BeyondTrust

BeyondInsight 22.4
User Guide

TC:2/8/2023

Table of Contents

BeyondInsight User Guide

BeyondInsight is a central management, policy, reporting, and analytics console for many products within the BeyondInsight portfolio. BeyondInsight enables IT and security professionals to collaboratively reduce user-based risks, mitigate threats to information assets, address security exposures across large, diverse IT environments, and comply with internal, industry, and government mandates.

This guide provides instructions and procedures for using BeyondInsight.

Components

Discovery Scanner

The Discovery Scanner is the scan engine responsible for scanning the assets in your environment. The Discovery Scanner agent receives instructions from the Central Policy service.

A security certificate is required by the Events Client to communicate with the agent. This certificate is created during the BeyondInsight installation.

Manager Service

This component is the BeyondInsight web interface.

The Manager Service also acts as a background service that gathers information from the Events Client, which retrieves information from the agents. The events are then encrypted and sent to the database.

Application Bus (AppBus)

The AppBus provides communications between BeyondTrust components and receives events to insert in the BeyondInsight database. This function can also be performed by a dedicated Event Server for scalability.

Events Client

The Events Client is responsible for forwarding information gathered by the Discovery Scanner agent.

The Events Client sends the information to the Manager Service. The Events Client is installed when a Discovery Scanner agent is installed.

Events Client Certificate

Generate security certificates to ensure secure transmission of data between clients and BeyondInsight. Use the BeyondInsight Configuration Tool to export certificates.

> *For more information, please see the BeyondInsight Installation Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/install/configuration-tool.htm.*

Central Policy Server

Central Policy is a service that sends Discovery Scanner agents their settings. Central Policy is the component responsible for sending the agents job information.

For example, the Discovery Scanner agent needs to know the scan targets. This information is selected in the BeyondInsight management console. When the scan starts, the Central Policy sends the job information to the agent.

Scheduling Service

Responsible for contacting the update server and downloading the latest product updates.

Log In to the BeyondInsight Console

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

The following authentication types can be used:

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

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

To log in:

1. Open a browser and enter the URL for your BeyondInsight / Password Safe instance: **https://<hostname>/WebConsole/index.html**.

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

2. Enter your username and password. The default username is **Administrator**, and the password is the administrator password you set in the Configuration Wizard.
3. If applicable, select a domain or LDAP Server from the **Log in to** list.

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

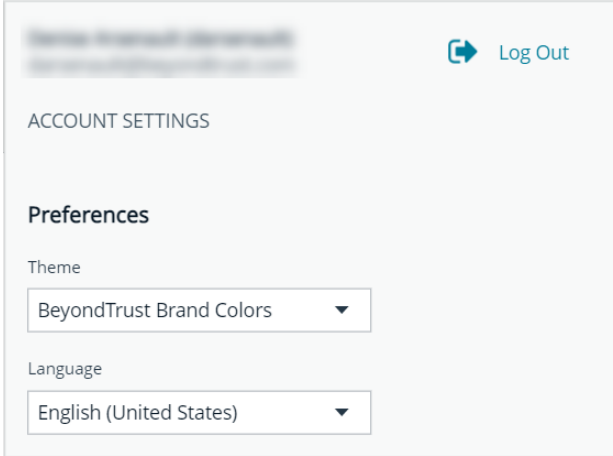
4. Click **Log In**.
5. To log in using SAML Authentication, click the **Use SAML Authentication** link below the **Log In** button. You are redirected to the single sign-on access site for the default SAML identity provider configured by your administrator in BeyondInsight.

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

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

Log Out of the Console

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



Select a Display Language

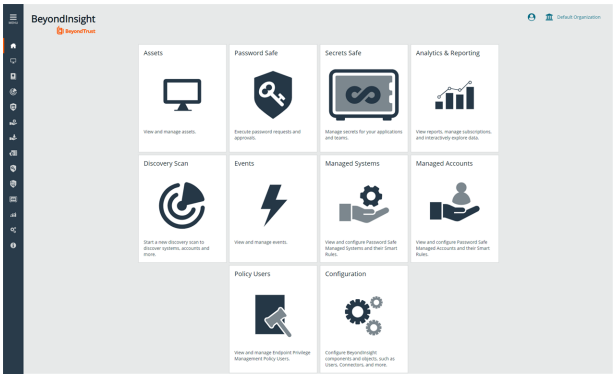
BeyondInsight and Password Safe can be displayed in the following languages:

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

If the **Show language picker** option is enabled in **Configuration > System > Site Options > Localization**, you can select a language from the list on the **Log In** page or by clicking the **Profile and preferences** button, and then selecting it from the **Language** list.

Navigate the Console

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



Available features include:

- **Assets:** Display and manage all assets. Access the **Smart Rules** page to create and manage Smart Groups. Add assets to Password Safe management.
- **Smart Rules:** View and manage Smart Rules.
- **Discovery:** Run and schedule discovery scans, review active, completed, and scheduled scans, and view the list of discovery scanners.
- **Endpoint Privilege Management**: View and manage Endpoint Privilege Management events, policies, policy users, agents, file integrity monitoring, and session monitoring.
- **Managed Systems:** View and configure properties for Password Safe managed systems, managed databases, managed directories, managed applications, and their associated Smart Rules.
- **Managed Accounts:** View and configure properties for Password Safe managed accounts and their associated Smart Rules.
- **Password Safe:** Access the Password Safe web portal to request passwords and remote access sessions and to approve requests.
- **Secrets Safe:** View and manage team secrets.
- **Analytics & Reporting:** Access reports on collected data.
- **Configuration:** Configure BeyondInsight and Password Safe components and objects, such as users and groups, authentication settings, connectors, and much more.
- **About**: Access helpful links and support tools, such as generating a support package and analysis to send to BeyondTrust Technical Support. View the current BeyondInsight version information, as well as the history of installed versions. View version information for currently installed plugins. View the maintenance expiry date and disable or enable the **Maintenance Expiry Warning Banner**.

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

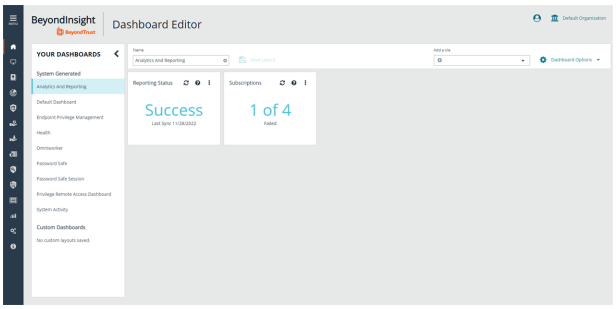
A warning banner displays at the top of the screen if your installation includes any Discovery Agents earlier than version 20.1. These must be updated by the end of 2021. You can go to ***Discovery > Discovery Scanners*** *to view all scanners in the system, and their version.*

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

Dynamic Dashboards

> ***Note:*** *Only admin access is supported at this time, and more features will be added in later releases.*

Dynamic Dashboards provide a faster, customizable experience, allowing administrators quick access to the information that is most important to them.

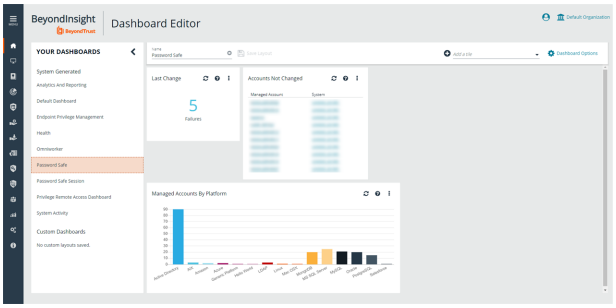


To access **Your Dashboards**, click **Menu > Dashboard (Preview)**. A list of available dashboards displays on the left. BeyondInsight comes with several prebuilt dashboard cards, including:

- **Analytics & Reporting**
- **Default Dashboard**
- **Endpoint Privilege Management**
- **Health**
- **Omniworker**
- **Password Safe**
- **Password Safe Session**
- **Privileged Remote Access Dashboard**
- **System Activity**

> ***Note:*** *The list of system-generated dashboards displayed can change depending on licensing, as well as data available in the system, and configuration settings. This also affects what tiles are shown in the* ***Add a tile*** *dropdown list.*

Each dashboard card comes with preset tiles, which display information for that particular feature. Icons allow you to control the tile:



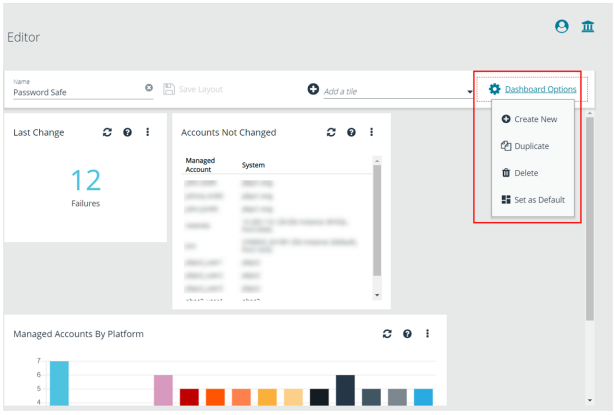
Click to refresh information displayed.

Click to get information on what is displayed on the tile.

Click to delete the tile. You can always add the tile later if needed.

Use **Dashboard Options** to:

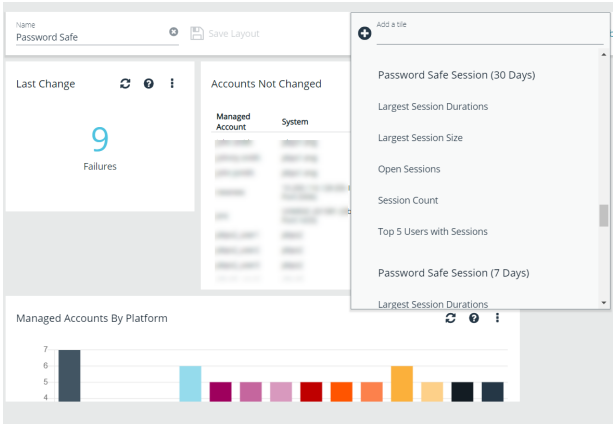
- **Create New:** Create a new empty dashboard, then add the tiles you want.
- **Duplicate:** Create a copy of the dashboard that can be modified.
- **Delete:** Delete the selected dashboard.
- **Set as Default:** Set the current dashboard as the default so it displays every time you click **Menu > Dashboards**.



Customize a Dashboard

You can customize a dashboard to display the information that is important to you. Tiles can be deleted, added, moved, and resized to allow you a personalized and more efficient experience.

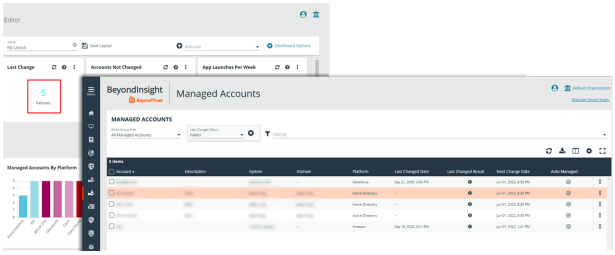
1. To create a custom dashboard, select one of the available dashboard cards. In this example we use the **Password Safe** card. If necessary, delete any of the existing tiles that come installed with that card.
2. From the **Add a tile** dropdown, select the tiles you want to add. Resize and reposition tiles in a manner that makes sense to you.
3. Next, under **Name**, give the layout a name so you can identify it.
4. Click **Save Layout**. Your custom layout now appears on the lower left side of the window, under **Custom Dashboards**.
5. If you want to make this your default layout so it opens every time you select **Menu > Dashboard**, click **Dashboard Options**, and then select **Set as Default**.



Note: *Setting a dashboard as default causes that dashboard to be displayed when the user logs in, or every time the user clicks on* ***Home****, and replaces the default dashboard.*

Access Dashboard Tile Information

The information displayed on some tiles can be used to access all relevant data associated with it. In this example, by clicking on the **Last Changed** tile *10 Failures* message, you are taken directly to the **Managed Accounts** page, where you can get full details on the issues mentioned. You can find linked tile information by hovering your mouse over it.

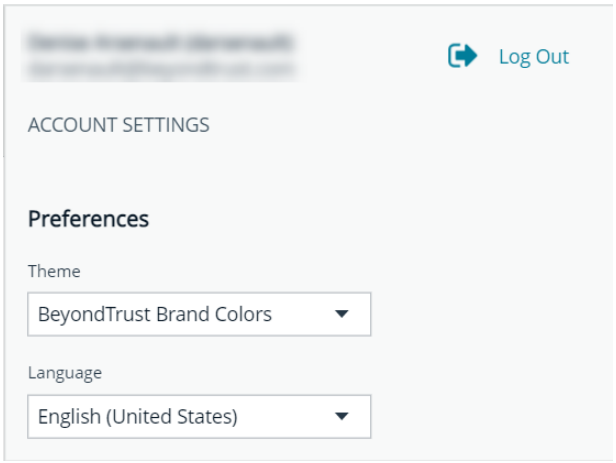


Change and Reset Login Passwords

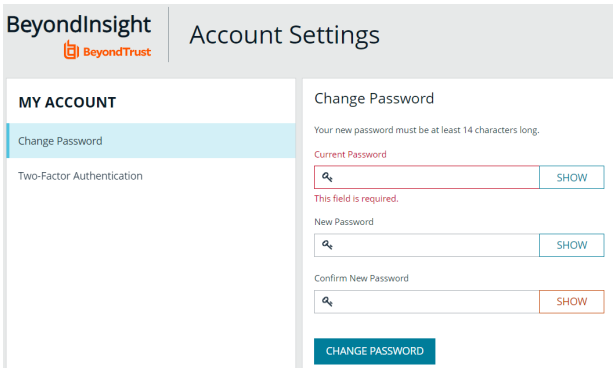
Change Password and Two-Factor Authentication Settings

If you are logging in with a BeyondInsight local user account, you can change your password and two-factor authentication app from the **Account Settings** page. You cannot change your password if you are logging in with Active Directory or LDAP credentials, or if your account is locked out.

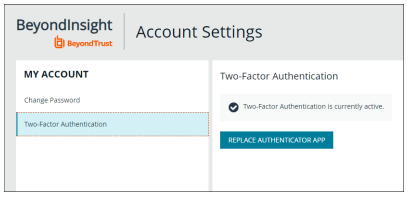
1. In the console, click the **Profile and preferences** icon in the top right corner.
2. Click **Account Settings**.



3. Update your password, and then click **Change Password**.



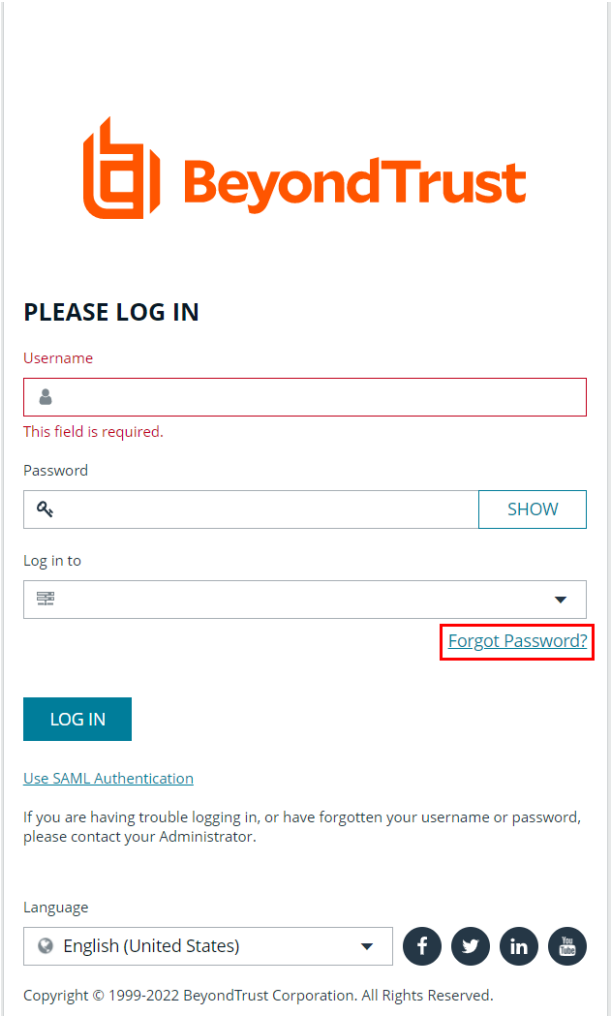
4. If your account has two-factor authentication enabled and registered with a device, you can update the authenticator app as follows:
   - Select **Two-Factor Authentication** from the **My Account** pane.
   - Click **Replace Authenticator App**.
   - Click **Reconfigure Authenticator App** to register a new authenticator app.



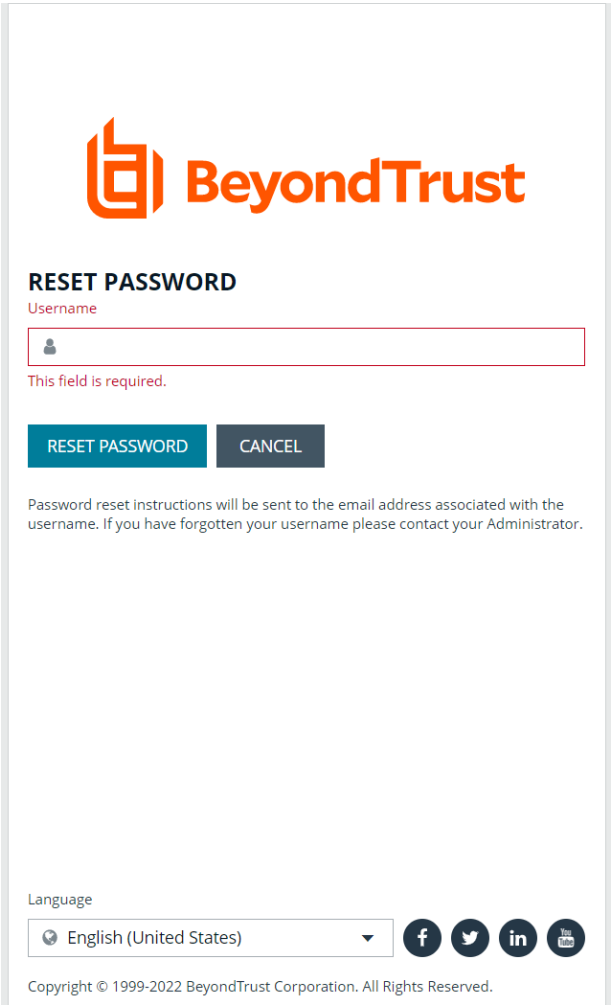
Reset Password

If you forget your console password, you can reset it as follows:

1. Click the **Forgot Password** link.



2. Enter your username, and then click **Reset Password**. An email containing a reset link is sent to the address associated with your username.



3. Click the link in the email to be taken to the **Enter New Password** page where you can change your password.

> ***Note:*** *Resetting the console password is not available to users logging in with Active Directory or LDAP credentials.*

Change and Set the Console Display Preferences

You can change the information displayed on BeyondInsight pages, including the columns, filters, grid size, and logos.

Set Display Preferences

You can set display preferences on grids and pages throughout your BeyondInsight instance.

> ***Note:*** *You can display domains and filter by domains. If the domain name is not known or the asset is not part of a domain, the field is blank. By default, the* ***Domain*** *filter is not displayed.*

1. Select an area of the site, such as **Assets**.
2. Above the grid, the following options and icons are available:

   - **Refresh:** Updates the displayed information with recent changes.
   - **Download:** Downloads the displayed information as a CSV file.
   - **Columns Chooser:** Select the columns to change the column headings and information displayed in the grid.
   - **Grid Configuration:** Choose the grid layout: **Compact**, **Default**, or **Expanded**.
   - **Expand Grid:** Enlarge the display area. When selected, the icon changes. It can be clicked again to **Collapse Grid**.

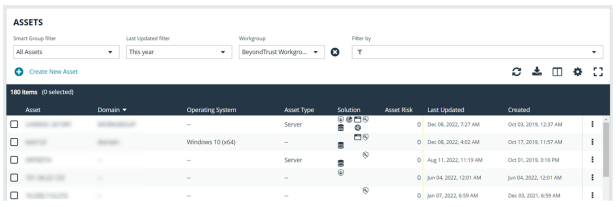
> ***Note:*** *Some options are not applicable to some grids, so fewer icons may display on those grids.*

3. An option to change the number of displayed **Items per page** is located below the grid.
4. The changes appear dynamically as they are selected.

Filter Records

Create a filter to match records you want to view on a page.

1. Select an area of the site, such as **Assets**.
2. Above the grid, there are options for filtering. The filter options available vary based on the page or grid selected. However, some common filtering options include:



   - **Smart Group filter:** Select to filter information by Smart Group association.
   - **Last Updated filter:** Select to filter by a specific period or a custom date range.
   - **Filter by:** Choose to filter the information by **Domain**, **Operating System**, **Workgroup**, etc., or other details specific to the information displayed. For each filter selected, enter the content you want to search for in the filter box's text field.
3. Apply as many filters as desired.
4. The information dynamically changes to match the selections.
5. Filter selections persist if the page is reloaded. To remove a filter, click the **X** on the filter.

6. To select all records listed on all grid pages, check one box in the grid and press **Ctrl+A**.
7. To deselect all records listed on all grid pages, press **Ctrl+Shift+A**.

Customize Console Logos

As a BeyondInsight administrator, you can add corporate logos to replace default brand logos in the management console.

Note: *The word "BeyondInsight" remains in the footer text on the* ***Login*** *page. This cannot be changed. After an upgrade, you must repeat these steps, because the upgrade overwrites the customized images and sets them back to default.*

Replace the following three SVG image files found in **<install path>/webconsole/assets/images/**:

- **app-logo-default.svg** (normal logo)
- **app-logo-darkmode.svg** (black and white version of the logo)

Tip: *The images must be 450px × 67px.*

Role-Based Access

BeyondInsight offers a role-based delegation model so that you can explicitly assign permissions to groups on specific product features based on their role. Users are provisioned based on the permissions of their assigned groups.

You can create BeyondInsight local groups, or you can use existing Active Directory, Azure Active Directory, or LDAP groups.

***Note:** By default, an **Administrators** user group is created. The permissions assigned to the group cannot be changed. The user account you created when you configured BeyondInsight is a member of the group.*

Create and Edit Directory Credentials

A directory credential is required for querying Active Directory (AD), LDAP, and Azure AD, and also for adding AD, LDAP, and Azure AD groups and users in BeyondInsight. Follow the steps below for creating each type of directory credential.

Note: *Before you can create an Azure AD credential, you must first register and configure permissions for an application in the Azure AD tenant where the user credentials reside. For more information, please see Register and Configure an Application in Azure Active Directory at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/azure-ad-app-registration.htm.*

1. Navigate to **Configuration > Role Based Access > Directory Credentials**.
2. Click **Create New Directory Credential**.
3. Follow the steps in the below sections based on the type of directory you are creating.

Create an Active Directory Credential

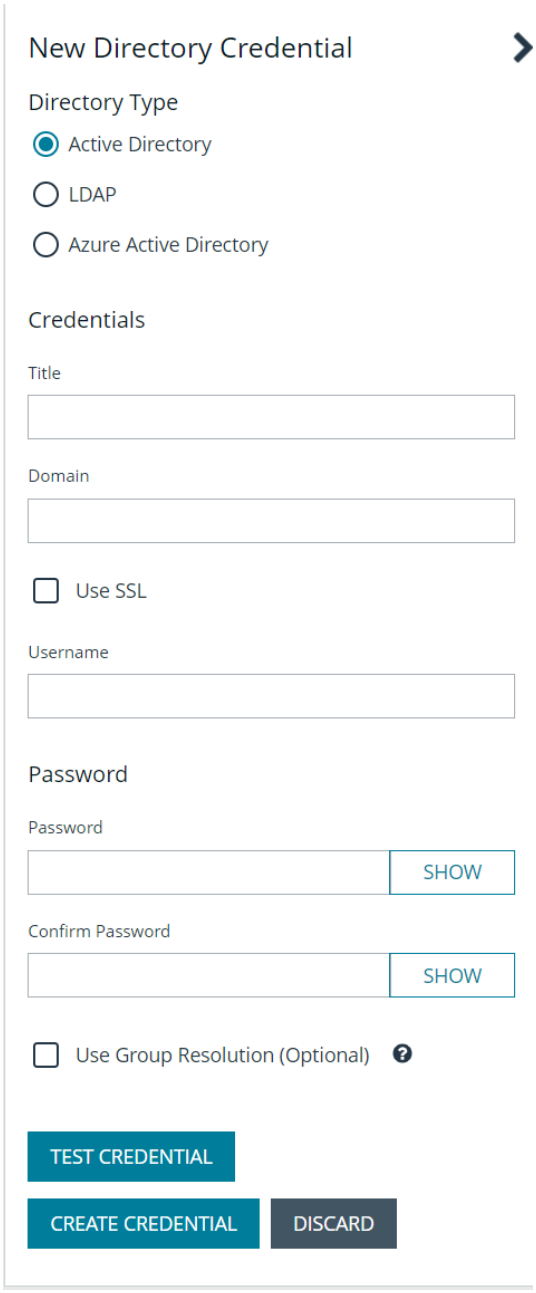
1. Select **Active Directory** for the **Directory Type**.
2. Provide a name for the credential.
3. Enter the name of the domain where the directory and user credentials reside.
4. Enable the **Use SSL** option to use a secure connection when accessing the directory.

> ***Note:*** *If **Use SSL** is enabled, SSL authentication must also be enabled in the BeyondInsight configuration tool.*

4. Enter the credentials for the account that has permissions to query the directory.
5. Enable the **Use Group Resolution** option to use this credential for resolving groups from the directory.

> ***Note:*** *Only one credential can be set for group resolution per domain or server.*

6. Click **Test Credential** to ensure the credential can successfully authenticate with the domain or domain controller before saving the credential.
7. Click **CreateCredential**.



Create an LDAP Credential

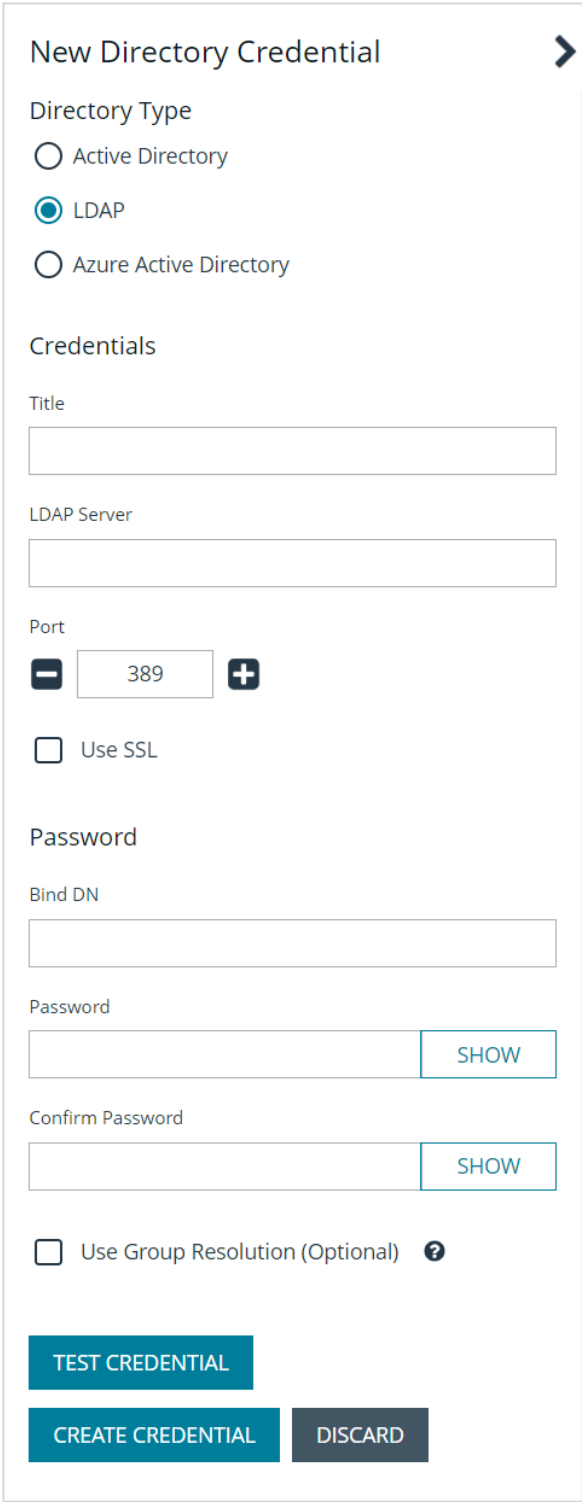
1. Select **LDAP** for the **Directory Type**.
2. Provide a name for the credential.
3. Enter the name of the LDAP server where the directory and user credentials reside.
4. Enable the **Use SSL** option to use a secure connection when accessing the directory.

> ***Note:*** *If **Use SSL** is enabled, SSL authentication must also be enabled in the BeyondInsight configuration tool.*

5. Enter the credentials for the account that has permissions to query the directory.
6. Enable the **Use Group Resolution** option to use this credential for resolving groups from the directory.

> ***Note:*** *Only one credential can be set for group resolution per LDAP server.*

7. Click **Test Credential** to ensure the credential can successfully authenticate with the domain or domain controller before saving the credential.
8. Click **Create Credential**.

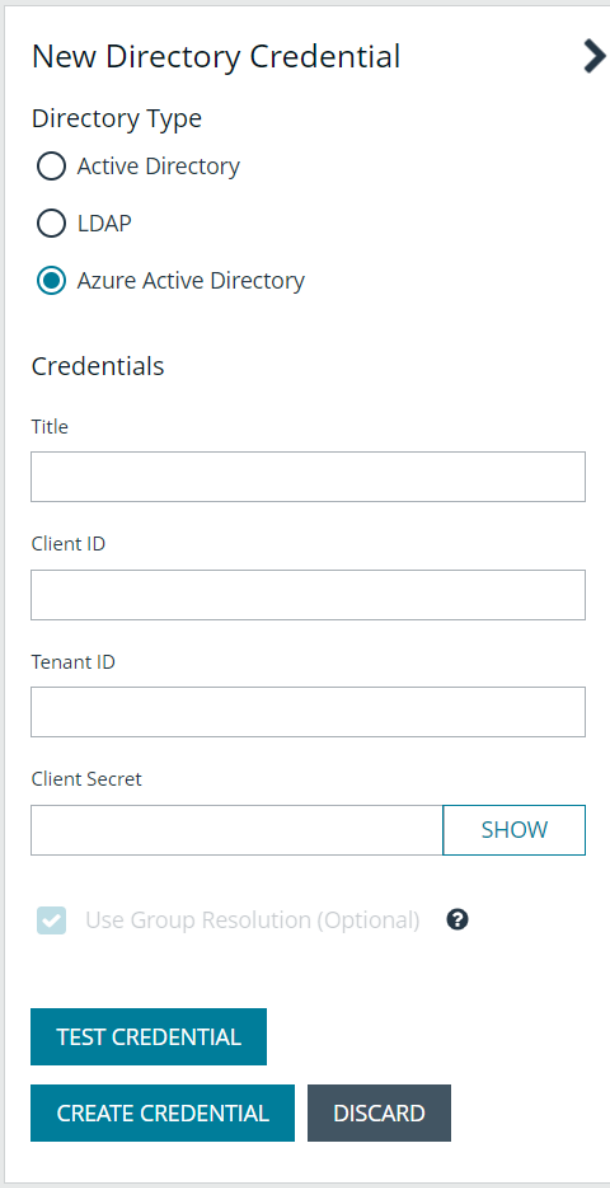


Create an Azure Active Directory Credential

1. Select **Azure Active Directory** for the **Directory Type**.
2. Provide a name for the credential.
3. Paste the **Client ID**, **Tenant ID**, and **Client Secret** that you copied when registering the application in your Azure AD tenant.
4. Enable the **Use Group Resolution** option to use this credential for resolving groups from the directory.

> ***Note:*** *Only one credential is supported per Azure AD tenant.*

5. Click **Test Credential** to ensure the credential can successfully authenticate with the domain or domain controller before saving the credential.
6. Click **Save Credential**.



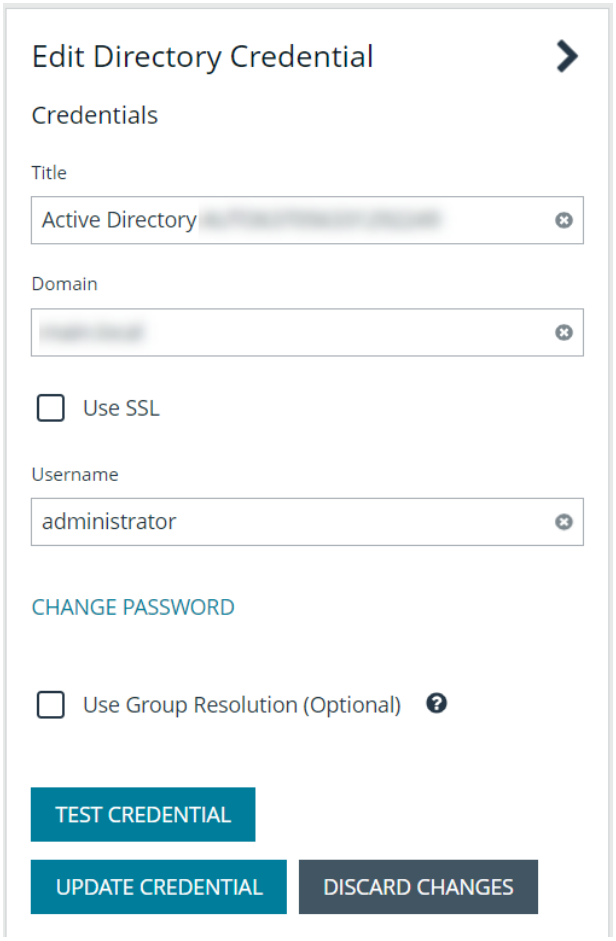
Edit a Directory Credential

1. From the **Directory Credentials** grid, click the vertical ellipsis for the credential, and then select **Edit**.

2. Make the changes required.

> ***Note:*** *For AD or LDAP credentials, if you change the* ***Domain*** *or* ***LDAP Server****, enable or disable the* ***Use SSL*** *option, or update the* ***Username*** *or* ***Bind DN****, you must change the password. Click* ***Change Password*** *to display fields to enter and confirm the new password.*

3. Click **Test Credential** to ensure the edited credential can successfully authenticate with the domain or domain controller before saving the credential.
4. Click **Save Credential**.



> ***Note:*** *To use Azure Active Directory credentials for logging into BeyondInsight, the accounts must use SAML authentication. For more information on configuring Azure AD SAML with BeyondInsight, please see Configure Azure Active Directory SAML with BeyondInsight SAML at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/security-provider.htm#configure-azure-ad.*

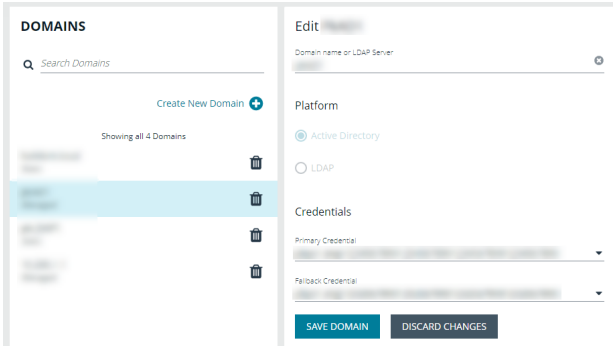
Map Directory Credentials to a Domain

Domain management allows you to map a default primary directory credential and an optional fallback credential as preferred binding credentials used for account resolution against domains in your environment when logging in to BeyondInsight.

> ***Note:*** *If credentials are not mapped, or both mapped credentials fail, BeyondInsight attempts login following the legacy process of not using mapped credentials.*

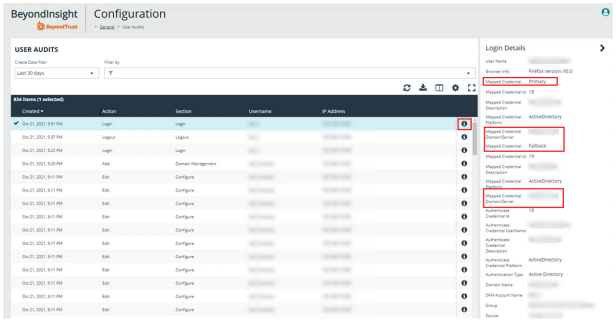
Follow these steps to add or edit primary and secondary credentials for a domain:

1. Navigate to **Configuration > Role Based Access > Domain Management**.
2. Click **Create New Domain** to create a new one.
3. Provide the name of the domain or LDAP server.
4. Select the type of platform.
5. Select a **Primary Credential** from the dropdown.
6. Select a **Fallback Credential** from the dropdown.
7. Click **Create Domain**.
8. To edit credentials for an existing domain, select the domain, make your edits, and then click **Save Domain**.



> ***Tip:*** *Primary and fallback credentials can include Password Safe managed accounts.*

When domain management is configured for a domain and user selects the domain when logging into BeyondInsight, the specified primary and fallback credentials are used to resolve their account. The credentials used for authentication are shown in the **Login Details** for the specific login activity on the **Configuration > General > User Audits** page.

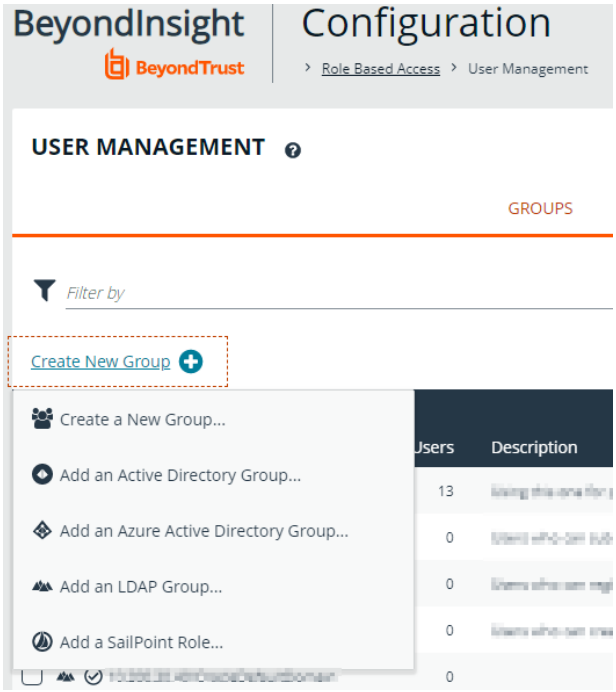


Create and Configure Groups

Create user groups and user accounts so that your BeyondInsight administrators can log in to BeyondInsight.

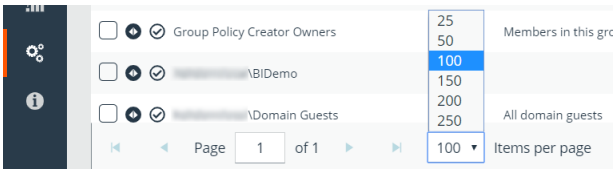
When a user is added to a group, the user is assigned the permissions assigned to the group.

You can create BeyondInsight local groups, as well as add Active Directory, Azure Active Directory, and LDAP groups into BeyondInsight.



You can filter the groups displayed in the grid by type of group, name of the group, group description, and the date the group was last synchronized.

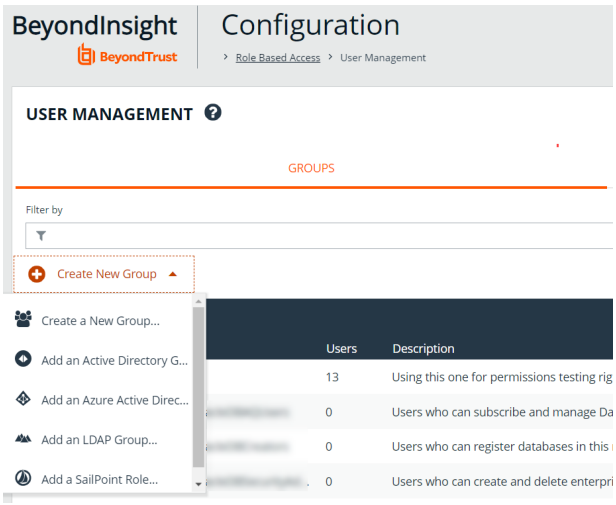
> ***Tip:*** *By default, the first 100 groups are displayed per page. You can change this by selecting a different number from the Items per page dropdown at the bottom of the grid.*



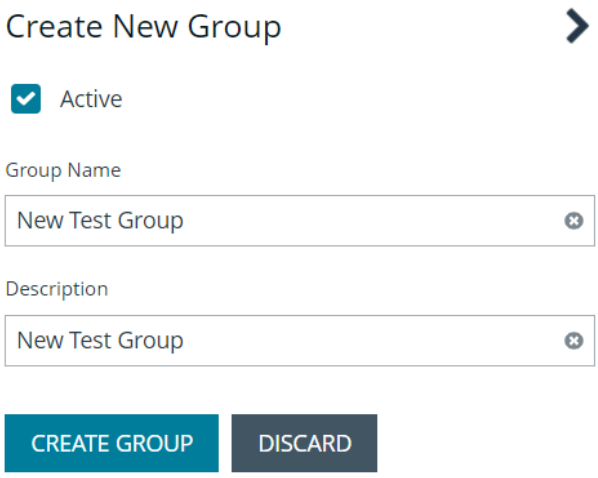
Create a BeyondInsight Local Group

1. Navigate to **Configuration > Role Based Access > User Management**.

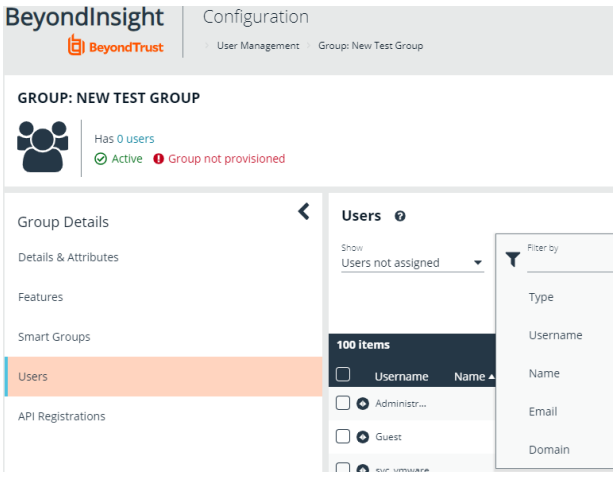
2. Under **Groups**, click **Create New Group**.
3. Select **Create a New Group**.



4. Enter a **Group Name** and **Description** for the group.
5. The group is set to **Active** by default. Check the box to deactivate it, if you prefer to activate it later.
6. Click **Create Group**.



7. Assign users to the group:
   - Under **Group Details**, select **Users**.
   - From the **Show** dropdown list, select **Users not assigned**.
   - Filter the list of users displayed in the grid by **Type**, **Username**, **Name**, **Email**, and **Domain**, if desired.



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

Note: *By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 40.*

Note: *When a local user logs in to BeyondInsight for the first time using SAML authentication, BeyondInsight provisions their account by mapping it to the groups assigned to their account.*

For releases prior to 21.3, and for upgrades to the 21.3 release, if the user account's group membership has changed (in the SAML claims provided) upon subsequent logins, BeyondInsight does not deprovision the user by removing them from the groups that were initially mapped to their account. Instead, BeyondInsight maps the user to any newly assigned groups, in addition to the groups their account is already mapped to.

You can configure BeyondInsight to synchronize group membership each time a local user logs in using SAML, as follows:

1. *Navigate to **Configuration > Authentication Management > Authentication Options**.*
2. *Under **SAML Logon for Local Users**, toggle the **Enable Group Resync** option to enable it.*

For new installs of release 21.3 and later releases, this option is enabled by default.

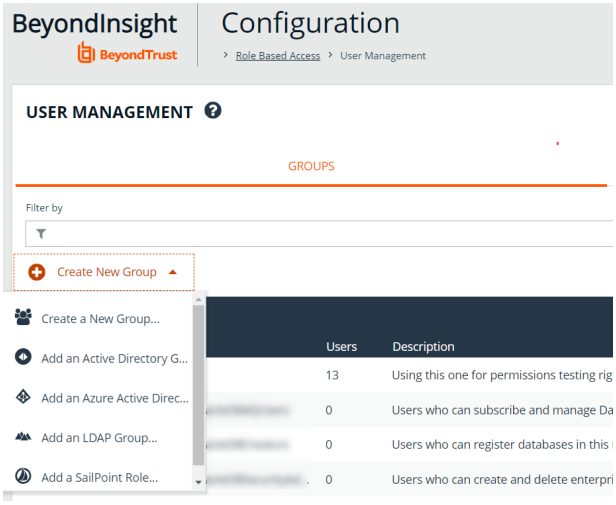
Add an Active Directory Group

Active Directory group members can log in to the management console and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller. Upon logging into BeyondInsight, users can select a domain from the **Log in to** list on the **Login** page.

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

***Note:** Active Directory users must log in to the management console at least once to receive email notifications.*

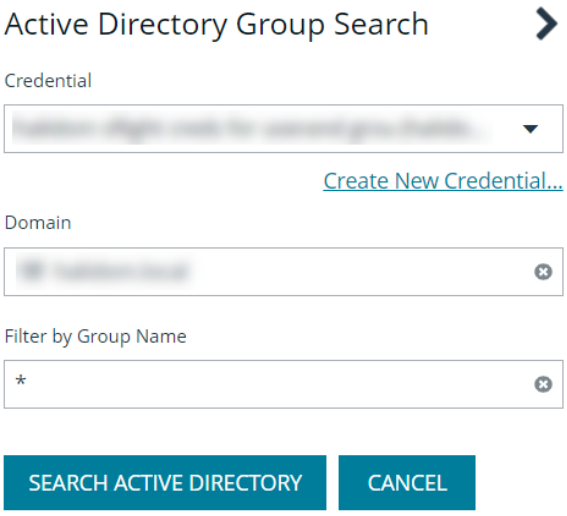
1. Navigate to **Configuration > Role Based Access > User Management**.
2. Under **Groups**, click **Create New Group**.
3. Select **Add an Active Directory Group**.



4. Select a credential from the list.

> ***Note:*** *If you require a new credential, click* ***Create New Credential*** *to create one. The new credential is added to the list of available credentials.*

5. If the **Domain** field is not automatically populated, enter the name of a domain or domain controller.
6. After you enter the domain or domain controller credential information, click **Search Active Directory**. A list of security groups in the selected domain is displayed.

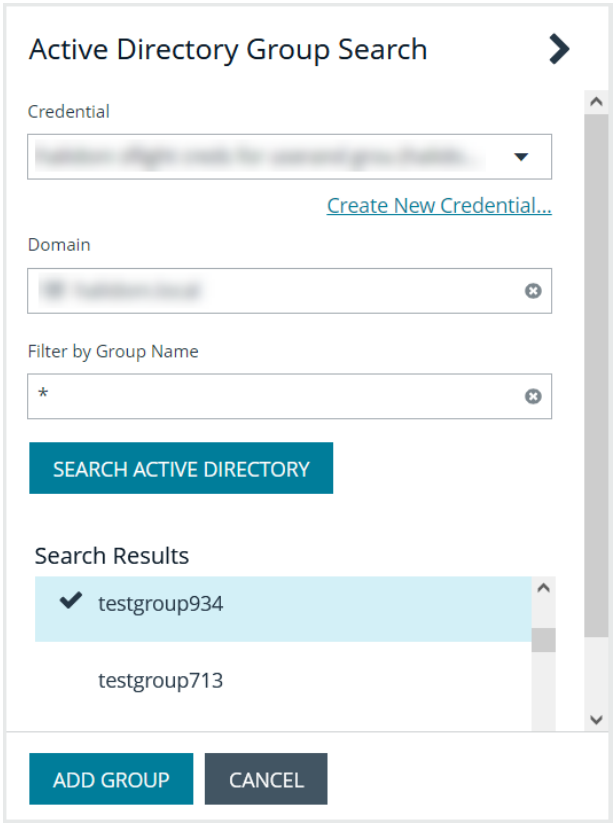


> ***Note:*** *The default filter is an asterisk (*), which is a wild card filter that returns all groups. For performance reasons, a maximum of 250 groups from Active Directory is retrieved.*

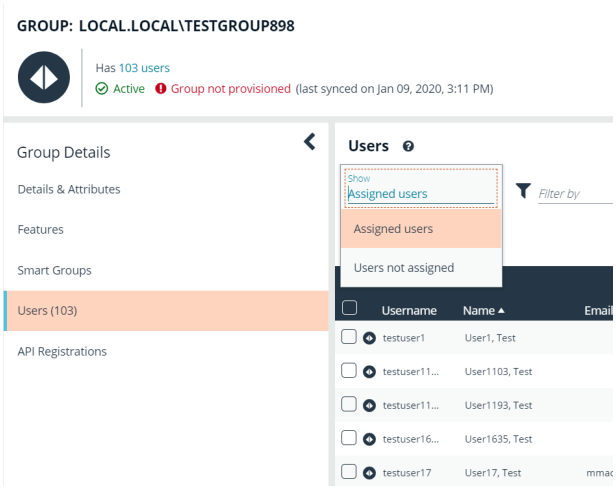
7. Set a filter on the groups to refine the list, and then click **Search Active Directory**.

> ***Example:*** *Sample filters:*
> - ***a**** *returns all group names that start with "a"*
> - ****d*** *returns all group names that end with "d"*
> - ****sql**** *returns all groups that contain "sql" in the name*

8. Select a group, and then click **Add Group**.



9. The group is added and set to **Active** but not provisioned or synchronized with Active Directory. Synchronization with Active Directory to retrieve users begins immediately.
10. Once the group has been synced with Active Directory, you can view the users assigned to the group, as well as unassigned users, by selecting **Users** from the **Group Details** section and then using the filters.



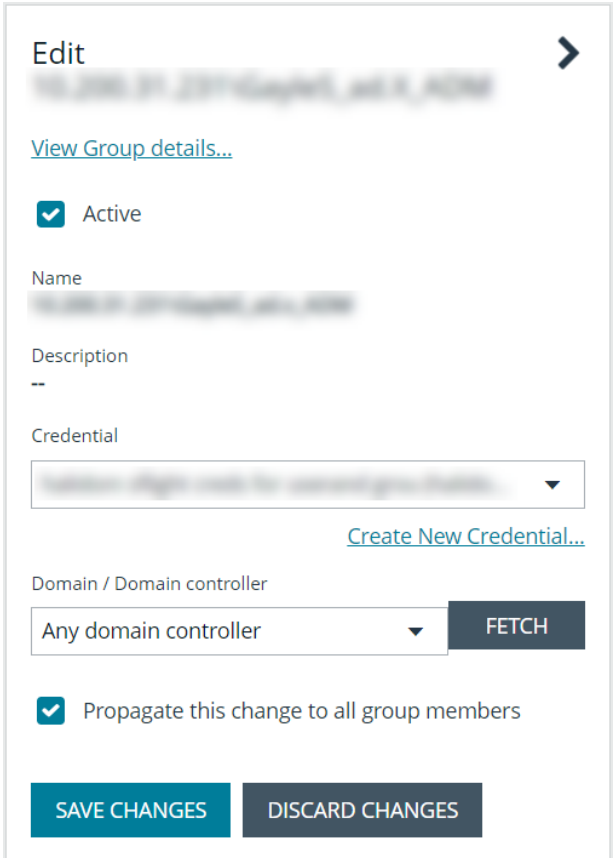
Note: *By default, new groups are not assigned any permissions. You must assign permissions on features and Smart Groups after creating a new group. For more information on permissions and how to assign them, please see* *"Assign Group Permissions" on page 40*.

For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 19.

Propagate Domain Changes

Domain changes can be propagated to all users in a group. By default, this is set to OFF. When enabled, changes to the preferred domain controller at the group level are applied to all group members.

When creating a new group, we advise turning this setting on by editing the new group details. This ensures that all users in the new group get a Preferred Domain Controller from the initial setup of the group.



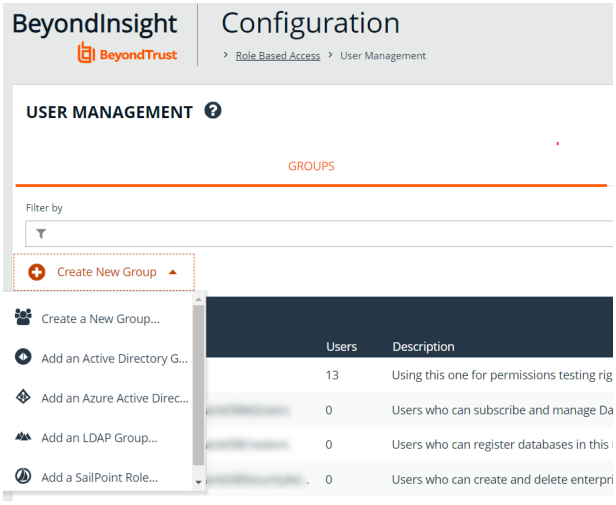
Add an Azure Active Directory Group

Azure Active Directory (AD) group members can log in to the management console using SAML authentication and perform tasks based on the permissions assigned to the group. Upon logging into BeyondInsight, users can select a domain from the **Log in to** list on the **Login** page.

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

> ***Note:*** *AD users must log in to the management console at least once to receive email notifications.*

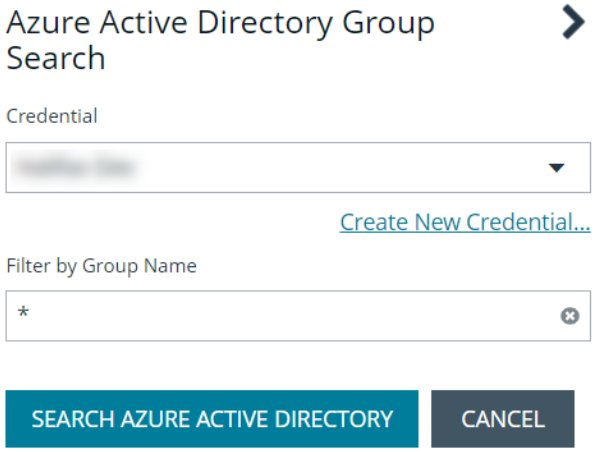
1. Navigate to **Configuration > Role Based Access > User Management**.
2. Under **Groups**, click **Create New Group**.
3. Select **Add an Azure Active Directory Group**.



4. Select a credential from the list.

> ***Note:*** *If you require a new credential, click **Create a New Credential** to create a new credential. The new credential is added to the list of available credentials.*

5. Click **Search Azure Active Directory**. A list of security groups displays.

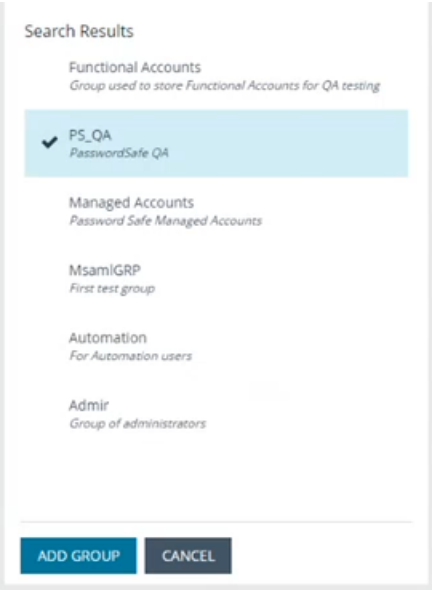


> ***Note:*** *For performance reasons, a maximum of 250 groups from Azure AD is retrieved. The default filter is an asterisk (*), which is a wildcard filter that returns all groups. Use the group filter to refine the list.*

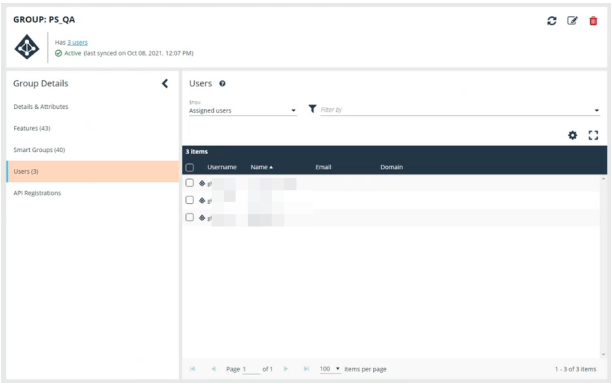
6. Set a filter on the groups that are to be retrieved, and then click **Search Azure Active Directory**.

> ***Example:*** *Sample filters:*
> - ***a**** *returns all group names that start with a.*
> - ****d*** *returns all group names that end with d.*
> - ****sql**** *returns all groups that contain sql in the name.*

7. Select a group, and then click **Add Group**.



8. The group is added and set to **Active** but not provisioned or synchronized with Azure AD. Synchronization with Azure AD to retrieve users begins immediately.
9. Once the group has been synced with Azure AD, you can view the users assigned to the group, as well as unassigned users, by selecting **Users** from the **Group Details** section and then using the filters.



Note: *By default, new groups are not assigned any permissions. You must assign permissions on features and Smart Groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 40.*

Note: *To use Azure Active Directory credentials for logging into BeyondInsight, the accounts must use SAML authentication. For more information on configuring Azure AD SAML with BeyondInsight, please see Configure Azure Active Directory SAML with BeyondInsight SAML at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/security-provider.htm#configure-azure-ad.*

For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 19.

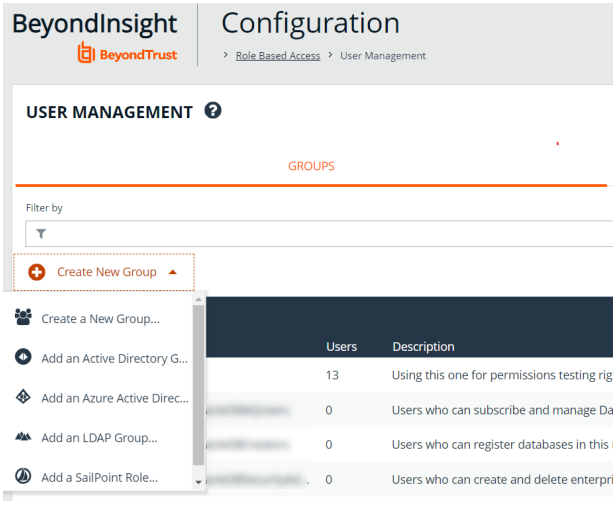
Add an LDAP Group

LDAP group members can log in to the management console and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller. Upon logging in to BeyondInsight, users can select a domain or LDAP server from the **Log in to** list on the **Login** page.

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

***Note:** LDAP users must log in to the management console at least once to receive email notifications.*

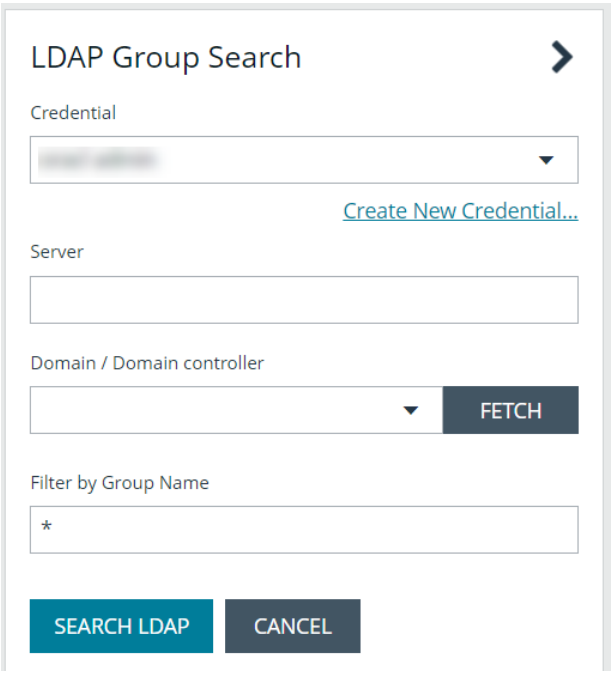
1. Navigate to **Configuration > Role Based Access > User Management**.
2. Under **Groups**, click **Create New Group**.
3. Select **Add an LDAP Group** from the list.



4. Select a credential from the list.

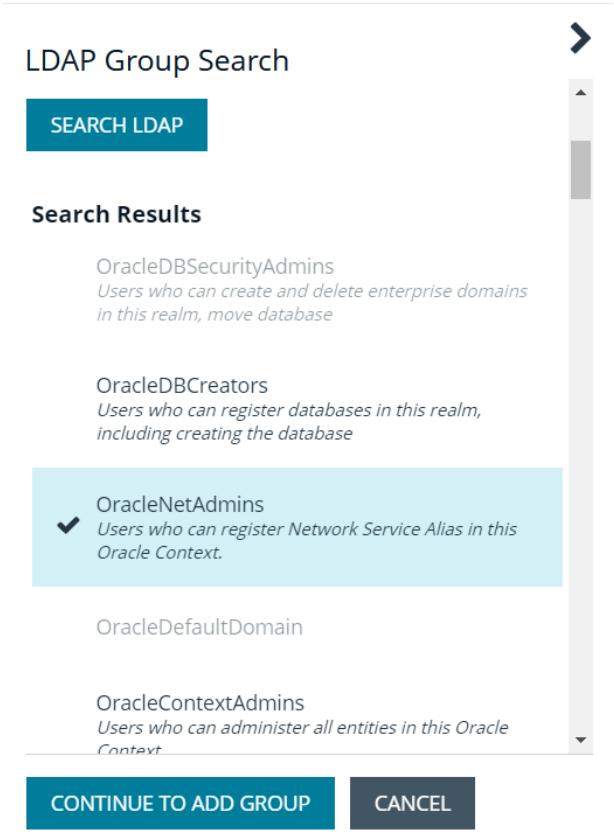
> ***Note:*** *If you require a new credential, click* ***Create a New Credential*** *to create a new one. The new credential is added to the list of available credentials.*

5. Click **Fetch** to load the list of Domain Controllers, and then select one.
6. To filter the group search, enter keywords in the group filter or use a wild card, and then click **Search LDAP**.

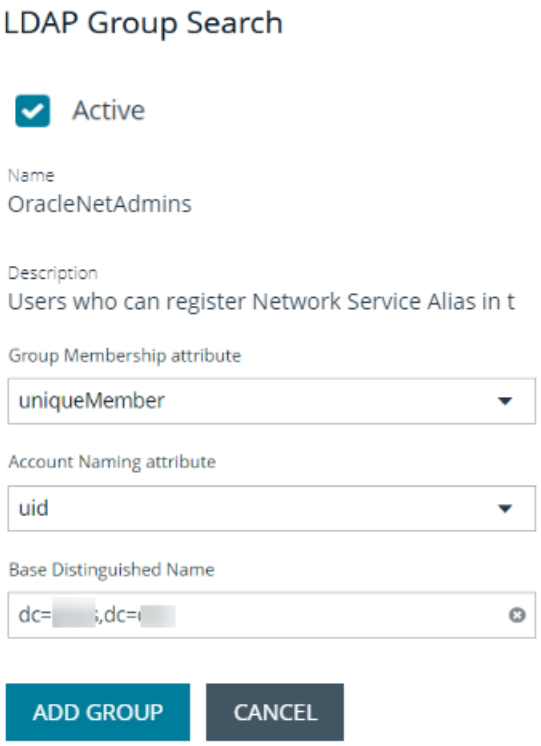


> ***Example:*** *Sample filters:*
> - ***a**** *returns all group names that start with a.*
> - ****d*** *returns all group names that end with d.*
> - ****sql**** *returns all groups that contain sql in the name.*

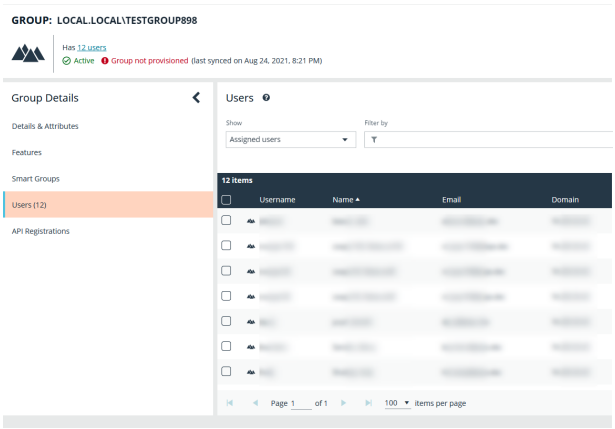
7. Select a group, and then click **Continue to Add Group**.



8. Select the **Group Membership Attribute** and **Account Naming Attribute**.
9. Enter a **Base Distinguished Name**, if not automatically populated.
10. Click **Add Group**.



11. The group is added and set to **Active** but is not provisioned or synchronized with LDAP. Synchronization with LDAP to retrieve users begins immediately.
12. Once the group has been synced with LDAP, you can view the users assigned to the group, as well as unassigned users, by selecting **Users** from the **Group Details** section, and then using the filters.



Note: *By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see* *"Assign Group Permissions" on page 40*.

For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 19.

Assign Group Permissions

Permissions

The following permissions may be assigned to user groups in BeyondInsight for each feature.

Permission	Description
No Access	Users cannot access the selected feature. In most cases, the feature is not visible to the users.
Read Only	Users can view selected areas, but cannot change information.
Full Control	Users can view and change information for the selected feature.

Permissions for a BeyondInsight user must be assigned cumulatively and at the group level. You must assign permissions on features and Smart Groups after creating a new group in order for users in that group to be able to access features in the product. For example, if you want a BeyondInsight administrator to manage discovery scans only, then you must assign full control for the following features:

- **Management Console Access**
- **Asset Management**
- **Reports Management**
- **Scan – Job Management**
- **Scan Management**

Note: *In addition to the group permissions noted, for the group to be provisioned, there must be at least one enabled Smart Group on the group. This sets the scope for the features.*

Assign Features Permissions

Note: *The features listed are based upon your BeyondInsight license. Only features relevant to your licensed installation are listed.*

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Click the vertical ellipsis button for the group, and then select **View Group Details**.
3. Under **Group Details**, click **Features**.
4. Filter the list of features displayed in the grid using the **Show** and **Filter by** dropdown lists.
5. Select the features you wish to assign permissions to, and then click **Assign Permissions** above the grid.
6. Select **Assign Permissions Read Only**, **Assign Permissions Full Control**, or **Disable Permissions**.

The following table provides information on the features permissions you can assign to your groups.

Feature	Provides Permissions To:
Analytics & Reporting	Log in to the console and access **Analytics & Reporting** to generate and subscribe to reports. ***Note:*** *After you create a group, go to the* ***Analytics & Reporting Configuration*** *page and run the process daily cube job. Data between the management console and the reporting cube must be synchronized.*
Appliance (U-Series) Access	Grant access to manage the U-Series Appliance as a BeyondInsight user.
Asset Management	Create Smart Rules. Edit and delete buttons on the **Asset Details** window. Create Active Directory queries. Create address groups.
Attribute Management	Add, rename, and delete attributes when managing user groups.
Credential Management	Add and change credentials when running scans and deploying policies.
Directory Credential Management	Grant access to the configuration area where directory credentials are managed. This feature must be enabled to support access to directory queries as well.
Directory Query Management	Grant access to the configuration area where directory queries are managed. ***Note:*** *Access to Directory Credential Management must also be granted.*
Domain Management	Grants the user permission to configure mappings of bind credentials to domains for account resolution.
Endpoint Privilege Management	Grant access to the Endpoint Privilege Management features, excluding Policy Editor and Reporting.
Endpoint Privilege Management Policy Editor	Grant access to the Endpoint Privilege Management Policy Editor feature.
Endpoint Privilege Management Reporting	Grant access to the Endpoint Privilege Management Reporting feature.
Endpoint Privilege Management for Unix & Linux	Grant access to the Endpoint Privilege Management for Unix & Linux features.
File Integrity Monitoring	Work with **File Integrity** rules.
License Reporting	View the **Licensing** folder in **Analytics & Reporting** (MSP reports, Privilege Management for Windows, Privilege Management for Mac true-up reports, and Assets Scanned report).
Management Console Access	Access the BeyondInsight management console.
Manual Range Entry	Allow the user to manually enter ranges for scans and deployments rather than being restricted to smart groups. The specified ranges must be within the selected smart group.
Option Management	Change the application options settings (for example, account lockout and account password settings).
Options - Connectors	Access the configuration area where connectors are managed.
Options - Scan Options	Access the configuration area where scan options are managed.

Feature	Provides Permissions To:
Password Safe Account Management	Grant read or write permissions to the following features on the **Managed Accounts** page and through the public API: • Bulk delete accounts • Add accounts to a Quick Group • Remove accounts from a Quick Group • Add, edit, and delete accounts
Password Safe Admin Session	Password Safe web portal admin sessions.
Password Safe Admin Session Reviewer	Grant a user admin session reviewer permissions only.
Password Safe Global API Quarantine	Access to the Quarantine APIs.
Password Safe Bulk Password Change	Change more than one password at a time.
Password Safe Domain Management	Check the **Read** and **Write** boxes to permit users to manage domains.
Password Safe Role Management	Allow a user to manage roles, provided they have the following permissions: **Password Safe Role Management** and **User Account Management**.
Password Safe System Management	Read and write managed systems through the public API.
Password Safe Ticket System Management	This feature is not presently used.
Reports Management	Run scans, create reports, and create report categories.
Scan - Job Management	Activate **Scan** and **Start Scan** buttons. Activate **Abort**, **Resume**, **Pause**, and **Delete** on the **Job Details** page.
Scan - Report Delivery	Allow a user to set report delivery options when running a scan: • Export Type • Notify when complete • Email report to • Include scan metrics in email (only available for All Audits Scan)
Scan Management	Delete, edit, duplicate, and rename reports on the **Manage Report Templates** page. Activate **New Report** and **New Report Category**. Activate the **Update** button on the **Edit Scan Settings** view.
Secrets Safe	Provides access to Secrets Safe for all members of the selected group.
Session Monitoring	Use the session monitoring features.

Feature	Provides Permissions To:
Smart Rule Management – Asset	Grants permission to view, create, and edit asset Smart Rules; editing is limited to Smart Rules that are enabled for groups the user is a member of. ***Note:*** *Newly created Smart Rules created by a non-administrator are automatically enabled with read permissions for all groups that the user is a member of, and with full permissions for all groups that the user is a member of AND has the Asset Management permissions for. For more information, see "Use Smart Rules to Organize Assets" on page 66.*
Smart Rule Management – Managed Account	Grants permission to view, create, and edit managed account Smart Rules; editing is limited to smart rules that are enabled for groups the user is a member of. ***Note:*** *Newly created Smart Rules created by a non-administrator are automatically enabled with read permissions for all groups that the user is a member of, and with full permissions for all groups that the user is a member of AND has the Asset Management permissions for. For more information, see "Use Smart Rules to Organize Assets" on page 66.*
Smart Rule Management – Managed System	Grants permission to view, create, and edit managed system Smart Rules; editing is limited to smart rules that are enabled for groups the user is a member of. ***Note:*** *Newly created Smart Rules created by a non-administrator are automatically enabled with read permissions for all groups that the user is a member of, and with full permissions for all groups that the user is a member of AND has the Asset Management permissions for. For more information, see "Use Smart Rules to Organize Assets" on page 66.*
Smart Rule Management – Policy User	Grants permission to view, create, and edit policy user Smart Rules; editing is limited to smart rules that are enabled for groups the user is a member of. ***Note:*** *Newly created Smart Rules created by a non-administrator are automatically enabled with read permissions for all groups that the user is a member of, and with full permissions for all groups that the user is a member of AND has the Asset Management permissions for. For more information, see "Use Smart Rules to Organize Assets" on page 66.*
Ticket System	View and use the ticket system.
Ticket System Management	Mark a ticket as inactive. The ticket no longer exists when **Inactive** is selected.
User Accounts Management	Add, delete, or change user groups and user accounts. A minimum of read access to Directory Credential Management must also be granted to enable creation of AD and LDAP Groups.
User Audits	View audit details for management console users on the **User Audits** page.
U-Series Appliance Administrator	Provides access to manage all aspects of the U-Series Appliance.
U-Series Appliance Backups	Provides access to manage the **Backup and Restore** options of the U-Series Appliance.

Feature	Provides Permissions To:
U-Series Appliance High Availability	Provides access to manage the **High Availability** features of the U-Series Appliance.
U-Series Appliance Login	Provides access to manage the U-Series Appliance as a BeyondInsight user.
U-Series Appliance Manage RDP	Provides access to manage Remote Desktop Protocol to the U-Series Appliance.
U-Series Appliance Patching	Provides access to manage updates to the U-Series Appliance.

For more information, please see the Managed Accounts section in the BeyondInsight and Password Safe API Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/api/password-safe/managed-accounts.htm.

Features Permissions Required for Configuration Options

Configuration Option	Feature and Permission
Active Directory Queries	Asset Management - Full Control.
Address Groups	Asset Management - Full Control.
Attributes	Asset Management - Full Control.
Connectors	Asset Management and Management Console Access - Full Control.
Organizations	User Accounts Management - Full Control.
Password Safe Connections	Member of the built-in BeyondInsight Administrators group.
Endpoint Privilege Management Module	Management Console Access and Endpoint Privilege Management - Full Control.
Scan Options	Scan Management - Full Control.
Services	Member of the built-in BeyondInsight Administrators group.
User Audits	User Audits - Full Control.
User Management	Everyone can access. Users without the Full Control permission to **User Account Management** feature can edit only their user record.
Workgroups	User Accounts Management - Full Control.

Assign Smart Groups Permissions

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Click the vertical ellipsis button for the group, and then select **View Group Details**.
3. Under **Group Details**, select **Smart Groups**.
4. Filter the list of Smart Groups displayed in the grid using the **Show** and **Filter by** dropdown lists.
5. Select the Smart Groups you wish to assign permissions to, and then click **Assign Permissions** above the grid.
6. Select **Assign Permissions Read Only**, **Assign Permissions Full Control**, or **Disable Permissions**.

Edit and Delete Groups

Edit Basic Group Details

Administrators can edit the following basic details for groups:

- For BeyondInsight local groups, administrators can change the active status, name, and description.
- For Active Directory groups, administrators can change the active status, credential, and domain controller.
- For LDAP groups, administrators can change the active status, credential, group membership attribute, and account naming attribute.

Follow these steps to edit a group:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Optionally, filter the list of groups in the grid by **Type**, **Name**, **Description**, or **Last Synchronization Date**.
3. Click the vertical ellipsis for the group, and then select **Edit Group**.
4. In the **Edit Group** pane, update the details as required, and then click **Update Group**.
    - For BeyondInsight local groups, administrators can change the active status, name, and description.
    - For Active Directory groups, administrators can change the active status, credential, and domain controller.
    - For LDAP groups, administrators can change the active status, credential, group membership attribute, account naming attribute, and base distinguished name.

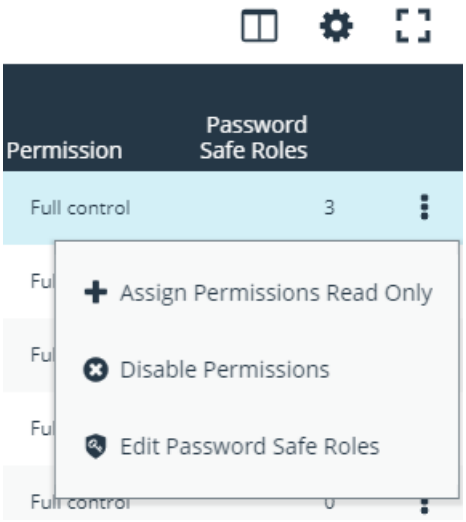
Edit Advanced Group Details

Administrators can edit advanced details, such as update permissions for features and smart groups, edit Password Safe roles, add and remove users from local groups, sync group users for Active Directory and LDAP groups, and update the API registrations.

Update Group Permissions for Features and Smart Groups

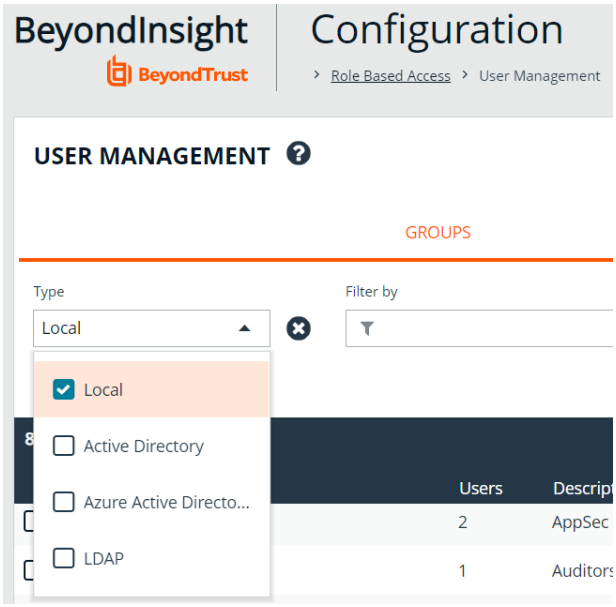
1. On the **User Management** page, optionally filter the list of groups in the grid by **Type**, **Name**, **Description**, or **Last Synchronization Date** to locate the group.
2. Click the vertical ellipsis button for the group, and then select **View Group Details**.

3. Select the desired features or Smart Groups, click the ellipsis button for the feature or Smart Group, and then select to assign or disable permissions accordingly.



Remove Users from Local BeyondInsight Groups

1. On the **User Management** page, filter the grid by local groups.



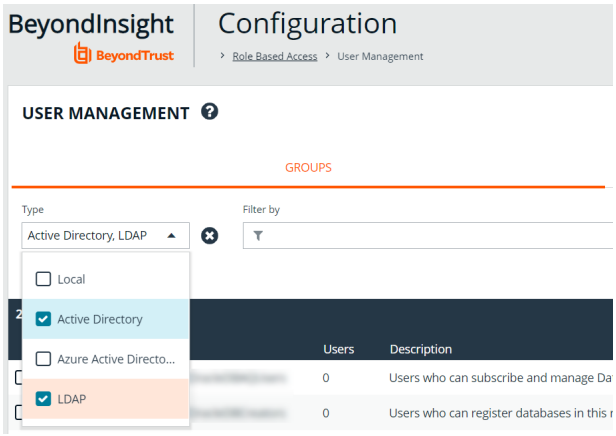
2. Click the vertical ellipsis button for the group, and then select **View Group Details**.
3. Under **Group Details**, select **Users**.
4. Filter the **Users** grid to show assigned users.
5. Select the user or users, and then click **Remove User** above the grid.

Add Users to Local BeyondInsight Groups

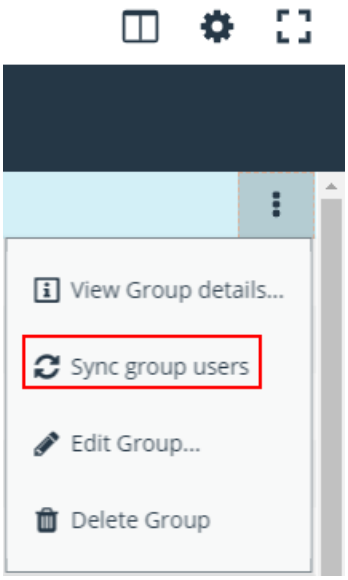
1. On the **User Management** page, filter the grid by local groups.
2. Click the vertical ellipsis button for the group, and then select **View Group Details**.
3. Under **Group Details**, select **Users**.
4. Filter the **Users** grid to show unassigned users.
5. Select the user or users, and then click **Assign User** above the grid.

Sync Group Users for Active Directory and LDAP Groups

1. On the **User Management** page, filter the grid by Active Directory and LDAP groups.



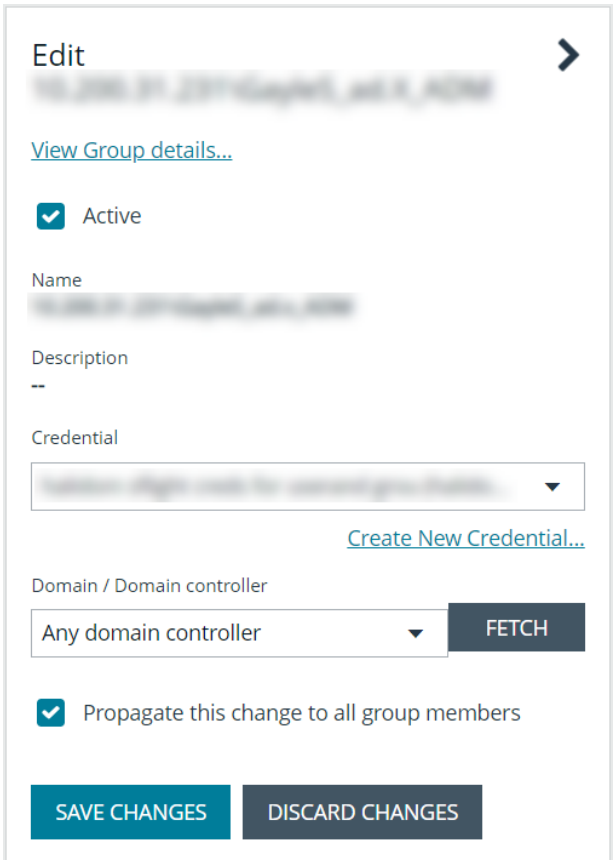
2. Click the vertical ellipsis button for the group, and then select **Sync Group Users**.



Propagate Domain Changes

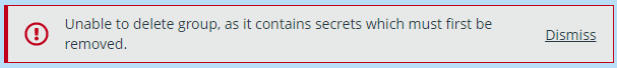
Domain changes can be propagated to all users in a group. By default, this is set to OFF. When enabled, changes to the preferred domain controller at the group level are applied to all group members.

When creating a new group, we advise turning this setting on by editing the new group details. This ensures that all users in the new group get a Preferred Domain Controller from the initial setup of the group.



Delete a Group

Note: *Groups associated with a secret or credential in Secrets Safe cannot be deleted. Users attempting this action receive the following warning:*



Administrators can delete groups as follows:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Optionally, filter the list of groups in the grid by **Type**, **Name**, **Description**, or **Last Synchronization Date**.
3. Select a group, and then click the **Delete** button above the grid, or click the vertical ellpsis button for the group, and then select **Delete Group**.

Create and Manage User Accounts

User accounts create the user identity that BeyondInsight uses to authenticate and authorize access to specific system resources. You can create local BeyondInsight users, as well as add Active Directory, Azure Active Directory, and LDAP users into BeyondInsight.

Note: *A user account must be a member of a BeyondInsight group. If a user is not a member of any groups in BeyondInsight, the user cannot log in to the console.*

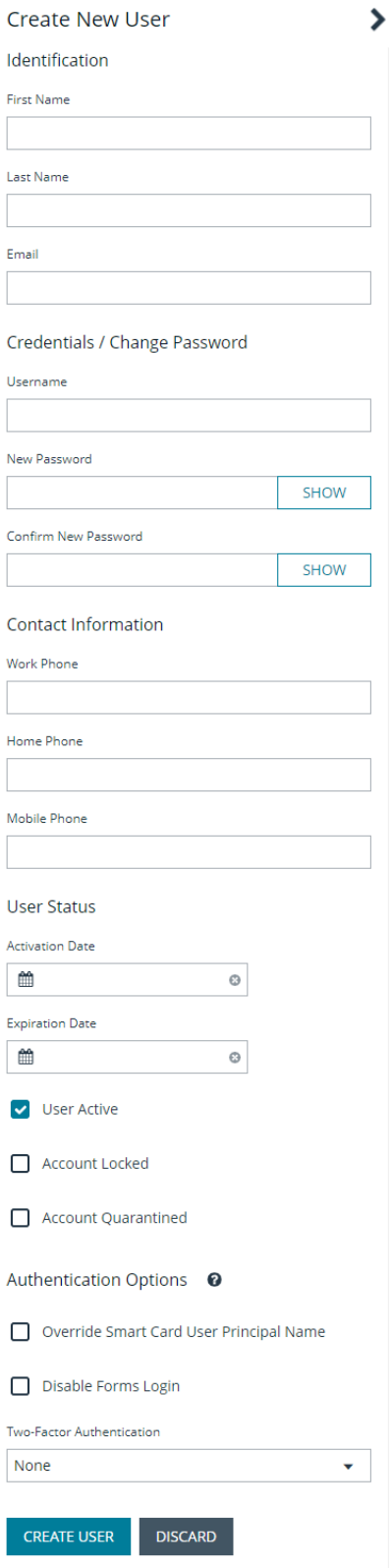
Create a BeyondInsight Local User Account

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Click **Users** to display the list of users in the grid.
3. Click **Create New User** above the grid.
4. Select **Create a New User**.

5. Complete the **Identification** and **Credentials / Change Password** sections. These fields are required.
6. Optionally, enter the user's contact information.
7. Select an **Activation Date** and an **Expiration Date** for the user account.

> ***Note:*** *These dates are based on UTC time on the BeyondInsight server and are considered during the user's login attempt. The attempt fails if the user account is not yet active or if the expiration date has passed.*

8. Check **User Active** to activate the user account.
9. Leave the **Account Locked** and **Account Quarantined** options unchecked.
10. Check the two **Authentication Options**, if applicable:
    - **Override Smart Card User Principal Name**: when enabled, allows a BeyondInsight user with a smart card that has a different Subject Alternative Name to log in to BeyondInsight and maps the smart card to the user.
    - **Disable Login Forms**: when enabled, disallows SAML users from using the standard BeyondInsight log in form. Check this option only if SAML is configured in your environment. Users authenticate with third party identity provider.
11. Select a **Two-Factor Authentication** method and mapping information, if applicable.
12. Click **Create User**.



13. The user is created and **User Details > Groups** is displayed. You can filter the list of groups displayed by type, name, or description. Select a group, and then click **Assign Group** above the grid.

> ***Note:*** *The user must belong to at least one group*

14. To remove the user from a group, select **Assigned Groups** from the **Show** dropdown, and then select a group and click **Remove Group**.

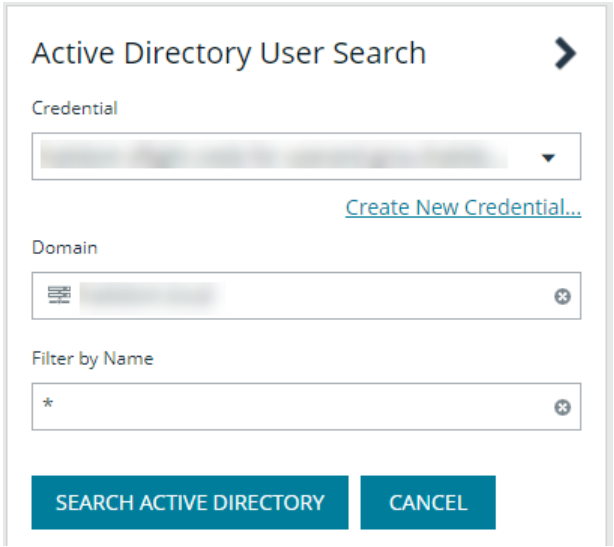
Add an Active Directory User

Active Directory users can log in to the management console and perform tasks based on the permissions assigned to their groups. The user can authenticate against either a domain or domain controller.

> ***Note:*** *Active Directory users must log in to the management console at least once to receive email notifications.*

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Click **Users** to display the list of users in the grid.
3. Click **Create New User** above the grid.
4. Select **Add an Active Directory User**.
5. Select a credential from the list.

> ***Note:*** *If you require a new credential, click* ***Create a New Credential*** *to create a new credential. The new credential is added to the list of available credentials.*



6. If not automatically populated, enter the name of a domain or domain controller.
7. After you enter the domain or domain controller credential information, click **Search Active Directory**. A list of users in the selected domain is displayed.

> ***Note:*** *For performance reasons, a maximum of 250 users from Active Directory is retrieved. The default filter is an asterisk (*), which is a wild card filter that returns all users. Filter by user name to refine the list.*

> ***Example:*** *Sample filters:*
> - ***a**** *returns all group names that start with a.*
> - ****d*** *returns all group names that end with d.*
> - ****sql**** *returns all groups that contain sql in the name.*

8. Click **Search Active Directory**.

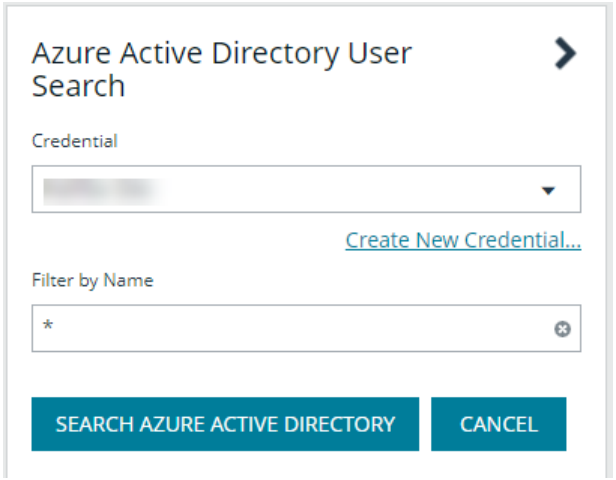
9. Select a user, and then click **Add User**.
10. Assign at least one group to the user.

Add an Azure Active Directory User

Azure Active Directory users can log in to the management console and perform tasks based on the permissions assigned to their groups. The user can authenticate against either a domain or domain controller.

> ***Note:*** *Azure Active Directory users must log in to the management console at least once to receive email notifications.*

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Click **Users** to display the list of users in the grid.
3. Click **Create New User** above the grid.
4. Select **Add an Azure Active Directory User**.
5. Select a credential from the list.



> ***Note:*** *If you require a new credential, click* ***Create a New Credential*** *to create a new credential. The new credential is added to the list of available credentials.*

> ***Note:*** *For performance reasons, a maximum of 250 users from Azure Active Directory is retrieved. The default filter is an asterisk (*), which is a wild card filter that returns all groups. Filter by user name to refine the list.*

> ***Example:*** *Sample filters:*
>
> - ***a**** *returns all group names that start with a.*
> - ****d*** *returns all group names that end with d.*
> - ****sql**** *returns all groups that contain sql in the name.*

6. Click **Search Azure Active Directory**.
7. Select a user, and then click **Add User**.
8. Assign at least one group to the user.

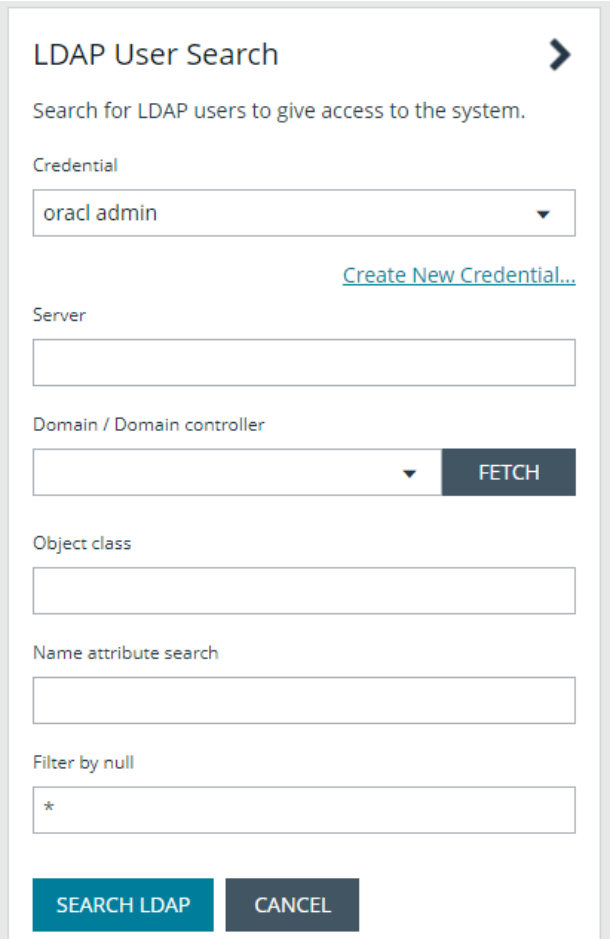
Add an LDAP User

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Click **Users** to display the list of users in the grid.
3. Click **Create New User** above the grid.
4. Select **Add an LDAP User** from the list.

5. Select a credential from the list.

> ***Note:*** *If you require a new credential, click* ***Create a New Credential*** *to create a new credential. The new credential is added to the list of available credentials.*

6. Click **Fetch** to load the list Domain Controllers, and then select one.
7. To filter the user search, enter keywords in the user filter or use a wild card.
8. Click **Search LDAP**.



9. Select a user, and then click **Add User**.
10. Assign at least one group to the user.

Edit a User Account

Administrators can edit user details such as change the name, username, email, and password, update active status, lock and unlock the account, and update multi-factor authentication settings as follows:

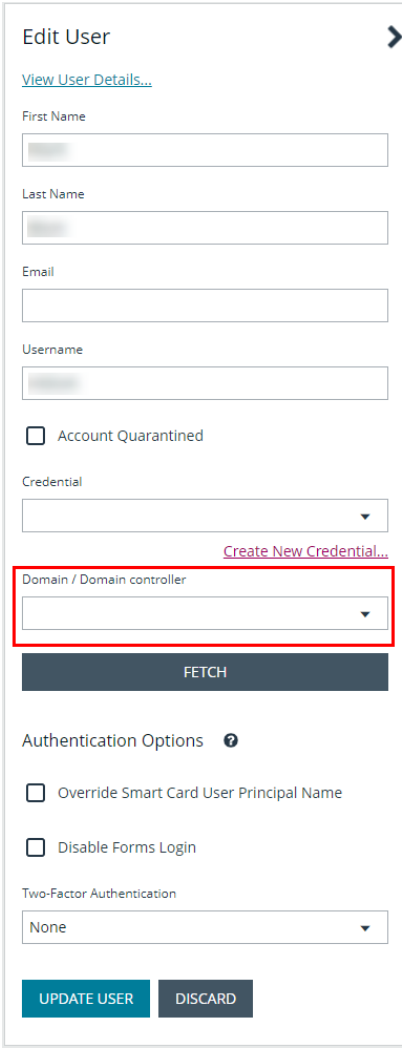
1. Navigate to **Configuration > Role Based Access > User Management**.
2. Click **Users** to display the list of users in the grid.
3. Optionally, filter the list of users displayed in the grid using the **Filter By** dropdown.
4. Select a user, click the vertical ellipsis button, and then select **Edit User Details**.
5. In the **Edit User** pane, update the details as required, and then click **Update User**.

Propagate Domain Changes

The preferred domain controller for a user is set by the group they are in, provided that the group was created with the propagate option turned on, and that this action happened before the user was set up.

If you want to change the preferred domain controller for a user, edit the user, select an appropriate credential, and then select a different preferred domain controller from the list.

> ***Note:*** *Any future change to the preferred domain controller at the group level can overwrite this setting if the propagate switch is turned on.*



> *For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 19.*

Delete a User Account

Administrators can delete user accounts as follows:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Click **Users** to display the list of users in the grid.
3. Optionally, filter the list of users displayed in the grid using the **Filter By** dropdown.

4. For local accounts, select the user, click the **Delete** button above the grid, and then click **Delete** to confirm.
5. For directory accounts, select the user, click the vertical ellipsis, select **Delete User**, and then click **Delete** to confirm.

Note: *If a user account is linked to any Password Safe session recordings, you cannot delete it for auditing reasons; however, you may disable the account.*

Note: *Directory accounts may be deleted only if they do not belong to any groups.*

Audit Console Users in BeyondInsight

You can track the following activities of users logging into the console:

- Login and logout times
- IP address from where the user logged in
- Password change events
- Other actions taken such as configuring user settings

To view user audit data, follow the steps.

1. Select **Configuration**.
2. Under **General**, select **User Audits**.
3. Select a filter. You can filter results by **Action**, **Section**, **Username**, **IP Address**, **Item**, and **Detail**.

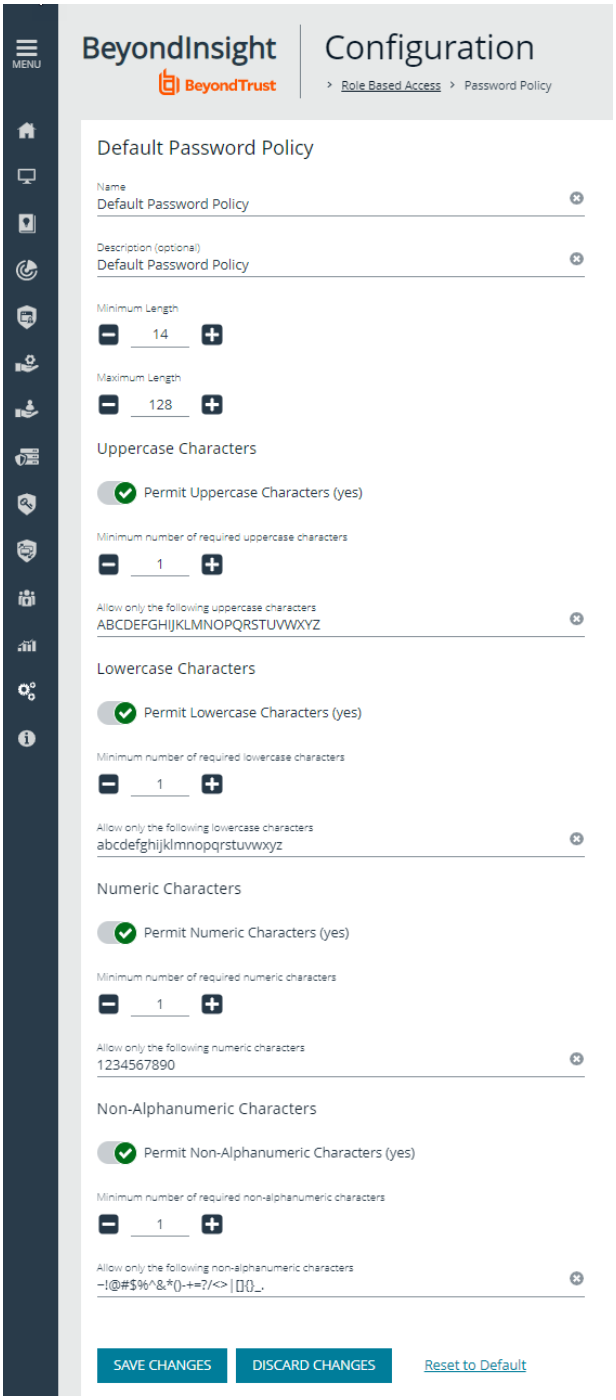
Note: *You can also configure display preferences and filters to refine the information displayed. For more information, please see* *"Change and Set the Console Display Preferences" on page 16**.*

Tip: *You can view more details for a specific user audit by clicking the* ***i*** *icon for the item. You can also export all of the data in the grid to a CSV file by clicking the* ***Download all*** *button above the grid.*

Create a Default Password Policy

You can create a password policy to set the password complexity requirements for local BeyondInsight users. This includes, for example, the minimum and maximum length, numeric characters, non-alphanumeric characters, etc. You can create only one policy.

1. Navigate to **Configuration > Role Based Access > Password Policy**.
2. Enter a name for the policy and an optional description.
3. Set the minimum and maximum password length, and select the types of characters to be used: lowercase, uppercase, numeric, and non-alphanumeric characters.
4. Click **Save Changes** when done. You can also discard changes or reset to default if desired.



Overview of BeyondInsight Tools

BeyondInsight provides a set of tools to help you organize assets for scanning.

Depending on the number of assets that you want to scan or the critical nature of some of your assets, consider organizing the assets using address groups or Active Directory queries which can be part of a Smart Rule.

The following list provides examples on ways you can use these tools:

- Create an IP address group that organizes assets by a range of IP addresses, including CIDR notation and named hosts.
- Use an Active Directory query that will organize assets by organizational unit. Create a Smart Rule and use the query as your selection criteria.
- Change the properties for assets, and then use the attributes as the selection criteria in the Smart Rule.

Scans can return a lot of information. To help you review scan results, you can create filters and set preferences on the **Assets** page to easily review scan results.

For more information, please see "Change and Set the Console Display Preferences" on page 16.

Create an Address Group

When creating a Smart Rule, you can create an address group to use as an IP address filter. An address group can contain included or excluded IP addresses. IP addresses are entered as a

- Single IP address
- IP range
- CIDR Notation
- Named host

> ***Note:*** *The BeyondInsight user must be a member of the* ***Administrators*** *group or be assigned the* ***Full Control*** *permission on the* ***Asset Management*** *and the applicable* ***Smart Rule Management*** *feature(s) to be able to create and edit Smart Rules. Users assigned* ***Read Only*** *permissions on these features may only view the details of Smart Rules.*

For more information, please see "Create and Configure Groups" on page 25.

Create an Always Address Group

You can create an address group and name it **Always**. The Discovery Scanner is designed to recognize this address group name and includes the group in every scan, regardless if the group is selected in the scan job. The address group can include and exclude IP addresses.

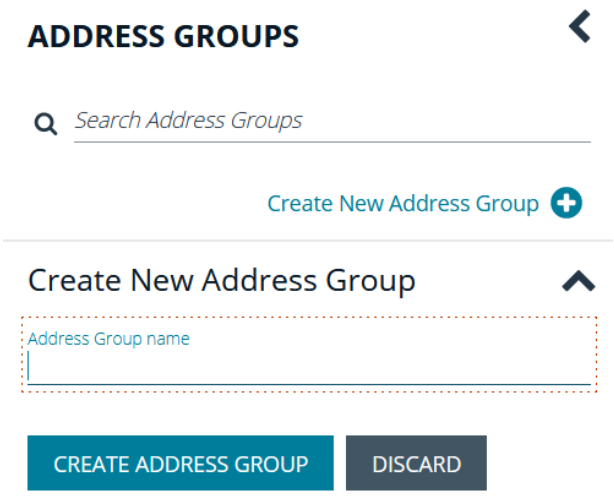
The next time a scan runs, the address group is synchronized with the Discovery Scanner. The IP addresses, whether they are included or omitted, are considered part of the running scan.

> ***Example:*** *If the* ***Always*** *address group is configured with* ***10.10.10.60*** *and* ***buffett-laptop (omitted)****, it scans* ***10.10.10.50*** *and* ***buffett-laptop****. The results are as follows:*
>
> - *The scan includes 10.10.10.60 since this IP address was added to the* ***Always*** *address group.*
> - *The scan excludes buffett-laptop since this asset was explicitly omitted in the* ***Always*** *address group.*
> - *10.10.10.50 is scanned as usual.*

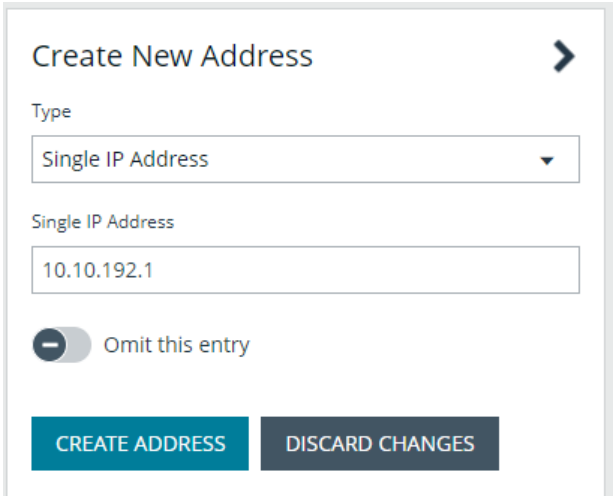
> ***Note:*** *If an asset was scanned and later added to the* ***Always*** *address group as* ***Omit****, the asset is not scanned but might be displayed in the report. This only occurs with some reports.*

1. Select **Configuration**.
2. Under **Discovery Management**, select **Address Groups**.

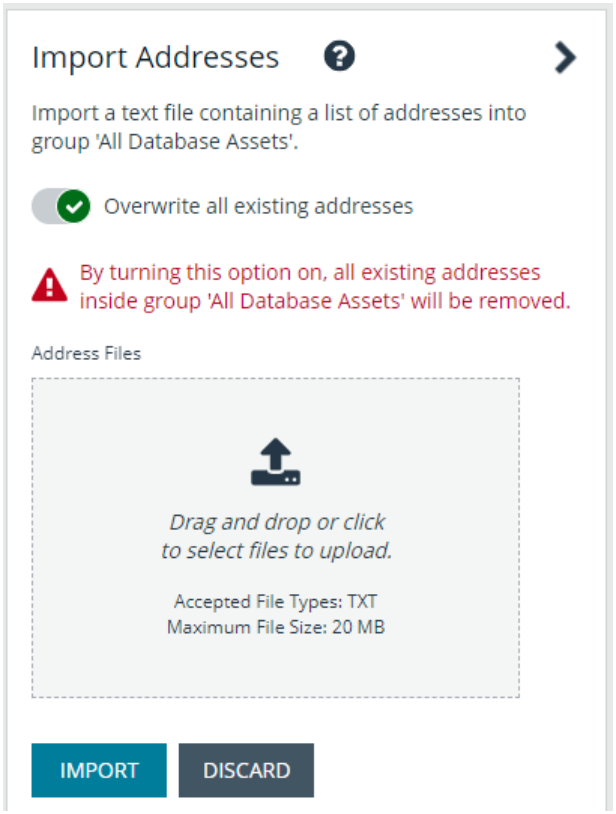
3. Click **Create New Address Group**.
4. Enter a name for the address group, and then click **Create Address Group**.
5. Select the address group, and then click **Create New Address** to manually add the IP addresses. Or, click **Import Addresses** to import them into the group using a file.



6. If manually adding the addresses:
   - Select the type from the list: **Single IP Address**, **IP Range**, **CIDR Notation**, or **Named Host**.
   - Enter the IP addresses, CIDR Notation, or host name, depending on which type you selected.
   - Enable **Omit this entry** to excluded addresses.
   - Click **Create Address**.

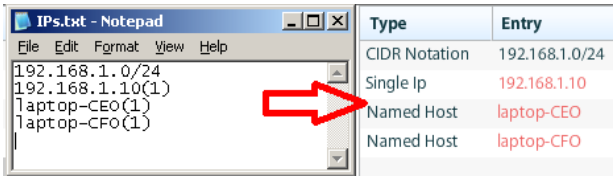


7. If importing the addresses:
    - Enable the **Overwrite all existing addresses** option, if desired.
    - Click **Drop File** to upload the import file.
    - Click **Upload File**.



The list in your import file depends on your particular needs. The list can contain all IP addresses that you wish to exclude. To exclude IP addresses, use the format: **192.x.x.x (1)**.

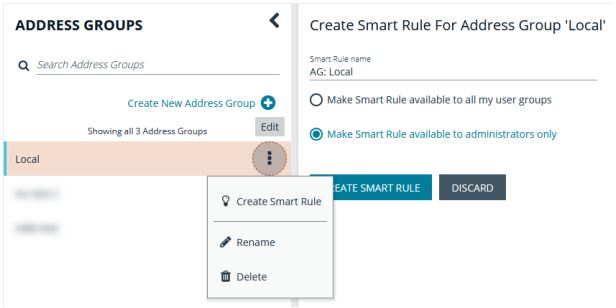
Here is an example of how a CIDR Notation, an excluded IP address, and excluded named hosts are displayed after importing.



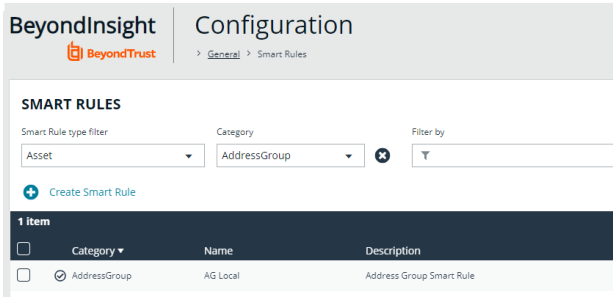
Create a Smart Rule Based on an Address Group

When configuring an address group, you can choose to create a Smart Rule based on the address group.

1. Select the address group, and then click **Edit** (vertical ellipsis).
2. Select **Create Smart Rule**.
3. Leave the default name, or name the Smart Rule as desired.
4. Select the option to make the Smart Rule available to all user groups or to administrators only.
5. Click **Create Smart Rule**.
6. A message stating *Smart Rule has been created for this Address Group* appears.



7. The group is displayed on the **Configuration > Smart Rules** page.



Create a Directory Query

You can create an Active Directory or LDAP query to retrieve information from Active Directory or LDAP to populate a Smart Rule. To work with directory queries, the BeyondInsight user must be a member of the **Administrators** group or assigned the **Asset Management** permission.

Create a new directory query or clone an existing query as follows:

1. In the BeyondInsight Console, navigate to **Configuration > Role Based Access > Directory Queries**.
2. Click **Create New Directory Query** or click the vertical ellipsis for an existing query and select **Clone**.
3. Select **Active Directory** or **LDAP** from the **Directory Type** list.

> ***Note:*** *Cloned queries keep the same directory type as the query being cloned.*

4. Enter a name for the query in the **Title** field.
5. Select a stored credential for running this query or click **Create New Credential** to be taken to the **Directory Credentials** page where you can add a new one.

> ***Note:*** *At minimum, the credential must have **Read** permissions on the computer assets you are enumerating.*

6. Enter the directory path for the **Query Target**, or click **Browse** to search for a path and add it.
7. Select a scope to apply to the container: **This Object and All Child Objects** or **Immediate Children Only**.
8. Select an object type: **Computer Objects** or **User Objects**.
9. Enter the directory path for the **Query Target**, or click **Browse** to search for a path and add it.
10. Select a scope to apply to the container: **This Object and All Child Objects** or **Immediate Children Only**.
11. Select an object type: **Computer Objects** or **User Objects**.
12. Enable or disable the **Dynamically refresh results each use** option.
13. Provide a **Name** and **Description** or use the * wild card character to match multiple values for the **Basic Filter**.
14. Optionally, click **Advanced Filter**to provide an **LDAP Query**.
15. Click **Test** to ensure the query returns expected results.
16. Click **Create Directory Query**.

> *For more information, please see the following:*
>
> - *"Create and Configure Groups" on page 25*
> - *"Create and Edit Directory Credentials" on page 19*

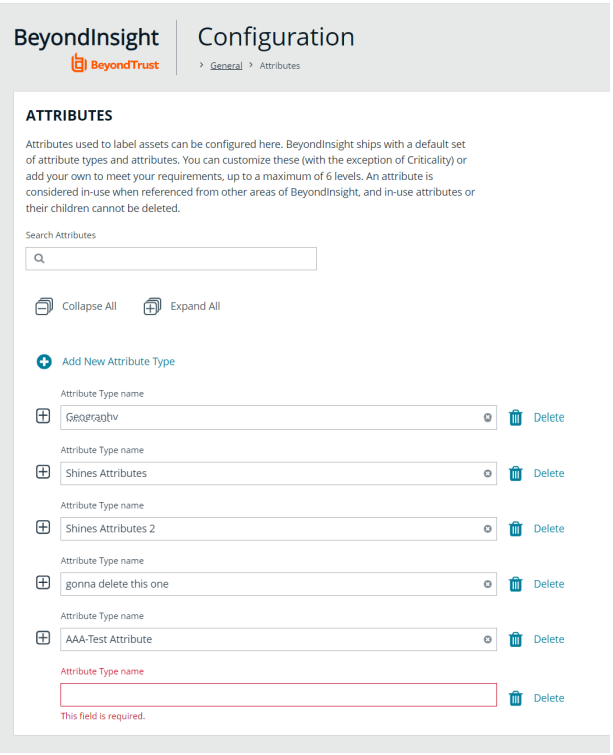
Attributes and Attribute Types

Attributes can be used to label assets, and you can set attributes for each asset in a group using a Smart Rule. BeyondInsight ships with a default set of attributes that can be customized, except for the **Criticality** type, and you can also add new attribute types and attributes to meet your requirements.

For more information, please see "Use Smart Rules to Organize Assets" on page 66.

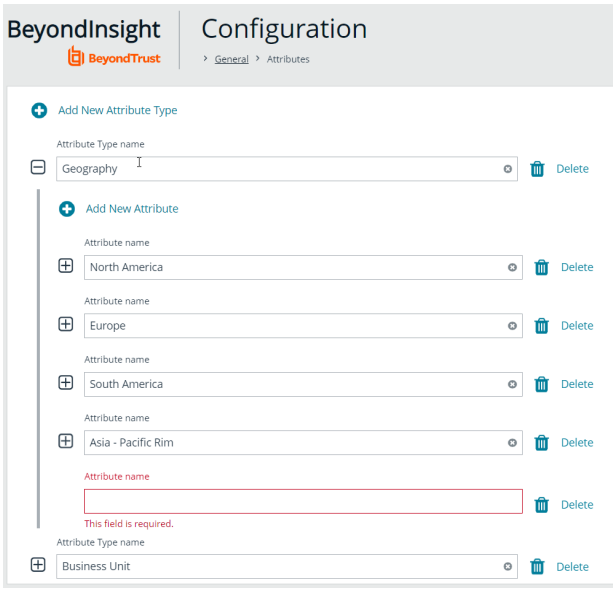
Add a New Attribute Type

1. In the BeyondInsight Console go to **Configuration > General > Attributes**.
2. Click **+ Add New Attribute Type**.
3. Type a name for the attribute type, and then press **Enter**.



Add a New Attribute

1. Click the plus sign for the desired attribute type to expand its attributes.
2. Click **+ Add New Attribute**.
3. Type a name for the attribute, and then press **Enter**.



Use Smart Rules to Organize Assets

A Smart Rule is a filter that you can use to organize assets into Smart Groups. Use an asset-based Smart Rule to organize assets based on the filters selected.

Note: *The BeyondInsight user must be a member of the* ***Administrators*** *group or be assigned the* ***Full Control*** *permission on the* ***Asset Management*** *and the applicable* ***Smart Rule Management*** *feature(s) to be able to create and edit Smart Rules. Users assigned* ***Read Only*** *permissions on these features may only view the details of Smart Rules.*

When a non-administrator user creates a Smart Group, the Smart Group is automatically associated with:

- Read permissions for all groups the user is a member of
- Full Control permissions for all groups the user is a member of and has the **Asset Management** and **Smart Rule Management** permissions for

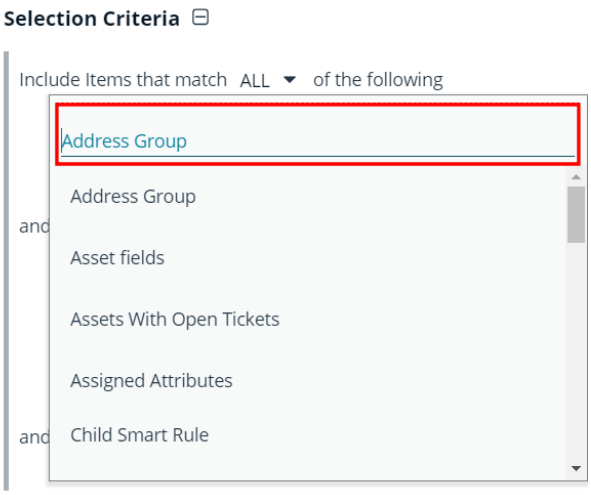
Use a Smart Rule to register assets as Smart Groups. This allows you to:

- Run Discovery Scans
- Monitor and view assets

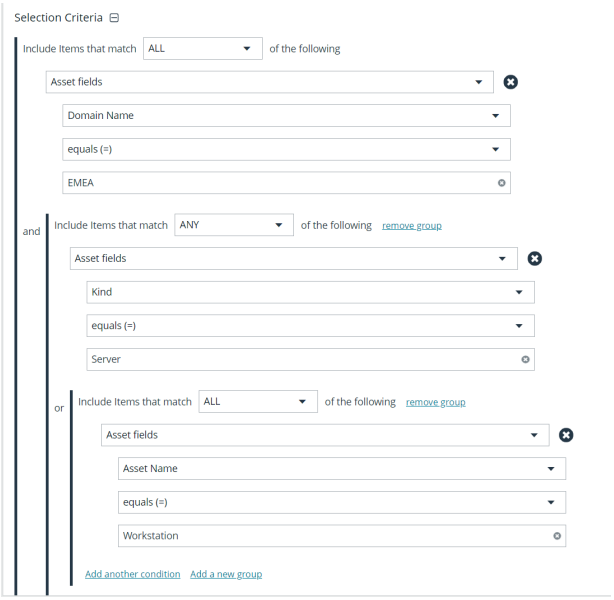
Smart Rules update results automatically, ensuring assets match the criteria and are current.

Use Smart Rule Filters and Smart Groups

There are many built-in filters available that you can use when creating Smart Rules. You can also create address groups or Active Directory queries from the **Configuration** page to use as Smart Rule filters.



You can use more than one filter to refine or extend the scope of assets in a Smart Rule. Filters can be joined with **and** (match **ALL** criteria) or **or** (match **ANY** criteria) conditions. If you select to match **ALL**, every indented filter must be set to **True** for an asset to be included. If you select to match **ANY**, only one of the indented filter items must be set to **True** for an asset to be included. The screen capture shows a filter example that includes all assets in the EMEA domain that are either servers or workstations.



Smart Rule Filters

Asset Smart Rule Filters

Address Group	Create a group of IP addresses.
Asset Fields	Group the Smart Rule by asset fields, such as, **Asset Name**, **Domain** or **DNS**, **Risk**, and **Kind**.

	You can include more than one asset field filter in the Smart Rule to refine the results.
Assets with Open Tickets	For ticket tracking, create a Smart Rule that filters on open tickets. The Smart Rule filter can be set to include overdue tickets.
Assigned Attributes	Create a filter based on an attribute. If the attribute is unassigned on a particular asset, you can choose to include or exclude the asset from the rule.
Child Smart Rule	You can reuse a Smart Rule to save time when creating new Smart Rules. This is especially useful if the Smart Rule is a complicated set of filters. Reusing a Smart Rule further refines the assets that will be a part of the Smart Rule.
Cloud Assets	Filter assets on the cloud connector.
Directory Query	Create an Active Directory or an LDAP query to include or exclude assets in the selected domain.
Installed Software	Filter on any combination of installed software.
MAC Address	Filter by MAC address of assets.
Operating System	Filter on any combination of OS. Operating systems included in the list are those detected in your network. Assets with no OS detected, can be included or excluded from the rule.
Processes	Filter on any combination of processes.
Services	Filter by any combination of services.
Software Version	Filter by software version. The software that you can filter on is determined by the software that is discovered during the scan.
User Account Attribute	Filters user accounts by SID or privilege. You can filter on both. If either value is not selected then it will be ignored. Using this filter you can determine if any users have administrator privileges that might no longer be required. You can create a Smart Rule using this filter and set the email alert action to notify you when a user account with admin privileges is detected.
Windows Events	Filter by Windows events that are available in the Windows Event Viewer. For example, **Application**, **Security**, or **System**.
Workgroup	Filter by workgroup.

For more information, please see the following:

- *"Create an Address Group" on page 59*
- *"Create a Directory Query" on page 63*

Predefined Smart Group Categories

Agents and Scanners	Detects assets where BeyondInsight scanners are deployed.
Assets and Devices	Includes default Smart Groups for all assets and all assets labeled as workstations.
Intelligent Alerts	Includes Smart Groups that detect assets added since the previous day, and mobile assets with critical vulnerabilities. Intelligent Alerts are inactive by default.
Servers	Includes Smart Groups that detect mail server, web server, database server, domain controller, and SCADA assets. Only the **Web Servers** Smart Group is marked as active.
Virtualized Devices	Includes Smart Groups for virtual environments, including **Microsoft Hyper-V** and **Parallels**. Assets detected as virtual environments belong to these Smart Groups. This default category also includes two Smart Groups: **Virtual Servers** and **Virtual Workstations**. Assets that are servers or workstations might not be detected, and as a result, not be included in the Smart Group. For example, the asset might be a router or unknown, resulting in exclusion from the Smart Group.

Create Smart Rules

You can configure an asset-based Smart Rule to:

- Create Smart Groups
- Send email alerts with a list of assets
- Set attributes on assets
- Create a ticket with a list of assets
- Set scanner pooling

Create an Asset Based Smart Rule

1. From the left menu in the BeyondInsight console, click **Smart Rules**.
2. Leave **Asset** selected for the **Smart Rule type** filter.
3. Click **Create Smart Rule**.
4. Select a category.
5. Enter a name and description.
6. By default, the Smart Rule is set to **Active (yes)**, so it is always available for processing. Disable the active setting to ensure the rule is not processed.
7. Select the filters in the **Selection Criteria** section.
8. From the **Actions** section, select one of the following:

Create Ticket	Select tickets parameters, including ticket assignment, severity, and email alert.
Export Data	Select to manage a Smart Group for the BMC Remedy connector.
Mark each asset for deletion	Select to create a Smart Group that contains assets to be marked for deletion.
Mark each asset inactive	Assets detected as inactive are no longer be displayed on the **Assets** page or in reports.
Send an email Alert	Select and enter the email addresses for notification when the rule criteria is matched. Emails are only sent if the list of assets that match the rule is changed from the last time the rule was processed.
Set attributes on each asset	Select the attribute type from the list, and then select the attribute.
Set Scanner Properties	Select one or more scanners to lock to the Smart Group.
Set attributes on each asset	Select attributes for each asset.
Show asset as Smart Group	When selected, the rule is displayed in the Smart Groups pane as a Smart Group. You can select the Smart Group to filter the list of assets in the Smart Groups pane. You can also select the default view to display on the **Assets** page when the Smart Group is selected. Smart Groups are also used for running scans and registering for patch updates.

9. Click **Create Smart Rule**.

Smart Rule Processing

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

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

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

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

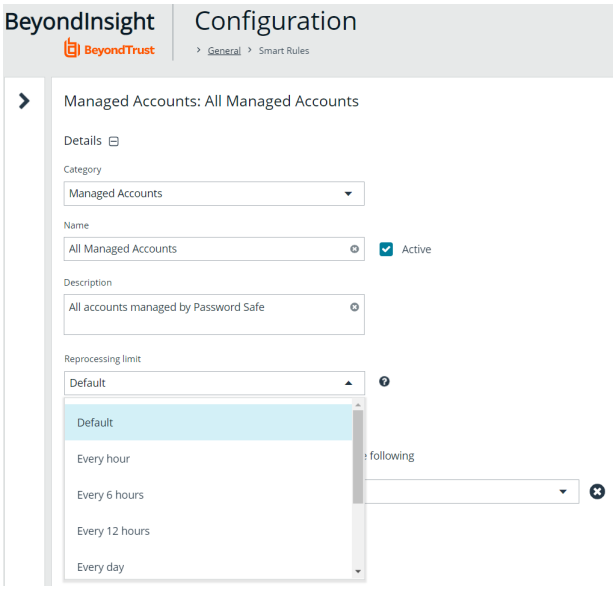
Change the Processing Frequency for a Smart Rule

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

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

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

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



Perform Other Smart Rule Actions

Clone a Smart Rule

You can clone custom or predefined Smart Rules.

1. From the left menu in the BeyondInsight console, click **Smart Rules**.
2. Click the vertical ellipsis button for the Smart Rule you wish to clone, and then select **Clone**.
3. If you are using the multi-tenant feature, select the organization from the list, and then click **Clone Smart Rule**.
4. Select the newly cloned Smart Rule from the grid, click the vertical ellipsis button, select **View Details**, and then edit the Smart Rule filters as needed.
5. Click **Save Changes**.

> ***Note:*** *Cloning a Smart Rule also clones the user group permissions.*

Deactivate a Smart Rule

You cannot delete predefined Smart Rules. However, if you have several smart groups, you can mark unused Smart Rules as inactive.

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

An inactive Smart Group is no longer displayed in the Smart Group browser pane until marked active again.

To deactivate a Smart Rule:

1. From the left menu in the BeyondInsight console, click **Smart Rules**.
2. Select the Smart Group or multiple Smart Groups, and then click **Deactivate** above the grid.

Delete a Smart Rule

1. From the left menu in the BeyondInsight console, click **Smart Rules**.
2. Select the Smart Rule.
3. Click the **Delete** icon above the grid.

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

Smart Rule Options

The **Smart Rule Omni Worker Options** allow you to configure multi-worker node usage, the number of Smart Rule threads per type, and the failure thresholds.

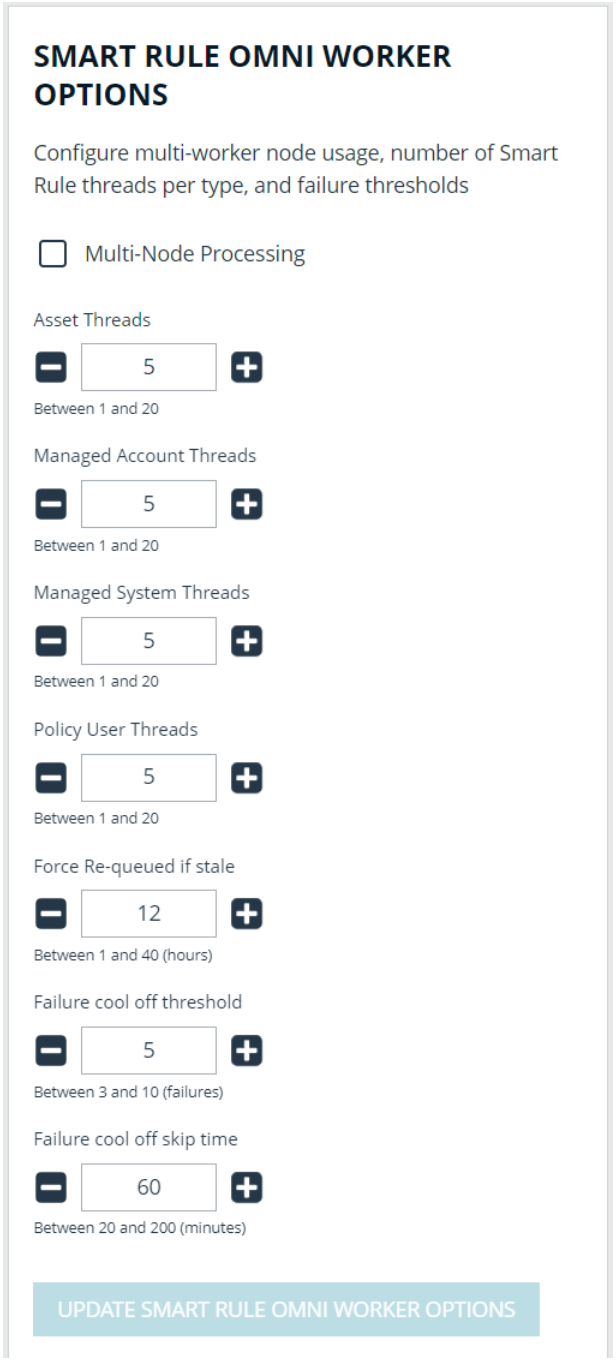
Multi-Node Processing: Off by default. Enable this to allow assignment of Smart Rules to process specific worker nodes. Choosing a worker node for a Smart Rule to process is accomplished by setting the **Target Processing to Workgroup** action on the Smart Rule in question. When enabled, this allows multiple Omni Workers to process Smart Rules.

IMPORTANT!

*For the following options to be available, you must enable **Multi-Node Processing**. An all Omni Worker restart is required to enable this processing.*

- **Asset Threads**: (Default **5**) Choose a number of threads to use for processing asset based Smart Rules.
- **Managed Account Threads**: (Default **5**) Choose a number of threads to use for processing managed account based Smart Rules.
- **Managed System Threads**: (Default **5**) Choose a number of threads to use for processing managed system based Smart Rules.
- **Policy User Threads**: (Default **5**) Choose a number of threads to use for processing policy based Smart Rules.
- **Force Re-queued if stale**: (Default **12**) Choose a number of hours after which an unprocessed Smart Rule is considered stale and re-queued for processing.
- **Failure cool off threshold**: (Default **5**) Choose a number of times to let a Smart Rule process fail after which a cool-off period is observed.
- **Failure cool off skip time**: (Default **60**) Choose a number of minutes to wait before trying to process the Smart Rule again after reaching the failure cool off threshold.

Click **Update Smart Rule Omni Worker Options** when you have finished setting the options.



Additional Multi-Node Processing Information

The **Multi-Node Processing** feature was added to allow more granular control over the performance of smart rule processing.

Impact of Multi-Node Processing

Multi-node processing is a combination of features:

- Controls the number of nodes and threads per node that are used for processing different types of Smart Rules.
- Restricts the processing of certain Smart Rules to specific nodes if required. This might come into play if the Smart Rule is built on a directory query that only one worker node has access to. Trying to process a Smart Rule like this across all Omni Workers would result in occasional failures if the node doing the processing lacks the necessary access to run the directory query.
- Controls certain behaviors in failure scenarios. The defaults should be sufficient, but are adjustable to give more control to support assisting customers in this area.
- When multi-node processing is turned off, then Smart Rule processing occurs on a single node using *N* threads, where *N* is configurable per Smart Rule **TYPE** in the configuration user interface (**Asset Threads**, **Managed Account Threads**, **Managed System Threads**, and **Policy User Threads**). While better than the historical single-threaded model, this can still be a lot of work for the Omni Worker and might cause poor performance in other areas (password rotations, event forwarding, etc.).
- When multi-node processing is turned on, then Smart Rule processing is shared across ALL worker nodes, using *N* threads per worker node, where *N* is configurable per Smart Rule **TYPE** in the configuration user interface (**Asset Threads**, **Managed Account Threads**, **Managed System Threads**, and **Policy User Threads**).
- The default setting for each Smart Rule type is **5** threads. The valid range is between **1** and **20** threads.
- Changes to the multi-node processing settings, as well as changes to thread counts and changes to failure scenario handling, can be made anytime but do not take effect until all Omni Worker services are restarted. This restart is a manual step. There is no risk to enabling or disabling these settings during production times, but you will not see any change in processing until Omni Worker services are restarted.

Overall Best Practices

The **Multi-Node Processing** setting is turned off by default. Turning it on is beneficial if multiple worker nodes or Omni Workers are available, and if the existing Omni Workers are running at full capacity. If turning this feature on doesn't help Omni Worker performance, support should be contacted.

The lower the thread count, the less benefit you may get from turning this setting on. However, setting the thread count too high can also result in problems if your Omni Worker or worker nodes are not powerful enough to handle the load. Start with the default and adjust up or down as necessary.

Reason for Multi-Node Processing

Before this feature was added, Smart Rule processing was only supported in a single-threaded model running in RemManagerService. Moving it to Omni Worker allows it to be multi-threaded on a single node. Adding the multi-node option allows Smart Rule processing to be scaled out even further.

Multi-Node Processing Environment

This feature is used in an environment with multiple worker nodes or Omni Workers, where an Omni Worker is taxed by Smart Rule processing.

Assign a Rule to a Node

If multi-node processing is turned on and a Smart Rule contains a specific criteria or action that only works if executed on a particular worker node, then that Smart Rule is expected to get an action of **Targeted to Workgroup** set. The Omni Worker or worker node that executes this Smart Rule should be manually set to the same work group under **Worker Nodes**. Some examples of criteria or actions that

only work on a particular node are directory queries that run on a specific network, or database account onboarding that runs on a specific network. Any network-specific Smart Rules are likely candidates to target a specific worker node.

Troubleshooting Methods

- **Smart Rule Grid**

  Three optional columns have been added to the Smart Rule grid to give some extra visibility into Smart Rule processing: **Processed Date** (checks to see if any rules were not processed recently), **Successful Attempts**, and **Failed Attempts**. Other columns that are helpful are **Reprocessing Limit**, **Average Time**, **Last Attempt**, and **Processing Status**.

- **Dynamic Dashboard**

  Troubleshooting also includes checking the Omni Worker Dynamic dashboard in the user interface (administrators only). There you can see the Omni Worker agents, queued messages, messages sent to dead-letter (undeliverable letters, reached the limit of processing attempts), and messages actively being processed.

- **Health Dashboard**

  This dashboard shows stats regarding issues on worker nodes, slowest Smart Rules, failed Smart Rules, and errors in the system.

- **Logfiles**

  There is one log file per Omni Worker. Because this can be hard to read across environments, we have added the **System Event Viewer** and **System Event Settings** features. Enabling **System Event Database Recording** logs error or warning messages from across the system into the BeyondInsight database so they can be viewed and searched using the **System Event Viewer**. Purging these events from the database is configurable. The default is **5** days.

Issues with Feature

The feature has been developed to avoid deadlocks, race conditions, memory leaks, etc., as part of our development and QA process. However, it is possible that some issues still exist. Contact BeyondTrust Support with any issues that arise for resolution.

Changed Behaviors in the Database

On its own, multi-node processing does not make changes in the database. Any database changes to schemas, tables, views, procedures, etc., that are required for this and other features in BeyondInsight are made during an upgrade, whether this feature is enabled or not. If the **Enable System Event Database Recording** setting is turned on, then database entries are made for warnings or errors in the system. Purging is enabled for this data, and the time frame is configurable.

Logged Nodes

Each Omni Worker has its own logs. Logging takes place across multiple nodes when this setting is turned on. The **System Event Viewer** shows any issues that are occurring.

Failover Processing

Existing support for worker node or Omni Worker service failover also encompasses the Smart Rule processing function. In the event of a failover situation, the secondary node picks up where the primary node leaves off.

View and Select Smart Rules Processing Statistics

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

To add this information to the grid:

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

Add Credentials for Use in Scans

You can create the following credential types that can be used for scans:

- Microsoft SQL Server
- MySQL
- Oracle
- SNMPv2
- SSH
- Windows

To create a credential:

1. Select **Configuration > Discovery Management > Credentials**.
2. Click **Create New Credential**.
3. Select a credential type from the **Type** list.

> ***Note:*** *The fields of information you need to enter change based on the type selection.*

4. Enter the user account information appropriate for the type of credential you are creating:

Type	Information
MS SQL Server	• Authentication Type • Domain (Optional) • Username • Password • Confirm password • Description • Port numbers • Key • Confirm key
MySQL	• Username • Password • Confirm password • Description • Port numbers • Key • Confirm key
Oracle	• Username • Password

	• Confirm password • Description • Access level • Connect to • Protocol • Port numbers • Key • Confirm key
MongoDB	• Username • Password • Confirm password • Description • Database • Host • Port numbers • Key • Confirm key
PostgreSQL	• Username • Password • Confirm password • Description • Database • Host • Port numbers • Key • Confirm key
Sybase	• Username • Password • Confirm password • Description • Host • Port numbers • Key • Confirm key
Teradata	• Username • Password • Confirm password

	• Description • Host • Port numbers • Key • Confirm key
SNMPv2	• Description • Key • Confirm key • Community string
SSH	• Authentication Type • Userrname • Password • Confirm password • Description • Port numbers • Key • Confirm key • Elevation
Windows	• Domain (Optional) • Username • Password • Confirm password • Description • Key • Confirm key

Note: *All credentials are stored in the database using an AES-256 block cipher by RijndaelManaged.*

Tip: *This feature propagates credentials stored in BeyondInsight to Discovery Scanner servers and allows end users and API calls to leverage credentials locally on the network scanner. This eliminates the need to provide credentials separately for those scanners.*

If the credential name matches an existing credential in the BeyondTrustDiscovery Scanner, the credential is overwritten with the value from BeyondInsight.

5. Click **Create New Credential**.

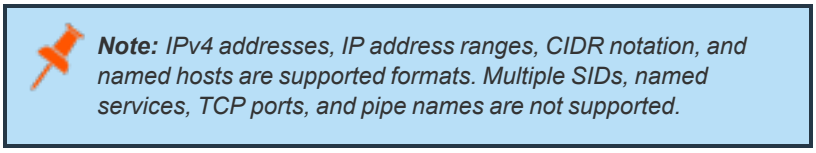
If creating Oracle, SSH, or SNMP credentials, please see the following:

- *"Create SSH Credentials" on page 83*
- *"Create Oracle Credentials" on page 81*
- *"Create SNMP Credentials" on page 82*

Create Oracle Credentials

If you are scanning Oracle databases, you can create Oracle credentials. The **tnsnames.ora** file is updated automatically after you create an Oracle credential.

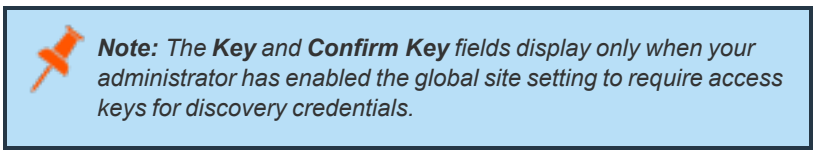
1. In the BeyondInsight console, navigate to **Configuration > Discovery Management > Credentials**.
2. Click **Create New Credential +**.
3. From the **Type** list, select **Oracle**.
4. Provide a **Username**, **Password**, and **Description**.
5. Select an **Access level** from the list: **Standard**, **SYSDBA**, or **SYSOPER**.
6. Select additional connection options:
    - **Connect To:** Select from: **Database SID** or **Named Service**.
    - Enter the database SID or name of the service, depending on which option you had selected.
    - **Protocol:** Select a protocol: **TCP**, **TCPS**, or **NMP**.
    - **Hosts:** Enter the host name where the Oracle database resides. If this credential is used for multiple Oracle hosts, separate each host name by a comma.



Note: *IPv4 addresses, IP address ranges, CIDR notation, and named hosts are supported formats. Multiple SIDs, named services, TCP ports, and pipe names are not supported.*

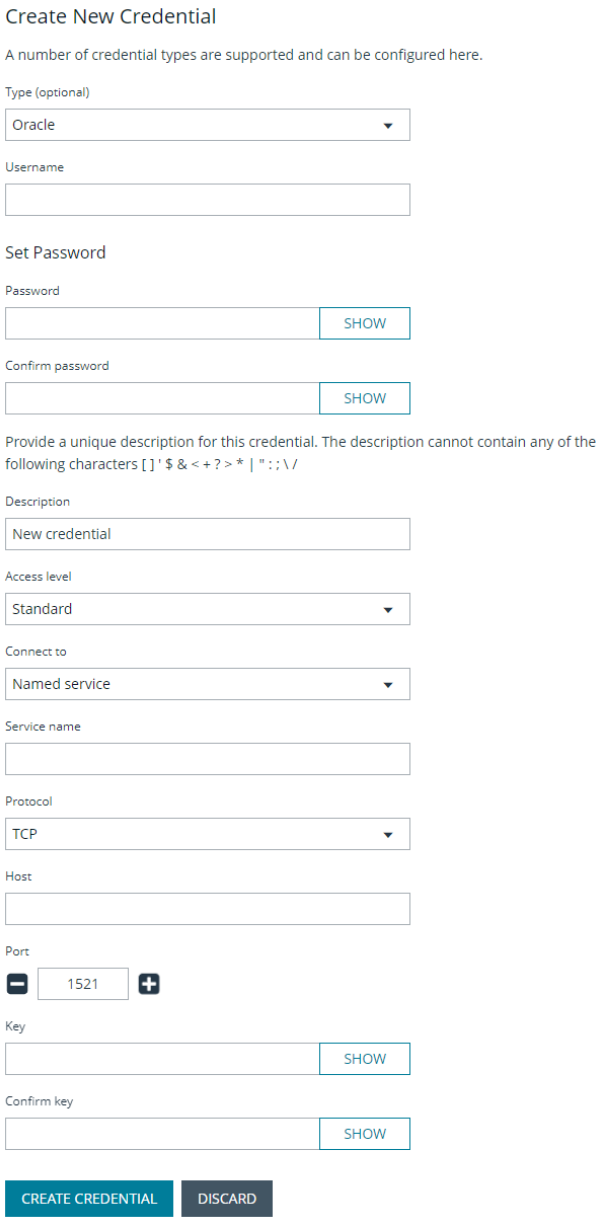
- **Port Numbers:** The default port is **1521**. Use the **+** and **-** buttons to change this if necessary.

7. Enter a key and confirm it.



Note: *The **Key** and **Confirm Key** fields display only when your administrator has enabled the global site setting to require access keys for discovery credentials.*

8. Click **Create New Credential**.



Create SNMP Credentials

If scanning devices are managed by an SNMP community, you can add your community strings.

1. In the BeyondInsight Console, navigate to **Configuration > Discovery Management > Credentials**.
2. Click **Create New Credential**.
3. From the **Type** list, select **SNMPv2**.
4. Enter a **Description**.
5. Enter a key and confirm it.

Note: *The **Key** and **Confirm Key** fields display only when your administrator has enabled the global site setting to require access keys for discovery credentials.*

6. Enter the **Community String**.
7. Click **Create New Credential**.

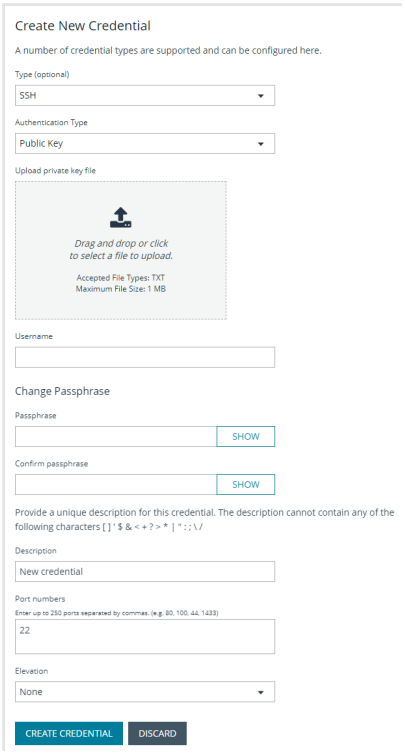
Create SSH Credentials

You can create Public Key Encryption credentials to connect to SSH-configured targets. You can select a credential that contains a public and private key pair used for SSH connections.

> ***Note:*** *DSA and RSA key formats are supported.*

Optionally, when configuring SSH, you can select to elevate the credential. Using **sudo**, you can access scan targets that are not configured to allow root accounts to log on remotely. You can log on as a normal user and use **sudo** to connect with a more privileged account. Additionally, you can use **sudo** to elevate the same account to get more permissions. Using **pbrun**, you can elevate the credential when working with Privilege Management for Unix & Linux target assets.

1. In the BeyondInsight Console, navigate to **Configuration > Discovery Management > Credentials**.
2. Click **Create New Credential**.
3. From the **Type** list, select **SSH**.
4. Select an authentication type.
    - **Plain text:** Enter a **Username** and **Password**.
    - **Public Key:** Upload a private key file, and then enter a **Username** and **Passphrase**. A public key is generated based on the contents of the private key.
5. Enter a **Description**.
6. Enter a key and confirm it.



> ***Note:*** *The **Key** and **Confirm Key** fields display only when your administrator has enabled the global site setting to require access keys for discovery credentials.*

7. Enter a port number, or multiple port numbers separated by commas.
8. Elevating credentials is optional. To elevate credentials, select one of the following from the **Elevation** list:
    - **sudo:** The optional sudo username should be blank in most cases. When blank, commands run with the effective privileges of the root account. If an optional username is entered, sudo runs in the security context of that user.
    - **Enable:** Enter the credentials for Cisco devices. If you are auditing Cisco devices, you can elevate the credentials to privileged for more thorough scans.
    - **pbrun:** Enter the pbrunuser username.
9. Click **Create New Credential**.

Run Discovery Scans

Run a discovery scan to locate network assets, such as workstations, routers, laptops, and printers. A discovery scan also determines if an IP address is active. You can periodically repeat discovery scans to verify the status of devices, programs, and the delta between the current and previous scans.

> ***Note:*** *Discovered assets do not count toward your license.*

- The TCP discovery ports are 22, 80, 110, 139, 389, 443, 445, 1025, 1433, 1521, 3306, 3389, 5000, 5432, and 27017.
- Use more than one scanner to distribute the coverage across the network.

Use the Scan Wizard to Create a Discovery Scan

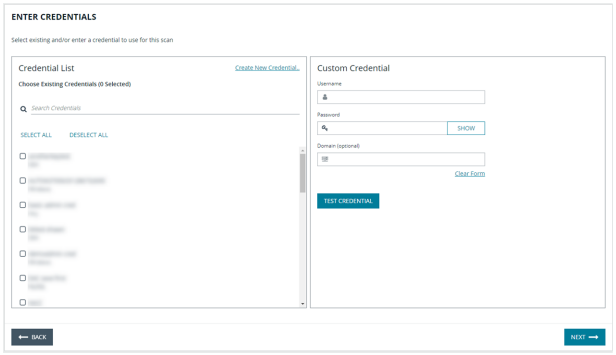
1. Click **Run a New Discovery Scan** on the left menu.
2. **Select Scan Type**: There are three types of scans to choose from. Select one and click **Next**.
    - **Discover Local Accounts**: This scan requires credentials and deploys a local scan service to the scan targets. This scan discovers systems as well as the local user accounts located on them.
    - **Detailed Discovery Scan**: This scan requires credentials and it deploys a local scan agent to the scan targets, which can be disabled if required. Besides systems, this scan provides associated information on services, scheduled tasks, users, and databases. This scan is customizable. Click **Customized Detailed Discovery** to select the type of data to collect.
    - **IP Discovery**: This scan does not use credentials for the scanning process and does not deploy any services to the scan targets. This scan discovers only the IP addresses for detected systems.

> ***Note:*** *Any assets discovered using the **IP Discovery** scan, if subsequently rescanned with another scan type, are listed in BeyondInsight as duplicates. This type of scan can only identify assets by IP address, while credentialed scans rely on a mix of hostname, DNS name, and workgroup to identify assets.*

3. **Select Scan Targets**: Enter scan targets in the field provided. You can enter single IP addresses, IP ranges, addresses in CIDR notation, or named hosts. Items must be separated by commas.
4. **Choose Scan Agent**: Select which agents are used to execute the scan. If more than one agent is selected, the scan targets are split between the selected agents. If you have a large number of agents, you can use the filter dropdown menu. Click **Next** to continue.

> ***Note:*** *A warning banner appears at the top of the screen if your installation includes any Discovery Agents earlier than version 20.1. These must be updated by the end of 2021. You can identify outdated agents by referring to the grid of agents on this screen, which includes the version of each agent.*
>
> *Click **Dismiss** to hide the warning banner until your next login. Dismissing the warning banner here does not hide it on the dashboard, and dismissing the warning banner on the dashboard does not hide it on this screen.*

5. **Enter Credentials**: If the type of scan you select requires credentials, you can select a credential from the **Credential List**, and/or use the **Custom Credential** section to provide a credential to use for this scan.



    - If you enter a **Custom Credential**, click **Test Credential** to verify its functionality.

> ***Note:*** *Clicking **Test Credential** tests only AD domain user accounts. It is not for use with local or SSH user accounts.*

    - If using the **Credential List**, select one or more credentials from a list of available credentials.
    - If keys are required for discovery credentials in your environment, either provide a key for each credential or enable the **Use the same key for all selected credentials** option to provide a **Universal Configuration Key** used for all selected credentials.

> ***Note:*** *Configuration keys are not used or validated for Password Safe credentials.*

> ***Tip:*** *Use the **Search Credentials** box to filter the list of available credentials.*

> ***Tip:*** *If you require a credential that isn't listed, click the **Create New Credential** hyperlink at the top of the **Credential List** section to open the **Create New Credential** form and create a new credential. The new credential is added to the list of existing credentials.*

6. Once credentials have been selected for the scan, click **Next**.
7. **Name the Scan**: Provide a unique name for this scan. The scan name cannot be longer than 58 characters and cannot contain any of the following characters: **[ ] ' $ & < + ? > * | " : ; \ /**. You can also set the following **Discovery Options**:
    - Apply job restrictions that allow you to abort the scan if it runs longer that a set number of minutes.
    - Toggle the option to enable or disable the use of a local scan service.

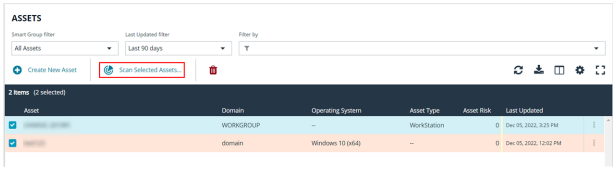
> ***Note:*** *Disabling the local scan service prevents the discovery of IIS app pools, Scheduled Tasks, and domain user information.*

    - Set a schedule, which can be **Immediate**, **One Time**, or **Recurring**.
8. Click **Finish** to complete the Scan Wizard.

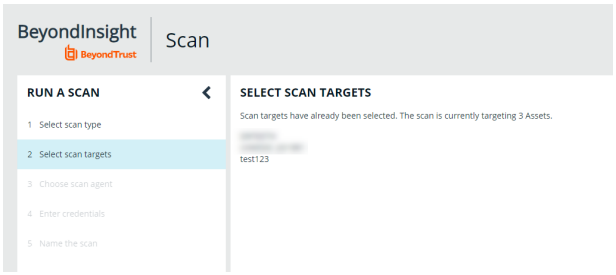
Run Scans from a List of Assets

If you want to run a scan but would prefer to select targets from a list of assets rather than type them, click **Assets** from the left menu.

From the **Assets** grid, select the assets you want to scan, and then click **Scan Selected Assets**.

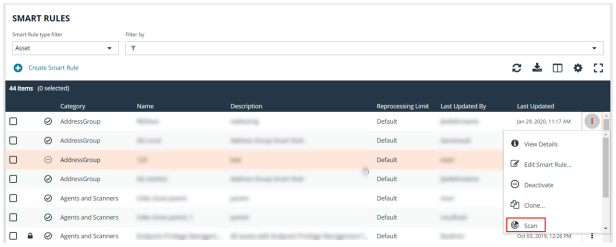


The Scan Wizard screen appears. Here you can select the type of scan to run. The difference is that when you click **Next** and go to the **Select Scan Targets** page, you will find the targets already selected. The next steps in the Scan Wizard are the same as those outlined above.



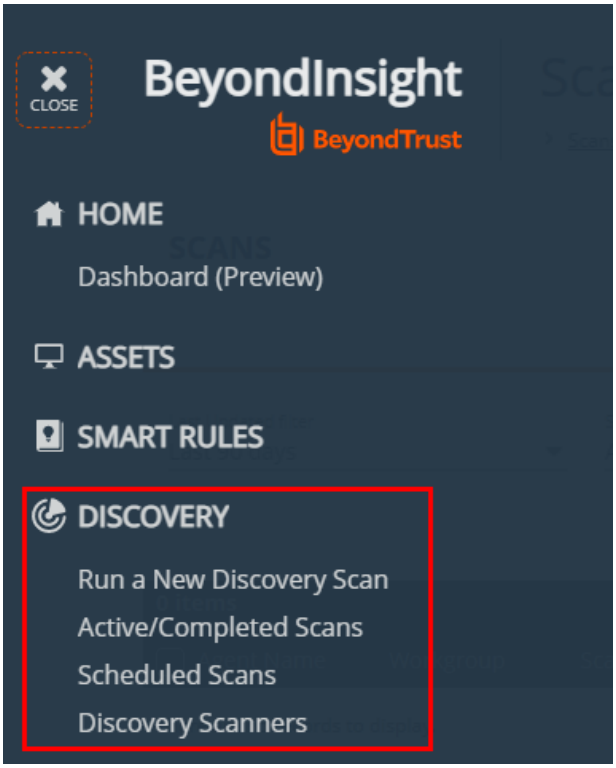
Use Smart Rules as Targets for Scans

You can also run a scan on Smart Rules. From the **Smart Rules** grid, select a rule, click the vertical ellipsis for the rule, and then select **Scan**. You are taken to the Scan Wizard, for which the targets are preselected, and if the Smart Rule is configured to use specific scanners, the scan agents are also preselected. The next steps in the Scan Wizard are the same as those outlined above.

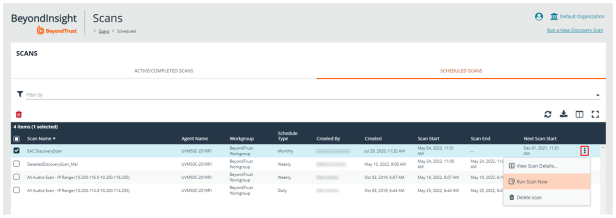


Check Completed and Scheduled Scans

If you want to check information on scans click **Menu** from the left navigation bar. Under **Discovery**, click **Active/Completed Scans** or **Scheduled Scans**.

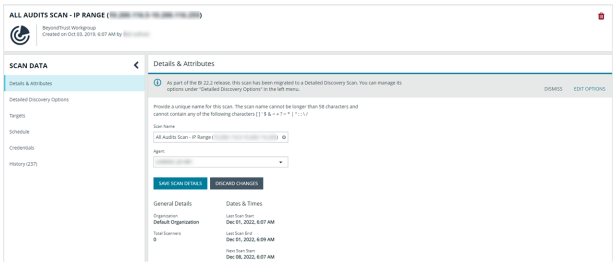


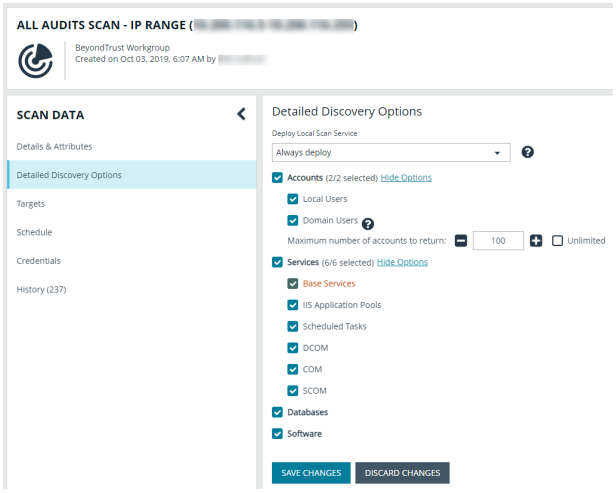
From the **Scans** page you can see active, completed, and scheduled scans, and you can delete a scan. You can also see the scan status for each active or completed scan. For each active and completed scan you can click the vertical ellipsis for the scan, and then select **Run Scan Now** or **Delete scan**. For each scheduled scan you can click the vertical ellipsis for the scan, and then select **View Scan Details**, **Run Scan Now**, or **Delete scan**.



When viewing the **Scan Data**, you can:

- Change the name of the scan
- Change the scanner associated with a scheduled scan job via **Details & Attributes > Agent**
- Change the **Detailed Discovery Options**
- View the scan targets and modify the target Smart Rule if one is selected
- Change the scheduled scan time
- Change the credentials
- View the history of the scan, if any exists





Discover Assets Using a Smart Group

When the Smart Group filter is an address group, Active Directory query, or cloud connector, you can discover assets. When the **Use to discover new** box is checked, any assets online since the Smart Group was last processed are detected . The scan results on the **Assets** page reflect the number of assets found.

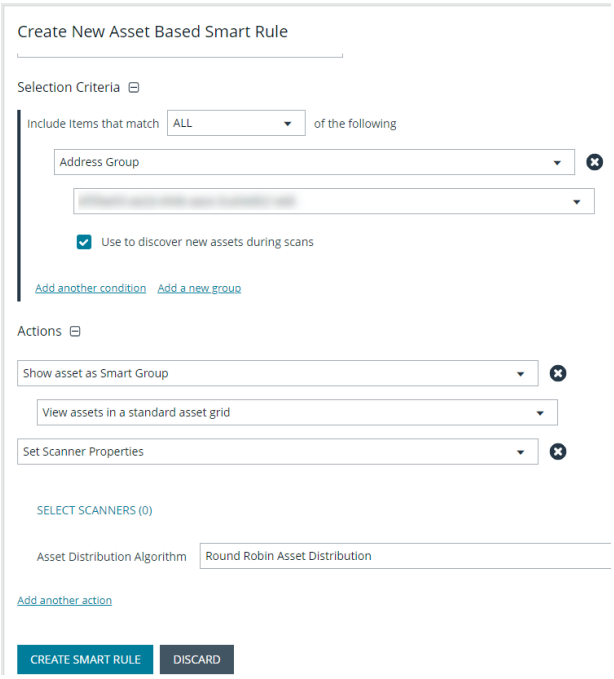
Tip: *If you create an address group that includes the /19 CIDR block, the range possesses 8190 potential assets. The Discovery Scan always tries to discover those assets. Keep this in mind when you are reviewing scan results.*

Key Steps

To create a Smart Group, go to **Configuration > General > Smart Rules > Create Smart Rule**.

- Create an address group or Active Directory query that includes the IP address range or domain.

- Create a Smart Group that includes the address group or query as the filter. Enable the **Use to discover new assets during scans** option.
- You can also configure the Smart Rule to use specific scanners by selecting the **Set Scanner Properties** action, and then selecting specific scan agents from the list.



***Tip:** We recommend you run a discovery scan at a regular interval. You can discover assets manually by entering a host name, IP address, or address range.*

For more information, please see the following:

- *"Create a Directory Query" on page 63*
- *"Create an Address Group" on page 59*

Manage Scan Jobs

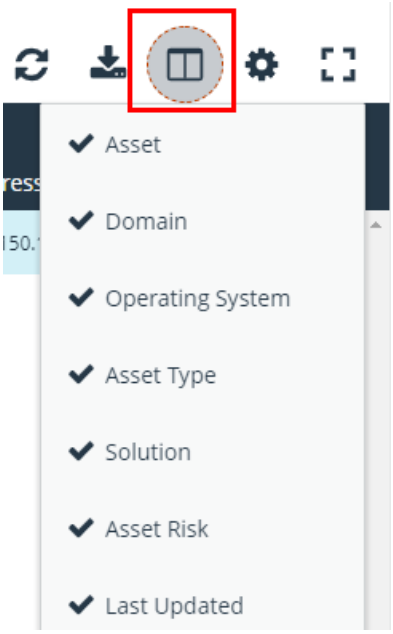
On the **Scans** page, you can:

- View active, completed, and scheduled scan jobs
- Locate specific jobs by using the date, status, agent name, workgroup, scan name, start time, and end time filters
- Stop active scan jobs
- Edit scheduled scan jobs
- Run completed and scheduled scan jobs now

Manage Assets

The **Assets** page allows you to review details about your assets quickly by filtering your assets by last update time, type of asset, domain, operating system, technical solutions applied to the asset (for example, an asset is a scanned host or database host), DNS name, Workgroup, and IP address.

You can modify which columns to display in the **Assets** grid by clicking the **Column Chooser** icon above the grid. From here you can add or remove columns.

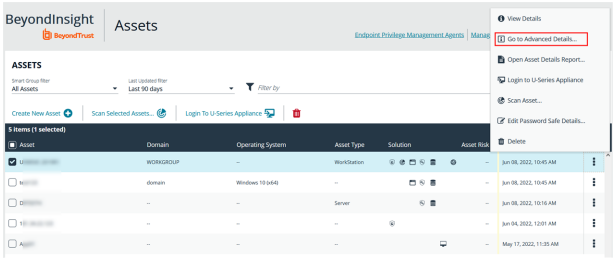


Review Asset Details

Tip: *Depending on the scan settings, information might not be detected and included in the scan results. If the following scan settings are turned on, more accurate scan results can be expected:*

- ***Perform Local Scanning***
- ***Enable WMI Service***
- ***Enable Remote Registry Service***

You can review the advanced details information for assets by clicking the vertical ellipsis button for an asset, and then selecting **Go to Advanced Details**.



General Data

- **Details & Attributes:** Displays details about the asset such as: IP address, DNS name, domain, system name, Workgroup, date the asset was added and updated, the operation system, etc.
- **Accounts:** If the asset is linked to a managed system, the managed accounts on that system are listed in the grid.

***Tip:** Click the **View Managed System** link above the grid to view the advanced details for the managed system that is linked to the asset. To return to the advanced details for the asset, click the **View Asset** link.*

- **Application Pools**: Displays IIS Application Pools discovered on the asset on the last successful scan of the system.
- **Databases:** Displays the databases that are on the asset and allows you to add a database.
- **Smart Groups:** Displays the Smart Groups that the asset is associated with.

Scan Data

***Note:** By default, the current snapshot of scan data is selected. You can select other available snapshots to load the data for that date.*

- **Certificates:** Displays all certificates installed on the asset. You can filter by expired certificates or search for certificates.
- **Hardware:** Displays disk drive information, system manufacturer, memory, and processor information.
- **Ports:** Displays the open port number, protocol, and description.
- **Scheduled Tasks:** Displays information about scheduled tasks for a particular asset, including task name, task to run, last time the task ran, schedule type, etc.
- **Services:** Displays discovered services, including name, description, state, logon details, startup type, and dependencies.
- **Software:** Lists all software discovered on the asset, including version.
- **Users:** Includes several attributes for user accounts, including: name, privileges, password age, last logon date, password expiry status, group membership, and status of the account, and allows you to filter by these attributes.

Create Assets Manually

Assets are added to BeyondInsight through discovery scans. Assets can also be manually added from the **Assets** page.

1. From the **Assets** page, select **All Assets** from the **Smart Group filter** dropdown.
2. Click **Create New Asset +**.
3. Complete the **Create Asset** form, and then click **Create Asset**.

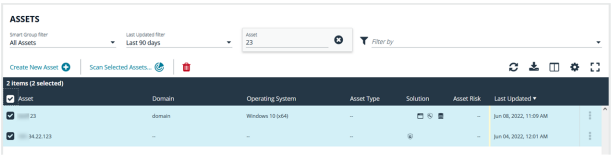
***Note:** New assets created in any Smart Group other than **All Assets** might not appear under the selected Smart Group if the Smart Rule criteria is not met or until the Smart Rule processes. We recommend that you create new assets using the **All Assets** Smart Group.*

Note: *A manually added asset can have its basic information edited, such as Name, DNS Name, Domain, Asset Type, IP Address, MAC Address, and Workgroup. Asset attributes cannot be edited at the individual asset level at this time. If this is necessary, Smart Rules can be used to modify the attributes associated with an asset.*

Delete Assets

You can remove assets from the **Assets** grid immediately. Assets removed from the grid are deleted from the BeyondInsight database during the nightly data purge.

1. From the **Assets** page, select an asset or multiple assets, and then click the **Delete** button above the grid.



Tip: *You can use the filters above the grid to narrow down your list of assets to those targeted for deletion, and then check the box in the header to select all assets in the grid to delete at once.*

2. Click **Delete** on the confirm deletion message.

For more information on discovering assets using a discovery scan, please see: *"Run Discovery Scans" on page 84**.*

U-Series Appliance

Log in to U-Series Appliance via BeyondInsight Console

Permissioned users have the option to log in to the U-Series Appliance directly from the **Asset** grid in the BeyondInsight Console. This eliminates the need for organizations to share their BTAdmin account. This feature also leverages BeyondInsight user audits to audit which user is logged in to which appliance when the login is initiated from the BeyondInsight **Asset** grid.

Note: *Requires BeyondInsight 22.2, Discovery Scanner 22.2, and U-Series Management Software 3.5.*

Prerequisites

- An API key exchange must be performed between the BeyondInsight Console appliance and the remote appliances.
    - SQL Free appliances that have already exchanged must be repeated.
- The crypto key must be exchanged for the BeyondInsight database. Use one database for all your appliances.
- A working DNS lookup for each appliance is required (no support for IP addresses).

For more information, please see the following:

- *On API keys, Manage the U-Series Appliance API Key at https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/administration/security.htm*
- *On crypto keys, Manage U-Series Appliance Security Settings at https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/administration/security.htm*
- *On crypto keys, Configure U-Series Appliance Roles at https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/administration/configure-roles.htm*

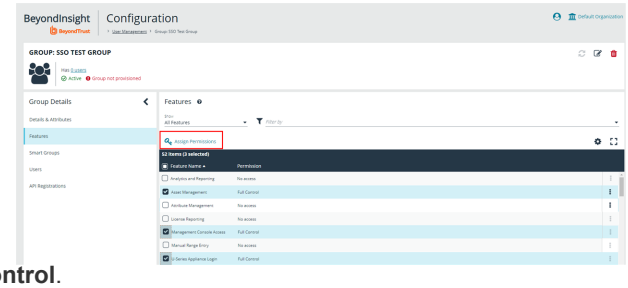
Setup Non-Admin Users in BeyondInsight

Non-admin users must be given permissions to view and sign on to the U-Series Appliance. This is done with a permissioned SSO (Single Sign On) group.

Create Permissioned Group

1. Log in to the BeyondInsight Console.
2. Go to **Configuration > Role Based Access > User Management > Groups** and click **Create New Group**.
3. Enter **Group Name** and **Description** and click **Create Group**. This opens the **Group Details** page.

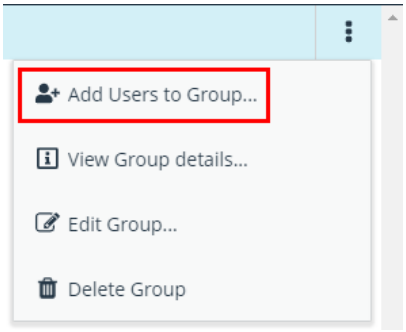
4. In the left menu, click **Features**. Under Feature Name:
    - Select **Management Console Access** for access to the BI Console.
    - Select **Asset Management** to view appliances you have access to.
    - Select **U-Series Appliance Login** for permission to log in to the appliance.



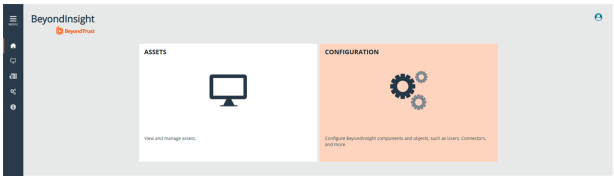
5. Click **Assign Permissions**, then select **Assign Permissions Full Control**.
6. In the left menu, click **Smart Groups.** Select assets to assign to the group. **U-Series Appliance** must be selected.
7. Click **Assign Permissions**, and then select **Assign Permissions Full Control**.

Assign SSO Users to Group

1. Go to **Configuration > Role Based Access > User Management > Groups**.
2. Select the permissioned group.
3. Click the ellipsis to the right of the goup, and then select **Add Users to Group**.
4. Search for the user name, and then check the box beside the name to add them to the group.

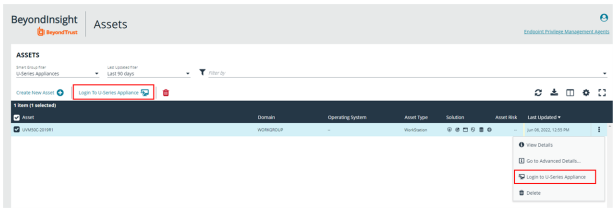


Once users have been added to the permissioned group, they will see a reduced version of the BeyondInsight Console when they log in. When they click on **Assets**, they will be able to select the assets they've been permissioned under the **Smart Group Filter**.



Users can log into the U-Series Appliance in one of two ways:

1. Select U-Series Appliance under the **Smart Group filter**.
2. Click the ellipsis to the left of the asset, and then select **Login to U-Series Appliance**



Or:

1. Select U-Series Appliance under the **Smart Group filter**.
2. Select the asset.
3. Click on the **Login To U-Series Appliance** button located above the grid.

For more information on creating a new user, please see Create and Manage User Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/role-based-access/user-accounts.htm.

Note: *Users that are delegated U-Series Appliance login permission are authenticated into the appliance(s) with admin privileges.*

Run Scans on Cloud Platforms in BeyondInsight

You can run scans on the following cloud types: Amazon EC2, Rackspace, IBM SmartCloud, Microsoft Azure, Microsoft Hyper-V, and Google Cloud.

Before you create a cloud connector, ensure the following requirements are in place.

Amazon EC2 Requirements

To use the Amazon EC2 connector, you must adhere to the following recommendation from Amazon:

- User accounts must have minimal permissions assigned (for example, describe instances).

The following minimum permissions are required to successfully enumerate a list of targets and run a scan:

- elasticloadbalancing:DescribeLoadBalancers
- ec2:DescribeInstances
- ec2:DescribeRegions
- ec2:DescribeInstanceStatus
- ec2:DescribeImages

Azure Requirements

The Azure connector extracts virtual machines and load balancers from Resource Manager. You must create an Azure Active Directory application.

You can either use the premade **Reader** role, or set up a new **Virtual Machine Contributor** role to the **Azure Resource Group**. You must choose where in the Azure hierarchy you are giving access — either as high as the subscription, or for a specific Resource Group. If you choose to set up a new role, the minimum permissions that must be granted are:

- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/instanceView/read
- Microsoft.Network/loadBalancers/read
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read
- Microsoft.Network/networkInterfaces/read
- Microsoft.Network/networkInterfaces/loadBalancers/read
- Microsoft.Network/publicIPAddresses/read

For detailed instructions, please see Create an Azure Active Directory Application at https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal.

Google Cloud Requirements

- **Key file:** You must download a key file from the Google cloud instance. The key file is uploaded when you create the connector in BeyondInsight.

Note: *The key file is not required if your BeyondInsight server is hosted on your Google cloud instance.*

- **Compute Engine Network Viewer Role:** The BeyondInsight service account that you create in the Google cloud instance requires the **Compute Engine Network Viewer** role.

For more information, please see Compute Engine IAM Roles at https://cloud.google.com/compute/docs/access/iam.

Hyper-V Requirements

Note: *The steps required for successful authentication vary depending on your environment. These instructions are to connect a Hyper-Vi virtual machine on the CIMV2 namespace off root (not connecting to a Hyper-V server).*

Set Firewall

1. Open Windows Firewall (**Start > Control Panel > Security > Windows Firewall**).
2. Select **Allow a program or feature through Windows Firewall**.
3. Check the Windows Management Instrumentation (WMI) box, and then check the **Public** box.
4. At this point you can send requests but receive unauthorized exceptions, whereas previously the host would not be found.

Add WMI user to COM Security

1. Start **Component Services**. Using the **Run** command, enter **dcomcnfg.exe**.
2. Expand **Component Services > Computers**.
3. Right-click **My Computer**, and then select **Properties**.
4. Select the **COM Security** tab, and then in **Access Permissions**, click **Edit Limits.**
5. Add the username you are using for WMI, and then select **Local Access** and **Remote Access**.
6. Click **OK**.
7. In **Launch and Activation Permissions**, click **Edit Limits**.
8. Add the WMI user, and then select **Remote Launch** and **Remote Activation**.

Change WMI Permissions

1. Start the **Computer Management** snap-in by using the **Run** command, and entering **compmgmt.msc**.
2. Expand **Services and Applications**.
3. Right-click **WMI Control**, and then select **Properties**.
4. Click the **Security** tab.
5. Select **Root\CIMV2**, and then click **Security**.
6. Add the user, and then click **Advanced**.
7. Double-click the user, and then check the following boxes: **Enable Account**, **Remote Enable**, and **Read Security**.

8. From the **Apply to** list, select **This namespace and subnamespaces**.
9. Restart the **WMI** service.

Test Connection

Use **WBEMTest** on the local machine (not your Hyper-V server) to test your connection.

1. Run **wbemtest.exe** from the command prompt.
2. Click **Connect**.
3. Enter the namespace in the format **\\HOST\root\CIMV2**, where host is a computer name on a domain or an IP address.
4. Enter a username and password.
5. Click **Connect**.

Configure a Cloud Connector

1. In the BeyondInsight console, go to **Configuration > General > Connectors**.
2. In the **Connectors** pane, click **Create New Connector**.
3. Provide a name for the connector, and then select a **Connector Type** from the list:
    - **AWS Scan Target Collector**
    - **Azure Scan Target Collector**
    - **Google Cloud Scan Target Collector**
    - **Hyper-V Scan Target Collector**
    - **Rackspace Scan Target Collector**
4. Click **Create Connector**.
5. Enter the connector information in the right pane:
    - For AWS cloud connections, required fields are: **Region**, **Access Key ID**, and **Secret Access Key ID**.

      Instances associated with the region are displayed in the **Connection Test Results** section.

    - For Azure, required fields are: **Region**, **Client ID**, **Client Server**, **Tenant ID**, and **Subscription ID**.
    - For Google Cloud, required fields are **Server** (the region), **Project Name** (the project ID), and the **Key File**. Upload the key that you downloaded from the Google Cloud.
    - Hyper-V server, required fields are: **Server** (IP address), **Username**, and **Password**.
    - For Rackspace, required fields are **Account Type**, **Username**, and **API Key**.
6. After you configure the connector, click **Test Connector** to ensure the connector works.
7. Click **Create Connector**.

After you create a cloud connector, you can run a scan and review the results to determine what cloud assets were discovered..

Cloud Connector Smart Groups

You can create Smart Groups based on the cloud connectors that you are using.

1. From the left menu, click **Smart Rules**.
2. Click **Create Smart Rule**.
3. Select a category, and then enter a name and description.
4. Under **Selection Criteria**, select **Cloud Assets**, and then select the cloud connector type to filter on (**AWS**, **Azure**, **Hyper-V**).
5. For AWS, click **Select AWS Instance Types** to pick specific instance types.
6. For AWS, Azure, and Google, check the **Use Private IP Address** box to scan internal IP addresses.
7. Under **Actions**, select **Show asset as Smart Group**.
8. Click **Create Smart Rule**.
9. Run a discovery scan on the smart group to see the cloud assets in reports.
10. On the **Assets** page, select the cloud connector, and then click the vertical ellipsis button to review the details.

Configure BeyondInsight AWS Connector

This section provides information on setting up an Amazon AWS connector, including details on the AWS configuration.

Set up a Policy

1. Log in to the **AWS Management Console**.
2. Select **Identity & Access Management**.
3. Select **Policies** from the **Details** menu.
4. Select **Create Policy**.
5. Select **Create Your Own Policy**.
6. Enter a policy name and description.
7. Paste the following JSON into **Policy Document**:

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "elasticloadbalancing:DescribeLoadBalancers",
            "ec2:DescribeInstances",
            "ec2:DescribeRegions",
            "ec2:DescribeInstanceStatus",
            "ec2:DescribeImages"
        ],
        "Resource": "*"
    }
]
}
```

***Note:** For **"Resource": "*"**, you must determine what JSON is required for your current needs. You may also need a condition with this, such as if you want only the **dev** group to have access to certain instances.*

Grant Access to a Third Party (Optional)

> ***Note:*** *The **ARN** and **External Name** fields are for granting access to a third party. For more information, please see How to Use an External ID When Granting Access to Your AWS Resources to a Third Party at https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html.*

After you configure the AWS settings, you can create the connector and smart groups in the BeyondInsight Console.

Work with the Multi-Tenant Feature in BeyondInsight

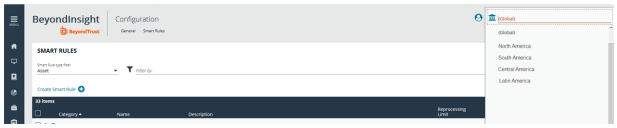
The multi-tenant feature in BeyondInsight allows you to define multiple organizations (or tenants) where each organization's asset data is kept isolated from all other organizations. Only Smart Rules marked as **Global** can combine asset data across multiple organizations.

Most BeyondInsight features are available with multi-tenant, including Smart Rules and connectors.

Features not available include exclusions, tickets, and report templates.

Select Tenants on the Smart Rule Page

All of the pre-packaged Smart Rules are part of the Global Rules. When a pre-packaged Smart Rule is turned on, the Smart Rule applies to all assets in every organization. You can use the **Organization** filter in the page header next to the **Profile and preferences** icon to easily switch the rules displayed in the grid from the **Global** rules to rules for specific tenants.



Note: *When you initially create an organization, both the default and the new organization is provisioned with the* ***All Assets*** *Smart Rule. Also, all active built-in Smart Rules are copied from the default organization to the new organization; inactive built-in Smart Rules are not copied from the default to the new organization.*

Note: *Create Smart Rules as usual. For more information, please see "Use Smart Rules to Organize Assets" on page 66.*

Quick Rules

When you create a quick rule from the **Address Group**, you can select the organization.

Organization Filters

When working with more than one customer, use the **Organization** filter to see assets and Discovery Scanner agents associated only with a particular customer.

The **Organization** filter is displayed only if more than one active organization is available to the currently logged-on user.

Many pages in the console are organization- aware and reflect the organization chosen in your profile. However, other pages may still require you to select an organization on that page. If there is no saved value for the organization in your profile, the **Global** organization is default.

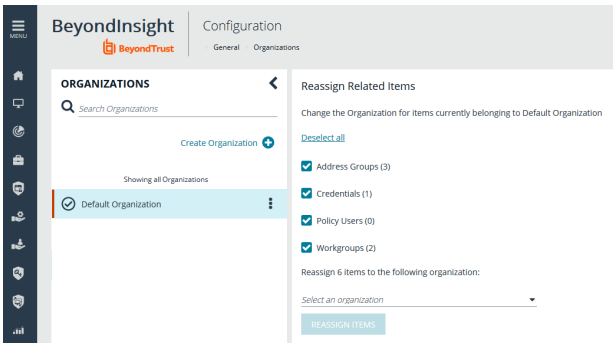
Address Groups

You can organize address groups by organization. When working in the **Address Groups** configuraton area, you can select an organization and see the address groups specific to that organization.

Reassign Related Items

To migrate existing organization-aware items to a different organization:

1. From the menu, select **Configuration**.
2. Under **General**, select **Organizations**.
3. In the **Organizations** pane, click **Actions** icon next to the name of the organization you wish to migrate, and then click **Reassign Related Items**.
4. Check the box next to the items you wish to migrate:
    - **Address Groups**
    - **Credentials**
    - **Policy Users**
    - **Workgroups**
5. Click the **Select an organization** drop down menu, and then select the name of the organization you wish to migrate the items to.
6. Click the **Reassign Items** button.



Select a Workgroup

For unknown assets (assets not scanned by BeyondInsight), you must select a workgroup associated with the organization. Assets might be unknown when using the settings:

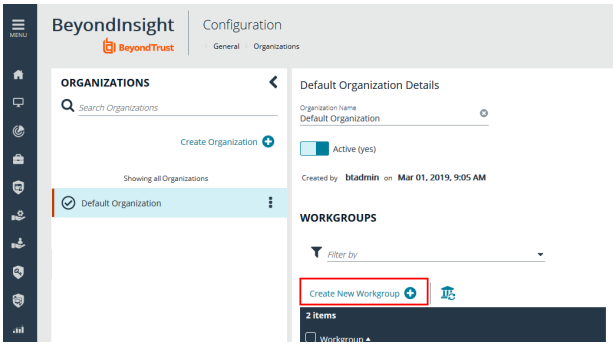
- **Single IP address**
- **IP range**
- **CIDR notation**
- **Named hosts**

For known assets (assets detected and in the BeyondInsight database), a workgroup does not need to be selected. The assets are already associated with a workgroup. Assets are known when using the settings:

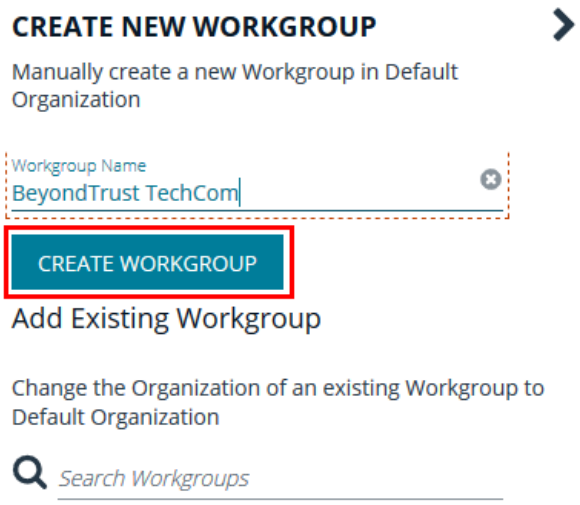
- **Currently selected Smart Group**
- **Currently selected Assets**

Create a New Workgroup

1. From the menu, select **Configuration**.
2. Under **General**, select **Organizations**.
3. In the **Organization Details** panel, under **Workgroups**, click the **Create New Workgroup** link.



4. In the **Create New Workgroup** pane, enter a **Workgroup Name**, and then click the **Create Workgroup** button.



Set Up Organizations

Create a Workgroup

The **Users Accounts Management** feature is required to assign workgroups to an organization.

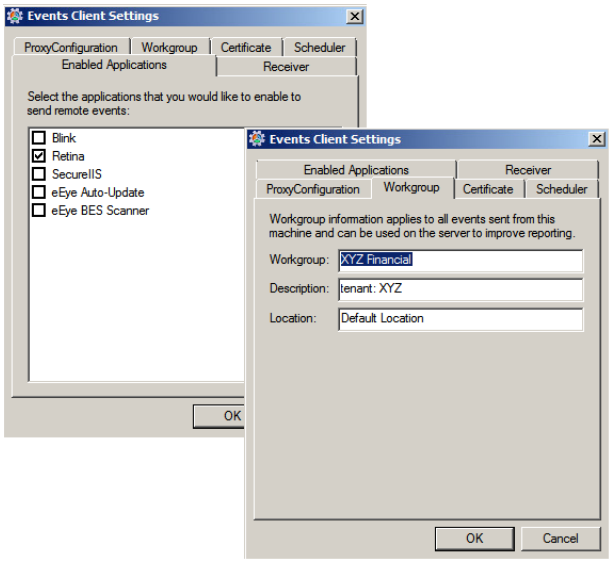
Each Discovery Scanner must be assigned a workgroup. A workgroup is typically created when the agent is initially deployed.

You can add and delete workgroups. However, you cannot rename workgroups.

You can delete a workgroup only if it is not associated with an organization, mobility connector, or Discovery Scanner.

Use the **Events Client Configuration** tool to create a workgroup.

1. Log on to the asset where the agent resides.
2. Start the **Events Client Configuration Tool**.
3. Select the **Enabled Application** tab, and check the box for the agent.
4. Select the **Workgroup** tab and enter a name and description.
5. Click **OK**.



Add an Organization

An organization is automatically populated with an **All Assets** Smart Group.

1. Select **Configuration**, and then click **Organizations**.
2. Click **Create Organization**.
3. Enter the name of the organization, and then click **Create**.
4. The **Active** option is enabled by default and must be enabled to successfully run scans on the tenant's assets.
5. Click **Workgroups**.
6. Click the edit icon for the organization, and then select the organization.
7. Click the check mark to save the changes.

Create a Group for a Tenant

You can create a group for a tenant. The users in the group can then log in to BeyondInsight and run reports. When creating the user group, ensure that you assign the BeyondInsight permission. Additionally, assign **Read** permissions to the tenant's Smart Rules. The users can then run reports based on the Smart Rules.

> ***Note:*** *Creating a group for a tenant is optional and only required if your client wants to run reports from BeyondInsight. For more information, please see* *"Role-Based Access" on page 18**.*

As a security measure, a tenant cannot log in to BeyondInsight.

Set BeyondInsight Options

Set Account and Email Options

> *If you use Clarity, for configuration information please see Configure Clarity Analytics at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/analytics/configure.htm#Clarity.*

Account Lockout Options

You can set lockout options, such as lockout threshold and duration.

1. Select **Configuration**.
2. Under **Role Based Access**, select **Local Account Settings**.
3. Under **Account Lockout**, set the following options:
    - **Account Lockout Duration:** Sets the number of minutes that the user is locked out after they hit the account lockout threshold. Once this time has elapsed, an attempt will be made to unlock the account during the user's next log in. Setting this value to **0** (zero) requires the account to be manually unlocked by an administrator.
    - **Account Lockout Threshold:** Sets the number of times a user can try their password before the account is locked out.
    - **Account Lockout Reset Interval:** Sets the number of minutes after an account is locked due to unsuccessful entry attempts before resetting the lockout counter.
    - **Unlock account upon password reset request:** When set to **Yes**, unlocks the account when the **Forgot Your Password** process is followed by the user. When set to **No**, the user may reset their password using the **Forgot Your Password** process, but the account remains locked until an administrator unlocks it.
    - **Send lockout notification:** When set to **Yes**, sends a notification to the email address configured in the **Lockout Notification Recipients** when any account becomes locked out.
    - **Lockout notification recipients:** Sets the email address where the lockout notification is sent. The **Send Lockout Notification** switch must be set to **Yes** for this to be relevant.
4. Click **Update Account Lockout Options**.

Account Password Options

You can set account password parameters, such as a complexity requirement and password length.

1. Select **Configuration**.
2. Under **Role Based Access**, select **Local Account Settings**.
3. Under **Account Password**, set the following options:
    - **Enforce Password History:** Enter the number of passwords a user must create before an old password can be reused. Enter **0** to not enforce a password history. There are no restrictions on using past passwords when **0** is entered.
    - **Maximum Password Age:** Enter the maximum number of days before a password must be changed.
    - **Minimum Password Age:** Enter the minimum number of days that a password must be used before it can be changed.
4. Click **Update Account Password Options**.

Email Notifications

The email notification functionality allows BeyondInsight to send email under certain circumstances. This includes, but is not limited to, emails sent upon ticket assignment, password reset, user lockout notifications, smart rule actions, or API authentication failures.

Note: *Email SMTP settings are initially set in the BeyondInsight configuration tool. Verify these settings are accurate and that you use the same information. Changes made here will be reflected in the configuration tool.*

1. Select **Configuration**.
2. Under **System**, select **Email Notifications**.
3. Enter an email address in the **From email address** box. This sets the email address that appears in the **From** and **Reply-To** fields for email notifications sent by BeyondInsight.
4. Optionally, enable the **Notify administrator on cloud connector failure** setting. When enabled, this option sends an email if an error occurs while collecting cloud data using a connector configured in BeyondInsight.
5. Click **Update Email Notification Options**.

Note: *An email is sent every 24 hours.*

Set Support Options

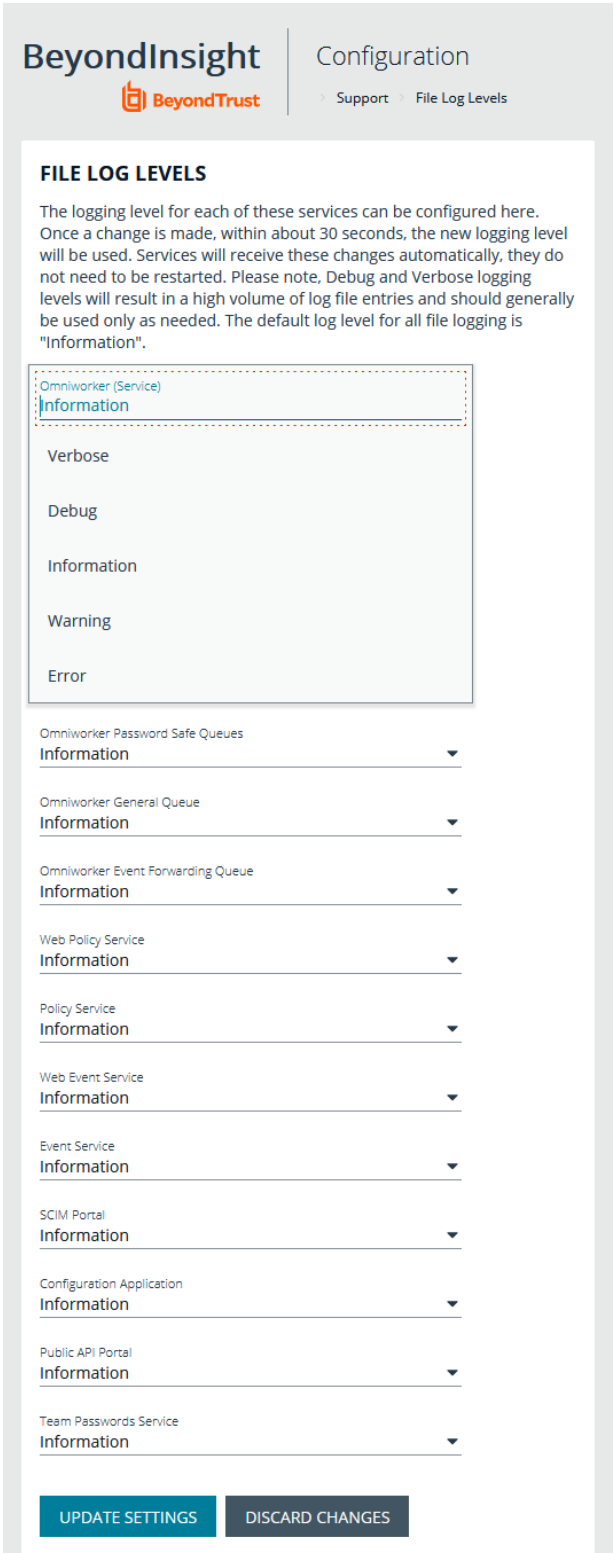
You can use the following support options to assist with troubleshooting issues with BeyondInsight:

- Select log levels for BeyondInsight services log files.
- Enable and configure system event recording. This feature consolidates selected events from multiple log files to the BeyondInsight database and displays this data in the System Event Viewer grid.
- View recorded system events.

Select File Log Levels

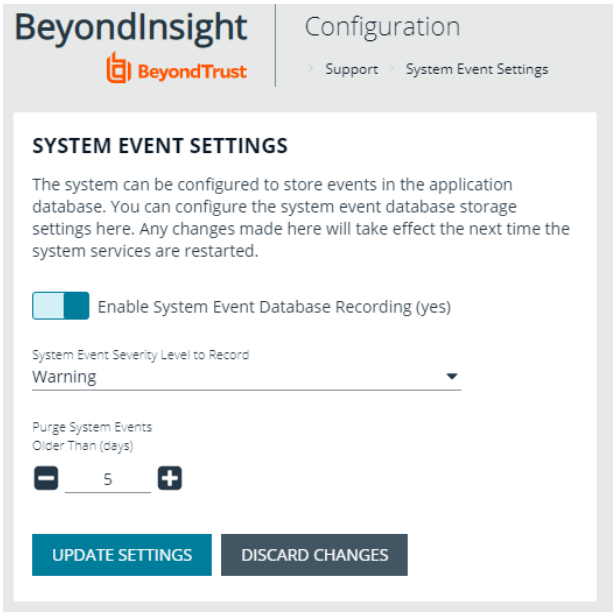
1. From the **Home** page in the BeyondInsight Console, select **Configuration**.
2. In the **Support** pane, select **File Log Levels**.

3. For each service, select the desired logging level:
    - The options are **Verbose**, **Debug**, **Information**, **Warning**, and **Error.**
    - The default for all services is **Information**.
    - **Verbose** and **Debug** create a large volume of entries and should be used only when necessary.
4. Click **Update Settings**.
5. Changes take effect in about 30 seconds. Services do not need to be restarted.



Enable System Event Recording

1. From the **Home** page in the BeyondInsight Console, select **Configuration**.
2. In the **Support** pane, select **System Event Settings**.
3. Click the toggle to **Enable System Event Database Recording**.
4. From the **System Events Severity Level to Record** dropdown, select:
    - **Warning**, to record warnings and errors
    - **Error**, to record errors only
5. Set the number of days to retain recorded events in the field **Purge System Events Older Than**.

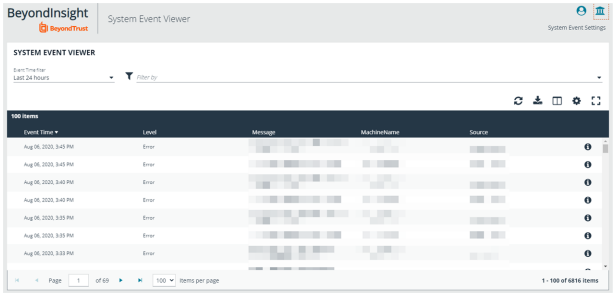


***Note:** Once events are purged, they are not available in the **System Event Viewer**.*

System Event Viewer

***Note:** System event recording must be enabled (as above) to view events in the **System Event Viewer**.*

1. From the **Home** page in the BeyondInsight Console, select **Configuration**.
2. In the **Support** pane, select **System Event Viewer**.
    - This screen shows the events recorded and retained as per the **System Event Settings**.
    - The list of events can be filtered by **Event Time** and additional filters can be added.
    - On the right, above the column headings, there are icons to refresh and download the list of events, and to modify the appearance of the list, including adding or removing columns.
    - You can sort any column by clicking on the heading. An arrow appears to indicate whether the sort is ascending or descending. Click again to reverse the sort.
    - At the bottom of the list, you can page through the events and set the number to display per page.



3. To view the full log file entry for any event, click the **i** at the right end of the event row.

Set Data Retention and Advanced Purging Options

When data is initially collected, it is stored as unprocessed data in the BeyondInsight database. After the data is processed and made available in the management console and reports, the unprocessed data is no longer needed. To maintain a manageable database size, the unprocessed data is purged at regular intervals. Go to **Configuration > System > Data Retention** to manage BeyondInsight's data retention.

Data Retention

Maintenance

To maintain a manageable database size, the unprocessed data is purged at regular intervals. These intervals are for the purging of Vulnerability Management data and can be configured here.

> ***Note:*** *Vulnerability Management has been deprecated and will be removed from the product in a future version.*

Purge general events older than	Sets the number of days to keep the data sent by the agents. General events can include events like checking in and trying to connect to assets, and firewall events which might indicate that the scan cannot process because of a firewall blocking the connection. The default number of days is **7**.
Purge attacks older than	Sets the number of days to keep attack data that was discovered by the protection agent. Recommended: **90 days**.
Purge application events older than	Sets the number of days to keep the application events sent by the agents. The default value is **7**.
Purge scans older than	Sets the number of days to keep the information defined in the scan settings. Recommended: **7 days** .
Purge scan events older than	Sets the number of days to keep the data collected in scans. Recommended: **7 days**.
Purge attack events older than	Sets the number of days to keep the data sent by the protection agents. Recommended: **7 days**.
Purge discovery agent jobs every N days	When enabled, sets the number of days to keep the discovery data collected by the agents. Recommended: **1 day**.

Click **Update Maintenance Options** to save your option settings.

Privileged Access Management

To maintain a manageable database size, older event data is purged at regular intervals. The intervals for the purging of privileged access management event data can be configured here.

Purge Windows events older than	Purges the information sent by the protection agents. **The default value is 90 days.**
Purge Endpoint Privilege Management events older than	Sets the number of days to keep Endpoint Privilege Management's unprocessed event data. **The default is 30 days.**
Purge Privilege Management for Unix & Linux events older than	Sets the number of days to keep events sent by Privilege Management for Unix & Linux Servers.
Purge file integrity events older than	Sets the number of days to keep File Integrity events captured by Endpoint Privilege Management.
Purge Endpoint Privilege Management Session Monitor events older than	Sets the number of days to keep the events collected when session monitoring is being used.
Purge Identity Services events older than	Sets the number of days to keep Identity Services unprocessed event data.

Click **Update Privileged Access Management Maintenance Options** to save your option settings.

Asset Maintenance

To maintain a manageable database size, the unprocessed data is purged at regular intervals. The intervals for the purging of asset data can be configured here.

Purge assets	When enabled, **Purge assets older than** sets the number of days to keep asset data for assets that were discovered once, but are never discovered again. Recommended: **30 days**.
Purge asset attributes	When enabled, **Purge asset attributes older than** sets the number of days to keep asset attribute data, such as ports, services, hardware, and attack events. Recommended: **7 days**.
Purge Cloud assets	When enabled, **Purge Cloud assets older than** sets the number of days to keep cloud asset data. Cloud asset purging does not run unless **Purge Assets** is also enabled. The **Purge cloud assets older than** setting must always be equal to or less than the **Purge assets older than** setting. Recommended: **30 days**.

Click **Update Asset Maintenance Options** to save your option settings.

Application Maintenance

To maintain a manageable database size, the unprocessed data is purged at regular intervals. The intervals for the purging of application data can be configured here.

Purge reports older than	Sets the number of days to keep report files that are stored on the file system and corresponding database. The default value is **90 days**.
Purge application user audits older than	Sets the number of days to keep user application audit data. Audit data is the record of user activities in the BeyondInsight system. Recommended: **120 days**.
Purge closed tickets older than	Sets the number of days before closed or inactive tickets are deleted. The calculation for purging ensures the ticket is closed and uses the date the ticket was last updated, not the due date. For example, a ticket has a due date 60 days in the future but the ticket was closed and not edited for over a week. If the purge setting is set to **7**, then the ticket is purged even though the due date is in the future.

Click **Update Application Maintenance Options** to save your option settings.

Third-Party Integration Maintenance

To maintain a manageable database size, the temporary data is purged at regular intervals. The interval for the purging of **Third Party Integration** temporary data can be configured here.

Purge third-party uploads older than	Sets the number of days to keep the information about the scan files that you upload. The default is **90 days**.

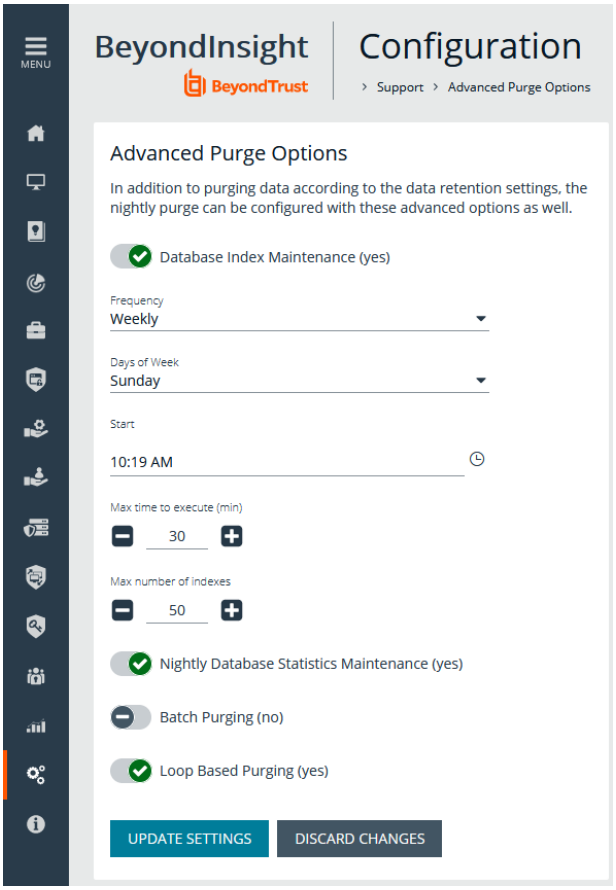
Note: *The data in the scan file is not purged.*

Click **Update Third-Party Integration Maintenance Options** to save your option settings.

Purging Options

In addition to purging data according to the data retention settings, the nightly purge can be configured with these advanced options. Go to **Configuration > Support > Purging Options** to set the following advanced options:

- **Database Index Maintenance:** (Disabled by default) When you enable this option, you can choose how frequently you want to purge the index, set the maximum time for the purge to execute in minutes, and set the maximum number of indexes to purge.
- **Nightly Database Statistics Maintenance:** (Enabled by default) This option purges database statistics each night.
- **Batch Purging:** (Disabled by default) Enable this option to purge multiple assets at one time in a batch. When this option is enabled, the complete asset, including all asset attributes is purged (all older data is removed from the asset). When this option is disabled, one asset is purged at a time, as opposed to a batch of assets.
- **Loop Based Purging:** (Disabled by default) When this option is enabled, after a round of purging is complete, the purge window is checked and if still in the purge window AND there are more than 1000 items left to purge, another round of purging begins. This looping cycle repeats until the purge window expires or there is not enough data worth deleting. The default purge window begins at 1:00 AM and is two hours long. When this option is disabled, only one round of purging is performed each day.



Configure Proxy Settings

You can configure a proxy server if your BeyondInsight server does not have direct internet access.

1. In the BeyondInsight Console, select **Configuration**.
2. Under **System**, select **Proxy Settings**.
3. Click the toggle to **Enable proxy support**.
4. Enter the IP address (including the prefix **http://**) or the FQDN (for example, **somehost.example.com**) of the proxy server, username, and password for the proxy server.

> ***Note:*** *The HTTPS protocol is not supported for the IP address or the fully qualified domain name.*

5. Click the toggle to override any local proxies.
6. Click **Update Proxy Settings**.

Configure Discovery Management Options

Set Job Refresh Options

You can set a refresh interval, which changes job refresh logic to avoid polling third party credentials. Instead, the jobs refresh a number of minutes before scan. You can set refresh intervals for scan jobs and Smart Rules. Scans can run more efficiently when Smart Rules are set to refresh at longer intervals.

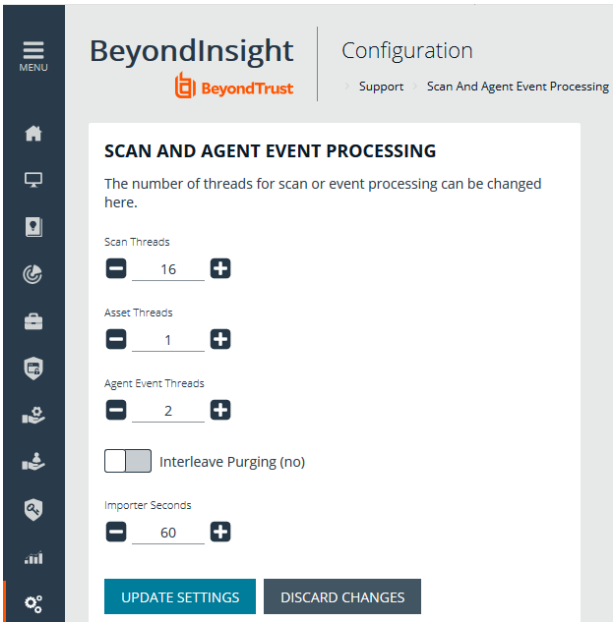
1. Select **Configuration > Discovery Management > Options**.
2. Under **Job Refresh**, set the following options:
    - **Maximum job refresh frequency:**BeyondInsight jobs are refreshed at the interval set. When the refresh occurs, updates to schedules, scanners, and Smart Rules are updated for the job. The default value is **360** minutes.
    - **Time to refresh before scan for third party credentials:** Sets a refresh interval which changes job refresh logic to avoid polling third party credentials. Instead, the jobs will refresh a number of minutes before scan.

Set Scan and Event Processing Options

Go to **Configuration > Support > Processing Options** to set the number of threads for scan and event processing. The following options are available:

- **Scan Threads**: The number of scans that can be processed at one time. The default is **16**.
- **Asset Threads**: The number of assets per scan that can be processed at one time. The default is **1**.
- **Agent Event Threads**: These are threads used for **Discovery Scan** data processing.
- **Interleave Purging**: When set to **yes**, uses idle threads to work on purging assets one at a time, if there are any assets queued up to be purged. If set to **no** (default), all purging activity is restricted to the dedicated purge window.
- **Importer seconds**: The number of seconds between each attempt to purge; only applies if **Interleave Purging** is set to **yes**.

Click **Update Settings** when done.



Configure Global Site Options

You can configure global website settings from the **Configuration > System > Site Options** page, including:

- Changing the **Login** page to include lists of domains and LDAP servers
- Displaying the **Forgot Password** link on the **Login** page
- Displaying social media links on the **Login** and **About** pages
- Changing the refresh interval for Smart Rules
- Configuring a pre-login banner to appear to users before logging into the site
- Configuring session options
- Enabling and disabling Endpoint Privilege Management options
- Enforcing certificate validation during communication for LDAPS managed account tasks and LDAPS / AD user authentication and directory queries
- Turning on language selection
- Enabling and disabling the requirement to provide an access key when creating, editing, or using discovery scan credentials.
- Creating a global access key to be used for all discovery scan credentials

List Domains and LDAP Servers on the Login Page

Users can log in to the management console using Active Directory or LDAP credentials. When this site setting is enabled, the user can select a domain or LDAP server from the **Log in to** list. Domain and LDAP server information is based on the Active Directory and LDAP user group information.

***Note:** The **Log in to** list is only displayed on the **Login** page when there are either Active Directory or LDAP user groups created in the management console.*

***Tip:** By default, the setting is enabled. If you do not want to display domains or LDAP severs on the **Login** page, disable the setting.*

1. Under **Login Page**, click the toggle to disable **Show list of domains/LDAP servers on login page**.
2. Click **Update Login Page Options**.

You must log out and log back in for the change to take effect.

Display Forgot Password Link

Users logging into the console using Active Directory credentials cannot use the **Forgot Password** feature. In this scenario, you can disable the setting so the link is no longer displayed on the **Login** page.

1. Under **Login Page**, click the toggle to disable **Show Forgot Password link on login page**.
2. Click **Update Login Page Options**.

You must log out and log back in for the change to take effect.

Display Social Media links on the Login and About pages

By default, links for Facebook, Twitter, LinkedIn, and YouTube are available at the bottom of the **Login** page and also on the **About** page.

1. Under **Login Page**, click the toggle to turn off **Show social media links on login and about pages**.
2. Click **Update Login Page Options**.

You must log out and log back in for the change to take effect.

Change the Refresh Interval for Smart Rules

Scans can run more efficiently when Smart Rules are set to refresh at longer intervals.

1. Under **General**, set the number of minutes for **Maximum Smart Rule refresh frequency for asset updates**. The default is **60**.
2. Click **Update General Options**.

Configure a Pre-Login Banner

You can configure a banner to appear to all users upon access to the site.

1. Under **Pre-Login Banner**, click the toggle to enable the **Show Banner**.
2. Provide a title and message, and then click **Update Pre-login Banner Options**.

Configure Session Options

You can configure the following session related options:

- Session timeout
- Notification time before session timeout
- Minimum interval between session extension requests
- User Quarantine Cache refresh interval

1. Under **Session**, set the following:
    - **Session timeout:** Sets the amount of time for session inactivity before the session times out. Session timeout can be set between 2 and 60 minutes, with the default set at 20 minutes.
    - **Notification time before session timeout:** Sets the amount of time, prior to the session timing out due to inactivity, that the system notifies the user that their session will timeout shortly. This value must always be less than the session timeout value.
    - **Minimum interval between session extension requests:** Sets the number of minutes that pass between session extension requests. In general, this setting should always be set low and should always be less than the session timeout value. The only time you should change this from the default of three minutes is if there are a severely high number of simultaneous users and session refresh requests to the server causing high loads.
    - **User Quarantine Cache refresh interval:** Account Quarantine is a feature that can be set at the user account level that prevents a user from logging on the console or API and also terminates any active sessions immediately. It is a preventative measure taken when suspicious activity is detected. The User Quarantine Cache refresh interval sets the number of seconds that pass before the database is updated with the most recently discovered user accounts from the

quarantine cache. The quarantine is only applied to the user account after the database is updated. The user can remain logged on and sessions remain active up until the refresh interval time passes, and the database is updated with a **Quarantine** status. The default value is **600** seconds. The maximum value is **1200** seconds.

2. Click **Update Session Options**.

Enable Language Selection (Localization)

The management console can be viewed in the following languages:

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

By default, the **Language** list is not displayed in the BeyondInsight console. Once localization is enabled, the **Language** list may be accessed from the **Profile and preferences** icon in the top right corner of the console and also from the bottom of the **Login** page.

1. Under **Localization**, click the toggle to enable the **Show language picker** option.
2. Click **Update Localization Options**.

You must log out and log back in for the change to take effect.

Enable Endpoint Privilege Management Options

Endpoint Privilege Management options are not enabled by default. You can enable the following options:

- Include arguments when creating rules
- Suppress events where rule has been applied
- Automatically retrieve initial grid data

Enable Certificate Validation

Certificate validation helps enforce the validity of a given certificate during communication. You can enforce the validation for LDAPS managed account tasks and LDAPS / AD user authenticaion and directory queries. Turning these options on will mean that valid certificates are required and Certificate Authorities must be installed on the server.

Configure Global Discovery Credential Access Keys

When the **Require a Discovery Credential Key** option is enabled, all discovery credentials require the global credential access key. Enable the option, and then enter a **Global Credential Key**.

> ***Note:*** *You may still set a custom key on individual credentials to something other than the default.*

When the **Require a Discovery Credential Key** option is disabled, all discovery credentials do not require an access key and all previously configured credential keys (including custom keys) are deleted.

> ***Note:*** *These settings apply to ALL discovery credentials for ALL tenants.*

BeyondInsight Clarity Analytics

BeyondInsight Clarity is a behavior analytics tool that examines and classifies events and activities to identify outliers or anomalies. An outlier is an observation which deviates so much from the other observations that it arouses suspicion. Clarity ranks activities and classifies assets according to their deviation from normal activity. The normal activity or baseline is formed from:

- History of past activities
- Risk attributes of an observed activity

Each activity or event has several key characteristics. When an observed characteristic goes beyond normal, an alert is issued. More flagged alerts indicates higher level of abnormality and threat level. The numeric threat level is the sum of all flagged alerts. In addition, all assets are grouped into clusters by similarity, taking into account all available information including vulnerabilities, attacks, installed applications, services, open ports, running applications, etc.

As a result, the behavior analytics:

- Assigns a threat level to each event from BeyondTrust Discovery Scanner, Endpoint Privilege Management, Privilege Management for Unix & Linux, and Password Safe.
- Assigns cluster ID to all assets.

You can use Clarity to analyze data from the following sources:

- Endpoint Privilege Management
- Privilege Management for Unix & Linux
- BeyondTrust Discovery Scanner
- Password Safe
- Third-party imports

Configure Clarity Analytics

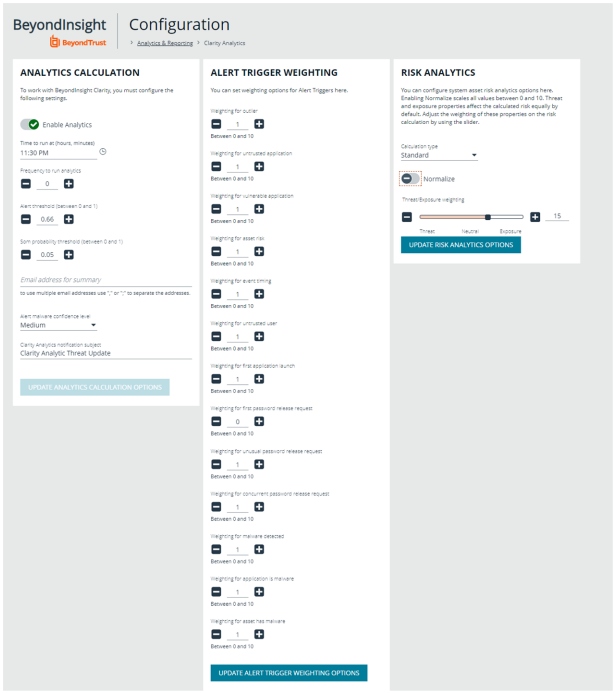
To work with BeyondInsight Clarity, you must configure settings in the BeyondInsight management console.

Note: *Malware and attack vulnerability risk detection features have been deprecated in BeyondInsight and no longer function. Options relating to malware and attack risk data are being removed in a future release.*

Configure the Analytics Calculation

1. In the console, click **Configuration**.
2. Under **Analytics & Reporting**, click **Clarity Analytics**.

3. From the **Analytics Calculation** section, you can:
    - Toggle **Enable Analytics** to turn on the feature.
    - Select the hours and minutes for **Time to run at**.
    - Select the frequency for running analysis.
    - Set the **Alert Threshold** for flagging explicit alerts. The higher the value, the higher the sensitivity and the fewer flagged alerts. The range is from **0** to **1**. The default value is **0.65**.
    - Set the **Som Probablity Threshold** for flagging pattern alerts. The lower the value, the higher the sensitivity and the fewer flagged alerts. The range is from **0** to **1**. The default value is **0.05**.
    - Enter an email address to send notifications to.
    - Set the notification subject.
4. Click **Update Analytics Calculation Options**.



Set Alert Trigger Weighing

From the **Alert Trigger Weighing** section, you can configure Clarity to prioritize or weigh specific alerts. If an alert with a higher weight is triggered, the alert appears more prominently in the Clarity analysis. This allows you to quickly see and react to critical alerts.

To configure a weight for an alert, click the minus and plus buttons to modify its numeric value, ranging from **0** to **10**. When you are satisfied with your selections, click **Update Alert Triggering Weighing Options** to finalize.

Configure Risk Analytics

Using the risk analytics values, you can focus the results data on the highest risk assets.

Enabling **Normalize** scales all values between 0 and 10. When you choose to normalize the data, the asset at the highest risk is assigned the highest rating. All other assets are rated and organized below the highest risk asset. Normalizing the results provides a way to distribute the assets in a more meaningful way to analyze the data.

Threat and exposure properties affect the calculated risk equally by default. Adjust the weighting of these properties on the risk calculation by using the slider. You can change the results to emphasize risk levels based on exposures or threats. For example, if you move the slider to **Exposure**, asset exposure risk factors are given greater weighting in the final risk calculation and increase an asset's risk score.

Clarity Reports

The following reports are available to run against Clarity data:

- **Event Review - Endpoint Privilege Management:** Breakdown of alert triggers for events by threat level. Includes relevant event details, and is ordered by threat level from largest to smallest.
- **Event Review - Password Safe Release Events:** Breakdown of alert triggers for Password Safe release events by threat level.
- **Event Review - Privilege Management for Unix & Linux** Breakdown of alert triggers for Privilege Management for Unix & Linux events by threat level. Includes relevant event details, and is ordered by threat level from largest to smallest.

- **Top 10 Assets by Total Threat Level:** Displays top 10 assets based on overall threat level.
- **Top 10 Users by Threat Level:** Displays top 10 users based on overall threat level.

Use the Clarity Dashboard

The Clarity Dashboard analyzes information stored in BeyondInsight's centralized database, which contains data gathered from across any or all BeyondInsight supported solutions deployed in the customer environment. These include:

- Endpoint Privilege Management
- Privilege Management for Unix & Linux
- BeyondTrust Discovery Scanner

Triggers

The **Triggers** list displays the total number of events which are affected by each trigger. The following triggers identify assets that are at risk.

> ***Note:*** *Malware and attack vulnerability risk detection features have been deprecated in BeyondInsight and no longer function. Options relating to malware and attack risk data are being removed in a future release.*

Trigger	Description
Untrusted User	Triggers when potentially untrusted users log into Administrator or local accounts. Can be triggered by events in the following products: • Endpoint Privilege Management • Privilege Management for Unix & Linux • BeyondTrustDiscovery Scanner
First Password Request	• Password Safe events • User requests password for a managed account and system they have never requested before
Outlier	Triggers when an event is determined to be an outlier based on Clarity analysis. Can be triggered by events in the following products: • Endpoint Privilege Management • Privilege Management for Unix & Linux • Password Safe • BeyondTrust Discovery Scanner
Unusual Password Release Request	• Password Safe events • User does not retrieve the password for approved request or the password is retrieved more than once
Concurrent Password Release Request	• Password Safe events • Triggers if a user requests more than one password at the same time.
Untrusted Application	• Endpoint Privilege Management events.

	• Triggers when unsigned and un-versioned applications are found on system.
First Application Launch	Triggers when an application is launched for the first time. Can be triggered by events in the following products: • Endpoint Privilege Management • Privilege Management for Unix & Linux • User launches an application they have never launched before

If a trigger has events, you can click the trigger to view the risk events that make up the count.

Risk Events by Threat Level

Drill into the risk events to learn more about the event, such as the trigger, type of event, or severity. Use the **Tab** key to navigate through the areas on the page and to view the metrics on the bubbles.

View Cluster Maps

> ***Note:*** *This feature is deprecated for new installations of BeyondInsight 22.1 and future releases. Cluster Maps and Cluster Analysis are available only for BeyondInsight releases prior to 22.1 and if upgrading to 22.1 from previous releases.*

A cluster map is a visual representation of the following cluster types.

- **Asset Cluster:** Larger clusters indicate more assets sharing similar traits within an organization. Smaller clusters indicate a potential anomaly. Clusters groups include:
    - Launched applications
    - Vulnerabilities
    - Attacks
- **User Cluster:** Represents Password Safe users that share similar characteristics in an organization.

Cluster Map Numbering

A cluster map number is randomly generated and does not have any meaning in the context of the actual data. However, the closer the cluster map numbers, the more similar the attributes of the assets to each other.

For example, assets assigned to cluster 14 and cluster 16 would have similar qualities. However, assets assigned to cluster 14 and cluster 68 would have fewer qualities in common.

The cluster map numbers can change at any time, but this does not reflect on the assets or any potential anomalies that might exist.

Cluster Shading

Asset

Shading is based on the **Asset Risk**, **Attacks**, **Vulnerability** app value. The Cluster Map uses the highest of the three, and the gradient is based on a range from 0.0 to 1.0.

User

Shading is based on the **User Risk** attribute for Password Safe users.

Asset Cluster Attributes

There are eight cluster attributes organized in the following categories:

- **Ordering attributes:** Attributes are ordered from low to high.
- **Pattern attributes:** A pattern value maps a set of characteristics to a single value (in the range 0 – 1). The difference in pattern values shows similarities between different sets of the same type characteristics.

Attribute	Type	Description
Attacks	Ordering	Number of detected attacks. Greater value means more detected attacks.
Vulnerable Apps	Ordering	Number of launches of vulnerable applications. Greater value means more started/running vulnerable applications.
Risk	Ordering	Asset risk. Greater value means greater risk.
App Set	Ordering	Running or/and elevated (depends on Privilege Management for Windows Servers) applications.
Vulnerabilities Set	Pattern	Discovered vulnerabilities.
Service Set	Pattern	Services
Software Set	Pattern	Installed software packages.
Port Set	Pattern	Opened ports.

User Cluster Attributes

Attribute	Type	Description
SharedSysAssetRisk	Ordering	Number of blocked commands in a Password Safe session, corresponds to block, block+lock, lock, and terminate command triggers.
SharedSysDenied	Ordering	Number of denied session requests.
SharedUsrRisk	Ordering	Maximum risk on an access policy associated with the user.
SharedSysSet	Pattern	Machines a user can access.
SharedSysVulnSet	Pattern	Vulnerabilities for machines a user can access.
SharedSysSrvSet	Pattern	Services for machines a user can access.
SharedSysSoftSet	Pattern	Software installed for machines a user can access.
SharedSysPortSet	Pattern	Ports for machines a user can access.

Analyze Cluster Maps

You must configure settings in BeyondInsight before any data is collected.

The following procedure shows examples from asset clusters. The procedure and analysis is similar for user clusters.

1. From the menu, select **Cluster Analysis**. By default, the **Cluster Map** tab is selected.
2. Select one of the following tabs to analyze cluster map data:
    - **Asset Counts:** Clusters the assets with similar characteristics. The smaller the cluster tile, the more likely there is an outlier.
    - **Cluster Risk:** Clusters the assets based on the common risk characteristics. The larger tiles in the cluster map have the greater risk.
    - **Attacks:** Clusters assets based on the common attack properties. The larger tiles indicate a greater attack level. Drill down to learn more about the assets and the attack data.
    - **Vulnerable Apps:** Clusters the assets by the similar installed vulnerable applications. The larger tiles indicate a greater threat as a result of installed vulnerable applications on the assets.
3. Hover over the tile to display a summary of the event data.
4. Double-click a cluster to view more detail, and click the tabs to view more information.

For more information, please see "BeyondInsight Clarity Analytics" on page 122.

Analyze Cluster Grids

Some key tips to keep in mind when analyzing threat conditions in your Clarity results data:

- Sort clusters by ordering attributes, such as **Vulnerable Apps**, **Attacks**, or **Risk**.
- Potential outliers could be clusters with a small number of members and greater ordering attributes.
- For outliers, review the pattern attributes to identify if the outliers have a unique or a different set of running applications, vulnerabilities, services, software, or ports.

To view the cluster grid, follow the steps.

1. From the menu, select **Cluster Analysis**.
2. Click the **Grid View** icon.
3. To review asset details for a cluster, double-click the row.

Alerts in BeyondInsight Clarity Analytics

There are two types of alerts:

- **Pattern:** Determined by correlation of all characteristics of an event.
- **Explicit:** Determined by selected specific characteristics.

Alert	Type	Description
a1	pattern	Maps all characteristics of an event into a single internal cluster using self-organizing maps clustering. Similar event characteristics lead to the same cluster. Thus, clusters with high share of mapped events represent typical behavior, while clusters with small number of events indicate outliers. Each user, host, or asset's characteristics are tracked independently with independent sets of clusters. ***Note:*** *Clusters are hidden and are used only for analysis. They do not behave the same as asset clusters.* Used characteristics: • Endpoint Privilege Management events, per user: **EventType**, **Exercised privilege**, **Path**, **Asset**, **Launch weekday and time** • Privilege Management for Unix & Linux events, per RunHost: **RunCommand**, **RunCWD**, **PBLUUser**, **Policy Server**, **SubmitHost**, **FinishStatus**, **Launch weekday and time**, **Accept**, **RiskLevel** • Vulnerability events, per Asset: Vulnerability type, Risk • Attack events, per Asset: Attack type, Category
a2	explicit	Untrusted Application Default value: 0.33 • If the application is unsigned, then value = value + 0.33 • If application has no version information, then value = value + 0.33
a5	explicit	Event Timing Event time within working hours and weekday Default value: 0.33 • If EventTime < WorkingHoursStart or EventTime > WorkingHoursEnd, then value = value + 0.33 • If EventDay is in WorkingWeekDaysMask, then value = value + 0.33
a6	explicit	Untrusted User Default value: 0.33 • If user is local (not domain) user, then value = value + 0.33 • If user is administrator, then value = value + 0.33
a7	explicit	First App Launch The alert is flagged when a user launches an application they have never launched before.

Alert	Type	Description
a8	explicit	First request for given managed account and system (Password Safe). The alert is flagged when a user request password for account and system have never requested before.
a9	explicit	Unusual password releases (Password Safe) The alert is flagged when a user does not retrieve the password for approved request or the password is retrieved more than once.
a10	explicit	Concurrent password requests (Password Safe). The alert is flagged when a user tries to acquire more than one password at a time.

Configure a Claims-Aware Website to Authenticate against SAML

You can configure a claims-aware website to bypass the current BeyondInsight login page and authenticate against any configured Federated Service that uses SAML to issue claims.

The claims-aware website is configured to redirect to a defined Federation Service through the **web.config**. Upon receiving the required set of claims, the user is redirected to the existing BeyondInsight website. At that point, it is determined if the user has the appropriate group membership to log in, given the claims associated with them.

If users attempting to access BeyondInsight have group claims matching a group defined in BeyondInsight, and the group has the **Full Control** permission to the **Management Console Access** feature, the user bypasses the BeyondInsight login screen. If the user is new to BeyondInsight, they are created in the system using the same claims information. The user is also added to all groups they are not already a member of that match in BeyondInsight, and as defined in the group claim information.

If the user is not a member of at least one group defined in BeyondInsight or that group does not have the **Full Control** permission to the **Management Console Access** feature, they are redirected to the BeyondInsight login page.

Create a BeyondInsight Group

Create a BeyondInsight group and ensure the group is assigned the **Full Control** permission to the **Management Console Access** feature.

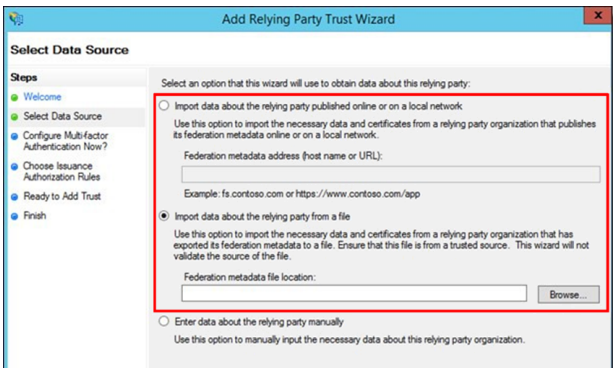
Add Relying Party Trust

After BeyondInsight is installed, metadata is created for the claims-aware website. Use the metadata to configure the relying party trust on the Federation Services instance.

The metadata is located in the following directory:

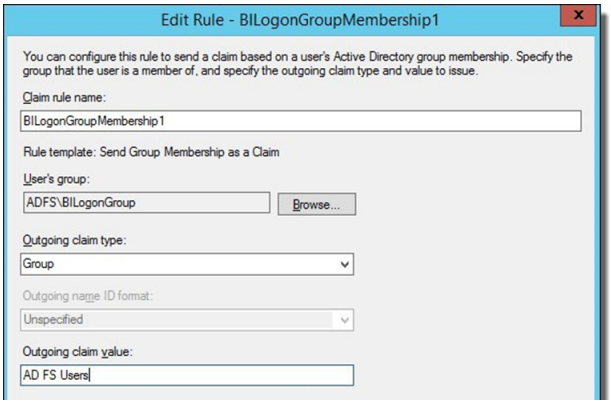
<Install path>\eEye Digital Security\Retina CS\WebSiteClaimsAware\FederationMetadata\2007-06

When selecting a **Data Source** in the **Add Relying Party Trust** Wizard, select the **FederationMetadata.xml** generated during the install.



Set Up Claim Rules

> ***Note:*** *Claims rules can be defined in a number of different ways. The example provided is simply one way of pushing claims to BeyondInsight. As long as the claims rules are configured to include at least one claim of outgoing type* ***Group*** *(with* ***Group*** *claim matching exactly what is in BeyondInsight) and a single outgoing claim of type* ***Name****, then BeyondInsight has enough information to potentially grant access to the site to the user.*



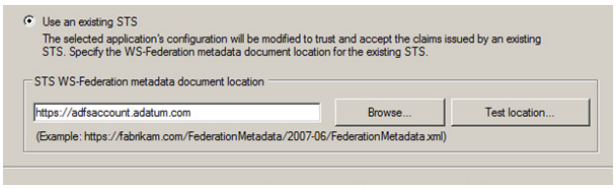
Supported Federation Service Claim Types

Outgoing Claim Type	Outgoing Claim Type	Mapping to BeyondInsight User Detail
http://schemas.xmlsoap.org/claims/Group	Required	Group membership
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Required	User name
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Optional	Surname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Optional	First name
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Optional	Email address

Claims-Aware SAML

The following procedure demonstrates how to set up a claims-aware website using the Windows Identity Foundation (WIF) SDK.

1. Start the **Windows Identity Foundation Federation Utility**.
2. On the **Welcome** page, browse to and select the **web.config** file for **BeyondInsight Claims Aware** site. The application URI automatically populates.
3. Click **Next**.
4. Select **Using an existing STS**.
5. Enter **Root URL of Claims Issuer** or **STS**.
6. Select **Test location**. **FederationMetadata.xml** is downloaded.
7. Click **Next**.
8. Select a STS signing certificate option, and then click **Next**.
9. Select an encryption option, and then click **Next**.



10. Select the appropriate claims, and then click **Next**.
11. Review the settings on the **Summary** page, and then click **Finish**.

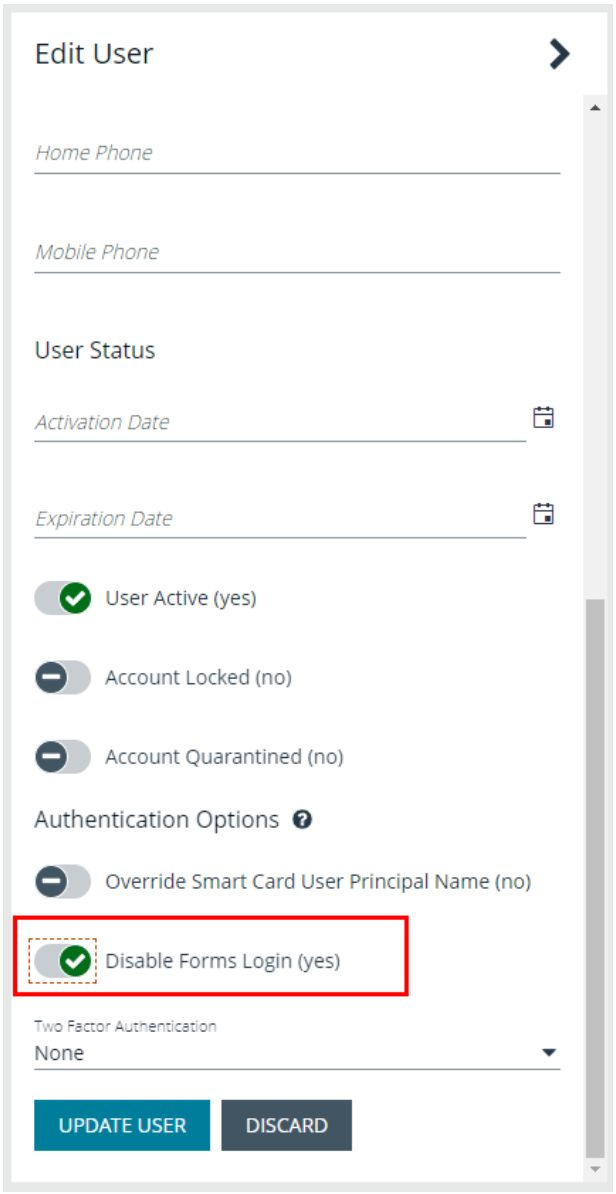
Disable Forms Login

In environments where SAML, smart card, or claims-aware is configured, we recommend enabling the **Disable Forms Login** authentication option to disallow users from using the standard login form in BeyondInsight.

To disable forms login for existing users, enable this option directly on a user account as follows:

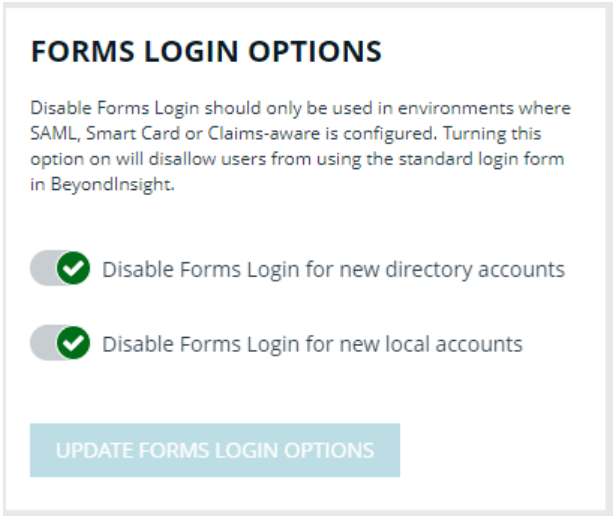
1. Click the vertical ellipsis for the user account, and then click **Edit User Details**.
2. Under **Authentication Options**, toggle **Disable Forms Login** to enable the option.

> ***Note:*** *Please contact support for assistance if you need to bulk-apply this setting to existing accounts.*



To configure login forms to automatically be disabled for newly created users:

1. Navigate to **Configuration > Authentication Management > Authentication Options**.
2. Under **Forms Login Options**, enable one or both options as applicable:
    - **Disable Forms Login for new directory accounts**
    - **Disable Forms Login for new local accounts**



Use Endpoint Privilege Management Features in BeyondInsight

When an Endpoint Privilege Management license is detected in BeyondInsight, you can view Endpoint Privilege Management events, file integrity monitoring events, and session details for monitored systems, from the BeyondInsight console. You can also view and deploy Endpoint Privilege Management policies, and view Endpoint Privilege Management agents.

If the Endpoint Privilege Management Web Policy Editor (WPE) is installed and configured you can view the details for each policy, unlock policies, edit policies, and delete policies.

If Endpoint Privilege Management Reporting is installed and configured, you can view dashboards and reports which may assist you with managing and auditing Endpoint Privilege Management activity in your environment.

The following sections provide details on using each of the above mentioned Endpoint Privilege Management features from the BeyondInsight console.

Manage Endpoint Privilege Management Events

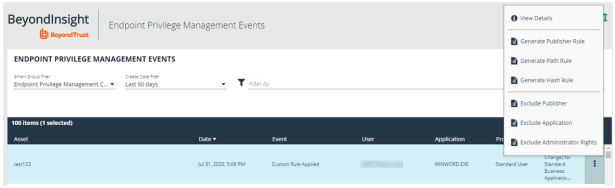
You can view Endpoint Privilege Management events on the **Endpoint Privilege Management Events** page.

Note: *This feature is available only when an Endpoint Privilege Management license is detected.*

View Events

You can view and download all events for monitored systems and you can select an event to view more details about that specific event.

1. From the left menu in the BeyondInsight Console, click **Endpoint Privilege Management**.
2. By default, displayed events are filtered by the **Discovery Scanners** Smart Group. Select a Smart Group from the **Smart Group filter** to view events for that Smart Group.
3. To further filter the displayed events, use the **Create Date filter**, or **Filter by** criteria.
4. For additional details about an event, click the vertical ellipsis for the event, and then select **View Details**.



5. A window opens displaying details related to Endpoint Privilege Management, the rule, and the application.
6. Click the **Download All** button above the grid to download the events to a CSV file.

Note: *Depending on the configuration of your grid and selected columns, not all event details may be visible. To configure display preferences, and see other options for the grid display, please see "Change and Set the Console Display Preferences" on page 16.*

Create Exclusion or Generate Rule from Event

To create an exclusion or generate a rule from an event:

1. Click the vertical ellipsis for the event.
2. Select the appropriate exclusion or rule type to generate.

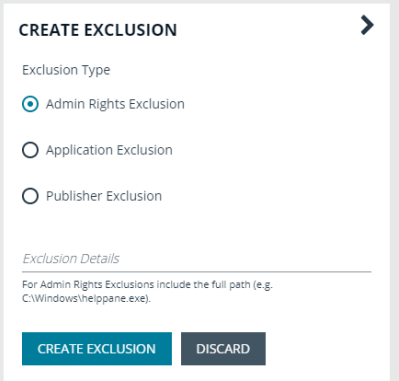
Note: *Exclusions can also be created from the **Exclusions** page. For more information, please see "Exclude Endpoint Privilege Management Events" on page 139.*

Exclude Endpoint Privilege Management Events

You can create exclusions to prevent recording unnecessary endpoint events. You can create and manage exclusions for Endpoint Privilege Management on the **Endpoint Privilege Management Exclusions** page.

Create an Endpoint Privilege Management Exclusion

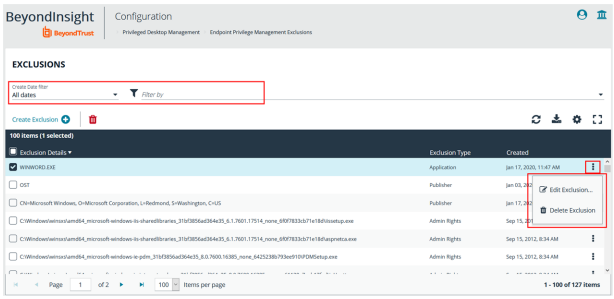
1. In the BeyondInsight Console, navigate to **Configuration > Privileged Desktop Management > Endpoint Privilege Management Exclusions**.
2. Click **Create Exclusion +** above the grid.
3. Select the **Exclusion Type**.
4. Enter the **Exclusion Details**.
5. Click **Create Exclusion**.



Tip: *Exclusions can also be created from selected events on the* ***Events*** *page. For more information, please see* *"Manage Endpoint Privilege Management Events" on page 138*.

Manage Exclusions

1. Use the filters above the grid to filter the list of exclusions by the date they were created, as well as the exclusion details and type of exclusion.
2. To edit or delete an exclusion, click the vertical ellipsis for the exclusion, and then select **Edit Exclusion** or **Delete Exclusion**.



To configure display preferences and see other options for the list display, please see *"Change and Set the Console Display Preferences" on page 16*.

Manage Endpoint Privilege Management Policies

Using BeyondInsight you can deploy Endpoint Privilege Management polices to assets and policy users. From the **Endpoint Privilege Management Polices** page, you can view a list of available Endpoint Privilege Management policies, and in single-tenant environments only, you can manage the global priority for the policies. You can also delete policies if you have sufficient permissions.

Note: *Endpoint Privilege Management features are only available when an Endpoint Privilege Management license is detected.*

If the Endpoint Privilege Management Web Policy Editor (WPE) is installed in your BeyondInsight instance, and your account has sufficient permissions, you can view the details for each policy, unlock policies, edit policies (which also locks the policy), and delete policies.

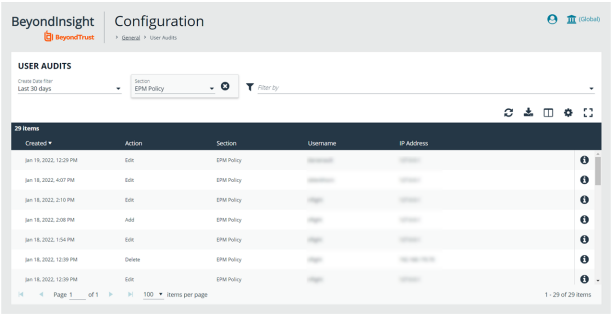
Note: *The WPE is not installed out of the box with BeyondInsight. Please contact your BeyondTrust representative for assistance with installing the WPE and its associated WPE service in your BeyondInsight environment.*

View Endpoint Privilege Management Policies

1. From the left menu in BeyondInsight, select **Policies** under **Endpoint Privilege Management**.
2. To filter the list of displayed policies, select the desired criteria from the **Filter by** list above the grid. Available filter options are:
    - Policy Name
    - Locked
    - Locked By
    - Policy Version
    - Policy Workgroup
    - Powered by

Note: *If you select **Filter by > Locked**, you can then select **Locked** or **Unlocked** as the filter criteria. If a policy is locked, this indicates that a user currently has it locked by a policy editor. The ability to lock, unlock, and edit policies within BeyondInsight is planned for a future release. If the WPE is installed in your BeyondInsight instance, and you have sufficient permissions, you can unlock a policy that is locked by another user, and then lock the policy so you can edit it.*

Tip: *You can see who added, modified, or deleted an Endpoint Privilege Management policy from the **Configuration > General > User Audits** page in BeyondInsight. Click the **i** button for a specific activity to view its details .*

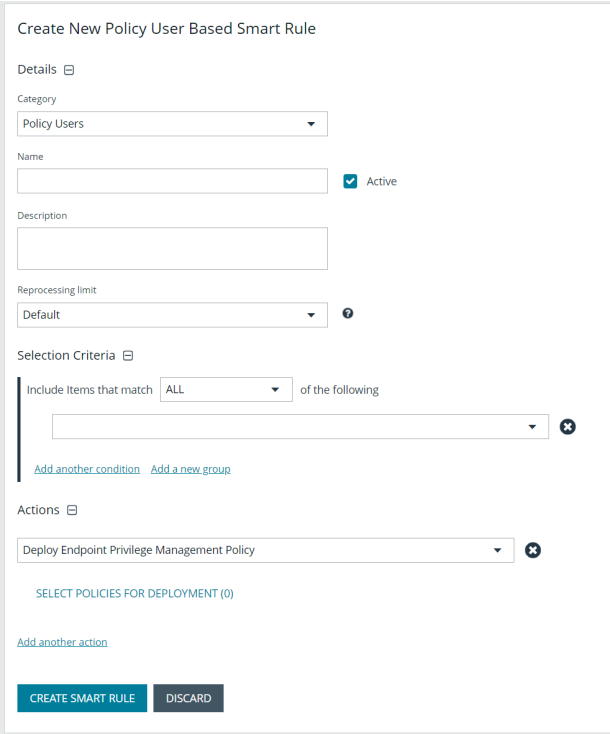


For more information on using the Endpoint Privilege Management Web Policy Editor, please see:

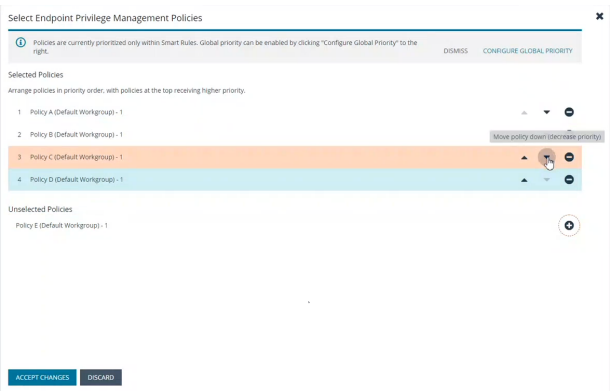
- *"Overview of Endpoint Privilege Management Web Policy Editor" on page 144*
- *"Create, View, and Edit Endpoint Privilege Management Policies" on page 149*

Deploy Endpoint Privilege Management Policies to Assets and Policy Users Using a Smart Rule

1. From the **Smart Rules** page in BeyondInsight, select **Asset** or **Policy User** from the **Smart Rule type Filter** dropdown, and then click **Create Smart Rule**.
2. Under **Actions**, select **Deploy Endpoint Privilege Management Policy** from the dropdown.
3. Click **Select Policies for Deployment**.

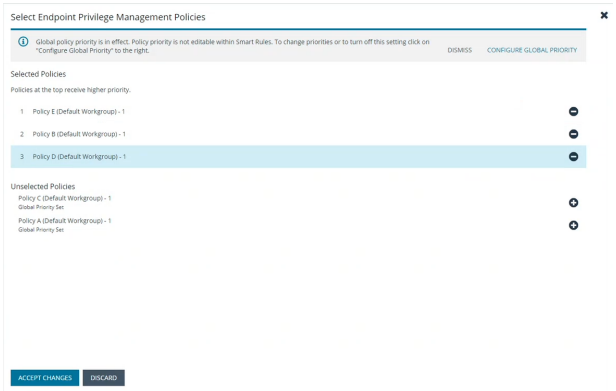


4. Select the policies using the plus sign next to the policy and set their priorities using the arrows. Click **Accept Changes**.



***Note:** The ability to set policy priorities within a Smart Rule is available only when **Use Global Priority** is not enabled, as indicated in the banner at the top of the page. Click **Dismiss** in the banner to continue setting priorities within the Smart Rule or click **Configure Global Priority** to enable that feature and set global policy priorities.*

Note: *When* ***Use Global Priority*** *is enabled, you do not have the ability to set the priority on a policy within the Smart Rule, as indicated in the banner at the top of the page. Click* ***Configure Global Priority*** *in the banner to disable that feature if you wish to set policy priorities within the Smart Rule.*



Note: *We recommend setting policy priority using the global policy priority feature over setting policy priority within a Smart Rule. For more information on managing global priority for policies, please see,* *"Manage Global Priority for Endpoint Privilege Management Policies" on page 142*.

For more information on working with Smart Rules to organize assets, please see *"Use Smart Rules to Organize Assets" on page 66*.

Manage Global Priority for Endpoint Privilege Management Policies

If multiple Smart Rules contain the same asset and have different policy priorities set within each of those Smart Rules, the Endpoint Privilege Management agent does not know which policy has the top priority on that asset. In this case, a different policy can take precedence each time the agent processes the Smart Rules. To prevent this, we recommend setting a global priority for your polices. With global policy priority enabled, BeyondInsight processes all policy-configured Smart Rules and serves all policies across all applicable Smart Rules to the Endpoint Privilege Management agent as per the defined global priority order.

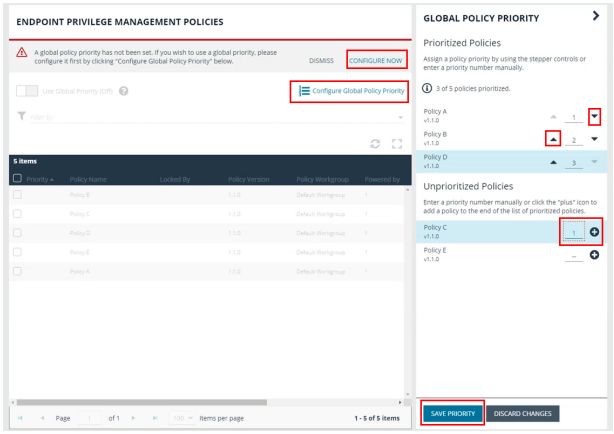
Note: *The global policy priority feature is enabled by default on new installations of BeyondInsight 21.1 or later. It is not enabled by default when upgrading BeyondInsight versions prior to 21.1 to the 21.1 release or later releases.*

Note: *The global policy priority feature is supported only in single-tenant BeyondInsight installations. This feature is disabled in multi-organization environments.*

Enable global policy priority as follows.

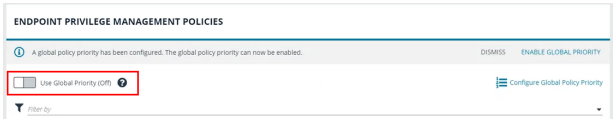
1. From the left menu in BeyondInsight, select **Policies** under **Endpoint Privilege Management**.

2. Click **Configure Global Priority Policy**, or if this is your first time using the global policy priority feature, click **Configure Now** in the banner that displays at the top of the page.
3. Select the policies using the plus sign next to the policy and set their priorities using the arrows. Alternatively, you can manually specify the priority number in the box for the policy, and then click the plus sign.

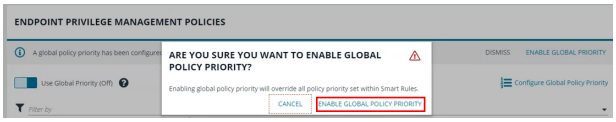


> ***Note:*** *All policies must be prioritized in order to enable the* ***Use Global Priority*** *option. Also, any policies added to BeyondInsight after global policy priority is enabled, are not available for assignment within Smart Rules until a priority has been explicitly set for them here.*

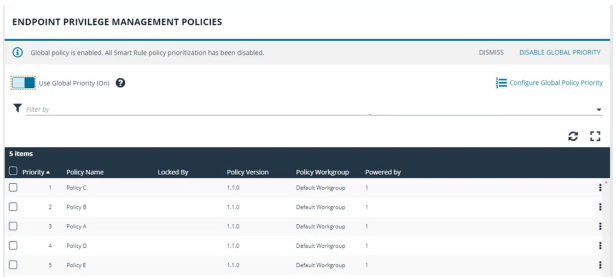
4. Click **Save Priority**.
5. The banner at the top of the page now indicates a global policy priority has been configured. Click the toggle to enable the **Use Global Priority** option.



6. A confirmation message displays. Click **Enable Global Policy Priority** in the message box.



7. The banner at the top of the page now indicates global policy is enabled and Smart Rule prioritization is disabled, and the policies display in the grid with their assigned priority.



Overview of Endpoint Privilege Management Web Policy Editor

The Endpoint Privilege Management Web Policy Editor (WPE), allows you to view, unlock, edit, and lock existing Endpoint Privilege Management policies, as well as create new policies directly from the BeyondInsight console, eliminating the need to use a standalone policy editor. Users with read-only permissions for the **Endpoint Privilege Management** feature can view policy information, while those with read/write permissions can create, view, unlock, edit, lock, and delete policies.

Note: *Only policies powered by Defendpoint can be viewed, unlocked, edited, and locked. Policies powered by PowerBroker can only be deleted.*

Policy Editor Components

Workstyles

Workstyles are used to assign Application Rules for a specific user, or group of users.

Note: *The WPE in BeyondInsight supports integration with Azure Active Directory (AD). Filters can be used within Workstyles to query Azure AD groups and users. Only one Azure AD tenant per organization is supported. For this integration to work, you must create an Azure AD directory credential in BeyondInsight.*

Application Groups

Application Groups are used by Workstyles to group applications together to apply certain Privilege Management behavior.

Content Groups

Content groups are used by Workstyles to group content together to apply certain Privilege Management behavior.

Messages

Messages are used by Workstyles to provide information to the end user when Privilege Management has applied certain behavior that you've defined and need to notify the end user.

Utilities

The WPE provides some useful tools to help with managing policies, including an import policy tool and a license management tool.

For more information on creating an Azure AD directory credential in BeyondInsight, please see "Create and Edit Directory Credentials" on page 19.

Use the QuickStart for Windows or Mac Template

To get started quickly using the WPE, create a new policy using either the **QuickStart For Windows** template, or the **Quickstart For Mac** template.

The QuickStart templates for Windows and Mac policies contain Workstyles, Application Groups, Messages, and Custom Tokens configured with Privilege Management and Application Control. The QuickStart policy is designed from BeyondTrust's experiences of implementing the solution across thousands of customers, and is intended to balance security with user freedom. As every environment is different, we recommend you thoroughly test this configuration to ensure it complies with the requirements of your organization.

Customize the QuickStart Policy

Before deploying the QuickStart policy to your users, you must make some company-specific customizations to the standard template.

At a minimum you must:

- Configure the users or groups that can authorize requests that trigger messages.
- Assign users and groups to the high, medium, and low flexibility Workstyles.
- Populate the **Block - Blocked Apps** Application Group with any applications that you want to block for all users.
- Set your shared key so you can generate a Privilege Management Response code.

QuickStart Template Summary

This section provides information about the properties for the Windows and Mac QuickStart templates, including the Workstyles and Application Groups that comprise the template.

WorkStyles

All Users

This Workstyle contains a set of default rules that apply to all standard users regardless of the level of flexibility they need.

The **All Users** Workstyle contains rules to:

- Block any applications in the **Block - Blocked Apps** group.
- Allow Privilege Management Support tools.
- Allow standard Windows and Mac functions, business applications, and applications installed through trusted deployment tools to run with admin rights.
- Allow approved standard user applications to run passively.

High Flexibility

This Workstyle is designed for users that require a lot of flexibility, such as developers.

The **High Flexibility** Workstyle contains rules to:

- Allow applications that are in the **Add Admin – High Flexibility** group to run with admin rights.
- Allow known business applications and operating system functions to run.

- Allow users to run signed applications with admin rights.
- Allow users to run unknown applications with admin rights once they confirm that the application should be elevated.
- Allow unknown business application and operating system functions to run on demand.

Medium Flexibility

This Workstyle is designed for users that require some flexibility, such as sales engineers.

- Allow applications that are in the **Add Admin – Medium Flexibility** group to run with admin rights.
- Allow known business applications and operating system functions to run.
- Allow users to run signed applications with admin rights once they confirm that the application should be elevated.
- Prompt users to provide a reason before they can run unknown applications with admin rights.
- Allow unknown business application and operating system functions to run on demand.
- Restricted OS functions that require admin rights are prevented and require support interaction.

Low Flexibility

This Workstyle is designed for users that don't require much flexibility, such as helpdesk operators.

- Allow applications that are in the **Add Admin – Low Flexibility** group to run with admin rights.
- Prompt users to contact support if a trusted or untrusted application requests admin rights.
- Prompt users to contact support if an unknown application tries to run.
- Allow known approved business applications and operating system functions to run (Windows only).

Administrators

This Workstyle provides visibility on the Administrator accounts in use in the environment.

The Administrators Workstyle contains general rules to:

- Capture user and host information.
- Block users from modifying local privileged group memberships.

Application Groups

The Application Groups that are prefixed with **(Default)** or **(Recommended)** are hidden by default and do not need to be altered. Click the **Show Hidden** button above the grid to see all Application Groups.

- **Add Admin – All Users (Business Apps)**: Contains applications that are approved for elevation for all users, regardless of their flexibility level.
- **Add Admin – All Users (Windows Functions)**: Contains operating system functions that are approved for elevation for all users.
- **Add Admin – High Flexibility**: Contains the applications that require admin rights that should only be provided to the high flexibility users.
- **Add Admin – Low Flexibility**: Contains the applications that require admin rights that should only be provided to the low flexibility users.

- **Add Admin – Medium Flexibility**: Contains the applications that require admin rights that should only be provided to the medium flexibility users.
- **Block - Blocked Apps**: This group contains applications that are blocked for all users.
- **Passive - Allowed Functions & Apps**: Contains trusted applications, tasks and scripts that should execute as a standard user.
- **Passive - High Business Apps**: Contains trusted applications, that should execute as a high flexibility administrative user.
- **Passive - Low Business Apps**: Contains trusted applications, that should execute as a low flexibility administrative user.
- **Passive - Medium Business Apps**: Contains trusted applications, that should execute as medium flexibility administrative user.
- **(Default) Any Application**: Contains all application types and is used as a catch-all for unknown applications.
- **(Default) Any Trusted & Signed UAC Prompt**: Contains signed (trusted ownership) application types that request admin rights.
- **(Default) Any UAC Prompt**: Contains application types that request admin rights.
- **(Default) Privilege Management Tools**: This group is used to provide access to a BeyondTrust executable that collects Privilege Management for Windows troubleshooting information.
- **(Default) Child Processes of TraceConfig.exe**: Contains application types that request to run child processes of **TraceConfig.exe**.
- **(Default) Signed UAC Prompt**: Contains signed (trusted ownership) application types that request admin rights.
- **(Default) Software Deployment Tool Installs**: Contains applications that can be installed by deployment tools such as System Center Configuration Manager (SCCM).
- **(Recommended) Restricted Functions**: This group contains OS applications and consoles that are used for system administration and trigger UAC when they are executed.
- **(Recommended) Restricted Functions (On Demand)**: This group contains OS applications and consoles that are used for system administration.
- **(Default) Trusted Parent Processes**: Contains trusted applications that request to run parent processes.

Messages

The following messages are created as part of the QuickStart policy and are used by some of the Application Rules:

- **Allow Message (Authentication)**: Asks the user to provide a reason and enter their password before the application runs with admin rights.
- **Allow Message (Select Reason)**: Asks the user to select a reason from a dropdown menu before the application runs with admin rights.
- **Allow Message (Support Desk)**: Presents the user with a challenge code and asks them to obtain authorization from the support desk. Support can either provide a response code or a designated, authorized user can enter their login details to approve the request.
- **Allow Message (Yes / No)**: Asks the user to confirm that they want to proceed to run an application with admin rights.
- **Block Message**: Warns the user that an application has been blocked.
- **Block Notification**: Notifies the user that an application has been blocked and submitted for analysis.
- **Notification (Trusted)**: Notifies the user that an application has been trusted.

Use the Server Role Template

The Server Roles policy contains Workstyles, Application Groups, and Content Groups to manage different server roles such as DHCP, DNS, IIS, and print servers.

Server Roles Template Summary

This template policy contains the following elements.

WorkStyles

- Server Role - Active Directory - Template
- Server Role - DHCP - Template
- Server Role - DNS - Template
- Server Role - File Services - Template
- Server Role - Hyper V - Template
- Server Role - IIS - Template
- Server Role - Print Services - Template
- Server Role - Windows General - Template

Application Groups

- Server Role - Active Directory - Server 2008R2
- Server Role - DHCP - Server 2008R2
- Server Role - DNS - Server 2008R2
- Server Role - File Services - Server 2008R2
- Server Role - General Tasks - Server 2008R2
- Server Role - Hyper V - Server 2008R2
- Server Role - IIS - Server 2008R2
- Server Role - Print Services - Server 2008R2

Content Groups

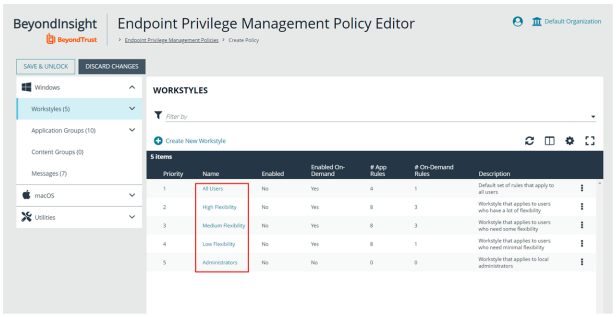
- AD Management
- Host Management
- IIS Management
- Printer Management
- Public Desktop

Create, View, and Edit Endpoint Privilege Management Policies

Create a Policy

1. From the left menu, select **Policies** under **Endpoint Privilege Management**.
2. Click **Create Policy +** above the grid.
3. Enter a name for the policy and select a Workgroup from the list.
4. Click **Create Policy**.
5. Select one of the following:
    - **QuickStart for Windows**: A preconfigured template with Workstyles, Application Groups, messages, and Custom Tokens already configured.
    - **QuickStart for Mac**: A preconfigured template with Workstyles, Application Groups, and messages already configured.
    - **Server Roles**: The Server Roles policy contains Workstyles, Application Groups, and Content Groups to manage different server roles such as DHCP, DNS, IIS, and print servers.
    - **Blank**: Select to configure a policy from scratch. There are no preconfigured settings in this template.

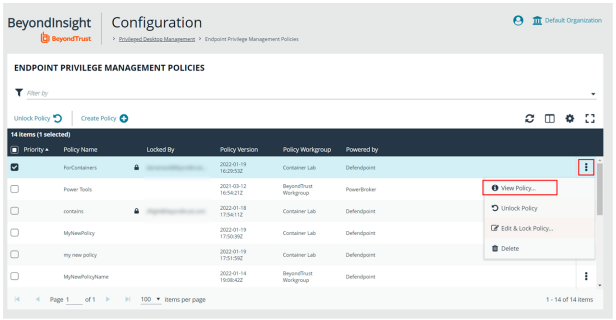
The Policy Editor opens to the **Workstyles** page. At this point you must configure the Workstyle, Application Groups, Application Rules and other policy configuration as required for your organization. The templates and their configuration components are described in more detail in the below sections.



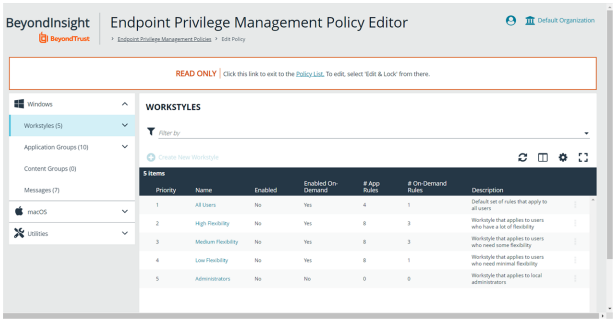
> ***Tip:*** *For quick access to the **Workstyles Summary** page, click the hyperlink for the Workstyle name.*

View a Policy

1. From the left menu, select **Policies** under **Endpoint Privilege Management**.
2. Click the vertical ellipsis for the policy you wish to view, and then select **View Policy**.



3. The Policy Editor opens in **Read Only** mode.



> ***Tip:*** *If you wish to edit the policy, click the* ***Policy List*** *link at the top of the page to go back to the main Policies page where you can select the policy to edit and lock it.*

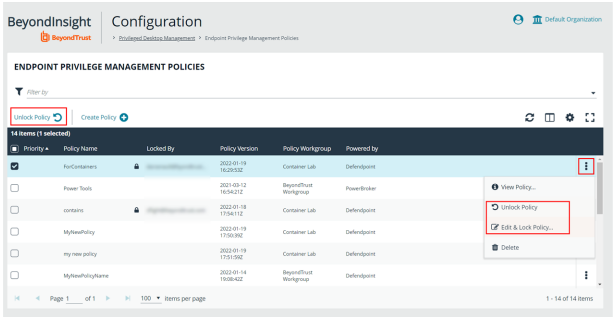
4. Use the options in the left navigation to view the following policy information:
    - For Windows policies:
        - Workstyles
        - Application Groups
        - Content Groups
        - Messages
    - For macOS policies:
        - Workstyles
        - Application Groups
        - Messages
    - Utilities:
        - Licenses
        - Import Policy
        - Template Policies

> ***Note:*** *You can also filter the contents displayed in each grid using the* ***Filter By*** *list above the grid.*

Edit a Policy

When you edit a policy, the policy is locked. Other policy administrators cannot access the policy to change the properties when the status is **Locked**. The policy is unlocked when changes are saved or discarded.

1. From the left menu, select **Policies** under **Endpoint Privilege Management**.
2. Click the vertical ellipsis for the policy you wish to edit.
3. If a policy is locked, the **Unlock Policy** action displays in the menu. Click to unlock the policy.
4. Select **Edit and Lock Policy**.



5. In the Policy Editor, go to the policy property you want to change and make your edits.
6. Click **Save** to save a draft of the policy. Clicking **Save** allows you to keep the Policy Editor open to continue changing the policy.
7. Once the policy is updated, click **Save and Unlock** to save a new revision of the policy, or **Discard Changes** to remove changes.
8. If **Discard Changes** is selected, you are prompted to **Continue Editing** or **Discard Changes**.
9. (Optional). On the **Save and Unlock** dialog box, you can enter **Annotation notes** about the policy changes. You can also check the **Auto Assign Policy to Groups?** box, to automatically assign the latest revision to groups the policy is currently assigned to.

Note: *The **Auto Assign Policy to Groups?** option is only available when the groups are currently on the latest policy. If they are on an older version, only the **Annotation notes** option is displayed.*

Tip: *You can export a policy and import a policy to overwrite the existing one while viewing a policy in read-only mode and while editing a policy in read/write mode. Select **Utilities > Import Policy** from the left navigation, click **Overwrite Policy**, and then click **Export Existing Policy** to export. Drop a file in the box to upload a new policy and then click **Upload File**.*

For more information on editing the various components of a policy, including Workstyles, Application Rules, and Application Groups, please see "Use the Policy Editor to Manage Policy" in the Privileged Management Cloud Administration Guide at https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pmc/pm-cloud-admin.pdf.

Create and View Smart Rules for Endpoint Privilege Management Policy Users

You can manage user-based policies for Endpoint Privilege Management users with Smart Rules, and view the policy users with the assigned policies.

> ***Note:*** *This feature is only available when an Endpoint Privilege Management license is detected.*

To deploy policies to users, you need to first create rules and policies in the Endpoint Privilege Management **Policy Editor**, and then you can log in to BeyondInsight to create applicable Smart Rules.

Create a Smart Rule

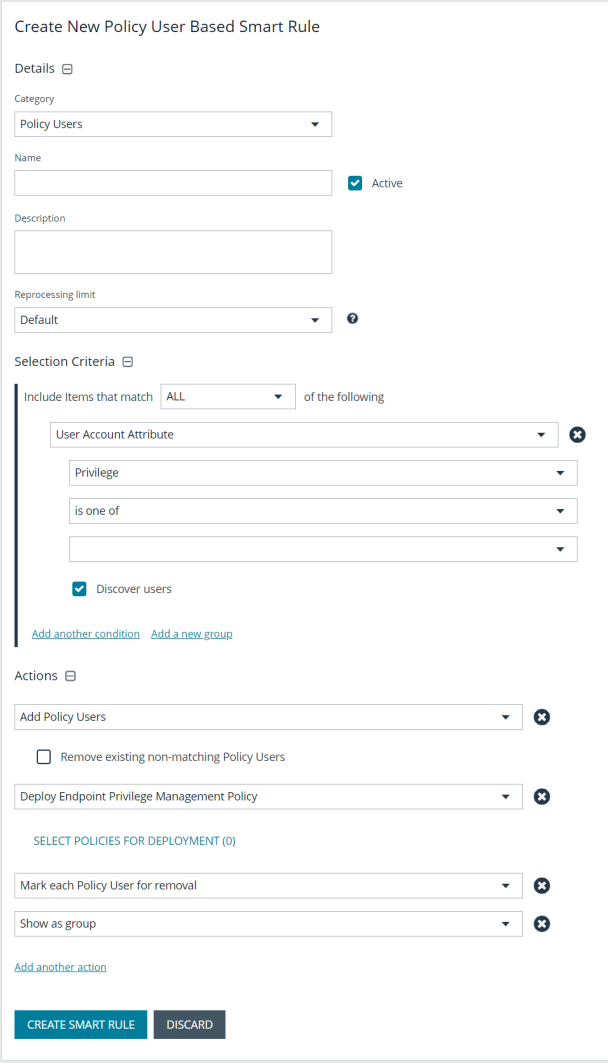
When a policy is deployed using a policy user-based Smart Rule, only the policy rules set in the **User Configuration Rule Management** section of the policy are processed by Endpoint Privilege Management clients that receive the policy. Policy deployment is controlled by the specifications in the Smart Rule.

A policy user-based Smart Rule can deploy policies to Windows Active Directory domain users and local users that are not part of a domain.

Create Policy User-Based Smart Rule

1. From the **Home** page in the BeyondInsight Console, click **Configuration**.
2. In the **General** pane, click **Smart Rules**.
3. Select **Policy User** from the dropdown for the **Smart Rule type filter**.
4. Click **Create Smart Rule +**. A new window opens.

5. Select **Policy Users** for the category.
6. Provide a **Name** and **Description** for the policy.
7. Select a **Reprocessing Limit** from the dropdown to set how often the Smart Rule runs.
8. In the **Selection Criteria** section, select and add your desired filters to add the Endpoint Privilege Management accounts.
    - To onboard local policy users, use the **User Account Attribute** filter after discovering users via scans. Then use their privilege attribute or their name for the **Selection Criteria**.
9. In the **Actions** section, select and add the following actions:
    - **Add Policy Users:** Adds users to BeyondInsight.
    - **Deploy Endpoint Privilege Management Policy:** Deploys policies to the user accounts.
    - **Mark each policy user for removal:** Deletes the user accounts from the Smart Group.
    - **Show as Group:** Displays the Smart Rule as a Smart Group on the **Policies** page.
10. Click **Create Smart Rule**.



View Policy Users

After the Smart Rule processes, you can view policy users on the **Policy Users** page. This page shows the policies assigned and applied.

1. To view the page, click **Policy Users** on the **Home** page, or on the menu under **Endpoint Privilege Management**.
2. Displayed policy users are filtered by the selected **Smart Group filter**.
3. Displayed policy users can also be filtered by other criteria.
4. Displayed policy users can be downloaded, and the grid view can be modified.

Note: *Depending the configuration of your grid and selected columns, not all policy user details may be visible. To configure display preferences, and see other options for the grid display, please see* *"Change and Set the Console Display Preferences" on page 16**.*

5. To remove a user from a policy, click the vertical ellipsis at the right end of the line and select **Delete Policy User**.

View Endpoint Privilege Management Agents

Agents are assets with Endpoint Privilege Management installed. You can view and download Endpoint Privilege Management agents on the **Endpoint Privilege Management Agents** page.

Note: *This feature is only available when an Endpoint Privilege Management license is detected.*

View Agents

1. In the BeyondInsight Console, click the **MENU**.
2. Under **Endpoint Privilege Management**, click **Agents**.

Tip: *You can also access the **Endpoint Privilege Management Agents** page from the **Assets** page by clicking the **Endpoint Privilege Management** link at the top of the page.*

3. By default, displayed agents are filtered by the **Discovery Scanners** Smart Group. Select a Smart Group from the **Smart Group filter** to view agents for that Smart Group.
4. To further filter the displayed agents, use the **Last Updated filter**, or **Filter by** criteria.
5. Click the **Download All** button above the grid to download the list of agents to a CSV file.

Note: *Depending on the configuration of your grid and selected columns, not all agent details may be visible. To configure display preferences, and see other options for the grid display, please see "Change and Set the Console Display Preferences" on page 16.*

View Endpoint Privilege Management File Integrity Monitoring

You can view file integrity monitoring events using Endpoint Privilege Management.

Note: *This feature is only available when an Endpoint Privilege Management license is detected.*

View File Integrity Monitoring Events

File integrity monitoring captures events related to created, edited, or deleted items in folders, according to the created rules.

1. In the BeyondInsight Console, click the **MENU**.
2. Under **Endpoint Privilege Management**, click **File Integrity Monitoring**.
3. By default, displayed events are filtered by the **Discovery Scanners** Smart Group. Select a Smart Group from the **Smart Group filter** to view events for that Smart Group.
4. To further filter the displayed events, use the **Create Date filter**, or **Filter by** criteria.
5. Click the **Download All** button above the grid to download the events to a CSV file.

Note: Grid Configuration *is not available for this grid.*

Note: *Depending on the configuration of your grid and selected columns, not all file monitoring event details may be visible. To configure display preferences, and see other options for the grid display, please see* *"Change and Set the Console Display Preferences" on page 16*.

Monitor Endpoint Privilege Management Sessions

You can view session details and replay sessions using Endpoint Privilege Management.

> ***Note:*** *This feature is only available when an Endpoint Privilege Management license is detected.*

View Session Details

1. In the BeyondInsight Console, click the **MENU**.
2. Under **Endpoint Privilege Management**, click **Session Monitoring**.
3. By default, displayed sessions are filtered by the **Discovery Scanners** Smart Group. Select a Smart Group from the **Smart Group filter** to view sessions for that Smart Group.
4. To further filter the displayed sessions, use the **Filter by** criteria above the grid.
5. For additional details about a session, click the vertical ellipsis for the session, and then select **View Details**.
6. Click the **Download All** button above the grid to download the sessions to a CSV file.

> ***Note:*** *Depending on the configuration of your grid and selected columns, not all session details may be visible. To configure display preferences, and see other options for the grid display, please see* *"Change and Set the Console Display Preferences" on page 16**.*

Session Replay

1. Follow the steps above to select a session.
2. Click the vertical ellipsis for the session, and then select **View Session...** . **View Session...** is also available when viewing all session details.
3. A new page opens, showing some details of the session, a list of the **Events** and when they occurred (which can be searched), and a slideshow of the session.
4. Buttons under the slideshow control session playback. You can change the speed of session playback by selecting a different **Slideshow Delay**.
5. You can download an image of any session view by clicking the **Snapshot** button.

View Endpoint Privilege Management Reports

Endpoint Privilege Management Reporting includes a rich set of dashboards and reports designed to simplify the centralized management and auditing of Endpoint Privilege Management activity throughout the desktop and server estate.

> ***Note:*** *Endpoint Privilege Management Reporting is not installed out of the box with BeyondInsight. Please contact your BeyondTrust representative for assistance with installing the Endpoint Privilege Management Reporting feature in your BeyondInsight environment.*

A report is a dashboard or a table, and is a generic term used to describe any form of data displayed in Endpoint Privilege Management Reporting. You can click on links within reports to see the data at greater levels of granularity. These are referred to as *drilldowns*.

A dashboard is a report, which at the top level, presents you with a series of charts and summarized data. Some dashboards have sub-reports that are presented as charts or tabular data. All dashboards have a Microsoft Windows view to display events from Windows endpoints. Some dashboards and reports also have a macOS view.

The following sections describe each of the dashboards, and the reports and event data accessible from each view.

Navigate the Endpoint Privilege Management Reporting Interface

The Endpoint Privilege Management Reporting interface allows you to switch between dashboards and reports and to filter data as required. This section covers the Endpoint Privilege Management Reporting interface elements and how to export a specific report.

Navigation Panel

The side navigation panel takes you to each top-level dashboard and the reports in that dashboard. Reports that are post-fixed with **All** indicate the data is in tabular form.

Dashboard and Reports Panel

This is the area where dashboards and reports are displayed. A dashboard is a report with multiple charts covering a wide range of data. A report is a summary table or a page focused on a particular entity.

The graphical elements of a dashboard or report are interactive. You can click on a chart to view the data at an additional level of granularity.

Filter Panel

Each dashboard and report has a panel above its table, chart, or graph area that displays the applied filters and a **Filters** dropdown. When you select the **Filters** dropdown, a **Filters** box appears where you can select filters to filter data based on various event properties. The **Filters** box also provides a link to select **Advanced Filters**, allowing for more granular report data. The filters displayed in the box are unique and relevant to the specific dashboard and report.

For example, if you want to filter the **Summary** report to include only a specific Workstyle:

1. From the **Summary** dashboard, click the link to open the report to filter.
2. Click the **Filters** dropdown.
3. Click the **Advanced Filters** link.
4. Select the **Workstyle** you are interested in from the dropdown.
5. Click **Apply Filters**.
6. The report data for that specific Workstyle displays in the table.

The filter options match text on substrings; partial or complete words can match on a filter.

Certain filter options support comma-separated values so you can specify a list of filter values. For example, to restrict the results to three users, enter *user1,user2,user3* in the **User Name** field.

Note: *Multiple "!" strings are accepted. For example, "!L-CZC13127L30l,!L-CNU410DJJ7"*

Any text field supports wildcards, comma-separated values (CSV), and the Does Not Match(!) options:

Filtering Effect	Filter Panel Operator	Effect
List separator	Comma (,)	Value1,value2,value3
Wildcard	%	part% part%part2,part3%part4

Filtering Effect	Filter Panel Operator	Effect
Negation or "Not"	!	!value !value1,!value2

Note: *When filtering tabular reports such as the* ***Users*** *>* ***All*** *table, an applied filter is displayed at the top of the table. To remove a filter, click on the* ***x*** *next to the filter text.*

Export Reports

You can export reports to a CSV file by clicking the **Export to CSV** button in the filter panel above the report.

Exported data is based on the data currently displayed in the report.

Use Quick Filters and Advanced Filters

Use Quick Filters

Below are descriptions of commonly used quick filter options available from the **Filters** dropdown.

Name	Description
Platform	• **Windows** Filters by endpoints running a Windows operating system. • **OS X** Filters by endpoints running a Mac operating system.
Time Range	This is the time range in which the actions are audited. For example, you can filter by the number of elevated actions in the last 24 hours in the **Actions > Elevated** report. You can choose from: • **24 Hours** • **7 Days** • **30 Days** • **12 Months**
Time First Reported	This is the time range filtered by the date the application was first entered in the database. For example, you can filter on the new Windows applications by publisher that were first reported in the last 7 days in the **Discovery > By Publisher** report. You can choose from: • **24 Hours** • **7 Days** • **30 Days** • **6 Months** • **12 Months**
Time First Executed	This is the time range the application was first executed. For example, you can filter on the new Windows applications, by type, that were first executed in the last 30 days in the **Discovery > By Type** report. You can choose from: • **24 Hours** • **7 Days** • **30 Days** • **6 Months** • **12 Months**

Name	Description
Target Type	This filter allows you to filter by a type of target. For example, you can filter on the applications canceled in the time range in the **Actions > Canceled** report. You can choose from: • **All** • **Applications** • **Services** • **COM** • **Remote PowerShell** • **ActiveX** • **URL** • **Content**
Action	This filter allows you to filter by a type of action. For example, you can filter on the services elevated in the time range in the **Target Types > Services** report. You can choose from: • **All** • **Elevated** • **Blocked** • **Passive** • **Sandboxed** • **Custom** • **Drop admin rights** • **Enforce default rights** • **Canceled**

Name	Description
Application Type	This filter allows you to filter by application type. For example, you can filter by applications that are executables used in the time range in **Target Types > Applications**. You can choose from: • **All** • **Executable** • **Control panel applet** • **Management console snapin** • **Installer Package** • **Uninstaller** • **Windows Script** • **PowerShell Script** • **Batch File** • **Registry Settings** • **Windows store application** • **Bundle** • **Package** • **System Preference** • **Sudo Control** • **Script**
Event Category	This filter allows you to filter by the category of the event. For example, you can filter by process events only that occur in the time range in the **Events > All** report. You can choose from: • **All** • **Process Control** • **Content Control** • **DLL Control** • **URL** • **Privileged Account Management** • **Agent started** • **User logon** • **Services**

Name	Description
Elevate Method	Allows you to filter by the elevation method used. For example, in the **Discovery > Requiring Elevation** report, you can filter by new applications which were accessed using on-demand elevation within the time range. You can choose from: • **All** • **Admin account used** • **Auto-elevated** • **On-demand**
Path	Allows you to filter by the path. For example, to filter on applications that were launched from the System path. You can choose from: • **All** • **System** • **Program Files** • **User Profiles**
Source	The media source of the application. For example, was the application downloaded from the internet or is it from removable media? You can choose from: • **All** • **Downloaded from internet** • **Removable media** • **Any external source**
Challenge / Response	Allows you to filter by challenge/response events. For example, you can filter the application that required elevation on those applications launched following a completed challenge/response message. You can choose from: • **All** • **Only C/R**
Admin Rights	Allows you to filter by the admin rights token. You can choose from: • **All** • **Detected** • **Not Detected**

Name	Description
Authorization	Allows you to filter by authorization. You can choose from: • **All** • **Required** • **Not Required**
Ownership	Allows you to group by the type of owner. You can choose from: • **All** • **Trusted owner** • **Untrusted owner**
Rule Match Type	Allows you to filter on the type of matching. You can choose from: • **All** • **Matched on Parent** • **Direct Match**

Use Advanced Filters

Below are descriptions of commonly used filter options available from the **Advanced Filters** link in the **Filters** box.

Name	Description
Action	There are nine actions to choose from: • **Elevated** • **Blocked** • **Passive** • **Custom** • **Drop Admin Rights** • **Enforce Default Rights** • **Canceled** • **Sandboxed** • **Allowed**
Activity ID	Each Activity Type in Privilege Management has a unique ID. This is generated in the database as required. For example, if you are in the **Target Types** dashboard and drill down in the **Top 10 Activities** chart, the **Events > AllI** report opens. If you look in the top advanced filter you will see that the Activity ID is populated.

Name	Description
Admin Rights Required	There are three options to choose from: • **All** • **Detected** • **Not Detected** Allows you to filter if Admin Rights are required, not required, or both. For example, if you are in the **Discovery > All** report and set the side quick filter to **Admin Rights**, only applications that required admin rights are listed.
Agent Version	The version of the Privilege Management agent.
Application Desc	A text field that allows you to filter on the application name. For example, in the **Discovery** report you can filter by **paint** in the **Application Desc** field. This filters applications that contain the string **paint** in the description.
Application Group	A text field that allows you to filter by Application Group. You can obtain the Application Group from the Policy Editor. It is also available in some reports such as **Process Detail**, which is accessed from **Events All**.
Application Type	A text field that allows you to filter by application type. You can obtain the application type from the Policy Editor. It's also available in some reports such as **Process Detail**, which is accessed from **Events All**.
Auth Methods	The type of authentication method selected in the Policy Editor. Multiple values can be present and are comma separated. Possible values: **Identity Provider**, **Password**, **Challenge Response**, **Smart Card**, and **User Request**.
Auth User Name	The name of the user that authorized the message.
Browse Source URL	The source URL of the sandbox.
Browse Destination URL	The destination URL of the sandbox.
Chassis	The physical form of the endpoint. **Other** is a virtual machine.
Command Line	A text field that allows you to filter on the command line. It is also available in some reports such as **Process Detail** that is accessed from **Events > All**.
Context	This field is used by Reporting. You do not need to edit it.
Date Field to filter on	There are three options to choose from: • **Time Generated**: This is the time that the event was generated. One application can have multiple events. Each event has a **Time Generated** attribute. • **Time App First Discovered**: This is the time that the first event for a single application was entered into the database. This can be delayed if the user is working offline. • **Time App First Executed**: This is the first known execution time of events for that application.
Default UI Language	The default language of the endpoint.

Name	Description
Device Type	The type of device that the application file was stored on. You can select from: • **Any** • **Removeable Media** • **USB Drive** • **Fixed Drive** • **Network Drive** • **CDROM Drive** • **RAM Drive** • **eSATA Drive** • **Any Removable Drive or Media**
Distinct Application ID	This field is used by Reporting. You do not need to edit it.
Elevation Method	There are five options to choose from: • **Not Set** • **All** • **Admin account** • **Auto-elevated** • **On-demand** These allow you to filter events by the type of elevation used.
Event Number	This field is used by Reporting. You do not need to edit it. This number assigned to the event type.
External Source	There are four options to choose from: • **Not Set** • **Downloaded over the internet** • **Removeable media** • **Any external source** These allow you to filter by the type of external source that the application file came from.
File Name	You can filter by a partial file name string if required. For example, in the **Process Detail** report.
File Version	You can filter on the file version in the Advanced View of the **Process Detail** report.
GPO Name	You can filter on the Group Policy Object (GPO) name in some of the advanced reports such as **Process Detail**.
Host Name	This field allows you to filter by the name of the endpoint the event came from.
Idp Authentication user name	The credential provided when adding an Identity Provider authorization message in the Policy Editor.
BeyondTrust Zone Identifier	The BeyondTrust Zone Identifier. This tag persists, to allow you to filter on it even if the ADS tag applied by the browser is removed.
Ignore "Admin Required" Events	This field is used by Reporting. You do not need to edit it.

Name	Description
Just Discovery Events	This field is used by Reporting. You do not need to edit it.
Message Name	The name of the message that was used.
Message Type	The type of Message: • **Any** • **Prompt** • **Notification** • **None**
Number to Get	The number of rows to get from the database.
Operating System Type	The type of operating system: • **Server** • **Workstation**
Operating System	The operating system of the client machine.
Parent PID	The operating system process identifier of the parent process.
PID	The operating system process identifier.
Product Name	The product name of the application.
Product Version	The product version of the application.
Program Files Path	Sets the Program Files path used by the **Discovery > By Path** report.
Publisher	The publisher of the application.
Range End Time	The end time of the range being displayed.
Range Start Time	The start time of the range being displayed.
Request Type	The type of request: • **Blocked with reason** • **Canceled challenge**
Row Limit	The maximum number of rows to be retrieved from the database.
Rule Match Type	Rule Match Type: • **Any** • **Direct match** • **Matched on parent**
Sandbox	The sandboxed setting: • **Not Set** • **Any Sandbox** • **Not Sandboxed**
Rule Script Affected Rule	True when the Rule Script (Power Rule) changes one or more of the Default Privilege Management rules, otherwise false.
Rule Script File Name	The Rule Script (Power Rule) file name on disk if applicable.

Name	Description
Rule Script Name	The name of the assigned Rule Script (Power Rule).
Rule Script Output	The output of the Rule Script (Power Rule).
Rule Script Publisher	The publisher of the Rule Script (Power Rule).

Rule Script Result	The result of the Rule Script (Power Rule). This can be:
	
	`<None>`
	`Script ran successfully`
	`[Exception Message]`
	`Script timeout exceeded: <X> seconds`
	`Script execution canceled`
	`Set Rule Properties failed validation: <reason>`
	`Script execution skipped: Challenge Response Authenticated`
	`Script executed previously for the parent process: Matched as a child process so cached result applied`
	`Script execution skipped: <app type> not supported`
	`Script execution skipped: PRInterface module failed signature check`
	`Set RunAs Properties failed validation: <reason>`

Rule Script Status	The status of the Rule Script (Power Rule). This can be:
	
	`<None>`
	`Success`
	`Timeout`
	`Exception`
	`Skipped`
	`ValidationFailure`

Rule Script Version	The version of the assigned Rule Script (Power Rule).
Shell or Auto	Whether the process was launched using the shell **Run with Privilege Management** option or by normal means (opening an application): • **Any** • **Shell** • **Auto**
Source URL	The source URL (where the file was downloaded from).
System Path	Sets the system path used by the **Discovery > By Path** report.
Target Description	This field allows you to filter by the target description.

Name	Description
Target Type	The type of target that triggered the event: • **Any** • **Application** • **URL** • **Services** • **COM** • **Remote PowerShell** • **ActiveX** • **Content**
Trusted Application Name	The trusted application that triggered the event.
Trusted Application Version	The trusted application version number.
Trusted File Owner	Whether the file owner of the target file is trusted. To be a trusted owner the user must be in one of the following Windows groups: • TrustedInstaller • System • Administrator
UAC Triggered	Whether or not Windows UAC was triggered: • Not Set • Triggered UAC • Did not trigger UAC
User Name	The user name of the user who triggered the event.
User Profiles Path	Sets the **User Profiles** path used by the **Discovery > By Path** report.
Workstyle	The name of the Workstyle that contained the rule that matched the application.

Overview of Endpoint Privilege Management Reporting Dashboards

Reporting includes several high level dashboards that summarize the Endpoint Privilege Management events. You can access the following from the side navigation panel.

Summary Dashboard	Displays bar charts for the most important activity that has occurred in the selected time period. Typically this information can result in Workstyle changes or investigation of anomalies. The charts allow you to view details when you click an action, either on a chart or in the legend. The bar charts are separated by Windows and Mac **Events by Action**.
Events Dashboard	Summarizes information about the types of events raised in the specified time frame. It also shows the time elapsed since a host raised an event.
Discovery Dashboard	Summarizes all the unique applications discovered. It differentiates between those that used elevated privileges and those that ran with standard privileges. This dashboard only shows new application items in the chosen time interval. For example, the Discovery dashboard can answer the question *what's new this week and how is it affecting my users?* The Discovery reports listed below the Discovery dashboard display the data from different angles such as by the location or publisher of the executable or the type of the executable.
Actions Dashboard	Summarizes audited items categorized by the type of action taken. This allows you to focus on the topic of interest. For example, elevation or blocking. The Actions reports show audits only of the selected type (**Elevated**, **Blocked**, **Passive**, **Canceled**, **Other**).
Target Types Dashboard	Lists all the Privilege Management activity over the specified time interval by target type. The report lists the targets in tabular form sorted by user count. You can click the targets in the list to view dashboard charts showing **Users**, **Hosts**, and **Process** activities and actions over a specified period of time.
User Experience Dashboard	Displays how users interacted with **Messages**, **Challenge/Response** dialog boxes, and the **Shell (On-Demand)** menu.
Privileged Logons Dashboard	Displays how many accounts with Standard rights, Power User rights, and Administrator rights generated logon events filtered by the time frame.
Privileged Account Management Dashboard	Displays any blocked attempts to modify privileged accounts over the specified time interval.
Trusted Application Protection Dashboard	Summarizes all the Trusted Application Protection incidents. Incidents are defined as a child process blocked from running because it matched the rules in the Trusted Application Protection policy or a DLL blocked from loading by a Trusted Application because it did not have a trusted owner or trusted publisher.

Summary Dashboard in Endpoint Privilege Management Reporting

The **Summary** dashboard displays bar charts for the most important activity that has occurred in the time period defined by the quick filter. The legends to the right of the charts display totals for the shown activities. You can use this information to inform Workstyle development or to show anomalous user behavior in your organization.

A warning message might display on the **Summary** page if there is a backlog of event processing. Verify your database configuration is set up to manage processing a large number of events.

The **Summary** dashboard includes the following tables:

Table	Description
Applications Discovered	The total number of newly discovered **Applications** filtered by the type of user rights required: • Admin rights required • Standard rights required **Discovered** applications are shown in the **Applications** table. Click the number next to the OS icon to show details.
User Requests	The total number of **User Requests** filtered by the type of request: • Blocked (user provided reason) • User canceled challenge Click the chart or legend to open the **Requests All** report with the **Request Type** filter applied.
Admin logons, by users, on endpoints	Summarizes the number of admin logons, the number of users, and the number of endpoints used. **Admin Logons** are shown in the **Administration** table. Click the number next to the OS icon to show details.
Trusted Application Protection	The number of Trusted Application (TAP) incidents, how many users, and how many endpoints were affected. **TAP** events are shown in the **Incidents** table. Click the number next to the OS icon to show details.
Attempts to modify privileged groups	The number of blocked attempts to modify privileged groups. **Attempts to modify privileged groups** are shown in the **Administration** table. Click the number next to the OS icon to show details.
Application run from external sources	The number of applications run from external sources. Applications **Run from external sources** are shown in the **Applications** table. Click the number next to the OS icon to show details.
Activities blocked	The number of applications blocked. Click the chart or legend to open the **Target Types All** report with the **Filter by Action** filter applied.

Table	Description
Applications used On-Demand privileges	The number of applications launched using on-demand privileges. Click the chart or legend to open the **Target Types All** report with the **Shell or Auto** filter applied. *Shell* indicates that on-demand privileges were used.
UAC matches	The number of applications that triggered User Account Control (UAC). **UAC** events are shown in the **Incidents** table. Click the number next to the OS icon to show details.

Events Dashboard in Endpoint Privilege Management

This report shows information about the types of events raised over the specified time period. It also shows the time elapsed since a host raised an event.

Chart	Description
Events over the last (time interval)	A column chart showing the number of the different Event types filtered by the time period. Clicking the chart opens the **Events All** report with the **Filter by Event Category** filter applied.
Event Types	A chart showing the number of events received filtered by the Event type. Clicking the chart opens the **Events All** report with the **Event Number** filter applied.
By Category	A chart displaying the events received filtered by category. Clicking the chart opens the **Events All** report with the **Filter by Event Category** filter applied.
Time since last endpoint event	A chart showing the number of endpoints in each time since last event category.

Events All Report

The following columns are available for the Windows and macOS **Events All** table:

- **Event Time:** The time of the event.
- **Event Category:** The category of the event.
- **Platform:** The platform where the event occurred.
- **Description:** The description of the event.
- **User Name:** The user name of the user who triggered the event.
- **Host Name:** The host name where the event was triggered.
- **Workstyle:** The Workstyle containing the rule that triggered the event.
- **Event Type:** The type of event.

Some of these columns allow you to drill down to additional information:

- **Event Time**: opens the event report listing all of the fields for that event.
- **Description:** opens the **Applications** Report.
- **User Name:** opens the **User** Report.
- **Host Name:** opens the **Host** Report.
- **Workstyle:** opens the **Workstyle** Report.

Process Detail Report

The **Process Detail** report provides a higher level of detail for Process events than the **Events > All** table. Other event categories are not shown in this table.

The following columns are available for the Windows and macOS **Process Details** table:

- **Start Time:** The start time of the event.
- **Platform:** The platform where the event occurred.

- **Description:** The description of the application.
- **Publisher:** The publisher of the application.
- **Application Type:** The type of application.
- **File Name:** The name of the file.
- **Command Line:** The command line of the process that triggered the event.
- **Product Name:** The product name of the application.
- **Product Version:** The product version of the application.
- **Trusted Application:** The name of the trusted application.
- **Trusted Application Version:** The version of the trusted application.
- **Group Policy Object:** The name of the Privilege Management policy (Windows only).
- **Workstyle:** The name of the Workstyle that the event was triggered from.
- **Message:** The message name if the event triggered a message.
- **Action:** The action associated with the event.
- **Application Group:** The Application Group the application assignment rule belongs to.
- **PID:** The process identifier of the process.
- **Parent PID:** The parent process identifier.
- **Parent Process File Name:** The parent process file name.
- **Shell / Auto:** Whether the process was triggered on-demand or automatically (Windows only).
- **UAC Triggered:** Whether user account control was triggered (Windows only).
- **Admin Rights Required:** Whether or not admin rights were required (Windows only).
- **Authorization Required:** Whether or not authorization rights were required (macOS only).
- **User Name:** The name of the user who triggered the event.
- **Host Name:** The name of the host where the event was triggered.
- **Rule Script File Name:** The name of the Rule Script (Power Rule).
- **Rule Script Affected Rule:** True when the Rule Script (Power Rule) changed one or more of the Default Privilege Management rules, otherwise false.
- **User Reason:** The reason given by the user if applicable.
- **COM Display Name:** The COM name if applicable (Windows only).
- **Source URL:** The URL of the event if applicable (Windows only).
- **BeyondTrust Zone Identifier:** The BeyondTrust Zone Identifier if present.
- **Uninstall Action:** This can be **None**, **Uninstall**, **Change/Modify**, or **Repair**.
- **Auth Methods:** The type of authentication method selected in the Policy Editor. Multiple values can be present and are comma separated. Possible values: **Identity Provider**, **Password**, **Challenge Response**, **Smart Card**, and **User Request**.
- **Idp Authentication User Name:** The credential provided when adding an Identity Provider authorization message in the Policy Editor.

Export Events to CSV File

The number of items that can be displayed at one time might be limited by the browser display. Click **Export to CSV** to enter the number of rows to export to the CSV file.

All event filters are saved to the file.

Discovery Dashboard in Endpoint Privilege Management Reporting

This dashboard displays information about applications discovered by the Reporting database for the first time. An application is first discovered when an event is received by the Privilege Management Reporting database. The **Discovery** dashboard displays events from Windows and macOS operating systems.

> ***Note:*** *Windows uses the terminology of* ***Admin Rights*** *and macOS uses the terminology of* ***Authorization****.*

The **Discovery** dashboard displays the following charts:

Chart	Description
Applications first reported in the specified time frame	A chart showing the number of applications discovered, filtered by the types of rights or authorization detected: For Windows: • **Admin Rights Detected** • **Admin Rights Not Detected** Click the **Admin rights detected** or **Admin rights not detected** lines in the graph to open the **Discovery** dashboard report with the **Admin Rights Required** filter applied. For macOS: • **Authorization Required** • **Authorization Not Required** Click the **Authorization Required** or **Authorization Not Required** lines in the graph to open the **Discovery** dashboard report with the **Authorization Required** filter applied.
Types of newly discovered applications	A chart showing the number of applications discovered by the type of application. The types are different for Windows and macOS operating systems. Click the chart to open the **Discovery** dashboard report with the **Admin Rights Required** filter applied.

The Discovery dashboard has the following tables:

New applications with admin rights detected	A list of discovered applications that are running with admin rights. This list is ordered by the number of users. Click **View all** to see the full list. Click any of the applications in the list to open the **Discovery** dashboard report with the **Admin Rights Required** and **Matched** filter applied.
New applications with admin rights not detected (top 10)	A list of discovered applications that are running with standard, not admin rights. This list is ordered by the number of users. Click **View all** to see the full list. Click any of the applications in the list to open the **Discovery** dashboard report with the **Admin Rights Required** and **Matched** filter applied.

New applications with admin rights detected (by type)	A list of the types of applications that required admin rights that were newly discovered within the time interval. They are ordered by the total number of applications for each type. Click **View all** to see the full list. Click any of the applications in the list to open the **Discovery** dashboard report with the **Admin Rights Required** and **Matched** filter applied.
New applications with admin rights not detected (by type)	The types of applications that did not require admin rights that were newly discovered within the time interval. They are ordered by the total number of applications for each type. Click any of the applications in the list to open the **Discovery** dashboard report with the **Admin Rights Required** and **Matched** filter applied.

Discovery Reports

The following reports are available from the navigation panel, under the **Discovery** dashboard. A description of each is in the below sections.

- **Discovery By Path**
- **Discovery By Publisher**
- **Discovery By Type**
- **Discovery Requiring Elevation**
- **Discovery From External Sources**
- **Discovery All**

Discovery by Path

This table displays the discovered applications grouped by path. Where there is more than one application per path, click **+** to expand the entry to examine each application.

The following columns are available for the Windows and macOS **Discovery By Path** table:

- **Path:** The path of the applications.
- **Description:** The description of the application.
- **Publisher:** The publisher of the applications.
- **Name:** The product name of the application.
- **Type:** The type of application.
- **Version:** The version number of a specific application.
- **# Users:** The number of users.
- **Median # Processes / User:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **# Applications:** The number of applications.
- **Date first Reported:** The date the application was first entered in the database.
- **Date first Executed:** The first known date the application was executed.

Some of these columns allow you to drill down to additional information:

- **Description**: Opens the **Applications** report for that application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table and lists the events received in the time period for the selected application.

Discovery by Publisher

This table displays the discovered applications grouped by publisher. Where there is more than one application per publisher, click **+** to expand the entry to examine each application.

The following columns are available for the Windows and macOS **Discovery By Publisher** table:

- **Publisher:** The publisher of the applications.
- **Description:** The description of the application.
- **Name:** The product name of the application.
- **Type:** The type of application.
- **Version:** The version number of a specific application.
- **# Users:** The number of users.
- **Median # Processes / User:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **# Applications:** The number of applications.
- **Date first Reported:** The date the application was first entered in the database.
- **Date first Executed:** The first known date the application was executed.

Some of these columns allow you to drill down to additional information:

- **Description**: Opens the **Applications** report for that application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table and lists the events received in the time period for the selected application.

Discovery by Type

This table displays applications filtered by type. When there is more than one application per type, click **+** to expand the entry to see each application.

The following columns are available for the Windows and macOS **Discovery By Type** table:

- **Type:** The type of application.
- **# Users:** The number of users.
- **Median # processes / user:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **Applications:** The number of applications.

- **Date first reported:** The date the application was first entered in the database.
- **Date first executed:** The first known date the application was executed.

Expanding the application type in the table, displays the following columns:

- **Description:** The description of the application.
- **Publisher:** The publisher of the applications.
- **Name:** The product name of the application.

Some of these allow you to drill down to additional information:

- **Description**: Opens the **Target Types** > **Applications** report which is filtered to that application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table and lists the events received in the time period for the selected application.

Discovery Requiring Elevation

This table displays the applications that were elevated or required admin rights.

The following columns are available for the Windows and macOS **Discovery Requiring Elevation** table:

- **Description:** The description of the application.
- **Publisher:** The publisher of the application.
- **Name:** The product name of the application.
- **Type:** The type of application.
- **# Users:** The number of users.
- **Median # Processes / User:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **Version:** The version number of a specific application.
- **Elevate Method:** The type of method used to elevate the application: **All**, **Admin account used**, **Auto-elevated**, or **on-demand**.
- **Date First Reported:** The date the application was first entered in the database.
- **Date First Executed:** The first known date the application was executed.

Some of these allow you to drill down to additional information:

- **Description:** Opens the **Target Types** > **Applications** report filtered to that application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table and lists the events received in the time period for the selected application.
- **Elevate Method:** Displays the **Events All** table with an extra **Elevate Method** column.

Discovery from External Sources

This table displays all applications that originated from an external source such as the internet or an external drive.

The following columns are available for the **Windows Discovery from External Sources** table:

- **Description:** The description of the application.
- **Publisher:** The publisher of the application.
- **Name:** The product name of the application.
- **Type:** The type of application.
- **Source:** The source of the application.
- **# Users:** The number of users.
- **Median # Processes / User:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **Version:** The version number of the application.
- **Date First Reported:** The date the application was first entered in the database.
- **Date First Executed:** The first known date the application was executed.

Some of these allow you to drill down to additional information:

- **Description:** Opens the **Applications** report for that application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Opens the **Events All** table and lists the events received in the time period for the selected application.

Discovery All

This table lists all applications discovered in the time period, grouped by the application description so that if multiple versions of the same application exist, they are grouped on the same line. Click **+** in the **Version** column to expand the list.

The following columns are available for the Windows and macOS **Discovery All** table:

- **Description:** The description of the application.
- **Publisher:** The publisher of the application.
- **Name:** The product name of the application.
- **Type:** The type of application.
- **Version:** The version number of the application.
- **# Users:** The number of users.
- **Median # Processes / User:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **Date First Reported:** The date the application was first entered in the database.
- **Date First Executed:** The first known date the application was executed.
- **Name:** The product name. This is hidden by default but you can select it from the **Actions > Choose Columns** menu.

Some of these columns allow you to drill down to additional information:

- **Description:** Opens the **Applications** report for that specific application.
- **# Users:** Displays a list of users the application events came from.

- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table.

Actions Dashboard in Endpoint Privilege Management Reporting

The **Actions** dashboard breaks down the application activity by the type of action. It also lists the most active targets.

The **Actions** dashboard has the following charts:

Chart	Description
All actions over the specified time frame	A chart showing the number of targets filtered by the type of action for each time frame for all target types. The types of action are: • **Elevated** • **Blocked** • **Passive** • **Canceled** • **Custom** • **Drop admin rights** Click the chart to open the **Target Types** report with the **Action** filter applied.
Distinct target count by target type	A chart showing the target count for each target type, filtered by the type of action. The targets types are: • **Application** • **Services** • **COM** • **Remote PowerShell** • **ActiveX** • **URL** • **Content** Click the chart to open the **Target Types** report with the **Action** and **Target Type** filters applied.
Top 10 targets	A chart showing the ten most used targets by process count. Click the chart to open the **Events All** report with the **Action** and **Target Description** filters applied.

Target Types Dashboard in Endpoint Privilege Management Reporting

The **Targets Types** report lists all targets for all actions over a specified period of time in a tabular format. Click the target in the **Description** column to view a dashboard containing charts showing the activity and actions for the target.

Chart	Description
Actions over the last (time interval)	A chart showing the number of processes for each action for the target. The actions are listed in the legend to the right of the chart. Click the action to open the **Events / All** report to view the events for that action and target.
Top 10 Users	A chart showing the 10 most common activities by process count for users. Click the chart to open the **Events / All** report to view the events for that user, action, and target.
Top 10 Hosts	A chart showing the 10 most common activities by process count for hosts. Click the chart to open the **Events / All** report to view the events for that host, action, and target.
Run Method	A chart showing the count and percentage for activities by run method (Shell or Automatic) count for hosts. Click the chart to open the **Events / All** report to view the specific events by run method.
Discovery - Admin Rights	A chart showing the count and percentage for activities that did not require admin rights. Click the chart to open the **Events / All** report to view the specific events that did not require admin rights.

Users Dashboard in Endpoint Privilege Management Reporting

The following dashboards are available from the navigation panel under **Users**. Overviews for each are described in the below sections.

- **User Experience**
- **Privileged Logons**
- **Privileged Account Management**

User Experience Dashboard

This dashboard shows how users interacted with Messages, Challenge/Response dialog boxes, and the Shell (On-Demand) menu.

Chart	Description
User Experience over the time period	A chart showing the percentage of users that experienced each interaction type filtered by the specified time period. Click the chart to display a list of users presented with that interaction.
Message Distribution	A chart showing how many users are in the defined categories of messages per time period. Click the chart to display a list of users in that category.
Messages per action type	A table showing message types displayed for **Allowed** and **Blocked** actions. Click the prompts, notifications or counts, or table to open the **Events All** report with the **Action** and **Message Type** filters applied.

Privileged Logons

This dashboard shows how many accounts with **Standard** rights, **Power User** rights and **Administrator** rights generated logon events filtered by the time frame.

Chart	Description
Privileged Logons over the last (time interval)	A chart and table showing the number of logons by the account types over time. Click the chart to open the **User Logons** table with the **Show Administrator Logons**, **Show Power User Logons** and **Show Standard User Logons** filters applied.
Logons by Account Privilege	A chart showing the total number of logons filtered by the different account types. Click the chart to open the **User Logons** table with the **Show Administrator Logons**, **Show Power User Logons** and **Show Standard User Logons** filters applied.
Logons by Account Type	A chart showing the total number of logons filtered by domain accounts and local accounts. Click the chart to open the **User Logons** table with the **Account Authority** filter applied.
Top 10 Logons by Chassis Type	A chart showing the total number of logons filtered by the top 10 chassis types. Click the chart to open the **User Logons** table with the **Chassis Type** filter applied.
Top 10 Logons by host Operating System	A chart showing the total number of logons filtered the top 10 host operating systems. Click the chart to open the **User Logons** table with the **OS** filter applied.

Chart	Description
Top 10 Accounts with Admin Rights	A chart showing the top 10 accounts with admin rights that have logged into the most host machines. Click the chart to open the **User Logons** table with the **User Domain** and **User Name** filter applied.
Top 10 hosts with Admin Rights	A chart showing the top 10 host machines logged on to by the most users with admin rights. Click the chart to open the **User Logons** table with the **Host Name**, **Show Administrator Logons** filter applied.

Privileged Account Management

This dashboard shows any blocked attempts to modify privileged accounts over the specified time interval.

Chart	Description
Privileged Account Management over the last (time interval)	A chart breaking down the privileged account management events by time period. Click the chart to display the **Privileged Account Management** table with the **Time Range** filter applied.
Table showing users blocked, hosts blocked, applications blocked, and total blocked modifications	A table showing the number of users, hosts, applications blocked, and the total number of blocked events within the specified time frame. Click the count numbers to open the **Privileged Account Management** table.
By Privileged Group	A chart showing the privileged account modification activity blocked by Windows group name. Click the chart to open the **Privileged Account Management** table with the **Group Name** filter applied.
Top 10 applications attempting account modifications	A chart showing the privileged account modification activity that was blocked, broken down by the **Application Description**. Click the chart to open the **Privileged Account Management** table with the **Application Description** filter applied.
Top 10 users attempting account modifications	A chart showing the top 10 users who attempted modifications. Click the chart to open the **Privileged Account Management** table with the **User Name** filter applied.
Top 10 hosts attempting account modifications	A chart showing the top 10 hosts attempting privileged account modifications. Click the chart to open the **Privileged Account Management** table with the **Host Name** filter applied.

Trusted Application Protection Dashboard in Endpoint Privilege Management Reporting

You can access this dashboard from the **Summary** dashboard. Click the number listed in the **Incidents** table, under **TAP**. This dashboard shows information about Trusted Application Protection (TAP) incidents. A TAP incident occurs when a child process of a trusted application is blocked due to a trusted application policy or when a DLL is prevented from loading by a trusted application because it lacks a trusted owner or publisher.

> ***Note:*** *There are no advanced filters for the* ***Trusted Application Protection*** *dashboard.*

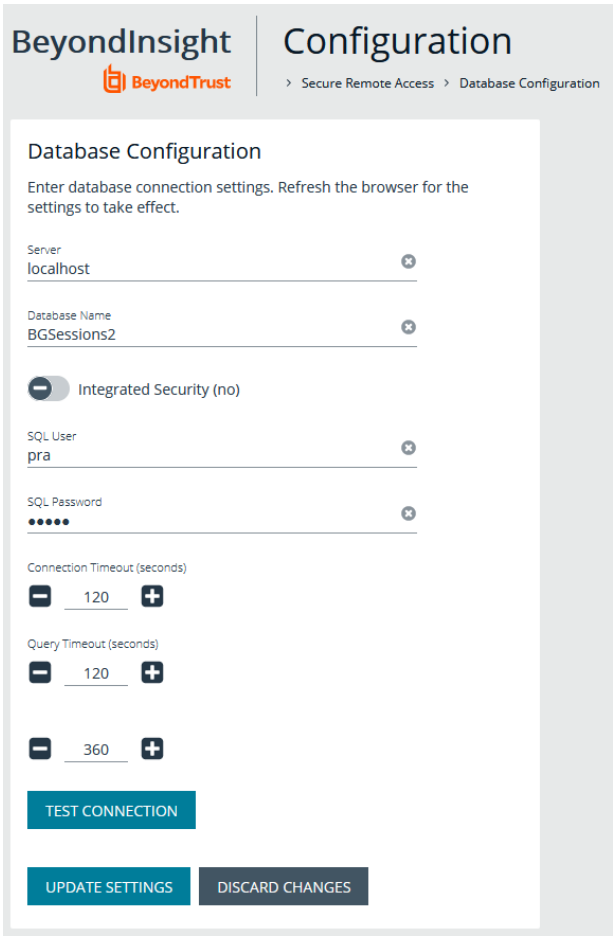
Chart	Description
Trusted Application Protection incidents over the time period.	A column chart showing the number of incidents filtered by the trusted application. Click the chart to open the **Process Details** report with **Time Range** filter applied.
Trusted Application Protection incidents, by application	A table listing each trusted application, the number of TAP incidents, the number of targets, the number of users, and the number of hosts affected. Click the **Incidents** number to open the **Process Details** report with the **Trusted Application Name** filter applied. Click the **Targets** number to open the **Targets > All** table with the **Trusted Application Name** filter applied.
Top 10 targets	The top 10 targets for TAP incidents. Click the **Target** to open the **Application** report with the **Application Type** and **Distinct Application ID** filters applied. Click the **Incident** number to open the **Process Details** report with the **Distinct Application ID** filter applied. Clicking the **Users** or **Hosts** number opens the **Users** or **Hosts** list, respectively.

View Privileged Remote Access Data

If you have a licensed instance of Privileged Remote Access configured in your environment, you can export session data to an export database. You can then review Privileged Remote Access session data in the BeyondInsight Console, using the Privileged Remote Access Dashboard.

Configure the Privileged Remote Access Database Connection

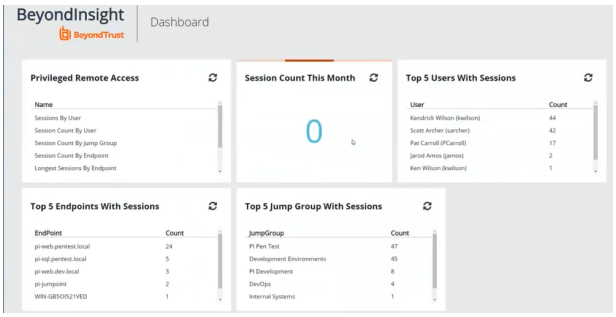
1. In the BeyondInsight Console, select **Configuration**.
2. Under **Secure Remote Access**, select **Database Configuration**.
3. Provide the settings to connect to your Privileged Remote Access export database, and then click **Test Connection**.
4. Click **Update Settings**.



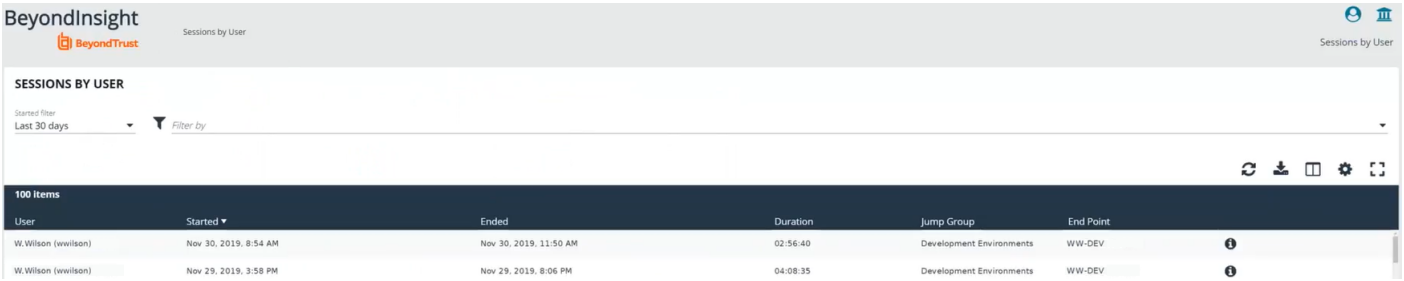
View the Privileged Remote Access Dashboard

1. From the menu, select **Privileged Remote Access**.

2. In the Dashboard you can quickly view a summary of Privileged Remote Access session data in each card.



3. You can click the items within each card to review the specific records for that item in a grid view that can be sorted, filtered, and exported as required.



Integrate the BeyondInsight API into Other Applications

You can integrate part of BeyondInsight's API into your applications using an API key.

> ***Note:*** *The **API Registration** page is only available to BeyondInsight administrators.*

The ID and key are generated by BeyondInsight.

1. Select **Configuration > General > API Registrations**.
2. Enter a name for the registration.
3. Click **Create New API Registration** to create a new application registration.

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

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

4. To configure a new registration or modify an existing one, select the registration, and then set the **Authentication Rule Options**.
    - **Client Certificate Required:** If enabled, a client certificate is required with the web request. If not, client certificates are ignored and do not need to be present. A valid client certificate is any client certificate 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.

      ```
      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 is 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. On the **Details** page, click **Add Authentication Rule** to create authentication rules. At least one IP rule, PSRUN rule, valid source IP address (IPv4 or IPv6), IP range, or CIDR from which requests can be sent for this API Key is required. Enter one IP address, IP Range, or CIDR per line.

   X-Forwarded-For rules can also be created by providing a valid source IP address (IPv4 or IPv6), an IP range, or CIDR. In a load-balanced scenario, IP Authentication rules are used to validate the load balancer IP(s), 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 for the HTTP Request . If the X-Forwarded-For header is missing, the request fails with a *401 unauthorized* error.
6. Click **Create Rule**.

Support and Product Updates

Click **Menu** in the left navigation toolbar, then **About**, to access support information and tools, product updates, and other resources including documentation links, version details, and the maintenance expiry date.

Send Files to BeyondTrust Technical Support

You can build and send file packages containing general information for support and collected events.

Create a Support Package

Create a support package that can be used by Support. The package includes:

- All logs in the BeyondInsight **Logs** folder
- Storage size statistics on the BeyondInsight database
- Certain database tables that contain information on scanner agents, and their jobs
- The **debug_syncit - log** file used to determine when files are updated from Auto Update

> ***Note:*** *Credentials are not stored in any of the package files.*

To generate the package:

1. From **Support Tools > Download Support Package**, click **Generate Support Package**.
2. A ZIP file is automatically created and saved to the **Downloads** folder.
3. Email the ZIP file to your support representative.

Send Analysis Files

Additionally, you can send events collected by Analyzer to provide additional troubleshooting details such as:

- The number of errors collected in the BeyondInsight logs
- Analysis of the events, including percentages of types (processed and purged)
- The percentage of duplicate and timed out agents
- Analysis of BeyondTrust components
- Customer name

To generate analysis files:

From **Support Tools > Send Analysis to Support**, click **Send Analysis to Support**. This generates an analysis file and sends it to Support.

> ***Tip:*** *Analysis files are retained for 30 days. You can click a link on the* ***About*** *page to request that the data be deleted prior to the 30 day expiry.*

Download Updates

BeyondInsight ships with BeyondTrust Updater.

Using the update tool, you can set up subscriptions to download product updates for BeyondInsight, Event Server, and BeyondTrust Updater.

Maintenance Information

This panel displays the contract **Maintenance Expiry Date** for BeyondInsight.

If your maintenance is close to expiry or has expired, a warning banner displays at the top of the Dashboard. The toggle **Hide Maintenance Expiry Warning Banner** can be set to on or off, to enable or disable this warning.

Note: *The **Maintenance Expiry Warning Banner** is only visible to administrators. Hiding the banner hides it from all administrators.*