BeyondTrust

BeyondInsight
User Guide 7.0

TC:9/3/2020

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 information about BeyondInsight components as well as instructions and procedures for using BeyondInsight.

Components

Network Security Scanner

The Network Security Scanner is the scan engine responsible for scanning the assets in your environment. The Network Security 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 Network Security Scanner agent.

The Events Client sends the information to the Manager Service. The Events Client is installed when a Network Security 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 www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-install.pdf.

Central Policy Server

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

For example, the Network Security Scanner agent needs to know the targets and the audits to run against those targets. This information is selected in the BeyondInsight management console. When the scan starts, the Central Policy sends the job information to the agent.

Updater Enterprise

Using the Central Policy, you can centrally manage updates for your BeyondTrust applications, receive updates automatically or manually, and distribute updates to client systems on your network.

You can schedule automatic updates to ensure that your assets are protected by the latest vulnerability audits.

Scheduling Service

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

Log into the BeyondInsight Console

Logging into the console varies depending on the type of authentication configured for your system.

The following authentication types can be used:

- **BeyondInsight**: Create a BeyondInsight user in the console and add the user to a group.
- **Active Directory:** Create a group and add Active Directory users as members.
- **LDAP:** Create a user group and add Active Directory users as members.
- **RADIUS:** Configure multi-factor authentication with a RADIUS server.
- **Password Safe Authentication:** Please see the Password Safe *Administration Guide*
- **Smart Card:** Please see the Password Safe *Administration Guide*
- **Third Party Authentication that supports SAML 2.0:** Please see the Password Safe *Administration Guide*

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

1. Select **Start > All Programs > BeyondInsight > BeyondInsight > BeyondInsight Console**.
2. Optionally, open a browser, and enter the URL, **https://<servername>/WebConsole/index.html**

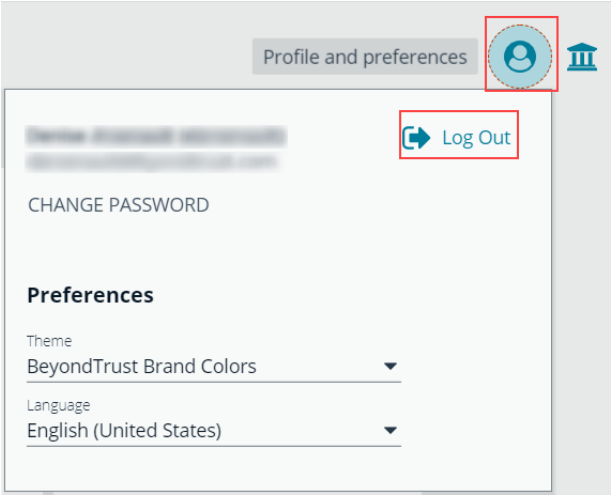
> ***Note:*** *A pre-login banner message might be configured on your system. You must click **OK** before you can enter your credentials.*

3. Enter your user name and password.
4. The default user name is **BTADMIN**, and the password is the administrator password you set in the **Configuration** wizard.
5. If applicable, select a domain.
6. Click **Login**.

> ***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.*

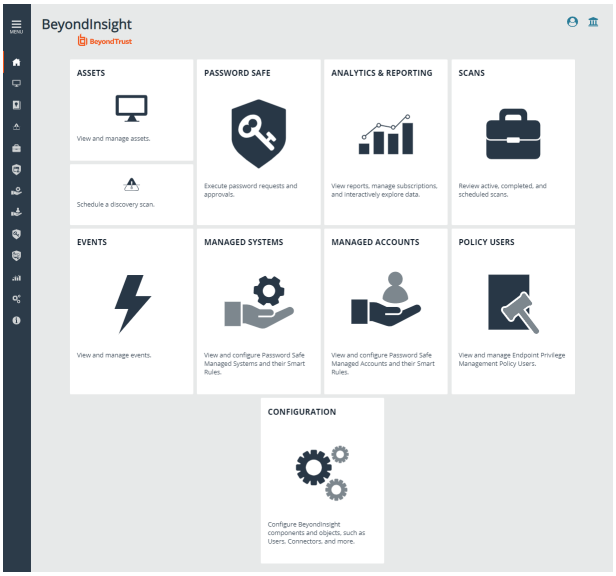
Log Out of the Console

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



Navigate the Console

Once logged into the BeyondInsight console, your suite of features are easily accessible by clicking the container cards or by clicking **Menu** in the left navigation.



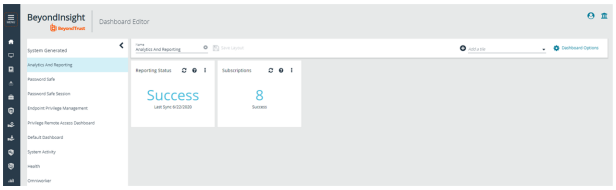
Features available on the home page include:

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

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.

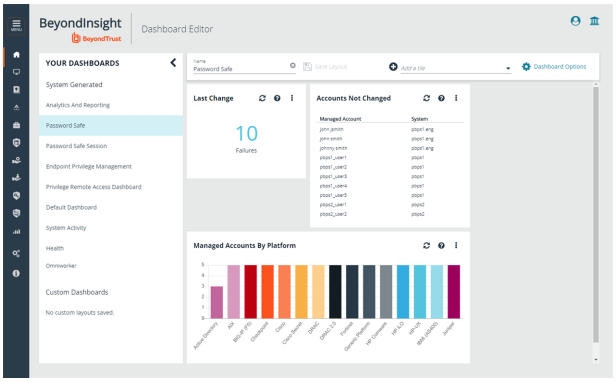


To access **Your Dashboards**, click **Menu > Dashboards**. A list of available dashboards displays on the left. BeyondInsight comes with several prebuilt dashboard cards, including:

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

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

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



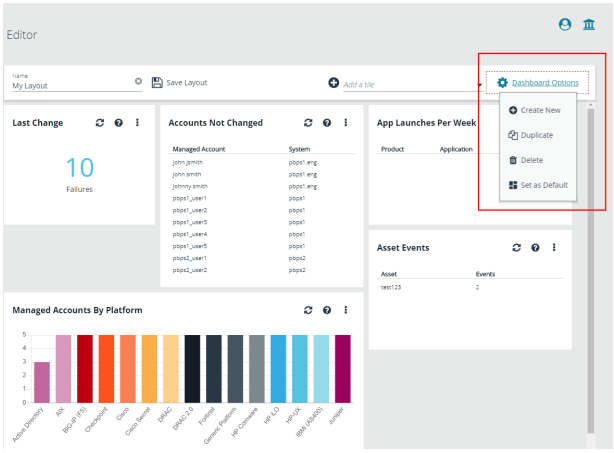
Click to refresh information displayed.

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:

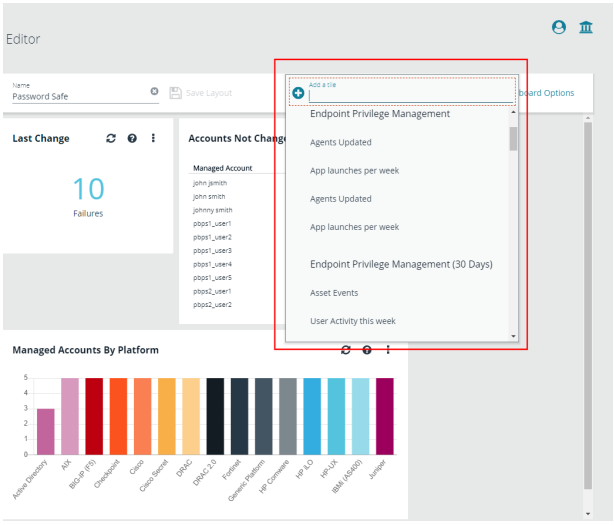
- **Create New:** Create a new empty dashboard, then add the tiles you want.
- **Duplicate:** Create a copy of the dashboard that can be modified.
- **Delete:** Delete the selected dashboard.
- **Set as Default:** Set the current dashboard as the default one so it displays every time you click on **Menu > 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 re-sized to allow you a personalized and more efficient experience.

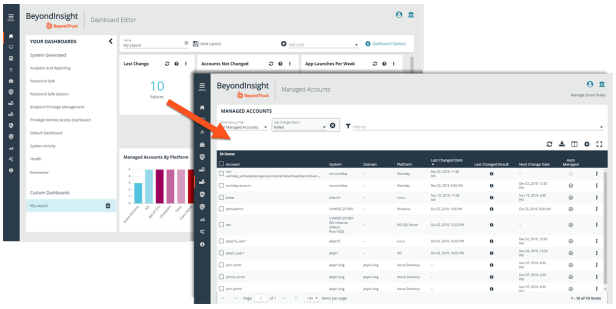
1. To create a custom dashboard, select one of the available dashboard cards. In this example we are using the **Password Safe** card. If necessary, delete any of the existing tiles that come installed with that card.
2. Click **Add a tile** and select the tiles you want from the drop-down menu. Resize and reposition tiles in a manner that makes sense to you.
3. Next, under **Name**, give your 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 click on **Menu > Dashboards**, click **Dashboard Options**, then **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****, replacing 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 Change** 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.



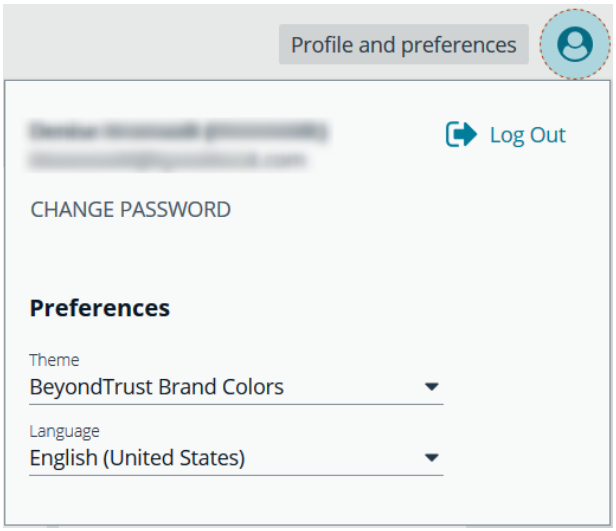
Change and Reset Login Passwords

You can change the password used to log into the console. You cannot change your password for the following scenarios:

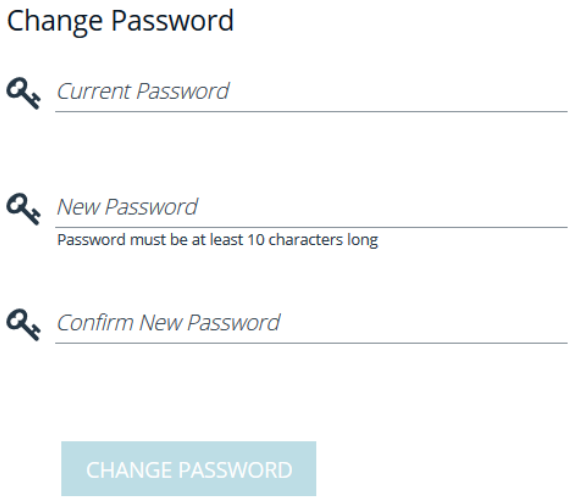
- You are logging in with Active Directory or LDAP credentials.
- Your account is currently locked out.

Change Password

1. In the console, click **Profile and preferences**, and then select **Change Password**.

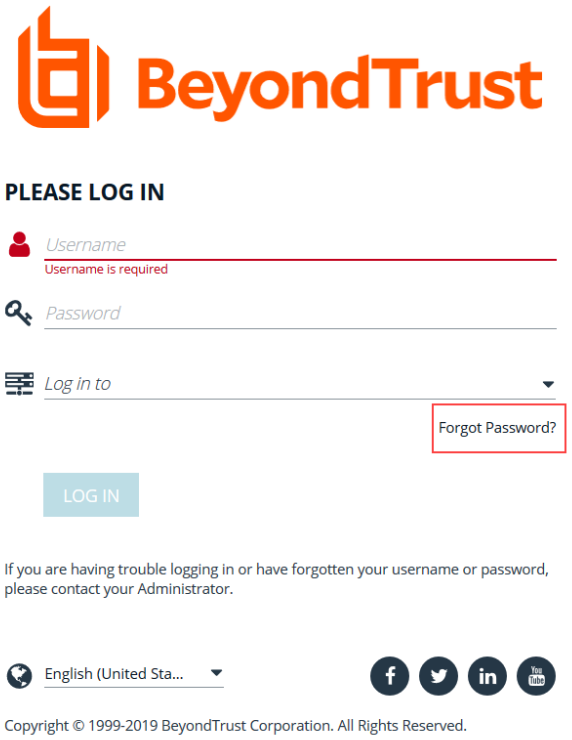


2. Change your password, and then click **Change Password**.



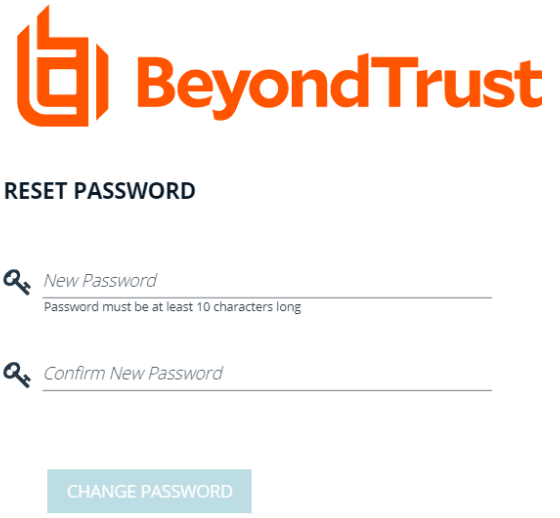
Reset Password

If you forget your console password, click **Forgot Password**, and then enter your username and click **Reset Password**. An email is sent from the console administrator with a reset link provided.



Click the link in the email to be taken to the **Reset 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 and 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.*

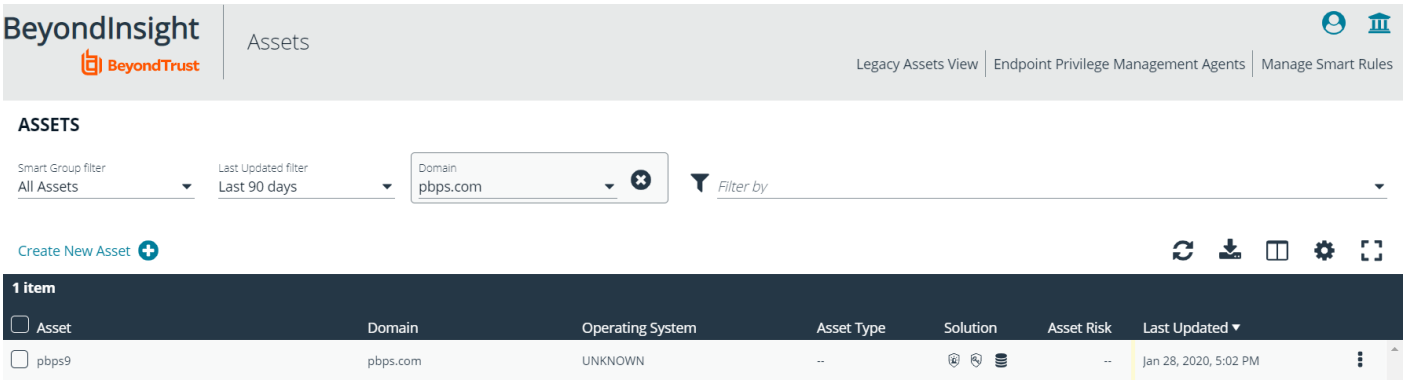
1. Select an area of the site, such as **Assets**.
2. Above the grid, you will see the following options and icons:

   - **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**.
3. 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, you will see filter options. The filter options available vary based on the page or grid selected. However, some consistent filtering options include:
   - **Smart Group filter:** Select to filter information by smart group association.
   - **Filter by:** Choose to filter the information by **Domain**, **Operating System**, **Workgroup**, etc. 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 your selections.
5. Filter selections persist if the page is reloaded. To remove a filter, click the **X** on the filter.



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" will still appear in the footer text on the* ***Login*** *page. This cannot be changed.*
>
> *After an upgrade, you will need to repeat these steps as the upgrade will overwrite the customized images and set 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-greyscale.svg** (black and white version of the logo)
- **app-logo-inverse.svg** (negative of default or simply all white)

> ***Tip:*** *The images must be 450px X 67px.*

Role Based Access

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

BeyondInsight offers a role-based delegation model so that you can explicitly assign certain read and write permissions to a user groups based on their role.

You can create a BeyondInsight user group, or you can use an existing Active Directory group.

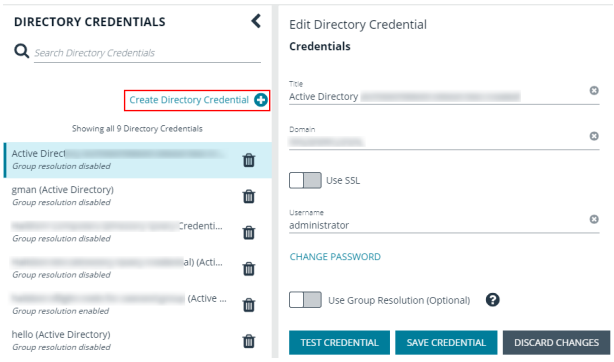
***Note:** By default, an **Administrators** user group is created. The permissions assigned to the group cannot be changed. The user account you created when you configured BeyondInsight is a member of the group.*

After a user group is created, create and add user accounts to the group. When a user is added to a group, the user is assigned the permissions assigned to the group.

Create and Edit Directory Credentials

A directory credential is required for querying Active Directory and LDAP, and also for adding Active Directory and LDAP groups and users in BeyondInsight.

1. Select **Configuration** .
2. Under **Role Based Access**, select **Directory Credentials**.
3. Click **Create Directory Credential**.



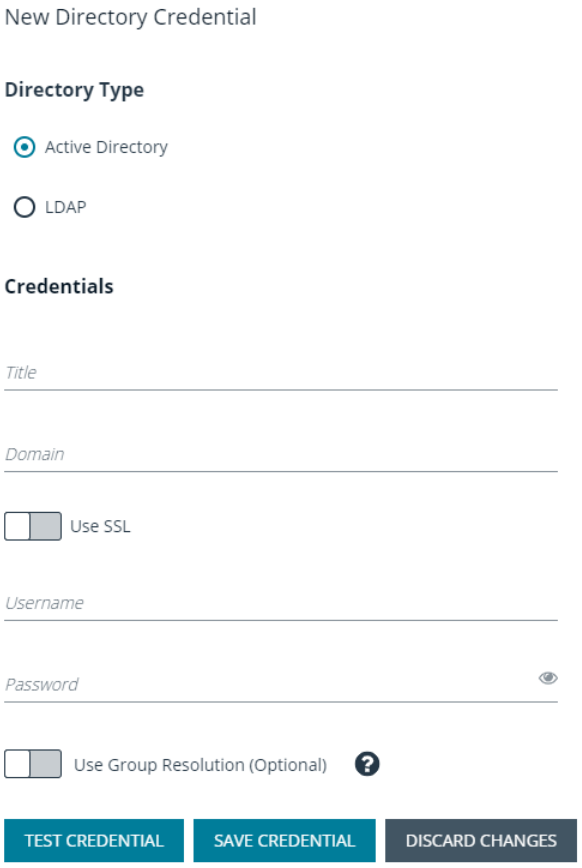
4. Select the directory type and provide a name for the credential.
5. Enter the name of the domain where the directory and user credentials reside.
6. Enable the SSL option to use a secure connection when accessing the directory.

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

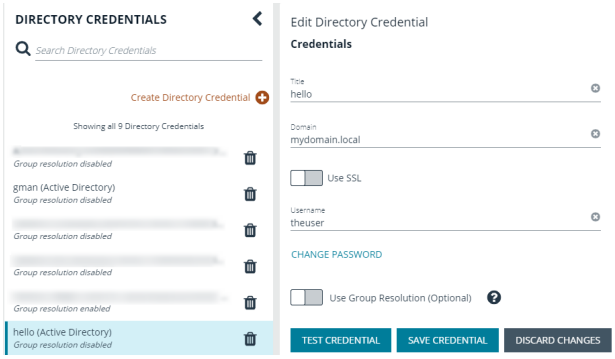
7. Enter the credentials for the account that has permissions to query the directory.
8. Enable the **Use Group Resolution** option to use this credential to for resolving groups from the directory.

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

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

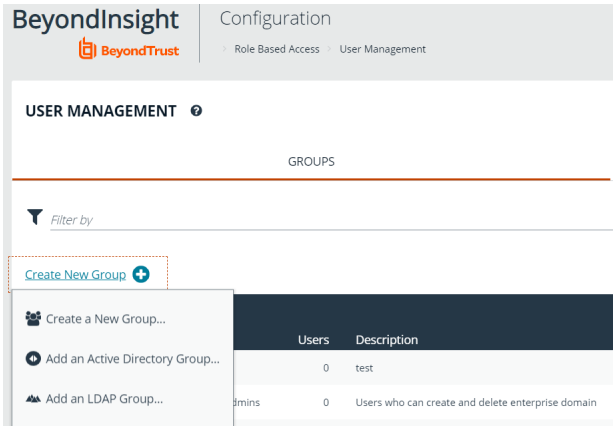


11. To edit a directory credential, select the credential and edit as desired.
    - If you change the **Domain**, **Use SSL** option, or the **Username**, you must change the password.
    - The **Change Password** section expands to display fields to enter and confirm the new password.
12. Click **Test Credential** to ensure the edited credential can successfully authenticate with the domain or domain controller before saving the credential.
13. Click **Save Credential**.

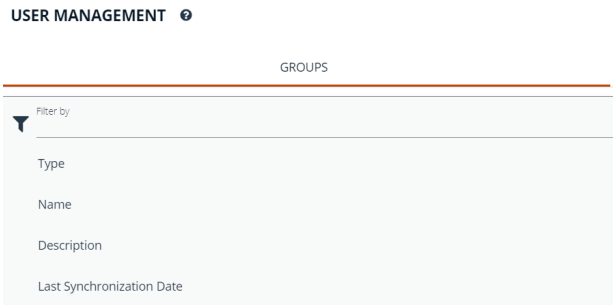


Create and Configure Groups

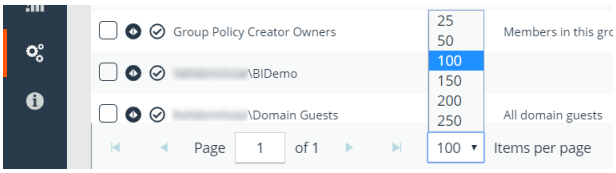
You can create BeyondInsight local groups, as well as add Active Directory and LDAP groups into BeyondInsight.



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.*

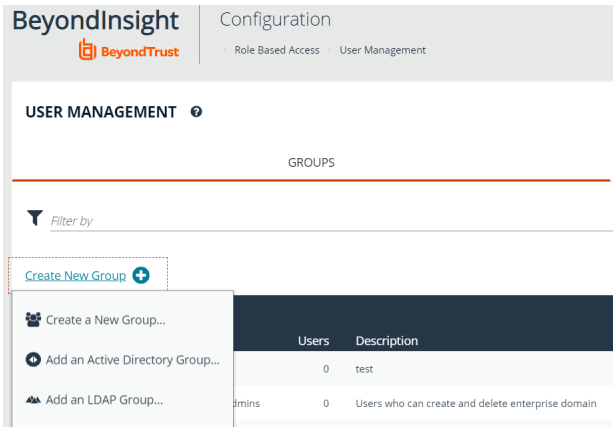


After a group is created, add user accounts to the group. When a user is added to a group, the user is assigned the permissions assigned to the group.

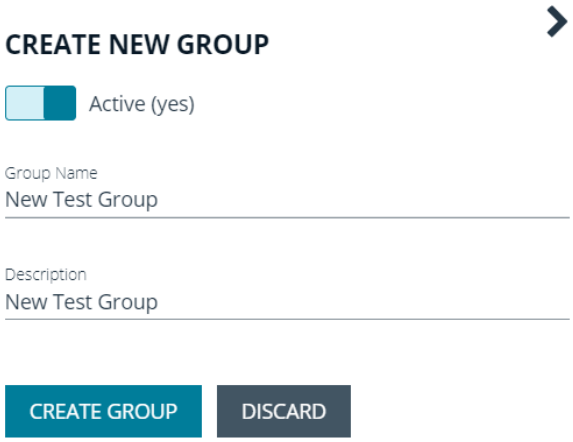
Create a BeyondInsight Local Group

1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.

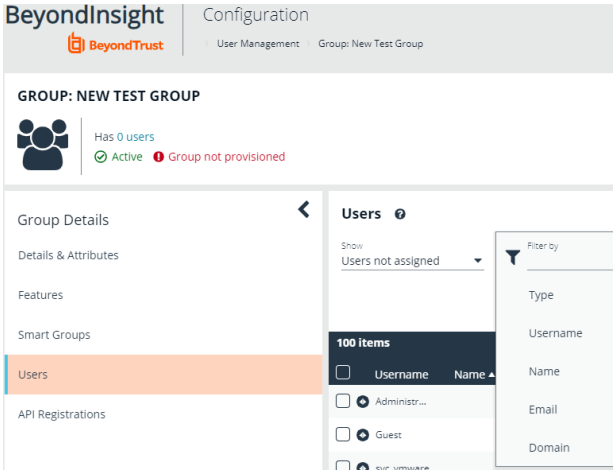
3. Under **Groups**, click **Create New Group**.
4. Select Create a New Group.



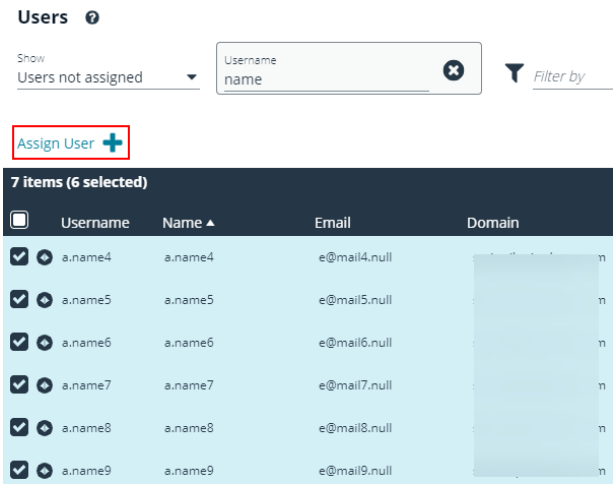
5. Enter a **Group Name** and **Description** for the group.
6. The group is set to **Active (yes)** by default. Click the slider to set the group to **Active (no)** if you wish to activate it later.
7. Click **Create Group**.



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



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



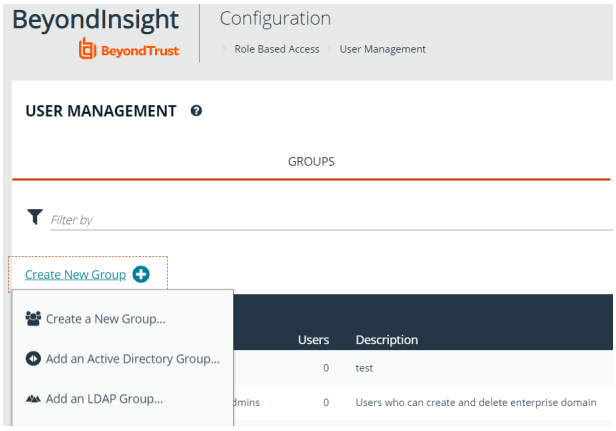
By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 27.

Add an Active Directory Group

Active Directory group members can log into 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.

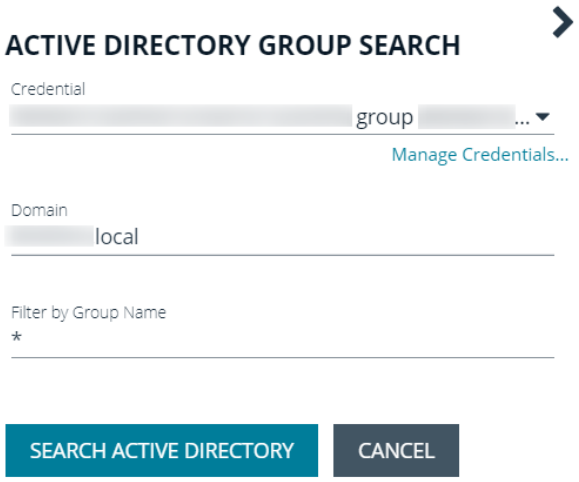
Note: *Active Directory users must log into the management console at least once to receive email notifications.*

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



5. Select a credential, or click **Manage Credentials** to add or edit a credential.

> For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 18.

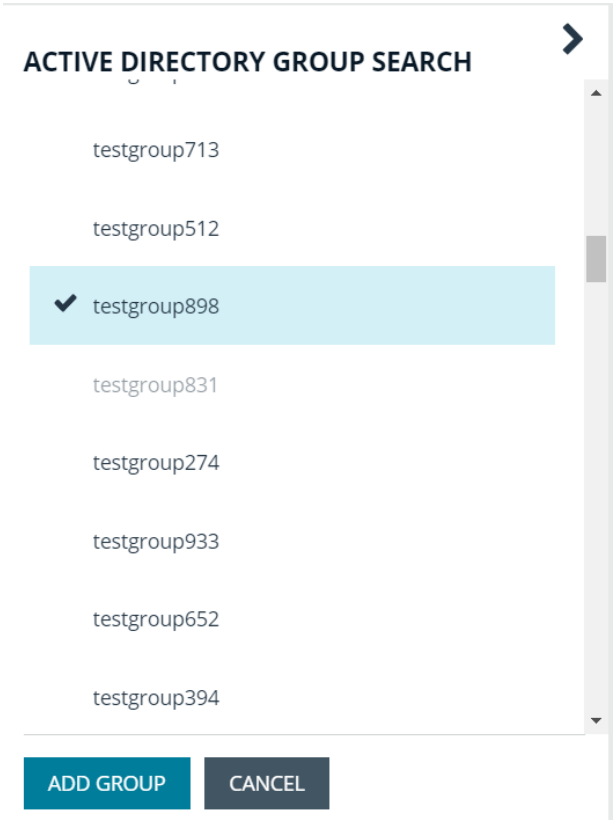


6. If not automatically populated, enter the name of a domain or domain controller.
7. After you enter the domain or domain controller credential information, click **Search Active Directory**. A list of security groups in the selected domain is displayed.

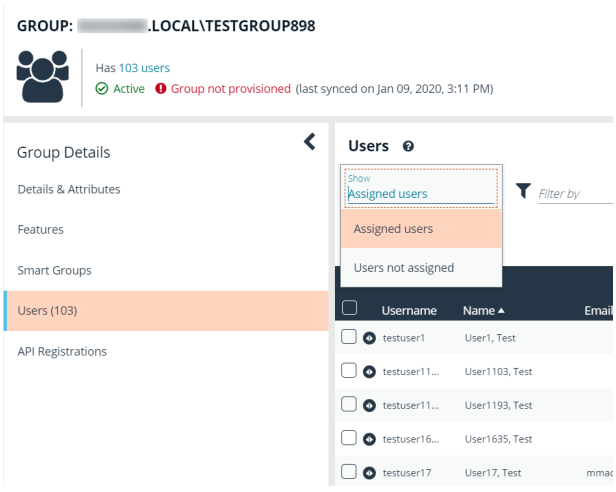
> ***Note:*** *The default filter is an asterisk (*), which is a wild card filter that returns all groups. For performance reasons, a maximum of 250 groups from Active Directory is retrieved.*

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

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



10. 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.
11. 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.



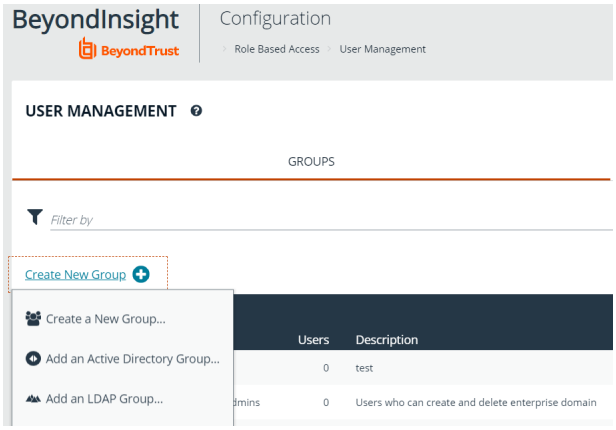
By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 27.

Add an LDAP Directory Group

LDAP group members can log into 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.

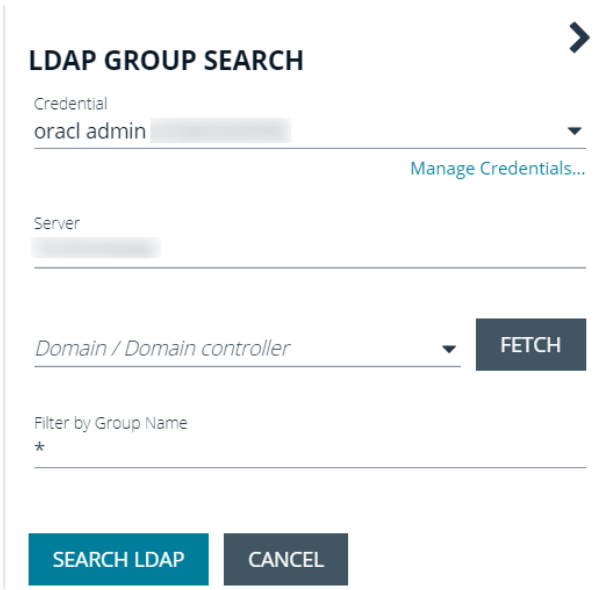
> ***Note:*** *LDAP users must log into the management console at least once to receive email notifications.*

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



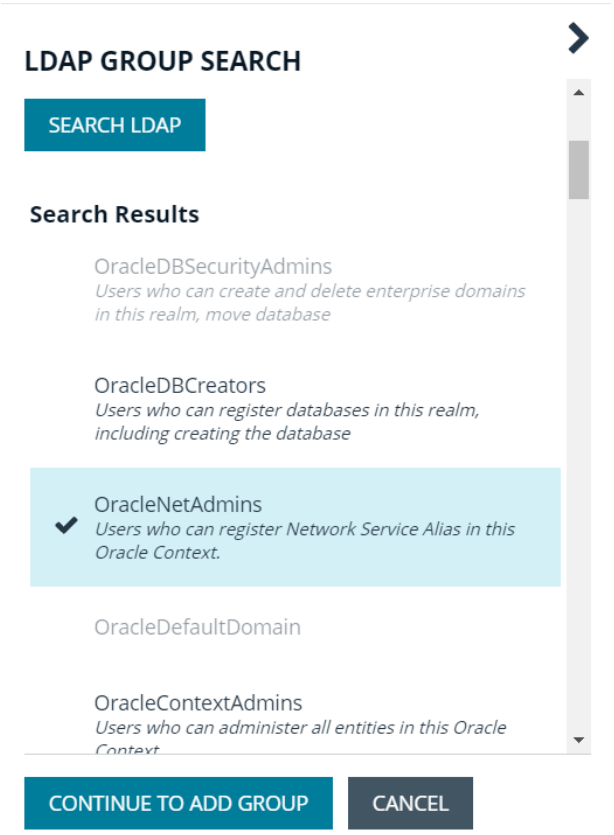
5. Select a credential, or click **Manage Credentials** to edit a credential or create a new one.

> For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 18.

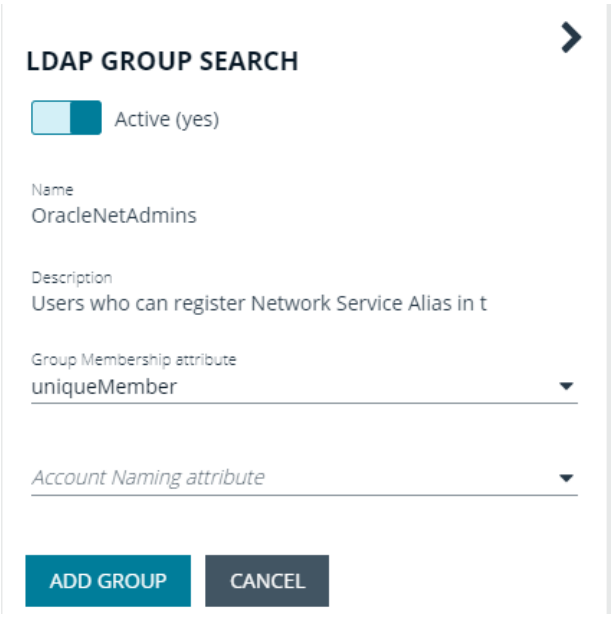


6. Click **Fetch** to load the list of Domain Controllers, and then select one.
7. To filter the group search, enter keywords in the group filter or use a wild card.
8. Click **Search LDAP**.

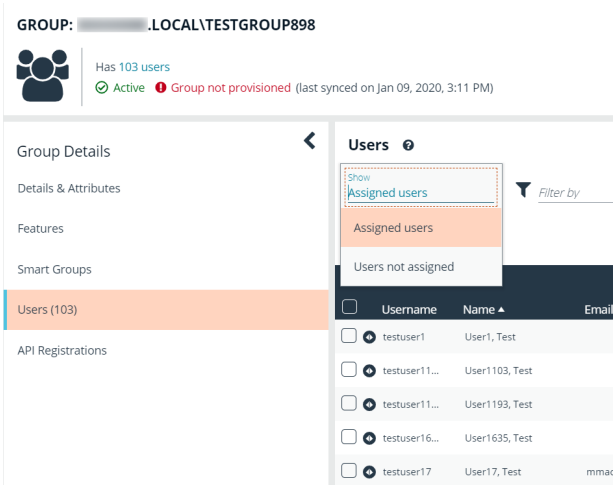
9. Select a group, and then click **Continue to Add Group**.



10. Select the **Group Membership Attribute** and **Account Naming Attribute**.
11. Click **Add Group**.
12. The group is added and set to **Active** but is not provisioned or synchronized with LDAP. Synchronization with LDAP to retrieve users begins immediately.



13. 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.



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 27.

Assign Group Permissions

Permissions

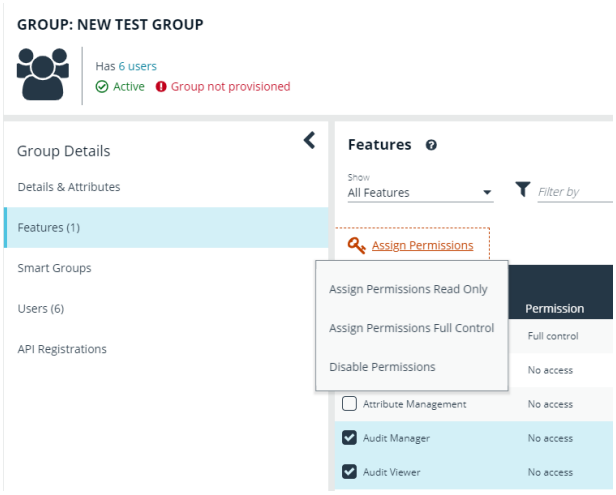
Permission	Description
No Access	Users cannot access the selected feature. In most cases, the feature will not be visible to the users.
Read Only	Users can view selected areas, but cannot change information.
Full Control	Users can view and change information for the selected feature.

Permissions must be assigned cumulatively. For example, if you want a BeyondInsight administrator to manage discovery scans only, then you must assign **Full Control** for the following features :

- **Asset Management**
- **Reports Management**
- **Scan - Job Management**
- **Scan Management**

Assign Features Permissions

1. Under **Group Details**, select **Features**.
2. Filter the list of features displayed in the grid using the **Show** and **Filter by** drop-down lists.
3. Select the features you wish to assign permissions to, and then click **Assign Permissions**.
4. Select **Assign Permissions Read Only**, **Assign Permissions Full Control**, or **Disable Permissions**.



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

Feature	Provides Permissions To:
Analytics and Reporting	Log into the console and access **Analytics & Reporting** to generate and subscribe to reports. ***Note:*** *After you create a group, go to the* ***Anayltics & Reporting Configuration*** *page and run the process daily cube job. Data between the management console and the reporting cube must be synchronized.*
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.
Audit Manager	**Audit Manager** on the **Configuration** page in the management console.
Audit Viewer	Use the **Audit Viewer** in **Analytics & Reporting**.
Benchmark Compliance	Configure and run benchmark compliance scans.
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.*
Endpoint Privilege Management	Use the **Endpoint Privilege Management** module, including asset details and the exclusions section on the **Configuration** page.

Feature	Provides Permissions To:
Endpoint Privilege Management for Unix and Linux	Use the **Endpoint Privilege Management for Unix and Linux** module.
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	Acces 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.
Password Safe Account Management	Grants 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 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/index.htm.
Password Safe Admin Session	Password Safe web portal admin sessions.
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 - Audit Groups	Create, delete, update, and revert audit group settings.

Feature	Provides Permissions To:
Scan - Job Management	Activate **Scan** and **Start Scan** buttons. Activate **Abort**, **Resume**, **Pause**, and **Delete** on the **Job Details** page.
Scan - Policy Manager	Activate the settings on the **Edit Scan Settings** view.
Scan - Port Groups	Create, delete, update, and revert port group settings.
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, PCI Compliance Report, and Vulnerabilities Report)
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.
Session Monitoring	Use the session monitoring features.
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.
User Audits	View audit details for management console users on the **User Audits** page.
Vulnerability Exclusions	Select this option to prevent users from excluding vulnerabilities from the display. You can exclude vulnerabilities from the display to view those that require remediation to satisfy regulatory compliance. In some situations, you might not want all of your users to set an exclusion on a vulnerability.

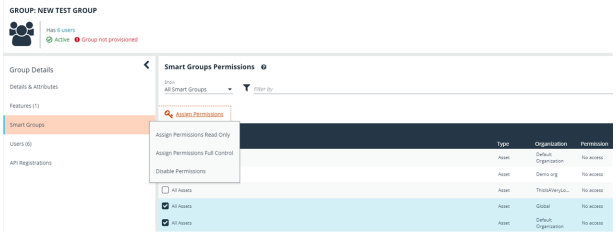
Feature Permissions Required for Configuration Options

Configuration Option	Feature and Permission
Active Directory Queries	Asset Management - Full Control
Address Groups	Asset Management - Full Control
Attributes	Asset Management - Full Control
Benchmark Compliance	Benchmark 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

Configuration Option	Feature and Permission
User Management	User and Group Management - Full Control
Workgroups	User Accounts Management - Full Control

Assign Smart Groups Permissions

1. Under **Group Details**, select **Smart Groups**.
2. Filter the list of smart groups displayed in the grid using the **Show** and **Filter by** drop-down lists.
3. Select the smart groups you wish to assign permissions to, and then click **Assign Permissions**.
4. Select **Assign Permissions Read Only**, **Assign Permissions Full Control**, or **Disable Permissions**.



Edit and Delete Groups

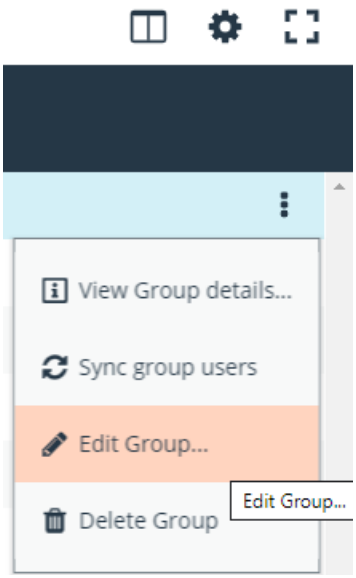
Edit Basic Group Details

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. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Optionally, filter the list of groups in the grid by **Type**, **Name**, **Description**, or **Last Synchronization Date**.
4. Select a group, and then click the **More Options** button, then select **Edit Group**.



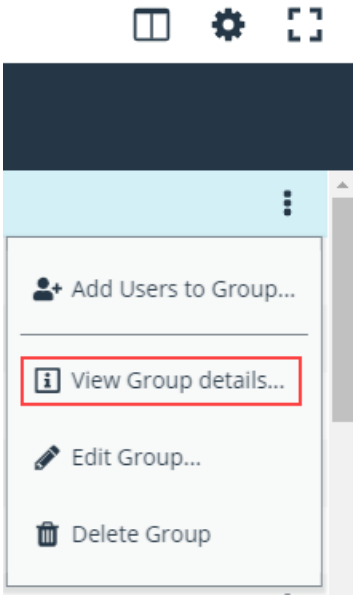
5. In the **Edit Group** pane, update the details as required, and then click **Update Group**.
   - For BeyondInsight local groups, administrators can change the active status, name, and description.
   - For Active Directory groups, administrators can change the active status, credential, and domain controller.
   - For LDAP groups, administrators can change the active status, credential, group membership attribute, and account naming attribute.

Edit Advanced Group Details

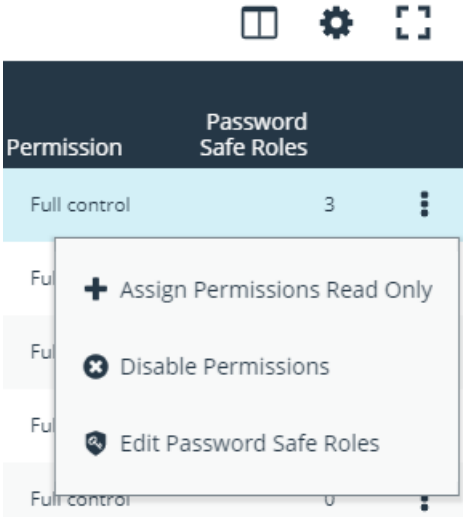
Administrators can edit advanced details, such as update permissions for features and smart groups, edit Password Safe roles, add and remove users from local groups, sync group users for Active Directory and LDAP groups, and update the API registrations.

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**, and then select a group.
2. Click the **More Options** button, and then select **View Group Details**.

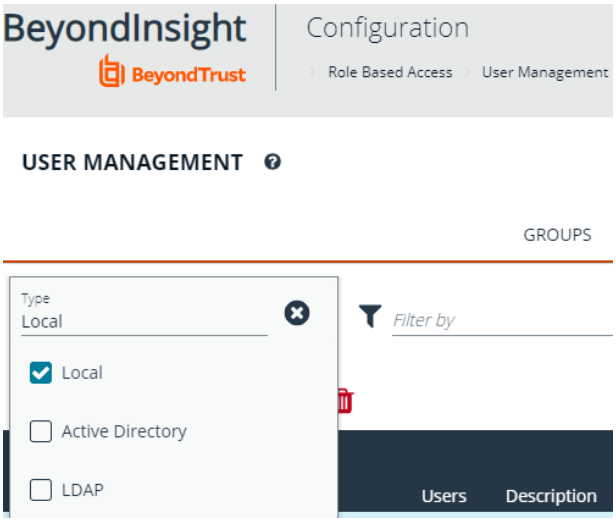


3. Select the desired features or smart groups, click **More Options**, and then select to assign or disable permissions accordingly.

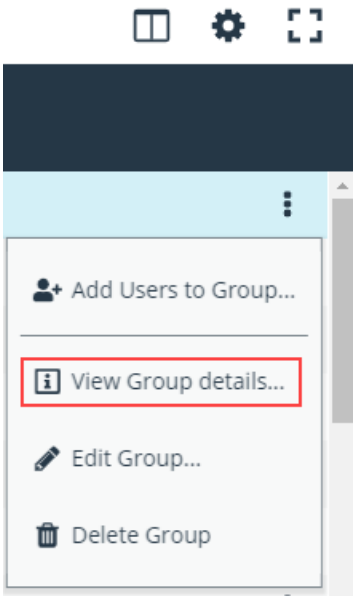


Remove Users from Local BeyondInsight Groups

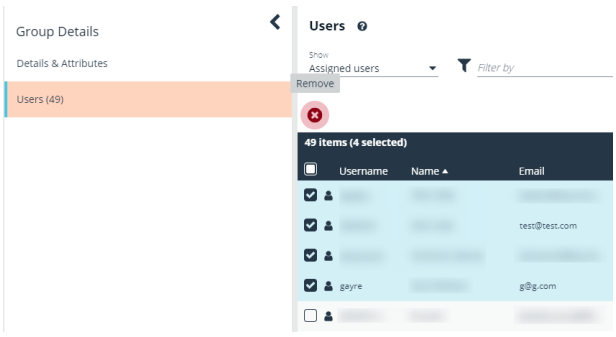
1. On the **User Management** page, filter the grid by local groups.



2. Select the group, click the **More Options** button, and then select **View Group Details**.

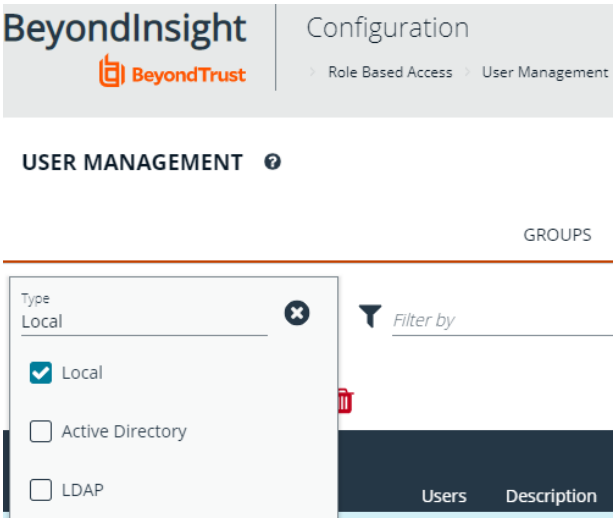


3. Under **Group Details**, select **Users**.
4. Filter the **Users** grid to show assigned users.
5. Select the user or users, and then click the **Remove** button.

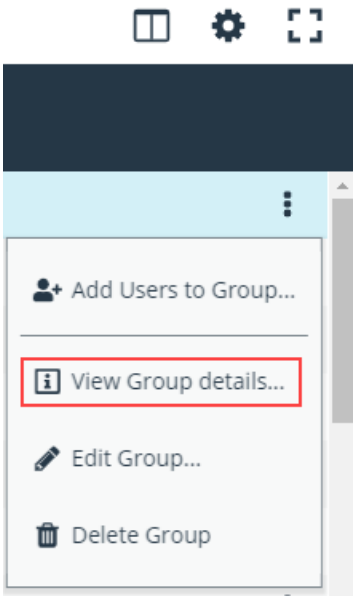


Add Users to Local BeyondInsight Groups

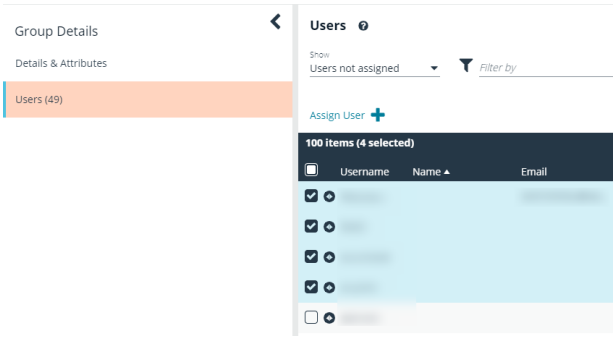
1. On the **User Management** page, filter the grid by local groups.



2. Select the group, click **More Options**, and then select **View Group Details**.

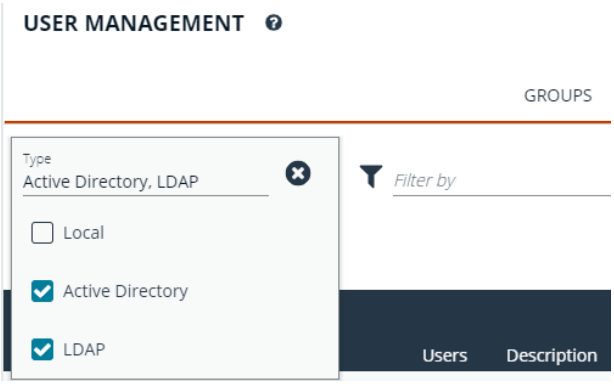


3. Under **Group Details**, select **Users**.
4. Filter the **Users** grid to show unassigned users.
5. Select the user or users, and then click **Assign User**.

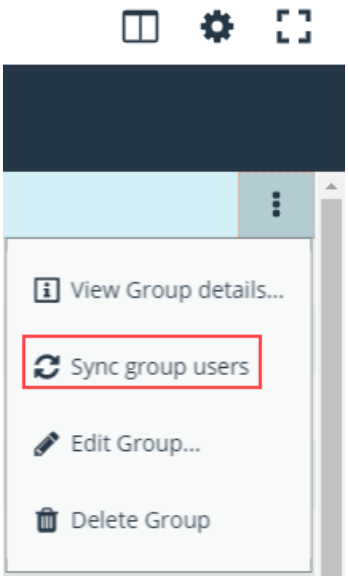


Sync Group Users for Active Directory and LDAP Groups

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



2. Select the group, click **More Options**, and then select **Sync Group Users**.



Delete a Group

Administrators can delete groups as follows:

1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Optionally, filter the list of groups in the grid by **Type**, **Name**, **Description**, or **Last Synchronization Date**.
4. Select a group, and then click the **Delete** button above the grid, or click the **More Options** button, and then select **Delete Group**.

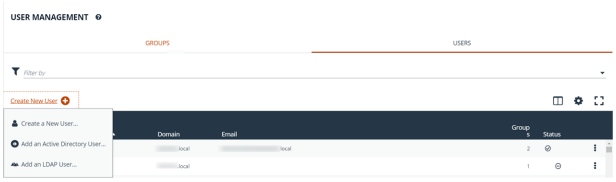
Create and Manage User Accounts

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

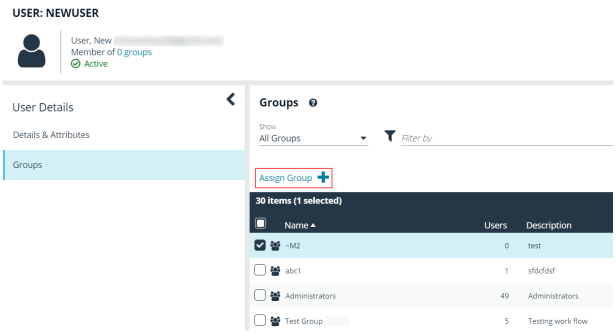
> ***Note:*** *A user account must be a member of a BeyondInsight group. If a user is not a member of any groups in BeyondInsight, the user will not be able to log into the console.*

Create a BeyondInsight Local User Account

1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Select **Users** to display the list of users in the grid.
4. Click **Create New User**.

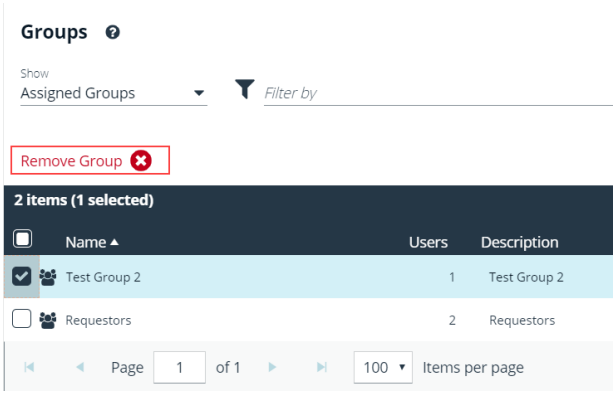


5. Select **Create a New User**.
6. Complete the **Identification** and **Credentials / Change Password** sections. These fields are required.
7. Enter the user's contact information *(Optional)*.
8. Select an **Activation Date** and an **Expiration Date** for the user account.
9. Enable the **User Active** option to activate the user account.
10. Leave the **Account Locked** and **Account Quarantined** options disabled.
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**.



> ***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**.

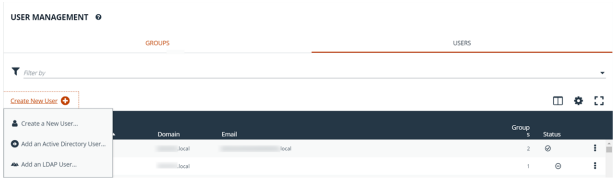


Add an Active Directory User

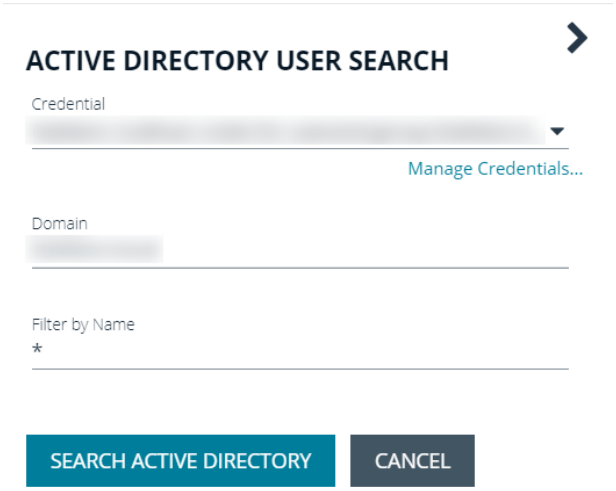
Active Directory users can log into the management console and perform tasks based on the permissions assigned to their groups. The user can authenticate against either a domain or domain controller.

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

1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Select **Users** to display the list of users in the grid.
4. Click **Create New User**.



5. Select **Add an Active Directory User**.
6. Select a credential for the directory, or click **Manage Credentials** to add or edit a credential.



For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 18.

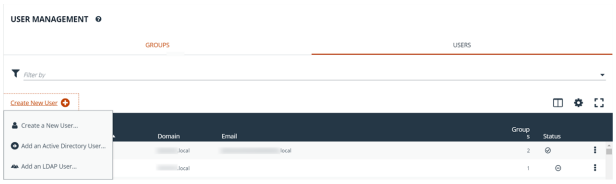
7. If not automatically populated, enter the name of a domain or domain controller.
8. After you enter the domain or domain controller credential information, click **Search Active Directory**. A list of users in the selected domain is displayed.

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

9. Set a filter on the groups that will be retrieved, and then click **Search Active Directory**. Example 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.
10. Select a user, and then click **Add User**.
11. Assign at least one group to the user.

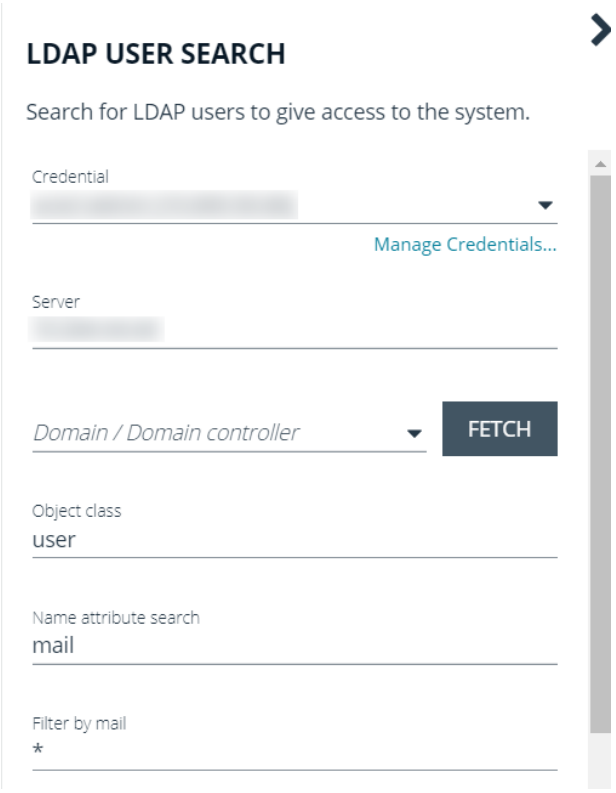
Add an LDAP User

1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Select **Users** to display the list of users in the grid.
4. Click **Create New User**.



5. Select **Add an LDAP User** from the list.

6. Select a credential for the directory, or click **Manage Credentials** to add or edit a credential.



For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 18.

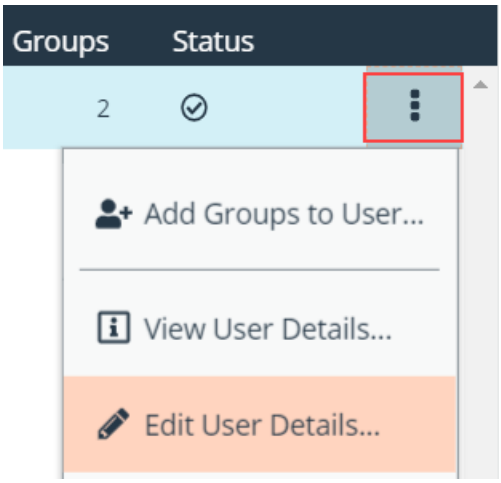
7. Click **Fetch** to load the list Domain Controllers, and then select one.
8. To filter the group search, enter keywords in the group filter or use a wild card.
9. Click **Search LDAP**.
10. Select a user, and then click **Add User**.
11. Assign at least one group to the user.

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:

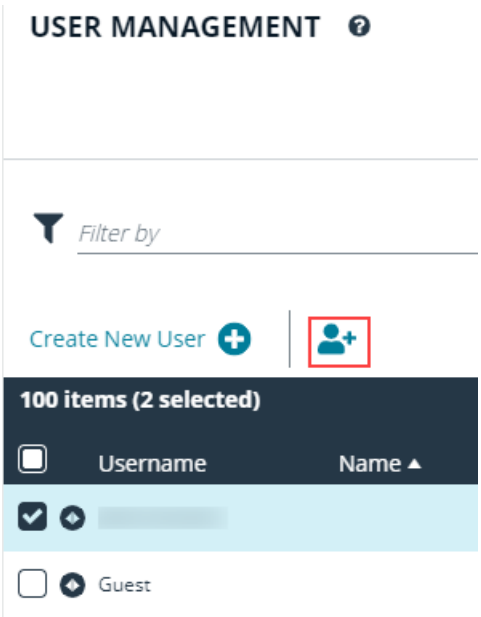
1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Click **Users** to display the list of users in the grid.
4. Optionally, filter the list of users in the grid by **Type**, **Username**, **Name**, **Domain**, or **Email**.

5. Select a user, and then click the **More Options** button, then select **Edit User Details**.
6. In the **Edit User** pane, update the details as required, and then click **Update User**.



Add Groups to User

1. From the **User Management** page, click **Users** to display the list of users in the grid.
2. Optionally, filter the list of users in the grid by **Type**, **Username**, **Name**, **Domain**, or **Email**.
3. Select a user or users, and then click the **Add User to Groups** button above the grid.



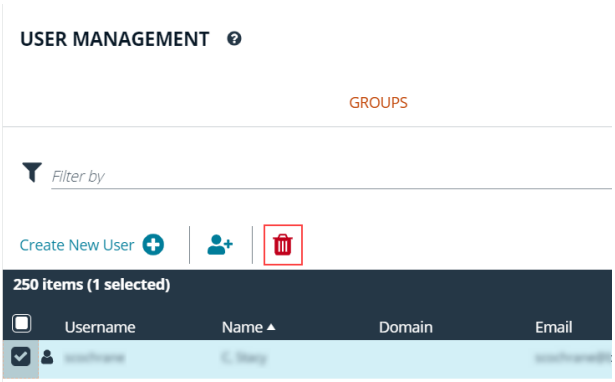
4. Search for the group or groups, and then select the group or groups to assign currently selected users to the selected groups.

> ***Note:*** *If a group already contains all of the selected users, a check mark will be displayed next to the group name.*

Delete a User Account

Administrators can delete user accounts as follows:

1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Click **Users** to display the list of users in the grid.
4. Optionally, filter the list of users in the grid by **Type**, **Username**, **Name**, **Domain**, or **Email**.
5. Select a user, and then click the **Delete** button above the grid, or click the **More Options** button, and then select **Delete User**.



> ***Note:*** *This process only removes the selected user(s) from their assigned group(s). It does not delete the user from BeyondInsight.*

Audit Console Users

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**.

You can also configure display preferences and filters to refine the information displayed. For more information, please see "Change and Set the Console Display and Preferences" on page 15.

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.*

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 and Preferences" on page 15.

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** feature to be able to create smart rules.*

For more information, please see "Create and Configure Groups" on page 20.

Create an Always Address Group

You can create an address group and name it **Always**. The Network Security 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.

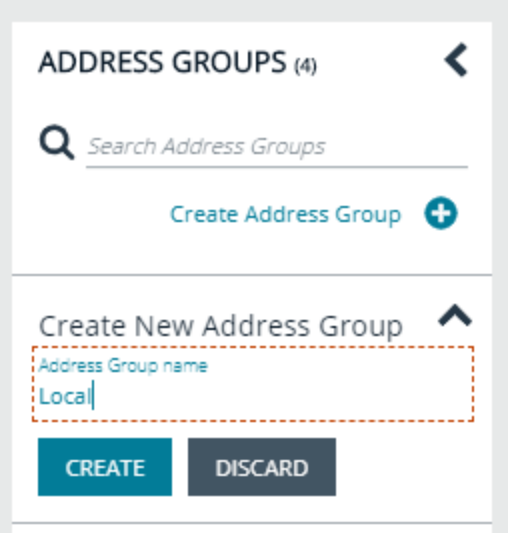
The next time a scan runs, the address group is synchronized with the Network Security Scanner. The IP addresses, whether they are included or omitted, are considered part of the running scan.

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.*

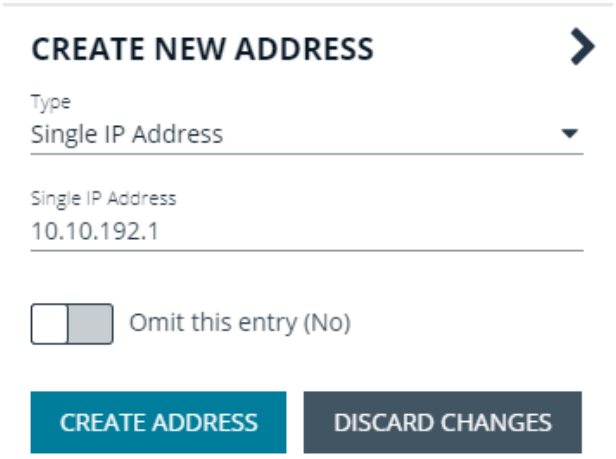
Note: *If an asset was scanned and later added to the **Always** address group as **Omit**, the asset is not scanned but might be displayed in the report. This only occurs with some reports.*

1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Address Groups**.
3. Click **Create Address Group**.
4. Enter a name for the address group, and then click **Create**.

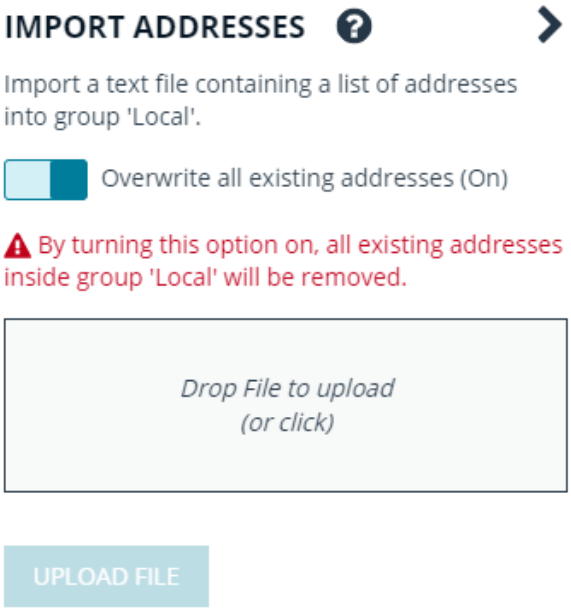


5. Select the address group, and then click **Add New Address** to manually add the IP addresses. Or, click **Import Addresses** to import them into the group using a file.

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

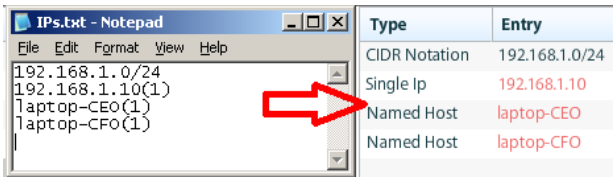


7. If importing the addresses:
    - Enable the **Overwrite all existing addresses** option, if desired.
    - Click **Drop File** to upload the import file.
    - Click **Upload File**.



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)**.

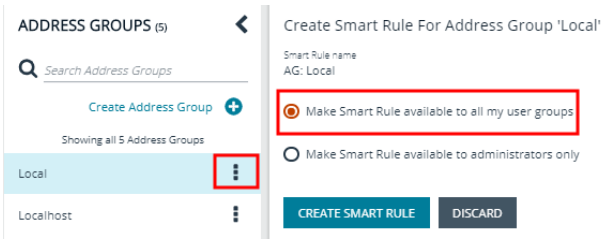
Here is an example of how a CIDR Notation, an excluded IP address, and excluded named hosts are displayed after importing.



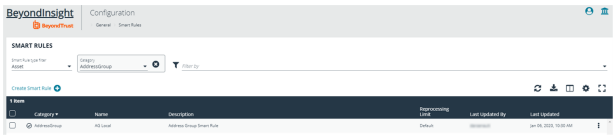
Create a Smart Rule Based on an Address Group

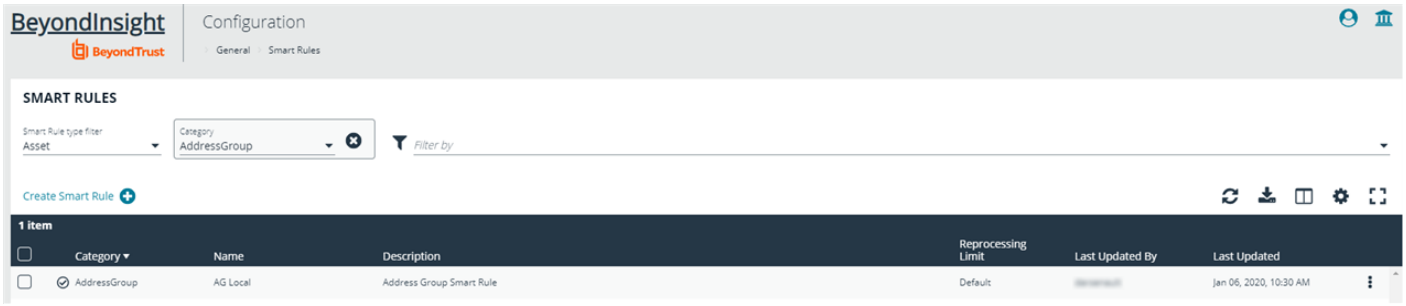
When configuring an address group, you can choose to create a smart rule based on the address group.

1. Select the address group, and click the **Edit** icon.
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. You will receive a message stating that a *Smart Rule has been created for this Address Group*.
7. The group is displayed on the **Configuration > Smart Rules** .





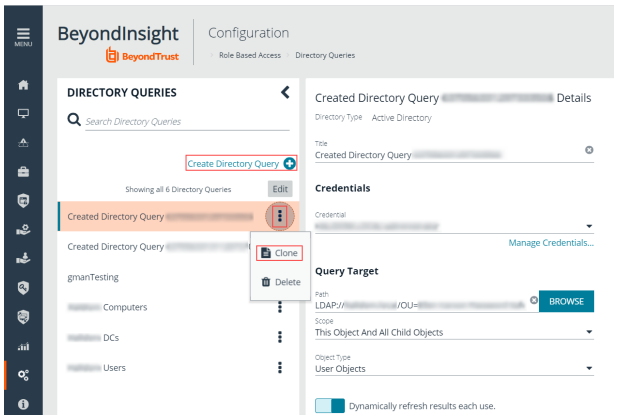
Create a Directory Query

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.

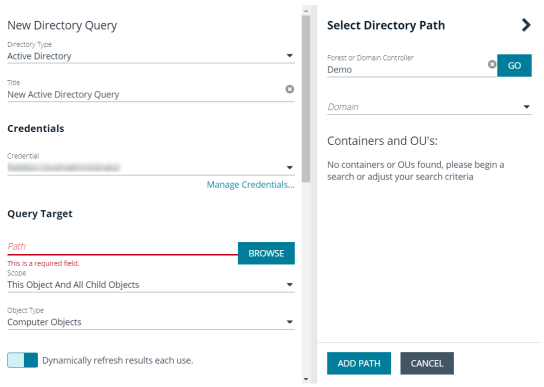
For more information, please see "Create and Configure Groups" on page 20.

1. Select **Configuration**.
2. Under **Role Based Access**, click **Directory Queries**.
3. Click **Create Directory Query**.

***Note:** To clone an existing query, hover over a query in the list, and then click the **Edit** icon, and select **Clone**.*



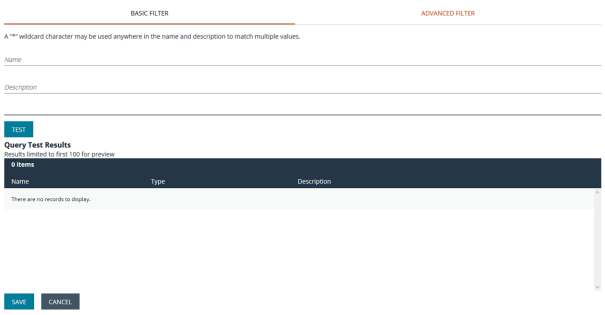
4. Select the directory type: **Active Directory** or **LDAP**.
5. Enter a name for the query.
6. Select a stored credential for running this query or click **Manage Credentials** to add or edit a credential.



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

> For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 18.

7. Enter a path, or click **Browse** to search for a path and add it.
8. Select a scope to apply to the container: **This Object and All Child Objects** or **Immediate Children Only**.
9. Select an object type.
10. Enter a name and description for the basic filter.
11. Click **Advanced Filter**, and then enter the LDAP query details.
12. Click **Test** to ensure the query returns expected results.
13. Click **Save**.



Attributes and Attributes Types

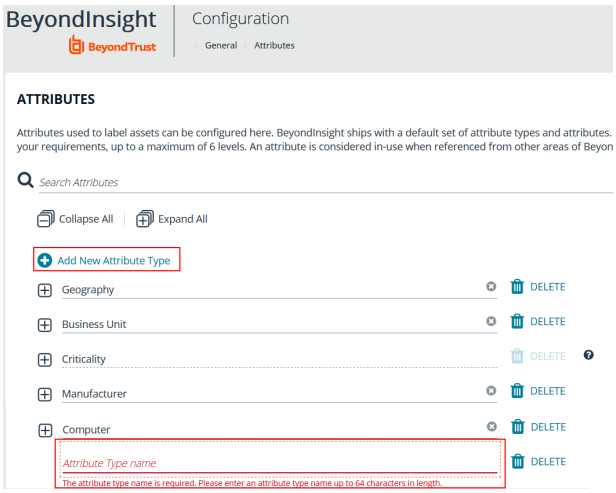
Attributes can be used to label assets, and you can set attributes for each asset in a group using a Smart Rule. BeyondInsight ships with a default set of attributes that can be customized, except for the **Criticality** type, and you can also add new attribute types and attributes to meet your requirements.

> For more information, please see "Use Smart Rules to Organize Assets" on page 51.

Add a New Attribute Type

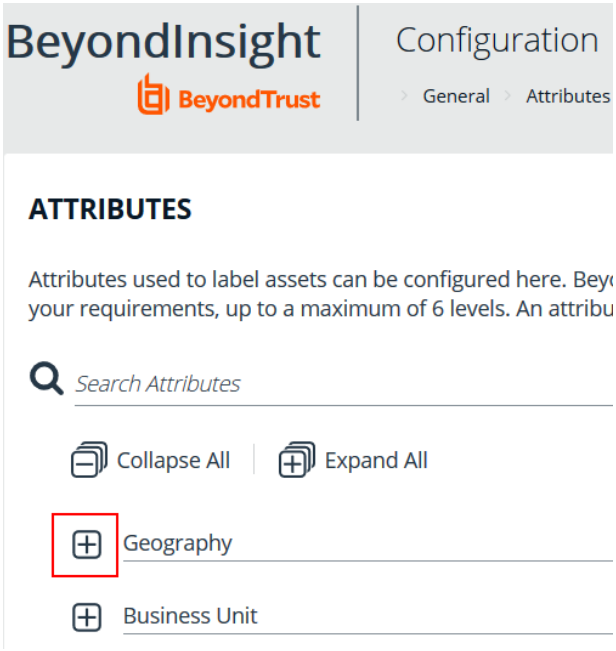
1. In the BeyondInsight console go to **Configuration > General > Attributes**.

2. Click **Add New Attribute Type**.
3. Type a name for the attribute type, and then press **Enter**.

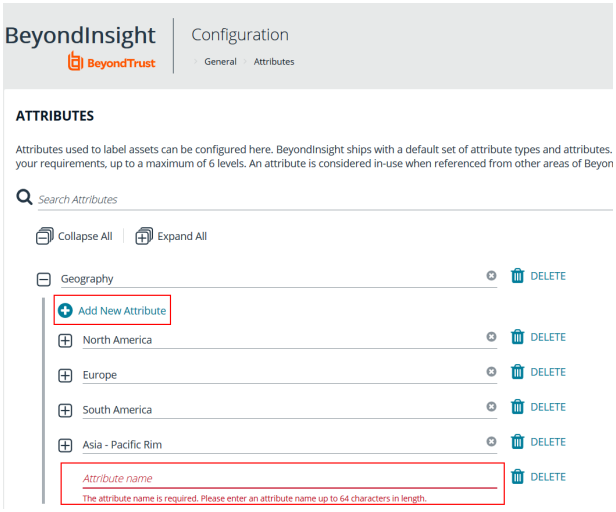


Add a New Attribute

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. You can organize the assets using one of the following smart rule types:

- **Asset Based Smart Rules:** Organizes the assets based on the filters selected.
- **Vulnerability Based Smart Rules:** Organizes the vulnerabilities based on the filter selected.

> ***Note:*** *The BeyondInsight user must be a member of the* ***Administrators*** *group or be assigned the* ***Full Control*** *permission on the* ***Asset Management*** *feature to be able to create 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** permissions for.

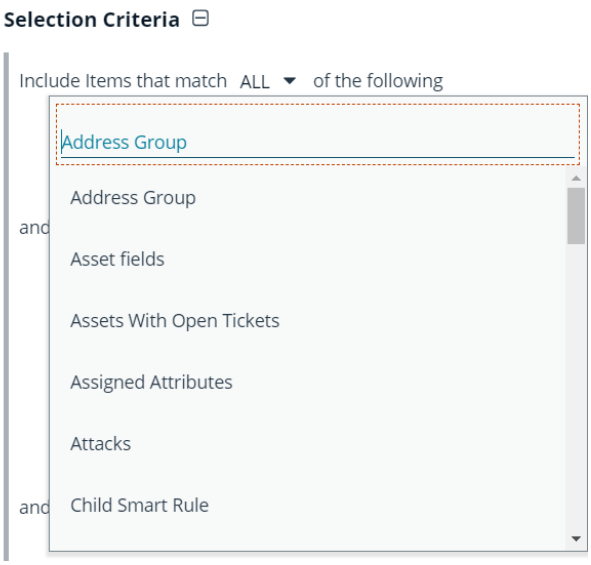
Use a smart rule to register assets as smart groups. This allows you to:

- Run discovery scans
- Apply protection policies
- Register for patch updates
- Monitor and view assets

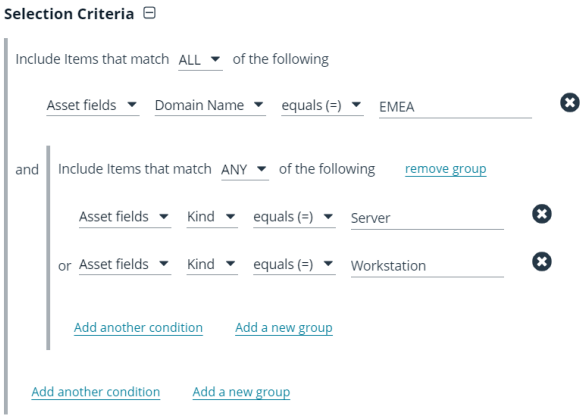
Smart rules update results automatically, ensuring assets match the criteria and are current.

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. For more information, please see "Create an Address Group" on page 44.
Asset Fields	Group the smart rule by asset fields, such as, **Asset Name**, **Device ID**, **Domain** or **DNS**, **Risk**, and **Kind**.

	You can include more than one asset field filter in the smart rule to refine the results. ***Note: Device ID** and **Serial Number** apply to mobile devices only.*
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.
Attacks	Filter assets based on attack, or filter on attack name or ID.
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. For more information, please see "Create a Directory Query" on page 47.
Installed Software	Filter on any combination of installed software.
MAC Address	Filter by MAC address of assets.
Malware	Filter assets based on malware, or filter on malware name or ID.
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.
Ports	Filter by port group. Assets with open ports in the port group can be included or excluded from the rule.
Processes	Filter on any combination of processes.
Protection Agents	Filter by protection agents.
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.
Vulnerabilities	Filter by vulnerability, CVSS score or vector, PCI severity, or vulnerabilities from an audit group.
Windows Events	Filter by Windows events that are available in the Windows Event Viewer. For example, Application, Security, or System.
Workgroup	Filter by workgroup.

Vulnerabilities Smart Rule Filters

Child Smart Rule	Filter the vulnerabilities by child smart rules.
Vulnerability CVE	Filter the vulnerabilities by **Common Vulnerabilities** and **Exposures Indentifiers** (CVE ID).
Vulnerability fields	Filter by the vulnerability fields: **Vulnerability Name**, **Description**, and **Solution**.
Vulnerability has exploits	Filter on vulnerabilities where exploits exist.
Vulnerability has mitigation patch	Filter by patch updates that are available to remediate the vulnerability. Filter by: • **Type:** Select **Combined** to apply OS and application patches. Select **Individual** to apply a specific patch to either an OS or application. • **Name or url:** Enter a string that matches either the name of the patch or the URL for the patch remediation. For example, enter **MS12-068** (the patch name) or part of the URL: **https://technet.microsoft.com/en-us/library/security/ms12-068.aspx** • **Prerequisite:** Enter the CPE information that represents the fix for the vulnerability. Only CPE data for platforms is accepted. For example, **cpe:/o:microsoft:windows_server_2003::sp2:x32**. • **Platform:** Enter the operating system that the mitigation patch applies to.
Vulnerability in audit group	Filter by audit group. For example, **All Audits**, **Zero-Day**, or any of the compliance audit groups available.
Vulnerability severity	Filter by severity level: • Low • Information • Medium • High
Vulnerability version updated	Filter on vulnerability version. Any audits that are updated through auto update are detected when the smart rule processes. Use with the send email alert action to receive an email notification when updated audits are available. The email will list updated audits. ***Note:** The **Send email alert** action is only available with this filter.*
Zero-day vulnerabilities	Filter on zero-day vulnerabilities. Include or exclude the vulnerabilities from the smart rule.

Predefined Smart Group Categories

Agents and Scanners	Detects assets where protection agents and BeyondInsight 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 yesterday, and mobile assets with critical vulnerabilities. Intelligent Alerts are inactive by default.
SCCM	Includes smart groups for systems managed by Microsoft System Center Configuration Manager. You can configure these smart groups to synchronize with SCCM every X hours.
Servers	Includes smart groups that detect assets that are mail servers, web servers, database servers, domain controllers, and SCADA. 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 are part of 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 therefore, not included in the smart group. For example, the asset might be a router or unknown and will not be part of the smart group.

Predefined Smart Groups for Vulnerabilities

All Vulnerabilities	Includes all assets where there are vulnerabilities detected.
Non Zero-Day Vulnerabilities	Includes all assets with non zero-day vulnerabilities.
Zero-Day Vulnerabilities	Includes all assets where zero-day vulnerabilities are detected.

Create Smart Rules

You can configure an asset 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 environmental metrics for CVSS scoring
- Set scanner pooling

Create an Asset Based Smart Rule

1. In the BeyondInsight console, click **Smart Rules** on the left menu.
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:

Assign to Host Scan Group	Select to create a smart group to apply to a selected Host Scan Group.
Create Ticket	Select tickets parameters, including ticket assignment, severity, and email alert.
Deploy PB Policy	Select to deploy Endpoint Privilege Management policies to the assets that match the criteria selected in the Smart Rule.
Enable for Patch Management	Select to create a smart group for managing patch updates to assets.
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 will no longer be displayed on the Assets page or in reports.
Remove from Host Scan Group	Select to create a smart group to remove assets from selected Host Scan Group.
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 Environmental CVSS Metrics	Select environmental metrics for CVSS.

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, applying protection policies, and registering for patch updates.

9. Click **Save**.

Create a Vulnerabilities Based Smart Rule

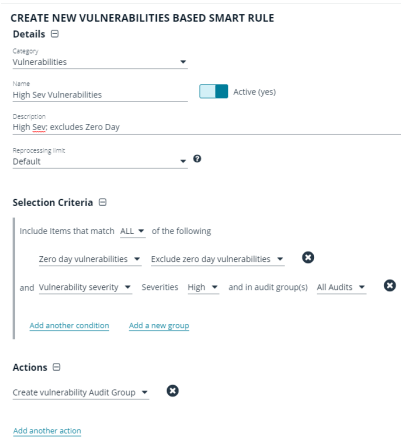
You can configure a vulnerabilities based smart rule to manage vulnerabilities.

1. In the BeyondInsight console, click **Smart Rules** on the left menu.
2. From the **Smart Rule type filter** list, select **Vulnerabilities**.
3. Click **Create Smart Rule**.
4. Enter a name and description.
5. 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.
6. Select the filters in the **Selection Criteria** section.
7. From the **Actions** section, select one of the following:
   - **Create Vulnerability Audit Group:** To create a read-only audit group.
   - **Show Vulnerability as Smart Group:** When selected, the rule is displayed on the **Vulnerabilities** page as a filter for the list of assets selected in the Smart Groups browser pane.
   - **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 vulnerabilities that match the rule is changed from the last time the rule was processed.
8. Click **Create Smart Rule**.

Example:
Create a vulnerability based smart rule that filters high severity vulnerabilities and excludes zero-day. Save the smart rule as an audit group.

Run a report and select the audit group for the smart rule. The report generated will display all high severity vulnerabilities and details for assets with the vulnerabilities.

*The **Audit Groups** filter is available with most vulnerability reports. Vulnerability based smart rules that are configured as an audit group will be available in the **Audit Groups** filter for these reports.*



Perform Other Smart Rule Actions

Clone a Smart Rule

You can clone custom or predefined smart rules.

1. In the BeyondInsight console, click **Smart Rules** on the left menu.
2. Select the smart rule you wish to clone, click the **More Options** button, 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. On the **Smart Rules** page, select the newly cloned smart rule, click **More Options > View Details**, and then edit the smart rule filters as needed.
5. Click **Save Changes**.

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. In the BeyondInsight console, click **Smart Rules** on the left menu.
2. Select the smart group or multiple smart groups, and then click **Deactivate** above the grid.

Delete a Smart Rule

1. In the BeyondInsight console, click **Smart Rules** on the left menu.
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 Processing

A smart rule processes and updates information in smart groups when certain actions occur, such as the following:

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

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

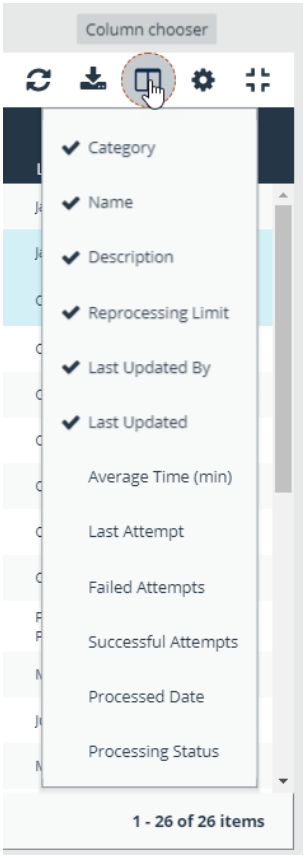
- A smart rule with smart rule children triggers the children to run before the parent completes.
- Managed account smart rules with selection criteria **Dedicated Account** will process when a change to a mapped group is detected. This can occur in the following scenarios:
    - A new user logs on.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

View and Select Smart Rules Processing Statistics

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

To add this information to the grid:

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



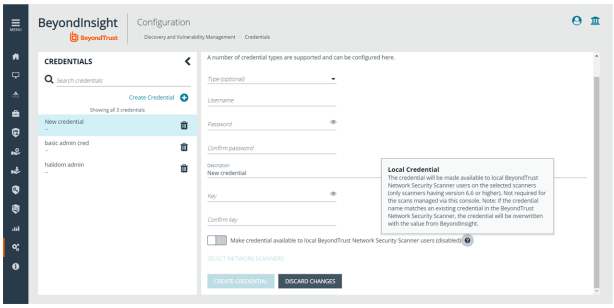
Add Credentials for Use in Scans

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 and Vulnerability Management > Credentials**.
2. Click **Create 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 • Key • Confirm Key
MySQL	• Username • Password • Confirm Password • Description • Key • Confirm Key

Oracle	• Username • Password • Confirm Password • Description • Access Level • Connect To • Protocol • Port Number • Key • Confirm Key
SNMPv2	• Description • Key • Confirm Key • Community String
SSH	• Authentication Type • Userrname • Password • Confirm Password • Description • Key • Confirm Key • Elevation
Windows	• Domain *(Optional)* • Username • Password • Confirm Password • Description • Key • Confirm Key

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

- "Create SSH Credentials" on page 65
- "Create Oracle Credentials" on page 63
- "Create SNMP Credentials" on page 64

5. If you would like this credential to be used for scanning by selected network scanners, click the toggle to make it available, and then select the scanner.

Tip: *This feature propagates credentials stored in Vulnerability Management to network 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.*

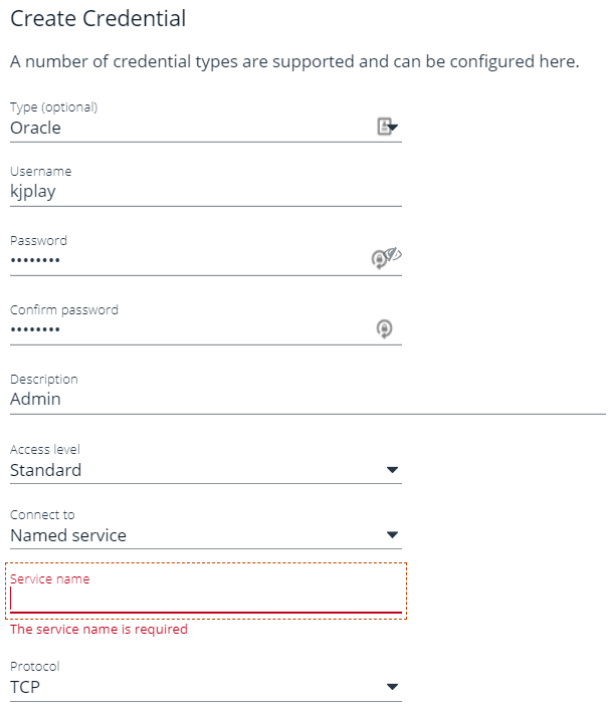
If the credential name matches an existing credential in the BeyondTrust Network Security Scanner, the credential is overwritten with the value from BeyondInsight.

6. Click **Create Credential**.

Create Oracle Credentials

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

1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Credentials**.
3. Click **Create Credential**.
4. From the **Type** list, select **Oracle**.
5. Provide a **Username**, **Password**, and **Description**.
6. Select an **Access level** from the list: **Standard**, **SYSDBA**, or **SYSOPER**.
7. Select additional connection options:
   - **Connect To:** Select from: **Database** or **Named Service**.
   - **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.
   - **Port Number:** Enter a port number.



> ***Note:*** *IPv4 addresses, IP address ranges, CIDR notation, and Named hosts are supported formats. Multiple SIDs, Named Services, TCP Ports or Pipe Names are not supported.*

8. Enter a key.
9. If you would like this credential to be used for scanning by selected local scanners, click the toggle to make it available and then select the scanner.

> ***Tip:*** *This feature propagates credentials stored in Vulnerability Management to network 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 BeyondTrust Network Security Scanner, the credential is overwritten with the value from BeyondInsight.*

10. Click **Create Credential**.

Create SNMP Credentials

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

1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Credentials**.
3. Click **Create Credential**.
4. From the **Type** list, select **SNMPv2**.
5. Enter a **Description**, **Key** and **Community String**.
6. If you would like this credential to be used for scanning by local scanners, click the slider to make it available and then select the scanner.

Tip: *This feature propagates credentials stored in Vulnerability Management to network 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 BeyondTrust Network Security Scanner, the credential is overwritten with the value from BeyondInsight.

7. Click **Create Credential**.

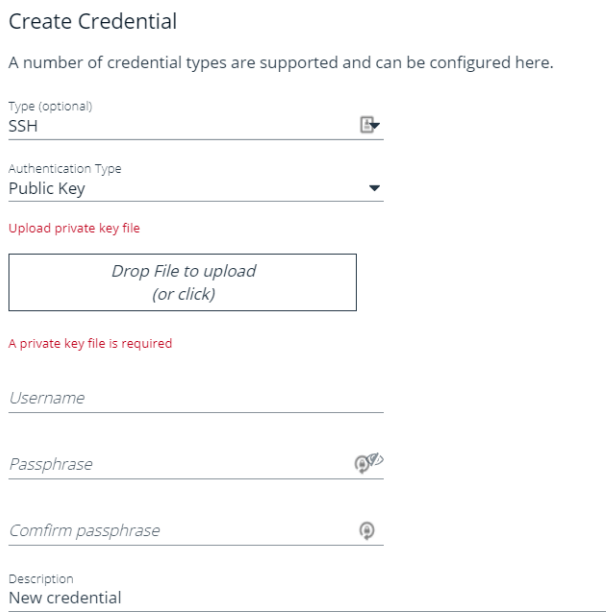
Create SSH Credentials

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 sudo to 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 for Unix and Linux target assets.

1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Credentials**.
3. Click **Create Credential**.
4. From the **Type** list, select **SSH** from the Type list.
5. 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.
6. Enter a **Description** and **Key**.
7. 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.
    - **pbrun:** Enter the pbrunuser username.
    - **Enable:** Enter the credentials for Cisco devices. If you are auditing Cisco devices, you can elevate the credentials to privileged for more thorough scans.



> ***Tip:*** *This feature propagates credentials stored in Vulnerability Management to network 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 BeyondTrust Network Security Scanner, the credential is overwritten with the value from BeyondInsight.*

8. Click **Create Credential.**.

Run Discovery Scans

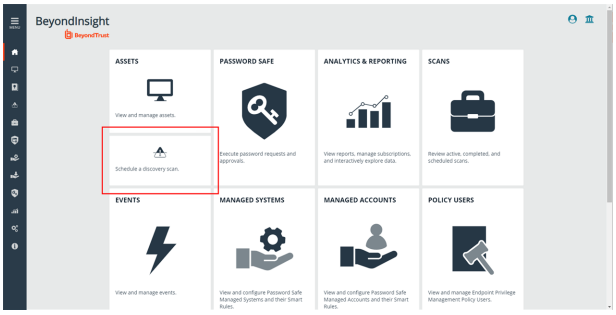
Run a discovery scan to locate network assets, such as workstations, routers, laptops, and printers. A discovery scan also determines if an IP address is active. You can periodically repeat discovery scans to verify the status of devices, programs, and the delta between the current and previous scans.

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

- The default TCP discovery ports are 21,22,23,25,80,110,139,443,445,554,1433, and 3389.
- Use more than one scanner to distribute the coverage across the network.

Use the Scan Wizard to Create a Discovery Scan

To run the scan wizard, click **Schedule a discovery scan** on the homepage, then follow the steps outlined below.



1. **Select Scan Type**: There are three types of scans to chose from. Select one and then click **Next**.
    - **Discovery Scan**: This is an uncredentialed scan that returns discovered assets. This type of scan does not collect any details on each of the assets, nor does it deploy any agent to the targets.
    - **Detailed Discovery Scan**: This scan requires credentials and it deploys a scan agent to the scan targets. Besides systems, this scan provides associated information on services, scheduled tasks, users, and databases.
    - **Advanced Discovery Scan**: This scan performs all the operations of the previous scan, but provides information on all associated attributes.
2. **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. If you wish to target existing assets or smart rules, this can be done from each of those product areas by using the grid actions to trigger a scan for a selected target.
3. **Enter Credentials**: If the type of test you selected requires credentials, you can select an existing credential from the **Credential List**, and/or use the **Custom Credential** fields to enter a new credential to use for this scan. If you enter a new credential, click **Test Credential** to verify its functionality. If using the Credential List, you have several options:
    - **Use the same key for all credentials**: If selected, enter a Universal Configuration Key, which will be used for all the credentials used in this scan.

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

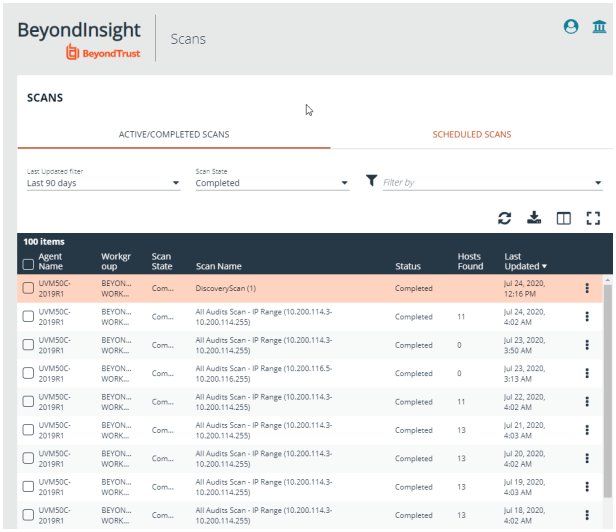
    - **Choose Existing Credentials**: You can use the search field to search for a specific credential, or select from a list of available credentials. You can select one or more. If necessary, enter the key and click **Validate**. Click **Next** to continue.
4. **Choose Scan Agent**: Select which agents will be 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.

5. **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:

   [' $ < + ? > * | " : ; \ /

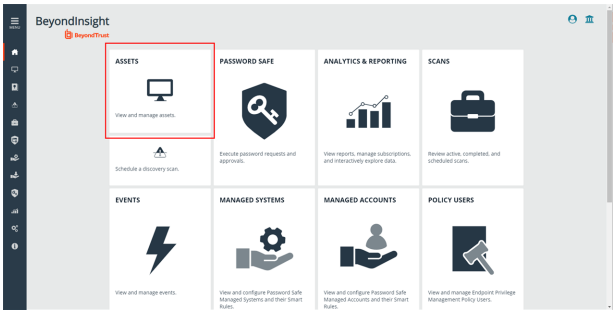
   You can also apply **Job Restrictions** that allow you to abort the scan if it runs longer that a set number of minutes, and set a **Schedule**, which can be **Immediate**, **One Time**, or **Recurring**. Click **Finished** to run the report.

On the **Scans** grid page you can see **Active** or **Completed** scans, delete a scan, and see a list of **Scheduled Scans**, if available. For each of the scheduled scans you can click on the vertical ellipsis icon at the end of the row to **View Scan Details**, or to **Delete a scan**. In **Scan Details** you can modify the target **Smart Rule**, the name of a scan, the scheduled scan time, change the credentials, and see the scan **History**, if that scan was run in the past.

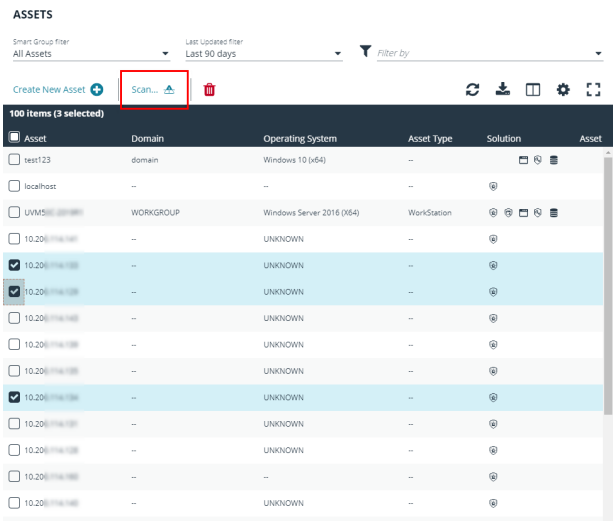


Run Scans from a List of Assets

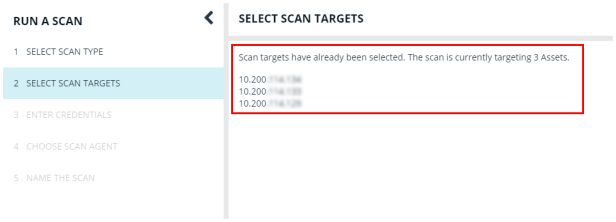
If you want to run a scan but would prefer to just select targets from a list of assets instead of typing them, click the **View and manage assets** tile.



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

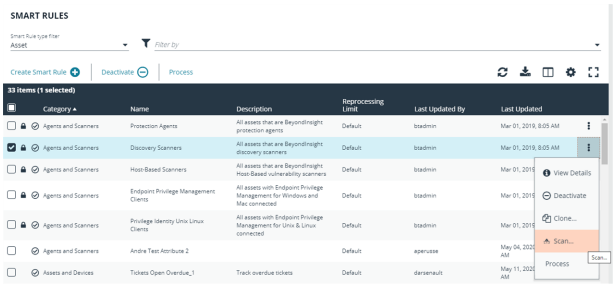


The scan wizard screen appears. Here you can select the type of scan to run. The difference is that when you click **Next** and go to the **Select Scan Targets** page, you will find the targets already selected. The next steps in the Scan Wizard are the same as those outlined above.



Use Smart Rules as Targets for Scans

You can also run a scan on smart rules. From the **Smart Rules** grid, select a rule and use the dropdown menu on the right side of the column and select **Scan**. You are taken to the scan wizard, where you will find the targets preselected. The next steps in the Scan Wizard are the same as those outlined above.



Check Completed Scans

If you want to check information on scans, click the **Menu** icon on the left navigation bar. Under **Scans** you can see links to **Active/Completed Scans** and to **Scheduled Scans**. Alternatively, you can access the list of scans by clicking the briefcase icon on the main page.

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.*

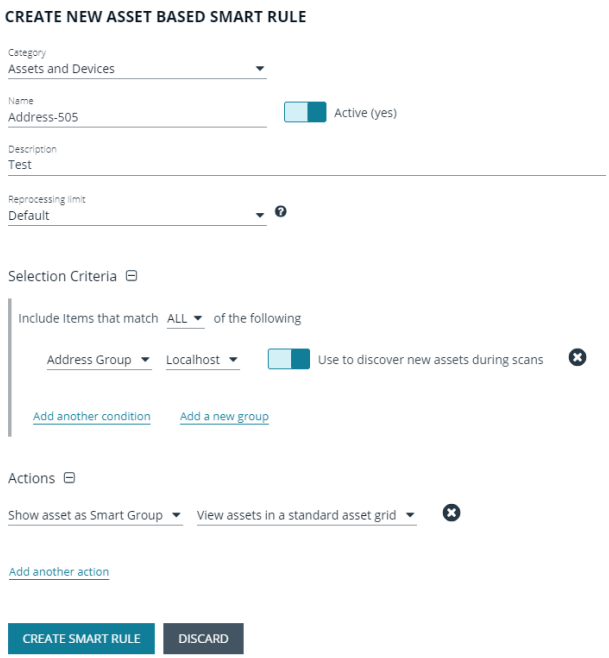
Key Steps

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.

> For more information, please see the following:
> - "Create a Directory Query" on page 47
> - "Create an Address Group" on page 44

- Create a smart group that includes the address group or query as the filter. Enable the **Use to discover new assets during scans** option.



> ***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.*

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
- View reports associated with the scan

Manage Assets

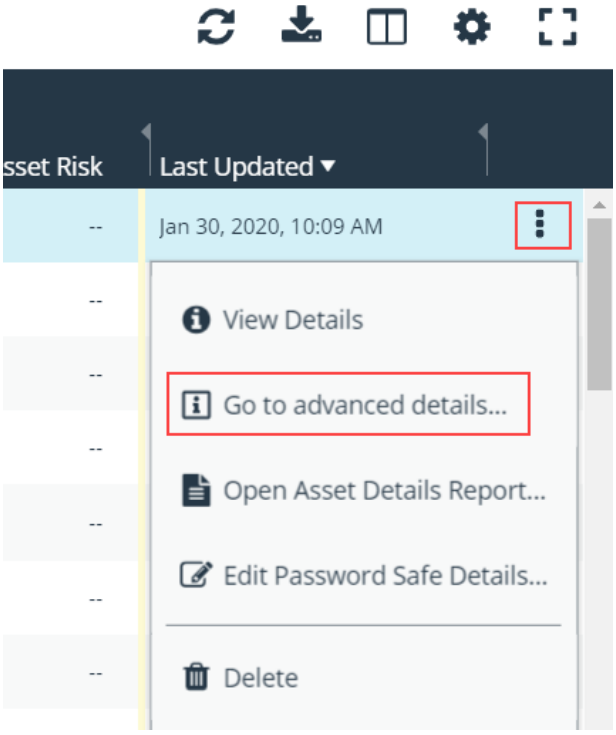
The Assets grid allows you to review details about your assets quickly by filtering your assets by smart groups, last update time, type of asset, domain, operating systems, technical solutions applied to the asset (i.e. asset is a scanned host or database host), DNS name, and workgroups,

Review Asset Details

> ***Tip:*** *Depending on the scan settings, information in the following list may 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****, and* ***Enable Remote Registry Service.***

You can review the following information about your assets on the advanced details page for each asset. To view the advanced details for an asset:

- In the grid, click the **More Options** button for an asset, and then select **Go to advanced details**.



> ***Note:*** *If the asset has not been scanned, you will only see information under* ***General Data****.*

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, and the operation system, etc.

- **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

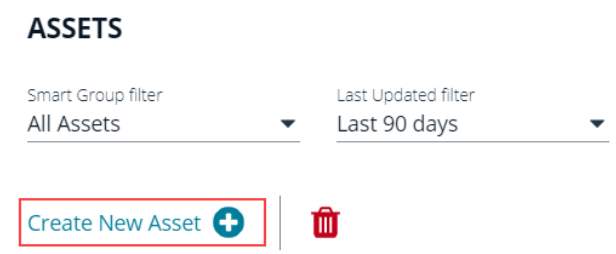
> ***Note:*** *By default, the current snapshot of scan data is selected. You can select other available snapshots to load the data for that date.*

- **Certificates:** Displays all certificates installed on the asset. You can filter by expired certificates or search for certifcates.
- **Hardware:** Displays disk drive information, system manufacturer, memory, and processor information.
- **Ports:** Displays the open port number, protocol, and description.
- **Processes:** Displays all the running processes and includes the PID and name of the process.
- **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, log on details, startup type, and dependencies.
- **Shares:** Displays the name and description of the shares on the asset.
- **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.

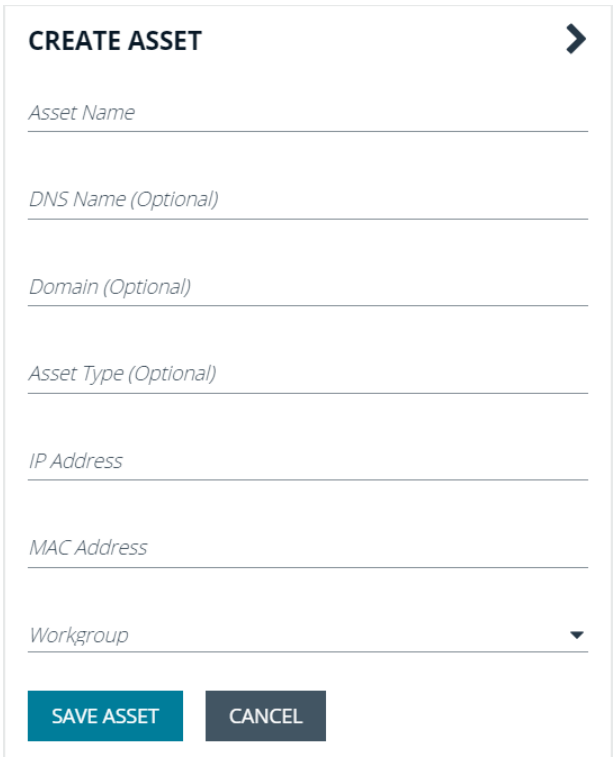
Create Assets

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

1. Select **Assets**.
2. From the **Smart Group Filter**, select **All Assets**.
3. Click **Create New Asset**.



4. Complete the **Create Asset** form, and then click **Save Asset**.



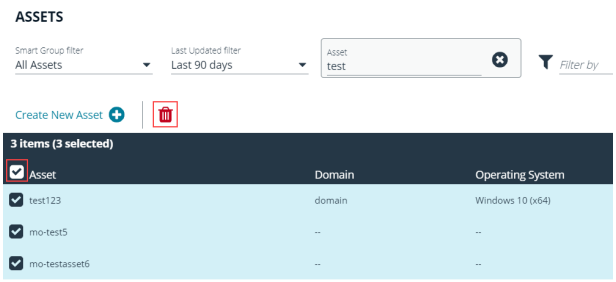
> ***Note:*** *New assets created in any smart group other than **All Assets** may not appear under the selected smart group if the smart rule criteria is not met or until the smart rule processes. We recommend that you create new assets using the **All Assets** smart group.*

> ***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 will be deleted from the BeyondInsight database during the nightly data purge.

1. Select **Assets**.
2. 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 select the check box in the header to select all assets in the grid to delete at once.*

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

Run Scans on Cloud Platforms in BeyondInsight

You can run scans on the following cloud types: Amazon EC2, VMware vCenter, 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 will extract virtual machines and load balancers from Resource Manager. You must create an Azure Active Directory application.

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**.

VMware vCenter Requirements

You can scan VMware virtual machines. Ensure the following requirements are in place before you configure the VMware connector in BeyondInsight.

- Network Security Scanner 5.17 or later
- BeyondInsight 3.5 or later
- **VMware Tools** must be installed on the targets that you want to scan.
- Log into the VMware website and download the **Virtual Disk Development Kit (VDDK)**: https://www.vmware.com/support/developer/vddk/
- Network Security Scanner supports only version 5.1 of the VDDK. Ensure you copy the following file: **VMware-vix-disklib-5.1.0-774844.i386.exe**.
- Run the VDDK installer on the scanner computer using local administrator credentials.
- BeyondInsight needs access to **https://<VMware server>/sdk** through port **443**.

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**
    - **VMware vCenter Scan Target Collector**
4. Enter the connector information:
    - For AWS cloud connections, required fields are: **Provider**, **Region**, **Access Key ID**, and **Secret Access Key**.

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

    - For Azure, required fields are: **Region**, **Client ID**, **Client Information**, **Tenant ID**, and **Subscription Information**.
    - 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) and logon credentials.
    - For Rackspace, required fields are **Account Type**, **Username**, and **API Key**.
    - For VMware, required fields are **Server** (https://[server]/sdk), **Username**, and **Password**.
5. After you configure the connector, click **Test Connector** to ensure the connector works.
6. 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..

Scan Paused or Offline VMware Images

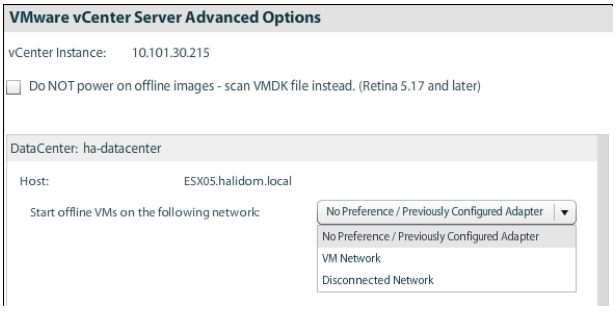
By default, paused or offline VMs are turned on during a scan. After the scan runs, the VMs are reverted to the paused or offline state.

If you suspect that a VM is at risk, you can turn on the VM in another secure network where other VMs will not be under potential threat. The scan runs as usual, and then the VM is reverted to the paused or offline state.

When creating the connector, click the **Advanced** button. You can configure each host that is a member of the vCenter instance.

The option that you select applies to all VMs on the host.

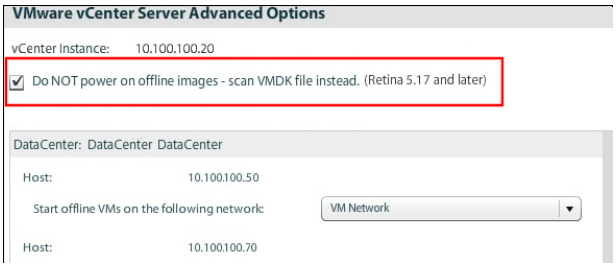
The advanced options dialog box varies depending on your vCenter configuration. The list of available options includes all other networks configured for your vCenter instance or on your ESX server.



Scan VMDK Files

You can scan a VMDK file rather than turning on a VM. Make sure you check the option **Do NOT power on offline images - scan VMDK file instead**.

Scan times are faster when VMs remain powered off. However, scan results might differ from scan results for VMs powered on (for example, open ports and running processes might not be detected for VMs powered off).



Cloud Connector Smart Groups

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

1. Select **Assets** from the menu.
2. Click the **Manage Smart Rules** link.
3. Click **Create Smart Rule**.
4. Select a category, and then enter a name and description.
5. Under **Selection Criteria**, select **Cloud Assets**, and then select the cloud connector type to filter on (**Amazon**, **Azure**, **Hyper-V**).
6. For the Amazon AWS, Azure, and Google Smart Groups, select the **Use Private IP Address** check 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 more options icon 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 into 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)

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

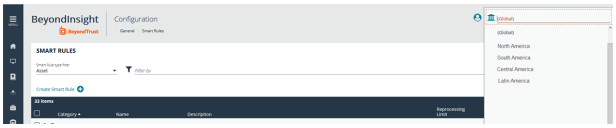
The multi-tenant feature in BeyondInsight allows you to define multiple organizations (or tenants) where each organization's asset data is kept isolated from all other organizations. Only smart rules marked as **Global** can combine asset data across multiple organizations.

Most BeyondInsight features are available with multi-tenant, including smart rules, the patch management module, and mobility 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.



When you initially create an organization, both the default and the new organization is provisioned with the **All Assets** smart rule.

Create smart rules as usual. For more information, please see "Use Smart Rules to Organize Assets" on page 51.

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 Network Security 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.

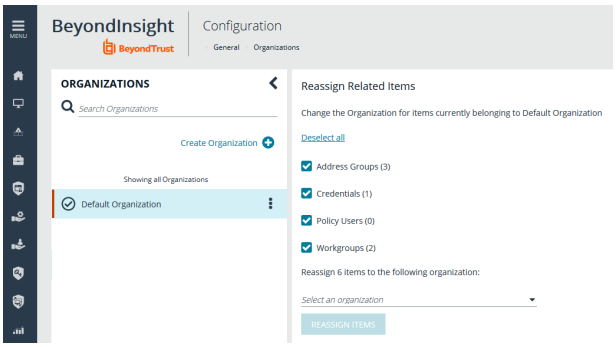
Address Groups

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:

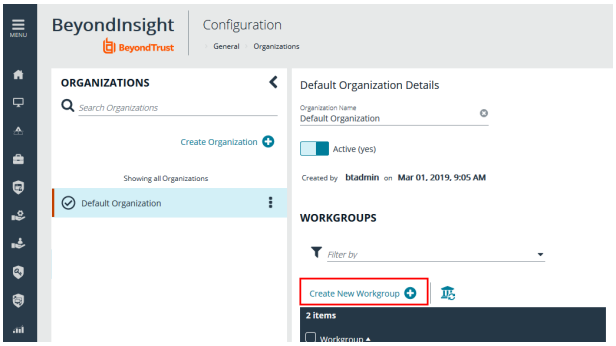
- Single IP address
- IP range
- CIDR notation
- Named hosts

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:

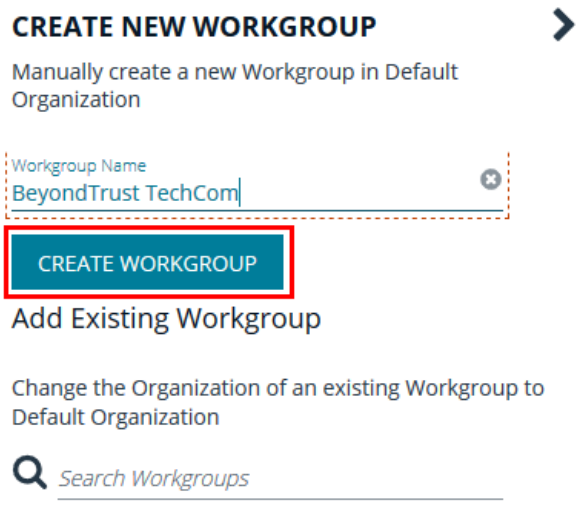
- Currently selected Smart Group
- Currently selected Assets

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.

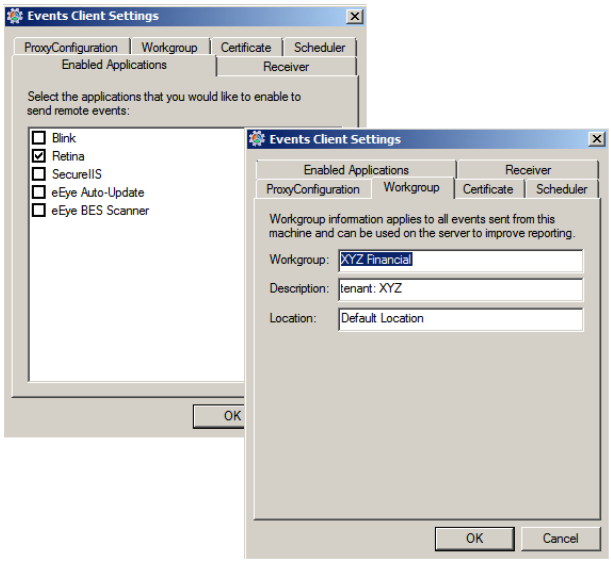
Each Network Security Scanner must be assigned a workgroup. A workgroup is typically created when the agent is initially deployed.

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 Network Security 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 into 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.

> 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 17.

As a security measure, a tenant cannot log into BeyondInsight.

Set BeyondInsight Options

Set Account and Email Options

> If you use Clarity, for configuration information please see the BeyondInsight Analytics and Reporting User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm.

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.
    - **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 will remain 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 will be 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 will send 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.*

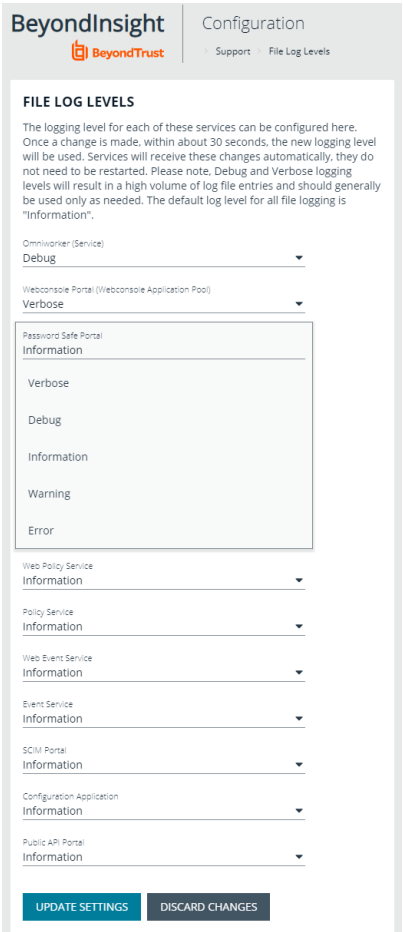
Set Support Options

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.

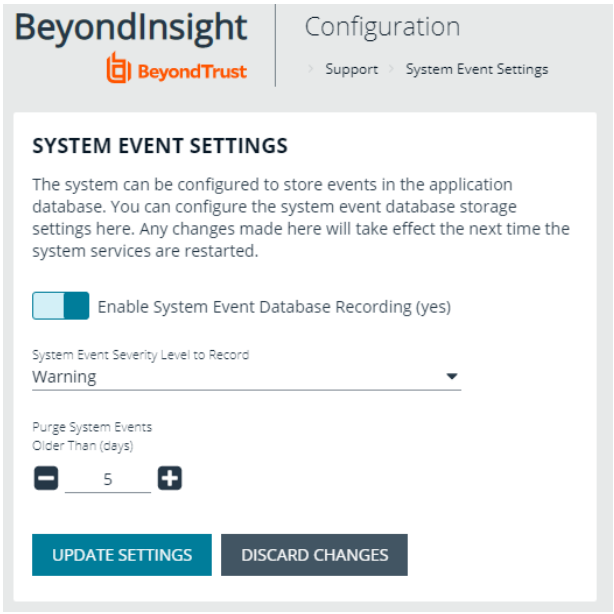


Enable System Event Recording

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**.

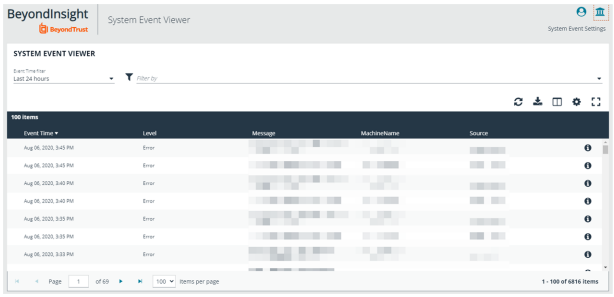
> ***Note:*** *Once events are purged, they are not available in the* ***System Event Viewer****.*



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.

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 vulnerabilities older than	Previously found vulnerabilities are stored in the database until fixed and rescanned or purged. However, this can vary for different environments. Once the data is purged, the vulnerabilities are removed from the database. **Recommended: 90 days**
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 vulnerability agent jobs every N days	When enabled, sets the number of days to keep the vulnerability 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.
PurgeEndpoint 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 will 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.**

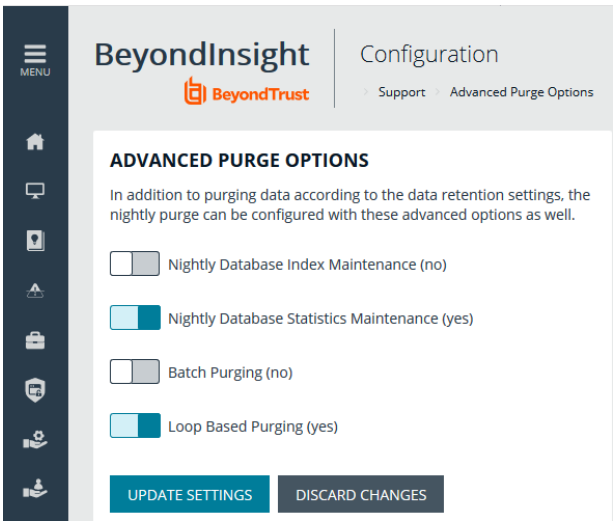
> ***Note:*** *The data in the scan file is not purged.*

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:

- **Nightly Database Index Maintenance (no)**
- **Nightly Database Statistics Maintenance (yes)**
- **Batch Purging (no)**
- **Loop Based Purging (yes)**



Configure Proxy Settings

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

1. Select **Configuration**.
2. Under **System**, select **Proxy Settings**.
3. Click the slider to **Enable proxy support**.
4. Enter the IP address or domain name of the proxy server, username, and password for the proxy server.
5. Click the slider to override any local proxies.
6. Click **Update Proxy Settings**.

Configure Discovery and Vulnerability 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 will 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 and Vulnerability 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 Vulnerability Aging

Set the number of days before older vulnerabilities are tagged as **Fixed**. Generally, this setting should be slightly longer than the typical scan frequency.

1. Select **Configuration > Discovery and Vulnerability Management > Options**.
2. Under **Vulnerability Aging**, set the number of days to pass before marking aged vulnerabilities as fixed, and then click **Update Vulnerabilities Aging Options**.

Enable Dynamic Workgroup Assignment for Multi-tenant

For multi-tenant installs, you can enable **Dynamic Workgroup Assignment** to allow for specific work groups to be scanned.

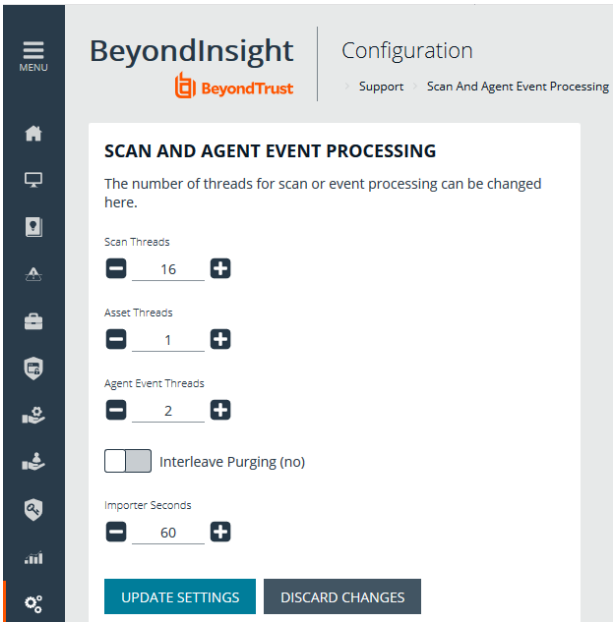
1. Select **Configuration > Discovery and Vulnerability Management > Options**.
2. Under **Multi-tenant**, click the slider to enable **Dynamic Workgroup Assignment**, and then click **Update Multi-tenant Options**.

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 Endpoint Privilege Management event processing and **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 Website Options

You can configure global website settings, including:

- Changing the **Login** page to include domain and LDAP menu items
- 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
- Setting the number of records to display in the console grids
- Configuring session options
- Turning on language selection

List Domains and LDAP Servers on the Login Page

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

***Note:** The log into list is only displayed on the **Login** page when there are either Active Directory user groups 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, disable the setting.*

1. Select **Configuration**.
2. Under **System**, select **Site Options**.
3. Under **Login Page**, click the slider to disable **Show list of domains/LDAP servers on login page**.
4. Click **Update Login Page Options**.

You will need to 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. Select **Configuration**.
2. Under **System**, select **Site Options**.
3. Under **Login Page**, click the slider to disable **Show Forgot Password link on login page**.
4. Click **Update Login Page Options**.

You will need to 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. Select **Configuration**.
2. Under **System**, select **Site Options**.
3. Under **Login Page**, click the slider to turn off **Show social media links on login and about pages**.
4. Click **Update Login Page Options**.

You will need to 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. Select **Configuration**.
2. Under **System**, select **Site Options**.
3. Under **General**, set the number of minutes for **Maximum smart rule refresh frequency for asset updates**. The default is **60**.
4. 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. Select **Configuration**.
2. Under **System**, select **Site Options**.
3. Under **Pre-Login Banner**, click the slider to enable the **Show Banner**.
4. Provide a title and message, and then click **Update Pre-login Banner Options**.

Configure Session Options

You can configure the following session related options on the **Options** page:

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

Note: *The default session timeout period is 20 minutes, as specified in the configuration tool. If you wish to lower the session timeout period, please contact BeyondTrust Technical Support*

1. Select **Configuration**.
2. Under **System**, select **Site Options**.
3. Under **Session**, set the following:
    - **Notification time before session timeout:** Sets the amount of time, prior to the session timing out due to inactivity, that the system will notify the user that their session will timeout shortly.

- **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.

4. Click **Update Session Options**.

Enable the Language Menu

The management console can be viewed in the following languages:

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

The **Language Settings** menu is accessed from the **Settings** icon in the console and also at the bottom of the **Login** page.

***Note:** By default, the Language Settings menu is not displayed.*

1. Select **Configuration**.
2. Under **System**, select **Site Options**.
3. Under **Localization**, click the slider to enable the **Show Language Picker**.
4. Click **Update Localization Options**.

***Tip:** Console users can select a language from the **Settings** menu and also from the bottom of the **Login** page. After the setting is enabled, the user must log out of the console and then log back in.*

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 and
- 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 in 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 Network Security 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 Network Security Scanner
- Password Safe
- Third Party Imports

Configure BeyondInsight Clarity Analytics

To work with BeyondInsight Clarity, you must configure the following settings.

1. Select **Configuration**.
2. Under **Analytics & Reporting**, select **Clarity Analytics**, and the set the following:
    - **Enable Analytics:** Check the box to turn on the BeyondInsight Clarity feature.
    - **Time to run (hours, minutes):** Set the time to run the data collection.
    - **Frequency to run Analytics:** Set the frequency to run analytics.
    - **Alert Threshold:** The threshold for flagging explicit alerts. The higher the value the higher the sensitivity and fewer flagged alerts. The range is between **0 – 1**. The default value is **0.65**.
    - **Som Probability Threshold:** The threshold for flagging pattern alerts. The range is between **0 – 1**. The lower the value the higher the sensitivity and fewer flagged alerts. The default value is **0.05**.
    - **Send notification to:** Enter an email address. An email is sent to the recipient after the analytics processing is complete. A summary of the analysis is included in the email.
    - **Alert malware confidence level:** Select a confidence level from the list. The default value is **Medium**. Use the setting to filter on the higher potential malware risks that are presented in the analytics data.

Set Risk Analytics Values

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

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.

Using the analysis influence 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 would be given greater weighting in the final risk calculation and increase an asset's risk score.

Note: *Analysis influence is only available for log calculations.*

Clarity Reports

The following reports are available to run against the cluster map data:

- **Event Review - Attacks:** Breakdown of alert triggers for attack events by threat level.
- **Event Review - Malware:** Breakdown of alert triggers for Malware events by threat level. This report can be used to display Clarity Malware events from BeyondInsight.
- **Event Review - Privilege Management for Windows:** 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 release events by threat level.
- **Event Review - Privilege Management for Unix & Linux** 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 - Scanner:** Breakdown of alert triggers for agent events by threat level. Includes relevant event details, and is ordered by threat level from largest to smallest.
- **Highest Populated Clusters:** Lists the most populated clusters.
- **Lowest Populated Clusters:** Lists the clusters with the least assets.
- **Top 10 Assets by Cluster Movement:** Displays differences in an asset's cluster assignment. Shows items by size of move (distance between clusters) and time frame (fast or slow). The time frame can indicate that an asset is an outlier if the changes occur quickly.
- **Top 10 Assets by Total Threat Level:** Displays top 10 assets based on overall threat level. This report can be used to display Clarity Malware events from BeyondInsight.
- **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 Network Security Scanner

Triggers

The following triggers identify assets that are at risk.

Trigger	Description
Outlier	Can be triggered by events in the following products: • Endpoint Privilege Management • Privilege Management for Unix & Linux • Password Safe • BeyondTrust Network Security Scanner • Malware and attack data from other solutions.
Untrusted Application	Endpoint Privilege Management events. Triggers in the following cases: • Application is unsigned • Application has no version information
Vulnerable Application	Endpoint Privilege Management events
Asset Risk Exceeds Threshold	Can be triggered by events in the following products: • Endpoint Privilege Management • Privilege Management for Unix & Linux • Password Safe • BeyondTrust Network Security Scanner • • Malware and attack data from other solutions.
Untrusted User	• Endpoint Privilege Management • Privilege Management for Unix & Linux • BeyondTrust Network Security Scanner
First Application Launch	• Endpoint Privilege Management • Privilege Management for Unix & Linux • User launches an application they have never launched before.
First Password Release Request	• Password Safe events.

	• User requests password for an account and system they have never requested before.
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. • User tries to acquire more than one password at a time.
Malware Detected	• Malware is detected on an asset.

The **Triggers** list displays the total number of events which are affected by each trigger. Click the **Trigger** link to list all of the events that make up the count. Event details include **Asset**, **Triggers**, **User**, **Description**.

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.

Risk Events by Application

Bubbles represent aggregated threat events. The data is displayed in a quadrant layout:

- The **X** axis indicates the average asset risk for each bubble.
- The **Y** axis indicates the average threat level for each bubble.

The location of the bubble indicates the level of risk. The highest risk assets are displayed in the upper right quadrant. Bubbles can be arranged by the following:

- **Asset:** Displays a bubble for each of the most active assets.
- **User** Displays a bubble for each of the most active users.
- **Application:** Displays a bubble for each high level threat data source application.

Drill into a bubble to learn more information, such as the event type or severity.

> ***Note:*** *The system restricts the number of bubbles for legibility.*

Use the **Tab** key to navigate through the areas on the page and to view the metrics on the bubbles.

View Cluster Maps

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

Attribute	Type	Description
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.

For more information, please see "BeyondInsight Clarity Analytics" on page 98.

The following procedure shows examples from asset clusters. The procedure and analysis is similiar 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 will be an outlier.
    - **Cluster Risk:** Clusters the assets based on the common risk characteristics. The larger tiles in the cluster map will 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 Applications:** 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 on 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.

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

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**, **MasterHost**, **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
a3	explicit	Vulnerable Application Vulnerability of launched application.
a4	explicit	Asset Risk
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

Alert	Type	Description
a7	explicit	First App Launch The alert is flagged when a user launches an application they have never launched before.
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.

BeyondInsight Clarity Malware Analysis

Clarity Malware evaluates events from BeyondTrust solutions and determines if there are any risks or malware associated with the events. Any malware detected is populated in the **Malware** tab of the **Assets** page on the BeyondInsight management console.

> ***Note:*** *By default, Clarity Malware is enabled.*

You can use the Clarity Malware Analysis tool to detect if any files are infected by malware or a virus. Two sources of data can be used to determine if malware is infecting files on your assets.

- **PowerBroker for Windows file hashes:** Create a policy in PowerBroker for Windows and apply the policy to the assets.
- **Network Security Scanner scans:** Only the **Service** and **All Audits** scans can be used with Clarity Malware. Create and run a scan using either the **Service** scan template or **All Audits** scan template

After you configure Clarity Malware and gather data, you can review the results on the **Malware** tab in the BeyondInsight management console.

Configure Clarity Malware

Allow up to 24 hours to pass before any data is populated in the BeyondInsight database.

1. Select **Configuration > Discovery and Vulnerability Management > Clarity Malware Options**.
2. Set the following:
    - **Enable Clarity Malware Analysis:** This controls whether or not Clarity Malware Analysis runs. The default setting is **Yes**. Setting it to **No** removes any previously detected malware from BeyondInsight and turns off analysis for future events.
    - **Time to run:** Sets the time of day at which you would like the Clarity Malware Analysis to run. The default value is **4 AM**. The first query starts at 4 AM after you initially install BeyondInsight. To change the time collection occurs, enter the number of minutes past midnight that you want collection to occur.
    - **Frequency to query:** Sets the desired Clarity Malware Analysis run frequency. Each time Clarity Malware Analysis runs it analyzes the events that have occurred since the previous run time. The default is every **4 hours**.
    - **Alert level:** Sets the minimum level required to trigger malware detection. This level comes from the Clarity Malware analysis. The lower the alert level, the more malware will be flagged. The higher the alert level, the less malware will be flagged. If unsure, start at a **Medium** level and adjust as needed.
3. Click **Update**.

Review Malware Information and Reports

The **Confidence Level** can be one of the following values:

- High
- Medium
- Low

The confidence level indicates the likelihood that the malware is a real threat to your environment. You can also use the **Malware Report** to view the information collected using Clarity Malware. You can review malware details by selecting an asset on the **Assets** page.

Use Reports to Analyze Results

You can use the **Malware Report** in the management console and the **Clarity Reports** in BeyondInsight Analytics and Reporting to analyze the collected information.

A daily sync job must be run to retrieve data from the BeyondInsight Analytics and Reporting database. The following reports in BeyondInsight Analytics and Reporting provide Clarity Malware details.

Top 10 Assets by Total Threat Level Report

In the chart area, each asset is displayed along with the total threat level and the severity level indicated by **I (Info)**, **L (Low)**, **M (Medium)**, or **H (High)**. The threat breakdown is presented in the lower section of the report. The Clarity Malware is indicated in red.

Click the **Overall Threat Level** link to view more information on the malware.

Event Review - Malware Report

Run the **Event Review - Malware Report** to view a list of assets and the malware detected on each asset.

Configure a Claims-Aware Website in BeyondInsight

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 will bypass the BeyondInsight login screen. If the user is new to BeyondInsight, they are created in the system using the same claims information. The user will also be 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

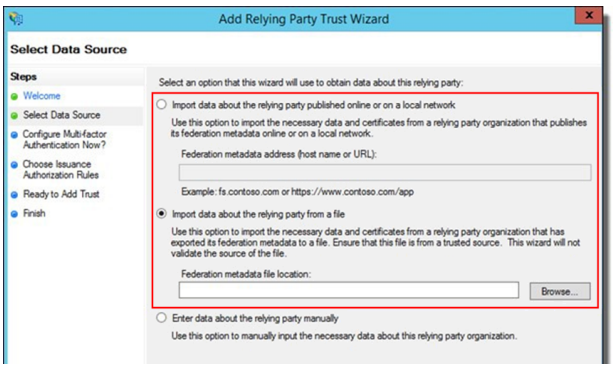
Create a BeyondInsight group and ensure the group is assigned the **Full Control** permission to the **Management Console Access** feature.

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.

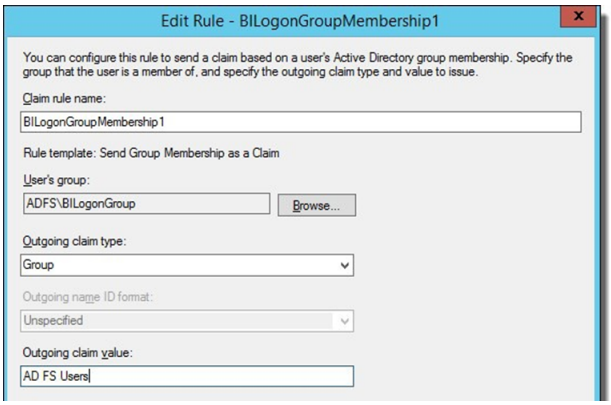
The metadata is located in the following directory:
<Install path>\eEye Digital Security\Retina CS\WebSiteClaimsAware\FederationMetadata\2007-06

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.*



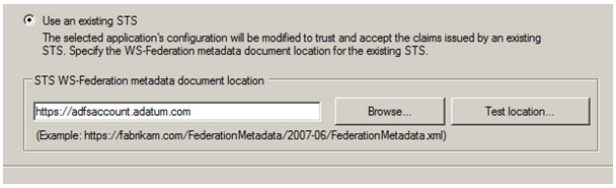
Supported Federation Service Claim Types

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 shows you 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 should automatically populate.
3. Click **Next**.
4. Select **Using an existing STS**.
5. Enter **Root URL of Claims Issuer** or **STS** .
6. Select **Test location**. **FederationMetadata.xml** will be 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**.

Manage Privilege Management for Unix & Linux, Essentials Edition Events

On the **Assets** page, you can review the run arguments and I/O logs captured for an asset that is running Privilege Management for Unix & Linux, Essentials Edition.

> ***Note:*** *PowerBroker for Unix & Linux has been renamed to Privilege Management for Unix & Linux. PowerBroker for Sudo has been renamed to Privilege Management for Unix & Linux, Essentials Edition, PBSudo Edition OR PMUL Basic.*

View Run Arguments and IO Logs

On the **Assets** page, you can review the run arguments and I/O logs captured for an asset.

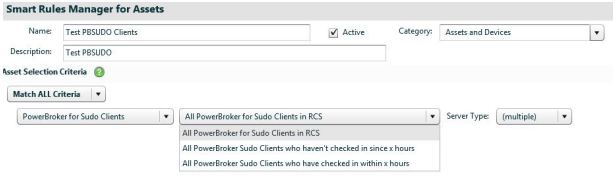
1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Select PowerBroker for Sudo from the list.
4. Click **i** for an asset.
5. Click the **Run Arguments** tab or **IO Logs** tab to view more information.

Create a Privilege Management for Unix & Linux, Essentials Edition Smart Group

You can create a Smart Group to organize Sudo assets. You can set filters based on assets and event types, including user name, command, exit status, and run arguments.

Create a Sudo Client Smart Group

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Manage Smart Rules**.
4. Select the Sudo clients that you want to include in the Smart Group data.
5. Select one of the following:
   - All Sudo clients
   - All Sudo clients that have not checked in
   - All Sudo clients that have checked in



6. Select the server type.
7. In the **Perform Actions** section, select **Show Asset as Smart Group**.
8. Click **Save**.

After the smart rule processes and the data is collected, you can view the details on the **Assets** page.

Create a Sudo Events Smart Group

1. Select **Assets**.
2. Click the **Legacy Assets View** link.

3. Click **Manage Smart Rules**.
4. Select the event fields that you want to include in the smart group data.
5. In the **Perform Actions** section, select **Show Asset as Smart Group**.
6. Click **Save**.
7. After the smart rule processes and the data is collected, you can view the details on the **Assets** page.
8. Go to the **Assets** page.
9. Click the **Legacy Assets View** link.
10. Select the smart group.
11. Select an asset and click **i**.
12. Click **PowerBroker for Sudo Events**.

Create Smart Rules for Endpoint Privilege Management Policy Users

You can manage user-based policies for Endpoint Privilege Management users with Smart Rules.

> ***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 into BeyondInsight to create applicable Smart Rules.

Create a Smart Rule

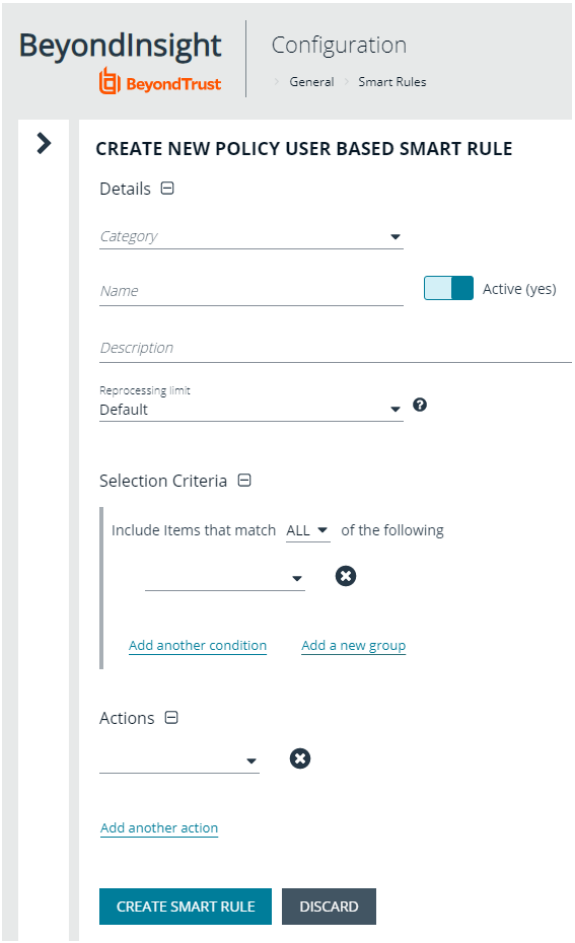
When a policy is deployed using a policy user-based Smart Rule, only the policy rules set in the **User Configuration Rule Management** section of the policy are processed by Endpoint Privilege Management clients that receive the policy. Policy deployment is controlled by the specifications in the Smart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

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

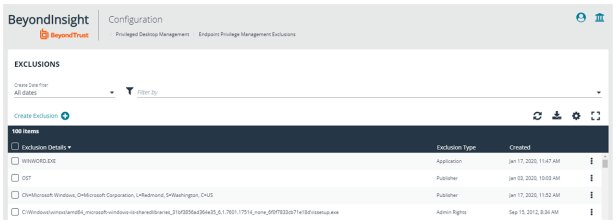
To view the page, select **Policy Users** on the **Home** page, or on the menu under **Endpoint Privilege Management.**

Endpoint Privilege Management Exclusions

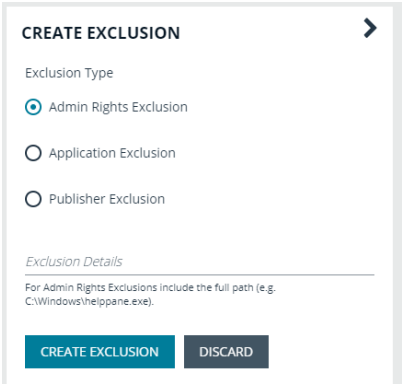
You can create and manage exclusions for Endpoint Privilege Management on the **Exclusions** page. Exclusions can also be created from events, on the **Events** page.

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

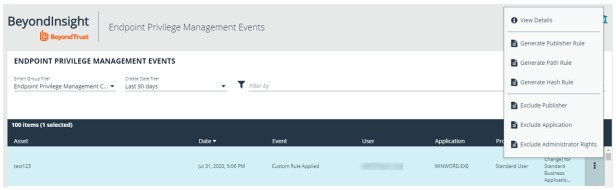
Create Exclusions



1. From the **Home** page in the BeyondInsight console, select **Configuration**.
2. In the Privileged Desktop Management pane, select **Endpoint Privilege Management Exclusions**.
    - This screen shows a list of existing exclusions.
    - At the top of the list, you can filter the exclusions by date, and/or by details or type.
    - You can sort by any column heading, by clicking on that 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 exclusions, and set the number to display per page.
3. Click **Create Exclusion +** .
    - Select the type.
    - Enter the details.
    - Click **Create Exclusion**.



Create Exclusion from Event



1. From the **Home** page in the BeyondInsight console, select **Events**.
2. For the desired event to exclude, click the vertical ellipsis at the right end of the line.
3. Click the appropriate exclusion type.

Manage Exclusions

For any exclusion in the list of exclusions, you can:

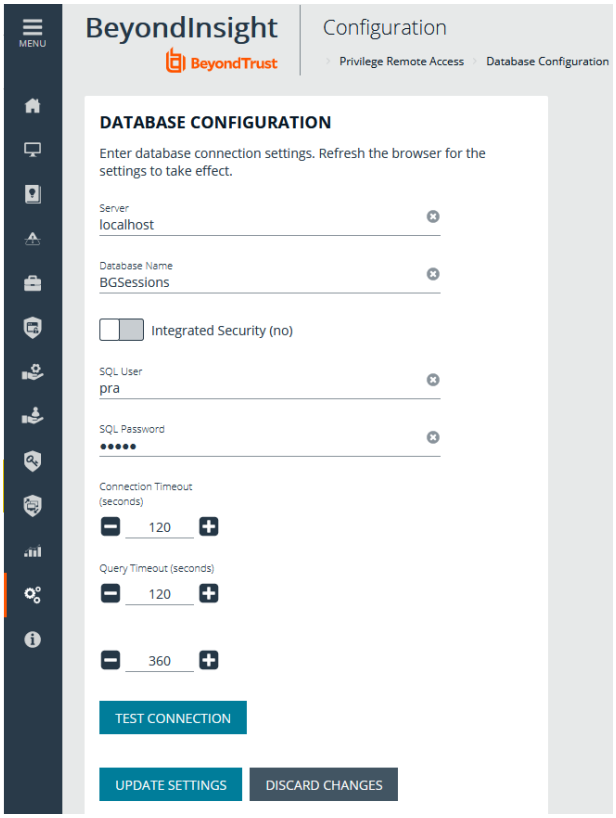
- Click the vertical ellipsis at the right end of the exclusion line to delete it, and confirm the deletion.
- Change the type or details and click **Save Exclusion**.

View Privileged Remote Access Session 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

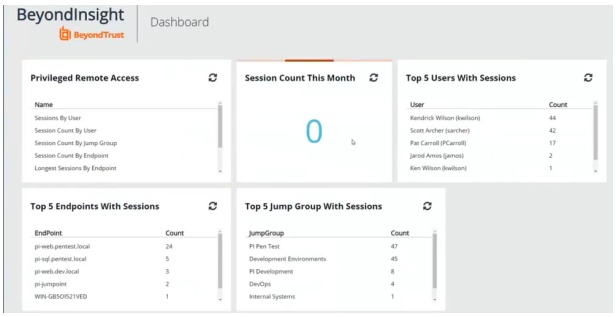
1. Select **Configuration**.
2. Under **Privileged Remote Access**, select **Database Configuration**.
3. Provide the settings to connect to your Privileged Remote Access export database, and then click **Test Connection**.
4. Click **Update Settings**.



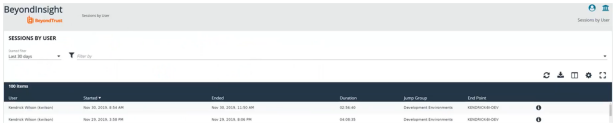
View the Privileged Remote Access Dashboard

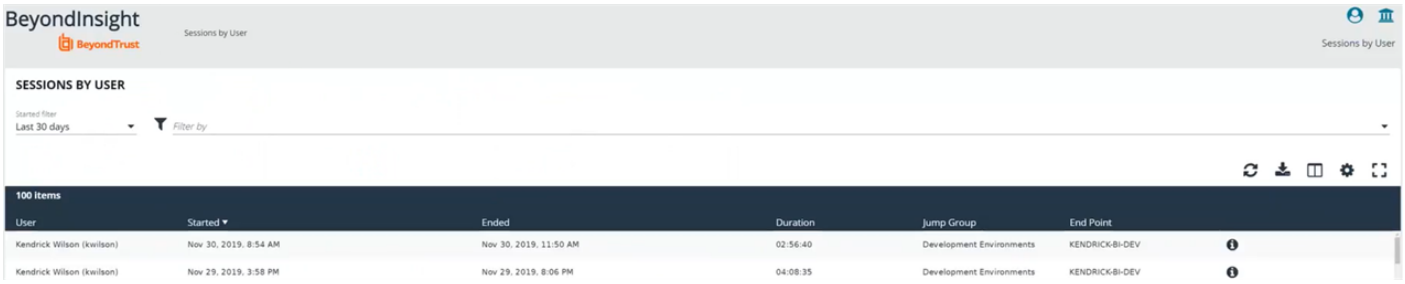
1. From the menu, select **Privileged Remote Access**.

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 Registration**.
2. Click **Create API Registration** to create a new application registration.
3. Enter a name for the new registration, and then click **Create**.

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

> ***Note:*** *Once the key has been changed, any script using the old key will receive a "401 unauthorized" error until the new key is used in its place. Read access and rotation of the key 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 iscomputed 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 will recompute the signature during factor validation and compare it against the one sent by the client. If the signatures matches, 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 will fail with a *401 unauthorized* error.
6. Click **Create Rule**.

Support and Product Updates

Send Files to BeyondTrust Technical Support

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 protection agents, 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 the menu, select **About**.
2. From **Support Tools > Download Support Package**, click **Generate Support Package**.
3. A .zip file is automatically created and saved to the **Downloads** folder.
4. 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 aged out agents
- Analysis of BeyondTrust components
- Customer name

To generate analysis files:

1. From the menu, select **About**.
2. 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 BeyondTrustUpdater.