



# BeyondTrust

## **BeyondInsight User Guide 21.2**

## Table of Contents

---

<b>BeyondInsight User Guide</b> .....	<b>6</b>
Components .....	6
Log In to the BeyondInsight Console .....	8
Navigate the Console .....	9
Dynamic Dashboards .....	10
Customize a Dashboard .....	11
Access Dashboard Tile Information .....	12
Change and Reset Login Passwords .....	12
Change and Set the Console Display and Preferences .....	15
Role-Based Access .....	17
Create and Edit Directory Credentials .....	17
Create and Configure Groups .....	19
Create a BeyondInsight Local Group .....	19
Add an Active Directory Group .....	21
Add an LDAP Directory Group .....	24
Assign Permissions .....	27
Assign Group Permissions .....	27
Assign Features Permissions .....	28
Assign Smart Groups Permissions .....	31
Edit and Delete Groups .....	31
Edit Basic Group Details .....	31
Edit Advanced Group Details .....	32
Delete a Group .....	36
Create and Manage User Accounts .....	36
Create a BeyondInsight Local User Account .....	37
Add an Active Directory User .....	37
Add an LDAP User .....	39
Edit a User Account .....	40
Add Groups to User .....	41
Delete a User Account .....	42
Audit Console Users in BeyondInsight .....	43

---

Overview of BeyondInsight Tools .....	44
Create an Address Group .....	44
Create a Directory Query .....	47
Attributes and Attribute Types .....	48
Use Smart Rules to Organize Assets .....	50
Use Smart Rule Filters and Smart Groups .....	50
Smart Rule Filters .....	51
Predefined Smart Group Categories .....	52
Create Smart Rules .....	52
Smart Rule Processing .....	53
Perform Other Smart Rule Actions .....	54
Add Credentials for Use in Scans .....	58
Create Oracle Credentials .....	61
Create SNMP Credentials .....	62
Create SSH Credentials .....	62
Run Discovery Scans .....	64
Use the Scan Wizard to Create a Discovery Scan .....	64
Run Scans from a List of Assets .....	65
Use Smart Rules as Targets for Scans .....	66
Check Completed Scans .....	67
Discover Assets Using a Smart Group .....	67
Manage Scan Jobs .....	69
Manage Assets .....	70
Review Asset Details .....	70
Create Assets .....	71
Delete Assets .....	72
Run Scans on Cloud Platforms in BeyondInsight .....	74
Configure a Cloud Connector .....	76
Cloud Connector Smart Groups .....	77
Configure BeyondInsight AWS Connector .....	77
Work with the Multi-Tenant Feature in BeyondInsight .....	79
Set Up Organizations .....	81
Set BeyondInsight Options .....	83

---

Set Account and Email Options .....	83
Account Lockout Options .....	83
Account Password Options .....	83
Email Notifications .....	84
Set Support Options .....	84
Set Data Retention and Advanced Purging Options .....	87
Data Retention .....	87
Purging Options .....	90
Configure Proxy Settings .....	90
Configure Discovery Management Options .....	91
Set Scan and Event Processing Options .....	91
Configure Global Website Options .....	91
BeyondInsight Clarity Analytics .....	95
Configure BeyondInsight Clarity Analytics .....	95
Clarity Reports .....	96
Use the Clarity Dashboard .....	96
View Cluster Maps .....	98
Analyze Cluster Maps .....	99
Analyze Cluster Grids .....	100
Alerts in BeyondInsight Clarity Analytics .....	100
BeyondInsight Clarity Malware Analysis .....	102
Configure Clarity Malware .....	102
Review Malware Information and Reports .....	102
Configure a Claims-Aware Website to Authenticate against SAML .....	104
Manage Endpoint Privilege Management Events .....	106
Exclude Endpoint Privilege Management Events .....	107
Create and View Smart Rules for Endpoint Privilege Management Policy Users .....	108
Manage Endpoint Privilege Management Policies .....	110
View Endpoint Privilege Management Agents .....	113
View Endpoint Privilege Management File Integrity Monitoring .....	113
Monitor Endpoint Privilege Management Sessions .....	114
View Privileged Remote Access Data .....	116
Integrate the BeyondInsight API into Other Applications .....	118

---

Support and Product Updates .....	119
Send Files to BeyondTrust Technical Support .....	119
Download Updates .....	119
Maintenance Information .....	120

# BeyondInsight User Guide

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

This guide provides instructions and procedures for using BeyondInsight.

## Components

### Discovery Scanner

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

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

### Manager Service

This component is the BeyondInsight web interface.

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

### Application Bus (AppBus)

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

### Events Client

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

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

### Events Client Certificate

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

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

### Central Policy Server

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

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

### Scheduling Service

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

## Log In to the BeyondInsight Console

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

The following authentication types can be used:

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



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

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



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

3. Enter your username and password.
4. The default username is **Administrator**, and the password is the administrator password you set in the Configuration Wizard.
5. If applicable, select a domain.
6. Click **Login**.



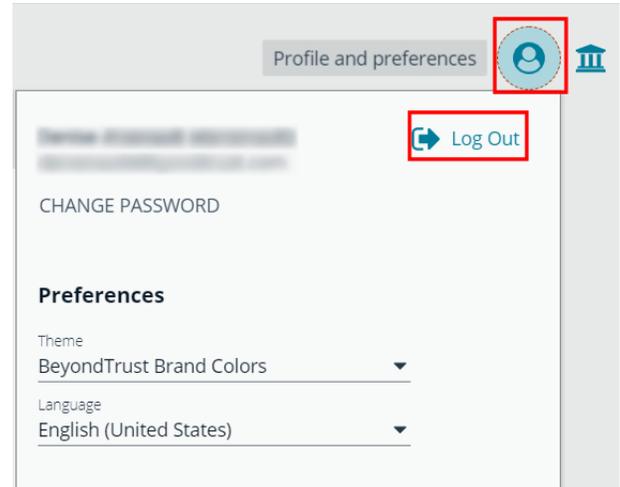
**Note:** If the initial login attempt fails, and two-factor authentication (2FA) is enabled, the user is taken to the 2FA page for security reasons.



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

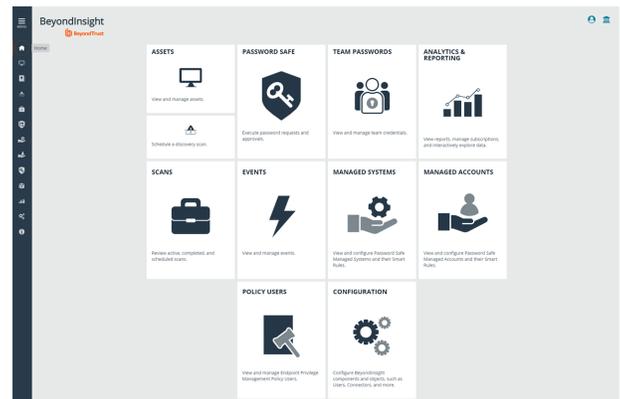
## Log Out of the Console

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



Available features include:

- **Assets:** Display and manage all assets. Access the **Smart Rules** page to create and manage Smart Groups. Add assets to Password Safe management.
- **Smart Rules:** View and manage Smart Rules.
- **Scan:** Schedule Discovery Scans.
- **Scans:** Review active, completed, and scheduled scans.
- **Endpoint Privilege Management:** View and manage Endpoint Privilege Management events, policies, policy users, agents, file integrity monitoring, and session monitoring.
- **Managed Systems:** View and configure properties for Password Safe managed systems, managed databases, managed directories, managed applications, and their associated Smart Rules.
- **Managed Accounts:** View and configure properties for Password Safe managed accounts and their associated Smart Rules.

- **Password Safe:** Access the Password Safe web portal to request passwords and remote access sessions and to approve requests.
- **Team Passwords:** View and manage team credentials.
- **Analytics & Reporting:** Access reports on collected data.
- **Configuration:** Configure BeyondInsight and Password Safe components and objects, such as users and groups, authentication settings, connectors, and much more.
- **About:** Access helpful links, support tools, version information, and the maintenance expiry date. The **Maintenance Expiry Warning Banner** can be disabled here.

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

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

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

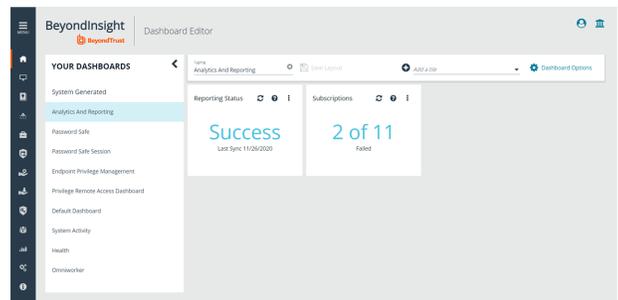
## Dynamic Dashboards

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

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

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

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



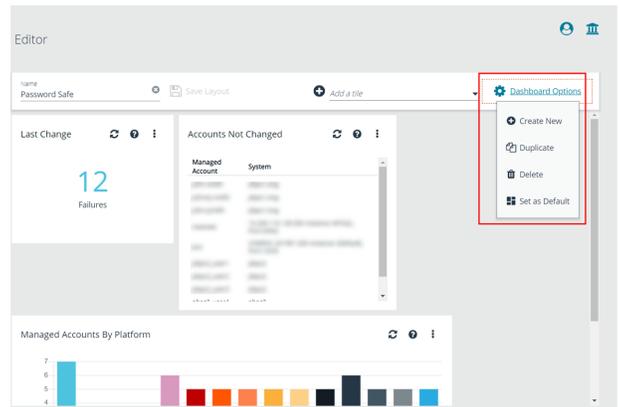
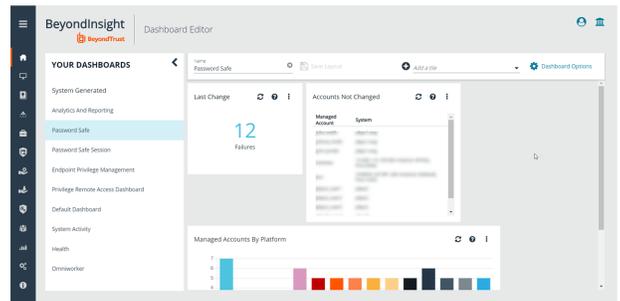
 **Note:** The list of system-generated dashboards displayed can change depending on licensing, as well as data available in the system, and configuration settings. This also affects what tiles are shown in the **Add a tile** dropdown list.

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:

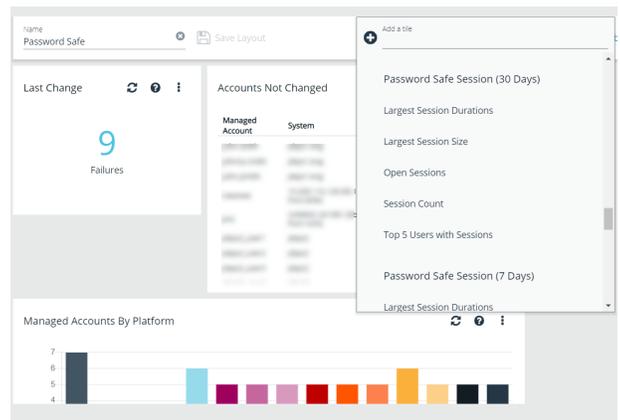
- **Create New:** Create a new empty dashboard, then add the tiles you want.
- **Duplicate:** Create a copy of the dashboard that can be modified.
- **Delete:** Delete the selected dashboard.
- **Set as Default:** Set the current dashboard as the default so it displays every time you click on **Menu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

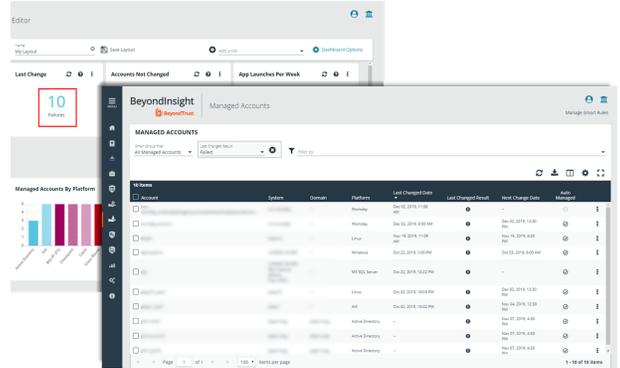
1. To create a custom dashboard, select one of the available dashboard cards. In this example we use the **Password Safe** card. If necessary, delete any of the existing tiles that come installed with that card.
2. From the **Add a tile** dropdown, select the tiles you want to add. Resize and reposition 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.



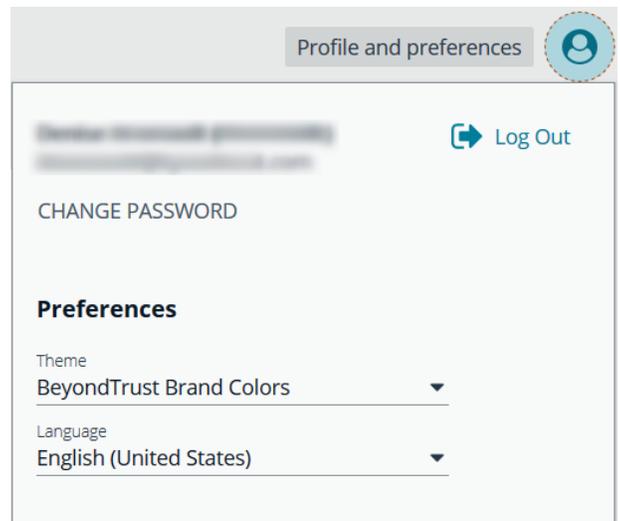
## Change and Reset Login Passwords

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**.

## Change Password

 *Current Password* \_\_\_\_\_

 *New Password* \_\_\_\_\_  
Password must be at least 10 characters long

 *Confirm New Password* \_\_\_\_\_

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.



## PLEASE LOG IN

 *Username* \_\_\_\_\_  
Username is required

 *Password* \_\_\_\_\_

 *Log in to* \_\_\_\_\_ ▾

Forgot Password?

LOG IN

If you are having trouble logging in or have forgotten your username or password, please contact your Administrator.

 English (United Sta... ▾



Copyright © 1999-2019 BeyondTrust Corporation. All Rights Reserved.

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.*



## RESET PASSWORD



*New Password*

Password must be at least 10 characters long



*Confirm New Password*

CHANGE PASSWORD

## Change and Set the Console Display and Preferences

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

### Set Display Preferences

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

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

1. Select an area of the site, such as **Assets**.
2. Above the grid, 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.

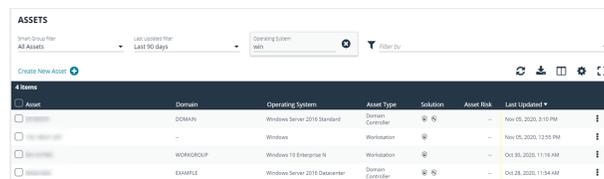
### Filter Records

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.



Asset	Domain	Operating System	Asset Type	Solution	Asset Risk	Last Updated
EXAMPLE	DOMAIN	Windows Server 2016 Standard	Domain Controller	IS	...	Nov 05, 2020, 3:10 PM
EXAMPLE	...	Windows	Workstation	IS	...	Nov 05, 2020, 12:55 PM
EXAMPLE	WORKGROUP	Windows 10 Enterprise N	Workstation	IS	...	Oct 30, 2020, 11:16 AM
EXAMPLE	EXAMPLE	Windows Server 2016 Datacenter	Domain Controller	IS	...	Oct 28, 2020, 11:54 AM

## Customize Console Logos

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



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

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

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



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

## Role-Based Access

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

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

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



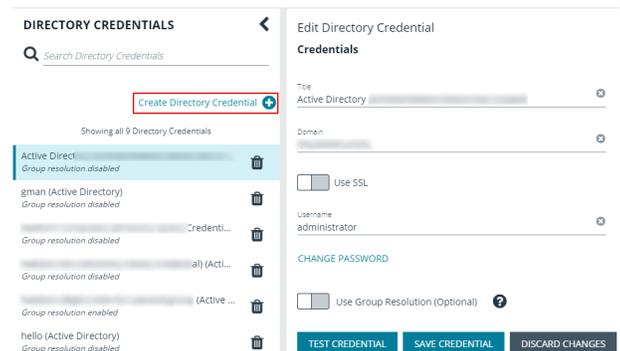
**Note:** By default, an **Administrators** user group is created. The permissions assigned to the group cannot be changed. The user account you created when you configured BeyondInsight is a member of the group.

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

## Create and Edit Directory Credentials

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

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



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



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

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



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

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

## New Directory Credential

### Directory Type

- Active Directory
- LDAP

### Credentials

Title

Domain

Use SSL

Username

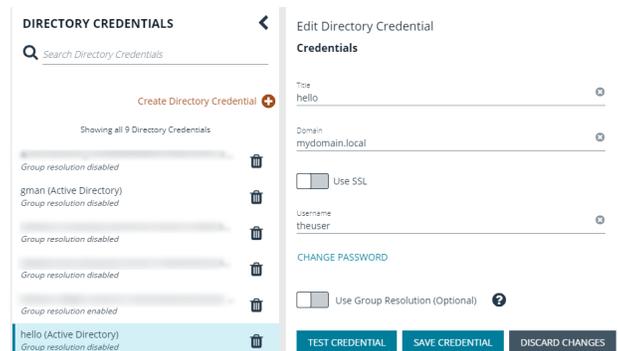
Password

Use Group Resolution (Optional) ?

TEST CREDENTIAL

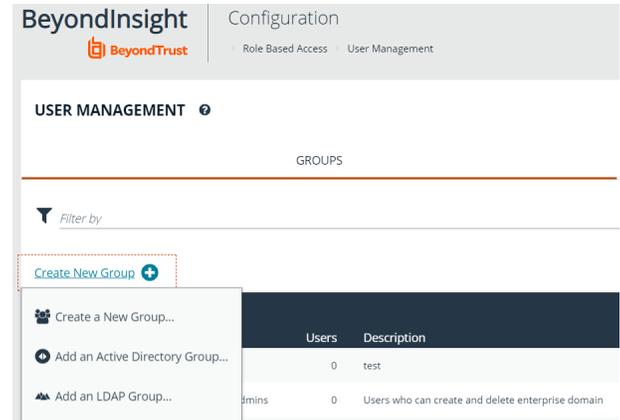
SAVE CREDENTIAL

DISCARD CHANGES

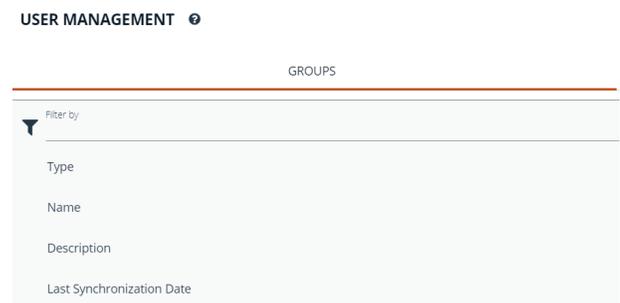


## Create and Configure Groups

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



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



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



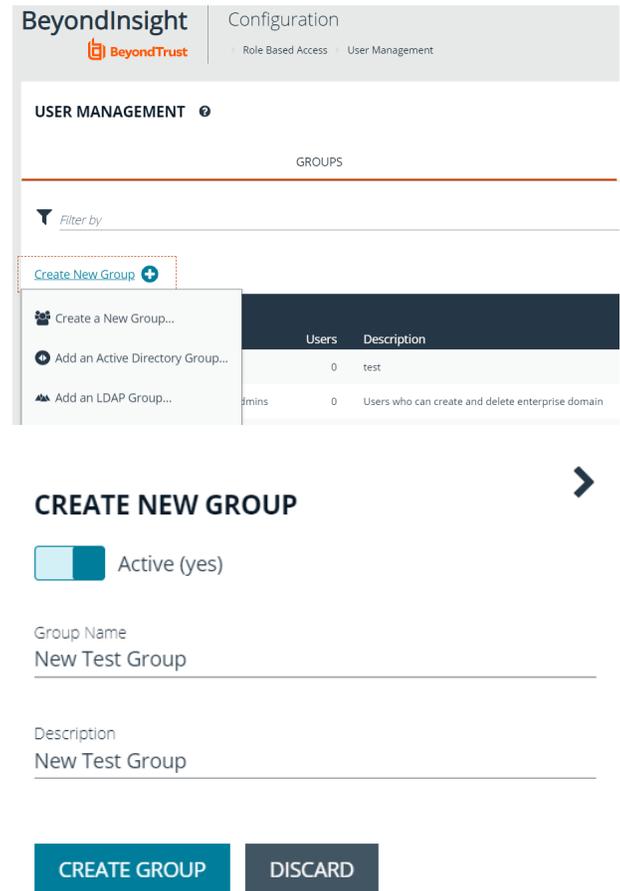
After a group is created, add user accounts to the group. When a user is added to a group, the user is assigned the permissions assigned to the group.

### Create a BeyondInsight Local Group

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

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

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



**Configuration**

Role Based Access | User Management

**USER MANAGEMENT**

GROUPS

Filter by

Create New Group +

- Create a New Group...
- Add an Active Directory Group...
- Add an LDAP Group...

Users	Description
0	test
0	Users who can create and delete enterprise domain

**CREATE NEW GROUP**

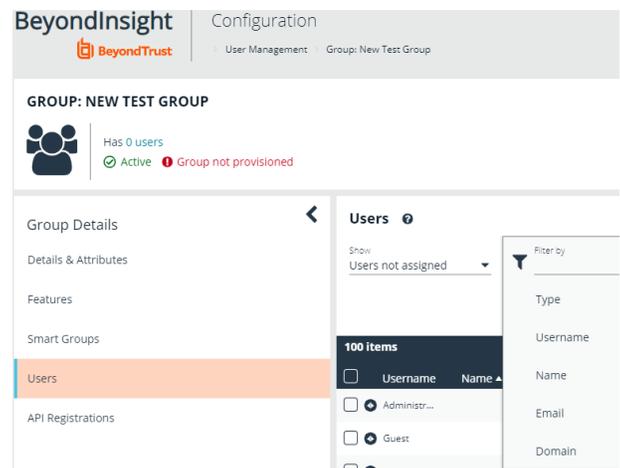
Active (yes)

Group Name  
New Test Group

Description  
New Test Group

CREATE GROUP DISCARD

8. 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.



**Configuration**

User Management | Group: New Test Group

**GROUP: NEW TEST GROUP**

Has 0 users  
Active Group not provisioned

Group Details

- Details & Attributes
- Features
- Smart Groups
- Users**
- API Registrations

Users

Show: Users not assigned

Filter by

- Type
- Username
- Name
- Email
- Domain

100 items

Username	Name
Administr...	
Guest	
...	

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

**Users** ⓘ

Show: Users not assigned ▾ Username: name ✕ Filter by: ▾

**Assign User** +

**7 items (6 selected)**

<input type="checkbox"/>	Username	Name ▲	Email	Domain
<input checked="" type="checkbox"/>	a.name4	a.name4	e@mail4.null	n
<input checked="" type="checkbox"/>	a.name5	a.name5	e@mail5.null	n
<input checked="" type="checkbox"/>	a.name6	a.name6	e@mail6.null	n
<input checked="" type="checkbox"/>	a.name7	a.name7	e@mail7.null	n
<input checked="" type="checkbox"/>	a.name8	a.name8	e@mail8.null	n
<input checked="" type="checkbox"/>	a.name9	a.name9	e@mail9.null	n

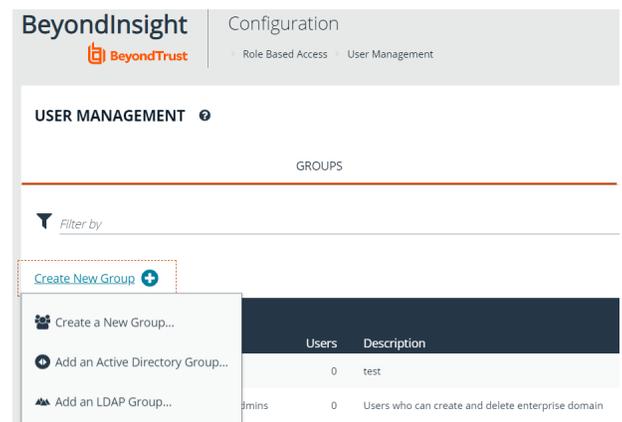
 **Note:** By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "[Assign Group Permissions](#)" on page 27.

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



**BeyondInsight** Configuration

Role Based Access > User Management

**USER MANAGEMENT** ⓘ

GROUPS

Filter by: ▾

**Create New Group** +

- Create a New Group...
- Add an Active Directory Group...**
- Add an LDAP Group...

Users	Description
0	test
0	Users who can create and delete enterprise domain

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

### ACTIVE DIRECTORY GROUP SEARCH ➤

Credential  
 ... ▼  
[Manage Credentials...](#)

Domain

Filter by Group Name

SEARCH ACTIVE DIRECTORY
CANCEL

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



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

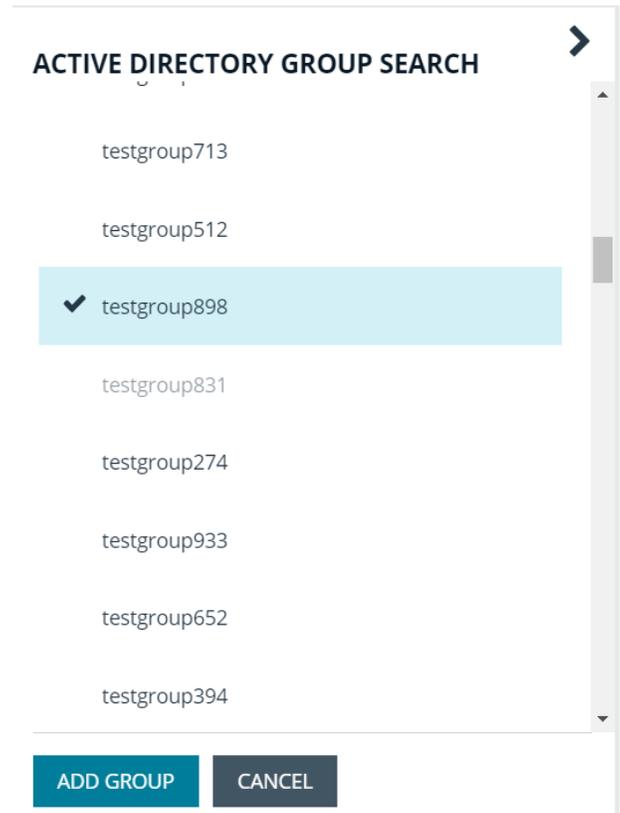
8. Set a filter on the groups to refine the list, and then click **Search Active Directory**.



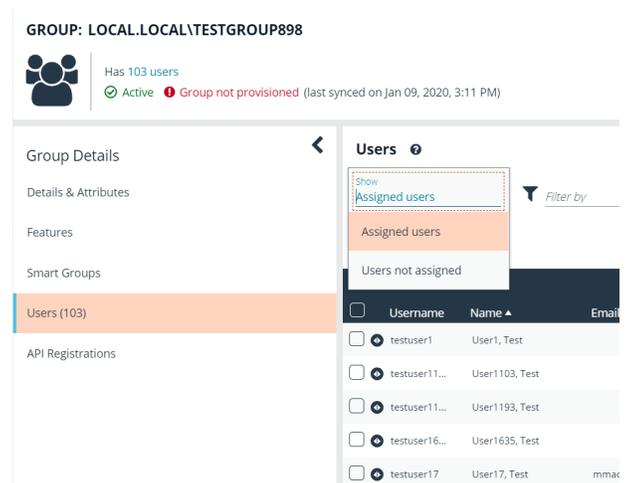
**Example:** Sample filters:

- **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

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



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



**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 27.

**i** For more information on creating and editing directory credentials, please see ["Create and Edit Directory Credentials"](#) on page 17.

## 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.

### Edit test.local\BIDemo

[Go to advanced details...](#)

Active (yes)

Name  
test.local\BIDemo

Description  
--

Credential  
test sflight creds for userand grou (test.local)   
[Manage Credentials...](#)

Domain / Domain controller  
Any domain controller  

Propagate this change to all group members (no)





## Add an LDAP Directory 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.



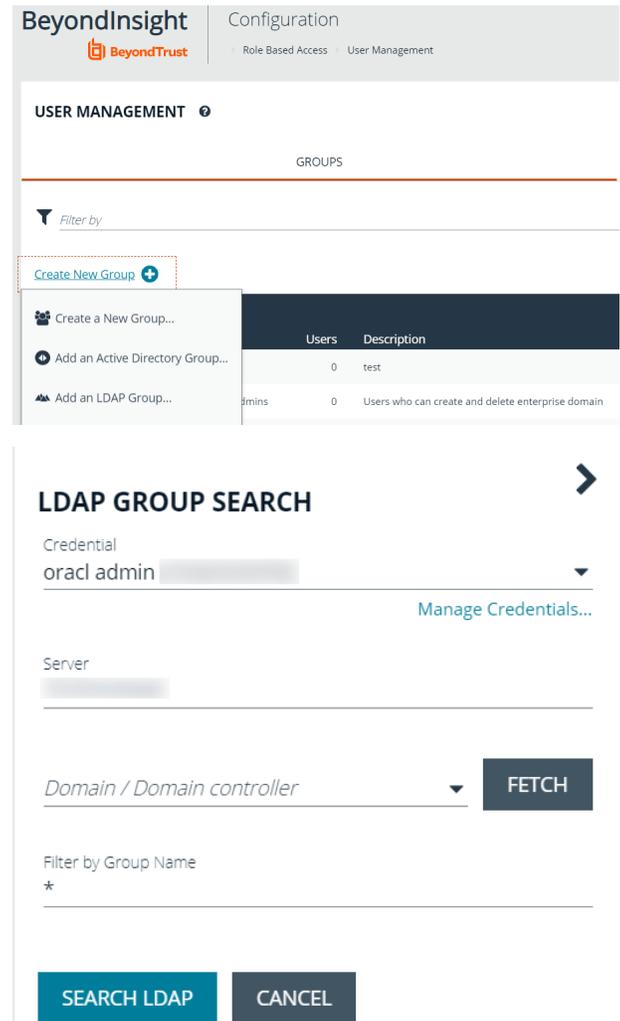
**Note:** LDAP users must log in to the management console at least once to receive email notifications.

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

3. Under **Groups**, click **Create New Group**.
4. Select **Add an LDAP Directory Group** from the list.

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

**i** For more information on creating and editing directory credentials, please see *"Create and Edit Directory Credentials"* on page 17.



**BeyondInsight** Configuration  
 > Role Based Access > User Management

**USER MANAGEMENT** ⓘ

GROUPS

Filter by

Create New Group +

- Create a New Group...
- Add an Active Directory Group...
- Add an LDAP Group...

Users	Description
0	test
0	admins Users who can create and delete enterprise domain

**LDAP GROUP SEARCH** >

Credential  
 oracl admin  Manage Credentials...

Server

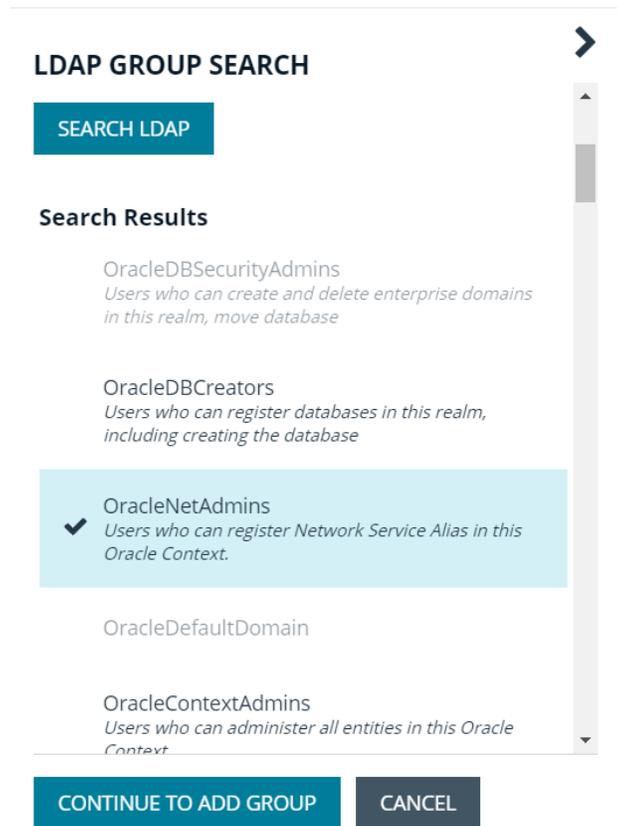
Domain / Domain controller  **FETCH**

Filter by Group Name  
 \*

**SEARCH LDAP** **CANCEL**

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

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



**LDAP GROUP SEARCH**

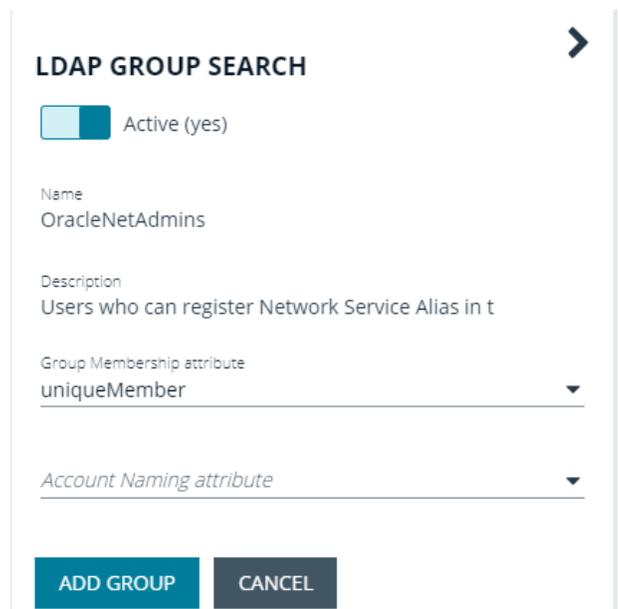
SEARCH LDAP

**Search Results**

- OracleDBSecurityAdmins  
*Users who can create and delete enterprise domains in this realm, move database*
- OracleDBCreators  
*Users who can register databases in this realm, including creating the database*
- OracleNetAdmins  
*Users who can register Network Service Alias in this Oracle Context.*
- OracleDefaultDomain
- OracleContextAdmins  
*Users who can administer all entities in this Oracle Context*

CONTINUE TO ADD GROUP CANCEL

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



**LDAP GROUP SEARCH**

Active (yes)

Name  
OracleNetAdmins

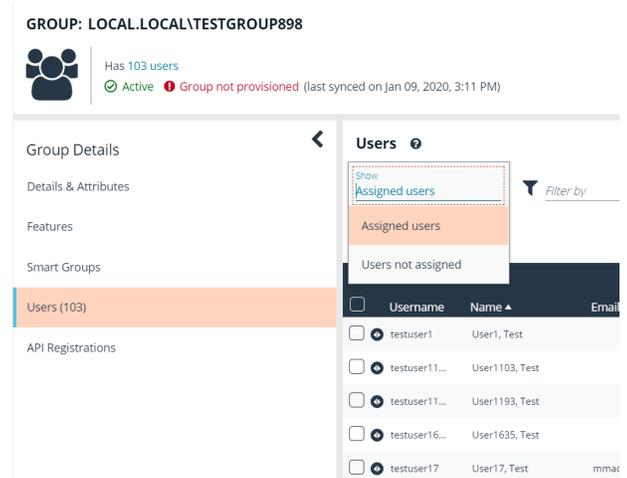
Description  
Users who can register Network Service Alias in t

Group Membership attribute  
uniqueMember

Account Naming attribute

ADD GROUP CANCEL

- 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.



**GROUP: LOCAL.LOCAL\TESTGROUP898**

Has 103 users  
● Active ● Group not provisioned (last synced on Jan 09, 2020, 3:11 PM)

Group Details

- Details & Attributes
- Features
- Smart Groups
- Users (103)**
- API Registrations

**Users**

Show  
 Assigned users  
 Users not assigned

Filter by

<input type="checkbox"/>	Username	Name	Email
<input checked="" type="checkbox"/>	testuser1	User1, Test	
<input checked="" type="checkbox"/>	testuser11...	User1103, Test	
<input checked="" type="checkbox"/>	testuser11...	User1193, Test	
<input checked="" type="checkbox"/>	testuser16...	User1635, Test	
<input checked="" type="checkbox"/>	testuser17	User17, Test	mmac

 **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 27.

 For more information on creating and editing directory credentials, please see "[Create and Edit Directory Credentials](#)" on page 17.

## Assign Permissions

### Assign Group Permissions

## Permissions

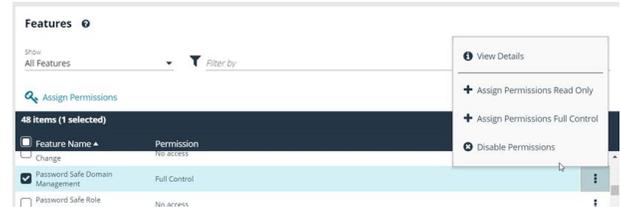
Permission	Description
No Access	Users cannot access the selected feature. In most cases, the feature is not visible to the users.
Read Only	Users can view selected areas, but cannot change information.
Full Control	Users can view and change information for the selected feature.

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



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

Feature	Provides Permissions To:
Analytics & Reporting	<p>Log in to the console and access <b>Analytics &amp; Reporting</b> to generate and subscribe to reports.</p> <div style="border: 1px solid black; background-color: #e1f5fe; padding: 5px;"> <p> <b>Note:</b> After you create a group, go to the <b>Analytics &amp; Reporting Configuration</b> page and run the process daily cube job. Data between the management console and the reporting cube must be synchronized.</p> </div>
Asset Management	<p>Create Smart Rules.</p> <p>Edit and delete buttons on the <b>Asset Details</b> window.</p> <p>Create Active Directory queries.</p> <p>Create address groups.</p>
Attribute Management	Add, rename, and delete attributes when managing user groups.
Audit Manager	<b>User Audits</b> on the <b>Configuration</b> 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.
	<div style="border: 1px solid black; background-color: #e1f5fe; padding: 5px;"> <p> <b>Note:</b> Access to <b>Directory Credential Management</b> must also be granted.</p> </div>
File Integrity Monitoring	Work with <b>File Integrity</b> rules.
License Reporting	View the <b>Licensing</b> folder in <b>Analytics &amp; Reporting</b> (MSP reports, Privilege Management for Windows, Privilege Management for Mac true-up reports, and Assets Scanned report) .
Management Console Access	Access the BeyondInsight management console.
Manual Range Entry	Allow the user to manually enter ranges for scans and deployments rather than being restricted to Smart Groups. The specified ranges must be within the selected Smart Group.
Option Management	Change the application options settings (for example, account lockout and account password settings).
Options - Connectors	Access the configuration area where connectors are managed.
Options - Scan Options	Access the configuration area where scan options are managed.

Feature	Provides Permissions To:
Password Safe Account Management	Grants permissions to the following features on the <b>Managed Accounts</b> page and through the public API: <ul style="list-style-type: none"> <li>• Bulk delete accounts</li> <li>• Add accounts to a Quick Group</li> <li>• Remove accounts from a Quick Group</li> <li>• Add, edit, and delete accounts</li> </ul>
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	Allow a user to assign permissions as <b>Read Only</b> , or <b>Full Control</b> .
Password Safe Role Management	Allow a user to manage roles, provided they have the following permissions: <b>Password Safe Role Management</b> and <b>User Account Management</b> .
Password Safe System Management	Read and write managed systems through the public API.
Password Safe Ticket System Management	This feature is not presently used.
Reports Management	Run scans, create reports, and create report categories.
Scan - Audit Groups	Create, delete, update, and revert audit group settings.
Scan - Job Management	Activate <b>Scan</b> and <b>Start Scan</b> buttons.  Activate <b>Abort</b> , <b>Resume</b> , <b>Pause</b> , and <b>Delete</b> on the <b>Job Details</b> page.
Scan - Policy Manager	Activate the settings on the <b>Edit Scan Settings</b> 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: <ul style="list-style-type: none"> <li>• Export Type</li> <li>• Notify when complete</li> <li>• Email report to</li> <li>• Include scan metrics in email (only available for All Audits Scan, and PCI Compliance Report)</li> </ul>
Scan Management	Delete, edit, duplicate, and rename reports on the <b>Manage Report Templates</b> page.  Activate <b>New Report</b> and <b>New Report Category</b> .  Activate the <b>Update</b> button on the <b>Edit Scan Settings</b> view.
Session Monitoring	Use the session monitoring features.
Smart Rule Management - Asset	Users can create and edit asset-based Smart Rules.
Smart Rule Management - Managed Account	Users can create and edit Managed Account Smart Rules.

Feature	Provides Permissions To:
Smart Rule Management - Managed System	Users can create and edit Managed System Smart Rules.
Smart Rule Management - Policy User	Users can create and edit Policy Smart Rules.
Smart Rule Omni Worker Options	Users can configure Smart Rule Omni Worker Options, such as multi-worker node usage, number of Smart Rule threads per type, and failure thresholds.
Team Passwords	Users can access the Team Passwords feature.
Ticket System	View and use the ticket system.
Ticket System Management	Mark a ticket as inactive. The ticket no longer exists when <b>Inactive</b> is selected.
User Accounts Management	Add, delete, or change user groups and user accounts.  <div style="border: 1px solid black; padding: 5px; background-color: #e0f0ff;">  <b>Note:</b> A minimum of read access to Directory Credential Management must also be granted to enable creation of AD and LDAP Groups. </div>
User Audits	View audit details for management console users on the <b>User Audits</b> page.



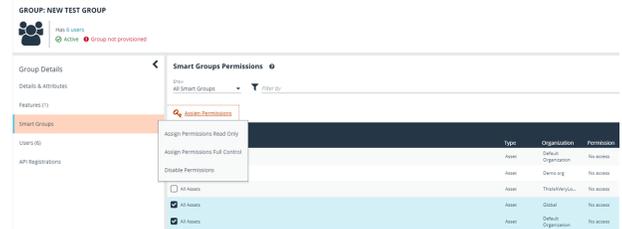
For more information, please see [Managed Accounts](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/api/password-safe/managed-accounts.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/api/password-safe/managed-accounts.htm>.

## Feature Permissions Required for Configuration Options

Configuration Option	Feature and Permission
Active Directory Queries	Asset Management - Full Control
Address Groups	Asset Management - Full Control
Attributes	Asset Management - Full Control
Connectors	Asset Management and Management Console Access - Full Control
Organizations	User Accounts Management - Full Control
Password Safe Connections	Member of the built-in BeyondInsight Administrators group
Scan Options	Scan Management - Full Control
Services	Member of the built-in BeyondInsight Administrators group
User Audits	User Audits - Full Control
User Management	User and Group Management - Full Control
Workgroups	User Accounts Management - Full Control

## Assign Smart Groups Permissions

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



## Edit and Delete Groups

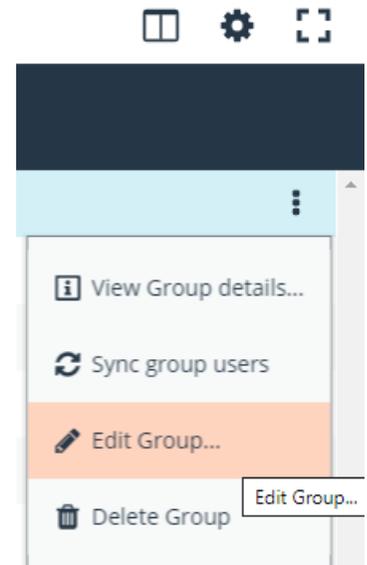
### Edit Basic Group Details

Administrators can edit the following basic details for groups:

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

Follow these steps to edit a group:

1. 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 **More Options** button, then select **Edit Group**.



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

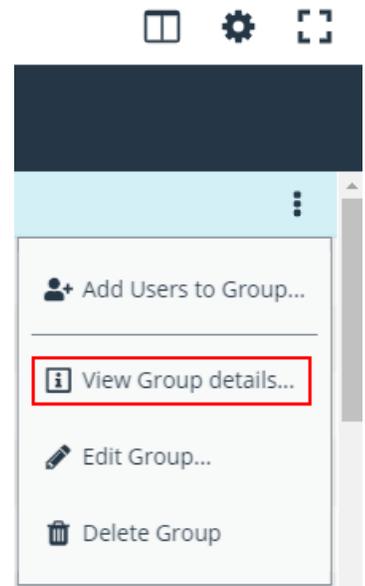
- For LDAP groups, administrators can change the active status, credential, group membership attribute, and account naming attribute.

### Edit Advanced Group Details

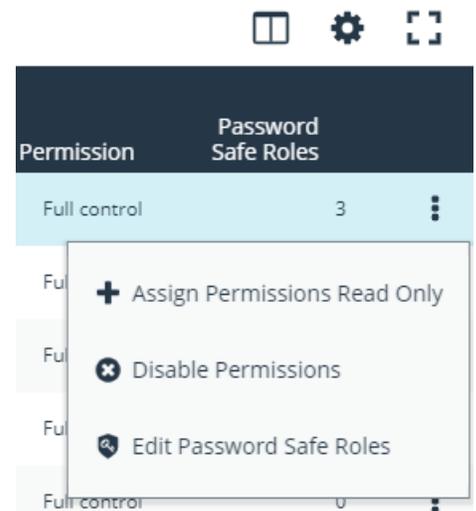
Administrators can edit advanced details, such as update permissions for features and smart groups, edit Password Safe roles, add and remove users from local groups, sync group users for Active Directory and LDAP groups, and update the API registrations.

### Update Group Permissions for Features and Smart Groups

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



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

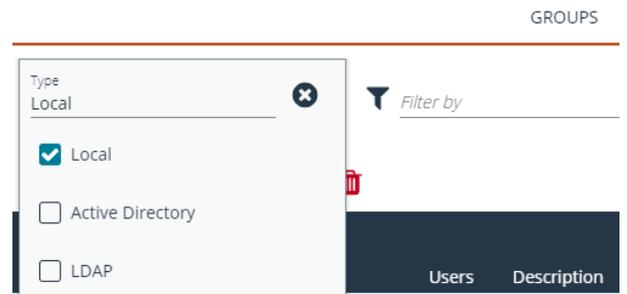


## Remove Users from Local BeyondInsight Groups

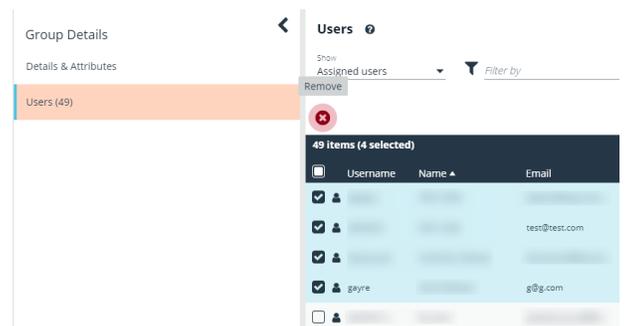
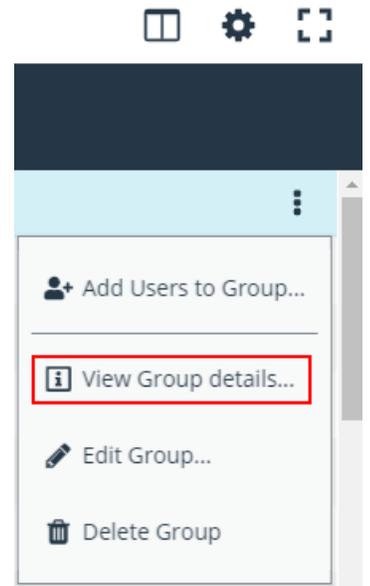
1. On the **User Management** page, filter the grid by local groups.



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

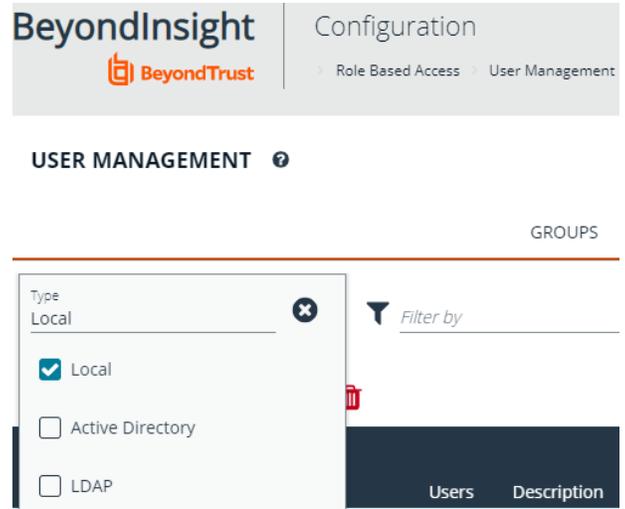


3. Under **Group Details**, select **Users**.
4. Filter the **Users** grid to show assigned users.
5. Select the user or users, and then click the **Remove** button.

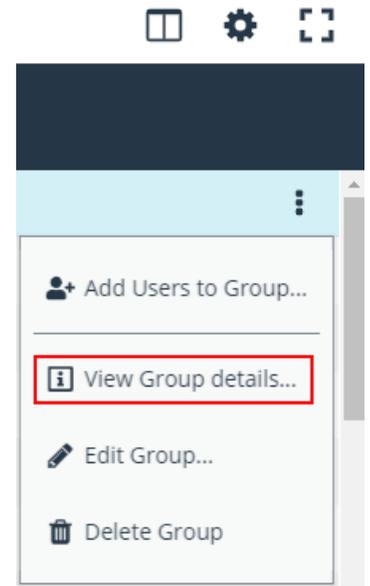


## Add Users to Local BeyondInsight Groups

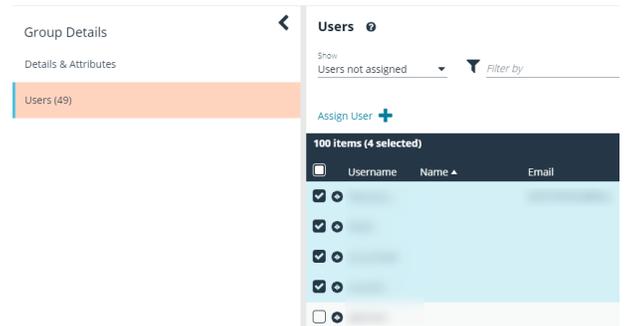
1. On the **User Management** page, filter the grid by local groups.



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

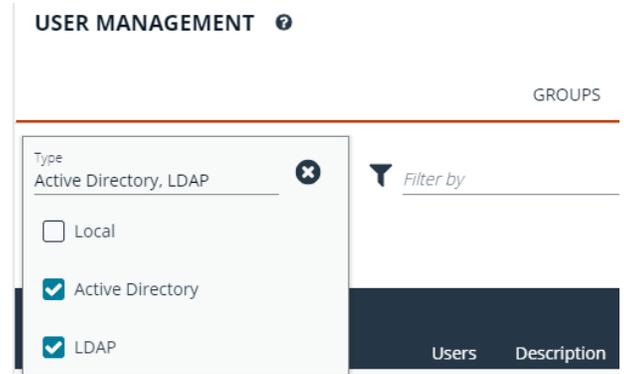


3. Under **Group Details**, select **Users**.
4. Filter the **Users** grid to show unassigned users.
5. Select the user or users, and then click **Assign User**.

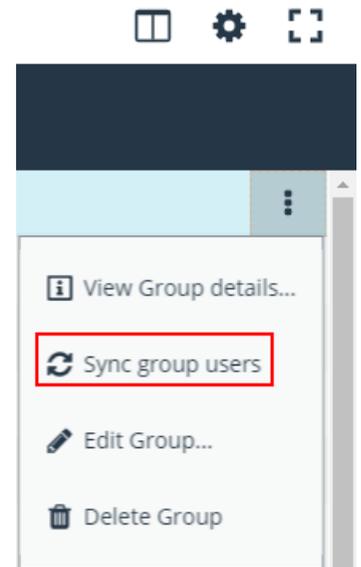


## Sync Group Users for Active Directory and LDAP Groups

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



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



## 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.

### Edit test.local\BIDemo ➤

[Go to advanced details...](#)

Active (yes)

Name  
test.local\BIDemo

Description  
--

Credential  
test sflight creds for userand grou (test.local) ▼  
[Manage Credentials...](#)

Domain / Domain controller  
Any domain controller ▼ **FETCH**

Propagate this change to all group members (no)

**SAVE CHANGES**

**DISCARD CHANGES**

## 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 **More Options** button, and then select **Delete Group**.

## Create and Manage User Accounts

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

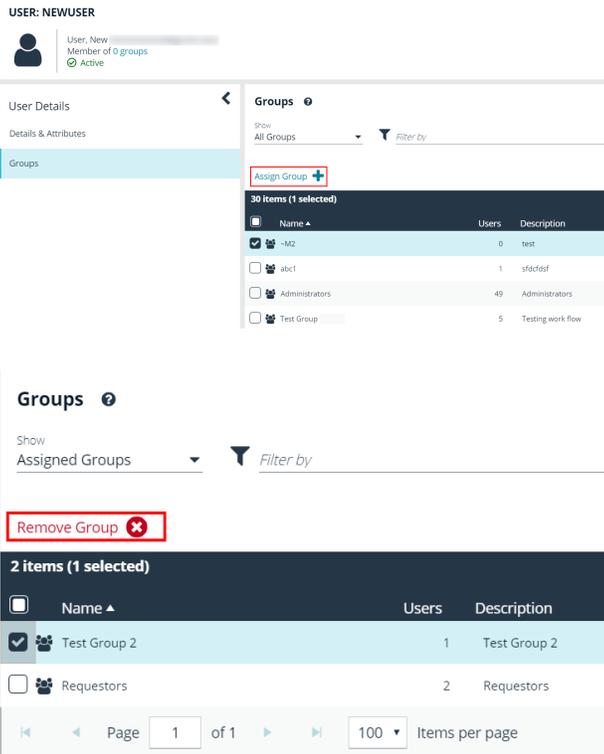
 **Note:** A user account must be a member of a BeyondInsight group. If a user is not a member of any groups in BeyondInsight, the user cannot log in to the console.

## Create a BeyondInsight Local User Account

1. Select **Configuration**.
  2. Under **Role Based Access**, select **User Management**.
  3. Select **Users** to display the list of users in the grid.
  4. Click **Create New User**.
- 
5. Select **Create a New User**.
  6. Complete the **Identification** and **Credentials / Change Password** sections. These fields are required.
  7. Optionally, enter the user's contact information.
  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**.



**USER: NEWUSER**

User, New  
Member of 0 groups  
Active

User Details

Details & Attributes

Groups

Groups

Show: All Groups

Assign Group

Name	Users	Description
-M2	0	test
abc1	1	sticief
Administrators	49	Administrators
Test Group	5	Testing work flow

Remove Group

2 items (1 selected)

Name	Users	Description
Test Group 2	1	Test Group 2
Requestors	2	Requestors

Page 1 of 1 100 Items per page

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



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

### ACTIVE DIRECTORY USER SEARCH ➔

Credential

[Manage Credentials...](#)

Domain

Filter by Name

SEARCH ACTIVE DIRECTORY
CANCEL

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 to retrieve, and then click **Search Active Directory**.



**Example:** Sample filters:

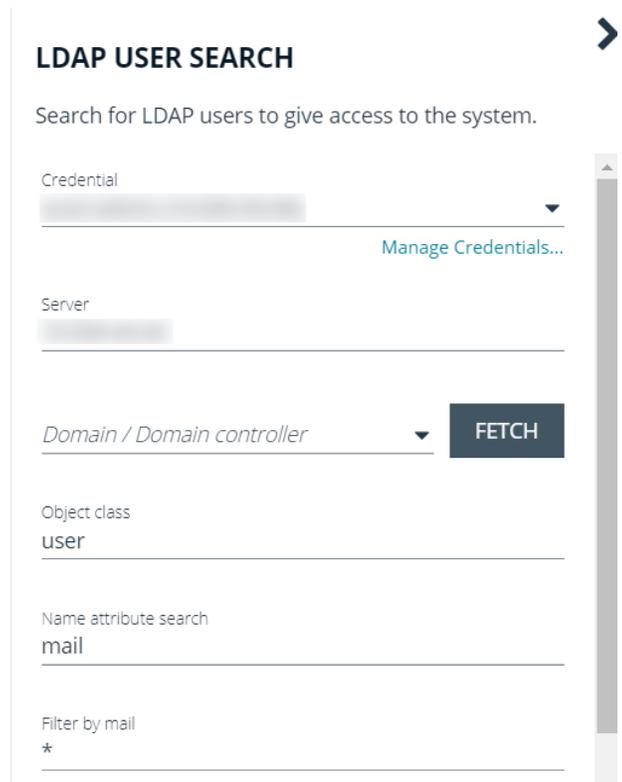
- **a\*** returns all group names that start with a.
- **\*d** returns all group names that end with d.
- **\*sql\*** returns all groups that contain sql in the name.

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

**i** For more information on creating and editing directory credentials, please see ["Create and Edit Directory Credentials"](#) on page 17.

## Add an LDAP User

1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Select **Users** to display the list of users in the grid.
4. Click **Create New User**.
  
5. Select **Add an LDAP User** from the list.
6. Select a credential for the directory, or click **Manage Credentials** to add or edit a credential.



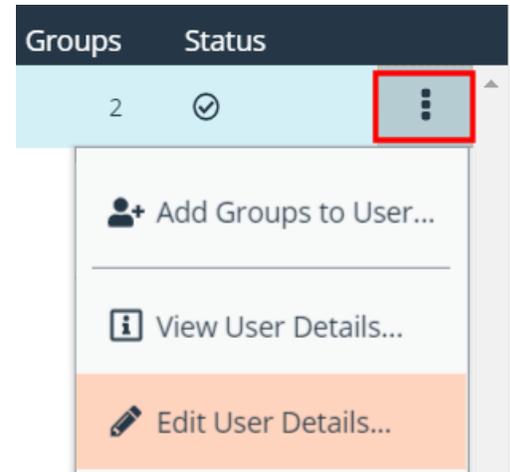
7. Click **Fetch** to load the list Domain Controllers, and then select one.
8. To filter the group search, enter keywords in the group filter or use a wild card.
9. Click **Search LDAP**.
10. Select a user, and then click **Add User**.
11. Assign at least one group to the user.

**i** For more information on creating and editing directory credentials, please see "[Create and Edit Directory Credentials](#)" on page 17.

## 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, click the vertical ellipsis button, and then select **Edit User Details**.
6. In the **Edit User** pane, update the details as required, and then click **Update User**.



## Propagate Domain Changes

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

If you want to assign this user a different preferred domain controller than the one defined and propagated from the group they are in, this can be updated by choosing an appropriate credential and selecting a different preferred domain controller from the list.



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

### Edit User ➤

[Edit advanced details...](#)

First Name  
Andrea

---

Last Name  
Admin

---

Email

---

Username  
Andrea

---

Account Quarantined (no)

Credential ▼  
[Manage Credentials...](#)

Domain / Domain controller ▼ FETCH

Multi-Factor Authentication

Disable Forms Login (no)

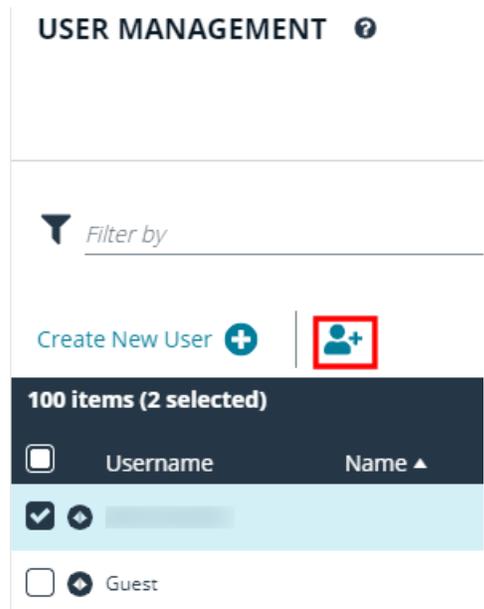
Two Factor Authentication ▼  
None

UPDATE USER
DISCARD

## Add Groups to User

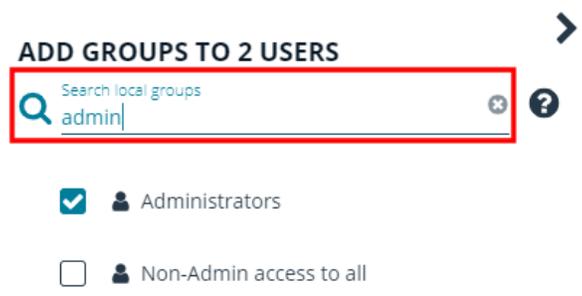
1. From the **User Management** page, click **Users** to display the list of users in the grid.
2. Optionally, filter the list of users displayed in the grid using the **Filter By** dropdown.

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

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 and Preferences](#)" on page 15.



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

## Overview of BeyondInsight Tools

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

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

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

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

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



For more information, please see "[Change and Set the Console Display and Preferences](#)" on page 15.

## Create an Address Group

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

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



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



For more information, please see "[Create and Configure Groups](#)" on page 19.

## Create an Always Address Group

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

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



**Example:** If the **Always** address group is configured with **10.10.10.60** and **buffett-laptop** (omitted), it scans **10.10.10.50** and **buffett-laptop**. The results are as follows:



- The scan includes 10.10.10.60 since this IP address was added to the **Always** address group.
- The scan excludes buffett-laptop since this asset was explicitly omitted in the **Always** address group.
- 10.10.10.50 is scanned as usual.



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

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

## ADDRESS GROUPS

 Search Address Groups

Create New Address Group 

### Create New Address Group

Address Group name

CREATE ADDRESS GROUP

DISCARD

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

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

### CREATE NEW ADDRESS

Type  
Single IP Address 

Single IP Address  
10.10.192.1

Omit this entry (No)

CREATE ADDRESS

DISCARD CHANGES

7. If importing the addresses:

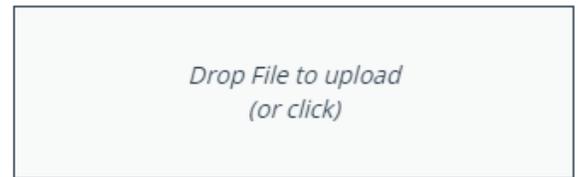
- Enable the **Overwrite all existing addresses** option, if desired.
- Click **Drop File** to upload the import file.
- Click **Upload File**.

## IMPORT ADDRESSES ? ➔

Import a text file containing a list of addresses into group 'Local'.

Overwrite all existing addresses (On)

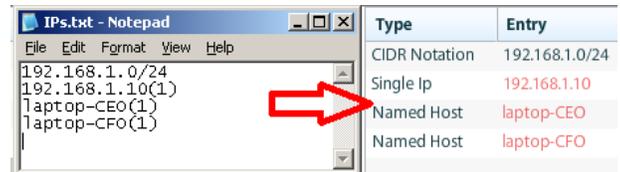
**⚠** By turning this option on, all existing addresses inside group 'Local' will be removed.



UPLOAD FILE

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

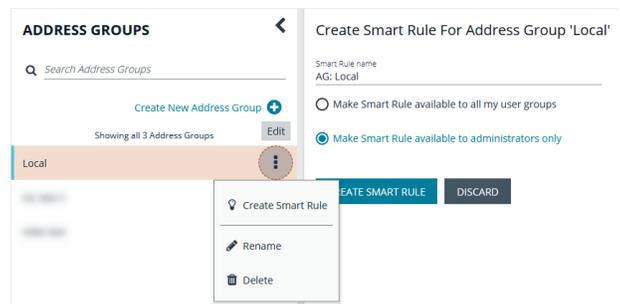
Here is an example of how a CIDR Notation, an excluded IP address, and excluded named hosts are displayed after importing.



### Create a Smart Rule Based on an Address Group

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

1. Select the address group, and then click **Edit** (vertical ellipsis).
2. Select **Create Smart Rule**.
3. Leave the default name, or name the Smart Rule as desired.
4. Select the option to make the Smart Rule available to all user groups or to administrators only.
5. Click **Create Smart Rule**.



6. A message stating *Smart Rule has been created for this Address Group* appears.
7. The group is displayed on the **Configuration > Smart Rules** page.



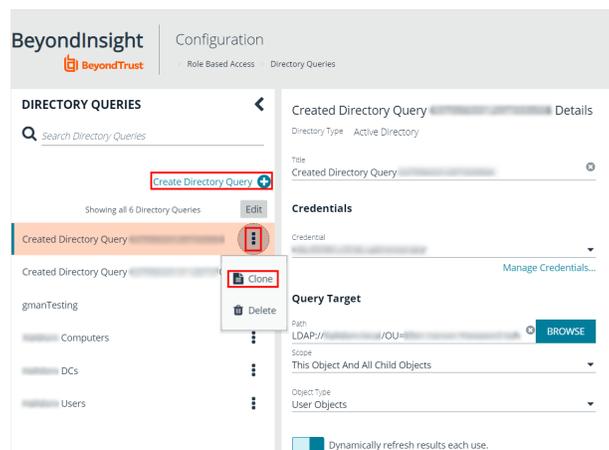
## Create a Directory Query

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

**i** For more information, please see *"Create and Configure Groups"* on page 19.

1. In the BeyondInsight Console, navigate to **Configuration > Role Based Access > Directory Queries**.
2. Click **Create Directory Query +**.

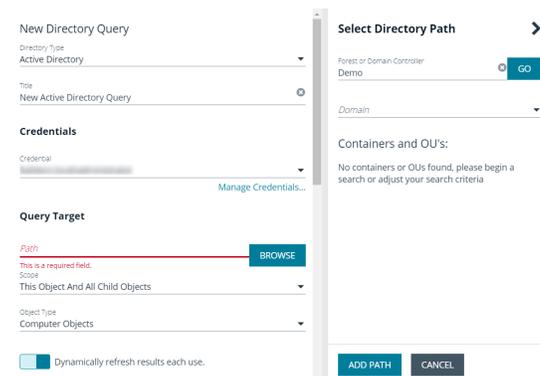
**Note:** To clone an existing query, hover over a query in the list, and then click the **Edit** icon, and select **Clone**.



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

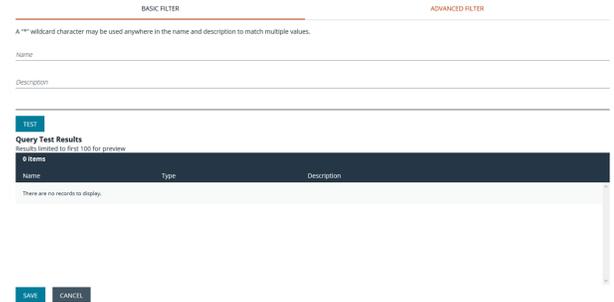
**Note:** At minimum, the credential must have **Read** permissions on the computer assets you are enumerating.

**i** For more information on creating and editing directory credentials, please see *"Create and Edit Directory Credentials"* on page 17.



6. Enter a path, or click **Browse** to search for a path and add it.
7. Select a scope to apply to the container: **This Object and All Child Objects** or **Immediate Children Only**.
8. Select an object type.

9. Enter a name and description for the basic filter.
10. Click **Advanced Filter**, and then enter the LDAP query details.
11. Click **Test** to ensure the query returns expected results.
12. Click **Save**.



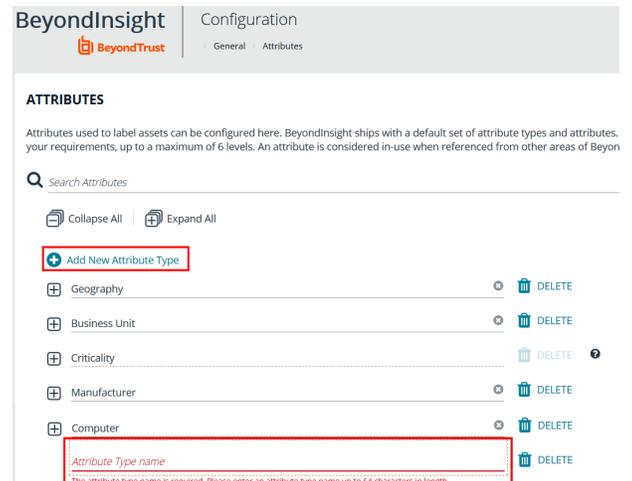
## Attributes and Attribute Types

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

**i** For more information, please see *"Use Smart Rules to Organize Assets"* on page 50.

### Add a New Attribute Type

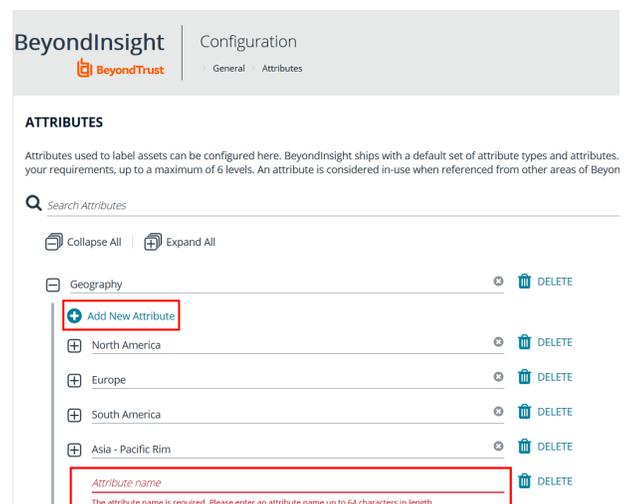
1. In the BeyondInsight Console go to **Configuration > General > Attributes**.
2. Click **+ Add New Attribute Type**.
3. Type a name for the attribute type, and then press **Enter**.



### 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.

### Selection Criteria

Include Items that match ALL ▼ of the following

Address Group

Address Group

and

Asset fields

Assets With Open Tickets

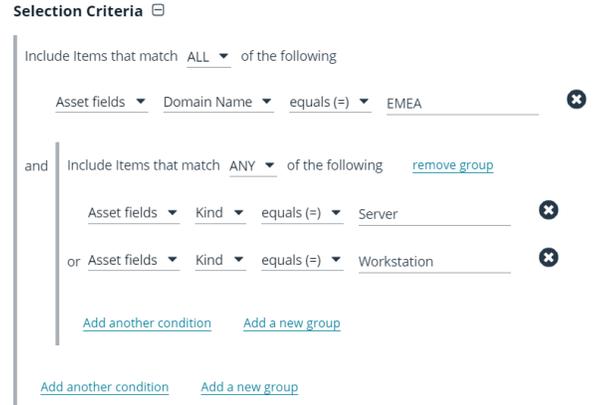
Assigned Attributes

Attacks

and

Child Smart Rule

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, <b>Asset Name</b> , <b>Domain</b> or <b>DNS</b> , <b>Risk</b> , and <b>Kind</b> . 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	<p>Filters user accounts by SID or privilege. You can filter on both. If either value is not selected then it will be ignored.</p> <p>Using this filter you can determine if any users have administrator privileges that might no longer be required.</p> <p>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.</p>
Windows Events	Filter by Windows events that are available in the Windows Event Viewer. For example, <b>Application</b> , <b>Security</b> , or <b>System</b> .
Workgroup	Filter by workgroup.

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

- ["Create an Address Group" on page 44](#)
- ["Create a Directory Query" on page 47](#)

## 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 <b>Web Servers</b> Smart Group is marked as active.
Virtualized Devices	<p>Includes Smart Groups for virtual environments, including <b>Microsoft Hyper-V</b> and <b>Parallels</b>. Assets detected as virtual environments belong to these Smart Groups.</p> <p>This default category also includes two Smart Groups: <b>Virtual Servers</b> and <b>Virtual Workstations</b>. 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.</p>

## Create Smart Rules

You can configure an asset-based Smart Rule to:

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

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

### Create an Asset Based Smart Rule

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

Create Ticket	Select tickets parameters, including ticket assignment, severity, and email alert.
Export Data	Select to manage a Smart Group for the BMC Remedy connector.
Mark each asset for deletion	Select to create a Smart Group that contains assets to be marked for deletion.
Mark each asset inactive	Assets detected as inactive are no longer be displayed on the <b>Assets</b> 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	<p>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.</p> <p>You can also select the default view to display on the <b>Assets</b> page when the Smart Group is selected.</p> <p>Smart Groups are also used for running scans and registering for patch updates.</p>

9. Click **Create Smart Rule**.

### Smart Rule Processing

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

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



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

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

### Change the Processing Frequency for a Smart Rule

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

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

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



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

#### MANAGED ACCOUNTS: ALL MANAGED ACCOUNTS

##### Details

Category  
Managed Accounts ▼

Name  
All Managed Accounts  Active (yes)

Description  
All accounts managed by Password Safe

Reprocessing limit  
Default ▼ 

### 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 Options

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

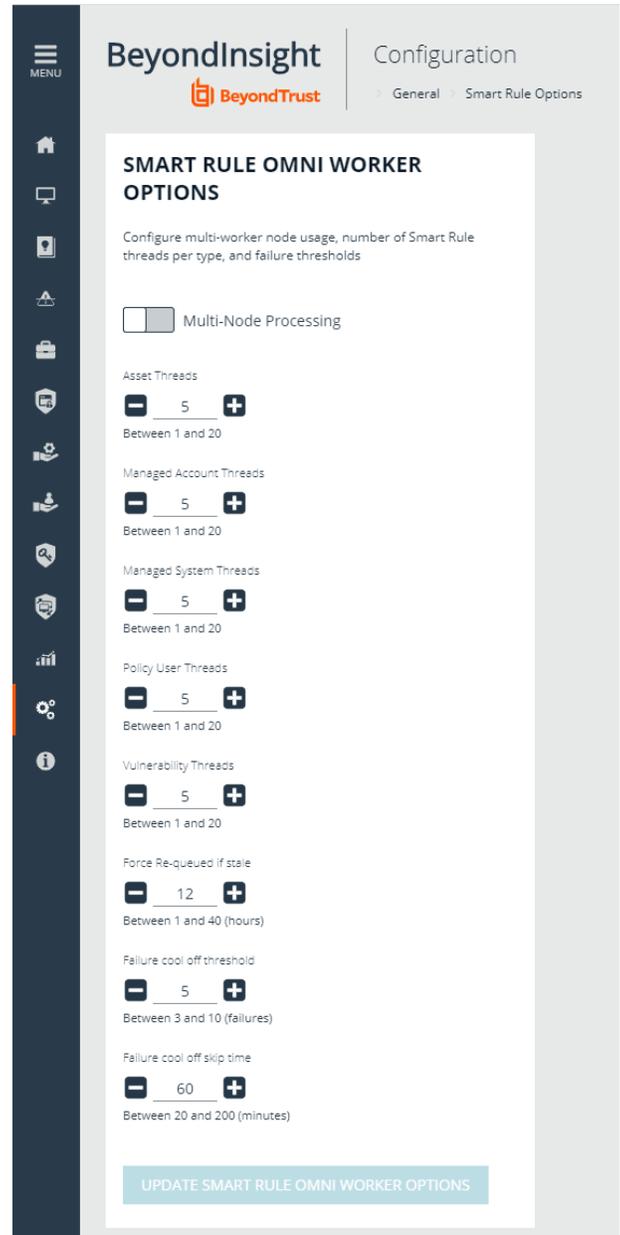
**Multi-Node Processing:** Off by default. Enable this to allow assignment of Smart Rules to process specific worker nodes. Choosing a worker node for a Smart Rule to process is accomplished by setting the **Target Processing to Workgroup** action on the Smart Rule in question. When enabled, this allows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

### ! IMPORTANT!

For the following options to be available, you must enable **Multi-Node Processing**.

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

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



The screenshot shows the 'BeyondInsight Configuration' interface. The breadcrumb trail is 'General > Smart Rule Options'. The main heading is 'SMART RULE OMNI WORKER OPTIONS'. Below the heading is a description: 'Configure multi-worker node usage, number of Smart Rule threads per type, and failure thresholds'. There are several configuration options, each with a toggle or a numeric input field with minus and plus buttons, and a range indicator below:

- Multi-Node Processing:** A toggle switch that is currently turned off.
- Asset Threads:** A numeric input field set to '5', with a range of 'Between 1 and 20'.
- Managed Account Threads:** A numeric input field set to '5', with a range of 'Between 1 and 20'.
- Managed System Threads:** A numeric input field set to '5', with a range of 'Between 1 and 20'.
- Policy User Threads:** A numeric input field set to '5', with a range of 'Between 1 and 20'.
- Vulnerability Threads:** A numeric input field set to '5', with a range of 'Between 1 and 20'.
- Force Re-queued if stale:** A numeric input field set to '12', with a range of 'Between 1 and 40 (hours)'.
- Failure cool off threshold:** A numeric input field set to '5', with a range of 'Between 3 and 10 (failures)'.
- Failure cool off skip time:** A numeric input field set to '60', with a range of 'Between 20 and 200 (minutes)'.

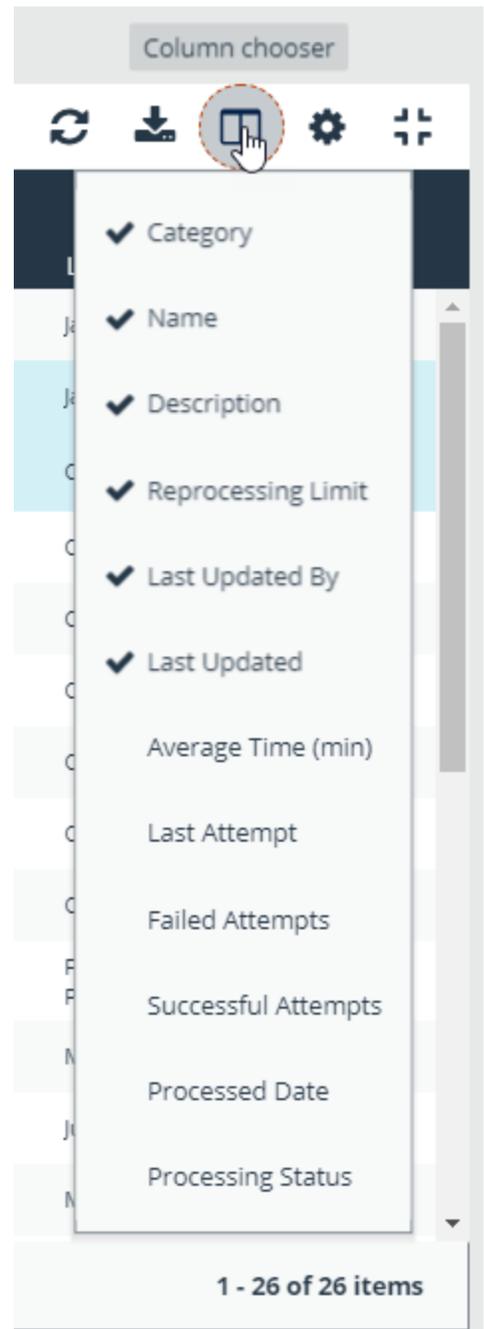
At the bottom of the configuration area is a blue button labeled 'UPDATE SMART RULE OMNI WORKER OPTIONS'.

### View and Select Smart Rules Processing Statistics

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

To add this information to the grid:

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



## Add Credentials for Use in Scans

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

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

To create a credential:

1. Select **Configuration > Discovery Management > Credentials**.
2. Click **Create 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	<ul style="list-style-type: none"> <li>• Authentication Type</li> <li>• Domain (Optional)</li> <li>• Username</li> <li>• Password</li> <li>• Confirm password</li> <li>• Description</li> <li>• Port</li> <li>• Key</li> <li>• Confirm key</li> </ul>
MySQL	<ul style="list-style-type: none"> <li>• Username</li> <li>• Password</li> <li>• Confirm password</li> <li>• Description</li> <li>• Port</li> <li>• Key</li> <li>• Confirm key</li> </ul>
Oracle	<ul style="list-style-type: none"> <li>• Username</li> <li>• Password</li> <li>• Confirm password</li> </ul>

	<ul style="list-style-type: none"> <li>• Description</li> <li>• Access level</li> <li>• Connect to</li> <li>• Protocol</li> <li>• Port number</li> <li>• Key</li> <li>• Confirm key</li> </ul>
MongoDB	<ul style="list-style-type: none"> <li>• Username</li> <li>• Password</li> <li>• Confirm password</li> <li>• Description</li> <li>• Database</li> <li>• Host</li> <li>• Port</li> <li>• Key</li> <li>• Confirm key</li> </ul>
PostgreSQL	<ul style="list-style-type: none"> <li>• Username</li> <li>• Password</li> <li>• Confirm password</li> <li>• Description</li> <li>• Database</li> <li>• Host</li> <li>• Port</li> <li>• Key</li> <li>• Confirm key</li> </ul>
Sybase	<ul style="list-style-type: none"> <li>• Username</li> <li>• Password</li> <li>• Confirm password</li> <li>• Description</li> <li>• Host</li> <li>• Port</li> <li>• Key</li> <li>• Confirm key</li> </ul>
Teradata	<ul style="list-style-type: none"> <li>• Username</li> <li>• Password</li> <li>• Confirm password</li> <li>• Description</li> </ul>

	<ul style="list-style-type: none"> <li>• Host</li> <li>• Port</li> <li>• Key</li> <li>• Confirm key</li> </ul>
SNMPv2	<ul style="list-style-type: none"> <li>• Description</li> <li>• Key</li> <li>• Confirm key</li> <li>• Community string</li> </ul>
SSH	<ul style="list-style-type: none"> <li>• Authentication Type</li> <li>• Username</li> <li>• Password</li> <li>• Confirm password</li> <li>• Description</li> <li>• Port</li> <li>• Key</li> <li>• Confirm key</li> <li>• Elevation</li> </ul>
Windows	<ul style="list-style-type: none"> <li>• Domain (Optional)</li> <li>• Username</li> <li>• Password</li> <li>• Confirm password</li> <li>• Description</li> <li>• Key</li> <li>• Confirm key</li> </ul>



**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**.

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

- "Create SSH Credentials" on page 62
- "Create Oracle Credentials" on page 61
- "Create SNMP Credentials" on page 62

## Create Oracle Credentials

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

1. In the BeyondInsight Console, navigate to **Configuration > Discovery Management > Credentials**.
2. Click **Create Credential +**.
3. From the **Type** list, select **Oracle**.
4. Provide a **Username**, **Password**, and **Description**.
5. Select an **Access level** from the list: **Standard**, **SYSDBA**, or **SYSOPER**.
6. Select additional connection options:
  - **Connect To:** Select from: **Database** 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.

### Create Credential

A number of credential types are supported and can be configured here.

Type (optional)  
Oracle

Username  
kjplay

Password  
\*\*\*\*\*

Confirm password  
\*\*\*\*\*

Description  
Admin

Access level  
Standard

Connect to  
Named service

Service name  
   
The service name is required

Protocol  
TCP



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

7. Enter a key.
8. 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.

9. Click **Create Credential**.

## Create SNMP Credentials

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

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

6. Click **Create Credential**.

## Create SSH Credentials

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



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

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

1. In the BeyondInsight Console, navigate to **Configuration > Discovery Management > Credentials**.
2. Click **Create Credential**.

3. From the **Type** list, select **SSH** from the **Type** list.
4. Select an authentication type.
  - **Plain text:** Enter a **Username** and **Password**.
  - **Public Key:** Upload a private key file, and then enter a **Username** and **Passphrase**. A public key is generated based on the contents of the private key.
5. Enter a **Description** and **Key**.
6. Elevating credentials is optional. To elevate credentials, select one of the following from the **Elevation** list:
  - **sudo:** The optional sudo username should be blank in most cases. When blank, commands run with the effective privileges of the root account. If an optional username is entered, sudo runs in the security context of that user.
  - **pbrun:** Enter the pbrunuser username.
  - **Enable:** Enter the credentials for Cisco devices. If you are auditing Cisco devices, you can elevate the credentials to privileged for more thorough scans.

### Create Credential

A number of credential types are supported and can be configured here.

Type (optional)  
SSH 

Authentication Type  
Public Key 

Upload private key file

Drop File to upload  
(or click)

A private key file is required

Username

Passphrase  

Confirm passphrase  

Description  
New credential



**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**.

## Run Discovery Scans

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



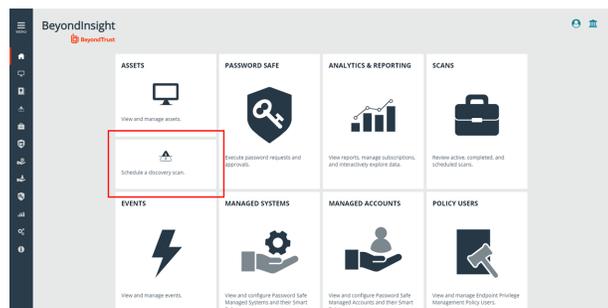
**Note:** Discovered assets do not count toward your license.

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

## Use the Scan Wizard to Create a Discovery Scan

To run the Scan Wizard, click **Schedule a discovery scan** on the homepage or left menu, and then follow the steps outlined below.

1. **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 scan agent to the scan targets. Besides systems, this scan provides associated information on services, scheduled tasks, users, and databases.
  - **Advanced Discovery Scan:** This scan performs all the operations of the previous scan, but provides information on all associated attributes.
2. **Select Scan Targets:** Enter scan targets in the field provided. You can enter single IP addresses, IP ranges, addresses in CIDR notation, or named hosts. Items must be separated by commas. If you wish to target existing assets or Smart Rules, this can be done from each of those product areas by using the grid actions to trigger a scan for a selected target.
3. **Enter Credentials:** If the type of test you 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.
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.

- Name the Scan:** Provide a unique name for this scan. The scan name cannot be longer than 58 characters and cannot contain any of the following characters:

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

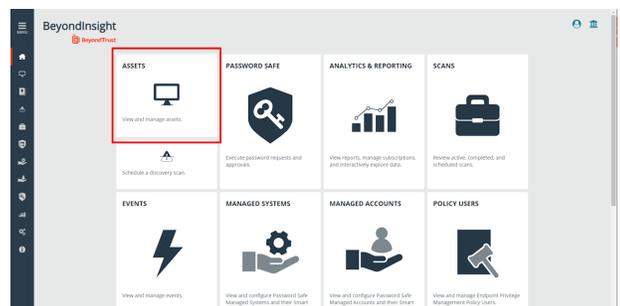
You can also apply **Job Restrictions** that allow you to abort the scan if it runs longer than a set number of minutes, and set a **Schedule**, which can be **Immediate**, **One Time**, or **Recurring**. Click **Finished** to run the report.

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

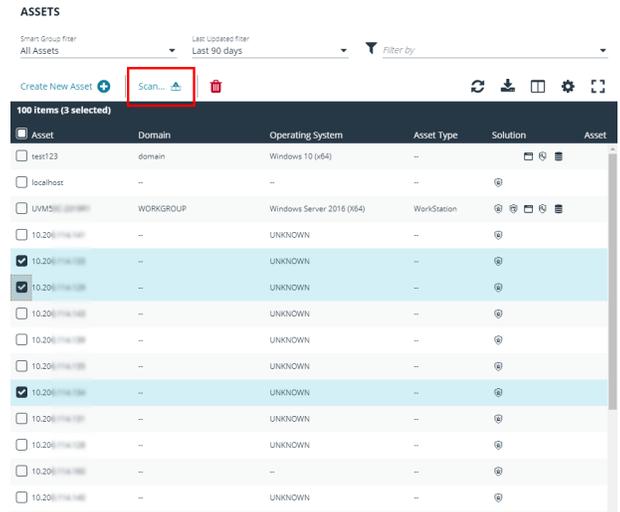
Agent Name	Workgroup	Scan State	Scan Name	Status	Hosts Found	Last Updated
UVM50C-2019R1	BEYON... WORK...	Com...	DiscoveryScan (1)	Completed		Jul 24, 2020, 12:16 PM
UVM50C-2019R1	BEYON... WORK...	Com...	All Audits Scan - IP Range (10.200.114.3-10.200.114.255)	Completed	11	Jul 24, 2020, 4:02 AM
UVM50C-2019R1	BEYON... WORK...	Com...	All Audits Scan - IP Range (10.200.114.3-10.200.114.255)	Completed	0	Jul 23, 2020, 3:50 AM
UVM50C-2019R1	BEYON... WORK...	Com...	All Audits Scan - IP Range (10.200.116.5-10.200.116.255)	Completed	0	Jul 23, 2020, 3:13 AM
UVM50C-2019R1	BEYON... WORK...	Com...	All Audits Scan - IP Range (10.200.114.3-10.200.114.255)	Completed	11	Jul 23, 2020, 4:02 AM
UVM50C-2019R1	BEYON... WORK...	Com...	All Audits Scan - IP Range (10.200.114.3-10.200.114.255)	Completed	13	Jul 21, 2020, 4:03 AM
UVM50C-2019R1	BEYON... WORK...	Com...	All Audits Scan - IP Range (10.200.114.3-10.200.114.255)	Completed	13	Jul 20, 2020, 4:02 AM
UVM50C-2019R1	BEYON... WORK...	Com...	All Audits Scan - IP Range (10.200.114.3-10.200.114.255)	Completed	13	Jul 19, 2020, 4:03 AM
UVM50C-2019R1	BEYON... WORK...	Com...	All Audits Scan - IP Range (10.200.114.3-10.200.114.255)	Completed	13	Jul 18, 2020, 4:02 AM

## Run Scans from a List of Assets

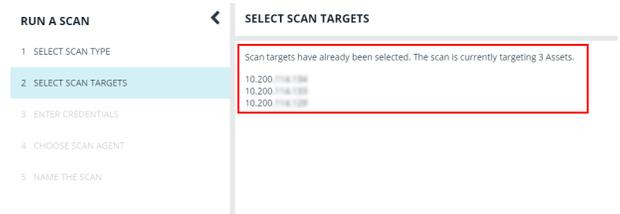
If you want to run a scan but would prefer to select targets from a list of assets rather than type them, click the **Assets** tile.



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

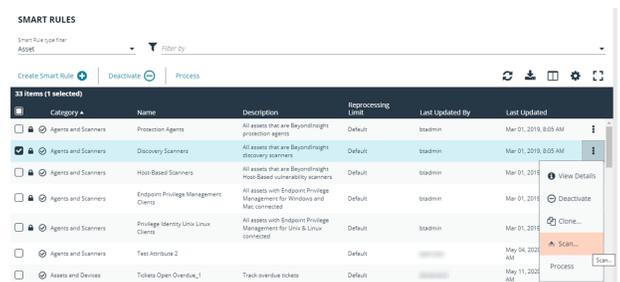


The Scan Wizard screen appears. Here you can select the type of scan to run. The difference is that when you click **Next** and go to the **Select Scan Targets** page, you will find the targets already selected. The next steps in the Scan Wizard are the same as those outlined above.



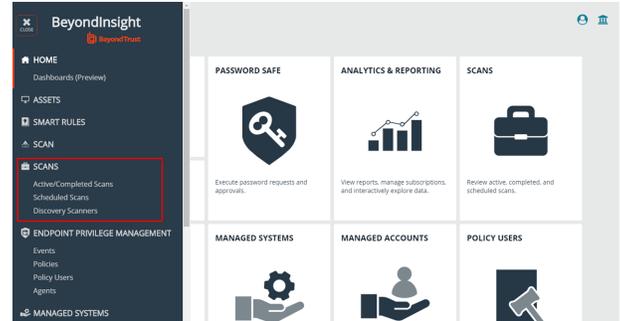
## Use Smart Rules as Targets for Scans

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



## Check Completed Scans

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



## Discover Assets Using a Smart Group

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

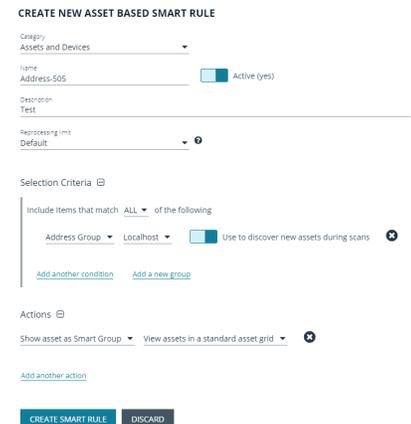


**Tip:** If you create an address group that includes the /19 CIDR block, the range possesses 8190 potential assets. The Discovery Scan always tries to discover those assets. Keep this in mind when you are reviewing scan results.

## Key Steps

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

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



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



*For more information, please see the following:*

- *"Create a Directory Query" on page 47*
- *"Create an Address Group" on page 44*

## 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

## Manage Assets

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

### Review Asset Details

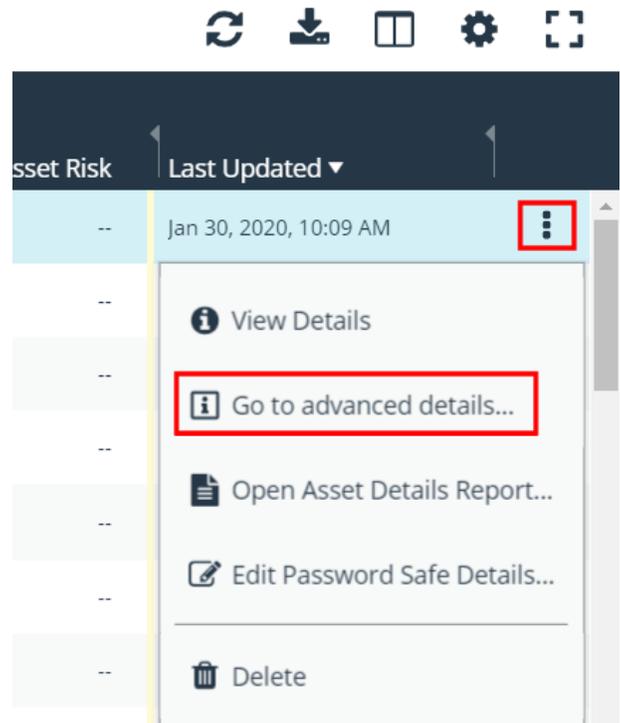


**Tip:** Depending on the scan settings, information in the following list might not be detected and included in the scan results. If the following scan settings are turned on, more accurate scan results can be expected:

- **Perform Local Scanning**
- **Enable WMI Service**
- **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 vertical ellipsis button for an asset, and then select **Go to advanced details**.



**Note:** If the asset has not been scanned, information is available only under **General Data**.

## General Data

- **Details & Attributes:** Displays details about the asset such as: IP address, DNS name, domain, system name, workgroup, date the asset was added and updated, and the operation system, etc.
- **Databases:** Displays the databases that are on the asset and allows you to add a database.
- **Smart Groups:** Displays the smart groups that the asset is associated with.

## Scan Data



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

- **Application Pools:** Displays IIS Application Pools discovered on the asset on the last successful scan of the system.
- **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. From the left menu in the BeyondInsight Console, 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.

### CREATE ASSET

Asset Name

DNS Name (Optional)

Domain (Optional)

Asset Type (Optional)

IP Address

MAC Address

Workgroup



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

## Delete Assets

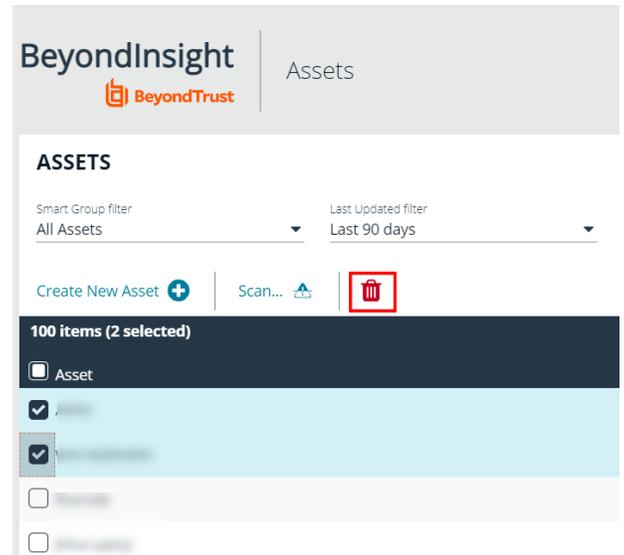
You can remove assets from the **Assets** grid immediately. Assets removed from the grid will be deleted from the BeyondInsight database during the nightly data purge.

1. From the BeyondInsight homepage click **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.



The screenshot shows the 'Assets' page in the BeyondInsight interface. At the top, there's a header with the BeyondTrust logo and the word 'Assets'. Below this, there's a section titled 'ASSETS' with two dropdown filters: 'Smart Group filter' set to 'All Assets' and 'Last Updated filter' set to 'Last 90 days'. There are three buttons: 'Create New Asset' with a plus icon, 'Scan...' with a cloud icon, and a 'Delete' button with a trash can icon, which is highlighted with a red box. Below the buttons, a dark header indicates '100 items (2 selected)'. The main area shows a list of assets, with the first two rows highlighted in light blue and having their selection checkboxes checked. The remaining rows have unchecked checkboxes.

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](https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal) 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](https://cloud.google.com/compute/docs/access/iam) 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://www.vmware.com/support/developer/vddk/>.
- 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

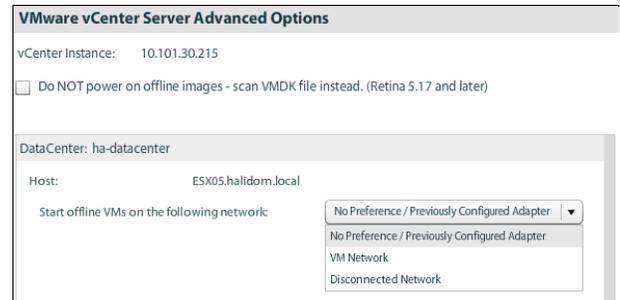
By default, paused or offline VMs are turned on during a scan. After the scan runs, the VMs are reverted to the paused or offline state.

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.

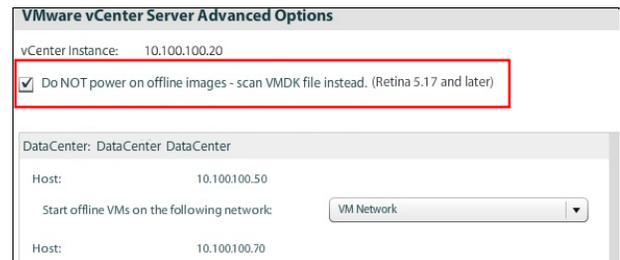
The advanced options dialog box varies depending on your vCenter configuration. The list of available options includes all other networks configured for your vCenter instance or on your ESX server.



### 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 may also need a condition with this, such as if you want only the **dev** group to have access to certain instances.

## Grant Access to a Third Party (Optional)



**Note:** The **ARN** and **External Name** fields are for granting access to a third party. For more information, please see [How to Use an External ID When Granting Access to Your AWS Resources to a Third Party at \[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\\_roles\\\_create\\\_for-user\\\_externalid.html\]\(https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_create\_for-user\_externalid.html\)](#).

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

## Work with the Multi-Tenant Feature in BeyondInsight

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

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

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

### Select Tenants on the Smart Rule Page

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



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

 **Note:** Create Smart Rules as usual. For more information, please see "[Use Smart Rules to Organize Assets](#)" on page 50.

### Quick Rules

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

### Organization Filters

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

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

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

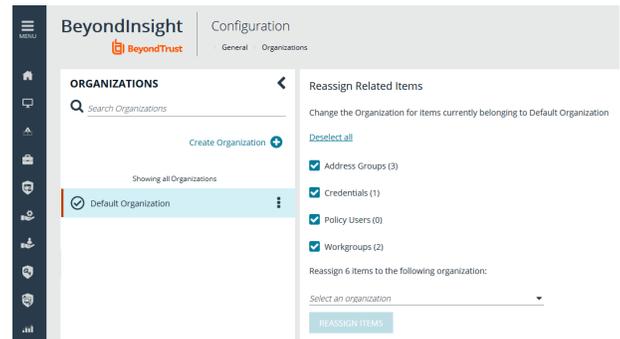
### Address Groups

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

### Reassign Related Items

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

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



### Select a Workgroup

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

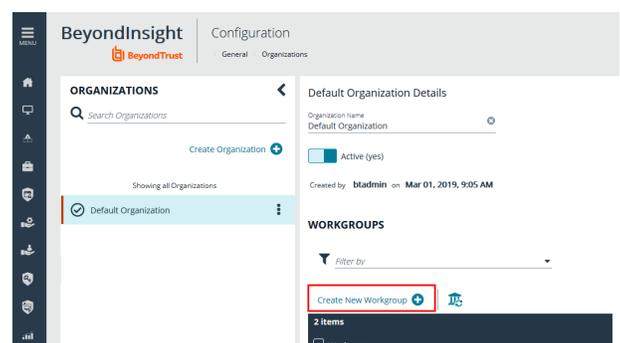
- **Single IP address**
- **IP range**
- **CIDR notation**
- **Named hosts**

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

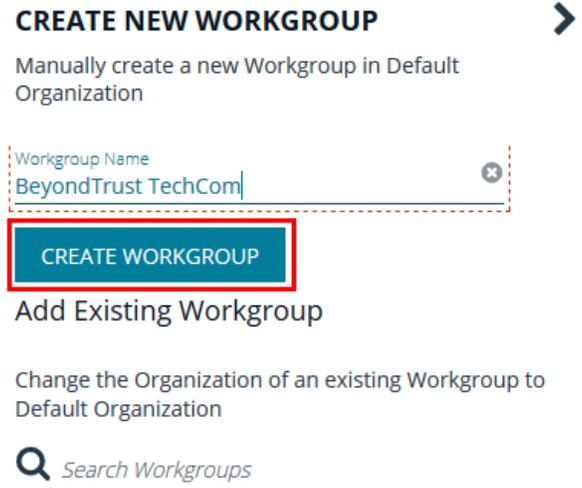
- **Currently selected Smart Group**
- **Currently selected Assets**

### Create a New Workgroup

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



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



## Set Up Organizations

### Create a Workgroup

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

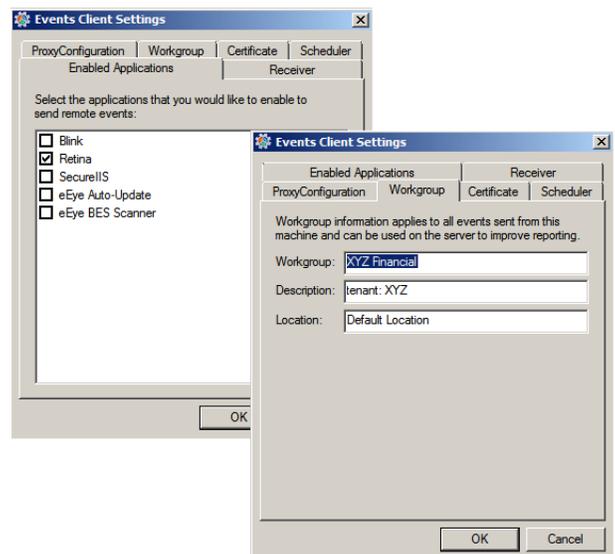
Each Discovery Scanner must be assigned a workgroup. A workgroup is typically created when the agent is initially deployed.

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

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

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

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



## Add an Organization

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

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

## Create a Group for a Tenant

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



**Note:** *Creating a group for a tenant is optional and only required if your client wants to run reports from BeyondInsight. For more information, please see ["Role-Based Access" on page 17](#).*

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

## Set BeyondInsight Options

### Set Account and Email Options

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

### Account Lockout Options

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

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

### Account Password Options

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

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

## Email Notifications

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



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

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



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

## Set Support Options

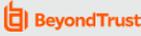
You can use the following support options to assist with troubleshooting issues with BeyondInsight:

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

### Select File Log Levels

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

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



**BeyondInsight**

Configuration
 

[Support](#) > [File Log Levels](#)

---

### FILE LOG LEVELS

The logging level for each of these services can be configured here. Once a change is made, within about 30 seconds, the new logging level will be used. Services will receive these changes automatically, they do not need to be restarted. Please note, Debug and Verbose logging levels will result in a high volume of log file entries and should generally be used only as needed. The default log level for all file logging is "Information".

Omniworker (Service)  
**Information**

Verbose  
  
 Debug  
  
 Information  
  
 Warning  
  
 Error

Omniworker Password Safe Queues  
**Information**

Omniworker General Queue  
**Information**

Omniworker Event Forwarding Queue  
**Information**

Web Policy Service  
**Information**

Policy Service  
**Information**

Web Event Service  
**Information**

Event Service  
**Information**

SCIM Portal  
**Information**

Configuration Application  
**Information**

Public API Portal  
**Information**

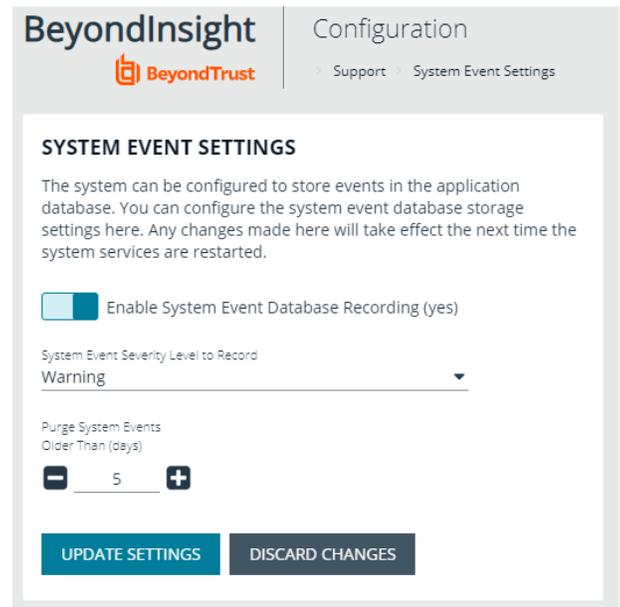
Team Passwords Service  
**Information**

UPDATE SETTINGS

DISCARD CHANGES

## Enable System Event Recording

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



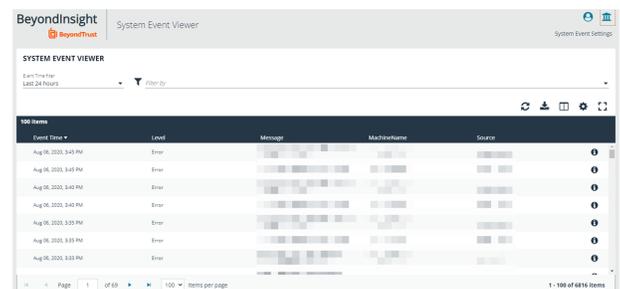
**Note:** Once events are purged, they are not available in the **System Event Viewer**.

## System Event Viewer



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

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



## Set Data Retention and Advanced Purging Options

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

### Data Retention

### Maintenance

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



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

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

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

## Privileged Access Management

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

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

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

## Asset Maintenance

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

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

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

## Application Maintenance

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

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

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

## Third-Party Integration Maintenance

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

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



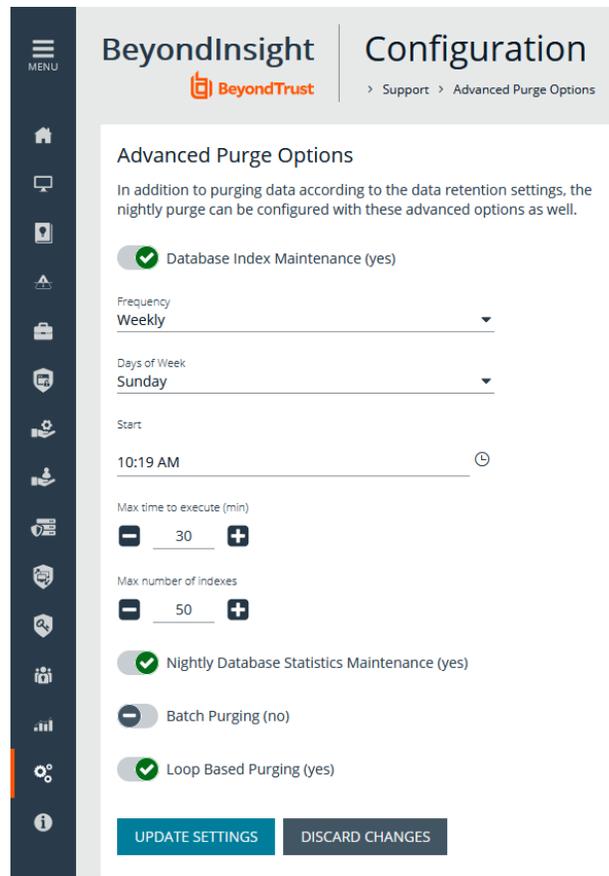
**Note:** The data in the scan file is not purged.

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

## Purging Options

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

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



The screenshot shows the 'Advanced Purge Options' configuration page in the BeyondInsight console. The page has a dark sidebar with a menu and a main content area. The main content area has a header with 'BeyondInsight' and 'Configuration' (with a breadcrumb trail: > Support > Advanced Purge Options). Below the header is the title 'Advanced Purge Options' and a sub-header: 'In addition to purging data according to the data retention settings, the nightly purge can be configured with these advanced options as well.' The configuration options are as follows:

- Database Index Maintenance (yes):** Enabled (checked). Frequency: Weekly. Days of Week: Sunday. Start: 10:19 AM. Max time to execute (min): 30. Max number of indexes: 50.
- Nightly Database Statistics Maintenance (yes):** Enabled (checked).
- Batch Purging (no):** Disabled (unchecked).
- Loop Based Purging (yes):** Enabled (checked).

At the bottom of the configuration area are two buttons: 'UPDATE SETTINGS' and 'DISCARD CHANGES'.

## Configure Proxy Settings

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

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

## Configure Discovery Management Options

### Set Job Refresh Options

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

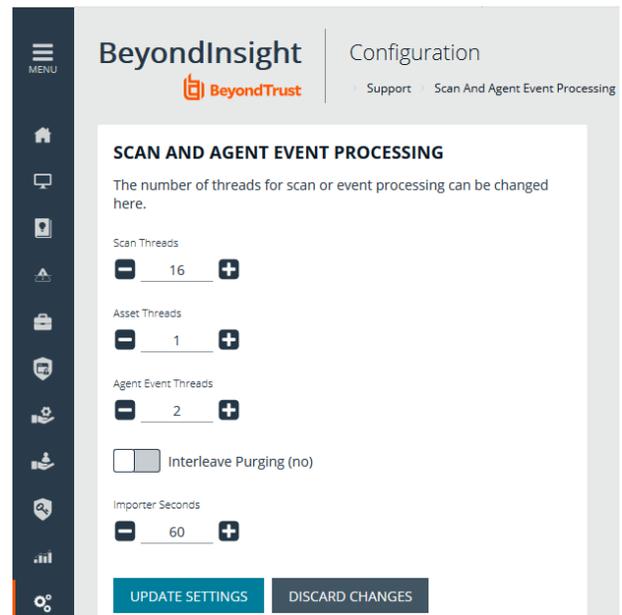
1. Select **Configuration > Discovery Management > Options**.
2. Under **Job Refresh**, set the following options:
  - **Maximum job refresh frequency:** BeyondInsight jobs are refreshed at the interval set. When the refresh occurs, updates to schedules, scanners, and Smart Rules are updated for the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

### Set Scan and Event Processing Options

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

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

Click **Update Settings** when done.



### Configure Global 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 servers, 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



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

1. 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.

## BeyondInsight Clarity Analytics

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

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

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

As a result, the behavior analytics:

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

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

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

## Configure BeyondInsight Clarity Analytics

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

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

## Set Risk Analytics Values

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

When you choose to normalize the data, the asset at the highest risk is assigned the highest rating. All other assets are rated and organized below the highest risk asset. Normalizing the results provides a way to distribute the assets in a more meaningful way to analyze the data.

Using the analysis influence slider, you can change the results to emphasize risk levels based on exposures or threats. For example, if you move the slider to **Exposure**, asset exposure risk factors are given greater weighting in the final risk calculation and increase an asset's risk score.



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

## Clarity Reports

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

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

## Use the Clarity Dashboard

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

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

## Triggers

The following triggers identify assets that are at risk.

Trigger	Description
Outlier	<p>Can be triggered by events in the following products:</p> <ul style="list-style-type: none"> <li>Endpoint Privilege Management</li> <li>Privilege Management for Unix &amp; Linux</li> <li>Password Safe</li> <li>BeyondTrust Discovery Scanner</li> <li>Malware and attack data from other solutions</li> </ul>
Untrusted Application	<p>Endpoint Privilege Management events. Triggers in the following cases:</p> <ul style="list-style-type: none"> <li>Application is unsigned</li> <li>Application has no version information</li> </ul>
Vulnerable Application	Endpoint Privilege Management events
Asset Risk Exceeds Threshold	<p>Can be triggered by events in the following products:</p> <ul style="list-style-type: none"> <li>Endpoint Privilege Management</li> <li>Privilege Management for Unix &amp; Linux</li> <li>Password Safe</li> <li>BeyondTrust Discovery Scanner</li> <li>Malware and attack data from other solutions</li> </ul>
Untrusted User	<ul style="list-style-type: none"> <li>Endpoint Privilege Management</li> <li>Privilege Management for Unix &amp; Linux</li> <li>BeyondTrust Discovery Scanner</li> </ul>
First Application Launch	<ul style="list-style-type: none"> <li>Endpoint Privilege Management</li> <li>Privilege Management for Unix &amp; Linux</li> <li>User launches an application they have never launched before</li> </ul>
First Password Release Request	<ul style="list-style-type: none"> <li>Password Safe events</li> <li>User requests password for an account and system they have never requested before</li> </ul>
Unusual Password Release Request	<ul style="list-style-type: none"> <li>Password Safe events</li> <li>User does not retrieve the password for approved request or the password is retrieved more than once</li> </ul>
Concurrent Password Release Request	<ul style="list-style-type: none"> <li>Password Safe events</li> <li>User tries to acquire more than one password at a time</li> </ul>

**Malware Detected**

- Malware is detected on an asset

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

### Risk Events by Threat Level

Drill into the risk events to learn more about the event, such as the trigger, type of event, or severity.

### Risk Events by Application

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

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

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

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

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



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

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

## View Cluster Maps

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

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

### Cluster Map Numbering

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

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

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

## Cluster Shading

### Asset

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

### User

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

## Asset Cluster Attributes

There are eight cluster attributes organized in the following categories:

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

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

## User Cluster Attributes

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

## Analyze Cluster Maps

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

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

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



For more information, please see "[BeyondInsight Clarity Analytics](#)" on page 95.

## Analyze Cluster Grids

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

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

To view the cluster grid, follow the steps.

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

## Alerts in BeyondInsight Clarity Analytics

There are two types of alerts:

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

Alert	Type	Description
a1	pattern	<p>Maps all characteristics of an event into a single internal cluster using self-organizing maps clustering. Similar event characteristics lead to the same cluster. Thus, clusters with high share of mapped events represent typical behavior, while clusters with small number of events indicate outliers. Each user, host, or asset's characteristics are tracked independently with independent sets of clusters.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note:</b> Clusters are hidden and are used only for analysis. They do not behave the same as asset clusters.                 </div> <p><b>Used characteristics:</b></p> <ul style="list-style-type: none"> <li>Endpoint Privilege Management events, per user: <b>EventType, Exercised privilege, Path, Asset, Launch weekday and time</b></li> <li>Privilege Management for Unix &amp; Linux events, per RunHost: <b>RunCommand, RunCWD, PBLUUser, Policy Server, SubmitHost, FinishStatus, Launch weekday and time, Accept, RiskLevel</b></li> <li>Vulnerability events, per Asset: Vulnerability type, Risk</li> <li>Attack events, per Asset: Attack type, Category</li> </ul>
a2	explicit	<p>Untrusted Application</p> <p>Default value: 0.33</p> <ul style="list-style-type: none"> <li>If the application is unsigned, then value = value + 0.33</li> <li>If application has no version information, then value = value + 0.33</li> </ul>
a3	explicit	<p>Vulnerable Application</p> <p>Vulnerability of launched application.</p>
a4	explicit	Asset Risk
a5	explicit	<p>Event Timing</p> <p>Event time within working hours and weekday</p> <p>Default value: 0.33</p> <ul style="list-style-type: none"> <li>If <math>EventTime &lt; WorkingHoursStart</math> or <math>EventTime &gt; WorkingHoursEnd</math>, then value = value + 0.33</li> <li>If <math>EventDay</math> is in <math>WorkingWeekDaysMask</math>, then value = value + 0.33</li> </ul>
a6	explicit	<p>Untrusted User</p> <p>Default value: 0.33</p> <ul style="list-style-type: none"> <li>If user is local (not domain) user, then value = value + 0.33</li> <li>If user is administrator, then value = value + 0.33</li> </ul>
a7	explicit	<p>First App Launch</p> <p>The alert is flagged when a user launches an application they have never launched before.</p>
a8	explicit	<p>First request for given managed account and system (Password Safe).</p> <p>The alert is flagged when a user request password for account and system have never requested before.</p>

Alert	Type	Description
a9	explicit	Unusual password releases (Password Safe)  The alert is flagged when a user does not retrieve the password for approved request or the password is retrieved more than once.
a10	explicit	Concurrent password requests (Password Safe).  The alert is flagged when a user tries to acquire more than one password at a time.

## BeyondInsight Clarity Malware Analysis

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



**Note:** Clarity Malware is disabled by default.

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

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

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

### Configure Clarity Malware

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

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

### Review Malware Information and Reports

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

- High
- Medium
- Low

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

### Use Reports to Analyze Results

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

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

### Top 10 Assets by Total Threat Level Report

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

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

### Event Review - Malware Report

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

## Configure a Claims-Aware Website to Authenticate against SAML

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

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

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

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

### Create a BeyondInsight Group

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

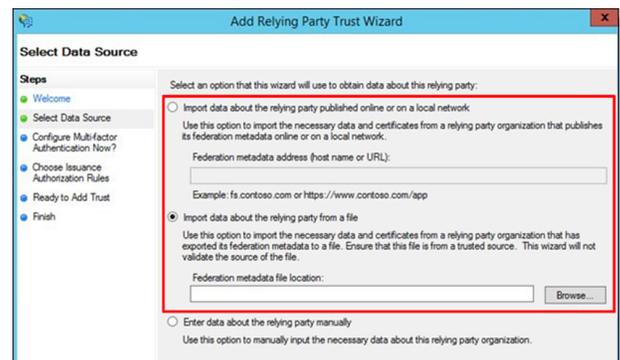
### Add Relying Party Trust

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

The metadata is located in the following directory:

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

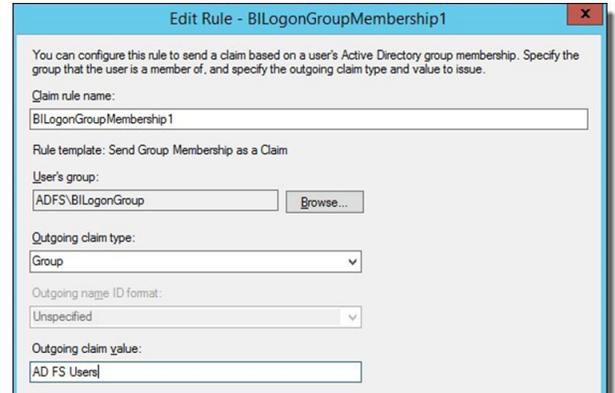
When selecting a **Data Source** in the **Add Relying Party Trust Wizard**, select the **FederationMetadata.xml** generated during the install.



## Set Up Claim Rules



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



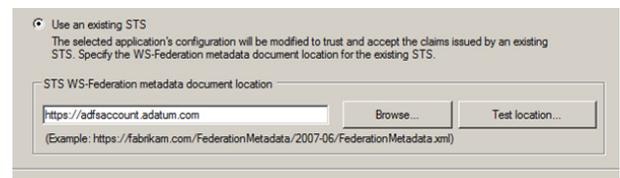
## Supported Federation Service Claim Types

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

## Claims-Aware SAML

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

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



## Manage Endpoint Privilege Management Events

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

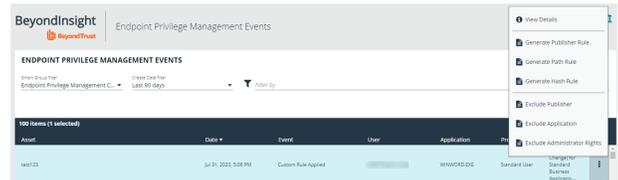


**Note:** This feature is available only when an Endpoint Privilege Management license is detected.

### View Events

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

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



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



**Note:** Depending on the configuration of your grid and selected columns, not all event details may be visible. To configure display preferences, and see other options for the grid display, please see ["Change and Set the Console Display and Preferences"](#) on page 15.

### Create Exclusion or Generate Rule from Event

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

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



**Note:** Exclusions can also be created from the **Exclusions** page. For more information, please see ["Exclude Endpoint Privilege Management Events"](#) on page 107.

## Endpoint Privilege Management Account Rotation

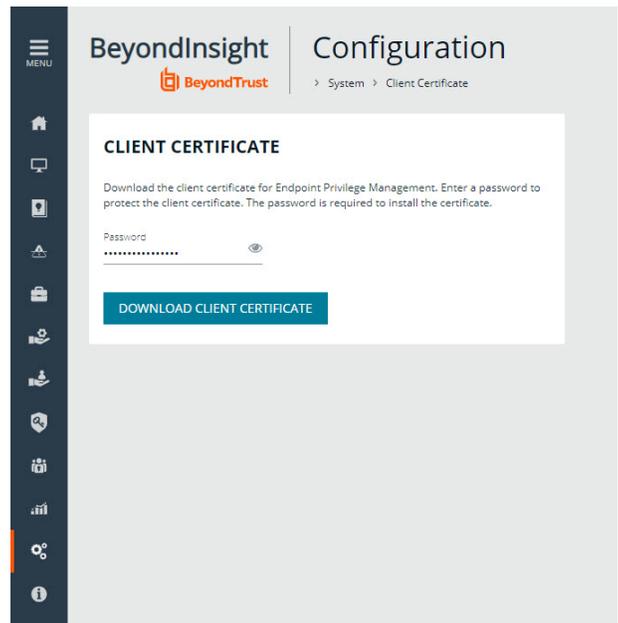
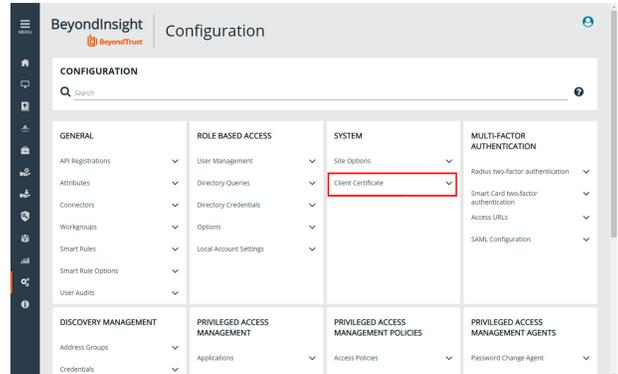


**Note:** Although the current release supports it, this functionality requires an upcoming release of EPM.

The client certificate needed to configure EPM can be downloaded from the Password Safe Cloud web console. BeyondInsight configuration segments can be included in the EPM policy to enable policy management from one console and password policy from Password Safe Cloud.

The integration between Password Safe and Endpoint Privilege Management allows for agent-based local account rotation and privileged account retrieval to *run as* actions. This integration is enabled for cloud deployments of Password Safe and Privilege Management.

To download the client certificate, go to **Configuration > System > Client Certificate** and click **Download Client Certificate**.



## Exclude Endpoint Privilege Management Events

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

### Create an Endpoint Privilege Management Exclusion

1. In the BeyondInsight Console, navigate to **Configuration > Privileged Desktop Management > Endpoint Privilege Management Exclusions**.
2. Click **Create Exclusion +** above the grid.



the specifications in the Smart Rule.

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

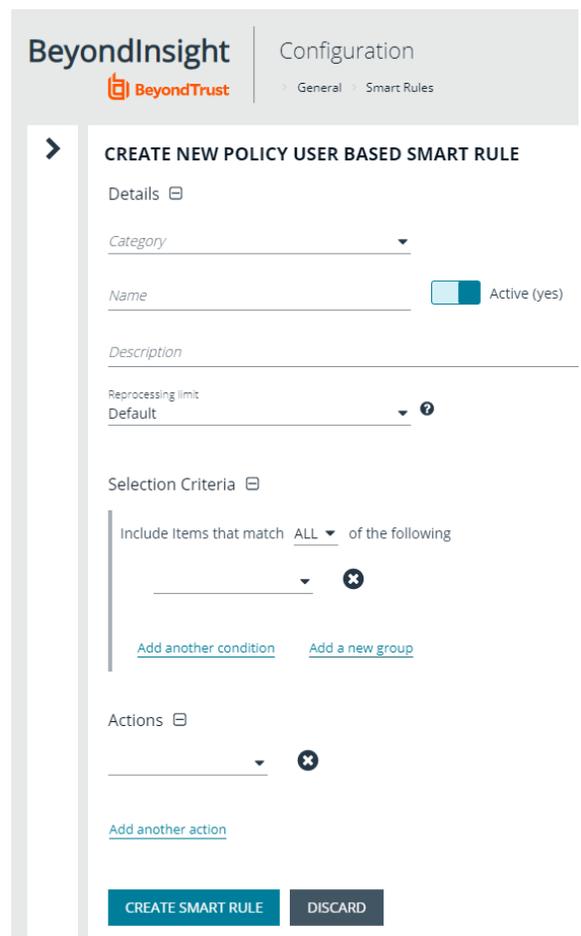
## Create Policy User-Based Smart Rule

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

### View Policy Users

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

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



The screenshot shows the 'Configuration' page in the BeyondInsight console, specifically the 'Smart Rules' section. The main heading is 'CREATE NEW POLICY USER BASED SMART RULE'. Below this, there are several sections: 'Details', 'Selection Criteria', and 'Actions'. The 'Details' section includes a 'Category' dropdown, a 'Name' field with an 'Active (yes)' toggle, and a 'Description' field. The 'Reprocessing limit' is set to 'Default'. The 'Selection Criteria' section shows 'Include Items that match ALL of the following' with a dropdown menu and an 'Add another condition' link. The 'Actions' section has a dropdown menu and an 'Add another action' link. At the bottom, there are two buttons: 'CREATE SMART RULE' and 'DISCARD'.



**Note:** Depending the configuration of your grid and selected columns, not all policy user details may be visible. To configure display preferences, and see other options for the grid display, please see "[Change and Set the Console Display and Preferences](#)" on page 15.

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

## Manage Endpoint Privilege Management Policies

Using BeyondInsight you can deploy Endpoint Privilege Management policies to assets and policy users. From the **Endpoint Privilege Management Policies** page, you can view the Endpoint Privilege Management policies and manage the global priority for the policies.



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

### View Endpoint Privilege Management Policies

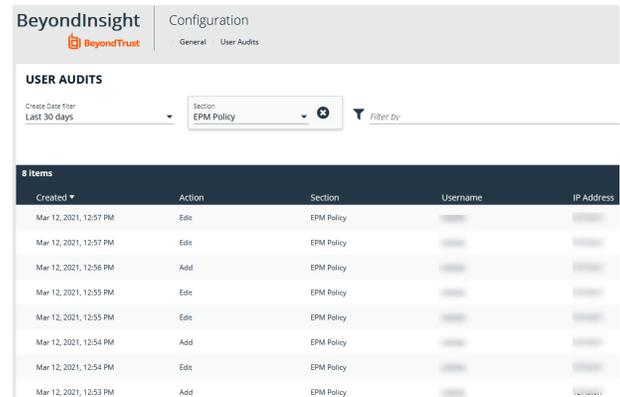
1. In the BeyondInsight Console, click the **MENU**.
2. Under **Endpoint Privilege Management**, click **Policies**.
3. To filter the list of displayed policies, select the desired criteria from the **Filter by** list above the grid. Available filter options are:
  - Policy Name
  - Locked
  - Locked By
  - Policy Version
  - Policy Workgroup
  - Powered by



**Note:** If you select **Filter by > Locked**, you can then select **Locked** or **Unlocked** as the filter criteria. If a policy is locked, this indicates that a user currently has it locked by an external policy editor. The ability to lock, unlock, and edit policies within BeyondInsight is planned for a future release.



**Tip:** You can see who added, modified, or deleted an Endpoint Privilege Management policy from the **Configuration > General > User Audits** page in BeyondInsight.



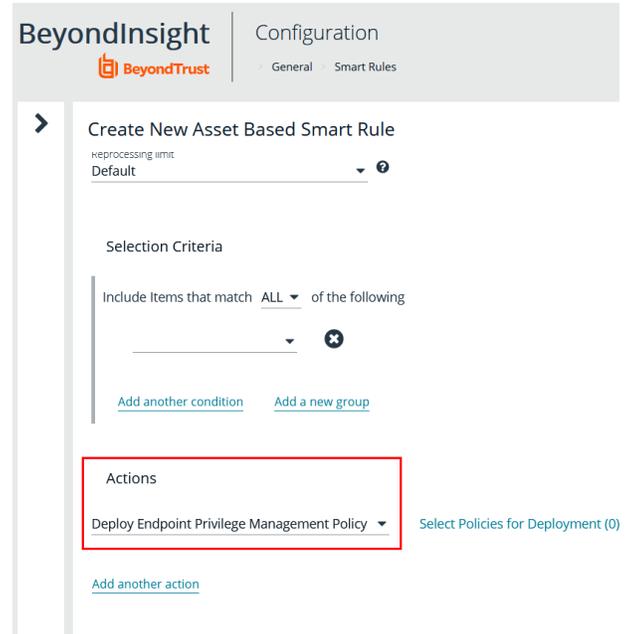
Created	Action	Section	Username	IP Address
Mar 12, 2021, 12:57 PM	Edit	EPM Policy	[REDACTED]	[REDACTED]
Mar 12, 2021, 12:57 PM	Edit	EPM Policy	[REDACTED]	[REDACTED]
Mar 12, 2021, 12:56 PM	Add	EPM Policy	[REDACTED]	[REDACTED]
Mar 12, 2021, 12:55 PM	Edit	EPM Policy	[REDACTED]	[REDACTED]
Mar 12, 2021, 12:55 PM	Edit	EPM Policy	[REDACTED]	[REDACTED]
Mar 12, 2021, 12:54 PM	Add	EPM Policy	[REDACTED]	[REDACTED]
Mar 12, 2021, 12:54 PM	Edit	EPM Policy	[REDACTED]	[REDACTED]
Mar 12, 2021, 12:53 PM	Add	EPM Policy	[REDACTED]	[REDACTED]



**Note:** You can configure display preferences and filters to refine the information displayed. For more information, please see ["Change and Set the Console Display and Preferences"](#) on page 15.

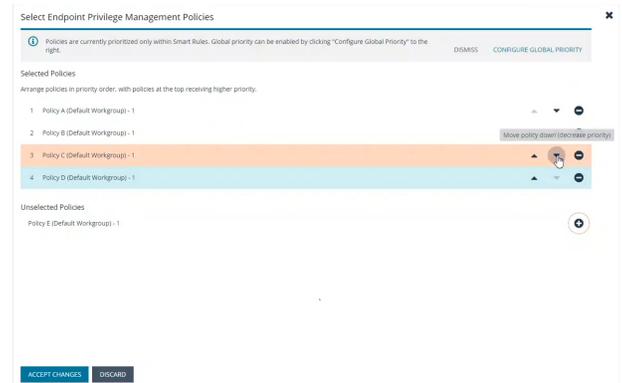
## Deploy Endpoint Privilege Management Policies to Assets and Policy Users Using a Smart Rule

1. From the **Smart Rules** page in BeyondInsight, create an asset or Policy User Based Smart Rule that has an action of **Deploy Endpoint Privilege Management Policy**.

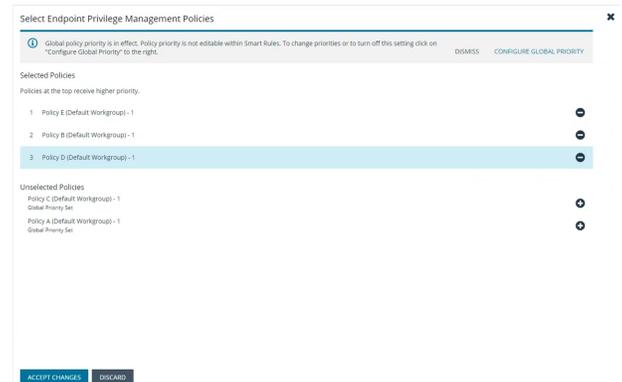


2. Select the policies using the plus sign next to the policy and set their priorities using the arrows. Click **Accept Changes**.

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



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



**Note:** We recommend setting policy priority using the global policy priority feature over setting policy priority within a Smart Rule. For more information on managing global priority for policies, please see, "[Manage Global Priority for Endpoint Privilege Management Policies](#)" on page 112.

**i** For more information on working with Smart Rules to organize assets, please see "[Use Smart Rules to Organize Assets](#)" on page 50.

### Manage Global Priority for Endpoint Privilege Management Policies

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

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

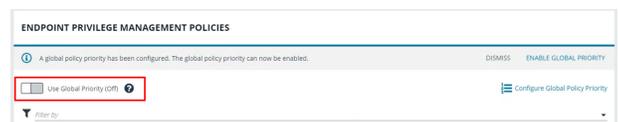
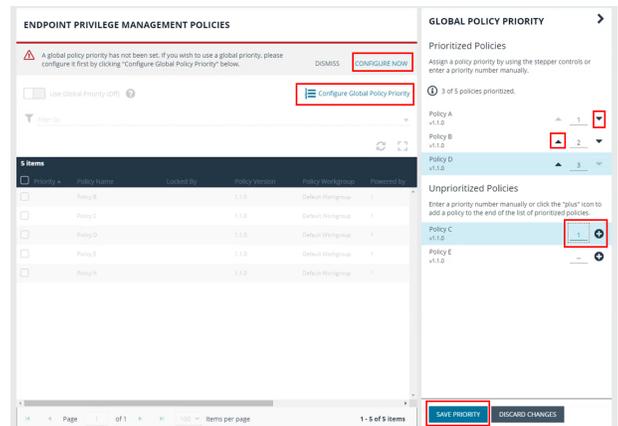
**Note:** The global policy priority feature is supported only in single-tenant BeyondInsight installations. This feature is disabled in multi-organization environments.

Enable global policy priority as follows.

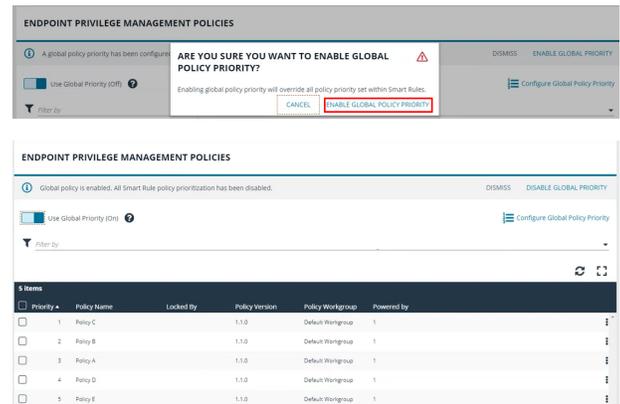
1. From the left menu in BeyondInsight, select **Policies** under **Endpoint Privilege Management**.
2. Click **Configure Global Priority Policy**, or if this is your first time using the global policy priority feature, click **Configure Now** in the banner that displays at the top of the page.
3. Select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

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

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



- A confirmation message displays. Click **Enable Global Policy Priority** in the message box.
- The banner at the top of the page now indicates global policy is enabled and Smart Rule prioritization is disabled, and the policies display in the grid with their assigned priority.



The screenshot shows two states of the 'ENDPOINT PRIVILEGE MANAGEMENT POLICIES' page. The top state shows a confirmation dialog: 'ARE YOU SURE YOU WANT TO ENABLE GLOBAL POLICY PRIORITY?' with a warning icon and a red box around the 'ENABLE GLOBAL POLICY PRIORITY' button. The bottom state shows the page after the action, with a banner indicating 'Global policy is enabled. All Smart Rule policy prioritization has been disabled.' and a table of policies.

Priority	Policy Name	Locked By	Policy Version	Policy Workgroup	Powered by
1	Policy C		1.1.0	Default Workgroup	1
2	Policy B		1.1.0	Default Workgroup	1
3	Policy A		1.1.0	Default Workgroup	1
4	Policy D		1.1.0	Default Workgroup	1
5	Policy E		1.1.0	Default Workgroup	1

## View Endpoint Privilege Management Agents

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



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

### View Agents

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



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

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



**Note:** Depending on the configuration of your grid and selected columns, not all agent details may be visible. To configure display preferences, and see other options for the grid display, please see "**Change and Set the Console Display and Preferences**" on page 15.

## View Endpoint Privilege Management File Integrity Monitoring

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



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

## View File Integrity Monitoring Events

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

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



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



**Note:** *Depending on the configuration of your grid and selected columns, not all file monitoring event details may be visible. To configure display preferences, and see other options for the grid display, please see "Change and Set the Console Display and Preferences" on page 15.*

## Monitor Endpoint Privilege Management Sessions

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



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

## View Session Details

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



**Note:** *Depending on the configuration of your grid and selected columns, not all session details may be visible. To configure display preferences, and see other options for the grid display, please see "Change and Set the Console Display and Preferences" on page 15.*

## Session Replay

1. Follow the steps above to select a session.
2. Click the vertical ellipsis for the session, and then select **View Session...** . **View Session...** is also available when viewing all session details.

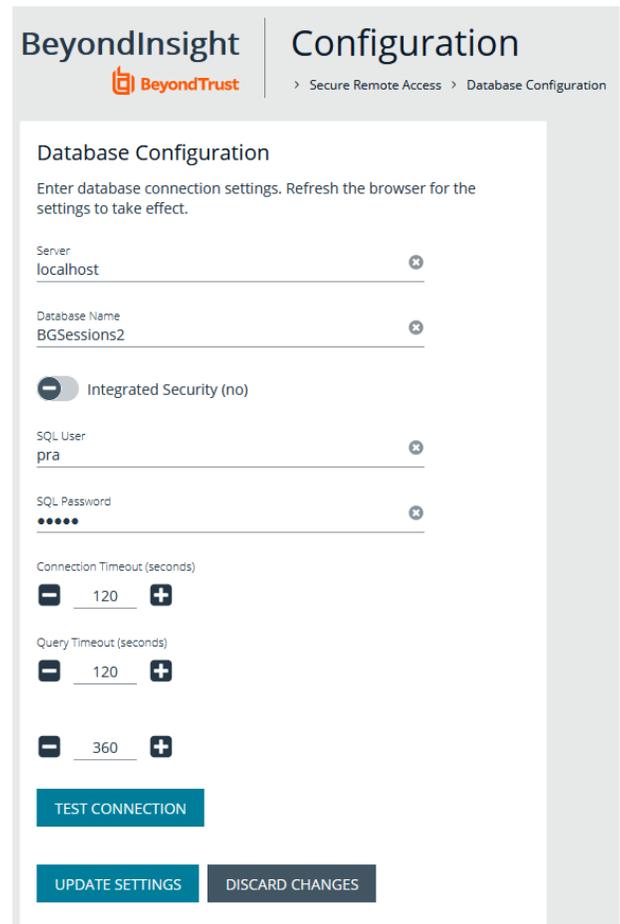
3. A new page opens, showing some details of the session, a list of the **Events** and when they occurred (which can be searched), and a slideshow of the session.
4. Buttons under the slideshow control session playback. You can change the speed of session playback by selecting a different **Slideshow Delay**.
5. You can download an image of any session view by clicking the **Snapshot** button.

## View 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**.



The screenshot shows the 'BeyondInsight Configuration' page. The breadcrumb trail is 'Secure Remote Access > Database Configuration'. The main heading is 'Database Configuration'. Below the heading is a note: 'Enter database connection settings. Refresh the browser for the settings to take effect.'

The form contains the following fields and controls:

- Server:** localhost
- Database Name:** BGSessions2
- Integrated Security:** A toggle switch is turned off, with the text 'Integrated Security (no)'.
- SQL User:** pra
- SQL Password:** A masked password field with four dots.
- Connection Timeout (seconds):** A numeric input field with a value of 120 and minus/plus buttons.
- Query Timeout (seconds):** A numeric input field with a value of 120 and minus/plus buttons.
- Additional Control:** A numeric input field with a value of 360 and minus/plus buttons.

At the bottom of the form are three buttons: 'TEST CONNECTION' (highlighted in blue), 'UPDATE SETTINGS', and 'DISCARD CHANGES'.

## View the Privileged Remote Access Dashboard

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

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

The dashboard displays several summary cards for Privileged Remote Access sessions:

- Privileged Remote Access:** A list of metrics including Sessions By User, Session Count By User, Session Count By Jump Group, Session Count By Endpoint, Longest Sessions By Endpoint, and a Name field.
- Session Count This Month:** A large blue '0' indicating the current session count.
- Top 5 Users With Sessions:** A table listing users and their session counts.
 

User	Count
Hendrick Wilson (bealson)	44
Scott Archer (sarcher)	42
Pat Carroll (PCarroll)	17
Jared Arnes (jarnes)	2
Kari Wilson (swilson)	1
- Top 5 Endpoints With Sessions:** A table listing endpoints and their session counts.
 

EndPoint	Count
pr-week.pentest.local	24
pr-ndg.pentest.local	5
pr-week.dev.local	3
pr-jumpgate	2
WIN-GB505021VED	1
- Top 5 Jump Group With Sessions:** A table listing jump groups and their session counts.
 

JumpGroup	Count
PI Pen Test	47
Development Environments	45
PI Development	8
DevOps	4
Internal Systems	1

- 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.

The 'Sessions by User' view shows a table of session records with the following columns: User, Started, Ended, Duration, Jump Group, and End Point. The table is filtered for the last 30 days and contains 100 items.

User	Started	Ended	Duration	Jump Group	End Point
W.Wilson (wwilson)	Nov 30, 2019, 8:54 AM	Nov 30, 2019, 11:50 AM	02:56:40	Development Environments	WW-DEV
W.Wilson (wwilson)	Nov 29, 2019, 3:58 PM	Nov 29, 2019, 8:06 PM	04:08:35	Development Environments	WW-DEV

## Integrate the BeyondInsight API into Other Applications

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



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

The ID and key are generated by BeyondInsight.

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

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



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

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

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

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

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

6. Click **Create Rule**.

## Support and Product Updates

Click **Menu** in the left navigation toolbar, then **About**, to access support information and tools, product updates, and other resources including documentation links, version details, and the maintenance expiry date.

### Send Files to BeyondTrust Technical Support

You can build and send file packages containing general information for support and collected events.

### Create a Support Package

Create a support package that can be used by Support. The package includes:

- All logs in the BeyondInsight **Logs** folder
- Storage size statistics on the BeyondInsight database
- Certain database tables that contain information on scanner agents, and their jobs
- The **debug\_syncit - log** file used to determine when files are updated from Auto Update



**Note:** Credentials are not stored in any of the package files.

To generate the package:

1. From **Support Tools > Download Support Package**, click **Generate Support Package**.
2. A ZIP file is automatically created and saved to the **Downloads** folder.
3. Email the ZIP file to your support representative.

### Send Analysis Files

Additionally, you can send events collected by Analyzer to provide additional troubleshooting details such as:

- The number of errors collected in the BeyondInsight logs
- Analysis of the events, including percentages of types (processed and purged)
- The percentage of duplicate and timed out agents
- Analysis of BeyondTrust components
- Customer name

To generate analysis files:

From **Support Tools > Send Analysis to Support**, click **Send Analysis to Support**. This generates an analysis file and sends it to Support.



**Tip:** Analysis files are retained for 30 days. You can click a link on the **About** page to request that the data be deleted prior to the 30 day expiry.

### Download Updates

BeyondInsight ships with BeyondTrust Updater.

Using the update tool, you can set up subscriptions to download product updates for BeyondInsight, Event Server, and BeyondTrust Updater.

## Maintenance Information

This panel displays the contract **Maintenance Expiry Date** for BeyondInsight.

If your maintenance is close to expiry or has expired, a warning banner displays at the top of the Dashboard. The toggle **Hide Maintenance Expiry Warning Banner** can be set to on or off, to enable or disable this warning.



**Note:** *The **Maintenance Expiry Warning Banner** is only visible to administrators. Hiding the banner hides it from all administrators.*