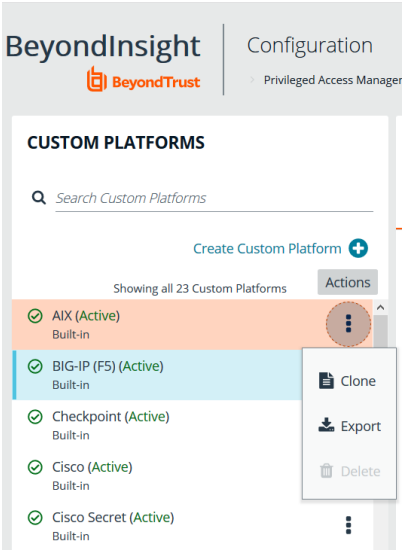
On the **Custom Platforms** page, you can add an SSH or Telnet platform tailored to your environment. Password Safe contains several built-in SSH and Telnet platforms such as Linux, Solaris, and Cisco, designed for the most common configurations. A custom platform can be created for advanced configurations that are not supported by the built-in platforms, or for a platform that is currently not supported by Password Safe. A custom platform can also be created by editing a built-in platform.

Custom and built-in platforms work 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 Custom Platform

1. In the BeyondInsight console, go to **Configuration > Privileged Access Management > Custom Platforms**.
2. In the **Custom Platforms** pane, click **Create Custom Platform**.
3. Select **Create New Platform** to create a new platform.
    - You can also create a new custom platform by editing a built-in platform or by cloning a built-in platform to create a new custom platform based on a built-in platform.
    - To create a new custom platform based on a built-in platform, select a built-in platform, click on the **Actions** menu at the right end of the platform name, and select **Clone**.

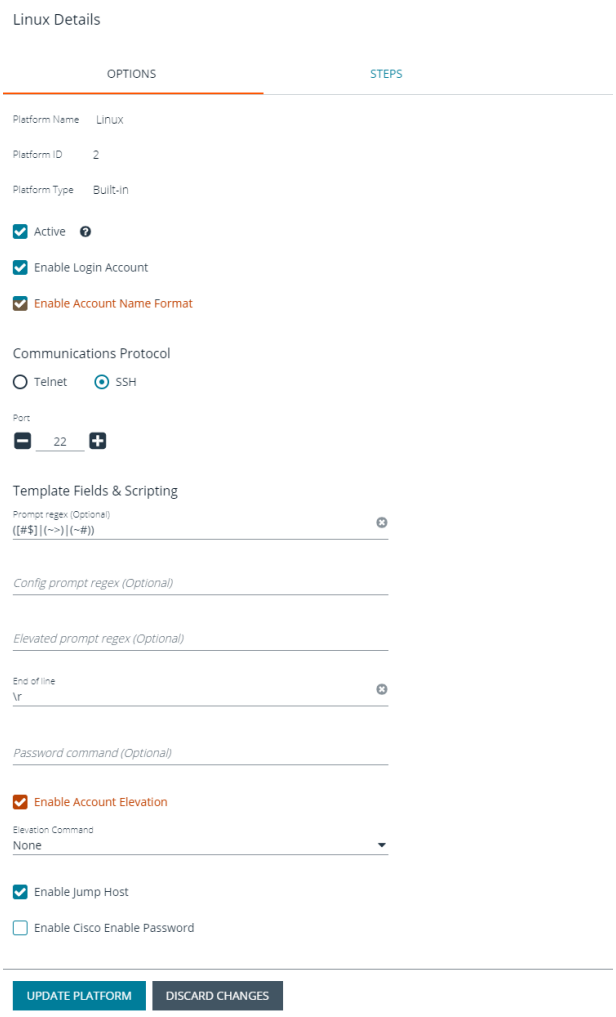
> ***Note:*** *Built-in platforms can be cloned but not deleted.*



4. Configure the settings on each tab as described below.

The following section provides details to configure settings for a custom Linux platform, created by modifying the built-in Linux platform.

Configure the Options Tab



1. **Platform Name:** The given name appears in the **Platform** lists throughout the application and must be unique. Platform names cannot be changed after they have been created.
2. **Platform ID** and **Platform Type** are assigned by the system and cannot be entered or edited.
3. **Active:** The platform is active in the system when the **Active** box is checked.
4. **Enable Logon Account:** Check the box to display the login account option on the **Managed Systems Settings** page. Use this feature when another account (not the functional account) is used to log in to the managed system.
5. **Enable Account Name Format:** Check the box to display the **Account Name Format** option on the **Managed Systems Settings** page.
6. **Communications Protocol:** Indicate if the custom platform will use **Telnet** or **SSH**.
7. **Port:** Use the default port for SSH or Telnet. Optionally, enter a port to test the settings.
8. **Template Fields and Scripting:**
    - **Prompt RegEx:** Regular expression that will evaluate to the shell prompt of the remote system; for example, **~]#**.
    - **Config Prompt Regex / 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 will indicate to the SSH or Telnet server that it is sending a command. The default is the carriage return character (**\r**).
    - **Password Command:** Enter the command to change the password.
9. **Enable Account Elevation:** Check the box, if applicable. This must be checked to enter an **Elevation Command**.
10. **Elevation Command:** Enter an elevated account to elevate the **Functional Account** permissions. The following are supported:
    - sudo
    - pbrun
    - pmrun
    - pbrun jumphost
11. **Enable Jump Host:** If you are using the elevated credential **pbrun jumphost**, you can configure the Privilege Management for Unix & Linux policy server host name to connect to. Check the box here. Select the **Check Password** tab to enter the policy server host name details.
12. **Enable Cisco Enable Password:** Check the box to display the **Enable Password** option on the **Functional Account Settings** page.

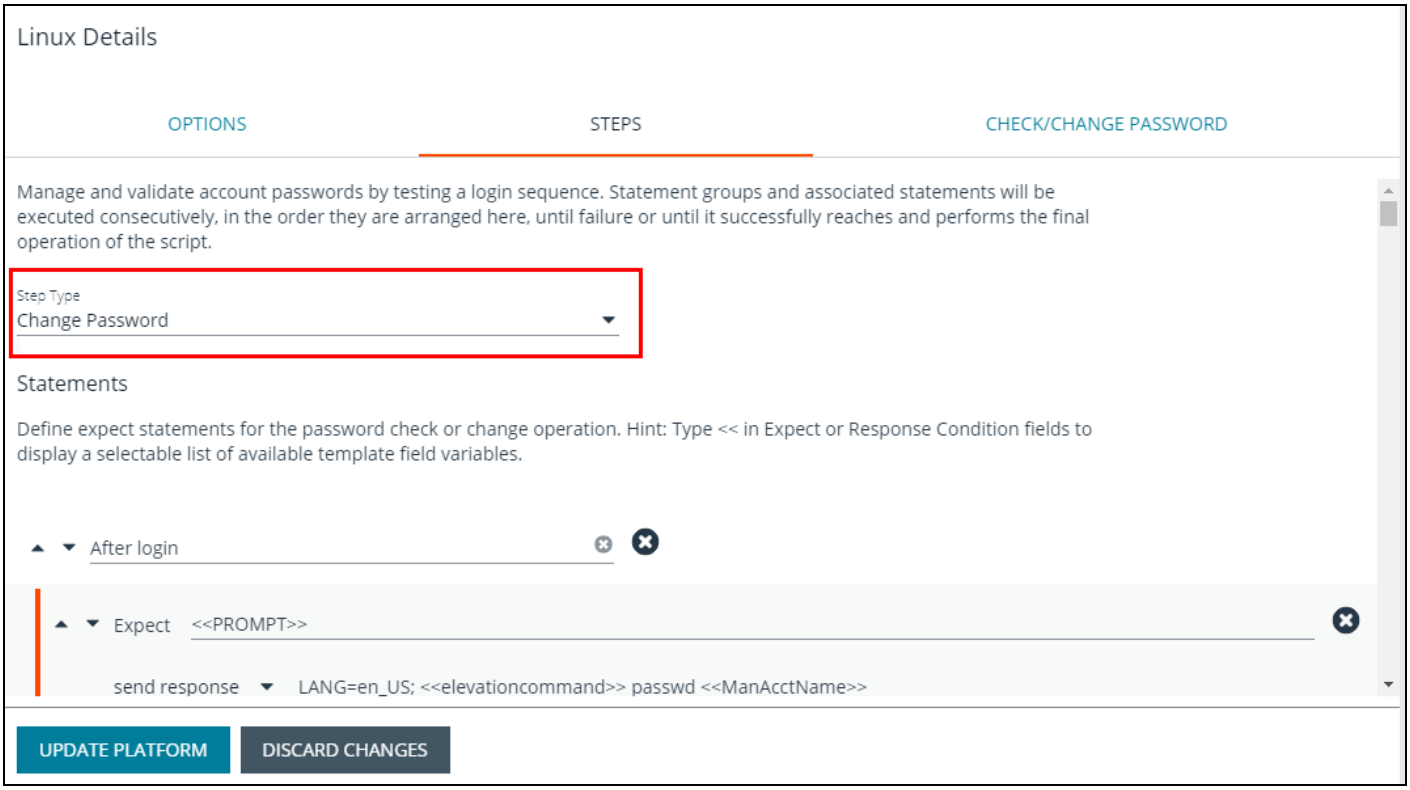
13. **Enable Account Name Format:** Check the box to display the **Account Name Format** option on the **Managed Systems Settings** page.
14. **Enable Account Elevation:** Check the box to display the **Account Elevation** option on the **Managed Systems Settings** page.
15. **Enable Cisco Enable Password:** Check the box to display the **Enable Password** option on the **Functional Account Settings** page.

Configure the Steps Tab

On 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**.

Using the below Linux example, the first **Expect** statement anticipates that the regular expression is **Enter your reason for login:** and replies with **changing password** if there is a match.

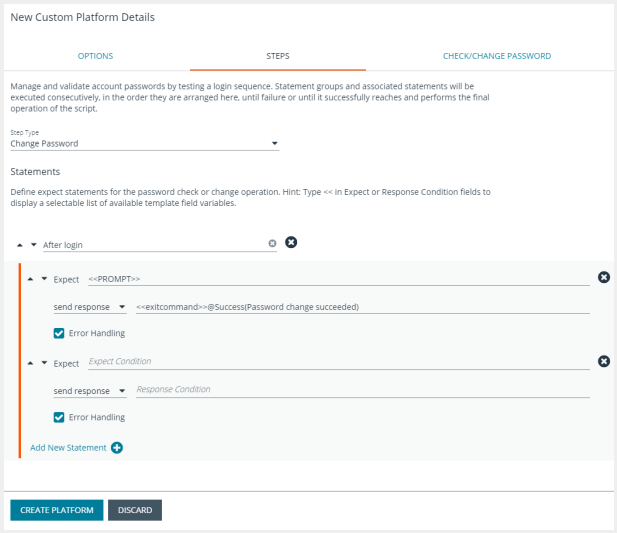
Before configuring the **Steps** tab, select the **Step Type** from the list. The **Steps** template changes depending on the selection:



- **Change Password:** Manually changes the password for the custom platform.
- **Check Password:** Tests the password by attempting a log on.
- **Change Public Key:** Runs a script to replace the public key.

Example: Steps Tab Configuration

1. *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.*
2. *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.*
3. *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.*
4. *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.*
5. *Error handling is selected by default.*
    - *De-select it if error handling is not required.*
    - *If error handling is required, ensure an error message is entered in the **Error handling expect** statement.*
6. *The order of statement processing can be changed by clicking the Up or Down icons at the left of each **Expect** statement.*
7. *When all statement groups have been completed, click **Create Platform**.*



The following is an explanation of the functionality for each setting on the **Steps** tab:

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

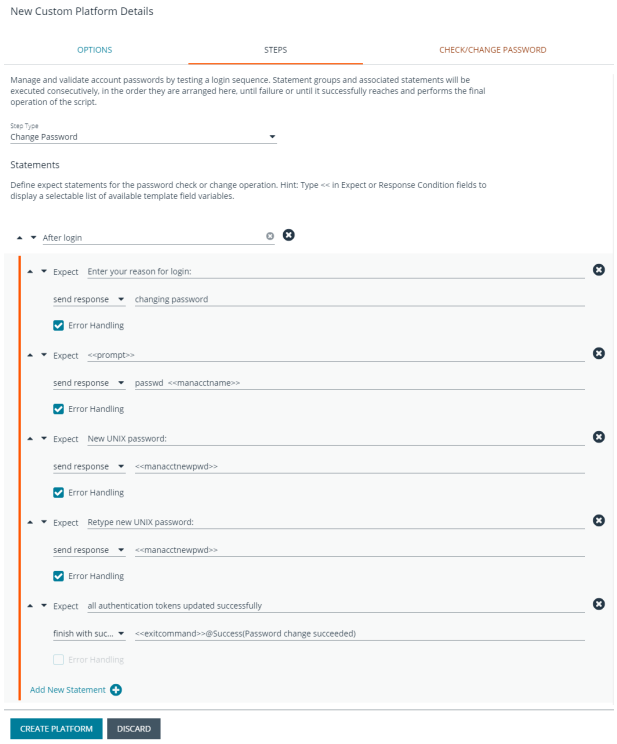
```
Welcome to Linux Mint
* Documentation:  http://www.linuxmint.com
Last login: Mon Apr 13 10:45:51 2015 from dev-machine
Enter your reason for login:
```

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

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

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

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



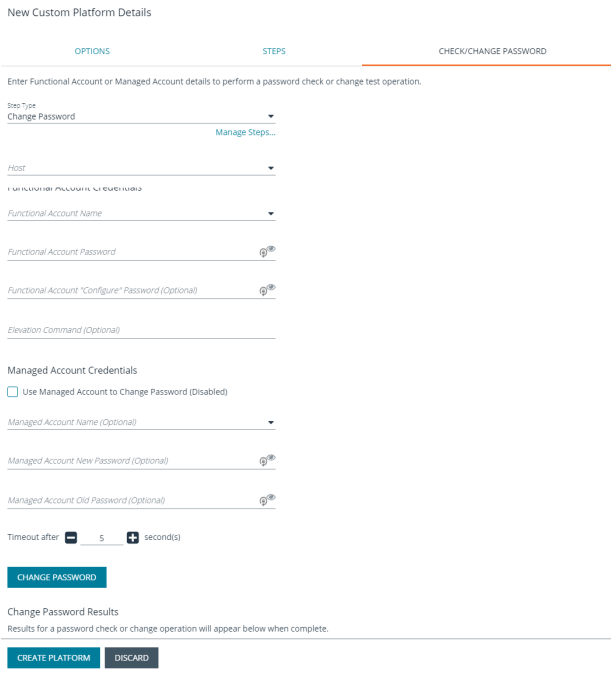
- **Expect Statement:** We recommend that you include the prompt in the regex of the **Expect** field to ensure the platform waits until all the data from the previous command is read from the target system before moving to the next statement.

  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.

Change Password and Check Password Tabs

After you complete the fields on the tab, Password Safe runs the credentials. Log into the host using the managed account name and follow through the configurations provided on the **Steps** tab.



1. Select the tab and enter the host and functional account.
2. If you are using the elevated credential **pbrun jumphost**, enter the IP address for the PBUL policy server.

   Ensure the **Enable Jump Host** box is checked on the **Options** tab. Otherwise, the Jump Host box is not displayed.

3. Use the default port for SSH or Telnet. Optionally, enter a port to test the settings.
4. In the **Elevation Command** box, enter an elevated account such as sudo or sudoer to elevate the functional account permissions.
5. Provide a managed account name and a new password to complete the test.
6. Click **Change Password** or **Check Password**.
7. When the test returns a successful connection, go to the **Options** tab, check the **Active** box, and then click **Create**. You can then select the custom platform in systems settings when you configure the platform to be managed by Password Safe.

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** icon for the platform you wish to export, and then select **Export**.
3. Save the .xml file.

Import a Custom Platform

1. In the BeyondInsight console, go to **Configuration > Privileged Access Management > Custom Platforms**.
2. In the **Custom Platforms** pane, click **Create 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 of 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 looks for other possible responses such as **User does not exist**.
7. If this 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 will reply with the new password.

Work with Smart Rules

You can use smart groups to add assets, systems, and accounts to Password Safe management. The smart rule filters that you configure for the smart groups determine the assets that will be 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 Systems**, and **Vulnerabilities**.

You can use smart rules to add the following types of assets:

- Systems
- 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 *BeyondInsightUser Guide* at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-user.pdf.

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 Manged Systems
Cloud Managed Systems	Types	Cloud Managed Systems
Asset Managed Systems	Types	All Managed Systems associated with BeyondInsight Assets
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 Mac OSX 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** will 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**.

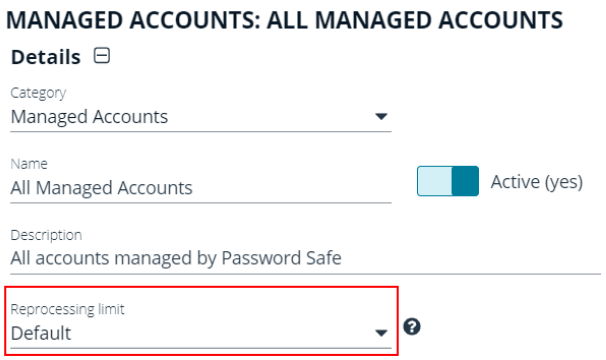
Change the Processing Frequency for a Smart Rule

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 will process in the selected time frame (for example, the rule will process 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 will always process when first saved or updated.*

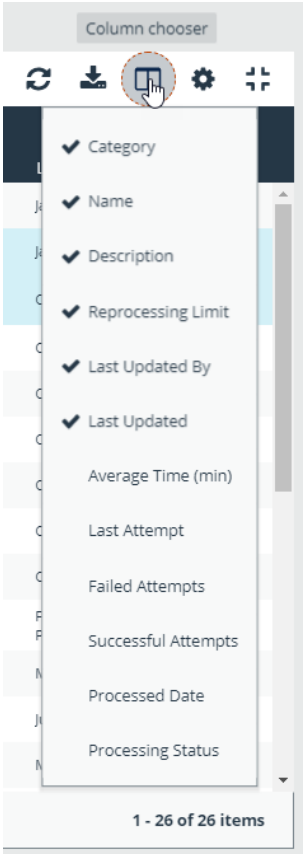


View and Select Smart Rules Processing Statistics

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

To add this information to the grid:

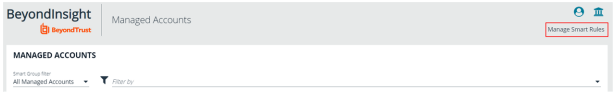
1. In the BeyondInsight console, click **Smart Rules** on the left menu.
2. Click the Column chooser icon in the upper right of the grid.
3. Click the desired column to add that information to the grid.
    - Check marks indicate columns currently displayed.
    - You can remove a displayed column by 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.



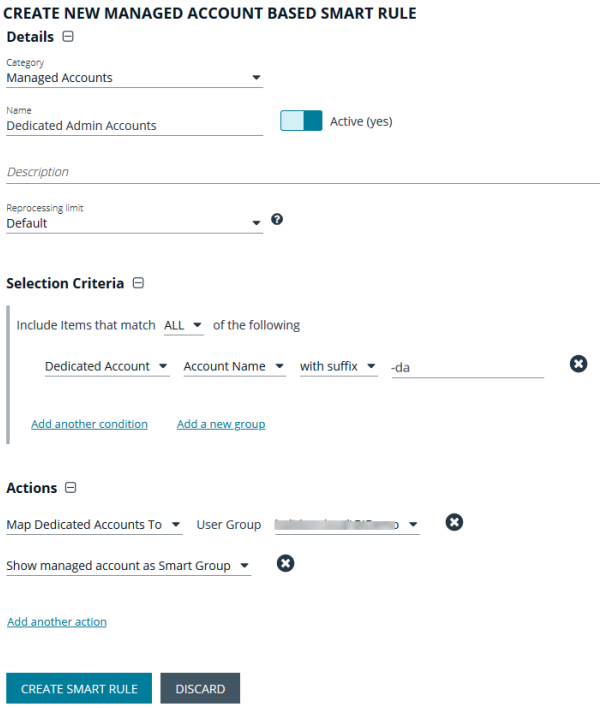
Use Dedicated Account Smart Rule

A dedicated account smart rule allows you to dynamically map dedicated administrator accounts outside of BeyondInsight to users in a BeyondInsight group.

1. In the console, click **Managed Accounts**.
2. Click **Manage Smart Rules**.

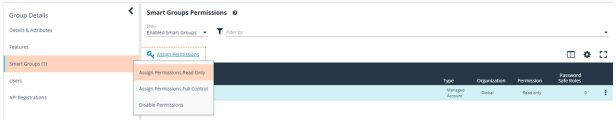


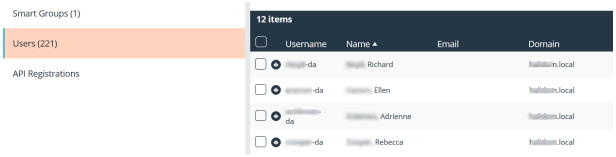
3. Click **Create Smart Rule**.
4. Under **Selection Criteria**, select **Dedicated Account**, and then define filter rules.
5. Under **Actions**, select **Map Dedicated Accounts To**, and then select a user group.
6. Click **Add another action**.
7. Select **Show managed account as Smart Group**.
8. Click **Create Smart Rule**.



After setting up the smart rule, you must assign permissions and roles to the group.

1. In the console, click **Configuration**.
2. Under **Role Based Access**, click **User Management**.
3. Select the group.
4. Click the **More Options** button for the selected group.
5. Click **View Group Details**.
6. In the **Group Details** pane, click **Smart Groups.**
7. In the **Smart Group Permissions** pane, select the newly created dedicated account smart group.
8. Click **Assign Permissions > Assign Permissions Read Only**.





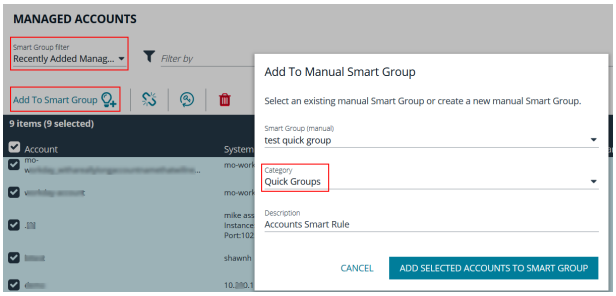
> ***Note:*** *If there is more than one match to the usernames which match the criteria in the dedicated accounts smart group, you must edit the smart group to exclude the duplicate matches.*

Use Quick Groups

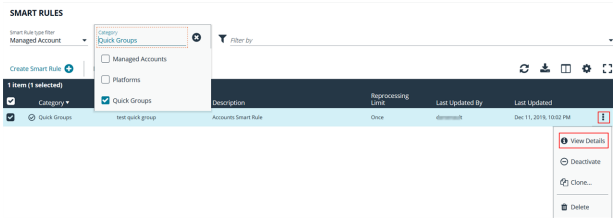
For a simpler way to organize managed accounts, you can group them using a Quick Group. The default processing time on a Quick Group is **Once**.

For more information about Smart Rule processing, please see "Change the Processing Frequency for a Smart Rule" on page 113.

1. In the console, click **Managed Accounts**.
2. From the **Smart Group filter**, select an existing Smart Group where the managed accounts are members.
3. Select the check boxes for the managed accounts that you want to add to the Quick Group.
4. Click **Add to Smart Group**.
5. Select **Quick Groups** from the **Category** list, and then select a Quick Group from the **Smart Group** list or create a new one.



6. Quick Groups are displayed in a **Quick Groups** category on the **Smart Rules** page.
7. You can change the name and description by clicking the **More Options** icon, and then selecing **View Details**.



Note: *You can add and remove accounts from Quick Groups on the* ***Managed Accounts*** *page.You cannot add or modify filters or actions for Quick Groups.*

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 - Asset	Users can create and edit Asset-based Smart Rules.
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.
Smart Rule Management - Policy User	Users can create and edit Policy Smart Rules.

Smart Rule Management - Vulnerabilites	Users can create and edit Vulnverabilities Smart Rules.
Smart Rule Omniworker Options	Users can configure Smart Rule Omni Worker Options, such as mult-worker node usage, number of Smart Rule threads per type, and failure thresholds.

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 and 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 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.

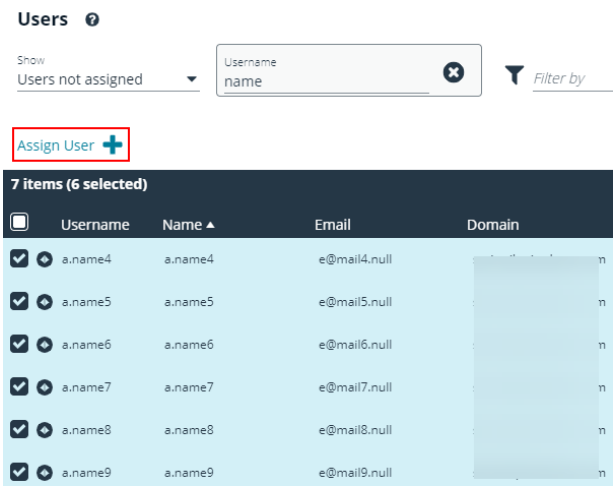
Create a Group and Assign Roles

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

Roles are only available to BeyondInsight features.

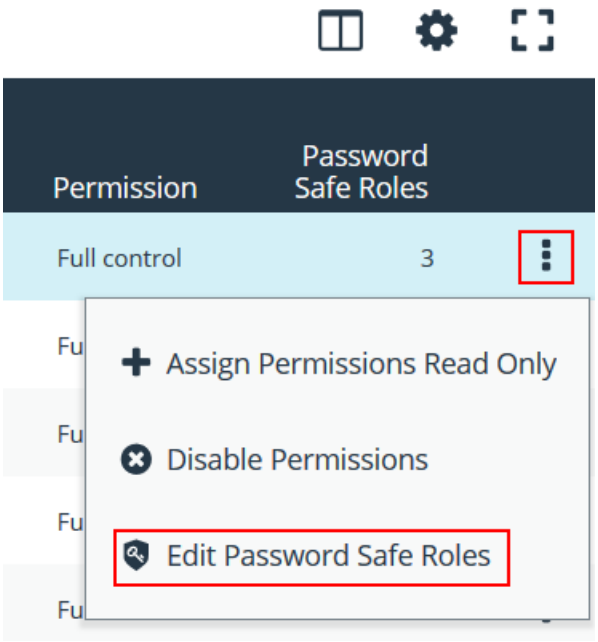
1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Click **Create New Group**.
4. Select **Create a New Group**.
5. Enter a name and description for the group.
6. Click **Create Group**.
    - Assign users to the group:
        - Under **Group Details**, select **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.

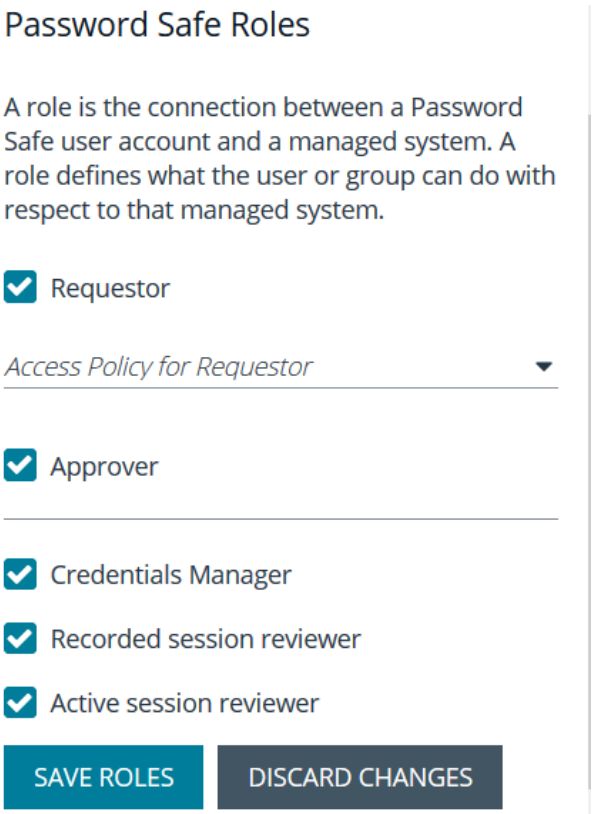
- Select the users you wish to add to the group, and then click **Assign User**.



7. 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**.
8. 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**.

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 into 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. 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. In the console, click **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 will have API access if at least one of the user groups they belong to has API access enabled.

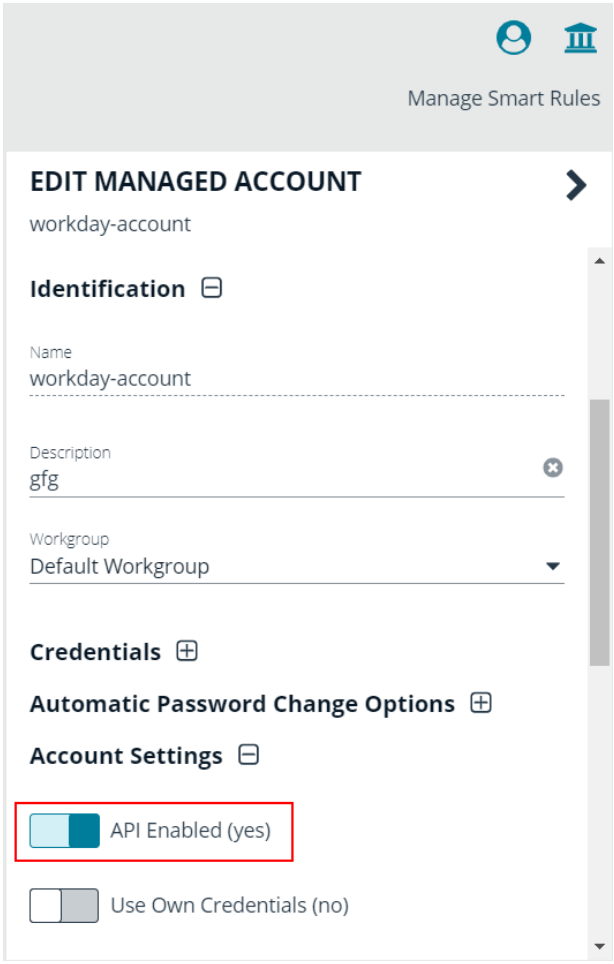
1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Select the group, and then click the **More Options** button.
4. Select **View Group Details**.

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 **More Options** button for a managed account, and then select **Edit Account**.
3. Expand **Account Settings**, and then click the toggle to change the **API Enabled** option to **yes**.
4. Click **Update Account**.



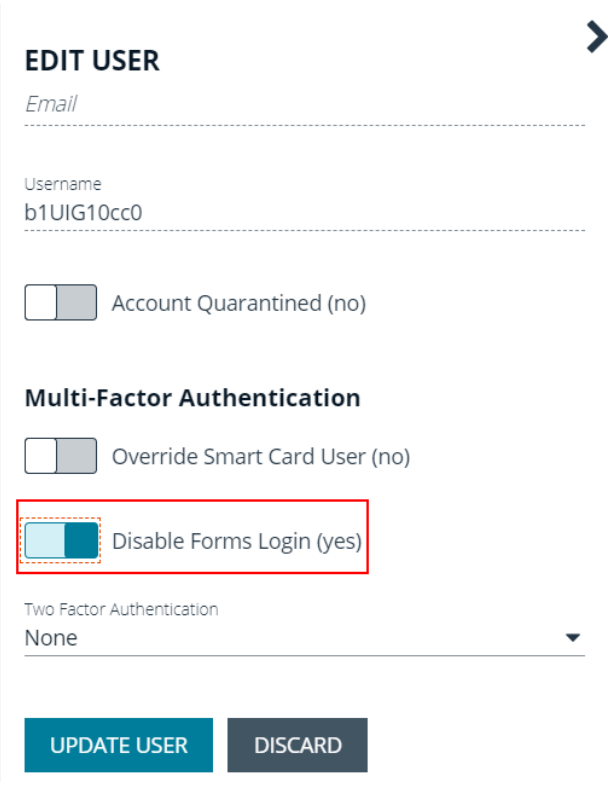
Restrict Access to Password Safe Login Page

When using SAML 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 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. 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**.



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.

For more information, please see "Create a Group and Assign Roles" on page 119.

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 "Add a Managed Account Manually" on page 34.

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, as 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 the The BeyondInsight User Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-user.pdf.

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 the The BeyondInsight User Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-user.pdf.

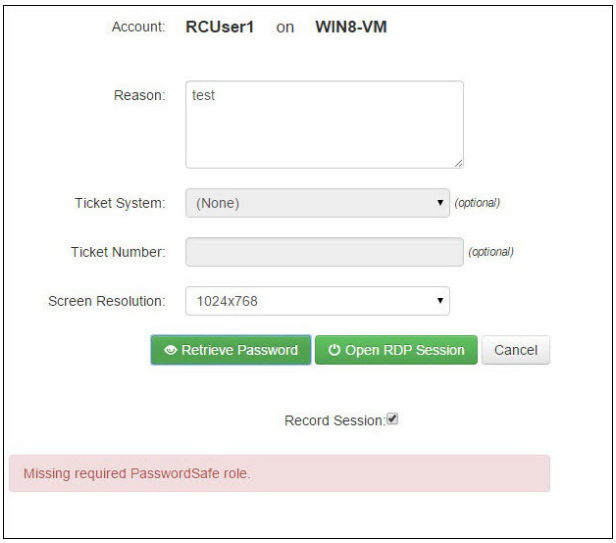
Real Time Authorization

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:

SOFTWARE\Wow6432Node\Beyondtrust\PBPS\EnableCheckoutAuthorization

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



Configure Workgroups for Multi-Node and Multi-Tenant Environments

Password Safe allows you to assign worker nodes to workgroups in Password Safe 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 will function on a global level and can change any account that does not have a designated workgroup assigned.

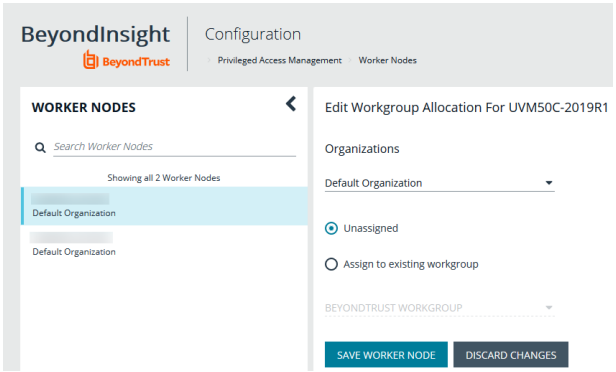
Create a Password Safe Worker Node

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 drop-down list to select the organization.
    - **Unassigned:** The node is not assigned.
    - **Assign to existing workgroup:** If selected, use the drop-down list to select the workgroup you want.
3. Click **Save Worker Node** when done.

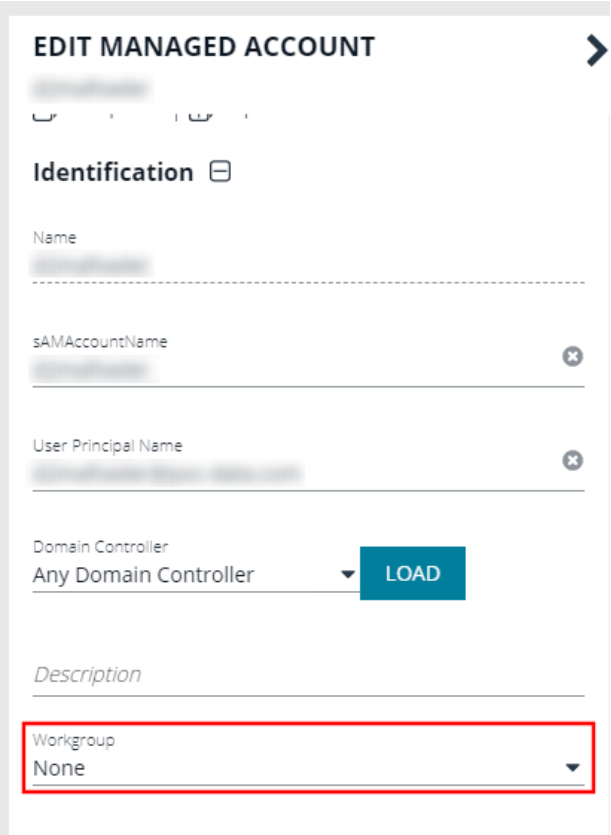


Assign a Workgroup to a Managed Account

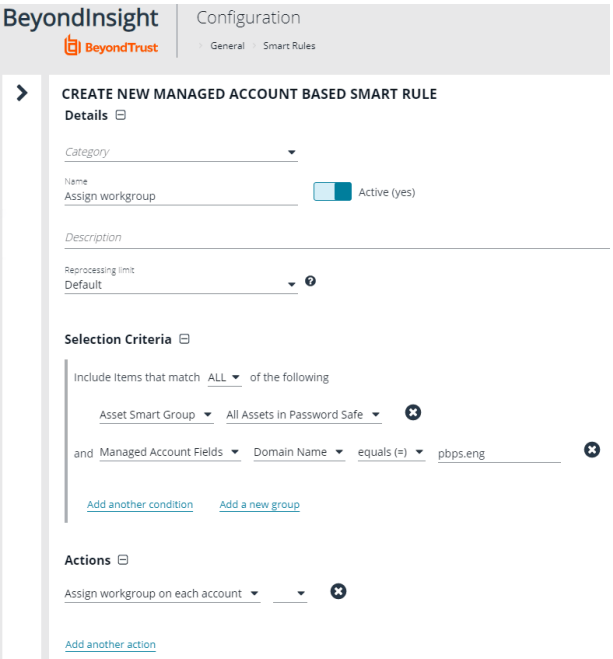
You can assign a workgroup to a particular managed account by editing the managed account or by using a Smart Rule.

To assign a workgroup to particular managed account, go the **Managed Accounts** page and select the account to edit. On the **Edit Managed Account** page, select a workgroup from the drop-down list.

> ***Note:*** *If you set the workgroup value to* ***None****, the account can be changed by any Password Safe agent.*



To assign a workgroup using a Smart Rule, go the **Smart Rules** page, and create or a edit an existing rule. Under **Actions**, select **Assign Workgroup on each account**.



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 re-assigned to a workgroup, the Password Safe omniservice must be restarted.*

After the worker nodes are assigned, managed accounts can be re-assigned 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 on assigning managed accounts to workgroups, please see "Assign a Workgroup to a Managed Account" on page 127.

For more information on how to configure a multi-tenant environment, please see the The BeyondInsight User Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-user.pdf.

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.