BeyondTrust

BeyondInsight 21.3
Cloud User Guide

TC:12/9/2021

Table of Contents

BeyondInsight User Guide - Cloud Deployment

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

This guide provides instructions and procedures for using BeyondInsight.

Log In to 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.*

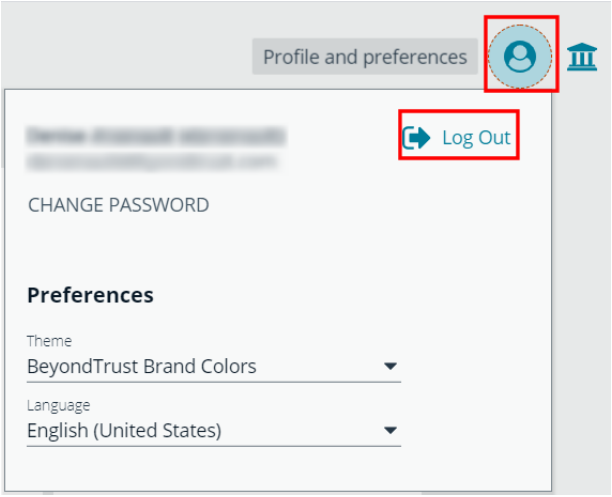
1. Open a browser and enter the URL for your BeyondInsight cloud instance.
2. Enter your username and password.
3. The default username is **Administrator**, and the password is the administrator password you set in the initialization email.
4. If applicable, select a domain.
5. Click **Login**.

***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.*

For more information, please see the Password Safe Administration Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm.

Log Out of the Console

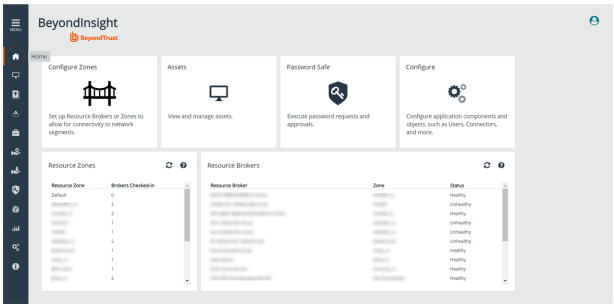
To log out of the console, click **Profile and preferences** in the top-right corner, and then click **Log Out.**



Navigate the Console

Once logged into Password Safe Cloud, you are taken to the **Home** page, where you can quickly access the following functionality from the container cards:

- Setup Resource Brokers and Zones to allow for connectivity to network segments.
- View and manage assets.
- Access Password Safe to execute password requests and approvals.
- Access configuration settings for BeyondInsight and Password Safe components and objects.



You can also view the following dynamically updated dashboard cards to see the most recent information for your Resource Zones and Resource Brokers:

- List of Resource Zones and how many Resource Brokers are checked in for each zone
- List of Resource Brokers, along with the Zone they are in, and their health status

To access the suite of features in the BeyondInsight Console, click **Menu** in the left navigation menu.

Available features include:

- **Assets:** Display and manage all assets. Access the **Smart Rules** page to create and manage Smart Groups. Add assets to Password Safe management.
- **Smart Rules:** View and mange Smart Rules.
- **Scan:** Schedule Discovery Scans.
- **Scans:** Review active, completed, and scheduled scans.
- **Managed Systems:** View and configure properties for Password Safe managed systems, managed databases, managed directories, managed applications, and their associated Smart Rules.

- **Managed Accounts:** View and configure properties for Password Safe managed accounts and their associated Smart Rules.
- **Password Safe:** Access the Password Safe web portal to request passwords and remote access sessions and to approve requests.
- **Team Passwords:** View and manage team credentials.
- **Analytics & Reporting:** Access reports on collected data.
- **Configuration:** Configure BeyondInsight and Password Safe components and objects, such as users and groups, authentication settings, connectors, and much more.

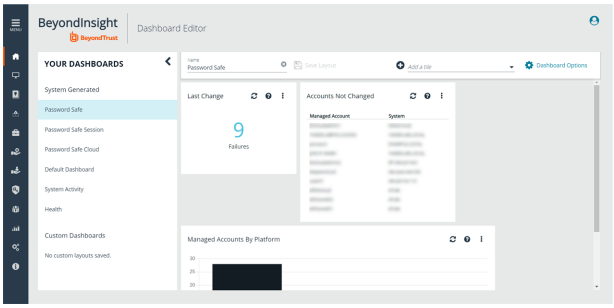
For more information on installing and configuring Resource Brokers and Zones, please refer to the Password Safe Cloud Resource Broker Configuration and Installation Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cloud/resource-broker/index.htm.

Dynamic Dashboards

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

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

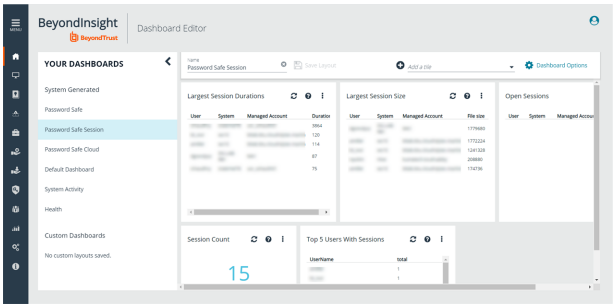
To access **Your Dashboards**, click **Menu > Dashboard (Preview)**. A list of available dashboards displays on the left. BeyondInsight comes with several prebuilt dashboard cards, including:



- **Password Safe**
- **Password Safe Session**
- **Password Safe Cloud**
- **Default Dashboard**
- **System Activity**
- **Health**

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

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



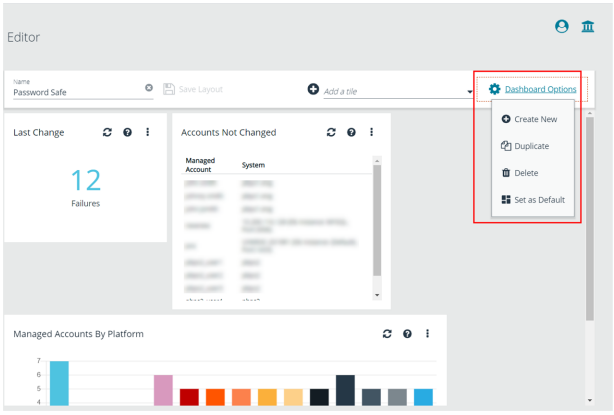
Click to refresh information displayed.

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

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

Use **Dashboard Options** to:

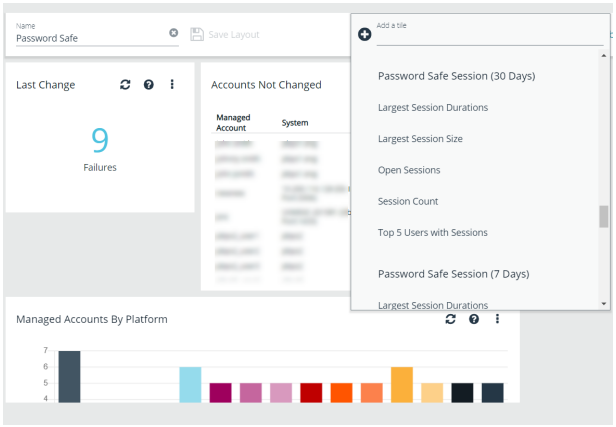
- **Create New:** Create a new empty dashboard, then add the tiles you want.
- **Duplicate:** Create a copy of the dashboard that can be modified.
- **Delete:** Delete the selected dashboard.
- **Set as Default:** Set the current dashboard as the default so it displays every time you click on **Menu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

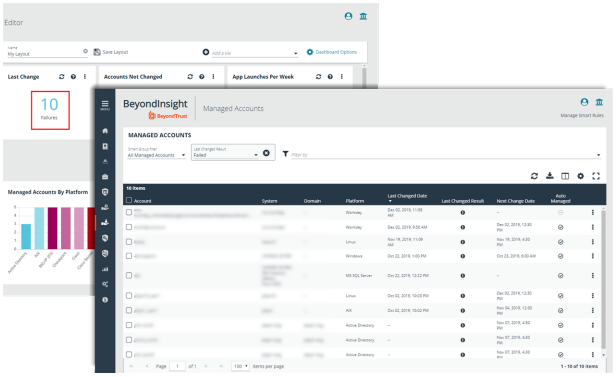
1. To create a custom dashboard, select one of the available dashboard cards. In this example we use the **Password Safe** card. If necessary, delete any of the existing tiles that come installed with that card.
2. From the **Add a tile** dropdown, select the tiles you want to add. Resize and reposition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



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

Access Dashboard Tile Information

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



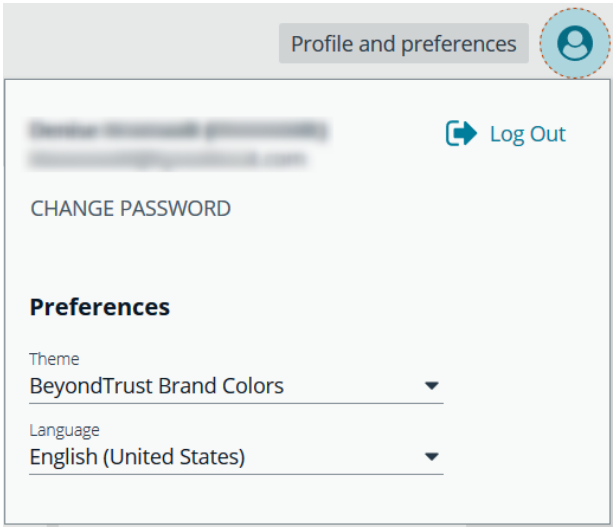
Change and Reset Console Login Passwords

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

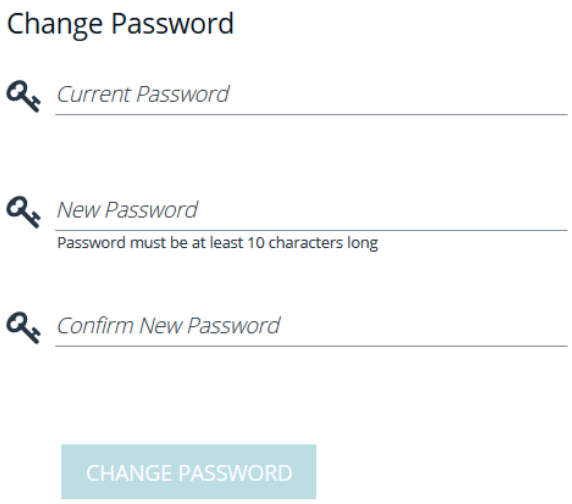
- You are logging in with Active Directory or LDAP credentials.
- Your account is currently locked out.

Change Password

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

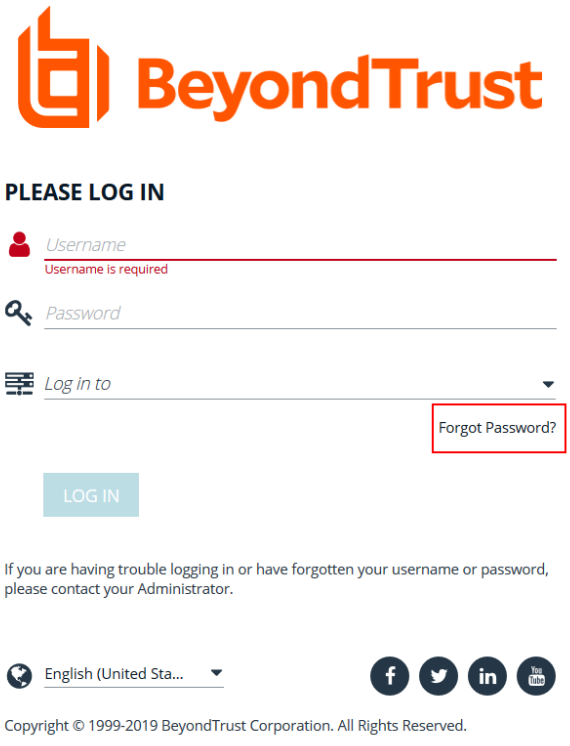


2. Change your password, and then click **Change Password**.



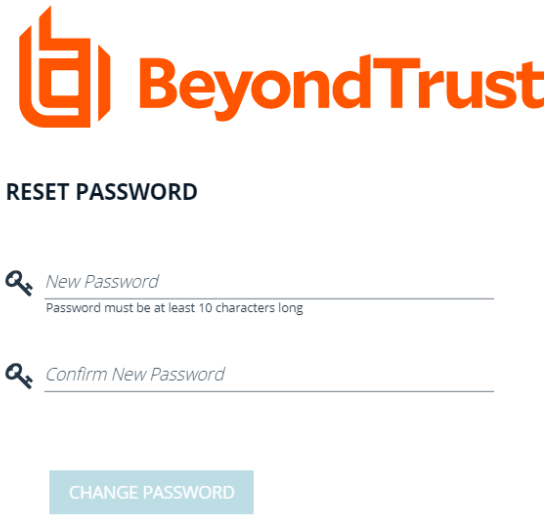
Reset Password

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 Preferences

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

Set Display Preferences

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

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

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

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

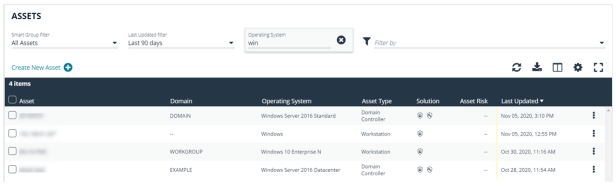
> ***Note:*** *Some options are not applicable to some grids, so fewer icons may display on those grids.*

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

Filter Records

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

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



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

Role Based Access

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

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

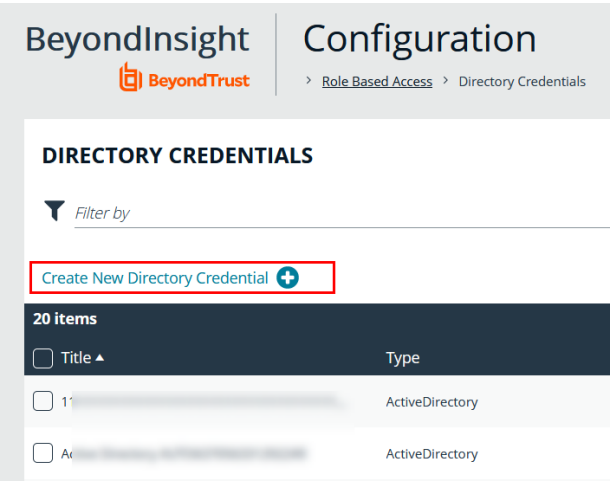
> ***Note:*** *By default, an* ***Administrators*** *user group is created. The permissions assigned to the group cannot be changed. The user account you created when you configured BeyondInsight is a member of the group.*

Create and Edit Directory Credentials

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

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

1. Navigate to **Configuration > Role Based Access > Directory Credentials**.
2. Click **Create New Directory Credential**.



3. Follow the steps in the below sections based on the type of directory you are creating.

Create an Active Directory Credential

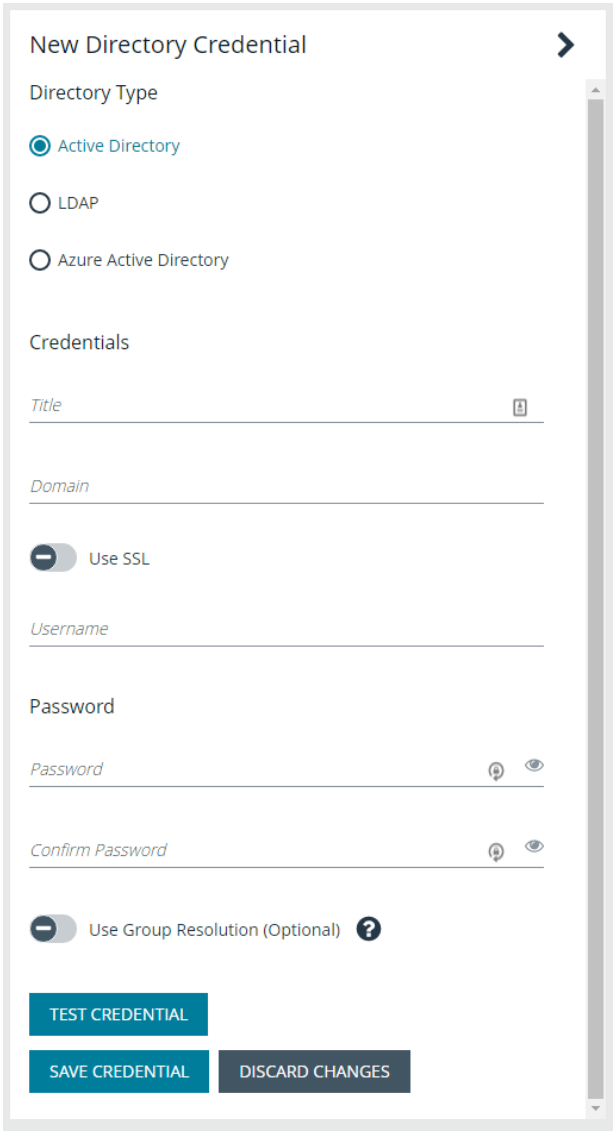
1. Select **Active Directory** for the **Directory Type**.
2. Provide a name for the credential.
3. Enter the name of the domain where the directory and user credentials reside.
4. Enable the **Use SSL** option to use a secure connection when accessing the directory.

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

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

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

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



Create an LDAP Credential

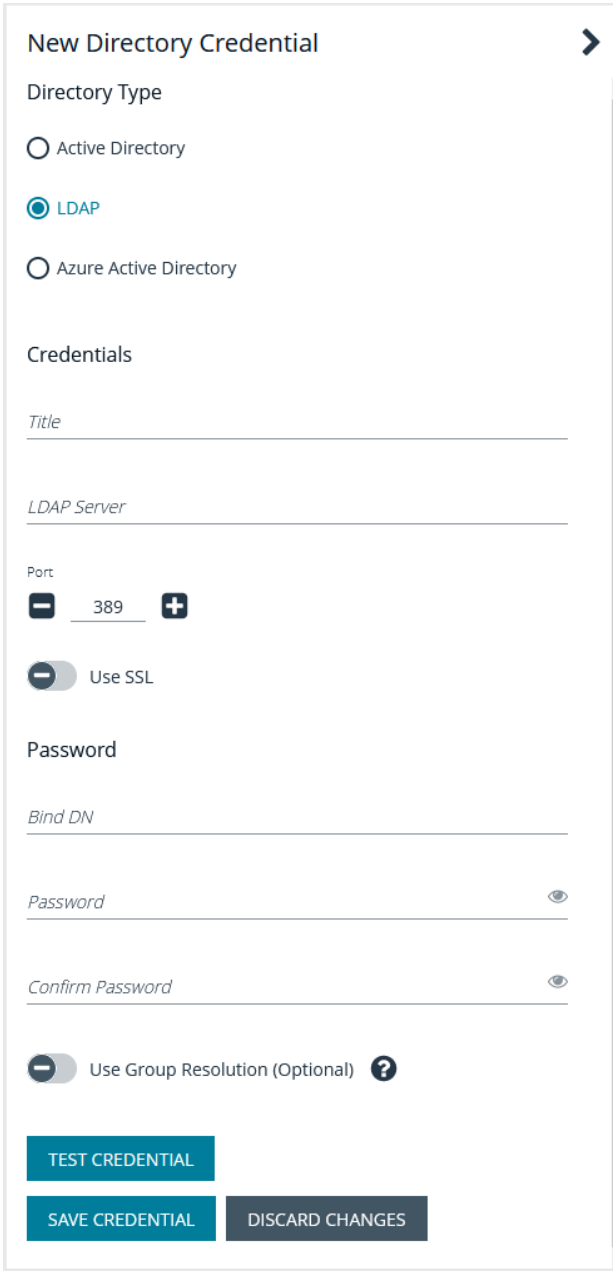
1. Select **LDAP** for the **Directory Type**.
2. Provide a name for the credential.
3. Enter the name of the LDAP server where the directory and user credentials reside.
4. Enable the **Use SSL** option to use a secure connection when accessing the directory.

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

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

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

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

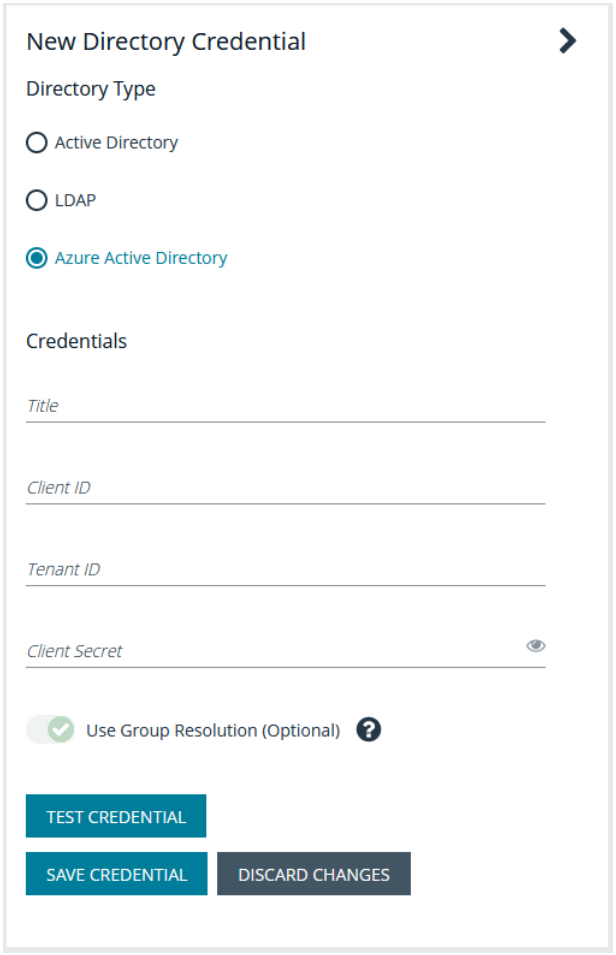


Create an Azure Active Directory Credential

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

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

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



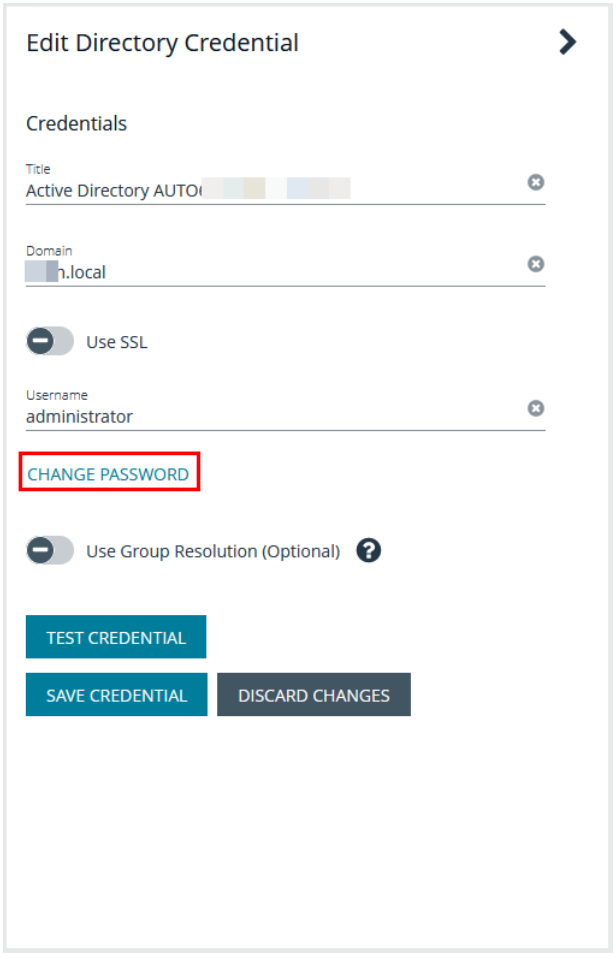
Edit a Directory Credential

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

2. Make the changes required.

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

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



Map Directory Credentials to a Domain

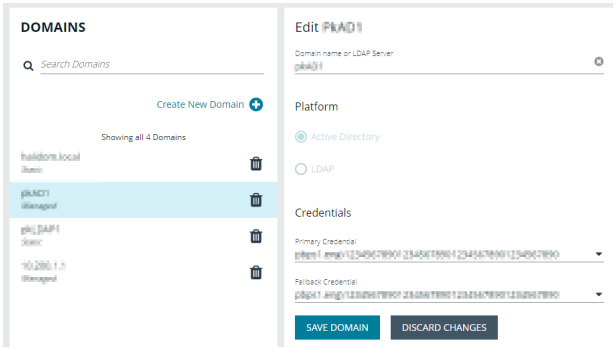
Domain management allows you to map a default primary directory credential and an optional fallback credential as preferred binding credentials used for account resolution against domains in your environment when logging in to BeyondInsight.

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

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

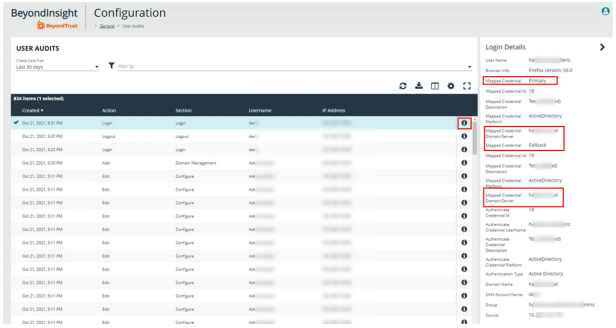
1. Navigate to **Configuration > Role Based Access > Domain Management**.

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



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

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

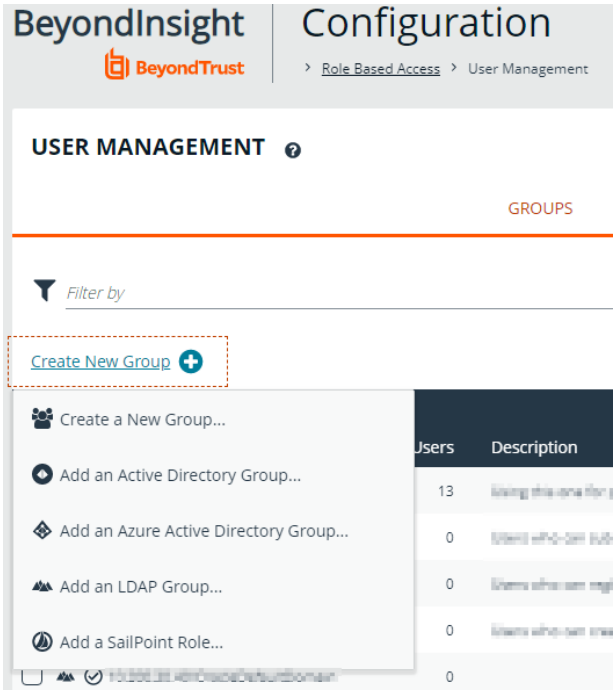


Create and Configure Groups

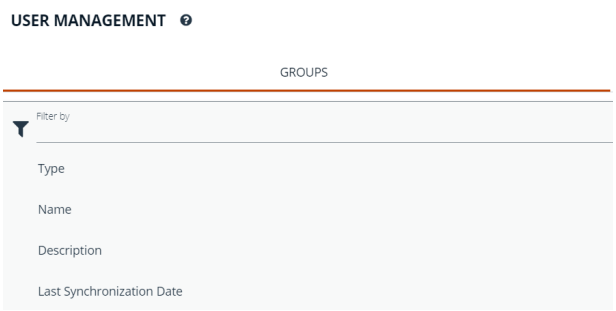
Create user groups and user accounts so that your BeyondInsight administrators can log in to BeyondInsight.

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

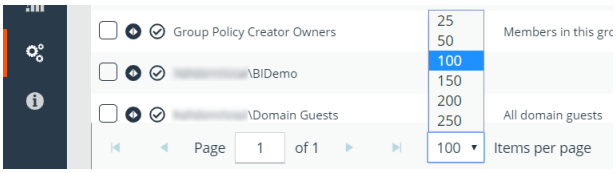
You can create BeyondInsight local groups, as well as add Active Directory, Azure Active Directory, and LDAP groups into BeyondInsight.



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



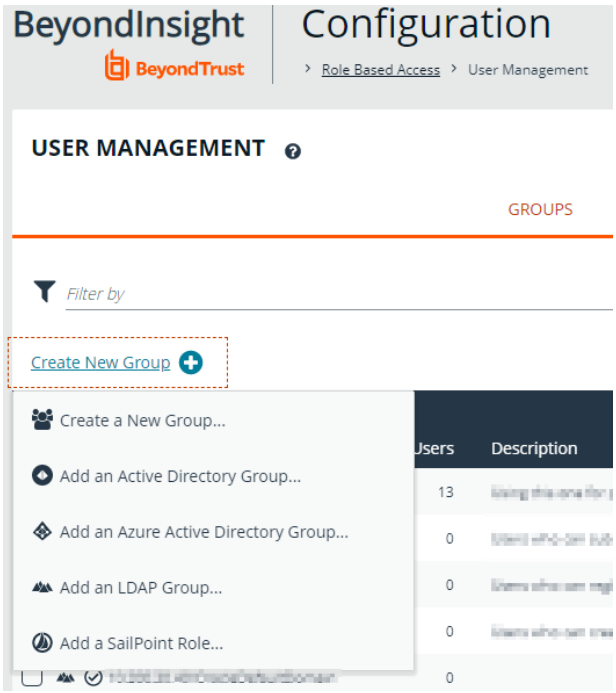
> ***Tip:*** *By default, the first 100 groups are displayed per page. You can change this by selecting a different number from the Items per page dropdown at the bottom of the grid.*



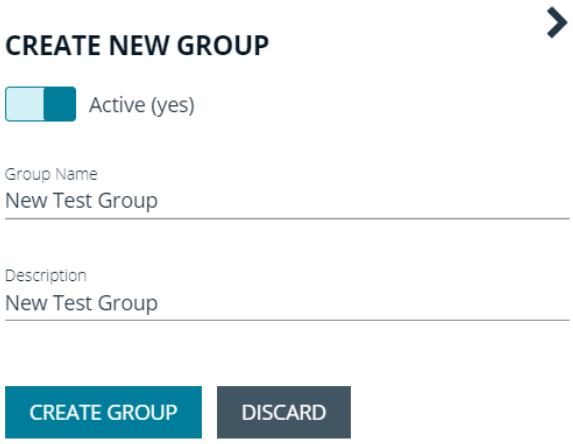
Create a BeyondInsight Local Group

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

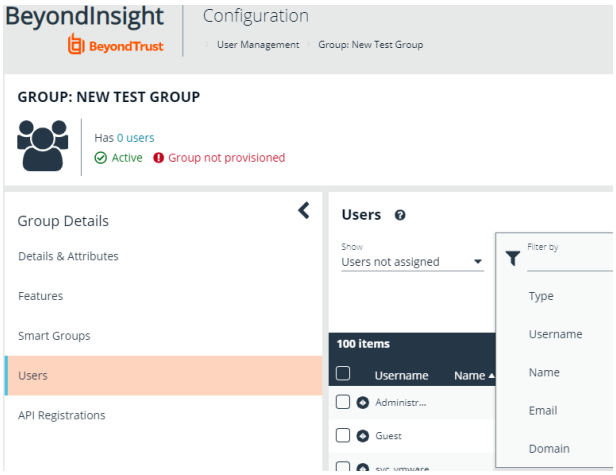
2. Under **Groups**, click **Create New Group**.
3. Select **Create a New Group**.



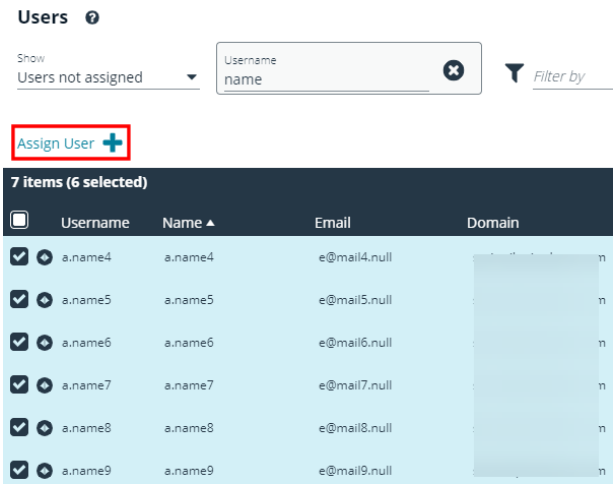
4. Enter a **Group Name** and **Description** for the group.
5. The group is set to **Active (yes)** by default. Click the toggle to set the group to **Active (no)** if you want to activate it later.
6. Click **Create Group**.



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



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



Note: *By default, new groups are not assigned any permissions. You must assign permissions on features and Smart Groups after creating a new group. For more information on permissions and how to assign them, please see* *"Assign Group Permissions" on page 31*.

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

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

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

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

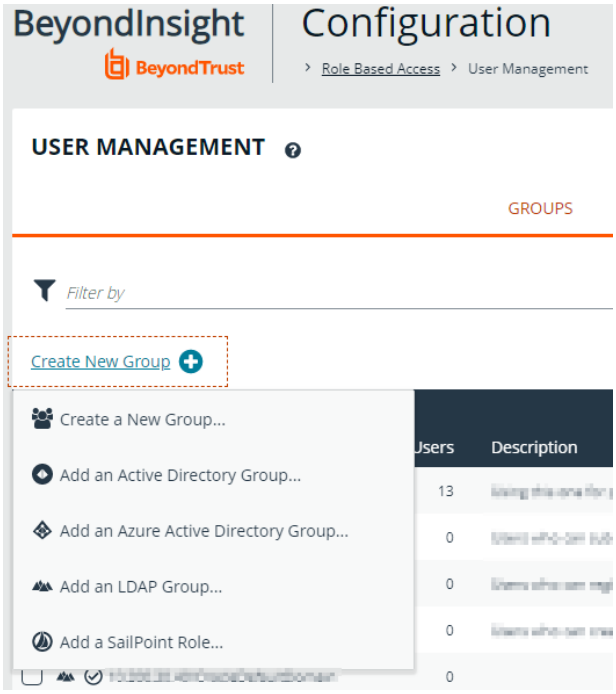
For new installs of release 21.3 and later releases, this option is enabled by default.

Add an Active Directory Group

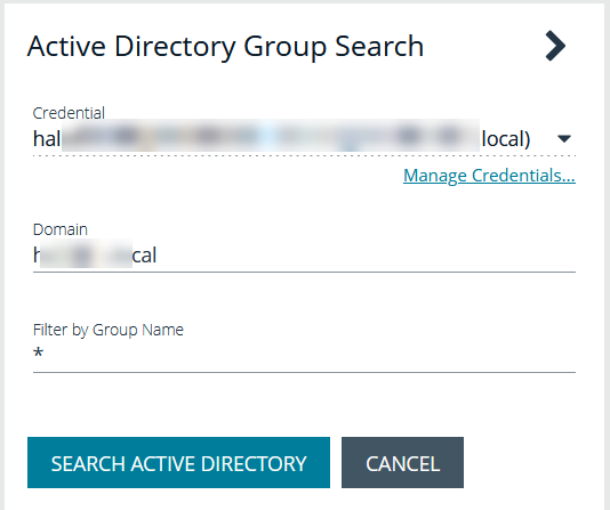
Active Directory group members can log in to the management console and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller.

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

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



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



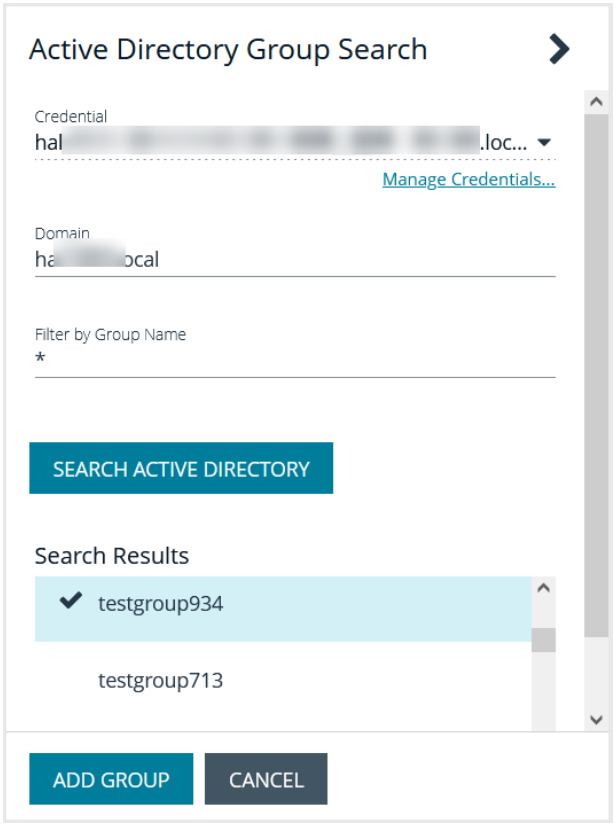
Note: *The default filter is an asterisk (*), which is a wild card filter that returns all groups. For performance reasons, a maximum of 250 groups from Active Directory is retrieved.*

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

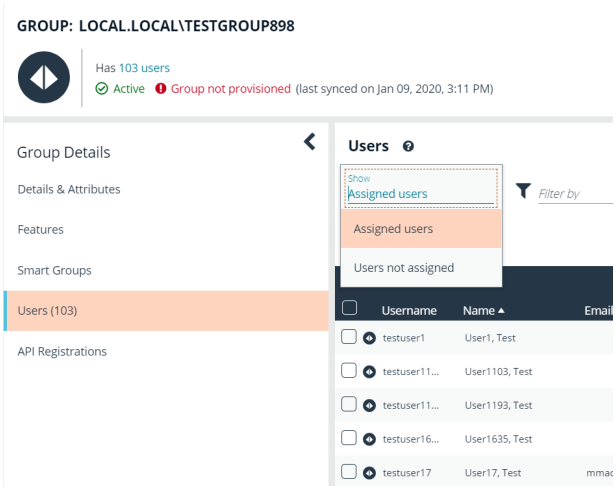
Example: *Sample filters:*

- ***a**** *returns all group names that start with "a"*
- ****d*** *returns all group names that end with "d"*
- ****sql**** *returns all groups that contain "sql" in the name*

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



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



> ***Note:*** *By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see* *"Assign Group Permissions" on page 31**.*

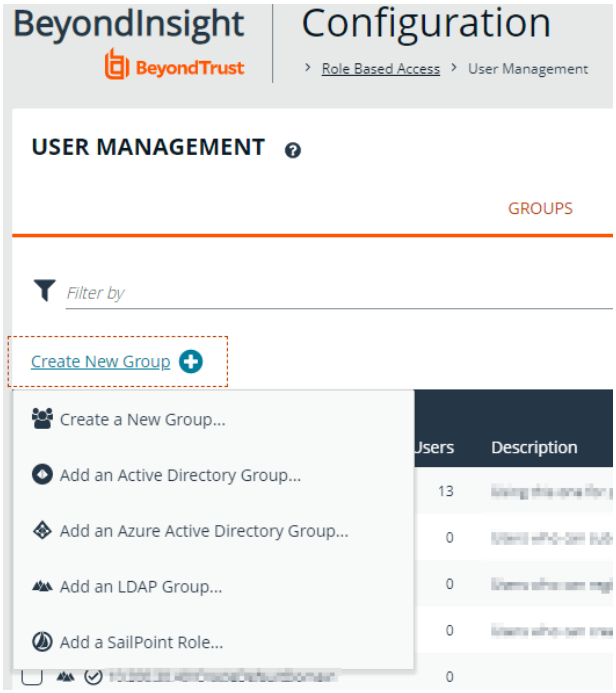
For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 14.

Add an Azure Active Directory Group

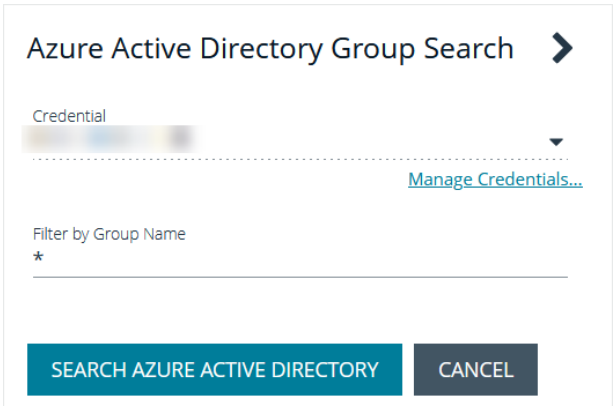
Azure AD group members can log in to the management console or a specific domain controller and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller.

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

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



4. Select a credential, or click **Manage Credentials** to add or edit a credential.
5. Click **Search Azure Active Directory**. A list of security groups displays.



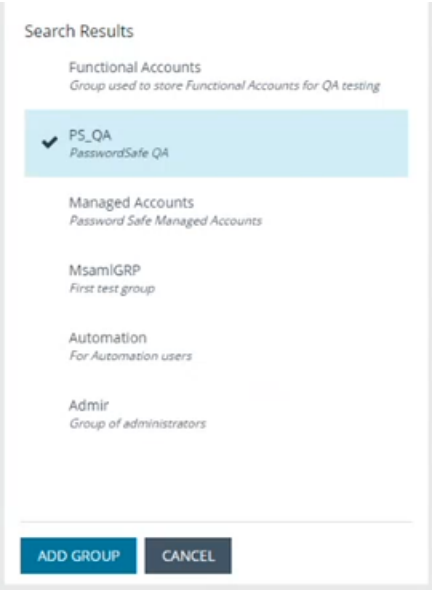
Note: *For performance reasons, a maximum of 250 groups from Azure AD is retrieved. The default filter is an asterisk (*), which is a wildcard filter that returns all groups. Use the group filter to refine the list.*

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

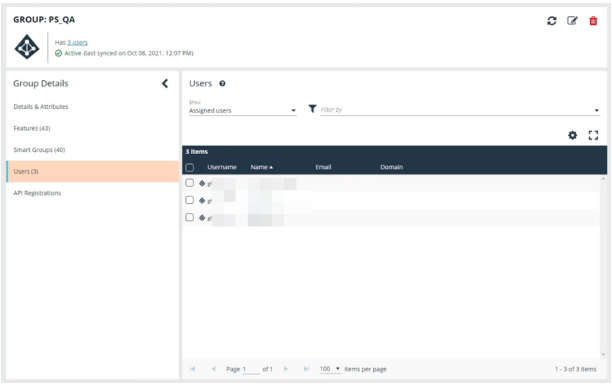
Example: *Sample filters:*

- ***a**** *returns all group names that start with a.*
- ****d*** *returns all group names that end with d.*
- ****sql**** *returns all groups that contain sql in the name.*

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



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



Note: *By default, new groups are not assigned any permissions. You must assign permissions on features and Smart Groups after creating a new group. For more information on permissions and how to assign them, please see* *"Assign Group Permissions" on page 31*.

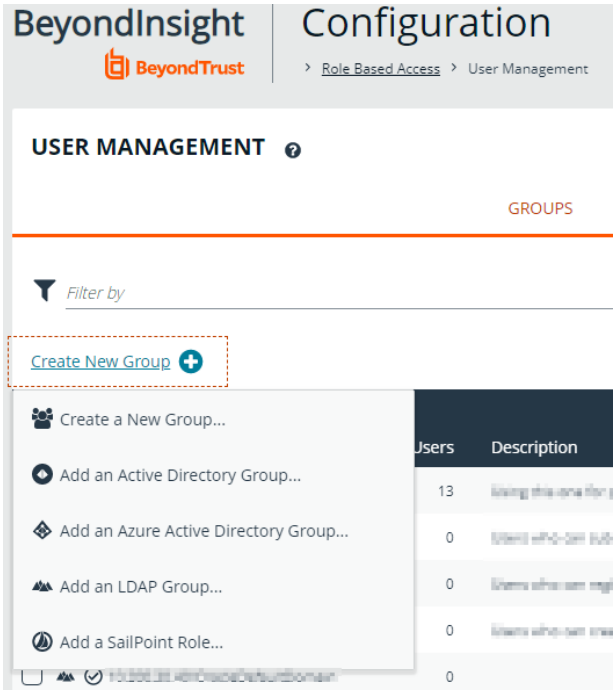
For more information on creating and editing directory credentials, please see *"Create and Edit Directory Credentials" on page 14*.

Add an LDAP Group

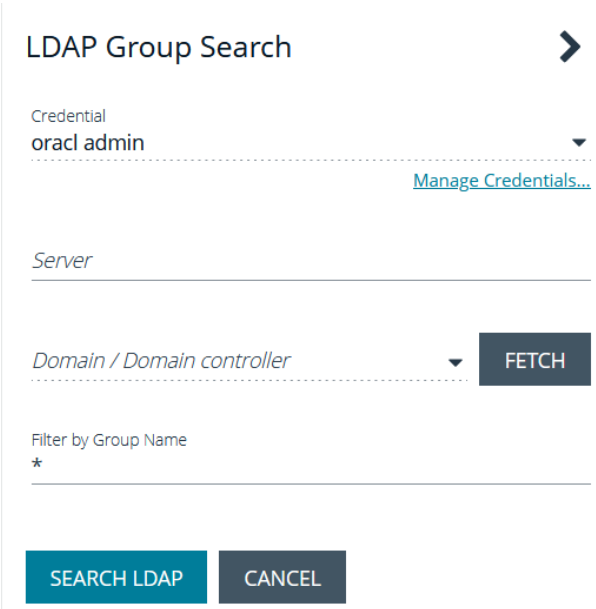
LDAP group members can log in to the management console and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller.

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

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



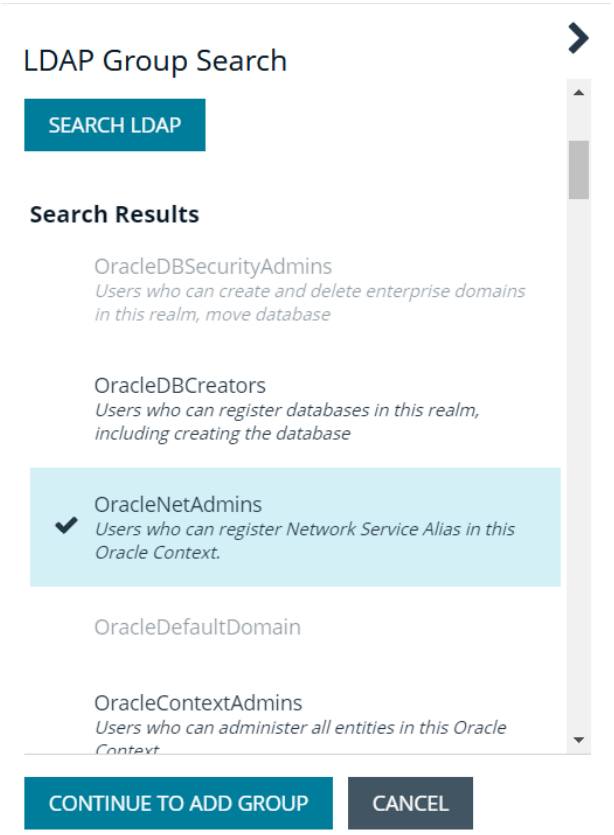
2. Select a credential, or click **Manage Credentials** to edit a credential or create a new one.
3. Click **Fetch** to load the list of Domain Controllers, and then select one.
4. To filter the group search, enter keywords in the group filter or use a wild card, and then click **Search LDAP**.



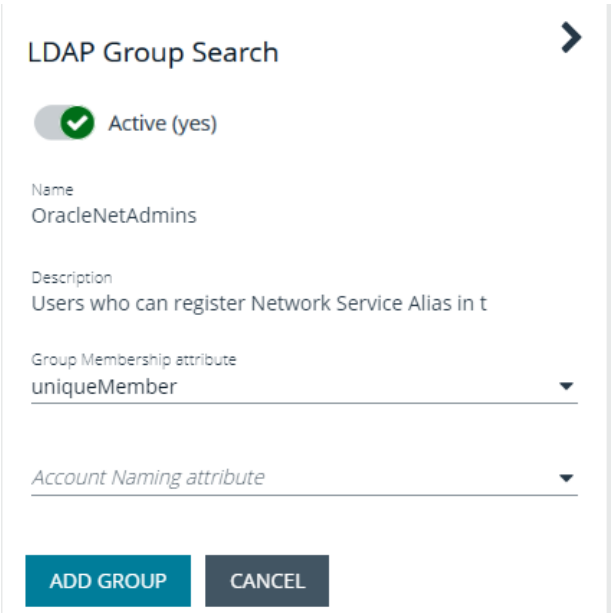
Example: *Sample filters:*

- ***a**** *returns all group names that start with a.*
- ****d*** *returns all group names that end with d.*
- ****sql**** *returns all groups that contain sql in the name.*

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

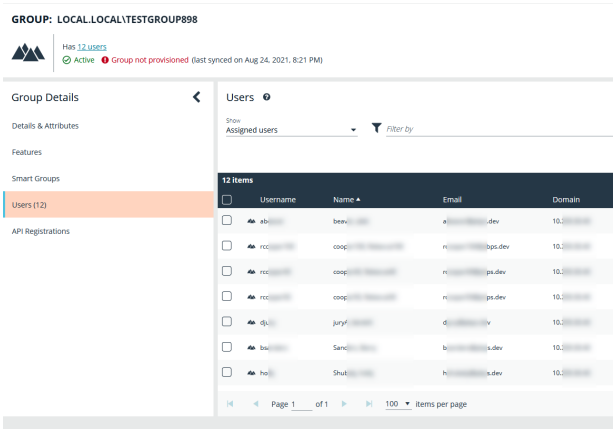


6. Select the **Group Membership Attribute** and **Account Naming Attribute**.
7. Click **Add Group**.



8. The group is added and set to **Active** but is not provisioned or synchronized with LDAP. Synchronization with LDAP to retrieve users begins immediately.

9. Once the group has been synced with LDAP, you can view the users assigned to the group, as well as unassigned users, by selecting **Users** from the **Group Details** section, and then using the filters.



***Note:** By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 31.*

For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 14.

Assign Group Permissions

Permissions

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

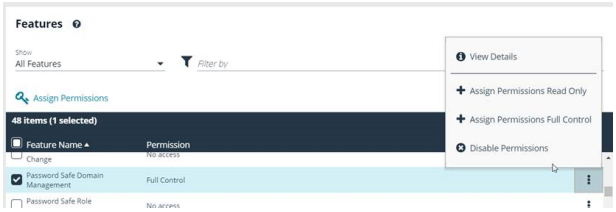
Permissions must be assigned cumulatively. For example, if you want a BeyondInsight administrator to manage Discovery Scans only, then you must assign **Full Control** for the following features:

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

Assign Features Permissions

1. From the left navigation pane in the console, select **Configuration**.
2. Under **Role Based Access**, select **User Management**.

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



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

Feature	Provides Permissions To:
Analytics & Reporting	Log in to the console and access **Analytics & Reporting** to generate and subscribe to reports.
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.
Credential Management	Add and change credentials when running scans and deploying policies.
Directory Credential Management	Grant access to the configuration area where directory credentials are managed. This feature must be enabled to support access to directory queries as well.
Directory Query Management	Grant access to the configuration area where directory queries are managed. ***Note:*** *Access to Directory Credential Management must also be granted.*
Domain Management	Grants the user permission to configure mappings of bind credentials to domains for account resolution.
Endpoint Privilege Management	Grant access to the Endpoint Privilege Management features.
Endpoint Privilege Management for Unix & Linux	Grant access to the Endpoint Privilege Management for Unix & Linux features.
File Integrity Monitoring	Work with **File Integrity** rules.
License Reporting	View the **Licensing** folder in **Analytics & Reporting** (MSP reports, Privilege Management for Windows, Privilege Management for Mac true-up reports, and Assets Scanned report).
Management Console Access	Access the BeyondInsight management console.
Manual Range Entry	Allow the user to manually enter ranges for scans and deployments rather than being restricted to smart groups. The specified ranges must be within the selected smart group.
Option Management	Change the application options settings (for example, account lockout and account password settings).
Options - Connectors	Access the configuration area where connectors are managed.

Feature	Provides Permissions To:
Options - Scan Options	Access the configuration area where scan options are managed.
Password Safe Account Management	Grant read or write permissions to the following features on the **Managed Accounts** page and through the public API: • Bulk delete accounts • Add accounts to a Quick Group • Remove accounts from a Quick Group • Add, edit, and delete accounts
Password Safe Admin Session	Password Safe web portal admin sessions.
Password Safe 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.
Protection Policy Management	Activate the protection policy feature. User groups can deploy policies, and manage protection policies on the **Configuration** page.
Reports Management	Run scans, create reports, and create report categories.
Scan - Audit Groups	Create, delete, update, and revert audit group settings.
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)
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.

Feature	Provides Permissions To:
Smart Rule Management – Asset	Grants permission to create and edit asset Smart Rules.
Smart Rule Management – Managed Account	Grants permission to create and edit managed account Smart Rules.
Smart Rule Management – Managed System	Grants permission to create and edit managed system Smart Rules.
Smart Rule Management – Policy User	Grants permission to create and edit policy user Smart Rules.
Team Passwords	Provides access to Team Passwords for all members of the selected group.
Ticket System	View and use the ticket system.
Ticket System Management	Mark a ticket as inactive. The ticket no longer exists when **Inactive** is selected.
User Accounts Management	Add, delete, or change user groups and user accounts. A minimum of read access to Directory Credential Management must also be granted to enable creation of AD and LDAP Groups.
User Audits	View audit details for management console users on the **User Audits** page.

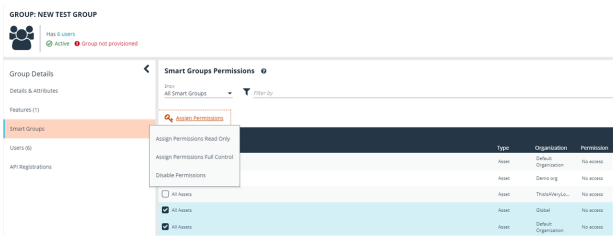
For more information, please see the Managed Accounts section in the BeyondInsight and Password Safe API Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/api/password-safe/managed-accounts.htm.

Features Permissions Required for Configuration Options

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

Assign Smart Groups Permissions

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



Edit and Delete Groups

Edit Basic Group Details

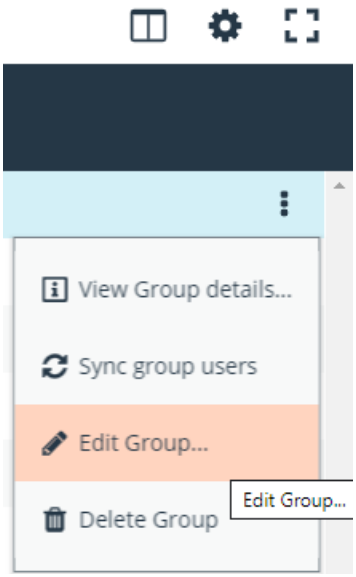
Administrators can edit the following basic details for groups:

- 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. From the left navigation pane in the console, 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. Click the vertical ellipsis for the group, and 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.

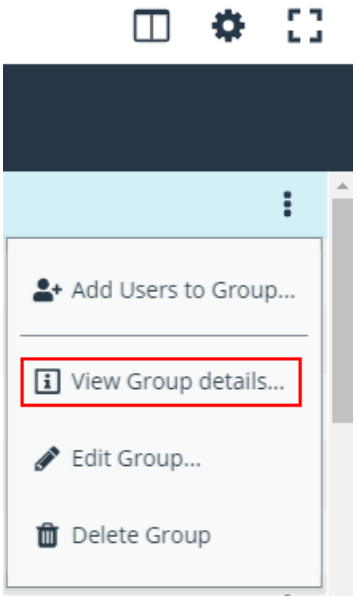
Edit Advanced Group Details

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.

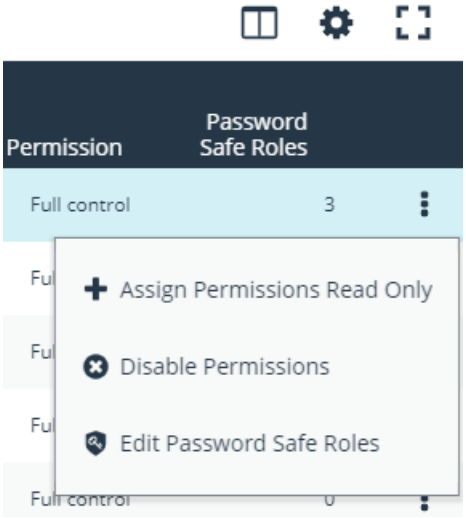
Update Group Permissions for Features and Smart Groups

1. On the **User Management** page, optionally filter the list of groups in the grid by **Type**, **Name**, **Description**, or **Last Synchronization Date** to locate the group.

2. Click the vertical ellipsis button for the group, and then select **View Group Details**.

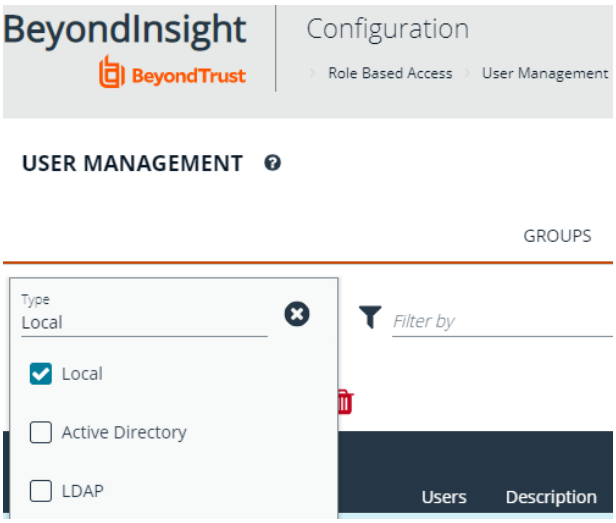


3. Select the desired features or Smart Groups, click the ellipsis button for the feature or Smart Group, and then select to assign or disable permissions accordingly.

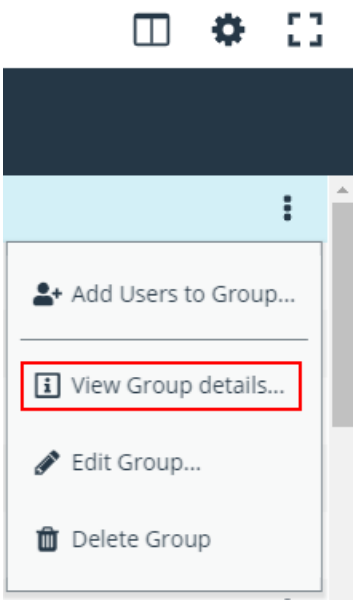


Remove Users from Local BeyondInsight Groups

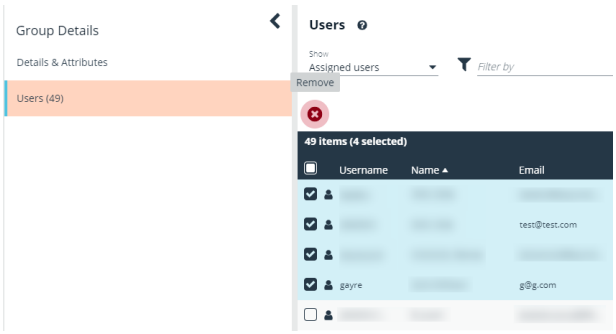
1. On the **User Management** page, filter the grid by local groups.



2. Click the vertical ellipsis button for the group, and then select **View Group Details**.

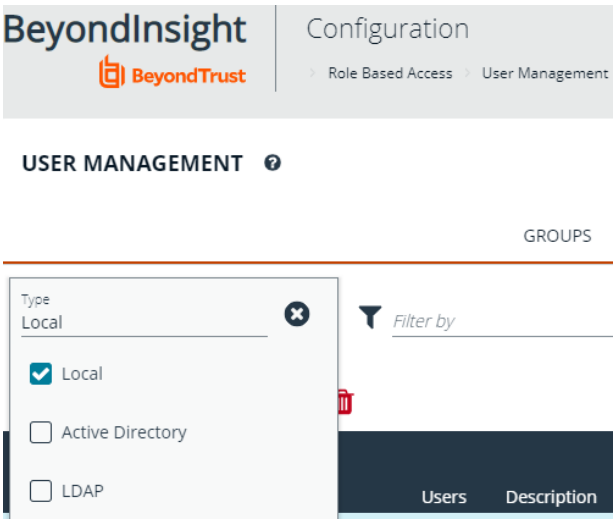


3. Under **Group Details**, select **Users**.
4. Filter the **Users** grid to show assigned users.
5. Select the user or users, and then click the **Remove** button.

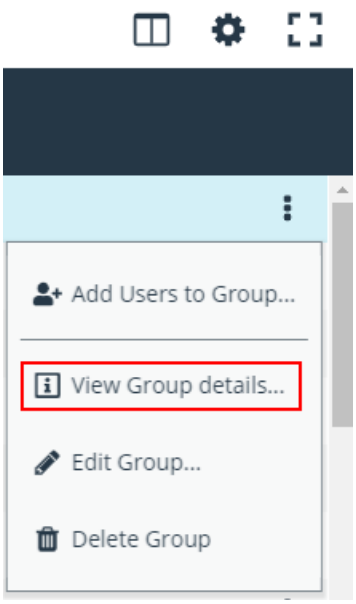


Add Users to Local BeyondInsight Groups

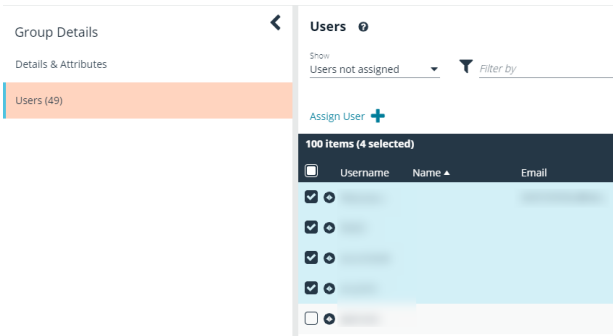
1. On the **User Management** page, filter the grid by local groups.



2. Click the vertical ellipsis button for the group, and then select **View Group Details**.

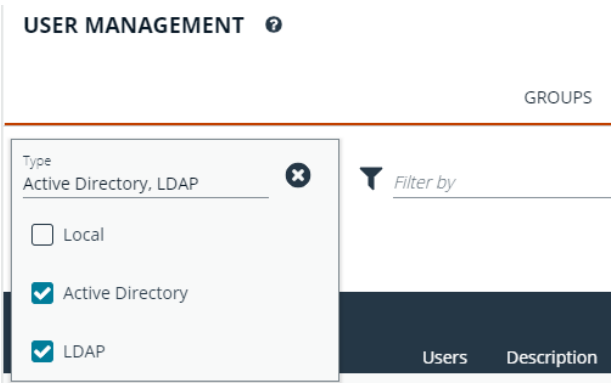


3. Under **Group Details**, select **Users**.
4. Filter the **Users** grid to show unassigned users.
5. Select the user or users, and then click **Assign User**.

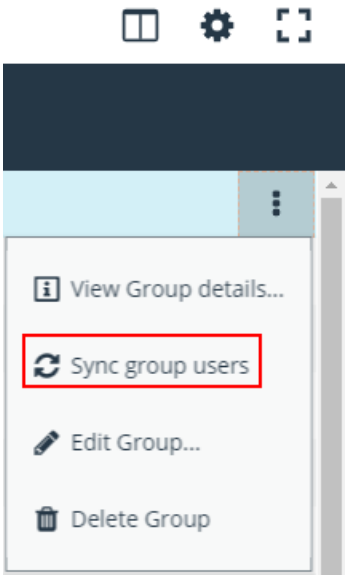


Sync Group Users for Active Directory and LDAP Groups

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



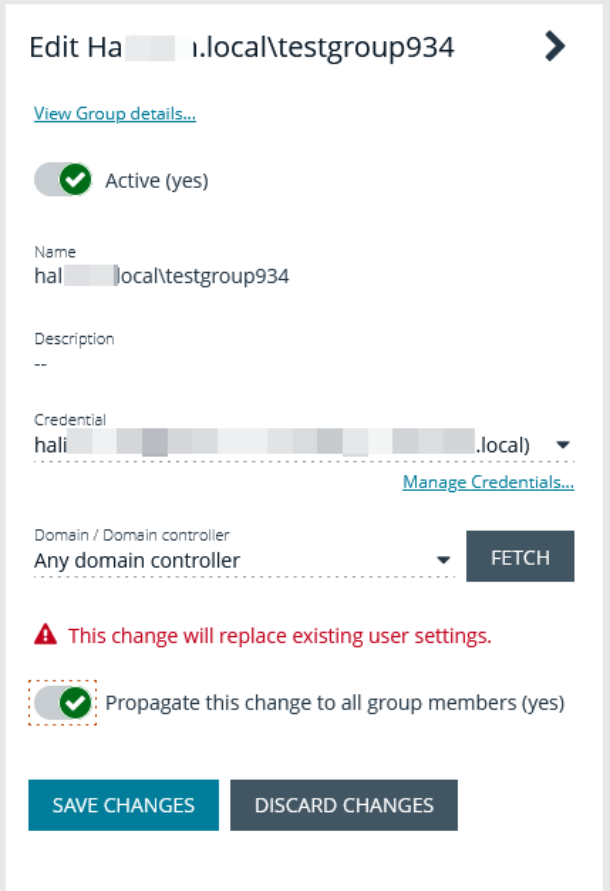
2. Click the vertical ellipsis button for the group, and then select **Sync Group Users**.



Propagate Domain Changes

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

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



Delete a Group

Administrators can delete groups as follows:

1. From the left navigation pane in the console, 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 vertical ellpsis button for the group, and then select **Delete Group**.

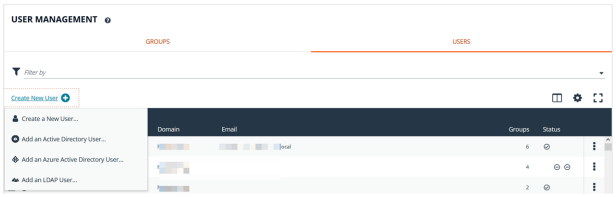
Create and Manage User Accounts

User accounts create the user identity that BeyondInsight uses to authenticate and authorize access to specific system resources. You can create 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 cannot log in to the console.*

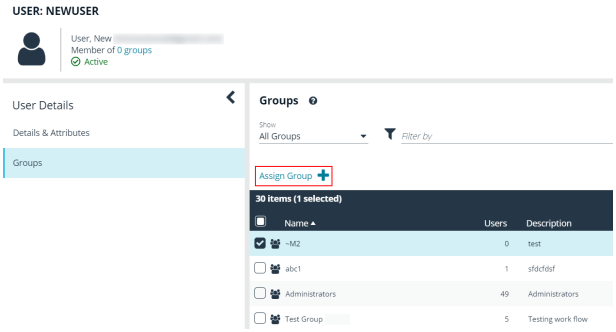
Create a BeyondInsight Local User Account

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

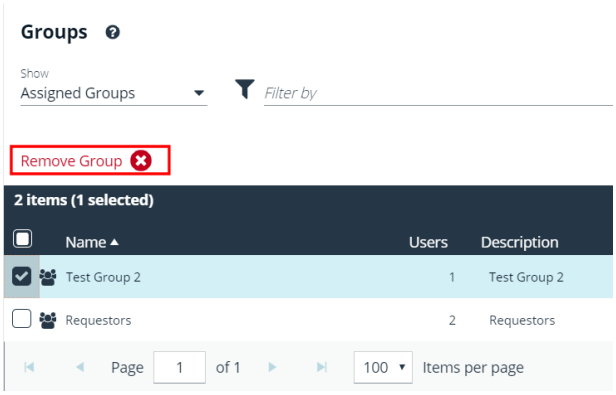


5. Select **Create a New User**.
6. Complete the **Identification** and **Credentials / Change Password** sections. These fields are required.
7. Enter the user's contact information *(Optional)*.
8. Select an **Activation Date** and an **Expiration Date** for the user account.
9. Enable the **User Active**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

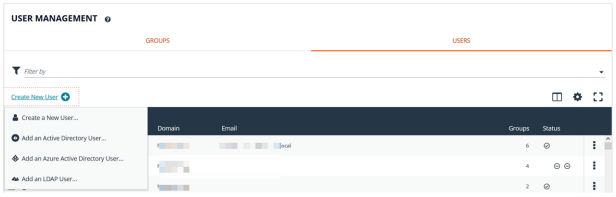


Add an Active Directory User

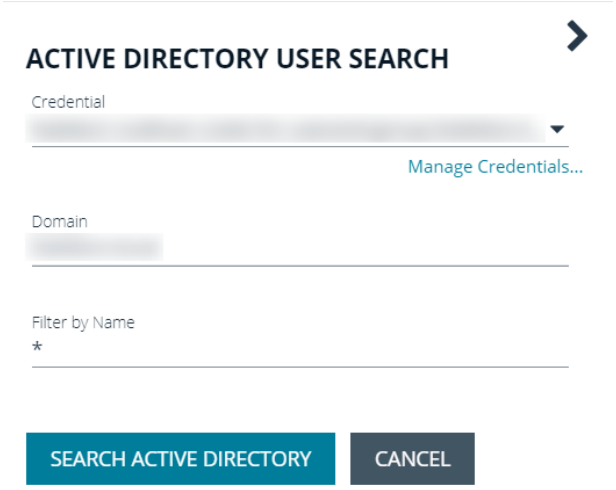
Active Directory users can log in to the management console and perform tasks based on the permissions assigned to their groups. The user can authenticate against either a domain or domain controller.

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

1. Navigate to **Configuration > Role Based Acess > User Management**.
2. Click **Users** to display the list of users in the grid.
3. 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.



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: *Sample filters:*

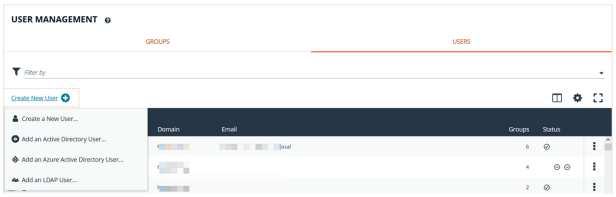
- ***a**** *returns all group names that start with "a"*
- ****d*** *returns all group names that end with "d"*
- ****sql**** *returns all groups that contain "sql" in the name*

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

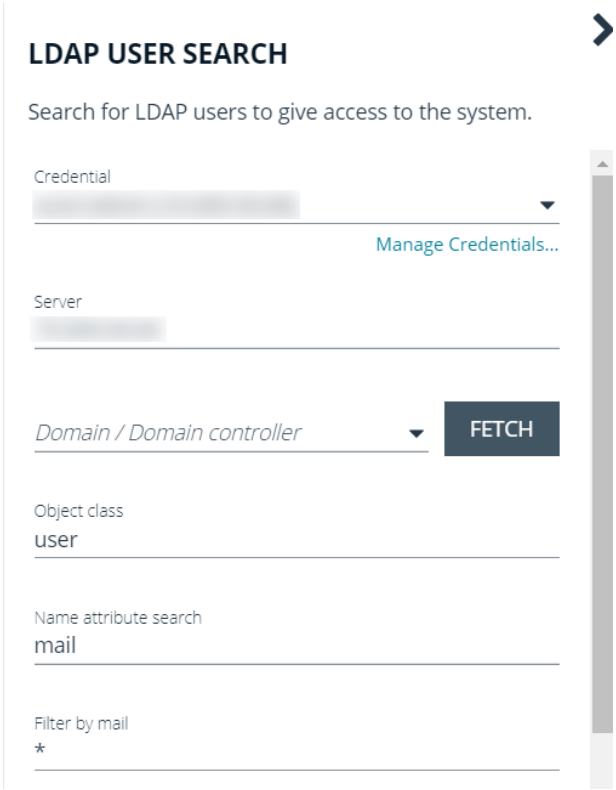
> *For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 14.*

Add an LDAP User

1. Navigate to **Configuration > Role Based Acess > User Management**.
2. Click **Users** to display the list of users in the grid.
3. 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.



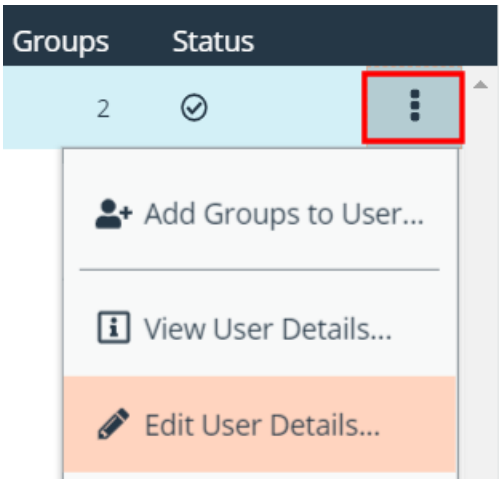
7. Click **Fetch** to load the list Domain Controllers, and then select one.
8. To filter the group search, enter keywords in the group filter or use a wild card.
9. Click **Search LDAP**.
10. Select a user, and then click **Add User**.
11. Assign at least one group to the user.

For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 14.

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:

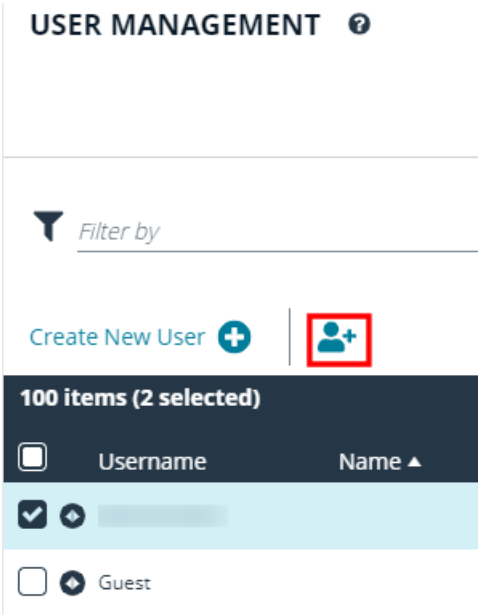
1. From the left navigation pane in the console, select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Click **Users** to display the list of users in the grid.
4. Optionally, filter the list of users displayed in the grid using the **Filter By** dropdown.
5. Select 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**.



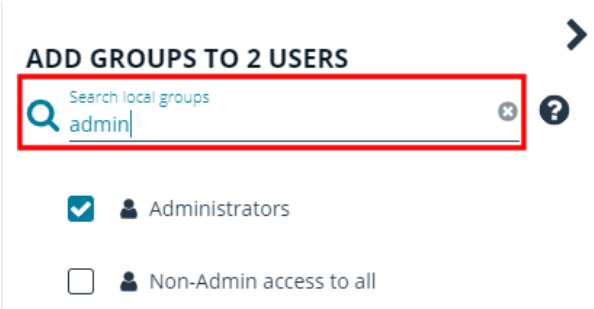
Add Groups to User

1. From the **User Management** page, click **Users** to display the list of users in the grid.
2. Optionally, filter the list of users displayed in the grid using the **Filter By** dropdown.

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 is displayed next to the group name.*

Delete a User Account

Administrators can delete user accounts as follows:

1. From the left navigation pane in the console, select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Click **Users** to display the list of users in the grid.
4. Optionally, filter the list of users displayed in the grid using the **Filter By** dropdown.
5. For local accounts, select the user, click the **Delete** button above the grid, and then click **Delete** to confirm.
6. For directory accounts, select the user, click the vertical ellipsis, select **Delete User**, and then click **Delete** to confirm.

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

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

Audit Console Users in BeyondInsight Cloud

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

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

To view user audit data, follow the steps.

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

Note: *You can also configure display preferences and filters to refine the information displayed. For more information, please see* *"Change and Set the Console Display Preferences" on page 13**.*

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 Preferences" on page 13.

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 19.

Create an Always Address Group

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

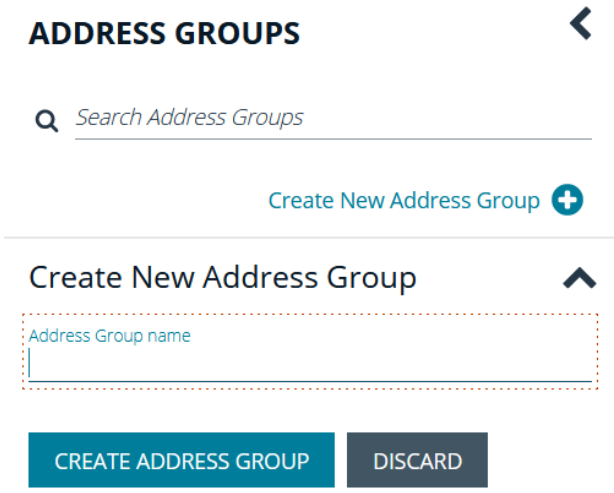
The next time a scan runs, the address group is synchronized with the BeyondInsight scanner. The IP addresses, whether they are included or omitted, are considered part of the running scan.

***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.*

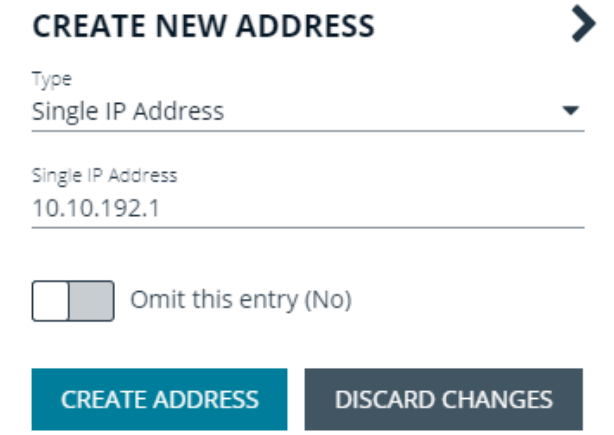
***Note:** If an asset is scanned and later added to the **Always** address group as **Omit**, the asset is not scanned but might be displayed in the report. This only occurs with some reports.*

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

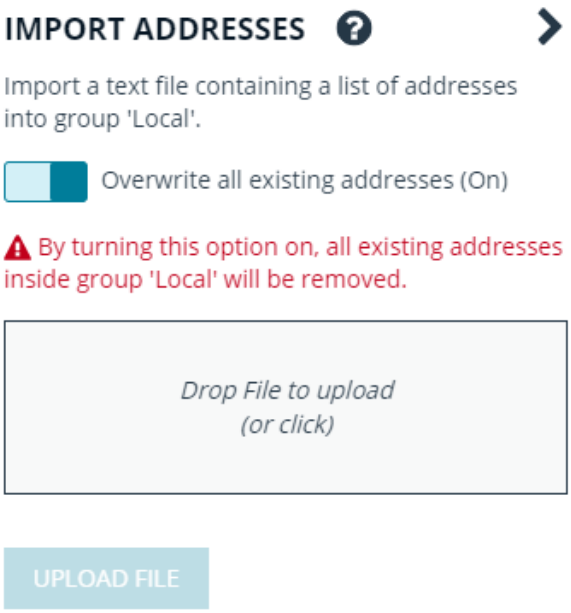


5. Select the address group, and then click **Add New Address** to manually add the IP addresses. Or, click **Import Addresses** to import them into the group using a file.

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

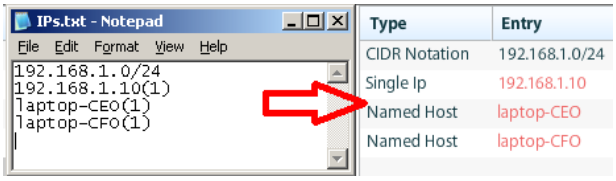


7. If importing the addresses:
   - Enable the **Overwrite all existing addresses** option, if desired.
   - Click **Drop File** to upload the import file.
   - Click **Upload File**.



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

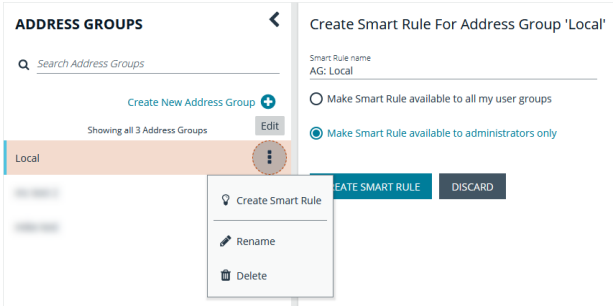
Here is an example of how a CIDR notation, an excluded IP address, and excluded named hosts are displayed after importing.



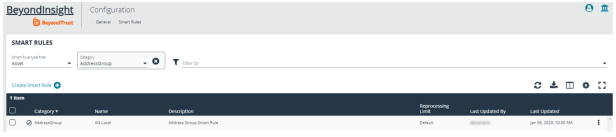
Create a Smart Rule Based on an Address Group

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

1. Select the address group, and 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** .

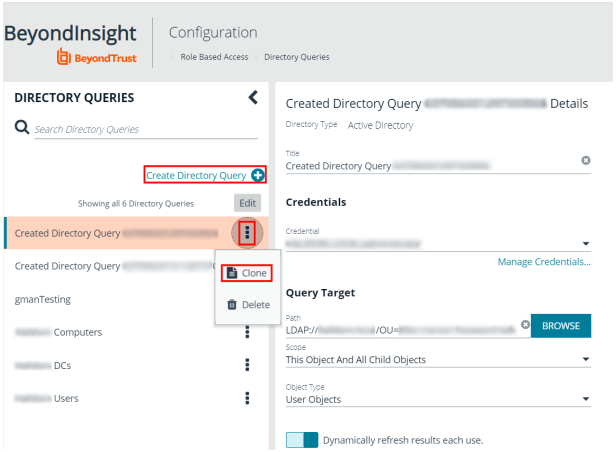


Create a Directory Query

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.

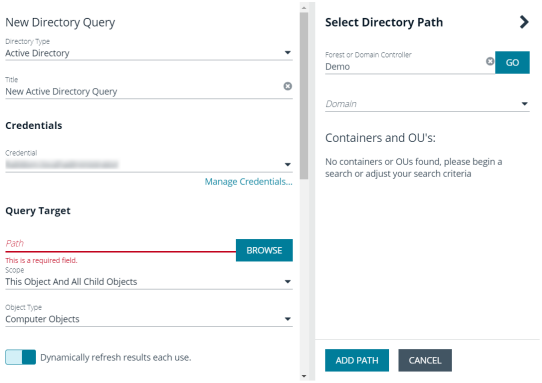
1. Select **Configuration**.
2. Under **Role Based Access**, click **Directory Queries**.
3. Click **Create Directory Query**.

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



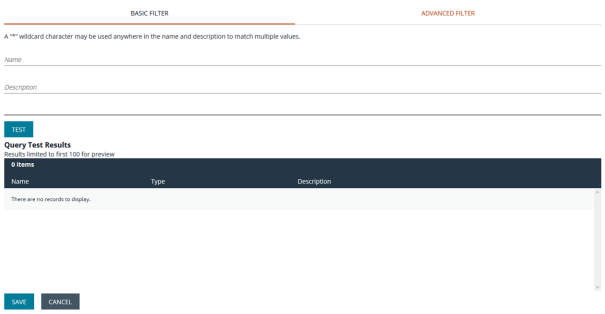
4. Select the directory type: **Active Directory** or **LDAP**.
5. Enter a name for the query.
6. Select a stored credential for running this query or click **Manage Credentials** to add or edit a credential.

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



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**.



For more information, please see the following:

- *"Create and Configure Groups" on page 19*
- *"Create and Edit Directory Credentials" on page 14*

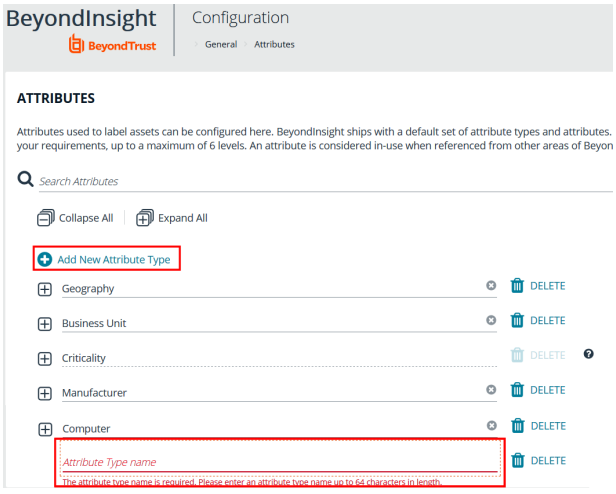
Attributes and Attribute Types in BeyondInsight

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 54.

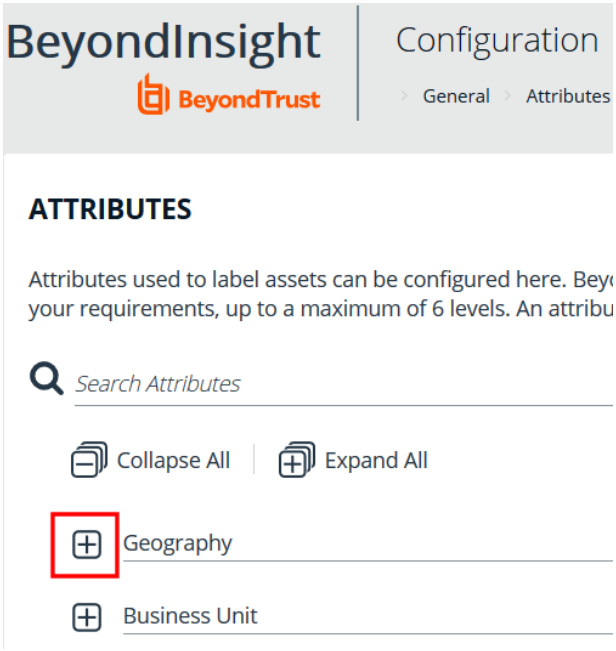
Add a New Attribute Type

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

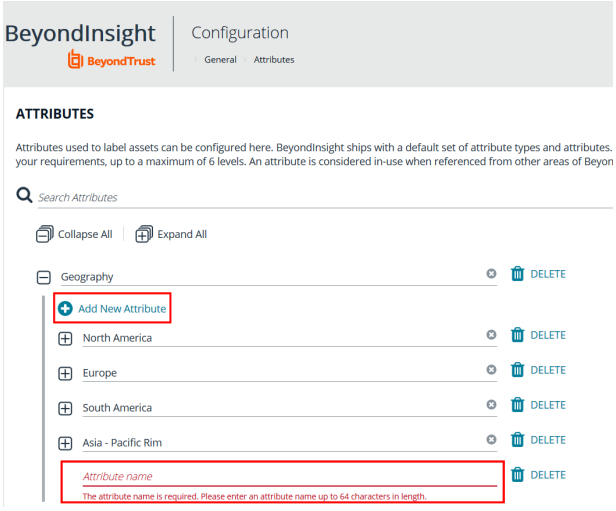


Add a New Attribute

1. Click the plus sign for the desired attribute type to expand its attributes.



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



Use Smart Rules to Organize Assets

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

> ***Note:*** *The BeyondInsight user must be a member of the* ***Administrators*** *group or be assigned the* ***Full Control*** *permission on the* ***Asset Management*** *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

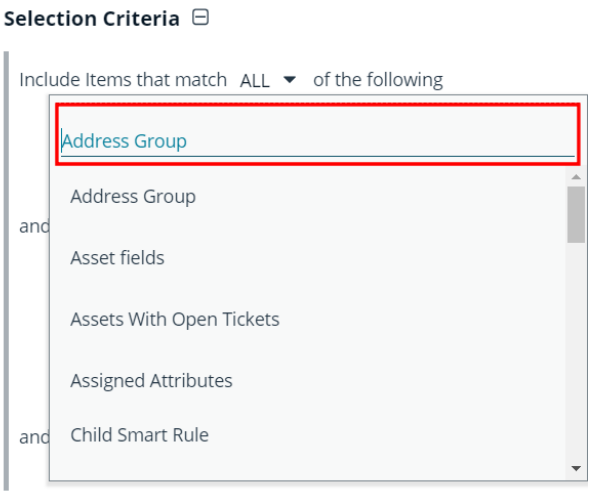
Use a Smart Rule to register assets as Smart Groups. This allows you to:

- Run Discovery Scans
- Monitor and view assets

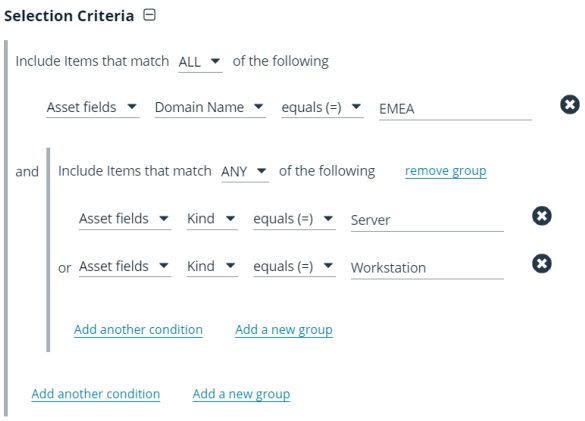
Smart Rules update results automatically, ensuring assets match the criteria and are current.

Use Smart Rule Filters and Smart Groups

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



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



Smart Rule Filters

Asset Smart Rule Filters

Address Group	Create a group of IP addresses.
Asset Fields	Group the Smart Rule by asset fields, such as, **Asset Name**, **Domain** or **DNS**, **Risk**, and **Kind**. You can include more than one asset field filter in the Smart Rule to refine the results.
Assets with Open Tickets	For ticket tracking, create a Smart Rule that filters on open tickets. The Smart Rule filter can be set to include overdue tickets.
Assigned Attributes	Create a filter based on an attribute. If the attribute is unassigned on a particular asset, you can choose to include or exclude the asset from the rule.
Child Smart Rule	You can reuse a Smart Rule to save time when creating new Smart Rules. This is especially useful if the Smart Rule is a complicated set of filters. Reusing a Smart Rule further refines the assets that will be a part of the Smart Rule.
Cloud Assets	Filter assets on the cloud connector.
Directory Query	Create an Active Directory or an LDAP query to include or exclude assets in the selected domain.
Installed Software	Filter on any combination of installed software.
MAC Address	Filter by MAC address of assets.
Operating System	Filter on any combination of OS. Operating systems included in the list are those detected in your network. Assets with no OS detected, can be included or excluded from the rule.
Processes	Filter on any combination of processes.

Services	Filter by any combination of services.
Software Version	Filter by software version. The software that you can filter on is determined by the software that is discovered during the scan.
User Account Attribute	Filters user accounts by SID or privilege. You can filter on both. If either value is not selected then it will be ignored. Using this filter you can determine if any users have administrator privileges that might no longer be required. You can create a Smart Rule using this filter and set the email alert action to notify you when a user account with admin privileges is detected.
Windows Events	Filter by Windows events that are available in the Windows Event Viewer. For example, **Application**, **Security**, or **System**.
Workgroup	Filter by workgroup.

For more information, please see the following:

- *"Create an Address Group" on page 48*
- *"Create a Directory Query" on page 51*

Predefined Smart Group Categories

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

Create Smart Rules

You can configure an asset-based Smart Rule to:

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

- Create a ticket with a list of assets
- Set scanner pooling

Create an Asset Based Smart Rule

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

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

9. Click **Create Smart Rule**.

Perform Other Smart Rule Actions

Clone a Smart Rule

You can clone custom or predefined Smart Rules.

1. From the left menu in the BeyondInsight Console, click **Smart Rules**.
2. 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**.

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

Deactivate a Smart Rule

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

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

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

To deactivate a Smart Rule:

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

Delete a Smart Rule

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

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

Smart Rule Processing

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

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

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

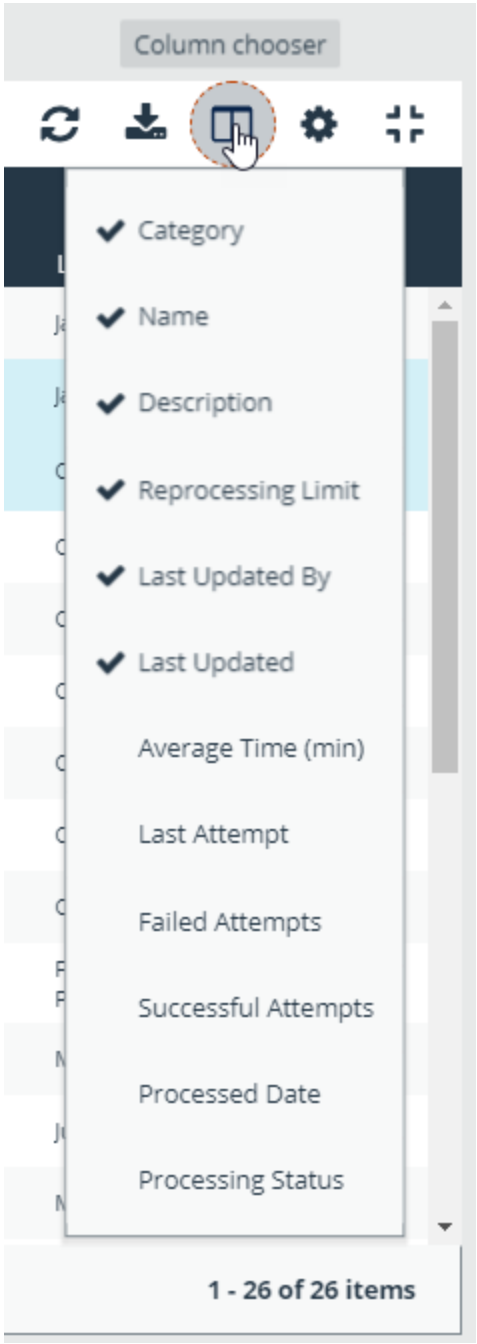
- A Smart Rule with Smart Rule children triggers the children to run before the parent completes.
- Managed account Smart Rules with selection criteria **Dedicated Account** process when a change to a mapped group is detected. This can occur in the following scenarios:
    - A new user logs on.
    -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

View and Select Smart Rules Processing Statistics

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

To add this information to the grid:

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



Add Credentials to Use in Scans

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

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

To create a credential:

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

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

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

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

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

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

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

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

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

5. Click **Create Credential**.

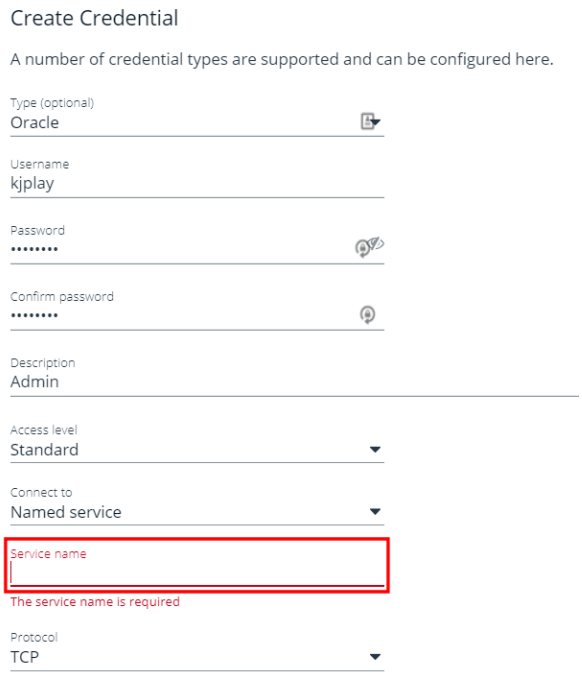
If creating Oracle, SSH, or SNMP credentials, please see the following:

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

Create Oracle Credentials

If you scan 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 BeyondInsight to Discovery Scanner servers and allows end users and API calls to leverage credentials locally on the network scanner. This eliminates the need to provide credentials separately for those scanners.*

If the credential name matches an existing credential in the BeyondTrust Discovery 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 BeyondInsight to Discovery Scanner servers and allows end users and API calls to leverage credentials locally on the network scanner. This eliminates the need to provide credentials separately for those scanners.*
>
> *If the credential name matches an existing credential in the BeyondTrust Discovery Scanner, the credential is overwritten with the value from BeyondInsight.*

7. Click **Create Credential**.

Create SSH Credentials

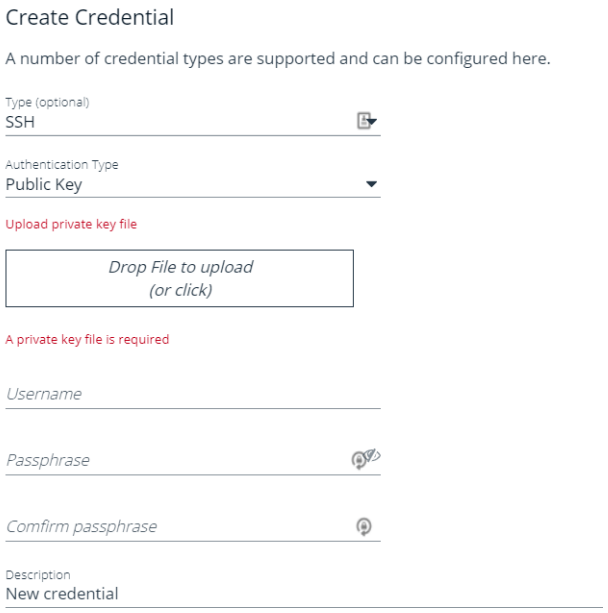
You can create Public Key Encryption credentials to connect to SSH-configured targets. You can select a credential that contains a public and private key pair used for SSH connections.

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

Optionally, when configuring SSH, you can choose 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 connect via 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 target assets.

1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Credentials**.
3. Click **Create Credential**.

4. 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 audit Cisco devices, you can elevate the credentials to privileged for more thorough scans.



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

If the credential name matches an existing credential in the BeyondTrust Discovery 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 TCP discovery ports are 22, 80, 110, 139, 389, 443, 445, 1025, 1433, 1521, 3306, 3389, 5000, 5432, and 27017.
- Use more than one scanner to distribute the coverage across the network.

Use the Scan Wizard to Create a Discovery Scan

1. Click **Scan** from the left menu.
2. **Select Scan Type**: There are three types of scans to choose 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 any of the assets, nor does it deploy any agent to the targets.
    - **Detailed Discovery Scan**: This scan requires credentials and it deploys a local scan agent to the scan targets, which can be disabled if required. Besides systems, this scan provides associated information on services, scheduled tasks, users, and databases.
    - **Advanced Discovery Scan**: This scan requires credentials and performs all the operations of the previous scan, as well as information on all associated attributes. This scan deploys a local scan agent to the scan targets, which can be disabled if required.
3. **Select Scan Targets**: Enter scan targets in the field provided. You can enter single IP addresses, IP ranges, addresses in CIDR notation, or named hosts. Items must be separated by commas.
4. **Choose Scan Agent**: Select which agents are used to execute the scan. If more than one agent is selected, the scan targets are split between the selected agents. If you have a large number of agents, you can use the filter dropdown menu. Click **Next** to continue.

Note: *A warning banner appears at the top of the screen if your installation includes any Discovery Agents earlier than version 20.1. These must be updated by the end of 2021. You can identify outdated agents by referring to the grid of agents on this screen, which includes the version of each agent.*

*Click **Dismiss** to hide the warning banner until your next login. Dismissing the warning banner here does not hide it on the dashboard, and dismissing the warning banner on the dashboard does not hide it on this screen.*

5. **Enter Credentials**: If the type of scan you select requires credentials, you can select 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 is 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.

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

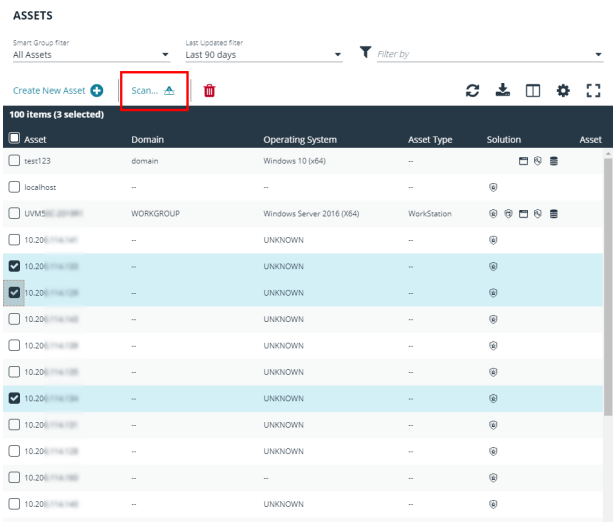
> ***Note:*** *Disabling the local scan service prevents the discovery of IIS app pools, Scheduled Tasks, and domain user information.*

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

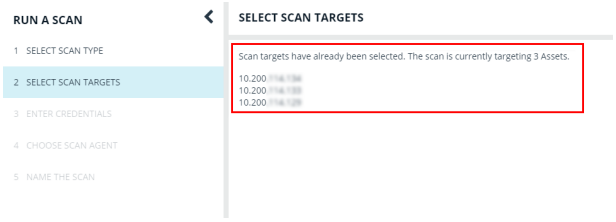
Run Scans from a List of Assets

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

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

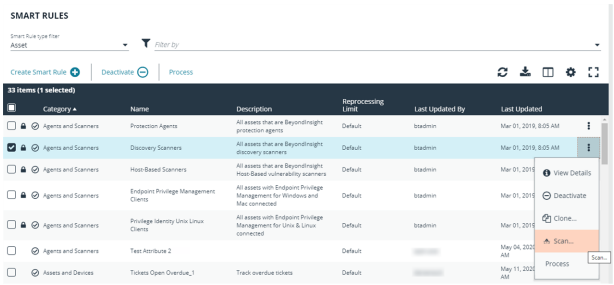


The Scan Wizard screen appears. Here you can select the type of scan to run. The difference is that when you click **Next** and go to the **Select Scan Targets** page, you will find the targets already selected. The next steps in the Scan Wizard are the same as those outlined above.



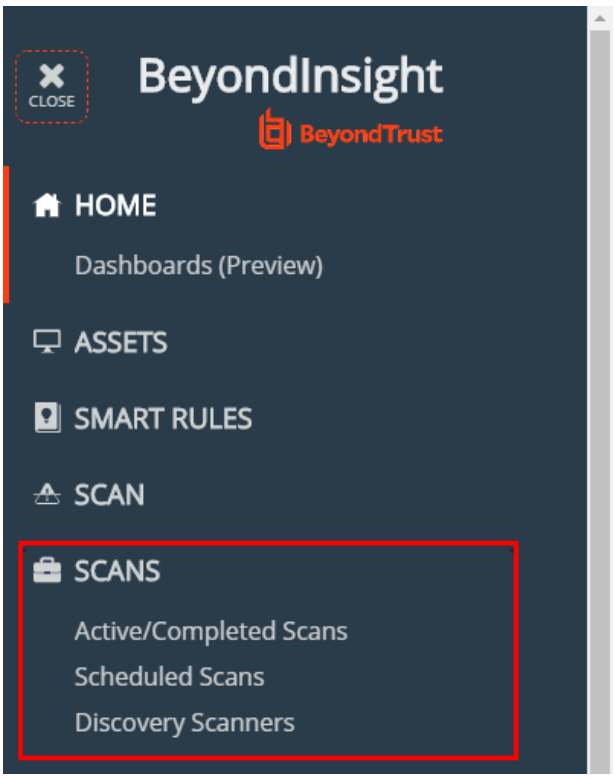
Use Smart Rules as Targets for Scans

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

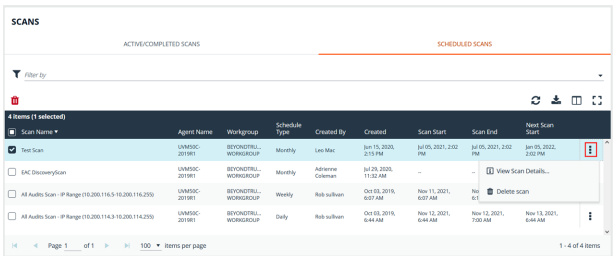


Check Completed and Scheduled Scans

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

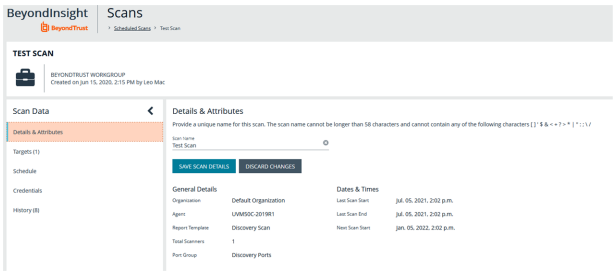


From the **Scans** page you can see active, completed, and scheduled scans, and you can delete a scan. For each of the scheduled scans you can click the vertical ellipsis for the scan, and then select **View Scan Details**, or **Delete scan**.



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

- Change the name of the scan
- View the scan targets and modify the target Smart Rule if one is selected
- Change the scheduled scan time
- Change the credentials
- View the history of the scan, if any exists



Discover Assets Using a Smart Group

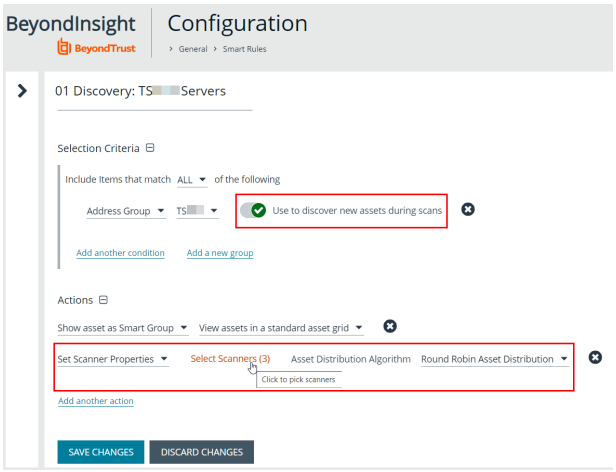
When the Smart Group filter is an address group, Active Directory query, or cloud connector, you can discover assets. When the **Use to discover new** box is checked, any assets online since the Smart Group was last processed are detected . The scan results on the **Assets** page reflect the number of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

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

Key Steps

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

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



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

For more information, please see the following:

- *"Create a Directory Query" on page 51*
- *"Create an Address Group" on page 48*

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

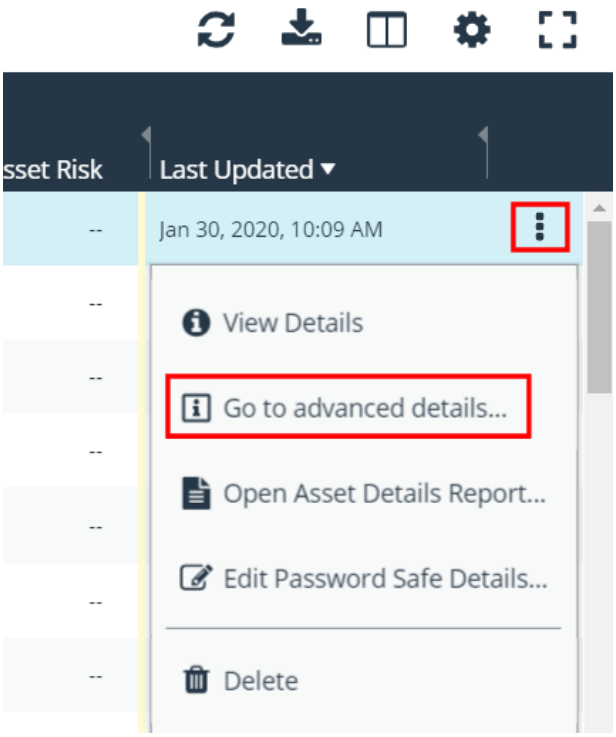
The **Assets** grid allows you to review details about your assets quickly by filtering your assets by Smart Groups, last update time, type of asset, domain, operating systems, technical solutions applied to the asset (asset is a scanned host or database host, for example), DNS name, and workgroups,

Review Asset Details

Tip: *Depending on the scan settings, information in the following list might not be detected and included in the scan results. If the following scan settings are turned on, more accurate scan results can be expected:* ***Perform Local Scanning***, ***Enable WMI Service***, *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, only information under* ***General Data*** *is shown.*

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

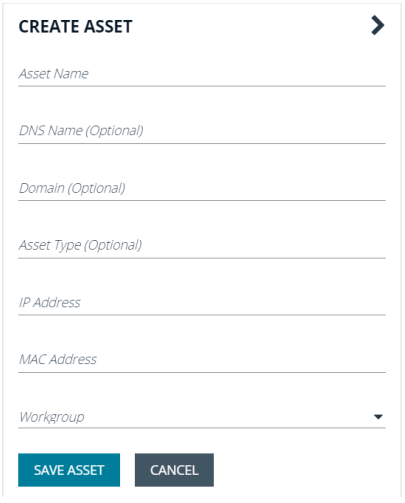
> ***Note:*** *By default, the current snapshot of scan data is selected. You can select other available snapshots to load the data for that date.*

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

Create Assets

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**.



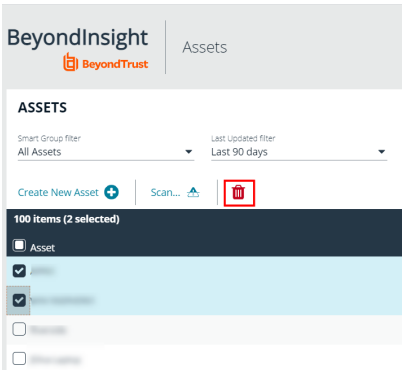
> ***Note:*** *New assets created in any smart group other than **All Assets** might not appear under the selected Smart Group if the Smart Rule criteria is not met or until the Smart Rule processes. We recommend that you create new assets using the **All Assets** Smart Group.*

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

Delete Assets

You can remove assets from the **Assets** grid immediately. Assets removed from the grid is 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 check the 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 extracts 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.

- Discovery Scanner 5.17 or later
- BeyondInsight 3.5 or later
- **VMware Tools** must be installed on the targets that you want to scan.
- Log in to the VMware website and download the **Virtual Disk Development Kit (VDDK)**: https://developer.vmware.com/home
- Discovery 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

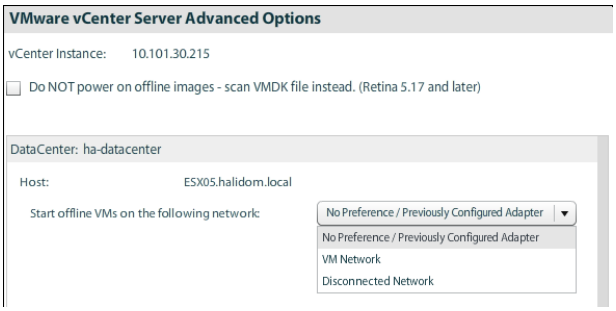
By default, paused or offline VMs are turned on during a scan. After the scan runs, the VMs are reverted to the paused or offline state.

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.

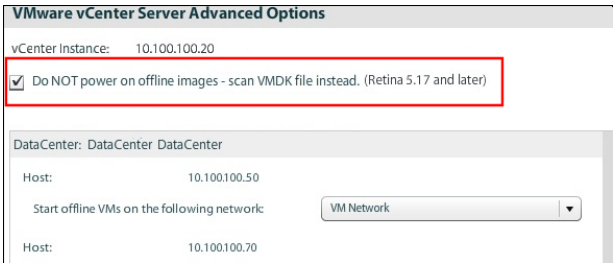
The advanced options dialog box varies depending on your vCenter configuration. The list of available options includes all other networks configured for your vCenter instance or on your ESX server.



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, check the **Use Private IP Address** box to scan internal IP addresses.
7. Under **Actions**, select **Show asset as Smart Group**.
8. Click **Create Smart Rule**.
9. Run a Discovery Scan on the Smart Group to see the cloud assets in reports.
10. On the **Assets** page, select the cloud connector, and then click the 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 in to the **AWS Management Console**.
2. Select **Identity & Access Management**.
3. Select **Policies** from the **Details** menu.
4. Select **Create Policy**.
5. Select **Create Your Own Policy**.
6. Enter a policy name and description.
7. Paste the following JSON into **Policy Document**:

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

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

Grant Access to a Third Party (Optional)

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

After you configure the AWS settings, you can create the connector and Smart Groups in the BeyondInsight Console.

Set BeyondInsight Options

Set Account and Email Options

Account Lockout Options

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

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

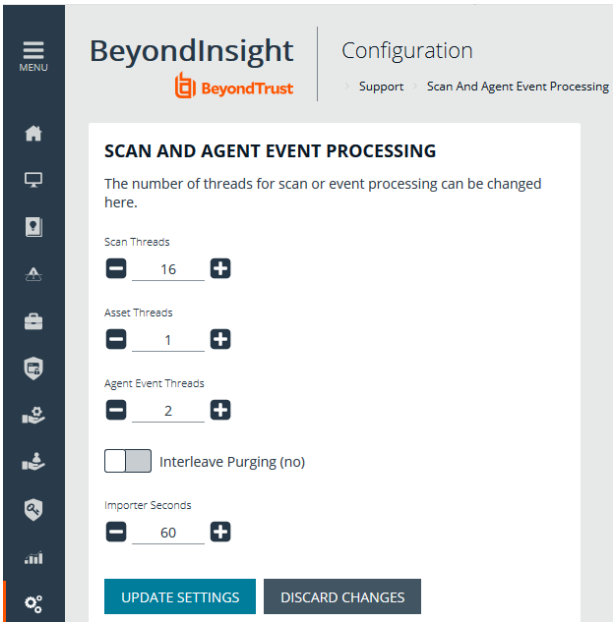
Account Password Options

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**.

Set Scan and Event Processing Options

1. 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**.
2. 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 in to the management console using Active Directory or LDAP credentials. When this site setting is enabled, the user can select a domain or LDAP server. Domain and LDAP server information is based on the Active Directory and LDAP user group information.

Note: *The log in to list is only displayed on the* ***Login*** *page when there are either Active Directory 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. In the BeyondInsight Console, go to **Configuration > System > Site Options**.
2. Under**Login Page**, click the toggle to disable **Show list of domains/LDAP servers on login page**.
3. Click **Update Login Page Options**.

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

Display Forgot Password Link

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

1. In the BeyondInsight Console, go to **Configuration > System > Site Options**.
2. Under **Login Page**, click the toggle to disable **Show Forgot Password link on login page**.
3. Click **Update Login Page Options**.

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

Display Social Media links on the Login and About pages

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

1. In the BeyondInsight Console, go to **Configuration > System > Site Options**.
2. Under **Login Page**, click the toggle to turn off **Show social media links on login and about pages**.
3. Click **Update Login Page Options**.

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

Change the Refresh Interval for Smart Rules

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

1. In the BeyondInsight Console, go to **Configuration > System > Site Options**.
2. Under **General**, set the number of minutes for **Maximum Smart Rule refresh frequency for asset updates**. The default is **60**.
3. 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. In the BeyondInsight Console, go to **Configuration > System > Site Options**.
2. Under **Pre-Login Banner**, click the toggle to enable the **Show Banner**.
3. 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

1. In the BeyondInsight Console, go to **Configuration > System > Site Options**.
2. 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 notifies 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.
3. 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. In the BeyondInsight Console, go to **Configuration > System > Site Options**.
2. Under **Localization**, click the toggle to enable the **Show language picker**.
3. 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.*

Configure a Claims-Aware Website to Log In with SAML

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

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

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

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

Create a BeyondInsight Group

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

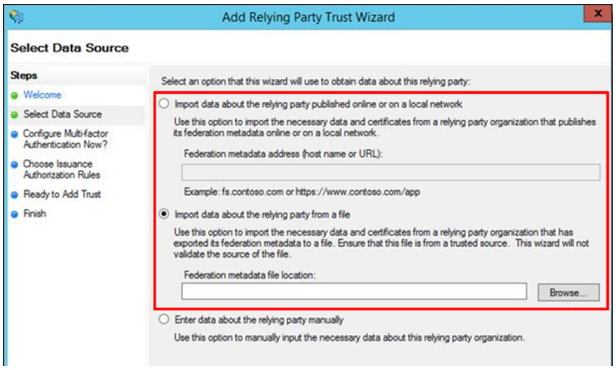
Add Relying Party Trust

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

The metadata is located in the following directory:

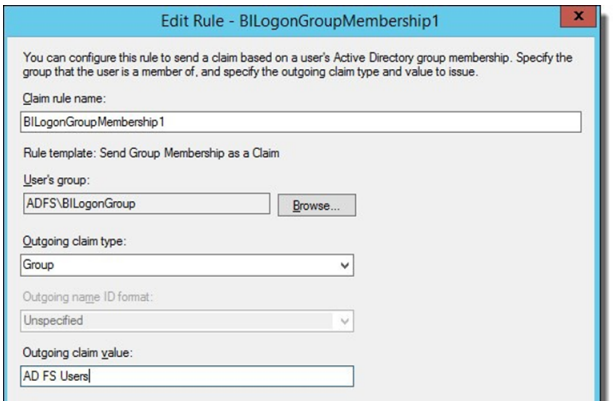
<Install path>\eEye Digital Security\Retina CS\WebSiteClaimsAware\FederationMetadata\2007-06

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



Set Up Claim Rules

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



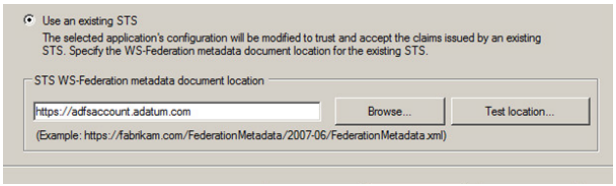
Supported Federation Service Claim Types

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

Claims-Aware SAML

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

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

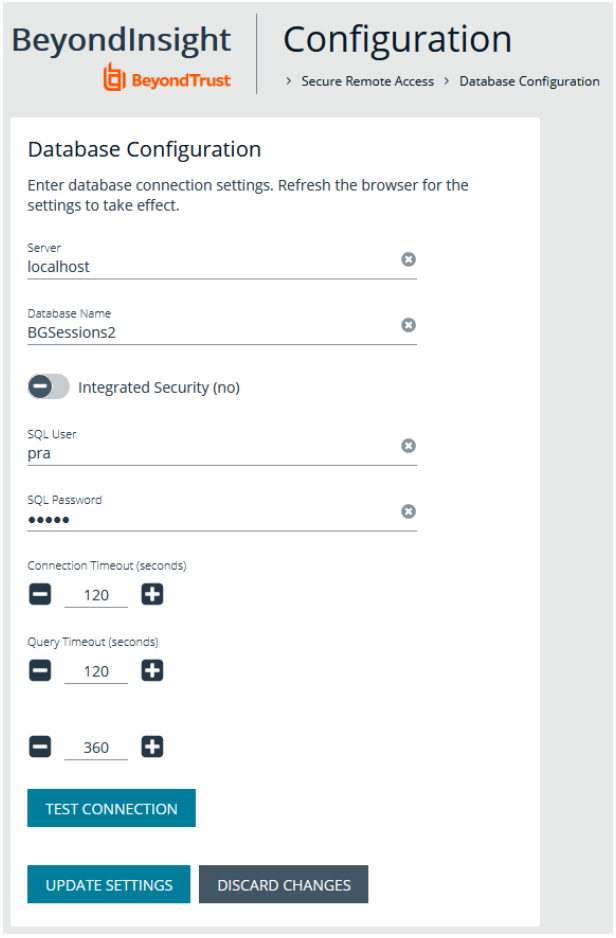


View Privileged Remote Access Data

If you have a licensed instance of Privileged Remote Access configured in your environment, you can export session data to an export database. You can then review Privileged Remote Access session data in the BeyondInsight Console, using the Privileged Remote Access Dashboard.

Configure the Privileged Remote Access Database Connection

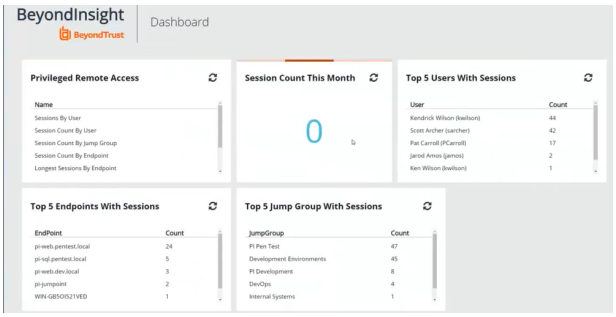
1. In the BeyondInsight Console, select **Configuration**.
2. Under **Secure Remote Access**, select **Database Configuration**.
3. Provide the settings to connect to your Privileged Remote Access export database, and then click **Test Connection**.
4. Click **Update Settings**.



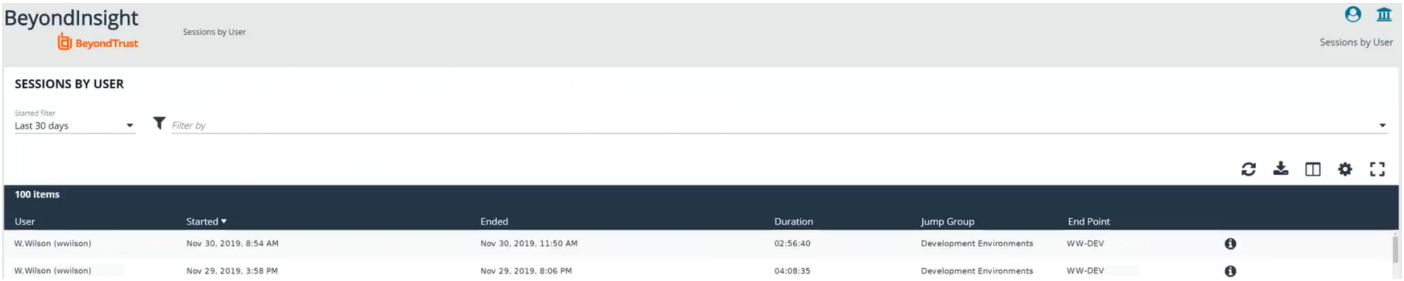
View the Privileged Remote Access Dashboard

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

2. In the Dashboard you can quickly view a summary of Privileged Remote Access session data in each card.



3. You can click the items within each card to review the specific records for that item in a grid view that can be sorted, filtered, and exported as required.



Integrate the BeyondInsight API into Other Applications

You can integrate part of BeyondInsight's API into your applications using an API key.

> ***Note:*** *The **API Registration** page is only available to BeyondInsight administrators.*

The ID and key are generated by BeyondInsight.

1. Select **Configuration > General > API Registrations**.
2. Enter a name for the registration.
3. Click **Create New API Registration** to create a new application registration.

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

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

4. To configure a new registration or modify an existing one, select the registration, and then set the **Authentication Rule Options**.
    - **Client Certificate Required:** If enabled, a client certificate is required with the web request. If not, client certificates are ignored and do not need to be present. A valid client certificate is any client certificate signed by a certificate authority trusted by the server on which BeyondInsight resides.
    - **User Password Required:** If enabled, an additional authorization header value containing the **RunAs** user password is required with the web request. If not enabled, this header value does not need to be present and is ignored if provided. Square brackets surround the password in the header.

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

    - **Verify PSRUN Signature:** The PSRUN signature is an extra level of authentication. It is computed from the factors using a shared secret between the client and server. PSRUN sends the signature as part of the header during its API request. If enabled, the server recomputes the signature during factor validation and compares it against the one sent by the client. If the signatures match, the client's identity is considered verified. The signature effectively keeps the client in sync with the server. Changing the secret on the server requires the client to be rebuilt and guarantees that out-of-date clients cannot authenticate.
5. On the **Details** page, click **Add Authentication Rule** to create authentication rules. At least one IP rule, PSRUN rule, valid source IP address (IPv4 or IPv6), IP range, or CIDR from which requests can be sent for this API Key is required. Enter one IP address, IP Range, or CIDR per line.

   X-Forwarded-For rules can also be created by providing a valid source IP address (IPv4 or IPv6), an IP range, or CIDR. In a load-balanced scenario, IP Authentication rules are used to validate the load balancer IP(s), and the X-Forwarded-For header is used to validate the originating client IP. Existing rules cannot be changed from an IP Rule to a X-Forwarded-For Rule or vice-versa. If an X-Forwarded-For rule is configured, it is required for the HTTP Request . If the X-Forwarded-For header is missing, the request fails with a *401 unauthorized* error.
6. Click **Create Rule**.