



BeyondTrust

BeyondInsight 23.2 Cloud User Guide

Table of Contents

BeyondInsight User Guide - Cloud Deployment	5
Log In to the BeyondInsight Console	6
Log Out of the Console	7
Select a Display Language	7
Navigate the Console	9
Switch Between BeyondTrust Applications	10
Dynamic Dashboards	11
Customize a Dashboard	12
Change and Reset Console Login Passwords	13
Change Password and Two-Factor Authentication Settings	13
Reset Password	14
Change and Set the Console Display Preferences	16
Set Display Preferences	16
Filter Records	16
Role Based Access	18
Create and Edit Directory Credentials	19
Create an Active Directory Credential	20
Create an LDAP Credential	21
Create an Azure Active Directory Credential	22
Edit a Directory Credential	22
Map Directory Credentials to a Domain	24
Create and Configure Groups	25
Create a BeyondInsight Local Group	26
Add an Active Directory Group	28
Configure Active Directory Group Synchronization	31
Add an Azure Active Directory Group	32
Add an LDAP Group	35
Assign Group Permissions	39
Assign Features Permissions	40
Assign Smart Groups Permissions	45
Edit and Delete Groups	46

Edit Basic Group Details	46
Edit Advanced Group Details	47
Delete a Group	49
Create and Manage User Accounts	50
Audit Console Users in BeyondInsight Cloud	60
Overview of BeyondInsight Tools	61
Create an Address Group	62
Create a Directory Query	66
Attributes and Attribute Types in BeyondInsight	67
Use Smart Rules to Organize Assets	69
Use Smart Rule Filters and Smart Groups	70
Create Smart Rules	73
Smart Rule Processing	75
Perform Other Smart Rule Actions	76
Add Credentials to Use in Scans	79
Create Oracle Credentials	83
Create SNMP Credentials	84
Create SSH Credentials	85
Run Discovery Scans	86
Use the Scan Wizard to Create a Discovery Scan	86
Run Scans from a List of Assets	87
Use Smart Rules as Targets for Scans	88
Check Completed and Scheduled Scans	89
Discover Assets Using a Smart Group	90
Key Steps	90
Manage Scan Jobs	92
Manage Assets	93
Review Asset Details	93
Create Assets Manually	94
Delete Assets	95
Run Scans on Cloud Platforms in BeyondInsight	96
Amazon EC2 Requirements	96
Azure Requirements	96

Google Cloud Requirements	97
Hyper-V Requirements	97
Configure a Cloud Connector	98
Cloud Connector Smart Groups	99
Configure BeyondInsight AWS Connector	99
Set BeyondInsight Options	101
Set Account Lockout Options	101
Set Account Password History	101
Configure the System Event Viewer	102
Configure Global Website Options	103
List Domains and LDAP Servers on the Login Page	103
Disable Forgot Password Link	103
Disable Social Media links on the Login and About pages	103
Change the Refresh Interval for Smart Rules	104
Configure a Pre-Login Banner	104
Configure Session Options	104
Enable Language Selection (Localization)	105
Configure Global Discovery Credential Access Keys	105
Configure a Claims-Aware Website to Log In with SAML	106
Create a BeyondInsight Group	106
Add Relying Party Trust	106
Set Up Claim Rules	107
Supported Federation Service Claim Types	107
Claims-Aware SAML	107
Disable Forms Login	108
Integrate the BeyondInsight API into Other Applications	110

BeyondInsight User Guide - Cloud Deployment

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

This guide provides instructions and procedures for using BeyondInsight.

Log In to the BeyondInsight Console

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

The following authentication types can be used:

- **BeyondInsight:** Create local users in BeyondInsight and add them to groups to assign permissions to features. Local users can log in to the console from the BeyondInsight login page.
- **Active Directory:** Add Active Directory users in BeyondInsight and add them to groups to assign permissions to features. Active Directory users can log in to the console from the BeyondInsight login page.
- **Azure Active Directory:** Add Azure Active Directory users in BeyondInsight and add them to groups to assign permissions to features. Azure Active Directory users can log in to the console from the BeyondInsight login page.



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

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



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

To log in:

1. Open a browser and enter the URL for your BeyondInsight / Password Safe cloud instance:
https://<hostname>/WebConsole/index.html.
2. Enter your username and password. The default username is **Administrator**, and the password is the administrator password you set in the initialization email.
3. If applicable, select a domain or LDAP Server from the **Log in to** list.



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

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



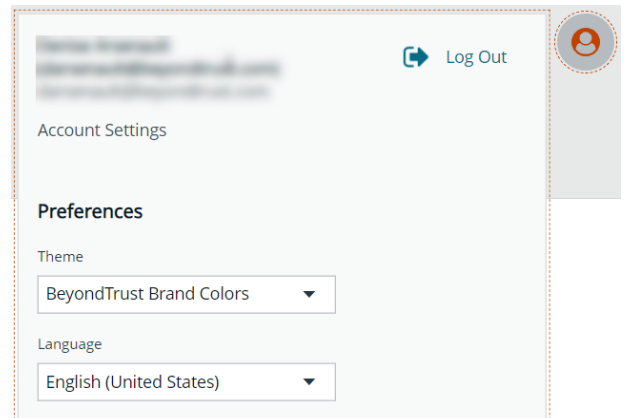
Note: If the initial login attempt fails, and two-factor authentication (2FA) is enabled, the user is taken to the 2FA page for security reasons.



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

Log Out of the Console

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



Select a Display Language

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

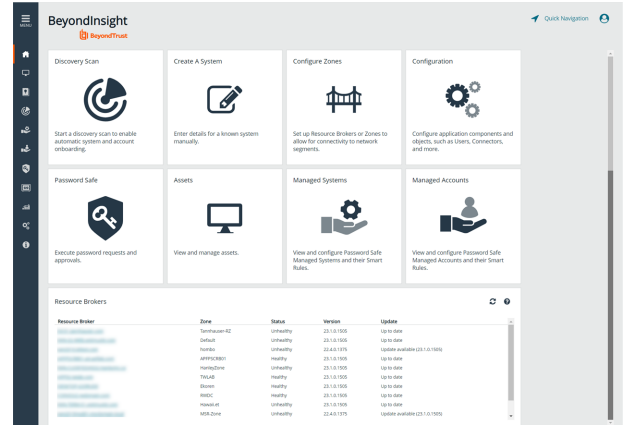
- English
- French
- German
- Japanese
- Korean
- Portuguese
- Spanish


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

Navigate the Console

Once logged into the BeyondInsight console, you are taken to the **Home** page, where the suite of features is easily accessible using any of the following methods:

- Click the container cards.
- Click the icons in the left navigation panel.
- Click **Menu** in the left navigation panel, and then click your desired feature.
- Click **Quick Navigation** in the top-right corner of the **Home** page or press **CTRL+K** to access it. Then locate your desired feature from the list by typing at least 3 characters of the feature name or by scrolling through the list, and then click the feature.





Tip: To access what you need in BeyondInsight with fewer clicks, use the **Quick Navigation** feature to favorite your most frequently visited pages. Click the star next to any of the listed options to add them to your favorites. Once you have made a list item a favorite, it is moved to the top of the **Quick Navigation** list, under **Favorites**. Click the star next to any favorite list item to remove it from **Favorites**.

You can quickly access the following functionality from the container cards:

- Initiate a discovery scan to discover new systems and accounts.
- Create a new managed system manually.
- Set up Resource Brokers and Resource Zones to allow for connectivity to network segments.
- Access configuration settings for BeyondInsight and Password Safe components and objects.
- Access Password Safe to execute password requests and approvals.
- View and manage assets.
- View and edit managed systems.
- View and edit managed accounts.

You can also view the following most recent information for your Resource Zones and Resource Brokers from the dynamically updated dashboard card:

- List of Resource Zones and how many Resource Brokers are checked in for each Zone
- List of Resource Brokers, as well as the Zone they are in, and their health statuses

The following features are available from the left navigation menu:

- **Dashboard (Preview):** Customize your dynamic dashboards using the **Dashboard Editor**.
- **Assets:** Display and manage all assets. Access the **Smart Rules** page to create and manage Smart Groups. Add assets to Password Safe management.
- **Smart Rules:** View and manage Smart Rules.
- **Discovery:** Run and schedule discovery scans, review active, completed, and scheduled scans, and view the list of discovery scanners.

- **Managed Systems:** View and configure properties for Password Safe managed systems, managed databases, managed directories, managed applications, and their associated Smart Rules.
- **Managed Accounts:** View and configure properties for Password Safe managed accounts and their associated Smart Rules.
- **Password Safe:** Access the Password Safe web portal to request passwords and remote access sessions and to approve requests.
- **Secrets Safe:** View and manage team secrets.
- **Analytics & Reporting:** Access reports on collected data.
- **Configuration:** Configure BeyondInsight and Password Safe components and objects, such as users and groups, authentication settings, connectors, and much more.
- **About:** Access helpful links. View the current BeyondInsight version information, as well as the history of installed versions.

Switch Between BeyondTrust Applications

If you have BeyondTrust Identity Security Insights, you can connect Password Safe Cloud and other BeyondTrust applications, and then switch between applications without needing to re-enter credentials. Re-entering credentials may be necessary in some circumstances, depending on the login configuration of the different applications.

The **App Switcher** menu appears in the upper right. Click the menu for a list of connected applications, and click an application. There can be more than one instance of an application, except for Identity Security Insights.

The menu only appears if there are connected applications. If all connected applications are removed from the Insights instance, then the menu no longer displays.

Configuration of this feature is managed in BeyondTrust Identity Security Insights.



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

Dynamic Dashboards

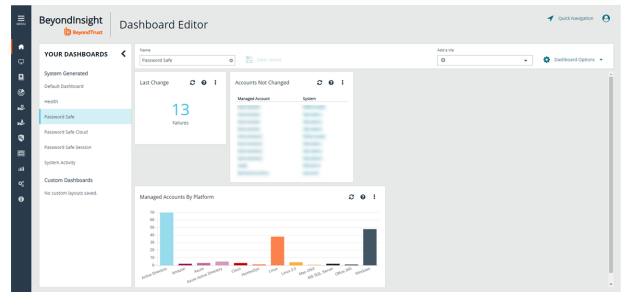


Note: Only admin access is supported at this time, and more features will be added in later releases.

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

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

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



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

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



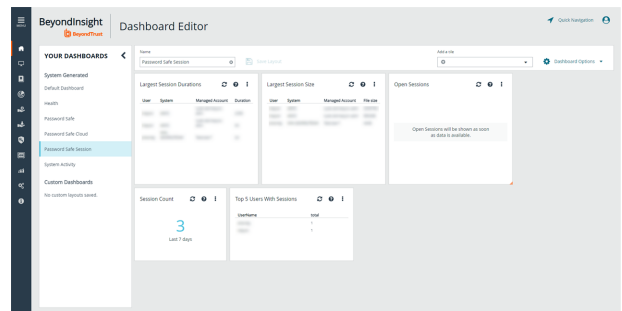
Click to refresh information displayed.



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

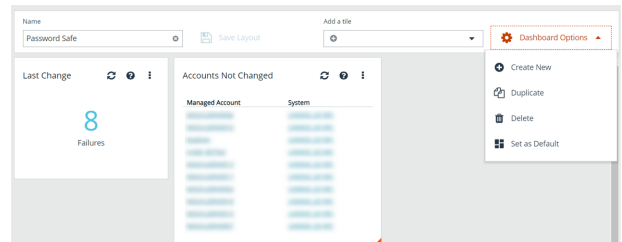


Click to delete the tile. You can always add the tile later if needed.



Use **Dashboard Options** to:

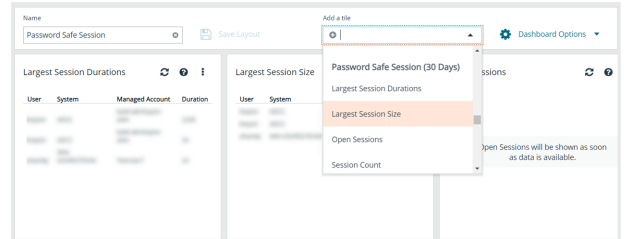
- **Create New:** Create a new empty dashboard, then add the tiles you want.
- **Duplicate:** Create a copy of the dashboard that can be modified.
- **Delete:** Delete the selected dashboard.
- **Set as Default:** Set the current dashboard as the default so it displays every time you click **Menu > Dashboards**.



Customize a Dashboard

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

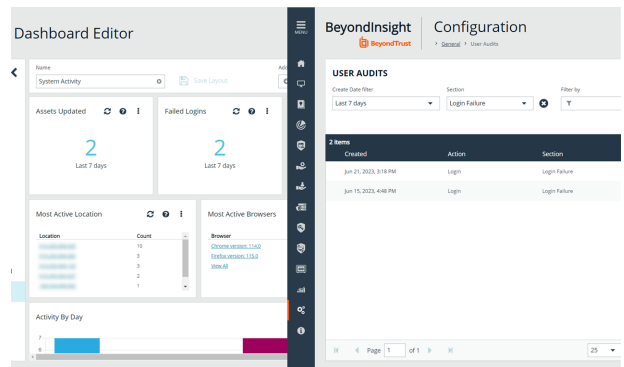
1. To create a custom dashboard, select one of the available dashboard cards. In this example we use the **Password Safe** card. If necessary, delete any of the existing tiles that come installed with that card.
2. From the **Add a tile** dropdown, select the tiles you want to add. Resize and reposition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



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

Access Dashboard Tile Information

The information displayed on some tiles can be used to access all relevant data associated with it. In this example, by clicking on the **2** in the **Failed Logins Last 7 days** tile, you are taken directly to the **User Audits** page, where you can get full details on the 2 failed logins. The grid is automatically filtered to show login failures for the last 7 days.

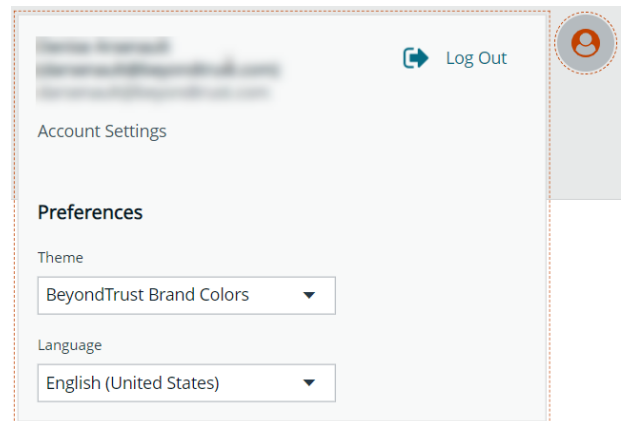


Change and Reset Console Login Passwords

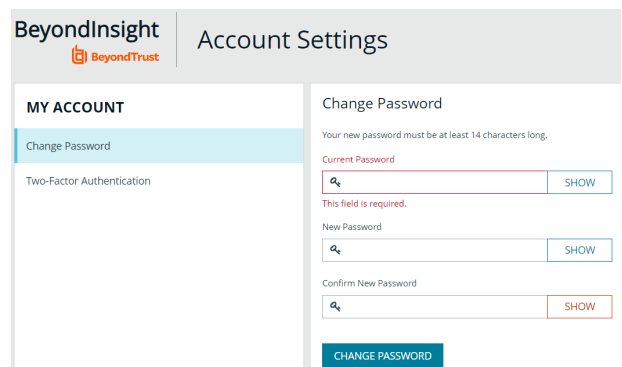
Change Password and Two-Factor Authentication Settings

Users can maintain the security and control of their account and protect it against unauthorized access. If you are logging in with a BeyondInsight local user account, you can change your password and two-factor authentication app from the **Account Settings** page. You cannot change your password if you are logging in with Active Directory or LDAP credentials, or if your account is locked out.

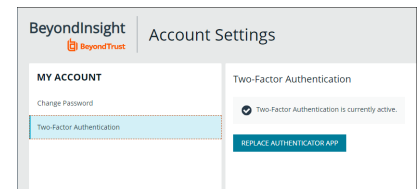
1. In the console, click the **Profile and preferences** icon in the top-right corner.
2. Click **Account Settings**.



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



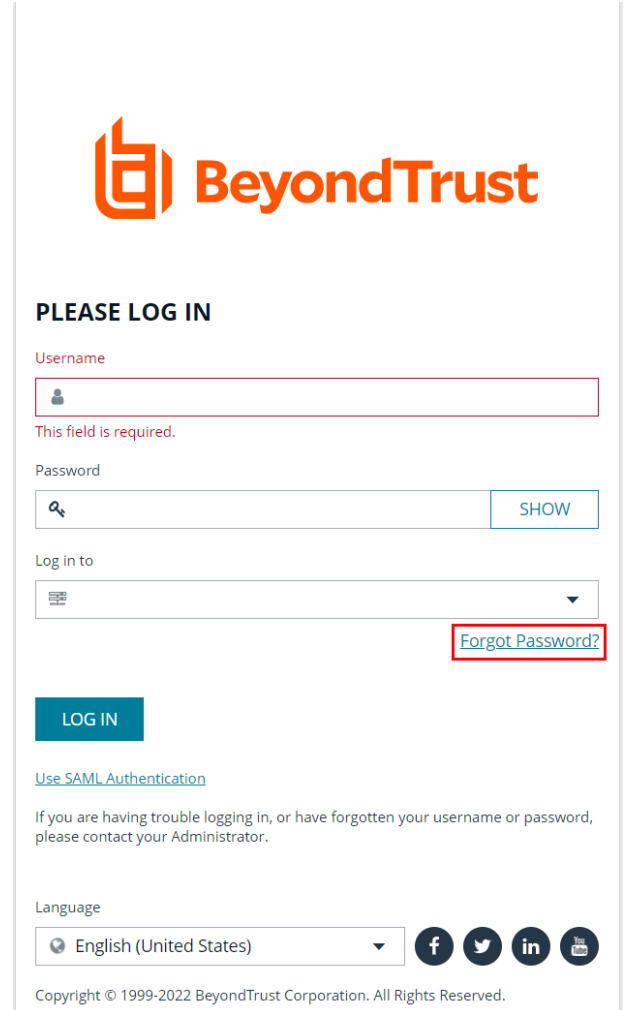
4. If your account has two-factor authentication enabled and registered with a device, you can update the authenticator app as follows:
 - Select **Two-Factor Authentication** from the **My Account** pane.
 - Click **Replace Authenticator App**.
 - Click **Reconfigure Authenticator App** to register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



Reset Password

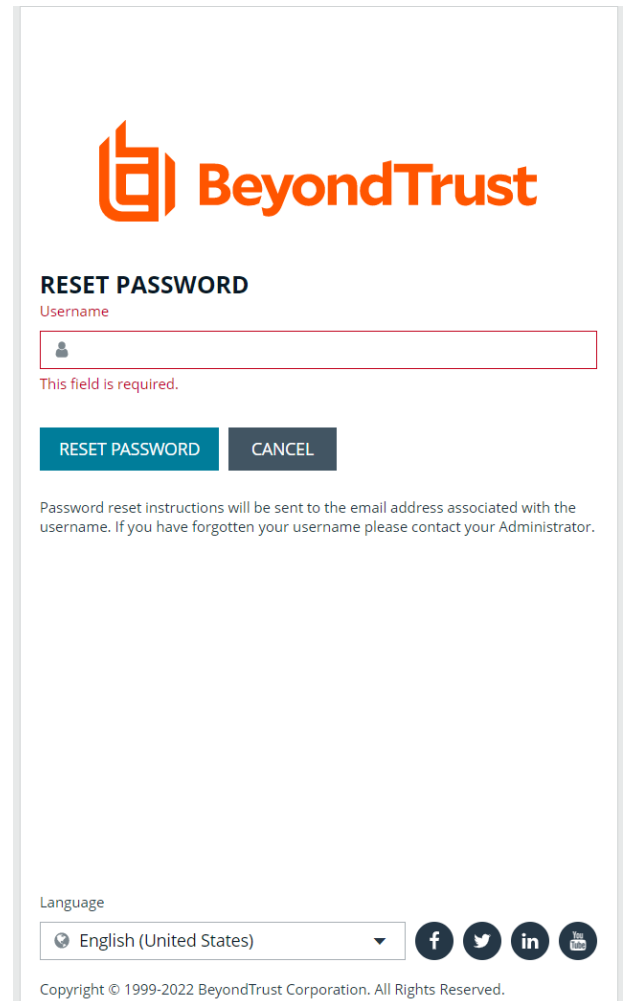
If you forget your console password, you can reset it as follows:


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



The screenshot shows the BeyondTrust login interface. At the top is the BeyondTrust logo. Below it is the heading "PLEASE LOG IN". There are three input fields: "Username" (with a red border and a "This field is required." error message), "Password" (with a "SHOW" button), and "Log in to" (with a dropdown arrow). A red box highlights the "Forgot Password?" link located to the right of the "Log in to" field. Below the fields is a blue "LOG IN" button, a link for "Use SAML Authentication", and a note: "If you are having trouble logging in, or have forgotten your username or password, please contact your Administrator." At the bottom, there is a "Language" dropdown menu set to "English (United States)" and social media icons for Facebook, Twitter, LinkedIn, and YouTube. The footer contains the copyright notice: "Copyright © 1999-2022 BeyondTrust Corporation. All Rights Reserved."

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



 **BeyondTrust**

RESET PASSWORD

Username





This field is required.

RESET PASSWORD **CANCEL**

Password reset instructions will be sent to the email address associated with the username. If you have forgotten your username please contact your Administrator.

Language

English (United States)

Copyright © 1999-2022 BeyondTrust Corporation. All Rights Reserved.

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



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

Change and Set the Console Display Preferences

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

Set Display Preferences

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



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

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

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



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

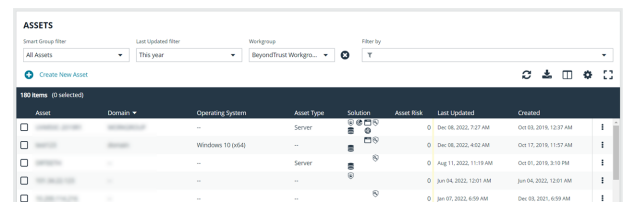
3. An option to change the number of displayed **Items per page** is located below the grid.
4. The changes appear dynamically as they are selected.

Filter Records

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

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

- **Smart Group filter:** Select to filter information by Smart Group association.
- **Last Updated filter:** Select to filter by a specific period or a custom date range.
- **Filter by:** Choose to filter the information by **Domain**, **Operating System**, **Workgroup**, etc., or other details specific to the information displayed. For each filter selected, enter the content you want to search for in the filter box's text field.



Asset	Domain	Operating System	Asset Type	Solution	Asset Risk	Last Updated	Created
...	Server	Dec 08, 2022, 7:27 AM	Oct 01, 2016, 12:37 AM
...	...	Windows 10 (x64)	Dec 08, 2022, 4:52 AM	Oct 17, 2016, 11:57 AM
...	Server	Aug 11, 2022, 11:19 AM	Oct 01, 2016, 9:18 PM
...	Jun 14, 2022, 12:01 AM	Jun 04, 2022, 12:01 AM
...	Jan 07, 2022, 6:09 AM	Dec 03, 2021, 6:09 AM

3. Apply as many filters as desired.
4. The information dynamically changes to match the selections.
5. Filter selections persist if the page is reloaded. To remove a filter, click the **X** on the filter.

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

Role Based Access

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

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



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

Create and Edit Directory Credentials

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



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

To create a directory credential in BeyondInsight:

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

Create an Active Directory Credential

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



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

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



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

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

New Directory Credential ➤

Directory Type

Active Directory

LDAP

Azure Active Directory

Credentials

Title

Domain

Use SSL

Username

Password

Password SHOW

Confirm Password SHOW

Use Group Resolution (Optional) ?

TEST CREDENTIAL
CREATE CREDENTIAL
DISCARD

Create an LDAP Credential

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



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

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



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

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

New Directory Credential ➤

Directory Type

Active Directory
 LDAP
 Azure Active Directory

Credentials

Title

LDAP Server

Port - +

Use SSL

Password

Bind DN

Password SHOW

Confirm Password SHOW

Use Group Resolution (Optional) ?

TEST CREDENTIAL

CREATE CREDENTIAL
DISCARD

Create an Azure Active Directory Credential

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



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

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

New Directory Credential ➤

Directory Type

Active Directory
 LDAP
 Azure Active Directory

Credentials

Title

Client ID

Tenant ID

Client Secret SHOW

Use Group Resolution (Optional) ?

TEST CREDENTIAL
CREATE CREDENTIAL
DISCARD

Edit a Directory Credential

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

2. Make the changes required.



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

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

Edit Directory Credential ➔

Credentials

Title

Domain

Use SSL

Username

CHANGE PASSWORD

Use Group Resolution (Optional) ?

TEST CREDENTIAL
UPDATE CREDENTIAL
DISCARD CHANGES



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

Map Directory Credentials to a Domain

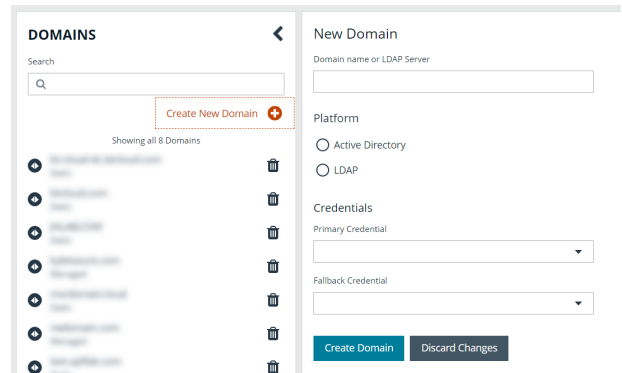
Domain management allows you to map a default primary directory credential and an optional fallback credential as preferred binding credentials used for account resolution against domains in your environment when logging in to BeyondInsight.



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

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

1. Navigate to **Configuration > Role Based Access > Domain Management**.
2. Click **Create New Domain** to create a new one.
3. Provide the name of the domain or LDAP server.
4. Select the type of platform.
5. Select a **Primary Credential** from the dropdown.
6. Select a **Fallback Credential** from the dropdown.
7. Click **Create Domain**.

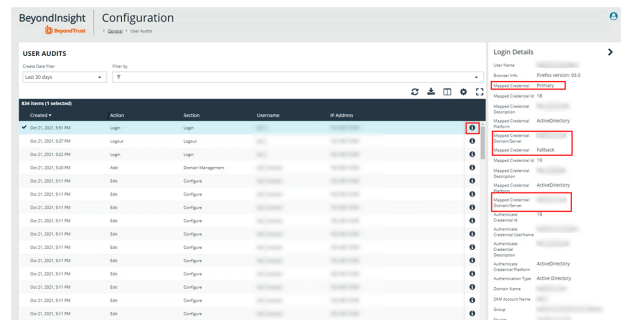


8. To edit credentials for an existing domain, select the domain from the left pane, make your edits, and then click **Save Domain**.



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

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

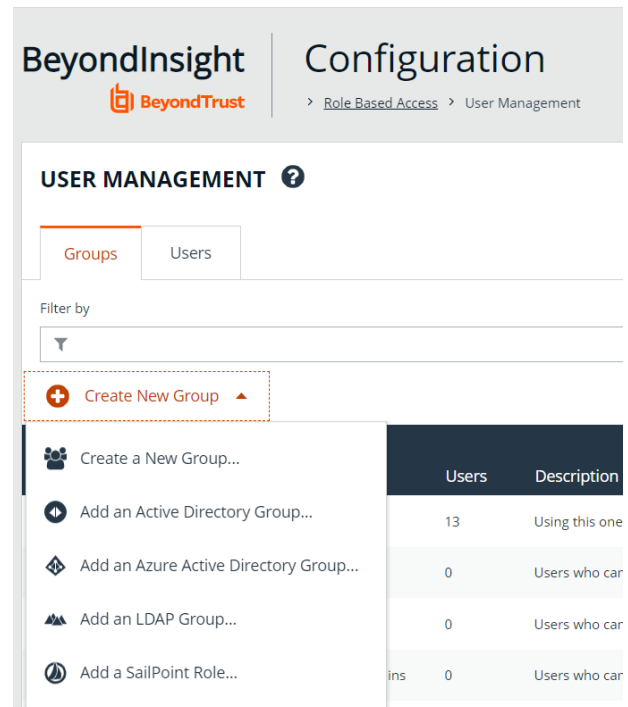


Create and Configure Groups

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

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

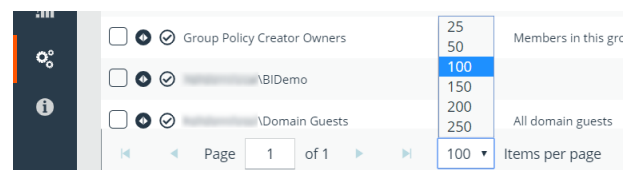
You can create BeyondInsight local groups, as well as add Active Directory, Azure Active Directory, and LDAP groups into BeyondInsight.



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



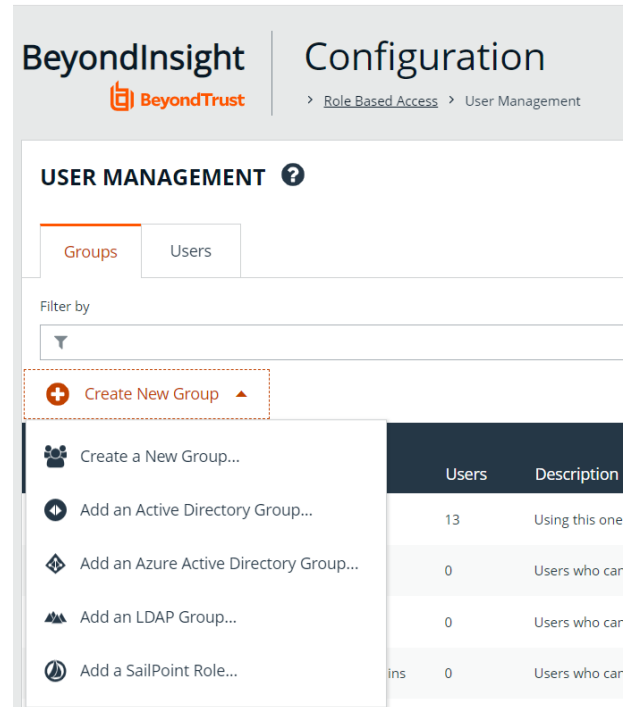
Tip: By default, the first 100 groups are displayed per page. You can change this by selecting a different number from the Items per page dropdown at the bottom of the grid.



Create a BeyondInsight Local Group

To create a local group in BeyondInsight, follow the below steps:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **Create New Group**.
3. Select **Create a New Group**.



The screenshot shows the 'Configuration' page in BeyondInsight, specifically the 'User Management' section. The 'Groups' tab is selected. A 'Filter by' dropdown is visible. The 'Create New Group' button is highlighted with a red dashed box, and its dropdown menu is open, showing several options: 'Create a New Group...', 'Add an Active Directory Group...', 'Add an Azure Active Directory Group...', 'Add an LDAP Group...', and 'Add a SailPoint Role...'. A table is partially visible on the right side of the page.


	Users	Description
Using this one	13	Using this one
Users who car	0	Users who car
Users who car	0	Users who car
Users who car	0	Users who car

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

Create New Group

Active

Group Name

New Test Group 

Description

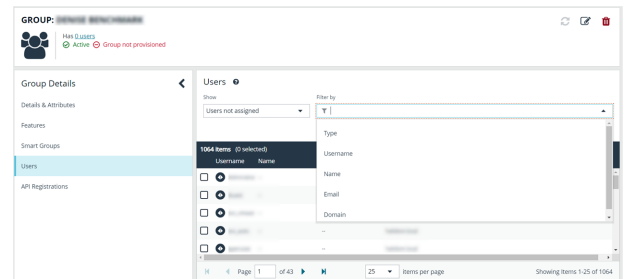
New Test Group 

CREATE GROUP

DISCARD

7. Assign users to the group:

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



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



Note: By default, new groups are not assigned any permissions. You must assign permissions on features and Smart Groups after creating a new group. For more information on permissions and how to assign them, please see "[Assign Group Permissions](#)" on page 39.



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

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

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

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

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

Add an Active Directory Group

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



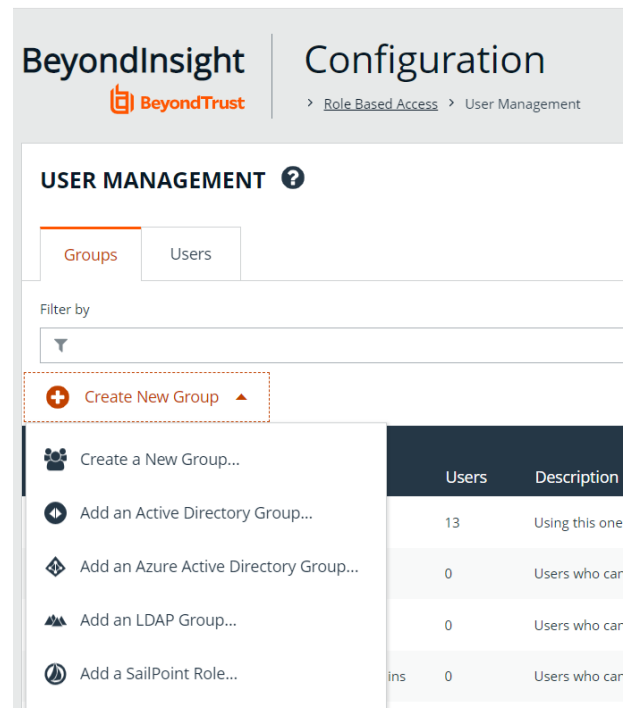
Tip: The **Log in to** list is only displayed on the **Login** page when there are either AD or LDAP user groups created in the BeyondInsight console. The **Log in to** list is displayed by default, but may be disabled / enabled by an admin user by toggling the **Show list of domains/LDAP servers on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



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

Create an Active Directory Group in BeyondInsight, as follows:

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



The screenshot shows the BeyondInsight Configuration page. The breadcrumb trail is **Configuration > Role Based Access > User Management**. The **USER MANAGEMENT** section has two tabs: **Groups** (selected) and **Users**. Below the tabs is a "Filter by" dropdown menu. A **Create New Group** button with a plus icon is highlighted with a dashed red box. A dropdown menu is open below it, listing several options: **Create a New Group...**, **Add an Active Directory Group...**, **Add an Azure Active Directory Group...**, **Add an LDAP Group...**, and **Add a SailPoint Role...**. To the right of the dropdown menu is a table with columns **Users** and **Description**.

	Users	Description
Add an Active Directory Group...	13	Using this one
Add an Azure Active Directory Group...	0	Users who car
Add an LDAP Group...	0	Users who car
Add a SailPoint Role...	ins 0	Users who car

4. Select a credential from the list.



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

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

Active Directory Group Search ➤

Credential

[Create New Credential...](#)

Domain

Filter by Group Name

SEARCH ACTIVE DIRECTORY

CANCEL



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

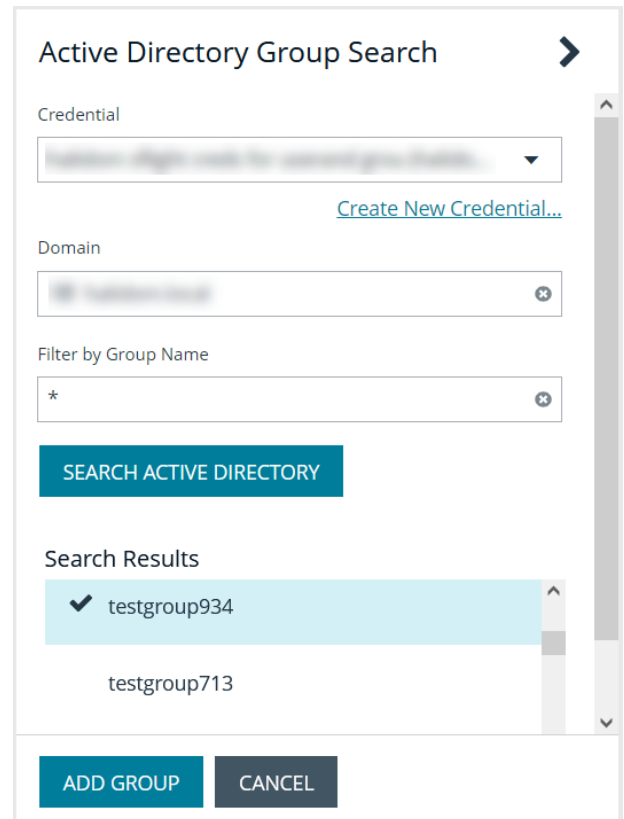
7. Set a filter on the groups to refine the list, and then click **Search Active Directory**.



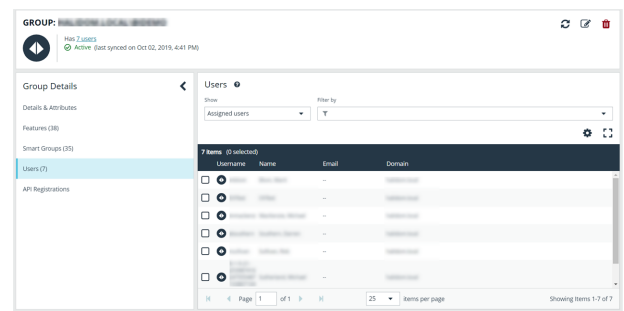
Example: Sample filters:

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

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



9. The group is added and set to **Active** but not provisioned or synchronized with AD. Synchronization with AD to retrieve users begins immediately.
10. Once the group has been synced with AD, you can view the users assigned to the group by selecting **Users** from the **Group Details** pane.




Tip: Use the filters above the grid to narrow down the list of users displayed in the grid by **Type**, **Username**, **Name**, **Email**, or **Domain**, or to show users not assigned to the group.



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 39.



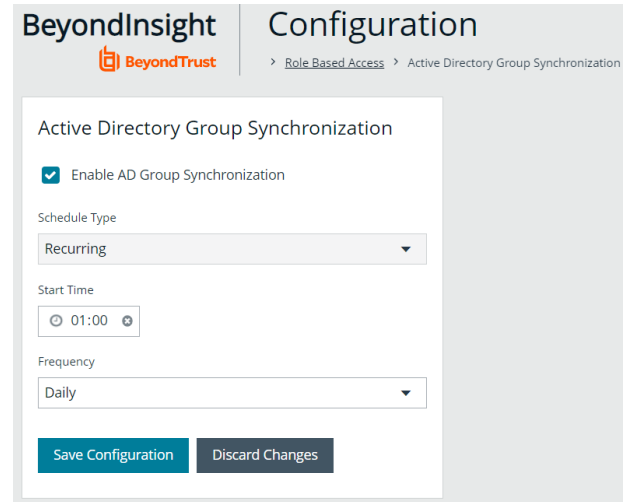
For more information on creating and editing directory credentials, please see ["Create and Edit Directory Credentials"](#) on page 19.

Configure Active Directory Group Synchronization

Create and enable a recurring schedule for AD groups to automatically synchronize at a specified time and frequency. This ensures your AD groups are up to date with the latest users added to that group in Active Directory. This schedule applies globally to all AD groups in your BeyondInsight instance; however, the global schedule can be overridden at the group level and a group can be configured to be excluded from the synchronization process.

To enable **Active Directory Group Synchronization**:

1. Navigate to **Configuration > Role Based Access > Active Directory Group Synchronization**.
2. Check the **Enable AD Group Synchronization** option.
3. Specify a **Start Time**.
4. Select your desired frequency of **Daily**, **Weekly**, or **Monthly**.
5. Click **Save Configuration**.



The screenshot shows the 'Active Directory Group Synchronization' configuration page in the BeyondInsight interface. The page has a breadcrumb trail: 'Configuration > Role Based Access > Active Directory Group Synchronization'. The main content area is titled 'Active Directory Group Synchronization' and contains the following settings:

- Enable AD Group Synchronization
- Schedule Type: Recurring (dropdown menu)
- Start Time: 01:00 (time picker)
- Frequency: Daily (dropdown menu)
- Buttons: Save Configuration (blue), Discard Changes (grey)



For more information on overriding the global AD synchronization schedule and excluding a group from the synchronization process, please see "[Edit Basic Group Details](#)" on page 46.

Add an Azure Active Directory Group

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



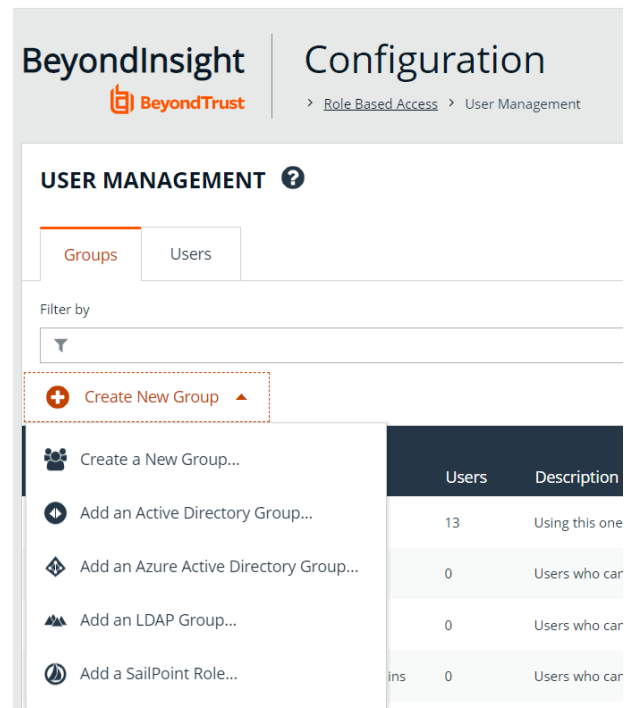
Tip: The **Log in to** list is only displayed on the **Login** page when there are either AD or LDAP user groups created in the BeyondInsight console. The **Log in to** list is displayed by default, but may be disabled / enabled by an admin user by toggling the **Show list of domains/LDAP servers on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



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

Create an Azure Active Directory Group in BeyondInsight, as follows:


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



The screenshot shows the BeyondInsight Configuration page. The breadcrumb trail is **Configuration > Role Based Access > User Management**. The main heading is **USER MANAGEMENT** with a help icon. There are two tabs: **Groups** (selected) and **Users**. Below the tabs is a 'Filter by' dropdown menu. A **Create New Group** button with a plus icon is highlighted with a dashed red box. A dropdown menu is open below it, listing several options: **Create a New Group...**, **Add an Active Directory Group...**, **Add an Azure Active Directory Group...**, **Add an LDAP Group...**, and **Add a SailPoint Role...**. To the right of the dropdown menu is a table with columns **Users** and **Description**.

	Users	Description
Add an Active Directory Group...	13	Using this one
Add an Azure Active Directory Group...	0	Users who car
Add an LDAP Group...	0	Users who car
Add a SailPoint Role...	ins 0	Users who car

- Select a credential from the list.

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

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

Azure Active Directory Group Search ➤

Credential


[Placeholder]
▼

[Create New Credential...](#)


Filter by Group Name

*
✕

SEARCH AZURE ACTIVE DIRECTORY
CANCEL

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

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

 **Example:** Sample filters:

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

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

Search Results

Functional Accounts
Group used to store Functional Accounts for QA testing

✓ **PS_QA**
PasswordSafe QA

Managed Accounts
Password Safe Managed Accounts

MsamiGRP
First test group

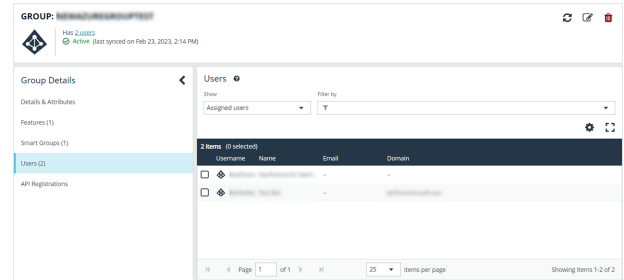
Automation
For Automation users

Admir
Group of administrators

ADD GROUP
CANCEL

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

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



Note: By default, new groups are not assigned any permissions. You must assign permissions on features and Smart Groups after creating a new group. For more information on permissions and how to assign them, please see ["Assign Group Permissions" on page 39](#).



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



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

Add an LDAP Group

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



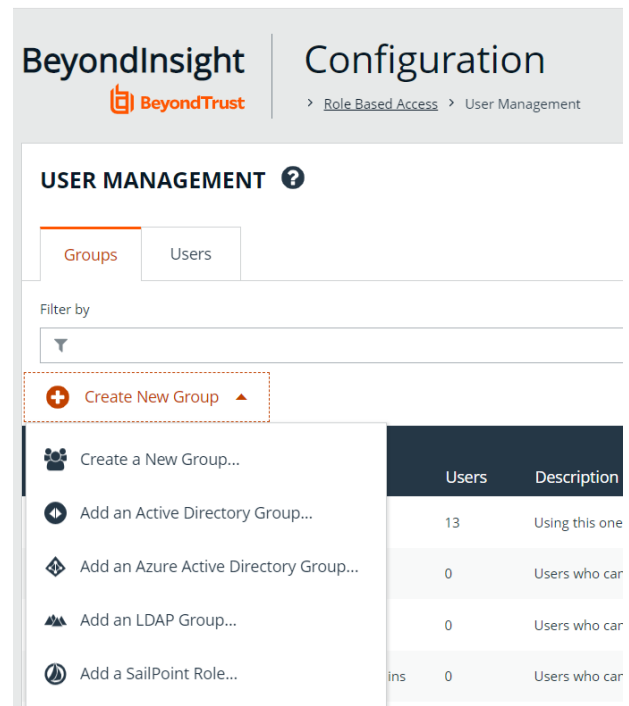
Tip: The **Log in to** list is only displayed on the **Login** page when there are either AD or LDAP user groups created in the BeyondInsight console. The **Log in to** list is displayed by default, but may be disabled / enabled by an admin user by toggling the **Show list of domains/LDAP servers on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



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

Create an LDAP Group in BeyondInsight, as follows:

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



The screenshot shows the BeyondInsight Configuration page. The breadcrumb trail is **Configuration > Role Based Access > User Management**. The **USER MANAGEMENT** section has two tabs: **Groups** (selected) and **Users**. Below the tabs is a "Filter by" search box. A **Create New Group** button with a plus icon is highlighted with a dashed red box. A dropdown menu is open below it, listing several options: **Create a New Group...**, **Add an Active Directory Group...**, **Add an Azure Active Directory Group...**, **Add an LDAP Group...**, and **Add a SailPoint Role...**. To the right of the dropdown is a table with columns **Users** and **Description**.

	Users	Description
Add an Active Directory Group...	13	Using this one
Add an Azure Active Directory Group...	0	Users who car
Add an LDAP Group...	0	Users who car
Add a SailPoint Role...	ins 0	Users who car

4. Select a credential from the list.



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

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

LDAP Group Search ➤

Credential

[Create New Credential...](#)

Server

Domain / Domain controller
 FETCH

Filter by Group Name

SEARCH LDAP **CANCEL**



Example: Sample filters:

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

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

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

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

LDAP Group Search

 Active

Name
OracleNetAdmins

Description
Users who can register Network Service Alias in t

Group Membership attribute

uniqueMember

Account Naming attribute

uid

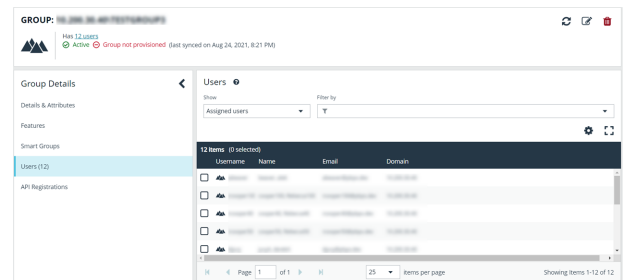
Base Distinguished Name

dc=,dc=

ADD GROUP

CANCEL

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



GROUP: OracleNetAdmins
 Active Group not provisioned (last synced on Aug 24, 2021, 8:21 PM)

Group Details

Users (12)

Username	Name	Email	Domain
...
...
...
...
...
...
...
...
...
...
...

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 39](#).

i For more information on creating and editing directory credentials, please see ["Create and Edit Directory Credentials" on page 19](#).

Assign Group Permissions

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

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

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

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



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

Assign Features Permissions






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


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

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

Feature	Provides Permissions To:
Analytics & Reporting	Log in to the console and access Analytics & Reporting to generate and subscribe to reports.
Appliance (U-Series) Access	Grant access to manage the U-Series Appliance as a BeyondInsight user.
Asset Management	Create Smart Rules. Edit and delete buttons on the Asset Details window. Create Active Directory queries. Create address groups.
Attribute Management	Add, rename, and delete attributes when managing user groups.
Credential Management	Add and change credentials when running scans and deploying policies.
Directory Credential Management	Grant access to the configuration area where directory credentials are managed. This feature must be enabled to support access to directory queries as well.
Directory Query Management	Grant access to the configuration area where directory queries are managed.
	 Note: Access to <i>Directory Credential Management</i> must also be granted.
Domain Management	Grants the user permission to configure mappings of bind credentials to domains for account resolution.
Endpoint Privilege Management	Grant access to the Endpoint Privilege Management features, excluding Policy Editor and Reporting.
Endpoint Privilege Management Policy Editor	Grant access to the Endpoint Privilege Management Policy Editor feature.
Endpoint Privilege Management Reporting	Grant access to the Endpoint Privilege Management Reporting feature.
Endpoint Privilege Management for Unix & Linux	Grant access to the Endpoint Privilege Management for Unix & Linux features.
File Integrity Monitoring	Work with File Integrity rules.
License Reporting	View the Licensing folder in Analytics & Reporting (MSP reports, Privilege Management for Windows, Privilege Management for Mac true-up reports, and Assets Scanned report).

Feature	Provides Permissions To:
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.
Password Safe Account Management	Grant read or write permissions to the following features on the Managed Accounts page and through the public API: <ul style="list-style-type: none"> • Bulk delete accounts • Add accounts to a Quick Group • Remove accounts from a Quick Group • Add, edit, and delete accounts
Password Safe Admin Session	Password Safe web portal admin sessions.
Password Safe Admin Session Reviewer	Grant a user admin session reviewer permissions only.
Password Safe Global API Quarantine	Access to the Quarantine APIs.
Password Safe Bulk Password Change	Change more than one password at a time.
Password Safe Agent Management	Grant a user administrator permissions to the Configuration > Privileged Access Management Agents page.
Password Safe Configuration Management	Grant a user administrator permissions to the Configuration > Privileged Access Management page.
Password Safe Domain Management	Check the Read and Write boxes to permit users to manage domains.
Password Safe Policy Management	Grant a user administrator permissions to the Configuration > Privileged Access Management Policies page.
Password Safe Role Management	Allows a user to manage roles, provided they have the following permissions: Password Safe Role Management and User Account Management .
Password Safe System Management	Read and write managed systems through the public API.
Password Safe Ticket System Management	This feature is not presently used.
Reports Management	Run scans, create reports, and create report categories.
Scan - Job Management	Activate Scan and Start Scan buttons. Activate Abort , Resume , Pause , and Delete on the Job Details page.

Feature	Provides Permissions To:
Scan - Report Delivery	Allow a user to set report delivery options when running a scan: <ul style="list-style-type: none"> • Export Type • Notify when complete • Email report to • Include scan metrics in email (only available for All Audits Scan)
Scan Management	Delete, edit, duplicate, and rename reports on the Manage Report Templates page. Activate New Report and New Report Category . Activate the Update button on the Edit Scan Settings view.
Secrets Safe	Provides access to Secrets Safe for all members of the selected group.
Session Monitoring	Use the session monitoring features.
Smart Rule Management – Asset	Grants permission to view, create, and edit asset Smart Rules; editing is limited to Smart Rules that are enabled for groups the user is a member of. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note: Newly created Smart Rules created by a non-administrator are automatically enabled with read permissions for all groups that the user is a member of, and with full permissions for all groups that the user is a member of AND has the Asset Management permissions for. For more information, see "Use Smart Rules to Organize Assets" on page 69.</p> </div>
Smart Rule Management – Managed Account	Grants permission to view, create, and edit managed account Smart Rules; editing is limited to smart rules that are enabled for groups the user is a member of. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note: Newly created Smart Rules created by a non-administrator are automatically enabled with read permissions for all groups that the user is a member of, and with full permissions for all groups that the user is a member of AND has the Asset Management permissions for. For more information, see "Use Smart Rules to Organize Assets" on page 69.</p> </div>
Smart Rule Management – Managed System	Grants permission to view, create, and edit managed system Smart Rules; editing is limited to smart rules that are enabled for groups the user is a member of. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note: Newly created Smart Rules created by a non-administrator are automatically enabled with read permissions for all groups that the user is a member of, and with full permissions for all groups that the user is a member of AND has the Asset Management permissions for. For more information, see "Use Smart Rules to Organize Assets" on page 69.</p> </div>

Feature	Provides Permissions To:
Smart Rule Management – Policy User	<p>Grants permission to view, create, and edit policy user Smart Rules; editing is limited to smart rules that are enabled for groups the user is a member of.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note: Newly created Smart Rules created by a non-administrator are automatically enabled with read permissions for all groups that the user is a member of, and with full permissions for all groups that the user is a member of AND has the Asset Management permissions for. For more information, see "Use Smart Rules to Organize Assets" on page 69.</p> </div>
Ticket System	View and use the ticket system.
Ticket System Management	Mark a ticket as inactive. The ticket no longer exists when Inactive is selected.
User Accounts Management	<p>Add, delete, or change user groups and user accounts.</p> <p>A minimum of read access to Directory Credential Management must also be granted to enable creation of AD and LDAP Groups.</p>
User Audits	View audit details for management console users on the User Audits page.
U-Series Appliance Administrator	Provides access to manage all aspects of the U-Series Appliance.
U-Series Appliance Backups	Provides access to manage the Backup and Restore options of the U-Series Appliance.
U-Series Appliance High Availability	Provides access to manage the High Availability features of the U-Series Appliance.
U-Series Appliance Login	Provides access to manage the U-Series Appliance as a BeyondInsight user.
U-Series Appliance Manage RDP	Provides access to manage Remote Desktop Protocol to the U-Series Appliance.
U-Series Appliance Patching	Provides access to manage updates to the U-Series Appliance.



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

Features Permissions Required for Configuration Options

Configuration Option	Feature and Permission
Active Directory Queries	Asset Management - Full Control.
Address Groups	Asset Management - Full Control.
Attributes	Asset Management - Full Control.
Connectors	Asset Management and Management Console Access - Full Control.
Password Safe Connections	Member of the Built-In Administrators group.
Endpoint Privilege Management Module	Management Console Access and Endpoint Privilege Management - Full Control.
Scan Options	Scan Management - Full Control.
Services	Member of the Built-In Administrators group.

Configuration Option	Feature and Permission
User Audits	User Audits - Full Control.
User Management	Everyone can access. Users without the Full Control permission to User Account Management feature can edit only their user record.
Workgroups	User Accounts Management - Full Control.

Assign Smart Groups Permissions

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

Edit and Delete Groups

The below sections detail how to make basic edits to the settings and options of BeyondInsight local groups, Active Directory groups, Azure Active Directory groups, and LDAP groups using the **Edit Group** functionality, as well as how to update more advanced group details such as assigning permissions, updating group members, and managing API registrations.

Edit Basic Group Details

Administrators can edit the following basic details for groups in BeyondInsight:

BeyondInsight Local Groups

- For BeyondInsight local groups, administrators can update the following:
 - Deactivate or activate a group by enabling or disabling the **Active** status.
 - Modify the **Group Name**.
 - Modify the **Description**.

Active Directory Groups

For Active Directory groups, administrators can update the following:

- Deactivate or activate a group by enabling or disabling the **Active** status.
- Change the credential used to query the group in Active Directory.
- Select a new domain or domain controller used for accessing the group in Active Directory.
- Enable or disable the option to propagate domain changes to all members of the group.
- Select **Sync Schedule Options** to control how the user accounts in this group are automatically synchronized on a periodic schedule. The following options are available:
 - **Global**: This is the default setting which uses the schedule settings specified in the **Active Directory Group Synchronization** configuration section.
 - **Custom**: Select **Custom** to ignore the global synchronization schedule and specify a unique synchronization schedule for this group instead.
 - **No Custom or Global**: Select this option to omit this group from any automatic synchronization. The group can still be synchronized manually.

Azure Active Directory Groups

- For Azure Active Directory groups, administrators can update the following:
 - Deactivate or activate a group by enabling or disabling the **Active** status.

LDAP Groups

- For LDAP groups, administrators can update the following:
 - Deactivate or activate a group by enabling or disabling the **Active** status.
 - Change the credential used to query the group in LDAP.
 - Select a new **Group Membership attribute** from the list. The following options are available:
 - **member**
 - **uniqueMember** (default)
 - **memberUID**
 - Select a new **Account Naming attribute** from the list. The following options are available:
 - **mail**
 - **cn**
 - **sAMAccountName**
 - **uid**
 - **userPrincipalName**
 - Edit the **Base Distinguished Name**.

To edit a group in BeyondInsight:

1. Navigate to **Configuration > Role Based Access > User Management > Users**.
2. Optionally, filter the list of groups in the grid by **Type**, **Name**, **Description**, **Last Synchronization Date**, or **Synchronization Settings**.
3. Click the vertical ellipsis for the group, and then select **Edit Group**.
4. In the **Edit Group** pane, update the details as required, and then click **Save Changes**.



For more information on configuring Active Directory Group Synchronization settings, please see ["Configure Active Directory Group Synchronization" on page 31](#).

Edit Advanced Group Details

Administrators can edit the following advanced details for groups:

- Update the group permissions for specific BeyondInsight and Password Safe features.
- Update the group permissions for specific Smart Groups.
- Edit Password Safe roles for Smart Groups
- Add and remove users from local groups.
- Manually synchronize group users for Active Directory and LDAP groups.
- Enable and disable API Registrations for the group.

Follow these steps to access advanced details for a group:

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

2. Optionally, filter the list of groups in the grid by **Type**, **Name**, **Description**, **Last Synchronization Date**, or **Synchronization Settings**.
3. Click the vertical ellipsis for the group, and then select **View Group Details**.
4. From the **Group Details** pane, you can select **Features**, **Smart Groups**, **Users**, and **API Registrations** to make updates for the group. Specific updates you can make for each of these options are detailed in the below sections.

Update Group Permissions for Features

Permissions provide the members of the group access to BeyondInsight system components and Password Safe features. Assign permissions to groups for specific features, as follows:

1. From the **Group Details** pane, click **Features**.
2. From the **Features** grid, select the feature.
3. Click **Assign Permissions** above the grid.
4. Click **Assign Permissions Read Only**, **Assign Permissions Full Control**, or **Disable Permissions**.

Update Group Permissions for Smart Groups

Assign permissions to groups to provide members of the group access to smart groups as follows:

1. From the **Group Details** pane, click **Smart Groups**.
2. From the **Smart Groups** grid, select the Smart Group.
3. Click **Assign Permissions** above the grid.
4. Click **Assign Permissions Read Only**, **Assign Permissions Full Control**, or **Disable Permissions**.

Edit Password Safe Roles for Smart Groups

Password Safe roles define the actions users can take when using the Password Safe web portal for password releases or access to applications. Assign Password Safe roles to groups as follows:

1. From the **Group Details** pane, click **Smart Groups**.
2. From the **Smart Groups** grid, click the vertical ellipsis for the Smart Group.
3. Select **Edit Password Safe Roles**.
4. Check or uncheck each role, as required.
5. Click **Save Roles**.

Add Users to Local BeyondInsight Groups

Manually add users to local groups in BeyondInsight as follows:

1. From the **Group Details** pane, click **Users**.
2. Filter the **Users** grid to show users not assigned.
3. Select the user or users, and then click **Assign User** above the grid.

Sync Group Users for Active Directory and LDAP Groups

To ensure your AD and LDAP groups contain the most recent group members, you can manually synchronize with AD and LDAP to retrieve the group's users. There are two methods for manually synchronizing group users, as follows:

- From the group header, above the **Group Details** pane, click the **Sync group users** icon.
- From the **User Management** page, click the vertical ellipsis for the group and select **Sync group users**.

Manage Group API Registrations

API Registrations provide a way to integrate part of the BeyondInsight and Password Safe functionality into your applications using an API key. Manage API registrations for groups as follows:

1. From the **Group Details** pane, click **API Registrations**.
2. Check or uncheck the API registrations to enable or disable them for this group or click **Select All** to enable all of them. Changes are automatically saved.



Tip: Use the filter above the list to narrow down the list of API registrations or to quickly find a specific registration by its name. If you need to create a new API registration, click the **Manage API Registrations** link above the filter box to go to the **API Registrations** page where you can create a new one.



For more detailed information on features permissions, Password Safe roles, and API registrations, please see the following:

- ["Assign Group Permissions" on page 39](#)
- [Configure API Registration](#)
- [Password Safe Roles](#)

Delete a Group



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



Unable to delete group, as it contains secrets which must first be removed.

[Dismiss](#)

Administrators can delete groups as follows:

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

Create and Manage User Accounts

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

You can also add application users, which are used to represent applications that interface with the public API. Application users cannot log in to the BeyondInsight console. They can only authenticate and interact with the public API.



Note: A user account must be a member of a BeyondInsight user group because permissions to features are assigned at the group level. If a user is not a member of any groups in BeyondInsight, the user cannot log in to the console, and application users cannot authenticate with the public API.

Create a BeyondInsight Local User Account

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

- Provide a **First Name**, **Last Name**, **Email**, and **Username** for the new user. These fields are required.



Note: You may use an email address for the username.

- Provide a password and confirm it.



Note: The password must meet the complexity requirements as defined by your default password policy, defined at **Configuration > Role Based Access > Password Policy**.

- Optionally, enter the user's contact information.
- Select an **Activation Date** and an **Expiration Date** for the user account.



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

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

Create New User ➤

Identification

First Name

Last Name

Email

Username

New Password Show

Confirm New Password Show

Contact Information

Work Phone

Home Phone

Mobile Phone

User Status

Activation Date

Expiration Date

User Active

Account Locked

Account Quarantined

Authentication Options ?

Override Smart Card User Principal Name

Disable Forms Login

Two-Factor Authentication

Create User Discard

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



Note: The user must belong to at least one group

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

Update Default Password Policy for Local Users

The default password policy defines the password complexity requirements for local BeyondInsight users. This includes the minimum and maximum length of the password and the type of characters required and permitted in the password. Update the default password policy as follows:

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

Default Password Policy Details

Password Policy Name
7 characters remaining.

Description (Optional)

Minimum length

Maximum length

Uppercase Characters
 Permit uppercase characters
 Minimum number of required uppercase characters

Allow only the following uppercase characters

Lowercase Characters
 Permit lowercase characters
 Minimum number of required lowercase characters

Allow only the following lowercase characters

Numeric Characters
 Permit numeric characters
 Minimum number of required numeric characters

Allow only the following numeric characters

Non-Alphanumeric Characters
 Permit non-alphanumeric characters
 Minimum number of required non-alphanumeric characters

Allow only the following non-alphanumeric characters

Add an Active Directory User

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



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

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



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

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



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



Example: Sample filters:

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

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

Add an Azure Active Directory User

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

Active Directory User Search

➔

Credential

▼

[Create New Credential...](#)

Domain

✖

Filter by Name

*
✖

SEARCH ACTIVE DIRECTORY

CANCEL



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

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



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



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



Example: Sample filters:

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

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

Azure Active Directory User Search ➔

Credential [Create New Credential...](#)

Filter by Name

* ✖

SEARCH AZURE ACTIVE DIRECTORY
CANCEL

Change the Preferred Domain Controller for Active Directory User Accounts

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

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



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

Edit User
➤

[View User Details...](#)

First Name

Last Name

Email

Username

Account Quarantined

Credential

[Create New Credential...](#)

Domain / Domain controller
 ▼ Fetch

Authentication Options ?

Override Smart Card User Principal Name

Disable Forms Login

Two-Factor Authentication

Update User
Discard

Add an LDAP User

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

5. Select a credential from the list.



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

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

LDAP User Search ➔

Search for LDAP users to give access to the system.

Credential

▼

[Create New Credential...](#)

Server

Domain / Domain controller

▼
FETCH

Object class

Name attribute search

Filter by null

SEARCH LDAP
CANCEL

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

Add an Application User

Application users represent applications that interface with the BeyondInsight public API. Application users cannot log in to the BeyondInsight console. They can only authenticate and interact with the public API, using Client ID and Client Secret for credentials within the OAuth client credential flow.

An API Registration type of API Access Policy must be assigned to an application user, and is used for processing IP rules. To create an application user:

1. Go to **Configuration > Role Based Access > User Management > Users**.
2. Click **Create New User**.
3. Select **Add an Application User** from the dropdown list. The **Create New Application User** screen is displayed.
4. Add a username.
5. Under **API Access Policy**, select the policy.
6. Copy the information from the **Client ID** and **Client Secret** fields for later use.
7. Click **Create User**.

8. Assign the user to a group that has the required permissions to access BeyondInsight and Password Safe features.
 - Click the vertical ellipsis for the user, and then select **View User Details**.
 - From the **User Details** pane, click **Groups**.
 - Locate the group, select it, and click **Assign Group** above the grid.

Recycle the Client Secret for an Application User

When editing an application user, you have an option to recycle their secret. Once recycled, you can copy or view the new secret. When a secret is recycled and the user account is updated with this change, the previous client secret is no longer valid.

To recycle the secret for an application user:

1. Go to **Configuration > Role Based Access > User Management > Users**.
2. Locate the application user in the grid.
3. Click the ellipsis to the right of the user, and then select **Edit User Details**.
4. Click the **Recycle** icon to the right of the **Client Secret**.
5. Click **Recycle** on the confirmation message that displays.
6. Copy the new secret for later use.
7. Click **Update User**.

View and Update OAuth Secret Expiry

The user's secret will eventually expire. The **Users** grid has an **OAuth Secret Expiry** column, which you can use to view what is close to expiring. The default duration of a client secret is **365** days. You can adjust the lifetime of the secret from the **Authentication Options** configuration area in BeyondInsight. Updating this value only changes the secret expiry date for new application users and recycled client secrets. Older secrets cannot be updated.

To view the OAuth Secret Expiry for an application user:

1. Go to **Configuration > Role Based Access > User Management > Users**.
2. Locate the application user. The **OAuth Secret Expiry** column lists the date and time that a client secret for that user expires.

To update the duration for client secrets:

1. Go to **Configuration > Authentication Management > Authentication Options**.
2. Under **Application User Authentication Settings**, enter the new duration of the client secret in the **Client Secret Expiry** field.
3. Click **Update Application User Authentications Settings**.

Edit a User Account

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

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

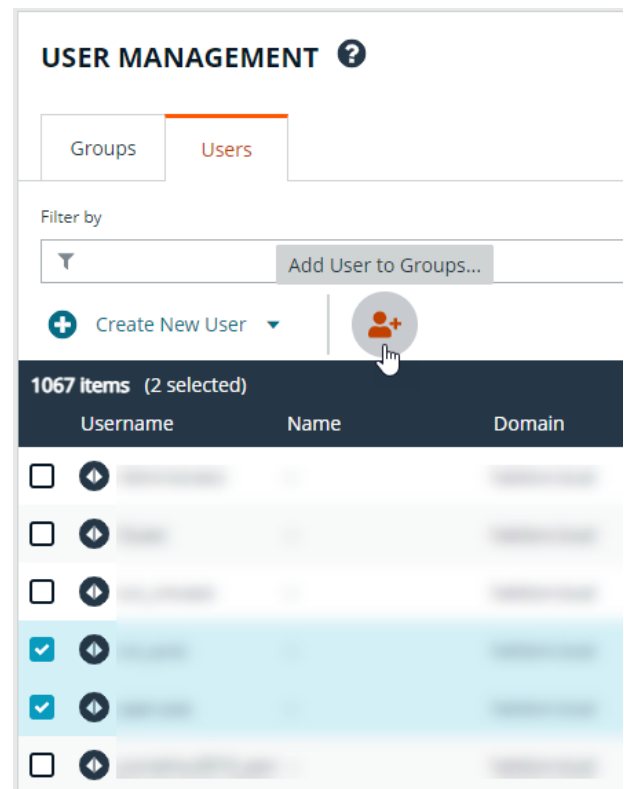
4. Select a user, click the vertical ellipsis button, and then select **Edit User Details**.
5. In the **Edit User** pane, update the details as required, and then click **Update User**.



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

Add User to Groups

1. From the **User Management** page, click the **Users** tab 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 multiple users, and then click the **Add User to Groups** button above the grid.




USER MANAGEMENT ?

Groups **Users**

Filter by

▼ Add User to Groups...

+ Create New User ▼ 

1067 items (2 selected)

	Username	Name	Domain
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input checked="" type="checkbox"/>			
<input checked="" type="checkbox"/>			
<input type="checkbox"/>			

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.

Add 2 Users To Groups ➤

Please enter three or more characters to begin searching against the Group Name or Description. If a group already contains all of the currently selected users, its result will display as checked. When one or more currently selected users are not part of a group, its result will display as unchecked. Check the box to assign all currently selected users to that group.

Search local groups

-  Administrators
-  mo-admin-reviewer
-  Non-Admin access to all
-  Unix BI Admins

Delete a User Account

Administrators can delete user accounts as follows:

1. Navigate to **Configuration > Role Based Access > User Management > Users**.
2. Click the **Users** tab to display the list of users in the grid.
3. Optionally, filter the list of users displayed in the grid using the **Filter by** dropdown.
4. For local accounts, select the user, click the **Delete** button above the grid, and then click **Delete** to confirm.
5. For directory accounts, select the user, click the vertical ellipsis, select **Delete User**, and then click **Delete** to confirm.



Note: For auditing purposes, if a user account is linked to any Password Safe session recordings, you cannot delete the account; however, you may disable the account.



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

Audit Console Users in BeyondInsight Cloud

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

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

To view user audit data:

1. Go to **Configuration > General > User Audits**.
2. User the filters above the grid to easily locate specific items listed. You can filter grid items by the following criteria:
 - Date the user took the action
 - Type of action taken
 - Which section of the application the action was taken
 - Username
 - IP Address
 - Key words of the item
 - Key words in the item details
3. Click the **i** icon for the item to view more specific details about the action taken.



Tip: You can export all of the data in the grid to a CSV file by clicking the **Download all** (downward arrow) button above the grid.



Note: User audits older than 120 days are purged from the database. Data retention for user audits is not configurable for BeyondInsight and Password Safe Cloud deployments.

Overview of BeyondInsight Tools

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

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

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

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

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



For more information, please see ["Change and Set the Console Display Preferences" on page 16.](#)

Create an Address Group

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

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



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



For more information, please see "[Create and Configure Groups](#)" on page 25.

Create an Always Address Group

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

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



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

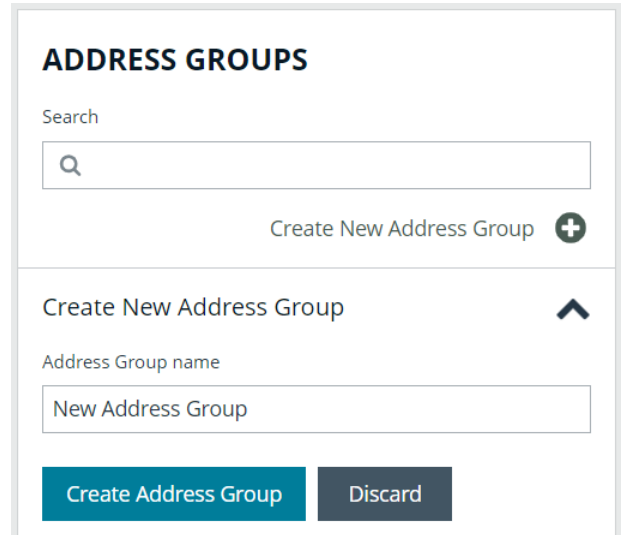
- The scan includes **10.10.10.60** since this IP address was added to the **Always** address group.
- The scan excludes **buffett-laptop** since this asset was explicitly omitted in the **Always** address group.
- **10.10.10.50** is scanned as usual.



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


1. Go to **Configuration > Discovery Management > Address Groups**.


2. Click **Create New Address Group**.
3. Enter a name for the address group, and then click **Create Address Group**.



ADDRESS GROUPS

Search

Create New Address Group 

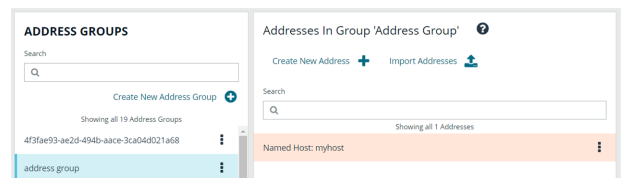
Create New Address Group 

Address Group name

New Address Group


Create Address Group **Discard**

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






ADDRESS GROUPS



Search

Create New Address Group 

Showing all 19 Address Groups


4f3fae93-ae2d-494b-aace-3ca04d021a68	
address group	

Addresses In Group 'Address Group' 

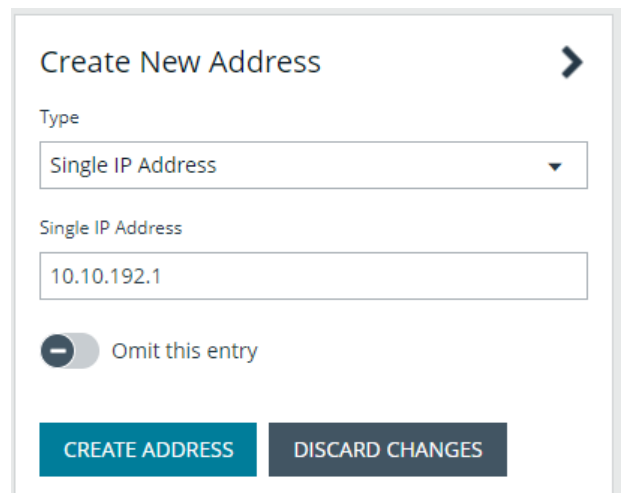
Create New Address  Import Addresses 


Search

Showing all 1 Address

Named Host: myhost	
--------------------	--

5. 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

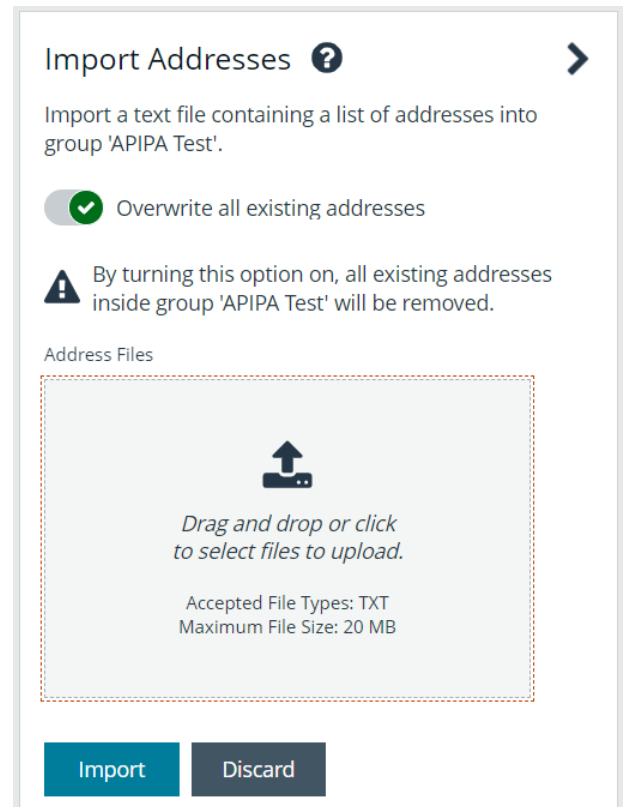
CREATE ADDRESS **DISCARD CHANGES**

6. If importing the addresses:

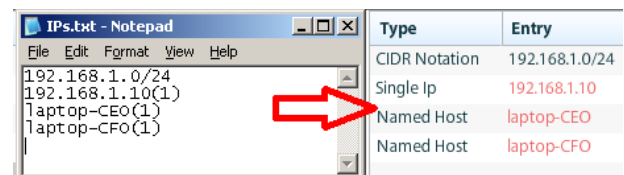
- Enable the **Overwrite all existing addresses** option, if desired.
- Click **Drop File** to upload the import file.
- Click **Upload File**.



Note: 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)**.



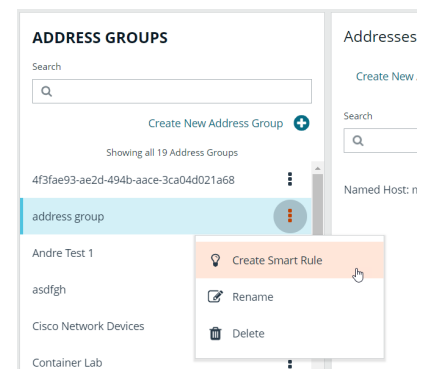
The image shows an example of how a CIDR Notation, an excluded IP address, and excluded named hosts are displayed after importing.



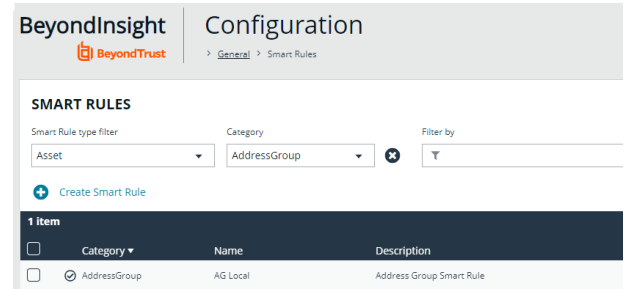
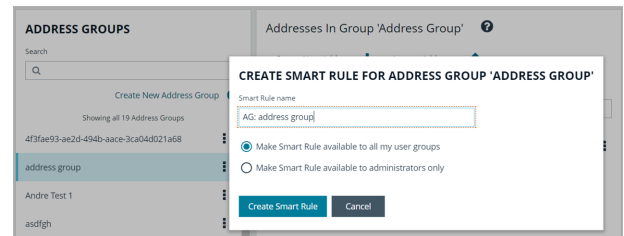
Create a Smart Rule Based on an Address Group

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

1. From the **Address Groups** pane, click the vertical ellipsis for the address group.
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 the option to make the Smart Rule available to administrators only.
5. Click **Create Smart Rule**.
6. A message stating *Smart Rule has been created for this Address Group* appears.
7. The group is displayed on the **Configuration > Smart Rules** page.



Create a Directory Query

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

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

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



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

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



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

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



For more information, please see the following:

- ["Create and Configure Groups" on page 25](#)
- ["Create and Edit Directory Credentials" on page 19](#)

Attributes and Attribute Types in BeyondInsight

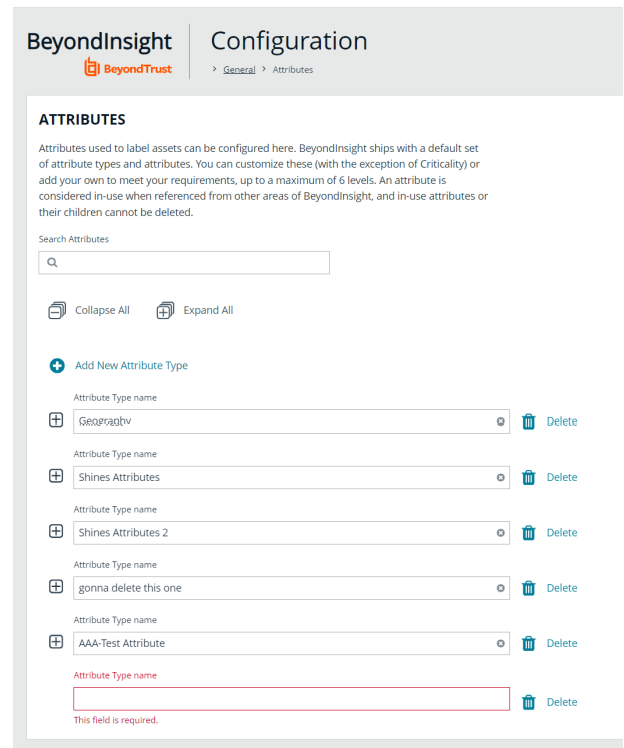
Attributes can be used to label assets, and you can set attributes for each asset in a group using a Smart Rule. BeyondInsight ships with a default set of attributes that can be customized, except for the **Criticality** type, and you can also add new attribute types and attributes to meet your requirements.



For more information, please see "[Use Smart Rules to Organize Assets](#)" on page 69.

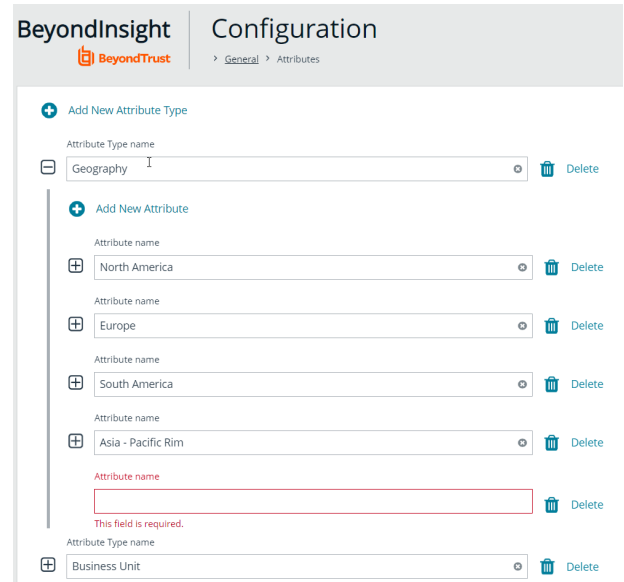
Add a New Attribute Type

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**.



The screenshot shows the 'BeyondTrust Configuration' interface. The breadcrumb trail is 'General > Attributes'. There are two main sections:

- Add New Attribute Type:** This section has a header with a plus sign and the text 'Add New Attribute Type'. Below it is a form with the label 'Attribute Type name' and a text input field containing 'Geography'. To the right of the input field is a trash icon and the text 'Delete'.
- Add New Attribute:** This section has a header with a plus sign and the text 'Add New Attribute'. It contains a list of attributes, each with a plus sign icon, a text input field for the 'Attribute name', and a trash icon with 'Delete' text to its right. The listed attributes are: 'North America', 'Europe', 'South America', and 'Asia - Pacific Rim'. Below these is an empty text input field with a red border and the text 'Attribute name' above it. Below the empty field is the text 'This field is required.' At the bottom of this section is another plus sign icon and a text input field containing 'Business Unit', with a trash icon and 'Delete' text to its right.

Use Smart Rules to Organize Assets

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



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

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

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

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

- Run Discovery Scans
- Monitor and view assets

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

Use Smart Rule Filters and Smart Groups

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

Selection Criteria

Include Items that match **ALL** ▼ of the following

Address Group

Address Group

and

Asset fields


Assets With Open Tickets

Assigned Attributes


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.


Selection Criteria 

Include Items that match **ALL** ▼ of the following

Asset fields 


Domain Name

equals (=)

EMEA 


and

Include Items that match **ANY** ▼ of the following [remove group](#)

Asset fields 


Kind

equals (=)

Server 


or

Include Items that match **ALL** ▼ of the following [remove group](#)

Asset fields 

Asset Name

equals (=)

Workstation 

[Add another condition](#) [Add a new group](#)

Smart Rule Filters

Asset Smart Rule Filters

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

	You can include more than one asset field filter in the Smart Rule to refine the results.
Assets with Open Tickets	For ticket tracking, create a Smart Rule that filters on open tickets. The Smart Rule filter can be set to include overdue tickets.
Assigned Attributes	<p>Create a filter based on an attribute.</p> <p>If the attribute is unassigned on a particular asset, you can choose to include or exclude the asset from the rule.</p>
Child Smart Rule	<p>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.</p> <p>Reusing a Smart Rule further refines the assets that will be a part of the Smart Rule.</p>
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	<p>Filter on any combination of OS. Operating systems included in the list are those detected in your network.</p> <p>Assets with no OS detected, can be included or excluded from the rule.</p>
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, Application , Security , or System .
Workgroup	Filter by workgroup.



For more information, please see the following:

- ["Create an Address Group" on page 62](#)
- ["Create a Directory Query" on page 66](#)

Predefined Smart Group Categories

Agents and Scanners	Detects assets where BeyondInsight scanners are deployed.
Assets and Devices	Includes default Smart Groups for all assets and all assets labeled as workstations.
Intelligent Alerts	Includes Smart Groups that detect assets added since the previous day, and mobile assets with critical vulnerabilities. Intelligent Alerts are inactive by default.
Servers	Includes Smart Groups that detect mail server, web server, database server, domain controller, and SCADA assets. Only the Web Servers Smart Group is marked as active.
Virtualized Devices	<p>Includes Smart Groups for virtual environments, including Microsoft Hyper-V and Parallels. Assets detected as virtual environments belong to these Smart Groups.</p> <p>This default category also includes two Smart Groups: Virtual Servers and Virtual Workstations. Assets that are servers or workstations might not be detected, and as a result, not be included in the Smart Group. For example, the asset might be a router or unknown, resulting in exclusion from the Smart Group.</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 BeyondInsight, click **Smart Rules**.
2. Leave **Asset** selected for the **Smart Rule type** filter.
3. Click **Create Smart Rule**.
4. Select a category.
5. Enter a name and description.
6. By default, the Smart Rule is set to **Active (yes)**, so it is always available for processing. Disable the active setting to ensure the rule is not processed.
7. Select the filters in the **Selection Criteria** section.
8. From the **Actions** section, select one of the following:

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



Tip: To view the contents of a new or edited Smart Rule, once it has been saved, click **View Results**. You are taken to the associated grid, where the contents of the Smart Rule are listed. If the Smart Rule is actively processing when **View Results** is clicked, a banner displays letting you know it is still processing.



Note: The **View Results** button displays only if you have permissions to the grid corresponding to the Smart Rule, i.e. Assets, Managed Accounts, Managed Systems. It also displays only when **Show <entity> as Smart Group** is selected under **Actions**.

The Smart Rule must process to display the contents in the grid; therefore, we recommend viewing the results of a Smart Rule before adding additional actions that may make changes to accounts and assets in your network. Once you have viewed the results of the Smart Rule using only the **Show <entity> as Smart Group** action and you have confirmed it contains your desired items, you can add additional actions to the 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 created, or 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 and managed system Quick Group Smart Rules, because these only run once upon creation and cannot be triggered to run again.

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

Change the Processing Frequency for a Smart Rule

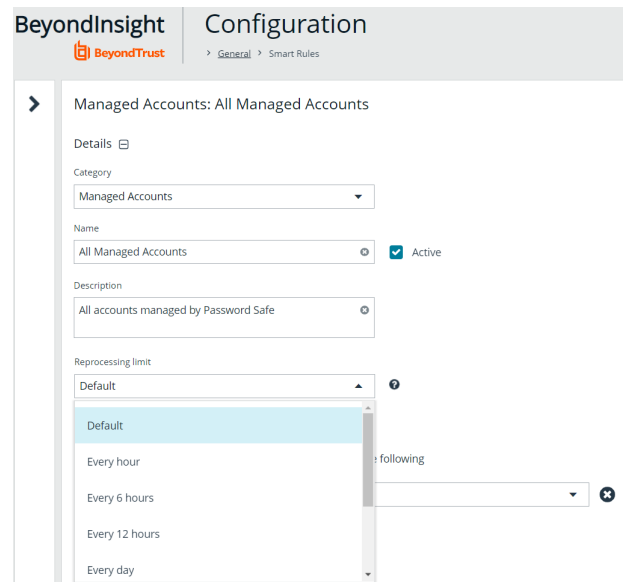
By default, Smart Rules process when asset changes are detected. The assets in the Smart Rule are then dynamically updated. For Smart Rules that require more intensive processing, you might want Smart Rules to process less frequently.

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

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



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

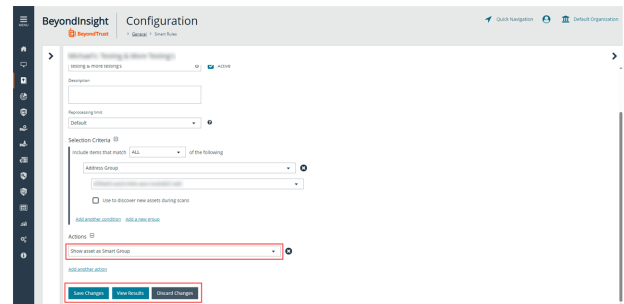


The screenshot shows the 'Configuration' page for 'Managed Accounts: All Managed Accounts'. The 'Reprocessing limit' dropdown is expanded, showing the following options: Default (selected), Every hour, Every 6 hours, Every 12 hours, and Every day. The 'Active' checkbox is checked. The 'Description' field contains 'All accounts managed by Password Safe'.

Perform Other Smart Rule Actions

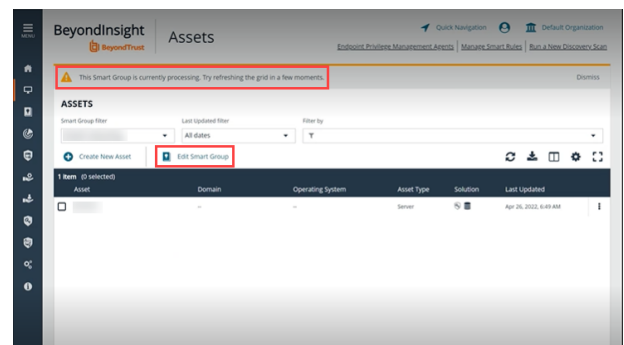
Edit a Smart Rule

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Click the vertical ellipsis to the right of the Smart Rule.
3. Select **Edit Smart Rule**.
4. Make the necessary changes and then click **Save Changes** or **Discard Changes**.
5. To view the contents of an edited Smart Rule once it has been saved and processed, click **View Results** to take you to the associated grid.



Note: The **View Results** button displays only if you have permissions to the grid corresponding to the Smart Rule, i.e. Assets, Managed Accounts, Managed Systems. It also displays only when **Show <entity> as Smart Group** is selected under **Actions**.

6. If the Smart Rule is actively processing when **View Results** is clicked, a banner displays to let the user know it is still processing.
7. To return to the Smart Rule editor, click **Edit Smart Group**.



Clone a Smart Rule

You can clone custom or predefined Smart Rules.

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



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

Deactivate a Smart Rule

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



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

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

To deactivate a Smart Rule:

1. From the left menu in BeyondInsight, 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 BeyondInsight, click **Smart Rules**.
2. Select one or more Smart Rules.
3. Click the Trash Can icon above the grid. You can also click the vertical ellipsis to the right of a single Smart Rule and select **Delete**.



Note: Built in Smart Rules cannot be deleted. These are identified by the Lock icon.



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

Audit Smart Rules

To audit new or edited Smart Rules:

1. Go to **Configuration > General > User Audits**.
2. Select **Section** from the **Filter by** dropdown.
3. Select **Smart Rule** from the **Section** dropdown.
4. Click the information icon to the right of the Smart Rule.
 - If a Smart Rule is added, the **Add Details** pane displays with all added information.
 - If a Smart Rule is edited, the **Edit Details** pane displays with all edited information.

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

Add Credentials to Use in Scans

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

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

To create a credential:

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



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

5. 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"> • Authentication Type • Domain (Optional) • Username • Password • Confirm password • Description • Port numbers • Key • Confirm key
MySQL	<ul style="list-style-type: none"> • Username • Password • Confirm password • Description • Port numbers • Key • Confirm key
Oracle	<ul style="list-style-type: none"> • Username

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

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



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



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

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

6. Click **Create New Credential**.



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

- ["Create SSH Credentials" on page 85](#)
- ["Create Oracle Credentials" on page 83](#)
- ["Create SNMP Credentials" on page 84](#)

Create Oracle Credentials

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

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



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

- **Port:** The default port is **1521**. Use the **+** and **-** buttons to change this if necessary.
8. Enter a key and confirm if those fields are available.



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

9. Click **Create Credential**.

Create New Credential

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

Provide a unique credential name for this credential. The credential name cannot contain any of the following characters [] \$ & < + ? > * | " : ; \ /

Credential Name

Type (optional)

Username

Password
 Show

Confirm password
 Show

Access level

Connect to

Database SID

Protocol

Host

Port
 - +

Create Credential Discard

Create SNMP Credentials

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

1. Navigate to **Configuration > Discovery Management > Credentials**.
2. Click **Create New Credential +**.
3. Enter a **Credential Name**.
4. From the **Type** list, select **SNMPv2**.
5. Enter a key and confirm it if those fields are available.



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

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

Create SSH Credentials

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



Note: DSA and RSA key formats are supported.

Optionally, when configuring SSH, you can select to elevate the credential. Using **sudo**, you can access scan targets that are not configured to allow root accounts to log on remotely. You can log on as a normal user and 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. Navigate to **Configuration > Discovery Management > Credentials**.
2. Click **Create New Credential +**.
3. Enter a **Credential Name**.
4. From the **Type** list, select **SSH**.
5. Enter a **Username**.
6. Select an **Authentication Type**:
 - **Password:** Enter a password and confirm it.
 - **SSH-DSS Key:** Upload a private key file. Enter key and confirm it if those fields are available.



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

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

Create New Credential

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

Provide a unique credential name for this credential. The credential name cannot contain any of the following characters [] ' \$ & < + ? > * | " : ; \ /


Credential Name

Type (optional)

Username

Authentication Type

Upload private key file



Drag and drop or click to select a file to upload.

All file types accepted.
Maximum File Size: 100 KB

Port numbers
Enter up to 250 ports separated by commas. (e.g. 80, 100, 44, 1433)

Key

Confirm key

Elevation

Run Discovery Scans

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



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

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

Use the Scan Wizard to Create a Discovery Scan

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



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

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

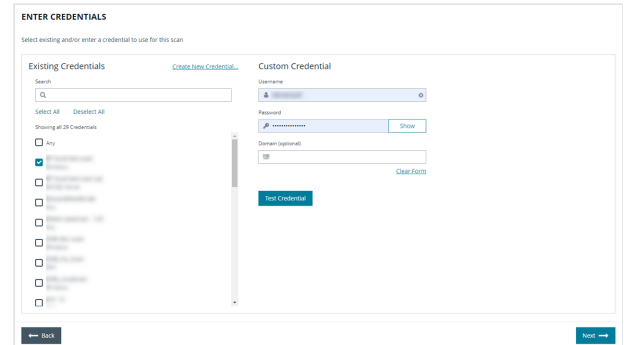


Note: *A warning banner appears at the top of the screen if your installation includes any Discovery Agents earlier than version 20.1. These must be updated by the end of 2021. You can identify outdated agents by referring to the grid of agents on this screen, which includes the version of each agent.*

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

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

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



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

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



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



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



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

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



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

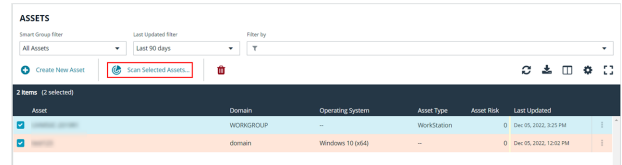
- Set a schedule, which can be **Immediate**, **One Time**, or **Recurring**.

8. Click **Finish** to complete the Scan Wizard.

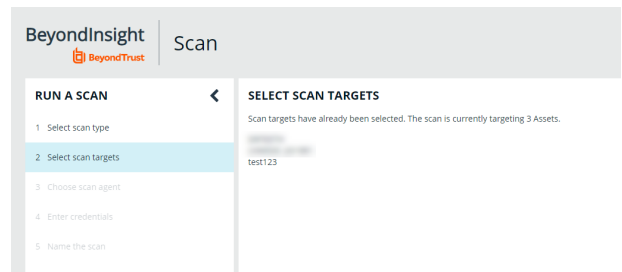
Run Scans from a List of Assets

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

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

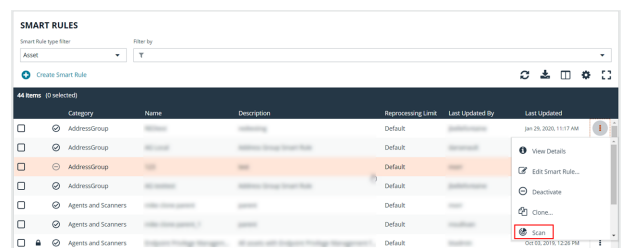


The Scan Wizard screen appears. Here you can select the type of scan to run. The difference is that when you click **Next** and go to the **Select Scan Targets** page, you will find the targets already selected. The next steps in the Scan Wizard are the same as those outlined above.



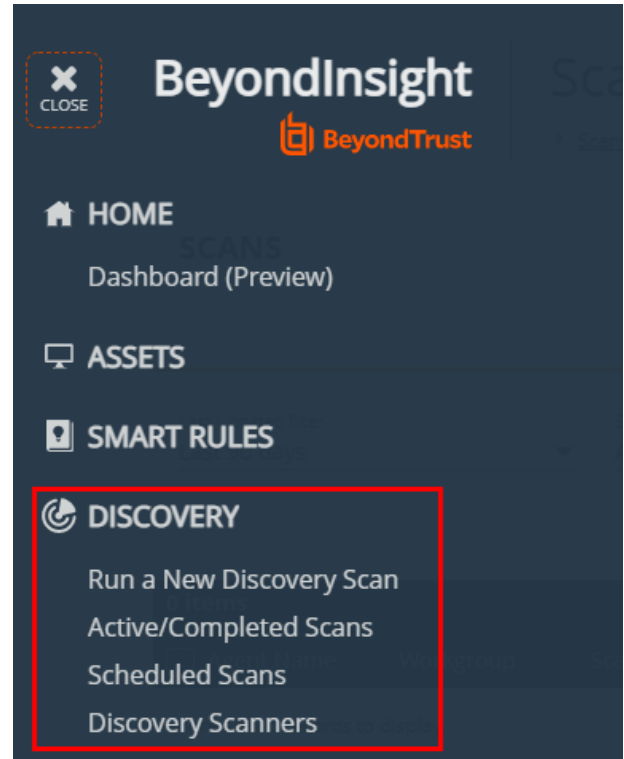
Use Smart Rules as Targets for Scans

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

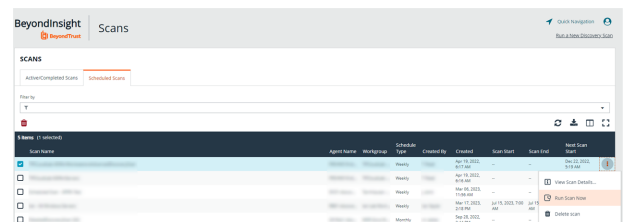


Check Completed and Scheduled Scans

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

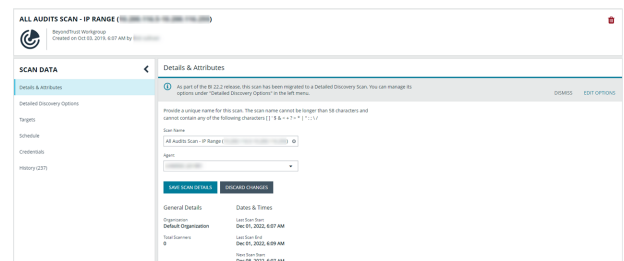


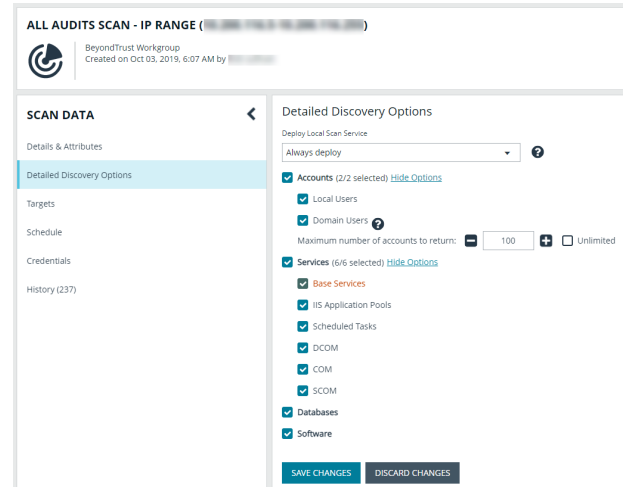
From the **Scans** page you can see active, completed, and scheduled scans, and you can delete a scan. You can also see the scan status for each active or completed scan. For each active and completed scan you can click the vertical ellipsis for the scan, and then select **Run Scan Now** or **Delete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



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

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





Discover Assets Using a Smart Group

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

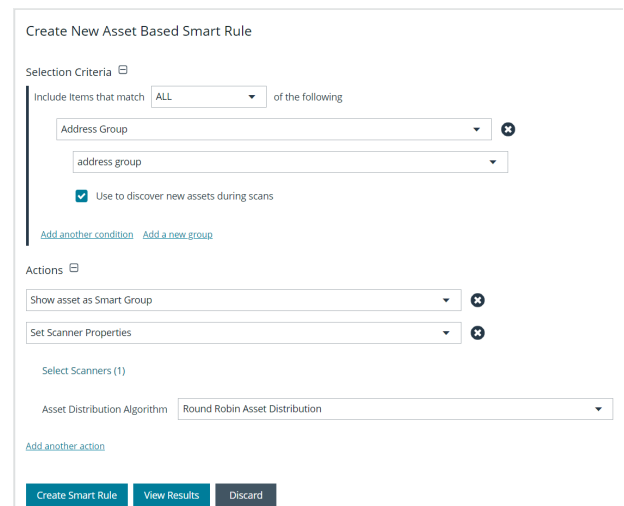


Tip: If you create an address group that includes the /19 CIDR block, the range possesses 8190 potential assets. The Discovery Scan always tries to discover those assets. Keep this in mind when you are reviewing scan results.

Key Steps

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

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





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



For more information, please see the following:

- ["Create a Directory Query" on page 66](#)
- ["Create an Address Group" on page 62](#)

Manage Scan Jobs

From the **Scans** page, you can perform the following:

- View active, completed, and scheduled scans
- Locate specific scans by using the date, status, agent name, workgroup, scan name, start time, and end time filters
- Use the row actions available from the vertical ellipsis menu for a scan to perform the following:
 - Open the discovery report for a completed scan
 - Stop active scans that are currently running
 - View and edit details for scheduled scans
 - Run completed and scheduled scans now

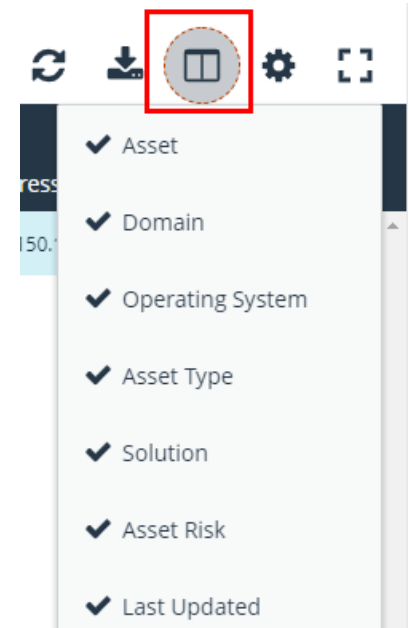
Manage Assets

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



Note: To maintain a manageable database size, asset details are purged every 30 days. We recommend running discovery scans at least every 30 days to refresh asset data.

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



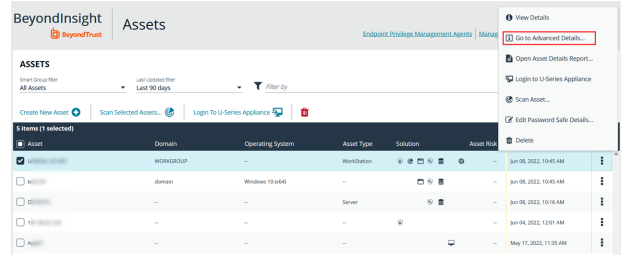
Review Asset Details



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

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

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



General Data

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



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

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

Scan Data



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

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

Create Assets Manually

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

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



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



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

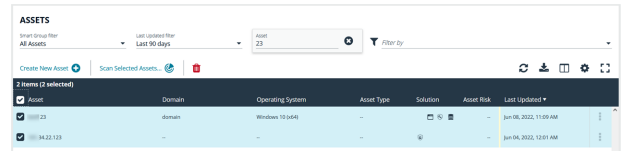
Delete Assets

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

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



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



Account	Domain	Operating System	Asset Type	Solution	Asset Risk	Last Updated
10.10.10.10	domain	Windows 10 (x64)	-	-	-	Jun 08, 2022, 11:00 AM
10.10.10.10	-	-	-	-	-	Jun 04, 2022, 10:01 AM

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



For more information on discovering assets using a discovery scan, please see: ["Run Discovery Scans" on page 86.](#)

Run Scans on Cloud Platforms in BeyondInsight

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

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

Amazon EC2 Requirements

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

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

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

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

Azure Requirements

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

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

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



For detailed instructions, please see [Create an Azure Active Directory Application](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**.

Configure a Cloud Connector

1. In the BeyondInsight console, go to **Configuration > General > Connectors**.
2. In the **Connectors** pane, click **Create New Connector**.
3. Provide a name for the connector, and then select a **Connector Type** from the list:
 - **AWS Scan Target Collector**
 - **Azure Scan Target Collector**
 - **Google Cloud Scan Target Collector**
 - **Hyper-V Scan Target Collector**
 - **Rackspace Scan Target Collector**
4. Click **Create Connector**.
5. Enter the connector information in the right pane:
 - For AWS cloud connections, required fields are: **Region**, **Access Key ID**, and **Secret Access Key ID**.
Instances associated with the region are displayed in the **Connection Test Results** section.
 - For Azure, required fields are: **Region**, **Client ID**, **Client Server**, **Tenant ID**, and **Subscription ID**.
 - For Google Cloud, required fields are **Server** (the region), **Project Name** (the project ID), and the **Key File**. Upload the key that you downloaded from the Google Cloud.
 - Hyper-V server, required fields are: **Server** (IP address), **Username**, and **Password**.
 - For Rackspace, required fields are **Account Type**, **Username**, and **API Key**.
6. After you configure the connector, click **Test Connector** to ensure the connector works.
7. Click **Create Connector**.

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

Cloud Connector Smart Groups

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

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

Configure BeyondInsight AWS Connector

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

Set up a Policy

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

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



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

Grant Access to a Third Party (Optional)



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

After you configure the AWS settings, you can create the AWS Scan Target Collector connector and Smart Group in the BeyondInsight console.



Note: When creating, editing, or viewing the connector, the **Cloud Scan Targets** grid only shows results immediately after a test is completed. The targets are not automatically loaded into the BeyondInsight UI each time the connector is viewed or edited.

Set BeyondInsight Options

Set 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**.

Set Account Password History

To set the account password history option:

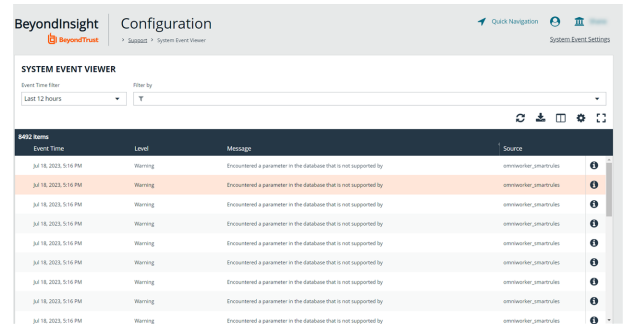
1. Select **Configuration**.
2. Under **Role Based Access**, select **Local Account Settings**.
3. Under **Account Password**, set the following options:
 - **Enforce Password History:** Enter the number of passwords a user must create before an old password can be reused. Enter **0** to not enforce 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**.

Configure the System Event Viewer

You can view recorded system events to assist with troubleshooting issues with BeyondInsight:

1. In BeyondInsight go to **Configuration > Support > 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.

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

Configure Global Website Options

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

- Changing the **Login** page to include lists of domains and LDAP servers
- Displaying the **Forgot Password** link on the **Login** page
- Displaying social media links on the **Login** and **About** pages
- Changing the refresh interval for Smart Rules
- Configuring a pre-login banner to appear to users before logging into the site
- Configuring session options
- Turning on language selection
- Enabling and disabling the requirement to provide an access key when creating, editing, or using discovery scan credentials.
- Creating a global access key to be used for all discovery scan credentials

List Domains and LDAP Servers on the Login Page

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



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



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

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

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

Disable Forgot Password Link

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

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

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

Disable Social Media links on the Login and About pages

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

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

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

Change the Refresh Interval for Smart Rules

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

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

Configure a Pre-Login Banner

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

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

Configure Session Options

You can configure the following session related options:

- Session timeout
 - Notification time before session timeout
 - Minimum interval between session extension requests
 - User Quarantine Cache refresh interval
1. Under **Session**, set the following:
 - **Session timeout:** Sets the amount of time for session inactivity before the session times out. Session timeout can be set between 2 and 60 minutes, with the default set at 20 minutes.
 - **Notification time before session timeout:** Sets the amount of time, prior to the session timing out due to inactivity, that the system notifies the user that their session will timeout shortly. This value must always be less than the session timeout value.
 - **Minimum interval between session extension requests:** Sets the number of minutes that pass between session extension requests. In general, this setting should always be set low and should always be less than the session timeout value. The only time you should change this from the default of three minutes is if there are a severely high number of simultaneous users and session refresh requests to the server causing high loads.
 - **User Quarantine Cache refresh interval:** Account Quarantine is a feature that can be set at the user account level that prevents a user from logging on the console or API and also terminates any active sessions immediately. It is a preventative measure taken when suspicious activity is detected. The User Quarantine Cache refresh interval sets the number of seconds that pass before the database is updated with the most recently discovered user accounts from the quarantine cache. The quarantine is only applied to the user account after the database is updated. The user can remain logged on and sessions remain active up until the refresh interval time passes, and the database is updated with a **Quarantine** status. The default value is **600** seconds. The maximum value is **1200** seconds.
 2. Click **Update Session Options**.

Enable Language Selection (Localization)

The management console can be viewed in the following languages:

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

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

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

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

Configure Global Discovery Credential Access Keys

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



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

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



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

Configure a Claims-Aware Website to Log In with SAML

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

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

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

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

Create a BeyondInsight Group

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

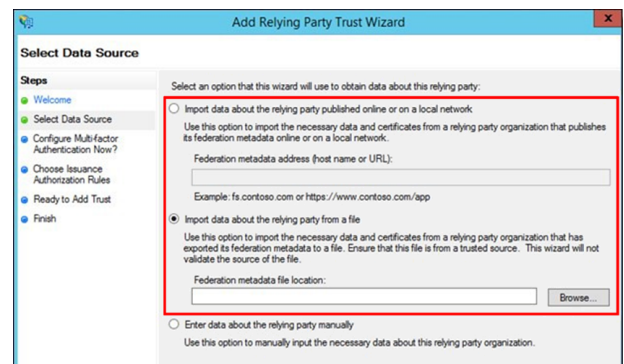
Add Relying Party Trust

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

The metadata is located in the following directory:

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

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



Set Up Claim Rules



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

Supported Federation Service Claim Types

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

Claims-Aware SAML

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

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

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

Disable Forms Login

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

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

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



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

Edit User
➤

[View User Details...](#)

First Name

Last Name

Email

Username

Account Quarantined

Credential

[Create New Credential...](#)

Domain / Domain controller

Fetch

Authentication Options ?

Override Smart Card User Principal Name

Disable Forms Login

Two-Factor Authentication

Two-factor Authentication is currently active for this account. Remove the device to deactivate TOTP.

Remove Device

Update User
Discard

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

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

FORMS LOGIN OPTIONS

Disable Forms Login should only be used in environments where SAML, Smart Card or Claims-aware is configured. Turning this option on will disallow users from using the standard login form in BeyondInsight.

Disable Forms Login for new directory accounts

Disable Forms Login for new local accounts

[Update Forms Login Options](#)

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=[unlqu3];
```

- **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**.