BeyondTrust

BeyondInsight
User Guide 6.10

TC:4/3/2020

Table of Contents

BeyondInsight User Guide

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

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

Components

Network Security Scanner

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

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

Protection Agent

The agent designed to protect your assets. The protection agent provides layers of protection, including virus and spyware, firewall, intrusion prevention, system protection, and vulnerability assessment.

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

Manager Service

This component is the BeyondInsight web interface.

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

Application Bus (AppBus)

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

Events Client

The Events Client is responsible for forwarding information gathered by the Network Security Scanner agent and protection agent.

The Events Client sends the information to the Manager Service. The Events Client is installed when a Network Security Scanner agent or protection agent is installed.

Events Client Certificate

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

For more information, please see the *BeyondInsight Installation Guide* at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/6-10/bi-install-6-10.pdf.

Central Policy Server

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

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

The same for the protection agent policies. The protection policy needs to know the policy to send to the selected protected assets. Policies are defined in the BeyondInsight management console, and when the policy is deployed, the Central Policy sends the job information to the agent to apply to the target asset.

Updater Enterprise

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

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

Third Party Patch Service

Gathers third party patches and makes them available for distribution using WSUS.

Scheduling Service

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

Shared Services Engine

Receives protection agent deployment details from the AppBus and sends those details to the assets where the protection agent is being deployed.

Log into the BeyondInsight Console

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

The following authentication types can be used:

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

For more information about configuring authentication, please see the BeyondInsight and Password Safe Authentication Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/6-10/bi-ps-authentication-guide-6-10.pdf.

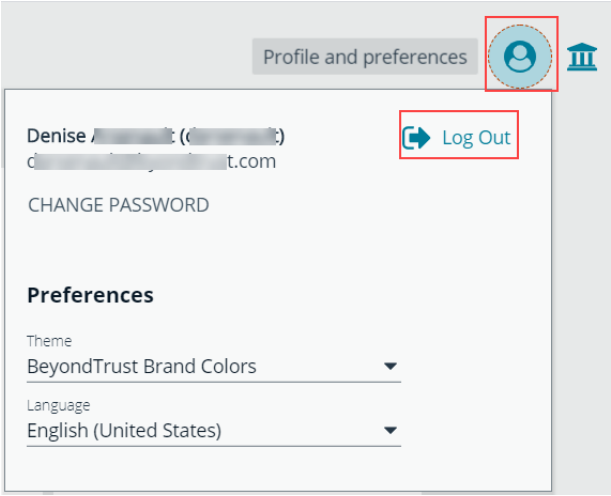
***Note:** When working in the console, the times displayed match the web browser on the local computer unless stated otherwise.*

1. Select **Start > All Programs > BeyondInsight > BeyondInsight > BeyondInsight Console**.
2. Optionally, open a browser, and enter the URL, **https://<servername>/WebConsole/index.html**
    - A pre-login banner message might be configured on your system. You must click **OK** before you can enter your credentials.
3. Enter your user name and password.
4. The default user name is **BTADMIN**, and the password is the administrator password you set in the **Configuration** wizard.
5. If applicable, select a domain.
6. Click **Login**.

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

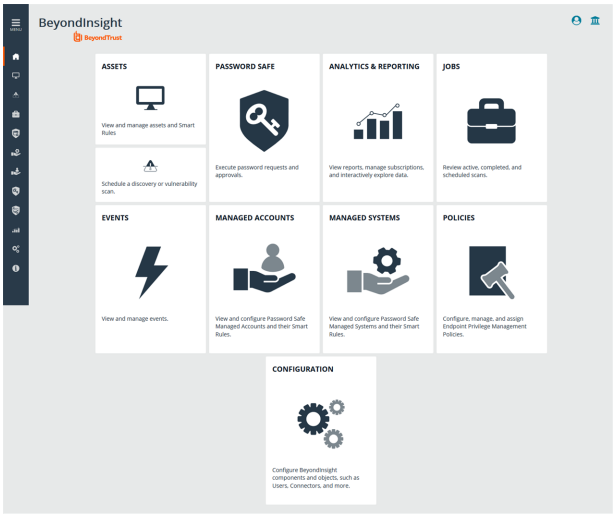
Log Out of the Console

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



Navigate the Console

When you log into the console, the cards displayed provide easy access to your suite of features. The cards displayed on the **Home** page vary depending on your license and the permissions assigned to your console account. Home page cards can include:



- **Assets:** View and manage assets and Smart Rules.
- **Scan:** Schedule discovery or vulnerability scans.
- **Password Safe:** Execute password requests and approvals.
- **Analytics and Reporting:** View reports, manage subscriptions, and interactively explore data.
- **Jobs:** Review active, completed, and scheduled scans.
- **Events:** View and manage events.
- **Managed Accounts:** View and configure Password Safe managed accounts and their associated Smart Rules.
- **Managed Systems:** View and configure Password Safe managed accounts and their associated Smart Rules.
- **Policies:** Configure, manage, and assign Endpoint Privilege Management policies.
- **Configuration:** Configure BeyondInsight components and objects, such as users and connectors.

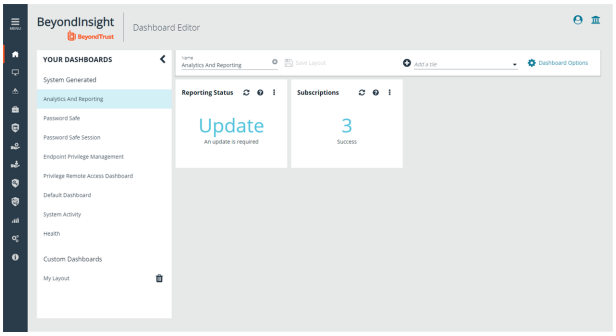
Optionally, click **Menu** in the left navigation pane to expand a complete list of the options available.

> ***Note:*** *Similar to the cards on the* ***Home*** *page, the menu items change depending on the license.*

Dynamic Dashboards

> ***Note:*** *Dynamic Dashboards a preview feature for BeyondInsight 6.10. Only admin access is supported at this time, and more features will be added in later releases.*

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

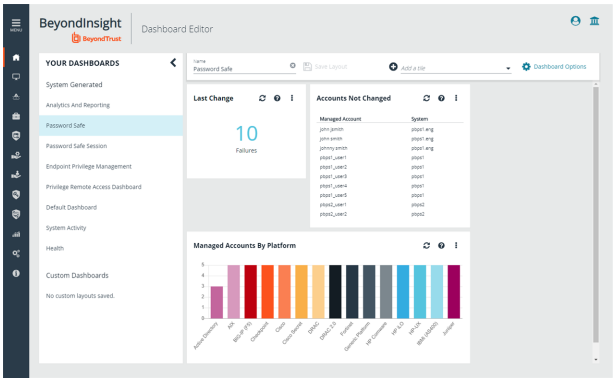


To access **Your Dashboards**, click **Menu > Dashboards**. A list of available dashboards displays on the left. BeyondInsight comes with several pre-built dashboard cards, including:

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

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

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

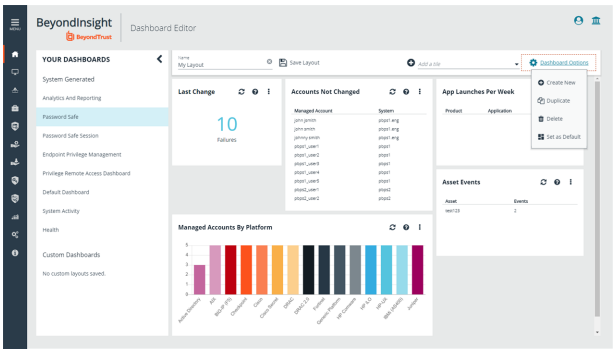


Click to refresh information displayed.

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

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

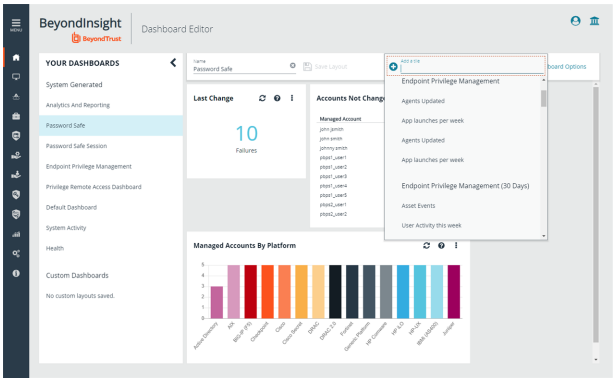
Use **Dashboard Options** to:



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

Customize a Dashboard

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

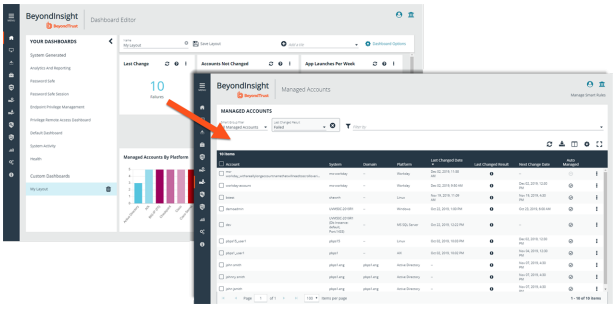


1. To create a custom dashboard, select one of the available dashboard cards. In this example we are using the **Password Safe** card. If necessary, delete any of the existing tiles that come installed with that card.
2. Click **Add a tile** and select the tiles you want from the drop-down menu. Resize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

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

Access Dashboard Tile Information

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



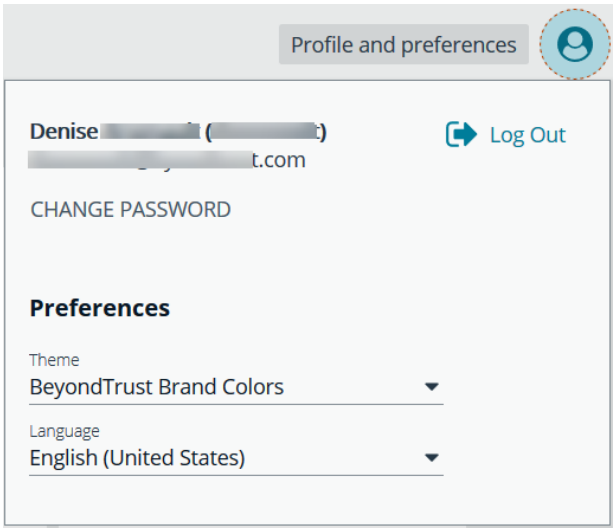
Change and Reset Login Passwords

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

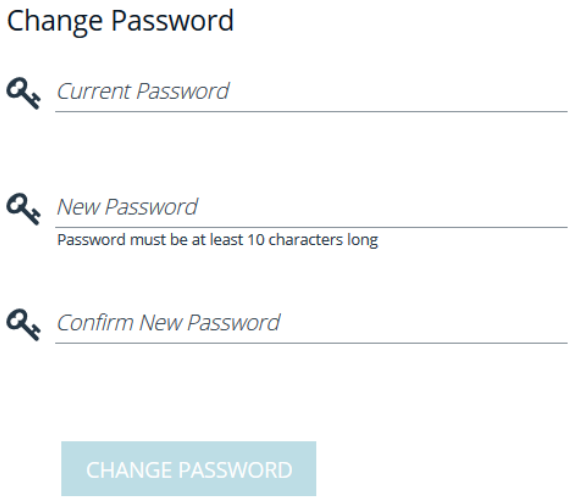
- You are logging in with Active Directory or LDAP credentials.
- Your account is currently locked out.

Change Password

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

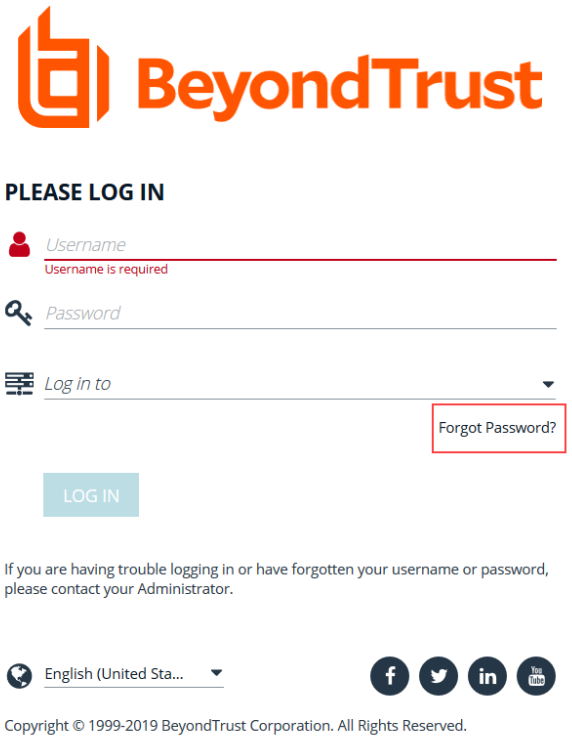


2. Change your password, and then click **Change Password**.



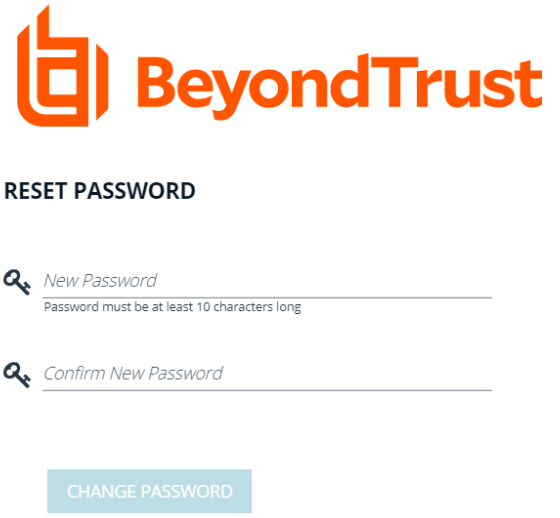
Reset Password

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



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

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



Change and Set the Console Display and Preferences

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

Set Display Preferences

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

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

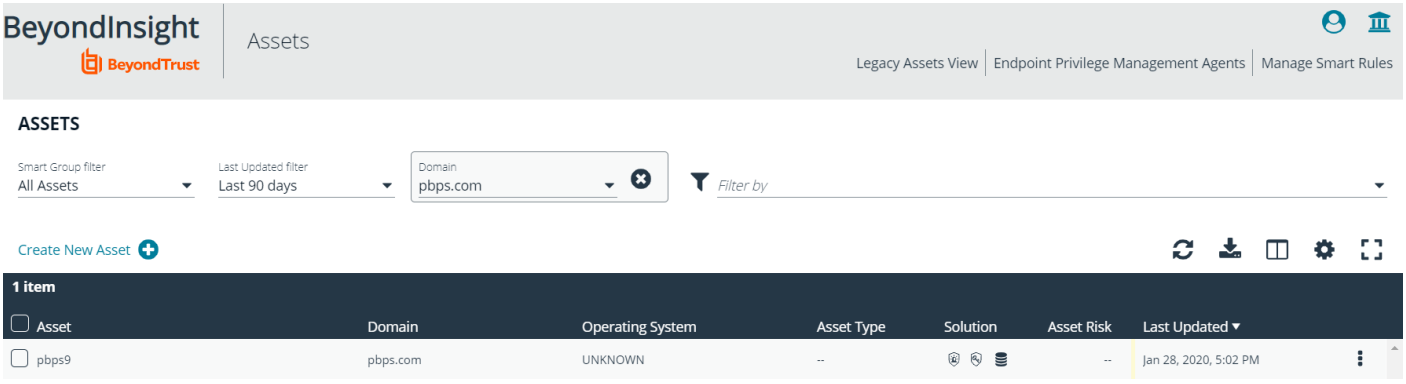
1. Select an area of the site, such as **Assets**.
2. Above the grid, you will see the following options and icons:

   - **Columns Chooser:** Select the columns to change the column headings and information displayed in the grid.
   - **Grid Configuration:** Choose the grid layout: **Compact**, **Default**, or **Expanded**.
3. The changes appear dynamically as they are selected.

Filter Records

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

1. Select an area of the site, such as **Assets**.
2. Above the grid, you will see filter options. The filter options available vary based on the page or grid selected. However, some consistent filtering options include:
   - **Smart Group filter:** Select to filter information by smart group association.
   - **Filter by:** Choose to filter the information by **Domain**, **Operating System**, **Workgroup**, etc. For each filter selected, enter the content you want to search for in the filter box's text field.
3. Apply as many filters as desired.
4. The information dynamically changes to match your selections. To remove a filter, click the **X** on the filter.



Customize Console Logos

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

Note: *The words "BeyondInsight" will still appear in the footer text on the* ***Login*** *page. This cannot be changed.*

After an upgrade, you will need to repeat these steps as the upgrade will overwrite the customized images and set them back to default.

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

- app-logo-default.svg (normal logo)
- app-logo-greyscale.svg (black and white version of the logo)
- app-logo-inverse.svg (negative of default or simply all white)

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

Role Based Access

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

BeyondInsight offers a role-based delegation model so that you can explicitly assign certain read and write permissions to groups based on their role. Creating groups gives you great flexibility in delegating access to assets and system components in BeyondInsight, using permissions and roles.

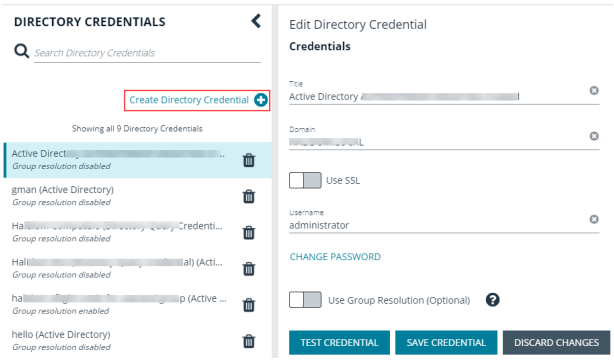
You can create a BeyondInsight local group, or you can use an existing Active Directory or LDAP group by adding it into BeyondInsight.

***Note:** By default, an **Administrators** 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 and LDAP, and also for adding Active Directory and LDAP groups and users in BeyondInsight.

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



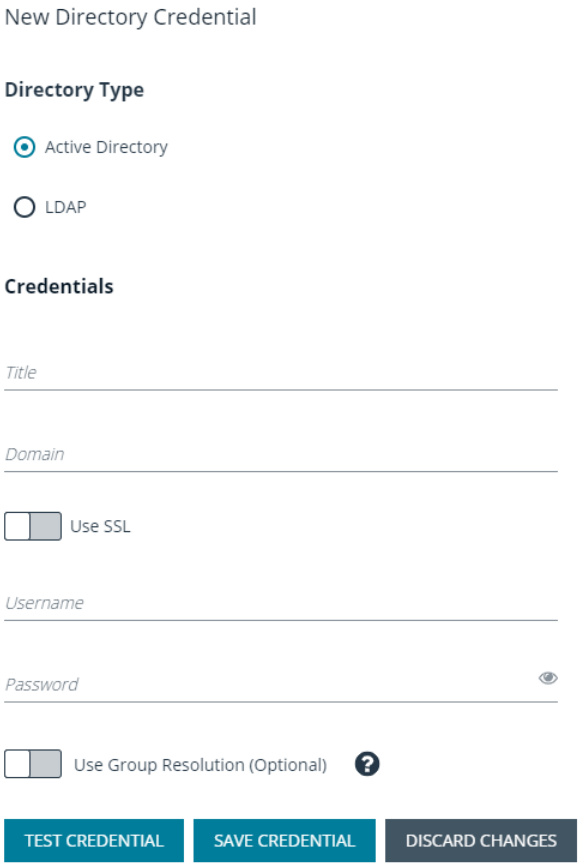
4. Select the directory type and provide a name for the credential.
5. Enter the name of the domain where the directory and user credentials reside.
6. Enable the SSL option to use a secure connection when accessing the directory.

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

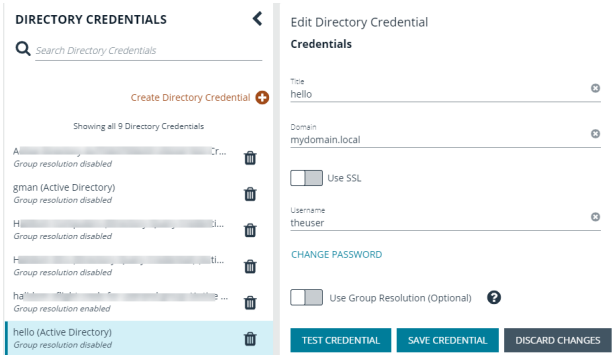
7. Enter the credentials for the account that has permissions to query the directory.
8. Enable the **Use Group Resolution** option to use this credential to for resolving groups from the directory.

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

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

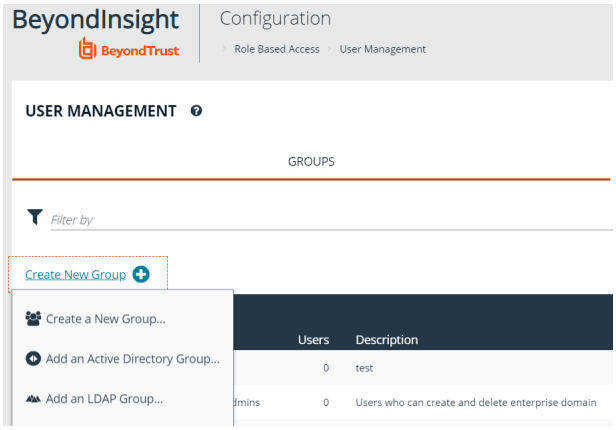


11. To edit a directory credential, select the credential, edit as desired, and then test and save the credential.

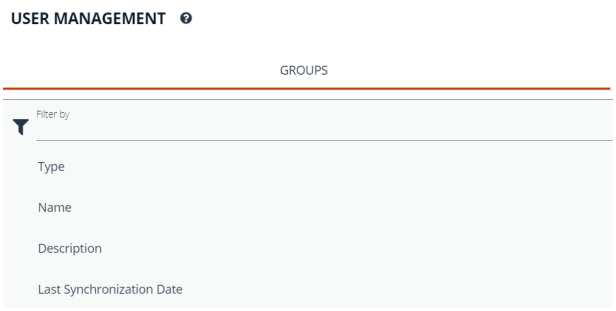


Create and Configure Groups

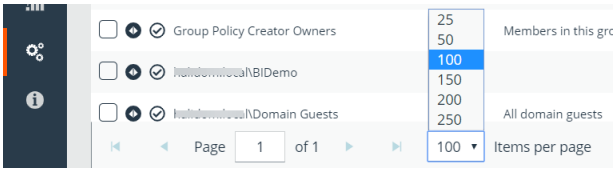
You can create BeyondInsight local groups, as well as add Active Directory and LDAP groups into BeyondInsight.



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



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

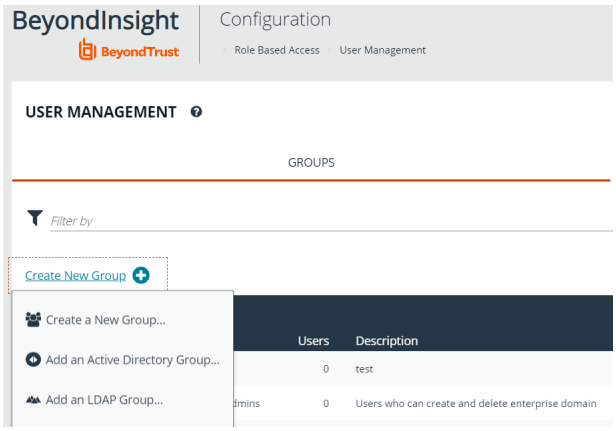


After a group is created, add user accounts to the group. When a user is added to a group, the user is assigned the permissions assigned to the group.

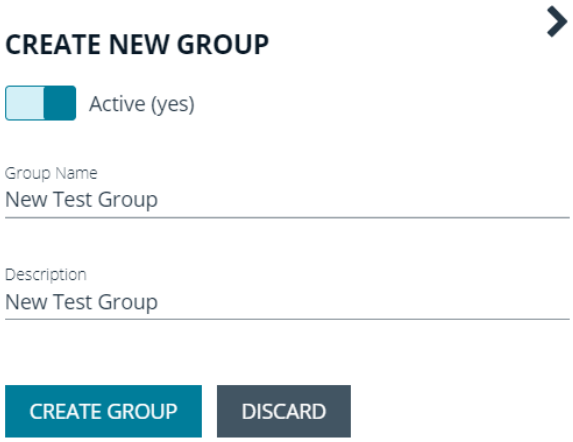
Create a BeyondInsight Local Group

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

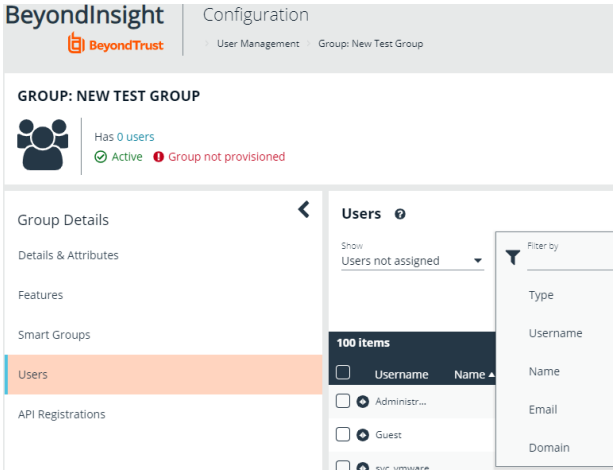
3. Under **Groups**, click **Create New Group**.
4. Select **Create a New Group**.



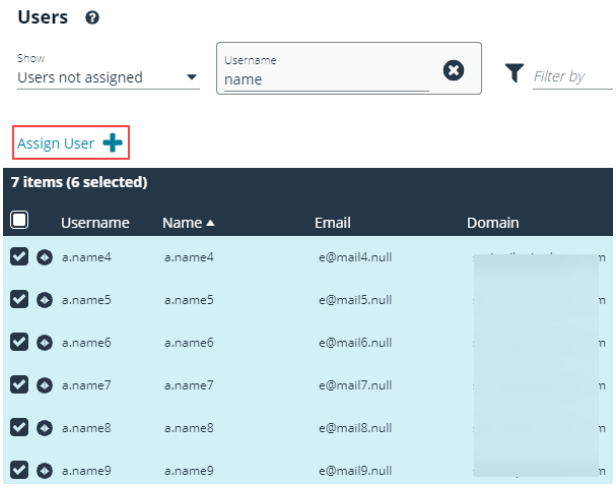
5. Enter a **Group Name** and **Description** for the group.
6. The group is set to **Active (yes)** by default. Click the slider to set the group to **Active (no)** if you wish to activate it later.
7. Click **Create Group**.



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



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



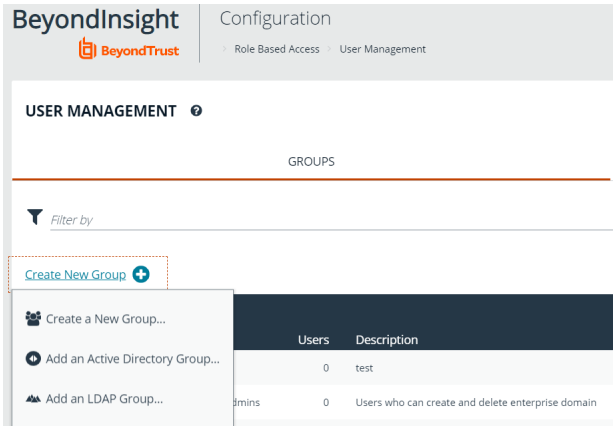
By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 29.

Add an Active Directory Group

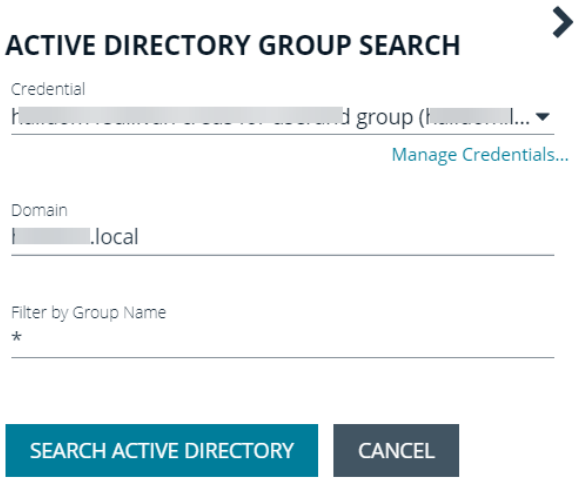
Active Directory group members can log into the management console and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller.

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

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



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



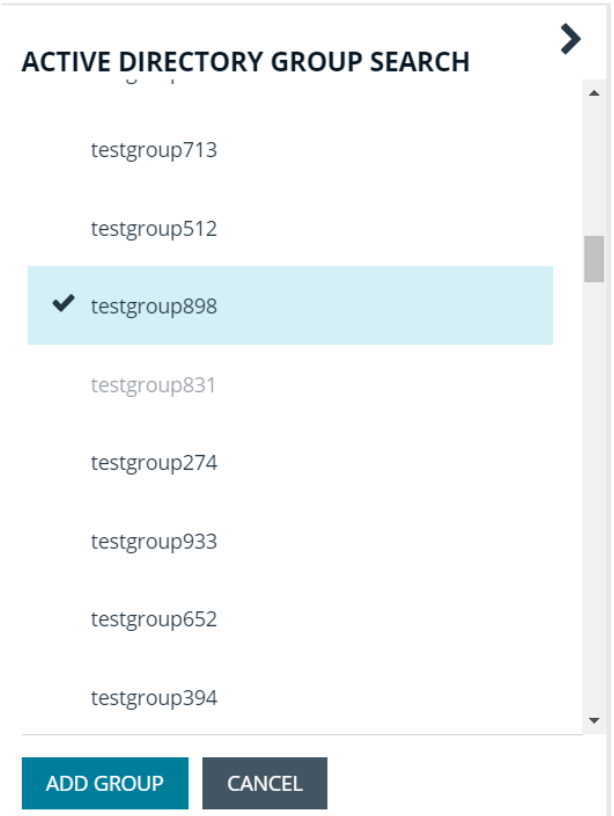
> For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 20.

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

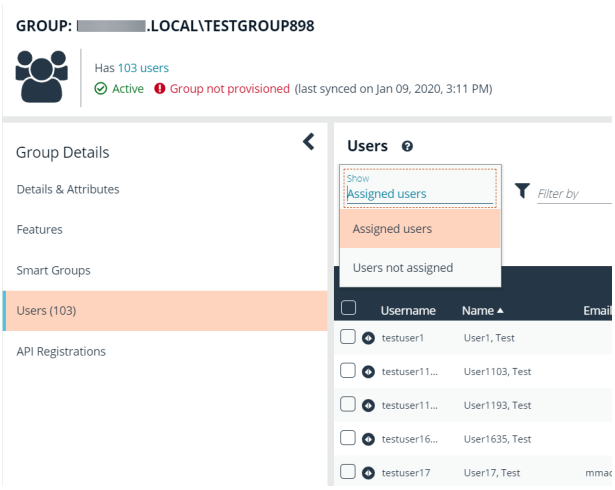
> ***Note:*** *For performance reasons, a maximum of 250 groups from Active Directory is retrieved. The default filter is an asterisk (*), which is a wild card filter that returns all groups. Use the group filter to refine the list.*

8. Set a filter on the groups that will be retrieved, and then click **Search Active Directory**. Example filters:
   - **a*** returns all group names that start with *a*
   - ***d** returns all group names that end with *d*
   - ***sql*** returns all groups that contain *sql* in the name

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



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



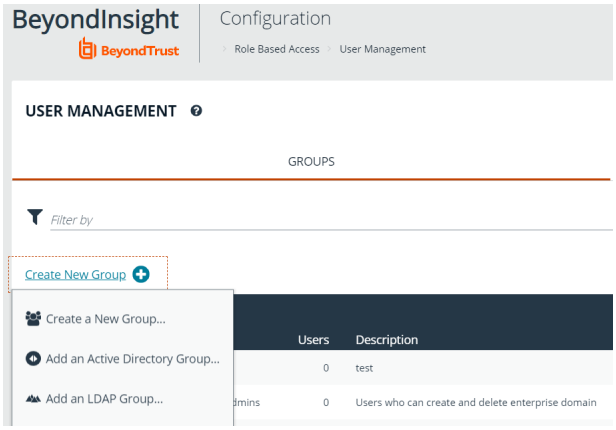
By default, new groups are not assigned any permissions. You must assign permissions onfeatures and smart groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 29.

Add an LDAP Directory Group

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

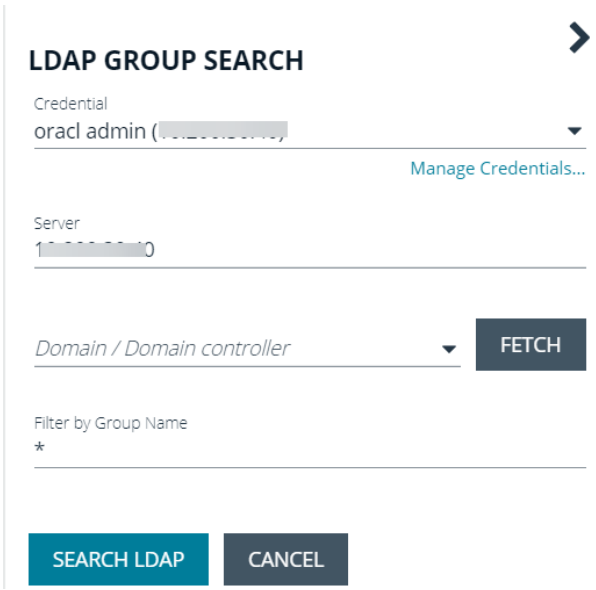
> ***Note:*** *LDAP users must log into the management console at least once to receive email notifications.*

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



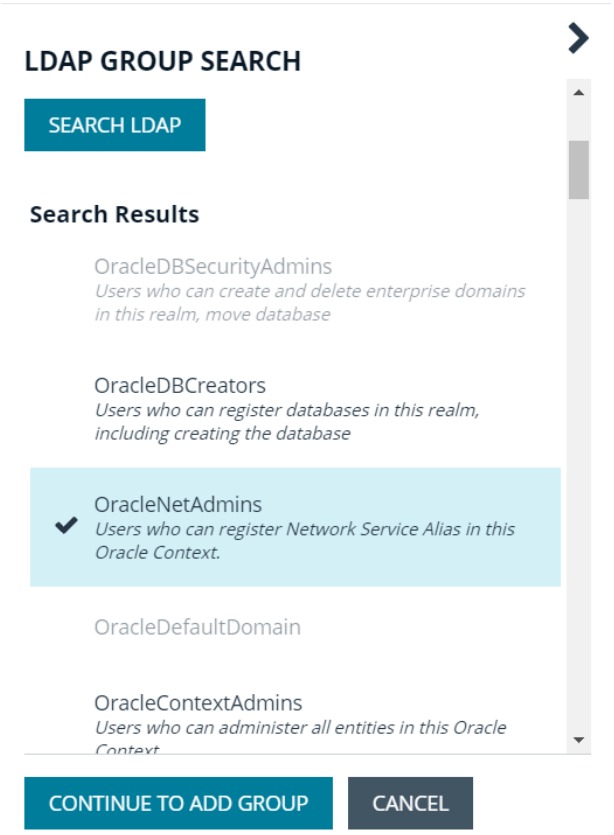
5. Select a credential, or click **Manage Credentials** to edit a credential or create a new one.

> For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 20.

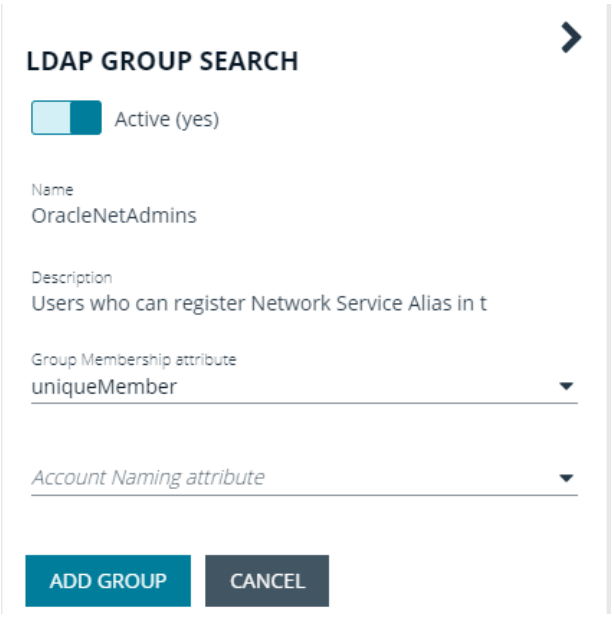


6. Click **Fetch** to load the list of Domain Controllers, and then select one.
7. To filter the group search, enter keywords in the group filter or use a wild card.
8. Click **Search LDAP**.

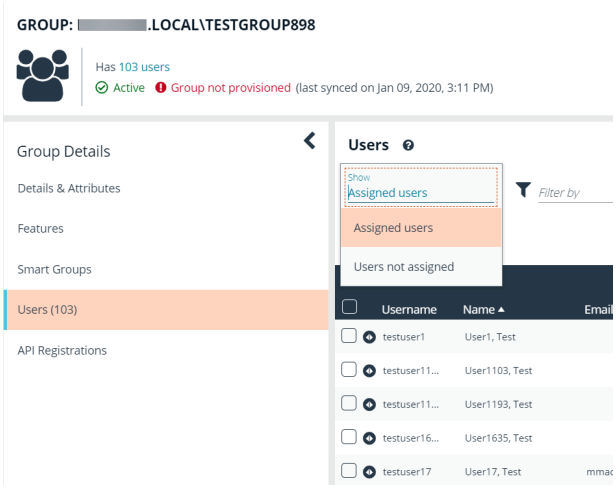
9. Select a group, and then click **Continue to Add Group**.



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



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



By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 29.

Assign Group Permissions

Permissions

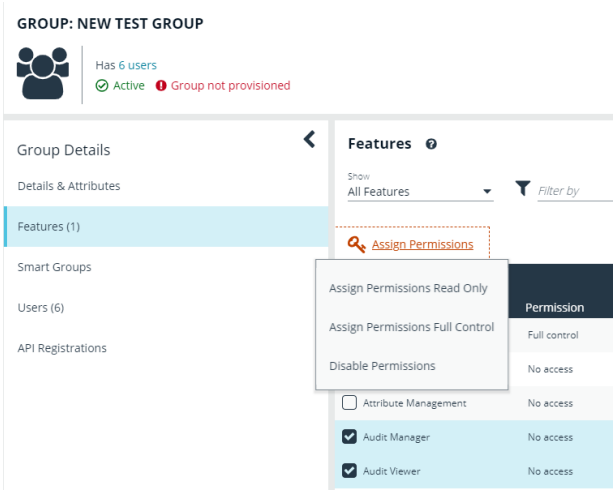
Permission	Description
No Access	Users cannot access the selected feature. In most cases, the feature will not be visible to the users.
Read Only	Users can view selected areas, but cannot change information.
Full Control	Users can view and change information for the selected feature.

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

- **Asset Management**
- **Benchmark Compliance**
- **Reports Management**
- **Scan - Job Management**
- **Scan Management**

Assign Features Permissions

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



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

Feature	Provides Permissions To:
Analytics and Reporting	Log into the console and access **Analytics & Reporting** to generate and subscribe to reports. ***Note:*** *After you create a group, go to the* ***Anayltics & Reporting Configuration*** *page and run the process daily cube job. Data between the management console and the reporting cube must be synchronized.*
Asset Management	Create smart rules. Edit and delete buttons on the **Asset Details** window. Create Active Directory queries. Create address groups.
Attribute Management	Add, rename, and delete attributes when managing user groups.
Audit Manager	**Audit Manager** on the **Configuration** page in the management console.
Audit Viewer	Use the **Audit Viewer** in **Analytics & Reporting**.
Benchmark Compliance	Configure and run benchmark compliance scans.
Credential Management	Add and change credentials when running scans and deploying policies.
Directory Credential Management	Grant access to the configuration area where Directory Credentials are managed. This feature must be enabled to support access to Directory Queries as well.
Directory Query Management	Grant access to the configuration area where Directory Queries are managed. ***Note:*** *Access to Directory Credential Management must also be granted.*
Endpoint Privilege Management	Use the **Endpoint Privilege Management** module, including asset details and the exclusions section on the **Configuration** page.

Feature	Provides Permissions To:
Endpoint Privilege Management for Unix and Linux	Use the **Endpoint Privilege Management for Unix and Linux** module.
File Integrity Monitoring	Work with **File Integrity** rules.
License Reporting	View the **Licensing** folder in **Analytics & Reporting** (MSP reports, Privilege Management for Windows, Privilege Management for Mac true-up reports, and Assets Scanned report) .
Management Console Access	Acces the BeyondInsight management console.
Manual Range Entry	Allow the user to manually enter ranges for scans and deployments rather than being restricted to smart groups. The specified ranges must be within the selected smart group.
Option Management	Change the application options settings (such as, account lockout and account password settings).
Options - Connectors	Access the configuration area where Connectors are managed.
Options - Scan Options	Access the configuration area where Scan Options are managed.
Password Safe Account Management	Grants permissions to the following features on the **Managed Accounts** page and through the public API: • Bulk delete accounts • Add accounts to a Quick Group • Remove accounts from a Quick Group • Add, edit, and delete accounts For more information, please see the **Managed Accounts** section in the BeyondInsight and Password Safe API Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/ps/6-10/ps-api-6-10.pdf.
Password Safe Admin Session	Password Safe web portal admin sessions.
Password Safe Global API Quarantine	Access to the Quarantine APIs.
Password Safe Bulk Password Change	Change more than one password at a time.
Password Safe Domain Management	Select the **Read** and **Write** check boxes to permit users to manage domains.
Password Safe Role Management	Allow a user to manage roles, provided they have the following permissions: **Password Safe Role Management** and **User Account Management**.
Password Safe System Management	Read and write managed systems through the public API.
Password Safe Ticket System Management	This feature is not presently used.
Patch Management	Use Patch Management module.
Reports Management	Run scans, create reports, and create report categories.

Feature	Provides Permissions To:
Scan - Audit Groups	Create, delete, update, and revert audit group settings.
Scan - Job Management	Activate **Scan** and **Start Scan** buttons. Activate **Abort**, **Resume**, **Pause**, and **Delete** on the **Job Details** page.
Scan - Policy Manager	Activate the settings on the **Edit Scan Settings** view.
Scan - Port Groups	Create, delete, update, and revert port group settings.
Scan - Report Delivery	Allow a user to set report delivery options when running a scan: • Export Type • Do not create a report for this vulnerability scan • Notify when complete • Email report to • Include scan metrics in email (only available for All Audits Scan, PCI Compliance Report, and Vulnerabilities Report)
Scan Management	Delete, edit, duplicate, and rename reports on the **Manage Report Templates** page. Activate **New Report** and **New Report Category**. Activate the **Update** button on the **Edit Scan Settings** view.
Session Monitoring	Use the session monitoring features.
Ticket System	View and use the ticket system.
Ticket System Management	Mark a ticket as inactive. The ticket no longer exists when **Inactive** is selected.
User Accounts Management	Add, delete, or change user groups and user accounts.
User Audits	View audit details for management console users on the **User Audits** page.
Vulnerability Exclusions	Select this option to prevent users from excluding vulnerabilities from the display. You can exclude vulnerabilities from the display to view those that require remediation to satisfy regulatory compliance. In some situations, you might not want all of your users to set an exclusion on a vulnerability.

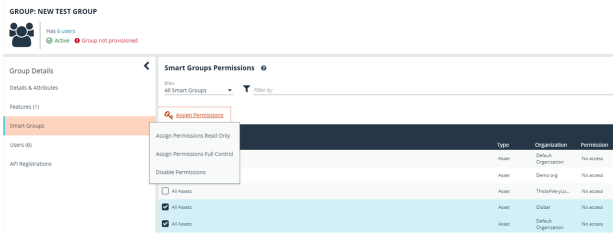
Feature Permissions Required for Configuration Options

Configuration Option	Feature and Permission
Active Directory Queries	Asset Management - Full Control
Address Groups	Asset Management - Full Control
Attributes	Asset Management - Full Control
Benchmark Compliance	Benchmark Management - Full Control
Connectors	Asset Management and Management Console Access - Full Control
Organizations	User Accounts Management - Full Control
Patch Management	Patch Management - Full Control
Password Safe Connections	Member of the built-in BeyondInsight Administrators group
Endpoint Privilege Management Module	Management Console Access and Endpoint Privilege Management - Full Control
Scan Options	Scan Management - Full Control

Configuration Option	Feature and Permission
SCCM	Patch Management - Full Control
Services	Member of the built-in BeyondInsight Administrators group
User Audits	User Audits - Full Control
User Management	User and Group Management - Full Control
Workgroups	User Accounts Management - Full Control

Assign Smart Groups Permissions

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



Edit and Delete Groups

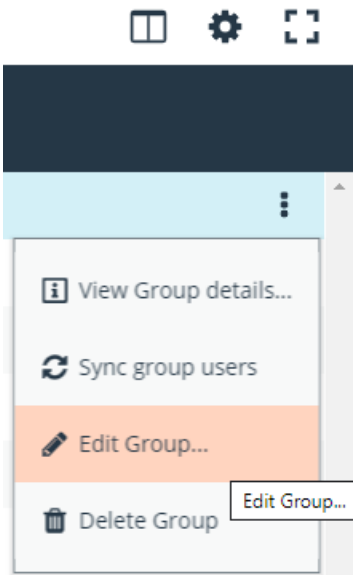
Edit Basic Group Details

Administrators can edit the following basic details for groups:

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

Follow these steps to edit a group:

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



5. In the **Edit Group** pane, update the details as required, and then click **Update Group**.

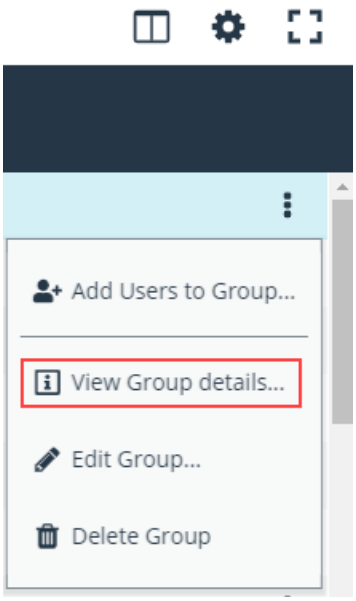
- For BeyondInsight local groups, administrators can change the active status, name, and description.
- For Active Directory groups, administrators can change the active status, credential, and domain controller.
- For LDAP groups, administrators can change the active status, credential, group membership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

Edit Advanced Group Details

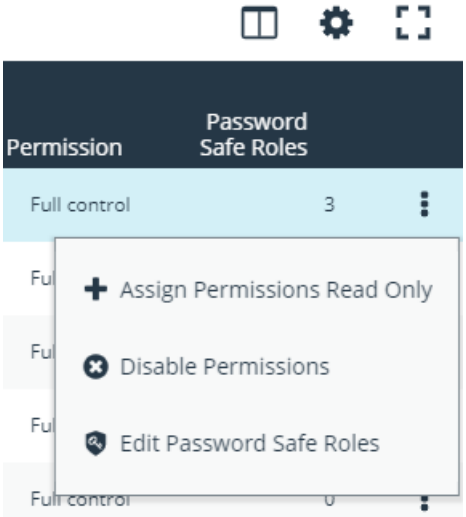
Administrators can edit advanced details, such as update permissions for features and smart groups, edit Password Safe roles, add and remove users from local groups, sync group users for Active Directory and LDAP groups, and update the API registrations.

Update Group Permissions for Features and Smart Groups

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

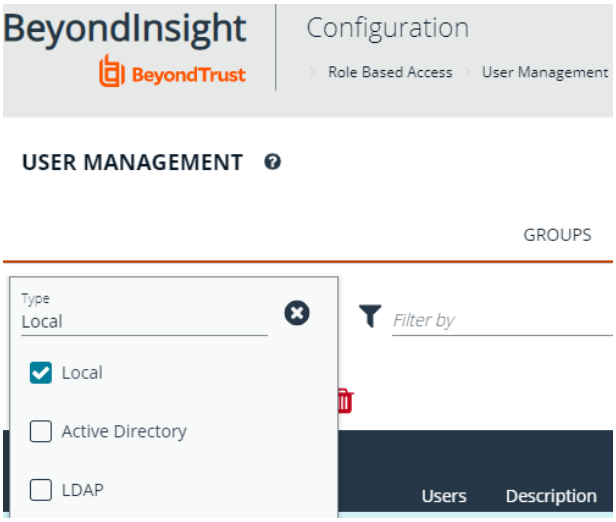


3. Select the desired features or smart groups, click **More Options**, and then select to assign or disable permissions accordingly.

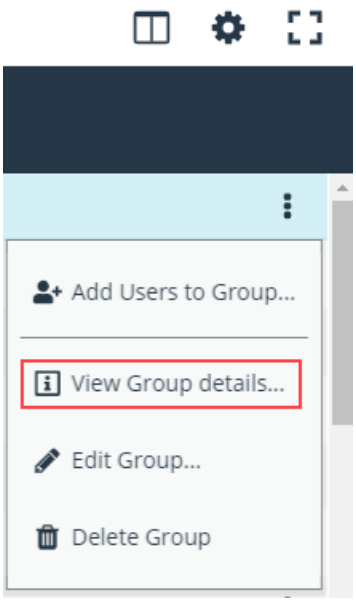


Remove Users from Local BeyondInsight Groups

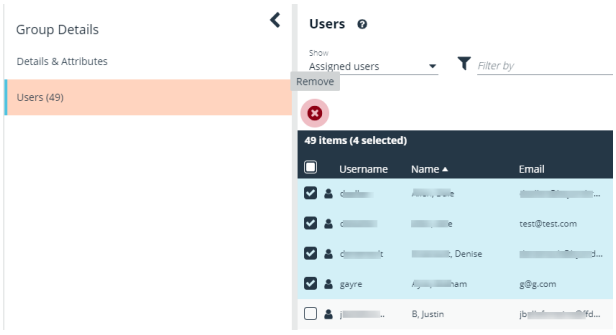
1. On the **User Management** page, filter the grid by local groups.



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

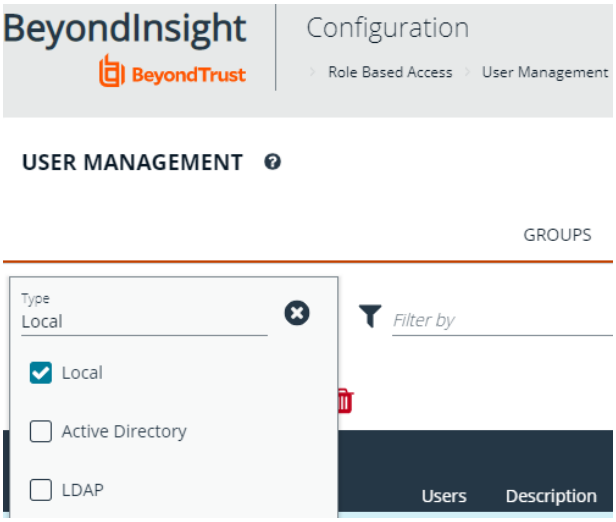


3. Under **Group Details**, select **Users**.
4. Filter the **Users** grid to show assigned users.
5. Select the user or users, and then click the **Remove** button.

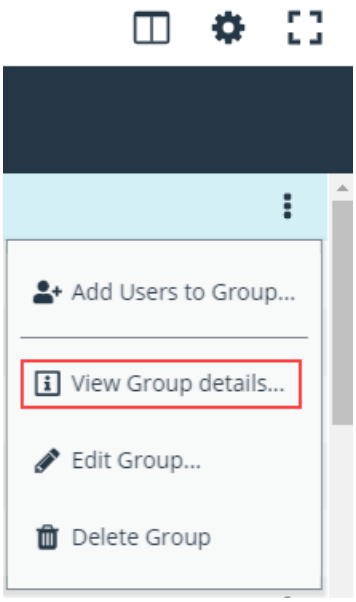


Add Users to Local BeyondInsight Groups

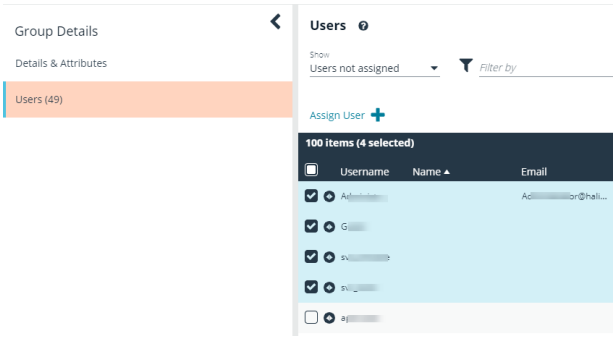
1. On the **User Management** page, filter the grid by local groups.



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

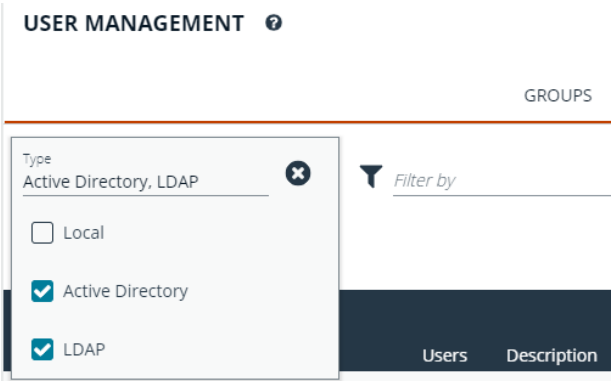


3. Under **Group Details**, select **Users**.
4. Filter the **Users** grid to show unassigned users.
5. Select the user or users, and then click **Assign User**.

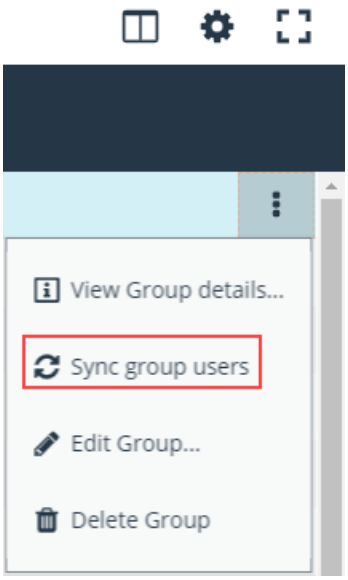


Sync Group Users for Active Directory and LDAP Groups

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



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



Delete a Group

Administrators can delete groups as follows:

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

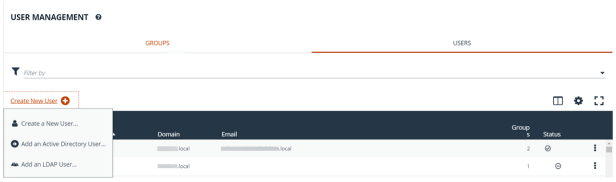
Create and Manage User Accounts

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

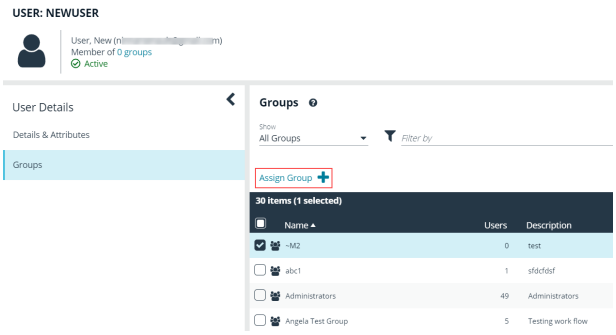
> ***Note:*** *A user account must be a member in a BeyondInsight group. If a user is not a member of any groups in BeyondInsight, the user will not be able to log into the console.*

Create a BeyondInsight Local User Account

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

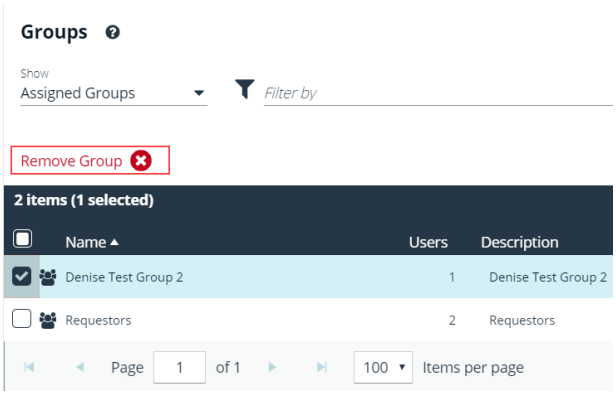


5. Select **Create a New User**.
6. Complete the **Identification** and **Credentials / Change Password** sections. These fields are required.
7. Enter the user's contact information *(Optional)*.
8. Select an **Activation Date** and an **Expiration Date** for the user account.
9. Enable the **User Active** option to activate the user account.
10. Leave the **Account Locked** and **Account Quarantined** options disabled.
11. Select a two-factor authentication method and mapping information, if applicable.
12. Click **Create User**.
13. The user is created and **User Details > Groups** is displayed. You can filter the list of groups displayed by type, name, or description. Select a group, and then click **Assign Group**.



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

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

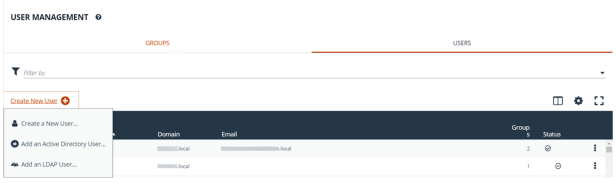


Add an Active Directory User

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

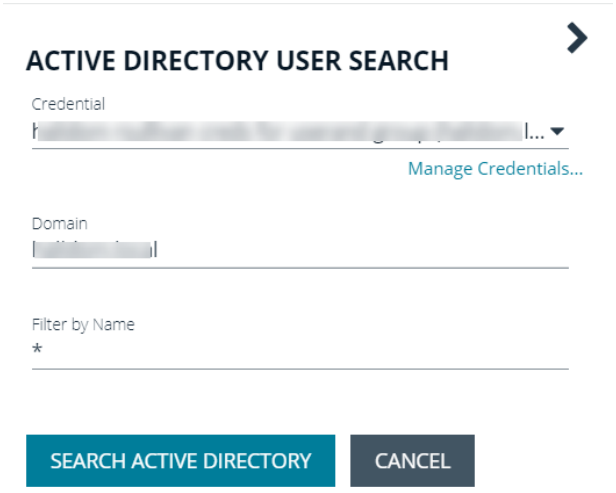
> ***Note:*** *Active Directory users must log into the management console at least once to receive email notifications.*

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



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

> For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 20.



7. If not automatically populated, enter the name of a domain or domain controller.

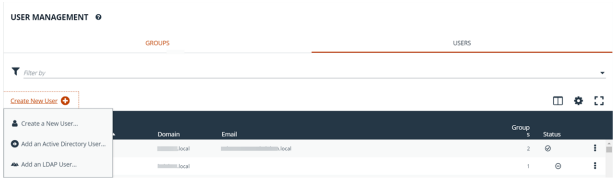
8. After you enter the domain or domain controller credential information, click **Search Active Directory**. A list of users in the selected domain is displayed.

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

9. Set a filter on the groups that will be retrieved, and then click **Search Active Directory**. Example filters:
   - **a*** returns all group names that start with *a*
   - ***d** returns all group names that end with *d*
   - ***sql*** returns all groups that contain *sql* in the name
10. Select a user, and then click **Add User**.
11. Assign at least one group to the user.

Add an LDAP User

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



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

> For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 20.

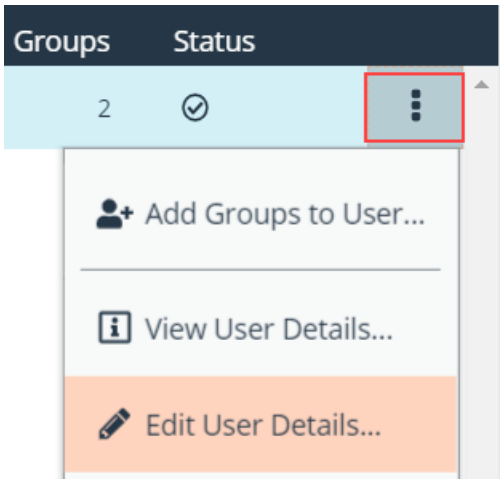
7. Click **Fetch** to load the list Domain Controllers, and then select one.
8. To filter the group search, enter keywords in the group filter or use a wild card.
9. Click **Search LDAP**.
10. Select a user, and then click **Add User**.
11. Assign at least one group to the user.

Edit a User Account

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

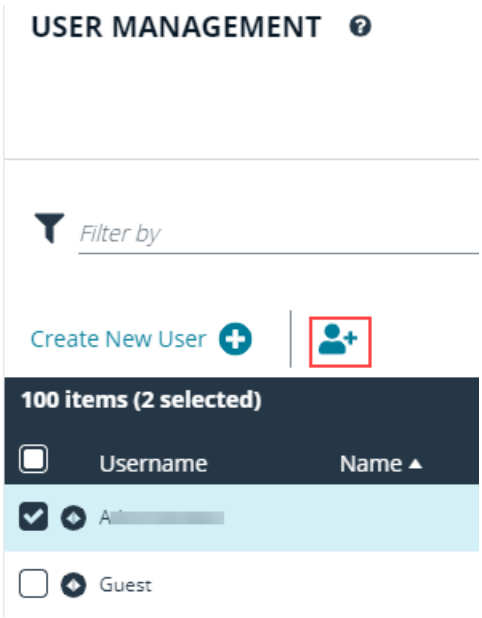
1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.

3. Click **Users** to display the list of users in the grid.
4. Optionally, filter the list of users in the grid by **Type**, **Username**, **Name**, **Domain**, or **Email**.
5. Select a user, and then click the **More Options** button, then select **Edit User Details**.
6. In the **Edit User** pane, update the details as required, and then click **Update User**.



Add Groups to User

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



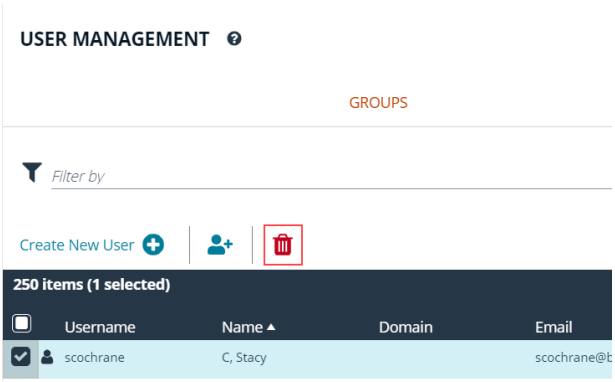
4. Search for the group or groups, and then select the group or groups to assign currently selected users to the selected groups.

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

Delete a User Account

Administrators can delete user accounts as follows:

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



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

Audit Console Users

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

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

To view user audit data, follow the steps.

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

You can also configure display preferences and filters to refine the information displayed. For more information, please see "Change and Set the Console Display and Preferences" on page 17.

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

Overview of BeyondInsight Tools

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

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

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

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

For more information, please see "Change Asset Properties" on page 111.

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

For more information, please see "Change and Set the Console Display and Preferences" on page 17.

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
- WebScan URL.

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

For more information, please see "Create and Configure Groups" on page 22.

Create an Always Address Group

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

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

For example, if the **Always** address group is configured with the following:

- 10.10.10.60 and buffett-laptop (omitted)

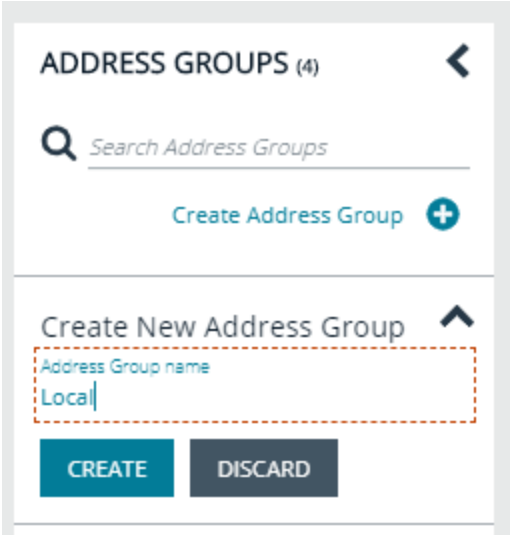
It scans 10.10.10.50 and buffett-laptop. The results are:

- 10.10.10.60 is included in the scan since that IP address was added to the Always address group
- buffett-laptop is excluded from the scan since that asset was explicitly omitted in the Always address group
- 10.10.10.50 is scanned as usual

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

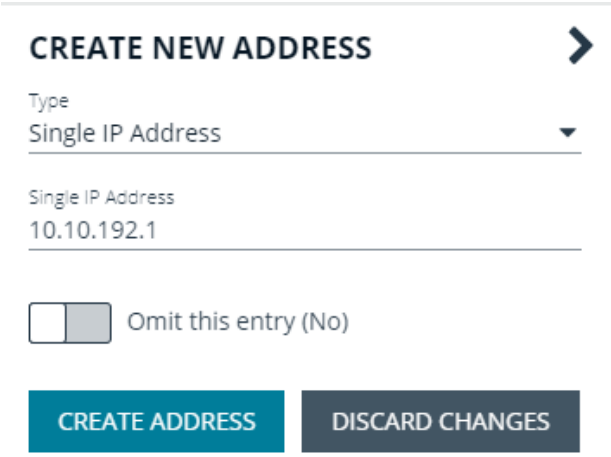
1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Address Groups**.

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

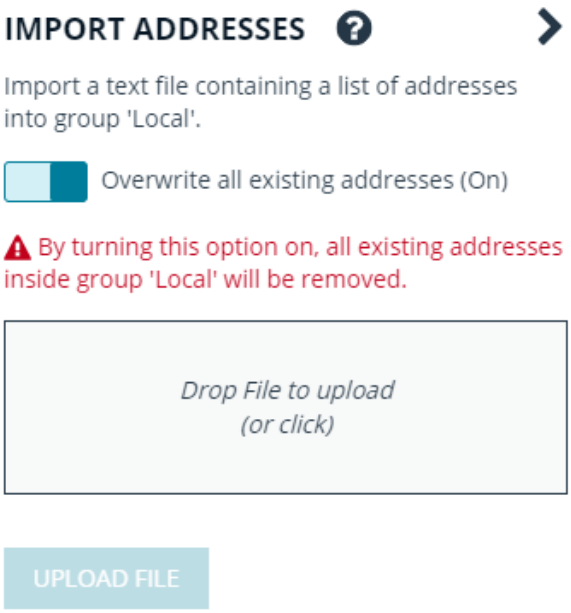


5. Select the address group, and then click **Add New Address** to manually add the IP addresses. Or, click **Import Addresses** to import them into the group using a file.

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

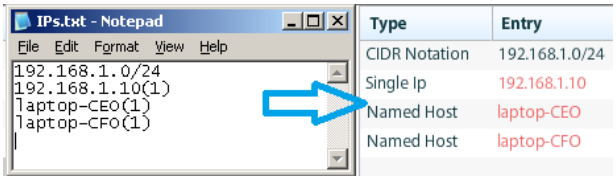


7. If importing the addresses:
    a. Enable the **Overwrite all existing addresses** option, if desired.
    b. Click **Drop File** to upload the import file.
    c. Click **Upload File**.



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

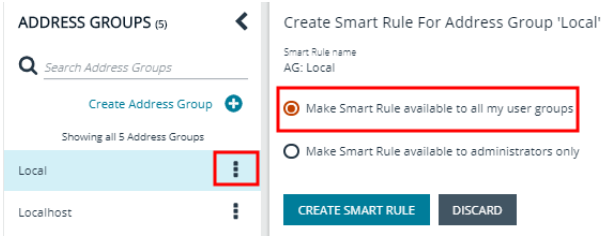
Here is an example of how a CIDR Notation, an excluded IP address, and excluded named hosts are displayed after importing.



Create a Smart Rule Based on an Address Group

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

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



6. You will receive a message stating that a *Smart Rule has been created for this Address Group*.
7. The group is displayed on the **Configuration > Smart Rules** .

Update Address Groups Using Stored Procedures

Util_VAAdressEdit

@EditAddressErrorMessage	Error messages (if any) generated during the execution of this procedure.
@VAAddressIdOut	Address Group ID.
@Action	Action to be performed. Valid actions are -> 1(add/edit)|2(delete)
@VAAddressGroupName	The parent address group.
@VAScanPolicy_RetinaInfoID	Associated scan policy info ID.
@Omit	Flag used to exclude IP address(es).
@Type	Specifies the address type. Valid types are -> single|range|cidr|name|url
@Value	Values must be in the following formats: **single :** [0-2][0-5][0-5].[0-2][0-5][0-5].[0-2][0-5][0-5].[0-2][0-5][0-5] **range :** [0-2][0-5][0-5].[0-2][0-5][0-5].[0-2][0-5][0-5].[0-2][0-5][0-5]-[0-2][0-5][0-5].[0-2][0-5][0-5].[0-2][0-5][0-5].[0-2][0-5][0-5] **cidr :** [0-2][0-5][0-5].[0-2][0-5][0-5].[0-2][0-5][0-5].[0-2][0-5][0-5]/[0-32] **name :** Cannot be NULL or empty **url :** Cannot be NULL or empty

Util_VAAddressListByAddressGroup

@VAAddressGroupName	The parent address group.

Example

```
/*
       --TEST
        DECLARE @ErrorMessage  NVARCHAR(4000) = ''
        DECLARE @Result INT = ''
        DECLARE @VAAddressIdOut INT = NULL

-- Create a new entry
EXEC @Result = [dbo].[Util_VAAddressEdit] @EditAddressErrorMessage = @ErrorMessage
  OUTPUT
        @VAAddressIdOut = @VAAddressIdOut OUTPUT,
        @Action = 1,
        @VAAddressGroupName = 'New Address Group 1',
        @VAScanPolicy_RetinaInfoID = NULL,
        @Omit = 0,
        @Type = 'range',  --@Type = 'single'
        @Value = '10.1.2.3-1.25.25.25' --@Value = '10.200.31.70'
SELECT * FROM [dbo].[VAAddress]
PRINT @ErrorMessage
IF(@Result = 0)
BEGIN

-- Edit the newly created entry
EXEC @Result = [dbo].[Util_VAAddressEdit] @EditAddressErrorMessage = @ErrorMessage
  OUTPUT,
               @VAAddressIdOut =       @VAAddressIdOut OUTPUT,
               @Action = 1,
               @VAAddressGroupName = 'New Address Group 1',
               @VAScanPolicy_RetinaInfoID = NULL,
               @Omit = 0,

               @Type = 'range',        --@Type = 'single'
               @Value = '10.1.2.3-10.10.10.10' --@Value = '10.200.31.71'
SELECT * FROM [dbo].[VAAddress]
PRINT @ErrorMessage

 -- Delete the new entry
 EXEC @Result = [dbo].[Util_VAAddressEdit] @EditAddressErrorMessage = @ErrorMessage
OUTPUT,@VAAddressIdOut = @VAAddressIdOut
  OUTPUT,
               @VAAdressIdOut = @VAAddressIdOut OUTPUT,
               @Action = 2
SELECT * FROM [dbo].[VAAddress]
PRINT @ErrorMessage
END
*/

 /*

--TEST
EXEC [dbo].[Util_VAAddressListByAddressGroup] 'Localhost' -- return only return addresses
  associated with address group with name 'Localhost'
-- OR --
EXEC [dbo].[Util_VAAddressListByAddressGroup] -- return all address groups and their
```

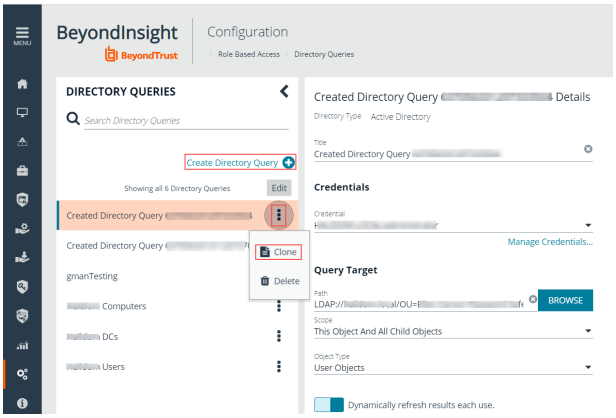
```
  associated addresses
*/
```

Create a Directory Query

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

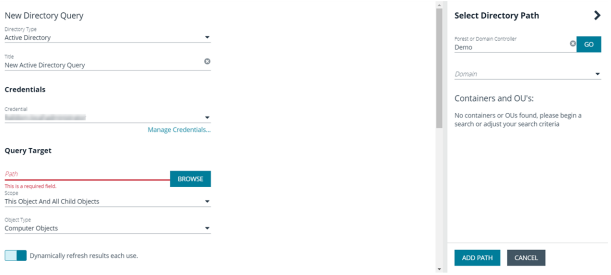
For more information, please see "Create and Configure Groups" on page 22.

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



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

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

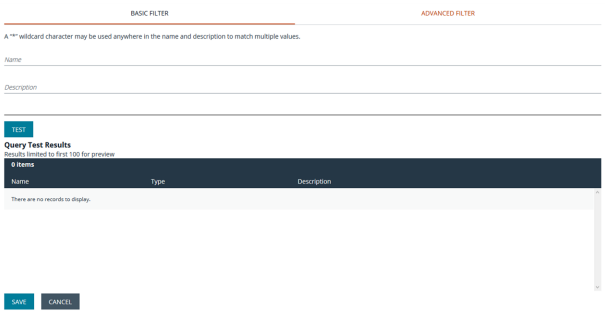


***Note:** At minimum, the credential must have **Read** permissions on the computer assets you are enumerating.*

For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 20.

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

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



Attributes and Attributes Types

Attributes can be used to label assets, and you can set attributes for each asset in a group using a Smart Rule. BeyondInsight ships with attributes already created, and you can also add attribute types to meet your requirements.

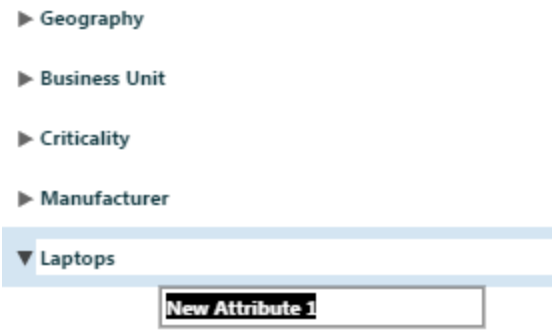
For more information, please see "Use Smart Rules to Organize Assets" on page 55.

Add Attribute Types

1. Select **Configuration**.
2. Under **General**, click **Attributes**.
3. Click **+ (Create New Attribute)**.
4. Select **Attribute Type**.
5. Type an attribute name.

Add Attributes

1. Select an attribute type.
2. Click **+ (Create New Attribute)**.
3. Select **Attribute**.
4. Type an attribute name.



Use Smart Rules to Organize Assets

A smart rule is a filter that you can use to organize assets into smart groups. You can organize the assets using one of the following smart rule types:

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

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

When a non-administrator user creates a smart group, the smart group is automatically associated with:

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

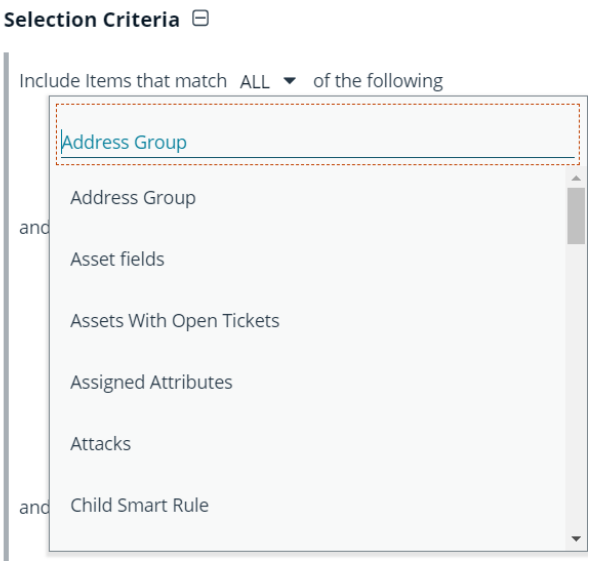
Use a smart rule to register assets as smart groups. This allows you to:

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

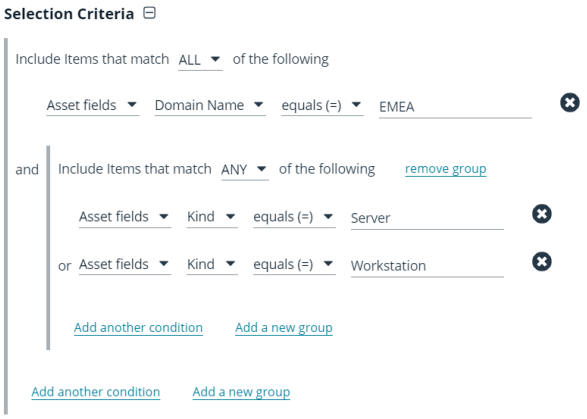
Smart rules update results automatically, ensuring assets match the criteria and are current.

Use Smart Rule Filters and Smart Groups

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



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



Smart Rule Filters

Asset Smart Rule Filters

Address Group	Create a group of IP addresses. For more information, please see "Create an Address Group" on page 46.
Asset Fields	Group the smart rule by asset fields, such as, **Asset Name**, **Device ID**, **Domain** or **DNS**, **Risk**, and **Kind**.

	You can include more than one asset field filter in the smart rule to refine the results. ***Note: Device ID** and **Serial Number** apply to mobile devices only.*
Assets with Open Tickets	For ticket tracking, create a smart rule that filters on open tickets. The smart rule filter can be set to include overdue tickets.
Assigned Attributes	Create a filter based on an attribute. If the attribute is unassigned on a particular asset, you can choose to include or exclude the asset from the rule.
Attacks	Filter assets based on attack, or filter on attack name or ID.
Child Smart Rule	You can reuse a smart rule to save time when creating new smart rules. This is especially useful if the smart rule is a complicated set of filters. Reusing a smart rule further refines the assets that will be a part of the smart rule.
Cloud Assets	Filter assets on the cloud connector.
Directory Query	Create an Active Directory or an LDAP query to include or exclude assets in the selected domain. For more information, please see "Create a Directory Query" on page 52.
Installed Software	Filter on any combination of installed software.
MAC Address	Filter by MAC address of assets.
Malware	Filter assets based on malware, or filter on malware name or ID.
Operating System	Filter on any combination of OS. Operating systems included in the list are those detected in your network. Assets with no OS detected, can be included or excluded from the rule.
Ports	Filter by port group. Assets with open ports in the port group can be included or excluded from the rule.
Processes	Filter on any combination of processes.
Protection Agents	Filter by protection agents.
Services	Filter by any combination of services.
Software Version	Filter by software version. The software that you can filter on is determined by the software that is discovered during the scan.
User Account Attribute	Filters user accounts by SID or privilege. You can filter on both. If either value is not selected then it will be ignored. Using this filter you can determine if any users have administrator privileges that might no longer be required. You can create a smart rule using this filter and set the email alert action to notify you when a

	user account with admin privileges is detected.
Vulnerabilities	Filter by vulnerability, CVSS score or vector, PCI severity, or vulnerabilities from an audit group.
Vulnerability Scanners	Filter by scanner. Can filter for responsive or unresponsive scanners.
Windows Events	Filter by Windows events that are available in the Windows Event Viewer. For example, Application, Security, or System.
Workgroup	Filter by workgroup.

Vulnerabilities Smart Rule Filters

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

Predefined Smart Group Categories

Agents and Scanners	Detects assets where protection agents and BeyondInsight are deployed.
Assets and Devices	Includes default smart groups for all assets and all assets labeled as workstations.
Intelligent Alerts	Includes smart groups that detect assets added since yesterday, and mobile assets with critical vulnerabilities. Intelligent Alerts are inactive by default.
SCCM	Includes smart groups for systems managed by Microsoft System Center Configuration Manager. You can configure these smart groups to synchronize with SCCM every X hours.
Servers	Includes smart groups that detect assets that are mail servers, web servers, database servers, domain controllers, and SCADA. Only the **Web Servers** smart group is marked as active.
Virtualized Devices	Includes smart groups for virtual environments, including **Microsoft Hyper-V** and **Parallels**. Assets detected as virtual environments are part of these smart groups. This default category also includes two smart groups: **Virtual Servers** and **Virtual Workstations**. Assets that are servers or workstations might not be detected, and therefore, not included in the smart group. For example, the asset might be a router or unknown and will not be part of the smart group.

Predefined Smart Groups for Vulnerabilities

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

Create Smart Rules

You can configure an asset smart rule to:

- Create smart groups
- Send email alerts with a list of assets
- Set attributes on assets
- Create a ticket with a list of assets
- Enable for Patch management
- Set environmental metrics for CVSS scoring
- Set scanner pooling

Create an Asset Based Smart Rule

1. Select **Configuration**.
2. Under **General**, select **Smart Rules**.
3. .Leave **Asset** selected for the **Smart Rule type filter**.
4. Click **Create Smart Rule**.
5. Select a category.
6. Enter a name and description.
7. 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.
8. Select the filters in the **Selection Criteria** section.
9. From the **Actions** section, select one of the following:

Assign to Host Scan Group	Select to create a smart group to apply to a selected Host Scan Group.
Create Ticket	Select tickets parameters, including ticket assignment, severity, and email alert. For more information, please see "Manage Ticket Details" on page 118.
Deploy PB Policy	Select to deploy Endpoint Privilege Management policies to the assets that match the criteria selected in the Smart Rule.
Enable for Patch Management	Select to create a smart group for managing patch updates to assets.
Export Data	Select to manage a smart group for the BMC Remedy connector.
Mark each asset for deletion	Select to create a smart group that contains assets to be marked for deletion.
Mark each asset inactive	Assets detected as inactive will no longer be displayed on the Assets page or in reports.
Remove from Host Scan Group	Select to create a smart group to remove assets from selected Host Scan Group.
Send an email Alert	Select and enter the email addresses for notification when the rule criteria is matched. Emails are only sent if the list of assets that match the rule is changed from the last time the rule was

	processed.
Set attributes on each asset	Select the attribute type from the list, and then select the attribute.
Set Environmental CVSS Metrics	Select environmental metrics for CVSS. For more information, see "Set Metrics" on page 88.
Set Scanner Properties	Select one or more scanners to lock to the smart group. For more information, please see "Use Scanner Pooling" on page 151.
Set attributes on each asset	Select attributes for each asset.
Show asset as Smart Group	When selected, the rule is displayed in the smart groups pane as a smart group. You can select the smart group to filter the list of assets in the smart groups pane. You can also select the default view to display on the **Assets** page when the smart group is selected. Smart groups are also used for running scans, applying protection policies, and registering for patch updates.

10. Click **Save**.

Create a Vulnerabilities Based Smart Rule

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

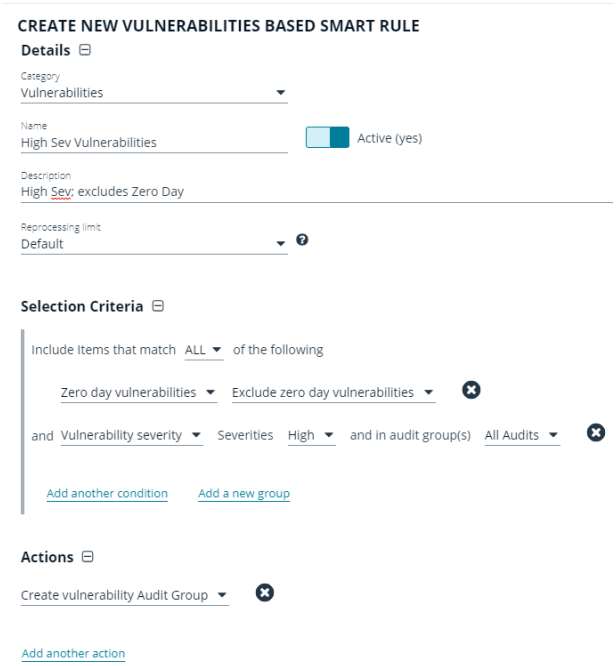
1. Select **Configuration > General > Smart Rules**.
2. From the **Smart Rule type filter** list, select **Vulnerabilities**.
3. Click **Create Smart Rule**.
4. Enter a name and description.
5. By default, the smart rule is set to **Active (yes)**, so it is always available for processing. Disable the active setting to ensure the rule is not processed.
6. Select the filters in the **Selection Criteria** section.
7. From the **Actions** section, select one of the following:
    - **Create Vulnerability Audit Group:** To create a read-only audit group.
    - **Show Vulnerability as Smart Group:** When selected, the rule is displayed on the **Vulnerabilities** page as a filter for the list of assets selected in the Smart Groups browser pane.
    - **Send an email Alert:** Select and enter the email addresses for notification when the rule criteria is matched. Emails are only sent if the list of vulnerabilities that match the rule is changed from the last time the rule was processed.
8. Click **Create Smart Rule**.

Example Scenario

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

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

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



Perform Other Smart Rule Actions

Clone a Smart Rule

You can clone custom or predefined smart rules.

1. Select **Configuration**.
2. Under **General**, select **Smart Rules**.
3. Select the smart rule you wish to clone, click the **More Options** button, and then select **Clone**.
4. If you are using the multi-tenant feature, select the organization from the list, and then click **Clone Smart Rule**.
5. On the **Smart Rules** page, select the newly cloned smart rule, and then click **More Options > View Details**, then edit the smart rule filters as needed.
6. Click **Save Changes**.

Deactivate a Smart Rule

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

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

An inactive smart group is no longer displayed in the smart group browser pane until marked active again.

To deactivate a smart rule:

1. Select **Configuration > General > Smart Rules**.
2. Select the smart group or multiple smart groups, and then click **Deactivate** above the grid.

Delete a Smart Rule

1. Select **Configuration**.
2. Under **General**, select **Smart Rules**.
3. Select the smart rule.
4. Click the **Delete** icon above the grid.

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

Smart Rule Processing

A smart rule processes and updates information in smart groups when certain actions occur.

The actions might be any of the following:

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

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

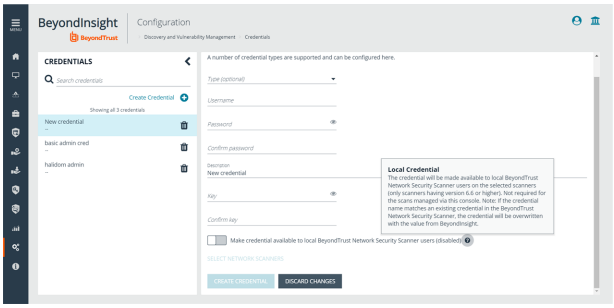
Add Credentials for Use in Scans

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

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

To create a credential:

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



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

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

Type	Information
MS SQL Server	• Authentication Type • Domain *(Optional)* • Username • Password • Confirm Password • Description • Key • Confirm Key
MySQL	• Username • Password • Confirm Password • Description • Key • Confirm Key

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

If you are creating Oracle, SSH, or SNMP credentials, please see "Create SSH Credentials" on page 70, "Create Oracle Credentials" on page 68, and "Create SNMP Credentials" on page 69.

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

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

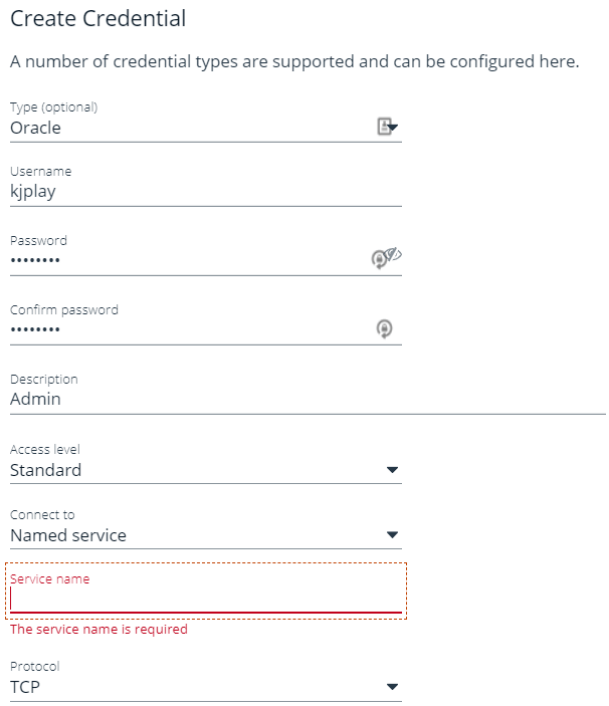
If the credential name matches an existing credential in the BeyondTrust Network Security Scanner, the credential is overwritten with the value from BeyondInsight.

6. Click **Create Credential**.

Create Oracle Credentials

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

1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Credentials**.
3. Click **Create Credential**.
4. From the **Type** list, select **Oracle**.
5. Provide a **Username**, **Password**, and **Description**.
6. Select an **Access level** from the list: **Standard**, **SYSDBA**, or **SYSOPER**.
7. Select additional connection options:
   - **Connect To:** Select from: **Database** or **Named Service**.
   - **Protocol:** Select a protocol: **TCP**, **TCPS**, or **NMP**.
   - **Hosts:** Enter the host name where the Oracle database resides. If this credential is used for multiple Oracle hosts, separate each host name by a comma.
   - **Port Number:** Enter a port number.



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

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

> ***Tip:*** *This feature propagates credentials stored in Vulnerability Management to network scanner servers and allows end-users and API calls to leverage credentials locally on the network scanner. This eliminates the need to provide credentials separately for those scanners.*
>
> *If the credential name matches an existing credential in the BeyondTrust Network Security Scanner, the credential is overwritten with the value from BeyondInsight.*

10. Click **Create Credential**.

Create SNMP Credentials

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

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

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

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

7. Click **Create Credential**.

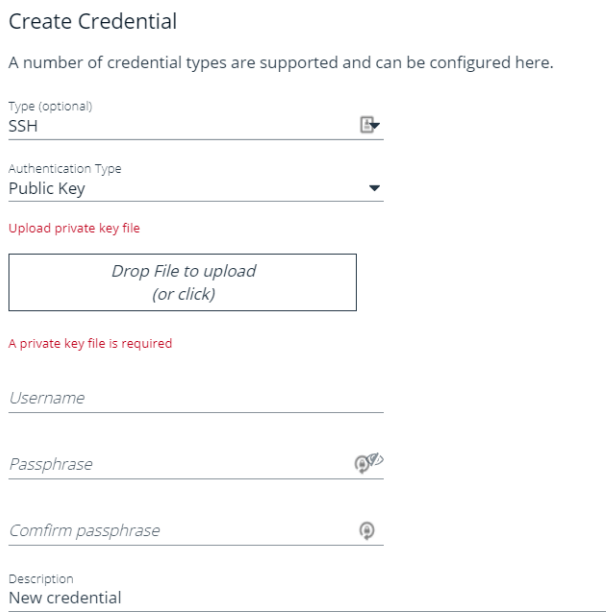
Create SSH Credentials

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

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

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

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



> ***Tip:*** *This feature propagates credentials stored in Vulnerability Management to network scanner servers and allows end-users and API calls to leverage credentials locally on the network scanner. This eliminates the need to provide credentials separately for those scanners.*
>
> *If the credential name matches an existing credential in the BeyondTrust Network Security Scanner, the credential is overwritten with the value from BeyondInsight.*

8. Click **Create Credential.**.

Run Discovery Scans

Run a discovery scan to locate network assets, such as workstations, routers, laptops, and printers. A discovery scan also determine 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 scan.

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

Review the following recommended discovery scan settings:

- On the **Set Scan Options** page, setting credentials is not required. Typically, setting credentials for other types of scan templates is recommended. However, for a discovery scan, all types of systems are detected and credentials are not necessary.
- After assets are detected, you can run audit scans using credentials to ensure more thorough scan results.
- On the **Scan Policy Options** page, here are some recommended settings:

Perform OS Detection	Select this check box.
Perform Traceroute	Select this check box.
Enumerate *	Clear all enumerate check boxes.
Randomize Target List	Select this check box.

To change the settings, please see "Edit Scan Settings" on page 76.

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

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.

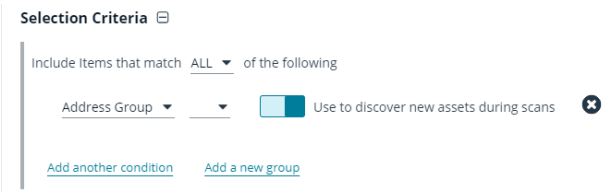
Tip: *If you create an address group that includes the /19 CIDR block, the range possesses 8190 potential assets. The discovery scan always tries to discover those assets. Keep this in mind when you are reviewing scan results.*

Key steps:

- Create an address group or Active Directory query that includes the IP address range or domain. Alternatively, you can create the address group or query when you are creating the smart group.

For more information, please see "Create a Directory Query" on page 52 or "Create an Address Group" on page 46.

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



Note: *You can check the* ***Discover New Assets*** *box on any scan. However, the scan is slower when this option is selected.*

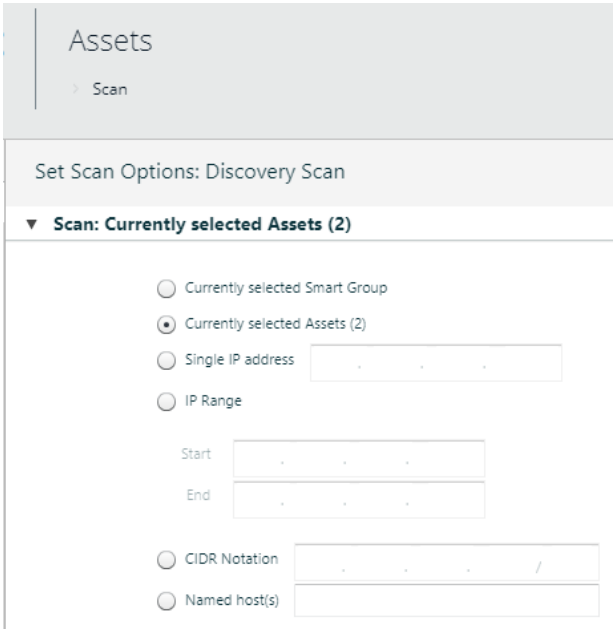
Tip: *It is recommended you run a discovery scan at a regular interval. Full vulnerability scans will then run only on known targets. You can discover assets manually by entering a host name, IP address, or address range.*

Run Vulnerability Scans

When you run a scan, you must select a report template to determine the scope of the scanning.

***Note:** On the **Legacy Assets View** page, you can individually select assets to scan.*

***Note:** You can enter any combination of IP address, IP address range, and CIDR notation in the **Named Hosts** box. Separate the entries using a comma.*



***Tip:** If an IP address is invalid, no error message indicates the address is invalid and will not be scanned.*

1. Select **Scan**.
2. Select a report, and then click **Scan**.
3. Expand **Scan**, and select one of the following:
4. Currently selected Smart Group, Currently selected Assets, a Single IP, an IP Range, a CIDR Notation, or Named Hosts for the assets selected.
5. You can enter more than one named host. Separate the entries using a comma.
    - If you select **Currently selected assets** and select a schedule other than **Immediate**, BeyondInsight automatically updates the scheduled job on the agent with the list of assets in the selected Smart Group as they change.
    - (Benchmark scans only) Expand **Benchmark Compliance Profile**, and select a scan profile.
    - Expand **Credentials Management**, and enter the credentials. You can use Active Directory credentials or BeyondInsight web server credentials.
6. Click **Test Windows Credential** to ensure the correct credentials are entered. The test only applies to Windows credentials. The test is not to verify access to target assets.

You can store credentials to reuse later. For more information, please see "Add Credentials for Use in Scans" on page 65.

7. Click the pencil icon.
8. Click **Add**.
9. Select the **Credential Type**.
10. Enter the **Username**, **Password**, **Description**, and **Key**.
11. Click **Save**.
12. If you are creating more than one credential, you can use the same confirmation key for all credentials. Select the **Use the same key for all** check box in the **Credentials Management** dialog, and then enter the key.
13. Select the new credential, and then click **OK**.
14. Expand **Report Delivery** to select the report delivery options.
    - **Export type:** Select a report format: **PDF**, **DOC**, **XLS**, or **NONE**. The export types available depend on the report selected.
    - **Do not create a report for this vulnerability scan:** Select this option if you want to only scan and collect the results. No report will be generated.
    - **Notify when complete:** Select the check box and enter email addresses. Separate entries using a comma. Alternatively, click + and select users or user groups. Email notification is sent when the scan and report are complete.
    - **Email report to:** Select the check box and enter email addresses. Separate entries using a comma. Alternatively, click + and select users or user groups. The report will be emailed to the users entered.
    - **Include Scan metrics in email:** This option is only available for **All Audits Scan**, **PCI Compliance Report**, and **Vulnerabilities Report**. Select this check box to have certain scan metrics included in the email, such as: number of exploitable, high, medium and low vulnerabilities, number of hosts scanned, number of targets with no response or access, start time, end time, duration, scanner version, audit group, port group, and address group. User must have read and write access set on the **Scan - Report Delivery** permission to be able to select the **Report Delivery** options on a scan.
15. Expand **Advanced** to select the agent to run the scan.
    a. **Job Name:** Type a job name. Otherwise, the default job name is used.
    b. **Agent:** Select the computer where the BeyondInsight resides.
    c. **Use job-specific Scan Restrictions:** Check the box to display a scheduling grid. Click the squares to set the restricted time frame. Scans will not run during those times.
    d. (Benchmark Scans only) **Store OVAL Test in database:** Check the box to store OVAL test results to the database.
16. Expand **Schedule** to select a schedule:
    a. **Immediate:** Select to run the job now.
    b. **One Time:** Select to schedule jobs to run one time. Select the start time and date.
    c. **Recurring:** Select one of the following:
    d. **Daily:** Schedules jobs for weekdays, or every x number of days. Enter the number of days.
    e. **Weekly:** Schedules jobs every week selected (1-52), starting on the day of the week selected.
    f. **Monthly:** Schedules jobs for the day of the month selected for every month selected. Options include the first, second, third, fourth, or last day of the month selected.

***Note:** If the server and client computers are located in different time zones, the scan runs during the server time zone. This applies to one-time scans and recurring schedules.*

> You can delete or change the recurring scan job later on the **Jobs** page. For more information, please see "Manage Jobs" on page 92.

17. Check the **Use the time zone of selected scanner** box if you want to use the time zone where a remote BeyondInsight resides.
18. Select **Abort the scan if it takes longer than**, and enter the time (in minutes) to restrict the length of time the scan runs.
19. Click **Start Scan**.
20. Click **Show Status** to view the progress of the scan. You can also view the progress on the dashboard or through the **Jobs** page.

Malware Toolkit Vulnerabilities

A malware toolkit can be detected if there is one associated with a vulnerability.

1. Select **Assets > Legacy Assets View > Vulnerabilties**.
2. Select a vulnerability, and click **i**.
3. A red **T** indicates if the vulnerability is associated with a malware toolkit.
4. Click **View Toolkits**.
5. Review more information about the malware toolkit and the recommended mitigation action.

Edit Scan Settings

The following scan settings can be set when you are configuring an audit scan:

- **Audits:** An audit contains the vulnerabilities and risks you can search for on selected assets. The audit information is organized in audit groups. The audit groups provided are industry standard and include: **SANS20(All)**, **SANS20(Windows)**, and **Zero-day**.

For a complete list, please see "Manage Audit Groups" on page 79.

- **Ports:** Select the port or port group ranges to include in the scan.
- **Options:** Select scan policy options, advanced options, and remote agent settings.

To configure an audit scan, follow the steps.

1. Select **Scan**.
2. Click the **Manage Report Templates** link.
3. Select the report, and click the arrow to display the menu.
4. Select **Edit Scan Settings**.
5. Select **Audits**, and then drag an audit group to the **Scan Settings** pane.
6. To search for an audit group, type the audit group name in the search.
7. Select **Ports**, and then drag port groups to the **Scan Settings** pane.
8. To search for a port group, type the port group name in the search.

For more information, please see "Manage Port Groups" on page 81.

9. Select **Options**.
10. Expand **Scan Policy Options**, and select the scan options:
    - **Perform OS Detection:** Determines the operating system for the target.
    - **Get Reverse DNS:** Scans for reverse Domain Name System (rDNS) and retrieves the domain name for the target IP address.
    - **Get MAC Address:** Scans for the Media Access Control address or unique hardware number.
    - **Perform Traceroute:** Determines packet routes across an IP network.
    - **Enumerate [parameter] Via NetBIOS:** Uses the NetBIOS protocol to determine and list audits specified in the Audit Group. The parameters include **Registry**, **Users**, **Shares**, **Files**, **Hotfixes**, **Named Pipes**, **Machine Information**, **Audit Policy**, **Per-User Registry Settings**, **Groups**, **Processes**, and **User and Group Privileges and Software**.
    - **Maximum Number of Users to Enumerate:** Sets a maximum number of users for providing detailed descriptions. All users are enumerated if you set the value to **0**.
    - **Hardware:** Determines the hardware for the target.
    - **Perform Web Scanning:** Scans remote web servers and audits installed applications.
    - **Web Scan Depth:** Sets the number of links to follow from the home page.
    - **Perform Database Application Scanning:** Scans remote database instances.
    - **Scan Docker Images:** Scans Linux or Windows host systems running Docker and hosting Docker images.

11. Expand the **Advanced Options** and select the scan options

> ***Note:*** *Performance issues may be experienced when running a Connect Scan, Force Scan, and UDP Scan simultaneously. These instruct the scanner to negotiate a full connection to each port on each device. On a Class B network, you could be waiting for 65,535 devices to time-out on a minimum of 65,535 connections each.*

- **Enable Connect Scan Mode:** Run if other methods, such as a slow dial-up, are unreliable. The operating system is negotiating a full connection to each device. Because multiple port scanning methods are not used, the scanner cannot determine a number of items, such as operating system.
- **Enable Force Scan:** Run if the targeted devices are not going to answer SYN or ICMP scanning. This forces the scanner to run protocol discovery on each port of each device to determine the protocol. Only use this in a highly locked down network where the standard port scanning methods will be filtered or blocked. **Force Scan** should not be used in IP ranges.
- **Extended UDP Scan:** Runs a complete scan on all User Datagram Protocol (UDP) frames without timing out. Forces the scanner to expect an answer. The IP will eventually timeout.
- **Disable Tarpit Detection:** Stops tarpit detection. A TCP tarpit program intentionally reduces the size of data packets to slow communication transmissions. This can cause incorrect scan results. To scan systems running tarpits, set the tarpit to allow unimpeded connections from the scanner.
- **Detailed Audit Status:** Retrieves data on the port, operating system and protocol scanned and details the vulnerabilities open, fixed and not verified.
- **Randomized Target List:** Uses a random list of target assets to scan rather than a sequential list of IP addresses. This load balances the target IP list across the network by distributing the target list across subnets rather than running all the targets in a subnet at the same time sequentially.

12. Expand **Network Security Scanner Local Scan Service Options** to set the following:

- **Perform Local Scanning:** Deploys a remote scanner to target assets during a scan or to run WMI and remote registry scans. After the scan runs, the deployed remote agent is removed from the asset.
- **Enumerate Ports via Local Scan Service:** Enumerates local ports using netstat, including active connections and the program or service using the port.
- **Enable WMI Service:** Starts and stops the WMI service. The service is only active during the scan.
- **Enable Remote Registry Service:** Starts and stops the remote registry on a target. The service is only active during the scan.

13. Click **Update**.

Target Requirements for all of the above options:

Windows Platform

All currently supported Windows Workstation and Server platforms.

Firewall Settings

RLSS requires that **TCP 445** (Microsoft-DS SMB file sharing) or **TCP 139** (NetBIOS Session Service) be open on the scan target. These are standard file sharing ports and are open by default on most versions of Windows. Once connected, the Network Security Scanner will communicate with RLSS over this port. All sessions are originated from the scanner, so there are no inbound port requirements on the host machine.

Write access to the ADMIN$ share of the target

When RLSS is deployed, it must first copy the service executable eeyelss.exe to the **%systemroot%** folder of the target. If the **ADMIN$** share is not available or the **SYSTEM** account does not have modify, read, or execute privileges, deployment will fail and RLSS will not be available. Agent deployment can also fail if antivirus software is active and has restricted the rights to the **%systemroot%** folder.

Permissions to remotely create and control a service

Once RLSS is copied, the scanner uses **Service Control Manager (SCM)** API calls to create a service entry, set the service permissions, and start the service. The service name is Local Scan Agent and will appear in the target's console. The service runs in the security context of the credentials used to scan the target and is configured with the **AutoStart** attribute. In the event that the service cannot be started, the scanner will restore the target to its original state.

Manage Audit Groups

BeyondInsight ships with audit groups that are populated with audits. Each audit group has a preconfigured set of audits. On the **Scan Settings** page for an audit group, you can:

- Change the audits in the audit group
- Create an audit group
- Copy an audit group
- Create an audit.

Available Audit Groups

- Access Scan
- Databases
- Domain Controllers
- FDCC-Windows XP
- Mail Servers
- SANS20 (All)
- SANS20 (Unix)
- SANS20 (Windows)
- Third Party Patch Assessment
- Virtualization
- Zero-Day

Regulatory Reporting Pack Audit Groups

- COBiT Compliance
- HIPAA Compliance
- ITIL Compliance
- NERC/FERC Compliance
- PCI Compliance
- SOX Compliance
- GLBA Compliance
- HITRUST
- ISO-27002 Compliance
- Mass 201 CMR 17 Compliance
- NIST 800-53 Compliance

For more information, please see "Create a Custom Audit" on page 82.

Revert the settings to the default values

> ***Note:*** *You cannot delete an audit group that ships with BeyondInsight.*

1. Select **Scan**.
2. Click the **Manage Report Templates** link.
3. Select a report, and click the arrow to display the menu.
4. Select **Edit Scan Settings**.
5. Select **Audits** in the **Settings** pane.
6. To search for an audit group, type the name in the search.
7. Click **Manage** in the **Audit Groups** pane to:
    - **Edit an audit:** Select the audit, and click the pencil icon. You cannot change all audits. Select **All Editable Audits** from the **Show** list to display all audits that you can change.
    - **Create an audit group:** Click **+** at the bottom of the **Audit Groups** pane. Enter the name of the new audit group.
    - **Copy an audit group:** Enter a name, and click **Copy**.
    - **Edit an audit group:** Select the audit group from the **Audit Groups** pane. You can also type the name of the audit group in the search for the audit group.
8. Check the **Automatically enable new audits in this group** box to add all the new audits.
9. Click **Revert** to revert to either the last saved version of the selected audit group or the default value.
10. Click **Update**.

Export an Audit Group

You can export an audit group and all audits associated with that audit group, including custom settings for an audit.

1. Select **Configuration > Discovery and Vulnerability Management > Audit Manager**.
2. In the **Audit Groups** pane, click the **Export an audit group** icon.
3. Click **Yes** on the **Save Export** dialog.
4. Select the location for the file, and then click **Save**.

Import an Audit Group

In the import, you can choose to overwrite the audit group or merge with an existing audit group. The version you export from must match the version for the install you are importing to. Verify the version from the **About** menu.

> ***Note:*** *If you decide to merge audit groups, the settings on the group you are importing takes precedence over the existing group.*

1. Select **Configuration > Discovery and Vulnerability Management > Audit Manager**.
2. In the **Audit Groups** pane, click the **Import an audit group** icon.
3. You must select whether to merge or replace an audit group.
4. Select the export file, and then click **Open**.

Manage Port Groups

Port groups contain the list of ports to scan. You can change the ports assigned in a port group, add port groups that will be available to all audit scans, and delete port groups.

BeyondInsight ships with port groups already configured with a range of ports (for example, HTTP Ports and Discovery Ports). Note that you cannot delete a port group that ships with BeyondInsight.

1. Select **Scan** .
2. Select the **Manage Report Templates** link.
3. Select the report, and click the arrow to display the menu.
4. Select **Edit Scan Settings**.
5. Select **Ports** in the **Settings** pane.
6. Click **Manage** in the **Port Groups** pane to:
    - **Add a port group:** Click **+** on the **Port Groups** pane. Enter the name of the port group, and click **Create**.
    - **Edit a port group:** Select the port group from the **Port Groups** pane. Type the name of the port group in the box to search for and display the port group.
    - **Remove a port from a group:** Select the port, and then select **Clear** from the **Protocol** menu.
    - **Add a port or group of ports:** Select the ports, and then select the protocol from the list: **Both**, **TCP**, **UDP**. The grid is updated with the corresponding color of the protocol.
7. To select multiple ports, drag and click on the range. Alternatively, enter the port number or port number range in the **Select Ports** box, and click the arrow.
8. Click **Revert** to cancel your changes.
9. Click **Update**.

Create a Custom Audit

You can create an audit that addresses particular risks or vulnerabilities that you want to protect your assets from. You can select the rule category, risk level associated with the rule, and the audit type and details.

1. Select **Scan** from the menu.
2. Select the **Manage Report Templates** link.
3. Select the report and click the arrow to display the menu.
4. Select **Edit Scan Settings**.
5. Select **Audits** in the Settings pane.
6. Click **Manage** in the Audit Groups pane.
7. Click +**New Audit** to start the Audit wizard.
8. Click **Next**.
9. On the **Audit Description** page:
    - Type the audit name.
    - Select the audit category, such as **Database**, **Mail Servers**, **Miscellaneous**, or **Windows**.
    - From the **Risk Level** list, select the severity level that corresponds to the severity of the vulnerability:

      High: Risks that allow a non-trusted user to take control of a susceptible host.

      Vulnerabilities that severely impact the overall safety and usability of the network.

      Medium: Risks that are serious security threats and would allow a trusted but non-privileged user to complete control of a host or would permit a non-trusted user to disrupt service or gain access to sensitive information.

      Low : Risks associated with specific or unlikely circumstances. These vulnerabilities can provide an attacker with information that could be combined with higher-risk vulnerabilities to compromise the host or users.

      Information - Host information that does not necessarily represent a security threat, but can be useful to the administrator to assess the security. These alerts are displayed with the list of vulnerabilities.
    - Describe the vulnerability.
    - Describe how to remediate, investigate, or mitigate the vulnerability.
10. On the Audit Type page, select the type of audit:
    - **Banner:** Determines vulnerabilities in the banner information, such as firewall name, IP addresses and server name.
    - **CGI Script:** Determines vulnerabilities in the common gateway interface that passes a Web user's request to an application program and to receive data back to forward to the user.
    - **Registry :** Detects vulnerabilities by scanning registry entries and values.
    - **Hotfix:** Determines vulnerabilities by scanning service packs, hotfixes and patches.
    - **File Version:** Determines if a file exists. The audit can check if the file exists or not.
    - **File Checksum:** Determines vulnerabilities based on file checksum comparisons.
    - Supported values include: MD5, SHA1, SHA256.
    - Network performance issues might occur if you use this feature. Use this feature with caution.
    - **Remote Check:** Verifies if a specific Unix program or patch is installed on an operating system.
    - **Mobile Software:** Determines if software exists for mobile devices.

- **BlackBerry Device** - Determines vulnerabilities based on BlackBerry device specifications.
- **Share:** Determines if a share is accessed by unauthorized users.

11. Enter the information for the audit type, and then click **Next**.
    - **Banner audit details:** Select the banner protocol, and then type the banner name.
    - **CGI Script audit details:** Type the URL path to the script name.
    - **Registry:** Select Path, Key, or Value from the menu. Select the operating systems that the vulnerability affects.
    - **Service Pack:** Hotfix - Determines vulnerabilities by scanning service packs, hotfixes and patches.
    - **File Version:** Verifies the software version. Enter the file name. Set file version information (optional), and select operating systems to check.
    - **File Checksum:** Select the file checksum from the list. Enter a file name, checksum value, and file version. Use an asterisk to compare all file versions.
    - **Remote Check:** Verifies if a specific Unix program or patch is installed on an operating system.
    - **Mobile Software:** Enter the name of the software, and set if software exists. Can also audit on the version number.
    - **Share:** Select user account access on the share, type of access on the share, and OS version. Optionally, list the accounts by SID.
12. On the **Vulnerability Details** page, enter the BugTraq and CVE details, as needed.
    - **BugTraq :** A security portal dedicated to issues about computer security, such as vulnerabilities, methods of exploitation and remediation.
    - **CVE:** Common Vulnerabilities and Exposures is a dictionary of publicly known information security vulnerabilities and exposures. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.
13. On the **Audit Wizard Summary** page, click the pencil to change the audit information.
14. Click **Finish**.

Review Vulnerability Scan Results

After you run vulnerability scans you can review the results to determine the assets that are vulnerable and require remediation. The scan results include the following key details about a particular vulnerability (if the information is available):

- Audit ID
- CVE IDs
- CWE IDs
- Microsoft Bulletin ID
- CVSS Score - includes CVSS v2 and CVSS v3
- Ports
- Mitigation

You can view vulnerabilities that can be exploited. For any vulnerability with a CVE-ID, exploit information associated with the CVE-ID is also displayed. In some cases, exploits are displayed that are not associated with a CVE-ID. The Microsoft Exploitability Index is also included in the exploit information. The index values correspond to the values that are provided in security bulletins issued from Microsoft.

For more information on interpreting the index values, please see Microsoft's documentation.

You can set display preferences and create filters to change the information displayed on the **Vulnerabilities** page. For more information, please see "Change and Set the Console Display and Preferences" on page 17.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Vulnerabilities**.
4. Click to expand the **Vulnerabilities** pane.
5. You can create smart rules based on vulnerabilities. Using this tool can provide additional filtering for selected assets.
6. Click **i** to view more information about a vulnerability.
7. On the **Vulnerabilities Details** pane, select the following to review more information:
    - **Description:** View information about the vulnerability including a solution.
    - **Audits:** Lists the ID and name for the audits included in the scan.
    - **Exploits:** The number indicates the exploits on the vulnerability. Review the database, module, and module URL.
    - **References:** The number indicates the available resources for remediation of the vulnerability. View the list of references. Select a website to find out more information on the vulnerability.
    - **Assets:** The number indicates the assets affected by the vulnerability. Review the asset information.
    - **Patches:** The number indicates the patches that can fix the vulnerability. Review more information about the patches.

For more information, please see "Patch Management Module" on page 158.

You can also set or remove an exclusion property on the vulnerability. For more information, please see "Exclude Vulnerabilities" on page 86.

Create a Quick Rule

After you run a scan, you can organize assets linked to a specific vulnerability, attack, or malware by creating a Quick Rule.

In the Attacks, Vulnerabilities, or Malware view, you can click the arrow to create a Quick Rule that instantly creates a grouping of assets in the Smart Groups pane.

Exclude Vulnerabilities

You can exclude vulnerabilities from the display to view those that require remediation to satisfy regulatory compliance.

Depending on your environment, accepted vulnerabilities might be reported in the scan. For example, if Anonymous FTP is configured on your network, vulnerabilities will be reported in your scan results. Since this type of vulnerability does not require remediation, patches, or compliance updates, you can ignore these scan results.

Records for exclusions reside in the database. During an audit, you can remove the exclusion on the record. You can run the **Vulnerability Exclusions Report** to keep track of the exclusions. The report includes the reason for the exclusion and the expiry date.

> In some situations, you might not want all of your users to set an exclusion on a vulnerability. You can set the permission Vulnerability Exclusions when creating a user group.
> For more information, please see "Create and Configure Groups" on page 22.

> ***Note:*** *Vulnerability exclusions do not apply to the parent smart group when the exclusion is set at a child smart group.*

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Vulnerabilities**.
4. Check the **Exclusions** box on a vulnerability.
5. On the **Manage Vulnerability Exclusion** dialog, select the options:
   - **Action:** Select to set or remove the exclusion.
   - **Exclude Vulnerability:** Select the smart group where you want to apply the exclusion. You can also select **Globally**, and the exclusion will apply to all assets.
   - **Reason/Note:** Provide a detailed description on why the vulnerability was excluded. For example, you might want to note that the vulnerability is an accepted false positive. The reason is required and is displayed in the Vulnerability Exclusions Report to help you keep track of the exclusions.
   - **Expiration Date:** Select the expiration date on the exclusion.
6. Click **Save**.

Edit Exclusion Properties

You can change the following properties for an exclusion: **Scope** and **Reason**. You can change the properties without having to create a new exclusion. Click the pencil icon to change the settings. All of the exclusions set on the vulnerability are listed.

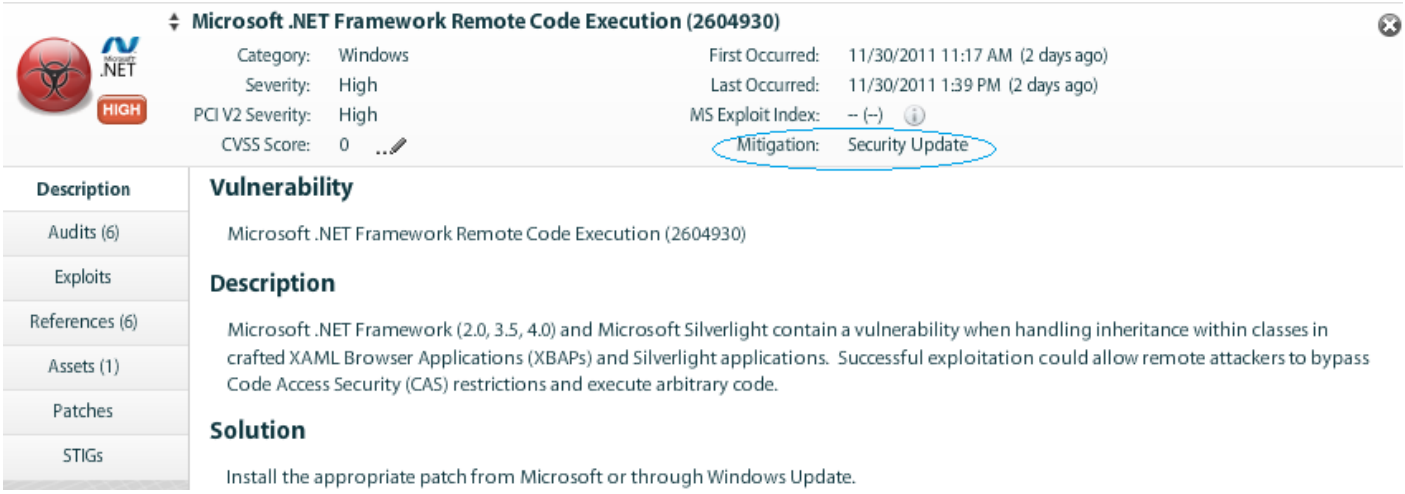
> ***Note:*** *You cannot change the expiration date.*

Remediate Vulnerabilities

You can remediate vulnerabilities by viewing solutions on the **Vulnerability Details** page.

> You can use the ticket system to assign a vulnerability to a member of your security team. For more information, please see "Work with Tickets" on page 117.

1. Select **Assets**.
2. Click the **Legacy Assets View**.
3. Click **Vulnerabilities**.
4. Click **i** on the vulnerability.
5. A description and solution are displayed. The **Mitigation** column provides information on the action to take to remediate the vulnerability.



Set Metrics

Depending on your security plan, you might want to change CVSS scores. Changing the score indicates to your security team the urgency to remediate a vulnerability.You can change the base and temporal values to change the CVSS score, depending on the weight of the vulnerability and the urgent nature to remediate the vulnerability.

- Environmental scores using the Smart Rules Manager.
- Base and temporal scores using the Vulnerability Details page.

> ***Tip:*** *You can view CVSS version 2 and CVSS version 3 in the console. You must be familiar with CVSS scoring definitions and concepts. Please see Common Vulnerability Scoring System SIG.*

Set CVSS Environmental Metrics

The environmental metrics are based on your security plans. Determine the level of impact a vulnerability has on your assets and assign environmental metrics accordingly. You can create a Smart Group that includes the assets you want to assign the environmental metrics.

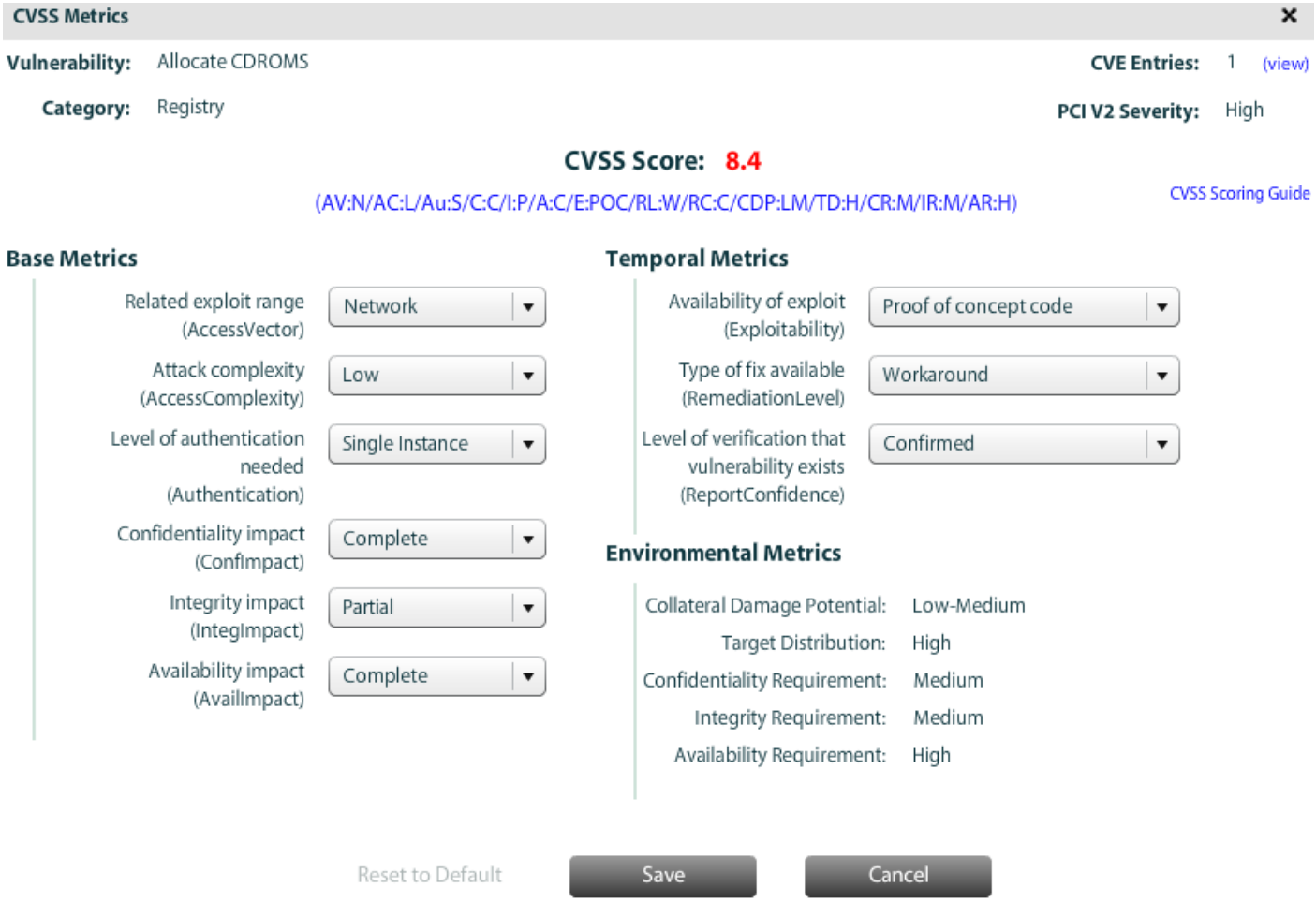
1. Select **Assets**.
2. Click the **Lecacy Assets View** link.
3. In the **Smart Groups**pane, click **Manage Smart Rules**.
4. Click **New** .
5. Enter a name and description, and set the smart rule criteria that determines the scope of the assets.
6. In the **Perform Actions** area, select **Set Environmental CVSS Metrics**.

7. Select the metrics from the corresponding lists.
8. Click **Save**. When you edit the smart group, the **Show asset as Smart Group** list is also displayed.

Set Base and Temporal Metrics

After you create a smart group that contains the assets with the preferred environmental metrics, you can update CVSS scores on the **Vulnerabilities** page.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Select the smart group with the environment metrics configured.
4. Select **Vulnerabilities**.
5. Select a vulnerability, and then click **i**.
6. Click the pencil.
7. Change the base and temporal values. The CVSS score and CVSS vector change as you change the base and temporal metrics.
8. Click the vector link to go to the **National Vulnerability Database CVSS v.2 Calculator** website.
9. Click **Save**.



Run Web Application Scans

Web Application Scanning includes these additional scan components:

- Web form authentication
- Performance settings
- Basic XSRF
- HTTP authentication brute force
- JavaScript crawling
- Whitelist/blacklist URLs
- Automatic form population
- HTTP response splitting.

To create a web application scan job, follow the steps.

1. Select **Scan**.
2. Scroll down to the **Web Application Scans** templates.
3. Select **Web Application Vulnerability Report**.
4. Click **Scan**.
5. In the **Target Selection** area, enter a URL to include in the audit. Additionally set the following:
    - **Max Links** - Enter the maximum number of links to crawl. The default is 5000 and the upper limit is 1000000.
    - **Maximum Directory Depth** - Enter the number of links to follow from the home page. The default is 10.
    - **Maximum Runtime** - The number of minutes within which the web scan must run. The lower limit is 0(which uses the default of 120) and the upper limit is 1440.
6. In the **URL Restrictions** section, set URL restrictions for the scan. Enter one or more regular expressions against which URLs will be matched. If a URL matches one or more of the regular expressions, the URL is skipped. Generally, the types of strings entered are those that match URLs associated with logging out or significantly changing the web application's state.
7. In the **Credentials Management** section, check the **Form Authentication Required** box, and enter the credentials.
8. The **Report Delivery**, **Advanced**, and **Schedule** settings are the same as when configuring a vulnerability scan.

For more information, please see "Run Vulnerability Scans" on page 73.

9. Click **Start Scan**.

Run Docker Image Scans

BeyondTrust Network Security Scanner and Host Security Scanner versions 6.5 or greater can scan Linux or Windows host systems running Docker and hosting Docker images. The Docker assets can be viewed in the new assets grid or the resulting report. The Docker image scan settings are the same as a typical audit scan.

1. Select **Scan**.
2. Scroll down to the **Docker Image Scans** templates.
3. Select **Docker Image Report**.
4. Click **Scan**.
5. Complete all areas of the form, and then click **Start Scan**.

All sections of the form are required. Only scanners with version 6.5 or higher are listed under **Advanced**. The **Report Delivery**, **Advanced**, and **Schedule** settings are the same as when configuring a vulnerability scan. For more information, please see "Run Vulnerability Scans" on page 73.

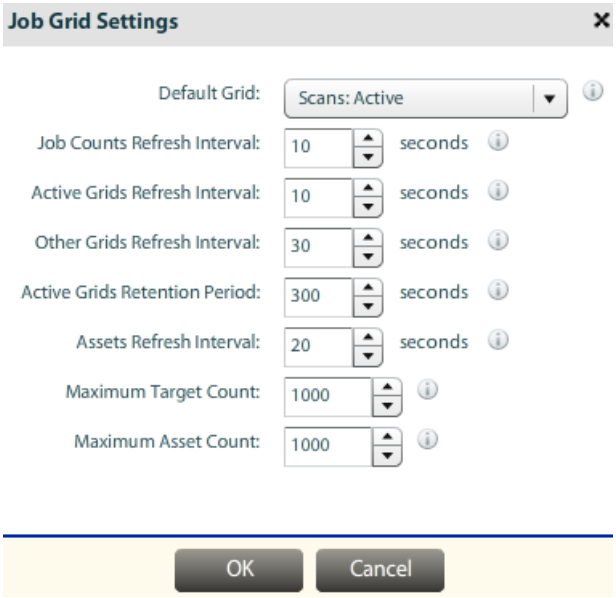
Manage Jobs

On the **Jobs** page, you can view:

- Active, scheduled, and completed scan jobs
- Active and completed protection agent deployments
- Active, scheduled, and completed reports
- Sheduled scans and scheduled reports
- SCCM package deployment status
- Windows event details

Configure Job Page Settings

1. Select **Jobs**.
2. Click the **Settings** icon to change display settings.
3. In the **Job Grid Settings** dialog, you can configure the default job type, refresh intervals, and the maximum number of assets displayed on the page.



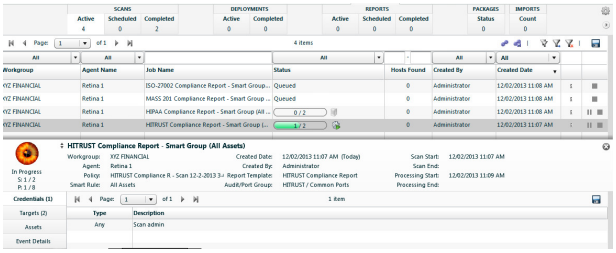
Review Job Details

On the **Job Details** page, you can view the number of assets scanned, the number of processes successfully scanned, credentials used for the scan, and the assets scanned.

A target is defined in a scan as a combination of a single IP address, a computer name, a list of IP addresses, a list of computer names, an IP range, and cloud devices. An asset is a device discovered from the range of targets defined in the scan. The agent name indicates if the scanner is in a scanner pool.

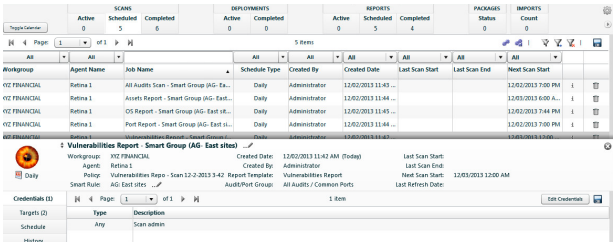
For more information, please see "Use Scanner Pooling" on page 151.

1. Select **Jobs**.
2. Click **Active**, **Scheduled**, or **Completed** in the **Scans** section.
3. Double-click a job to open its details.



> ***Note:*** *You can review the job details while the job is in progress.*

You can change the following settings for a scheduled job:



- Job name
- Smart Rule
- Credentials
- Schedule

The **Last Refresh Date** indicates the date when the smart rule was processed. Assets added or removed after the last refresh date are not reflected in the smart rule.

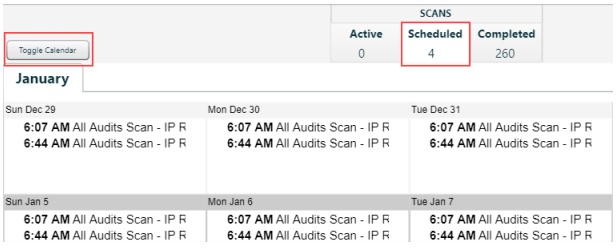
Smart rules are processed every 6 hours. Depending on the schedule and how frequently assets change in your environment, you might want to change the refresh rate. Otherwise, assets might not be included in the scan as you expect.

> For more information, please see "Discovery and Vulnerability Management Options" on page 145.

View Scheduled Scans in the Calendar View

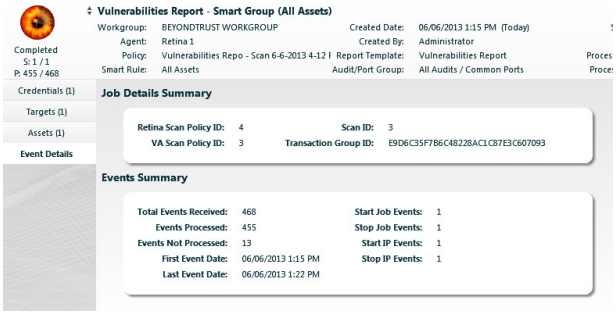
You can view scheduled scans in a calendar that shows a summary of the scans scheduled for the month.

1. Select **Jobs**.
2. Click **Scheduled** in the **Scans** section.
3. Click **Toggle Calendar**.



View Scan Event Details

1. Select **Jobs**.
2. Click **Completed** in the **Scans** section.
3. Double-click a scan to open its details.
4. Select the **Event Details** tab to view a summary.



View a Report for Completed Scans

1. Select **Jobs**.
2. Click **Completed** in the **Scans** section.
3. In the **Report** column, click the icon to open a report for a completed job.

Set a Scan to Complete

To see this setting, you must be a BeyondInsight administrator or have the **Full Control** permission on the **Scan Management** feature assigned to your group. The setting is available only if there is at least one start job or one stop job event.

Go to the **Event Details** page on the **Jobs** page.

Click **Set Scan to Complete**.

IMPORTANT!

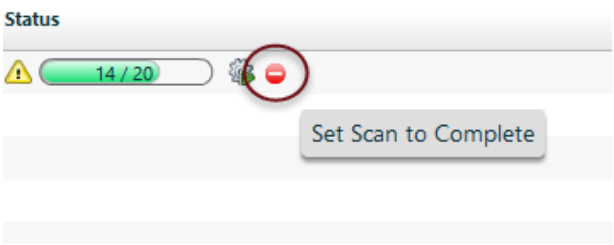
If a scan has stopped running and it is set to complete, data that has already been collected might be lost.

Troubleshoot Issues With a Scan Job

You can determine if a scan job is idle on the **Jobs** page. If the scan job is idle, you can stop the scan. In this scenario, scan data will not be usable, and some data might be lost.

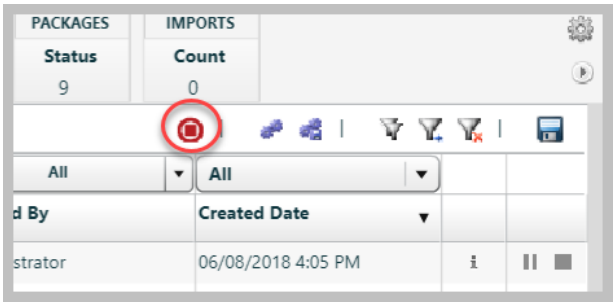
If there has been no action on the scan for at least 24 hours, the **Alert** icon is displayed.

1. Select **Jobs** from the menu.
2. Click the **Alert** icon.
3. On the dialog, click **Set Scan to Complete**.



Pause or Abort a Job

Select the respective icons to abort or pause a job. You can also stop all jobs that are actively running by clicking the stop all jobs icon as shown.



> ***Note:*** *The* ***Stop All Jobs*** *icon displays only if there are jobs actively running. When clicked, it aborts jobs in a state when it can be stopped. Any job pending or not yet actively running is not cancelled.*

Stopped jobs will be moved to the **Scans** section on the **Completed** tab with a status of **Aborted**.

> ***Tip:*** *This feature does not apply to host scanners.*

Manage Reports

There are two report template types available:

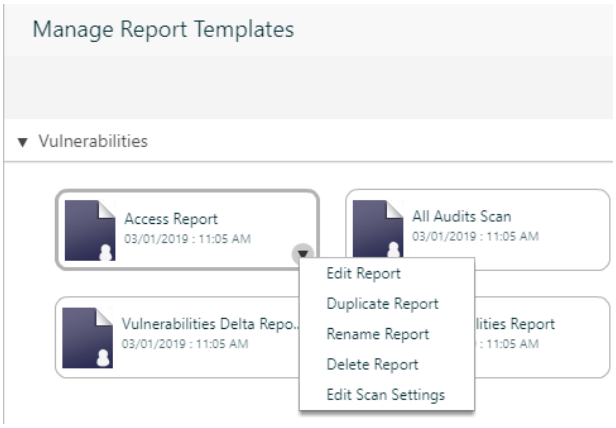
- Scanning only
- Scanning and running reports on existing data

For more information, please see "Run a Report" on page 105.

Report Templates

You can customize template settings, including sections in the report output and scan settings.

1. To access a report template, select **Scan**.
2. Click the **Manage Report Templates** link.
3. Select a report template, and then click the arrow to select a menu item.
    - **Edit Report**
    - **Duplicate Report**
    - **Rename Report**
    - **Delete Report**
    - **Edit Scan Settings**



The following tables list the report templates available with BeyondInsight You can run reports on existing scan information that is stored in the BeyondInsight database.

You can run all reports from BeyondInsight Analytics and Reporting. For more information, please see the *BeyondInsight Analytics & Reporting Guide*.

Vulnerabilities

Report Name	Description
Access	Lists targets that are inaccessible. Includes a reason and job metrics details such as, agent name that ran the scan, credentials, and scan duration.
All Audits Scan	Lists all vulnerabilities found. Review information such as fixes, references, exploits, and affected assets.

Report Name	Description
PCI Compliance Report	Details the vulnerability results of PCI security scans. ***Note:*** *Payment Card Industry Data Security Standard (PCI DSS) specifies security requirements for merchants and service providers that store, process, or transmit cardholder data. PCI Security scans are conducted over the Internet by an Approved Scanning Vendor (ASV).* ***Note:*** *The Retail Report pack is required for this report.*
Vulnerabilities - Personally Identifiable Information	Lists vulnerabilities based on the Personally Identifiable Information audits. Includes personal and financial information.
Vulnerabilities - VMware Security Hardening	Lists vulnerabilities based on the VMware Security Hardening audits. The audits adhere to the VMware Security Hardening Guides to ensure that your VMware assets are secure.
Vulnerabilities by Reference	Lists vulnerabilities by CVE reference ID. View information such as assets affected and potential fixes.
Vulnerabilities Delta	Provides the vulnerability differences between two scans.
Vulnerabilities	Lists vulnerabilities grouped by assets. The report details the vulnerabilities with criticality, including descriptions, fix information, and references. The references provide a link to the CVE website. You can run custom or standard reports to review the system, users, and any security issues.
Vulnerability Exclusions	Lists vulnerabilities that are set to exclude. Includes the expiry date and reason properties.
Vulnerability Export	Provides a tabular list of all vulnerabilities discovered and their associated details.

Attacks

The Attacks report uses information gathered by the protection agents.

Report Name	Description
Attack	Displays the total number of attacks, attacks per asset, assets attacked, attacker IP address, a list of the top *x* attacks, criticality and trends over time. View information such as action, port, protocol, and attacker.
Malware	Displays the total number of malware attacks, a list of the top *x* malware attacks, trends over time, and assets affected. View information such as location of the malware, asset and IP address, etc.

Assets

Delta reports are useful for comparing changes such as the addition and removal of user accounts, software, or OS upgrades.

Report Name	Description
Asset Export	Displays assets in a selected scan in a .csv format. Information includes: the asset name, IP address, DNS, domain and operating system.
Assets	Provides asset and risk information by hardware, MAC address, operating system, port, process, services, share and user account.
Discovery Report	Displays discovery information based on the selected scans. You can select more than one scan to report on. ***Note:*** *You can include assets that are unreachable.*
Discovery Scan	Lists the targets found on the network, including: workstations, routers, laptops, printers. Credentials are not required for a discovery scan.
OS Delta	Displays the differences in operating systems between two scans.
OS	Lists top 100 and bottom 100 discovered operating systems. Assets are grouped by OS, IP address, asset name, DNS name and risk.
Port Delta	Displays the port differences between two scans.
Port	Lists top 100 and bottom 100 discovered ports for the assets included in the scan. Assets are grouped by OS, IP address, asset name, DNS name and risk.
Service Delta	Details the service differences between two scans.
Service	Lists top 100 and bottom 100 discovered services for the assets included in the scan. Assets are grouped by OS, IP address, asset name, DNS name and risk.
Share Delta	Displays the shares differences between two scans.
Share	Provides a summary of top and bottom shares and a breakdown by IP address, asset name, DNS name, operating system and criticality.
Software	Lists top 100 and bottom 100 discovered software for the assets included in the scan. Assets are grouped by OS, IP address, asset name, DNS name and risk.
Software Delta	Displays the software differences between two scans.
User Delta	Lists the number of new, unchanged and removed users. Review a summary of the user updates.
User	Lists top 100 and bottom 100 discovered users for the assets included in the scan. Assets are grouped by OS, IP address, asset name, DNS name and risk.
Windows Events Report	Lists Windows event types based on your selection: Application, System, Security. Protection agent module required.

Executive Overview

Report Name	Description
Executive Summary	Provides an overview summary of assets and trends, such as audits by machine and audits by severity.

Patches

Report Name	Description
Patches	Lists the assets included in the scan and the number of patches that need to be applied to each asset. Lists each patch available and includes a link to more information for the patch. Each patch also provides the name of the violated audit. ***Note:*** *Collects data on Windows assets only.*

Hardware

Report Name	Description
Hardware Delta	Lists a summary of hardware differences between two scans. Review differences.
Hardware	Lists the hardware discovered on each asset included in the scan.

Regulatory Compliance

Report Name	Description
COBiT Compliance	Provides a report that ensures your environment satisfies the framework identified in the COBiT framework. (Additional Component) Any report pack.
FERC-NERC	Maps monitored controls to NERC requirements. (Additional Component) Government report pack.
GLBA Compliance	Provides security risk assessments that satisfy the requirements in the GLBA. (Additional Component) Financial report pack.
HIPAA Compliance	Maps configuration, patch and zero-day vulnerabilities to HIPAA security rules. ***Note:*** *Running a scan using the default scan settings ensures compliance to Section 164.308 Administrative safeguards, (a)(8) Standard: Evaluation.* (Additional Component) Healthcare report pack.
HITRUST Compliance	Displays vulnerabilities mapped to HITRUST regulatory compliance standards. Supported sections from the standard and vulnerability counts are displayed.
ISO-27002 Compliance	Maps configuration, patch and zero-day vulnerabilities to satisfy ISO-27002. (Additional Component) Any report pack.
ITIL Compliance	Maps compliance violations and vulnerabilities back to ITIL best categories. (Additional Component) Any report pack.

Report Name	Description
MASS 201	Maps configuration, patch and zero-day vulnerabilities to MASS 201. (Additional Component) Government report pack.
NIST 800-53	Maps configuration, patch and zero-day vulnerabilities to NIST 800-53 standard used to support FISMA compliance. (Additional Component) Government report pack.
SOX Compliance	Maps configuration, patch and zero-day vulnerabilities to defined SOX requirements. (Additional Component) Retail or Healthcare report pack.

Protection

Report Name	Description
Protection Agent Configuration	Displays the policies applied on an asset. Protection agent module.
Protection Agent Version	Display detailed information about the protection agents including, computer installed on, version, when the agent was last updated.
Protection Policy Differences Report	Provides a summary of differences in a protection policy. You cannot run reports on existing data for the Protection reports. This report is intended to provide configuration information for your protection agent policies.

Configuration Compliance

Report Name	Description
Benchmark Compliance	Runs a benchmark scan based on a selected benchmark template and policy.
Benchmark Export	Provides a summary of differences in a benchmark policy.

Patch Management

(Additional components) Configuration Compliance module

Report Name	Description
Approved Patches	Lists assets where patches are approved.
Installed Patches	Lists installed patches.
Required Patches	Lists required patches.
WSUS Audits Report	Displays the data that is imported from WSUS.

Tickets

(Additional components) Patch Management module

Report Name	Description
Ticket Report	Displays details such as Status (Open, New, Closed), Severity, Assigned user, due date, ID, and ticket title.

Mobility

Report Name	Description
Mobile Assets	Lists mobile assets discovered.
Mobile Vulnerabilities	Lists vulnerabilities associated with mobile assets.

Endpoint Privilege Management

Report Name	Description
Application ActiveX Details	Displays information about installation events for ActiveX controls in Internet Explorer.
Applications by Computer	Displays information about application usage on a client.
Applications By Hash	Displays information about all applications under management tracked by hash code. Details include, hash code of the binary file, application name, file version, product name, and certificate publisher, etc.
Applications By Path	Displays information about all applications under management tracked by launch path.
Dashboard Report	Displays charts about the applications most frequently launched, requiring elevation, triggering User Account Control (UAC), launched by Shell rule. Also, charts about ActiveX controls, rules applied, local administrators, and the ratio of administrator users to standard users.
Detailed Discovery Scan	Enumerates Shares, Groups, Processes, User and Group Privileges, Hardware , Services, Software on PowerBroker for Windows assets.
File Integrity by Asset	Displays the assets managed using PowerBroker for Windows File Integrity rules.
File Integrity by Rule	Displays the assets organized by the PowerBroker for Windows rules.
Risk Compliance	Displays assets with risk compliance rules in place, group by vulnerabilities. Filter the report on rule name, application, path, and user.
Rule Justification	Displays the assets that have a justification that provides information on the reasons for elevation. Filter the report on rule name, application, path, and user.
Shell Rule Executions	Displays information about all applications that run based on a shell-rule.

Administrative

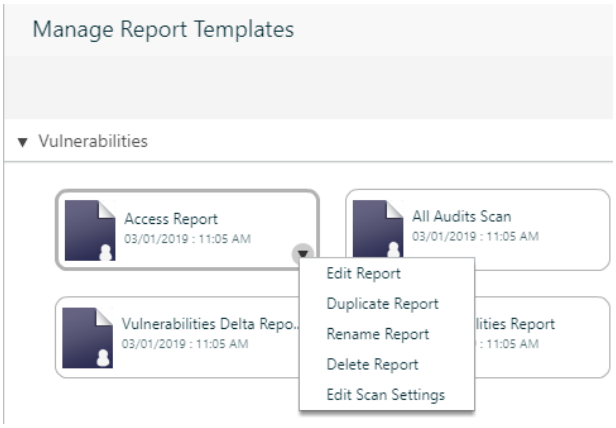
Report Name	Description
Password Safe User Licensing	Provides details on licensing for Password Safe.

Set Report Output Options

You can select the sections to include in reports, such as cover page and report content.

1. Select **Scan.**
2. Select the **Manage Report Templates** link.

3. Select a report, and click the arrow to display the menu.
4. Select **Edit Report**.



5. Select a report section.
6. For some reports, you can edit parameters on the Header section. Click the pencil icon to display and select the parameters.
7. The **Section Parts** pane displays the sections that you can use. Drag a section part into the middle pane. You can also enter the name of the **Section Parts** in the search.
8. To remove a section from the report, select the section, and select the garbage can.
9. Click **Save**.
10. Enter a name for the report and the report category.
11. Click **Save**.

Create a Report

You can create a report template based on an existing report template. A report template consists of:

- **Report output settings:** Select options to determine how information is presented in the report output. This includes report sections that present the information collected from the scan.
- **Scan settings:** Select options to determine the data to collect from assets. This includes audits, ports, and additional scan options that make up the scan.

Report templates are organized using report categories.

1. Select **Scan**.
2. Select the **Manage Report Templates** link.
3. Click **New Report**.
4. Select a template, and click **Create**
5. Select a section, and then drag section parts into the section pane. You can enter the name of the section part in the text box. Section parts vary based on the report template selected.
6. Check the **Shared** box if this report template can be used by other BeyondInsight users.
7. Click **Save**.
8. Enter the name of the report and the report category.
9. Click **Save**.

Create a Report Category

A report category is a container that helps to organize similar reports. Every report that you create must be assigned to a category.

1. Select **Scan**.
2. Select the **Manage Report Templates** link.
3. Click **New Report Category**.
4. Enter a name for the report category, and click **Create**.
5. Drag an existing report from another category to populate the new category.

Customize the Report Logo

You can change the logo that displays on management console reports.

1. Create your image. Make sure the size is 758 x 128 pixels.
2. Name the image reportlogo.jpg.
3. Copy the image to the following location in the BeyondInsight installation directory:
    - <Install Path>\eEye Digital Security\BeyondInsight\WebSite\images

The change occurs immediately. All new reports generated will use the new logo. Any downloaded reports will not change. Download the report again to include the new logo.

Run a Report

You can run reports on scan information that is stored in the BeyondInsight database.

You cannot run reports on existing data using the Protection reports.

> Create a smart group to scope the assets to include in the report. For more information, please see "Use Smart Rules to Organize Assets" on page 55.

Reports open in a new window. Make sure pop-up blockers are disabled for the management console website.

1. Select **Scan** from the left navigation.
2. From the **Smart Groups** pane, select the smart group.
3. Select a report, and then click **Report**.
4. Select parameters,

> ***Note:*** *The **NONE** export type provides a snapshot of the data and produces results faster than selecting the PDF output.*

5. By default, the **All** box is checked. Be sure to clear the box if you want to use specific parameters for your report. Selecting **All** uses all criteria available for that parameter.
6. Click **Run Report**.

Create Scheduled Reports

1. Set report parameters.
2. Click **Subscription**, and then set the following:
   - **Notify when complete:** Check the box, and enter email addresses. Separate entries using a comma. Alternatively, click **+**, and select users or user groups.
   - **Email report to:** Check the box, and enter email addresses. Separate entries using a comma. Alternatively, click **+** and select users or user groups.
   - **Schedule Type:** Select **One Time** or **Recurring**. If you select **Recurring**, select the frequency of the schedule run times.
3. Click **Save** after you enter the scheduling information.

View Scheduled Reports in the Calendar View

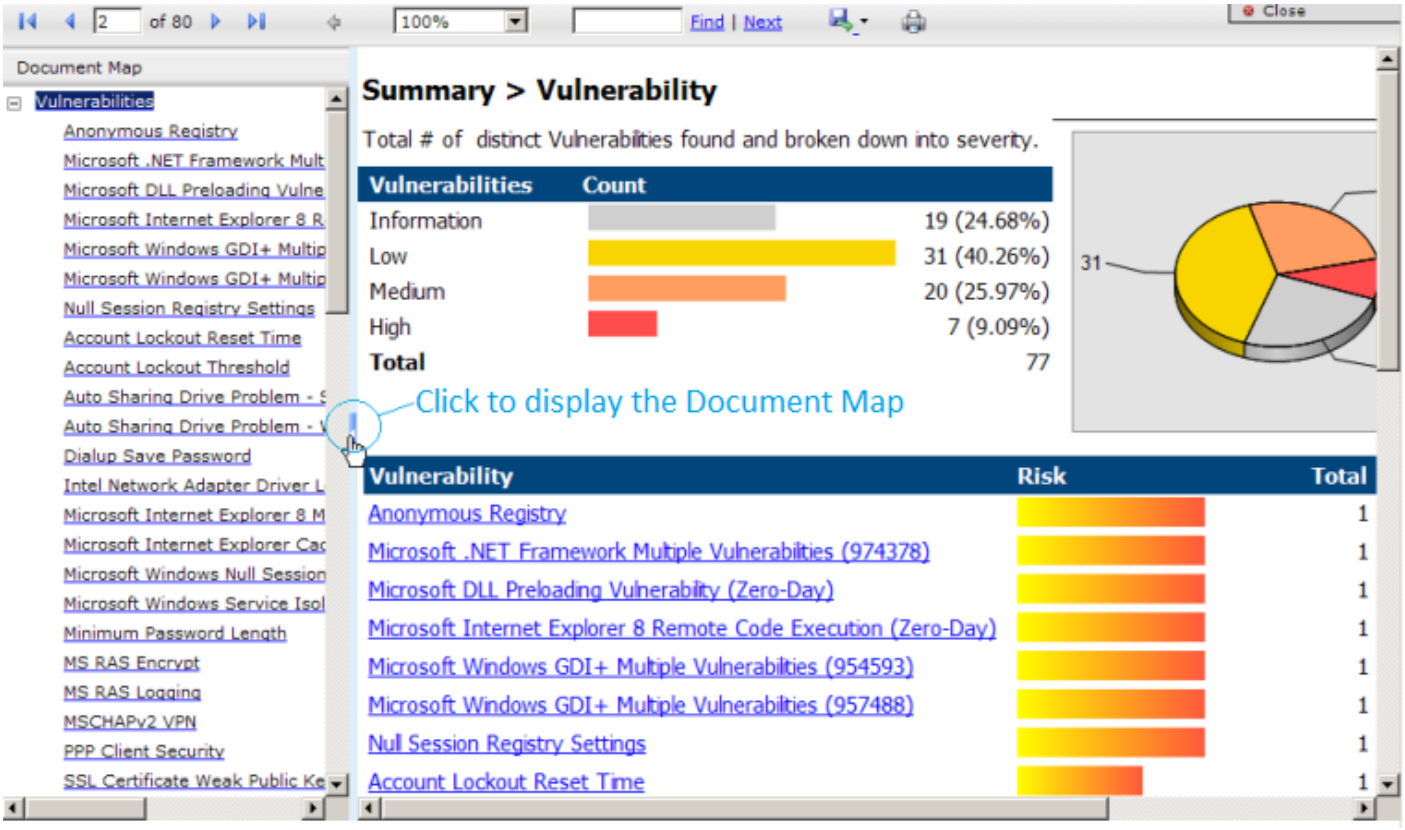
You can review the scheduled reports in a calendar that shows a summary of the reports scheduled for the month.

1. Click **Jobs**, and then click **Scheduled** in the **Reports** section.
2. Click **Toggle Calendar**.
3. Click the **Report** icon to open the report for a completed report.

Review Report Results

Expand the document map to view the list of vulnerabilities.

Click the link for the vulnerability in the document map list or in the main report. You can review more information about the vulnerability such as: description, fix information, references, and CVSS score.



If you export the report to PDF output, the list of vulnerabilities in the document map is displayed as bookmarks in the PDF.

View and Download Reports

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

- View reports
- Download a report to PDF format
- Access the Manage Report Templates page.

For more information, please see "Manage Reports" on page 97.

1. Select **Jobs**.
2. Select one of the following:
    a. Double-click a report to view it. Or, select a report, and then click **i**.
    b. Click the **Download** button, and then click **Save File** to save the report in PDF format.
3. Enter the report name, or use the default. Click **Save**.

***Tip:** Click the **Delete** button to delete the report.*

Manage Assets

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

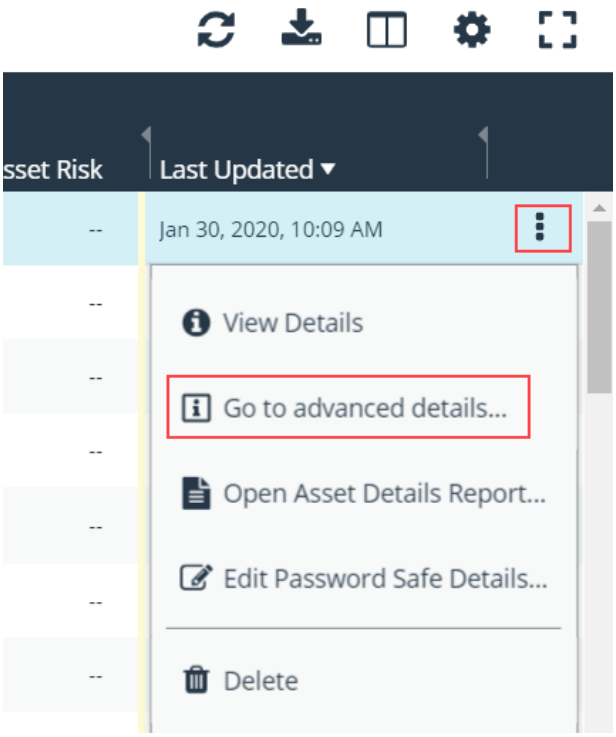
Review Asset Details

Tip: *Depending on the scan settings, information in the following list may not be detected and included in the scan results. If the following scan settings are turned on, more accurate scan results can be expected:* ***Perform Local Scanning****,* ***Enable WMI Service****, and* ***Enable Remote Registry Service.***

For more information, please see "Edit Scan Settings" on page 76.

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

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



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

General Data

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

Scan Data

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

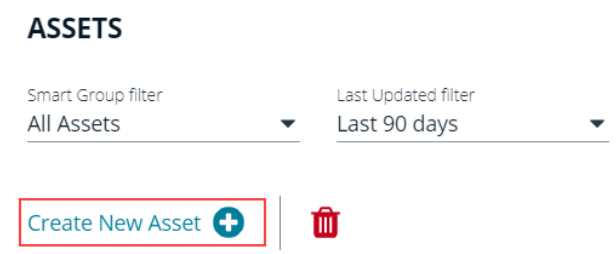
- **Certificates:** Displays all certificates installed on the asset. You can filter by expired certificates or search for certifcates.
- **Hardware:** Displays disk drive information, system manufacturer, memory, and processor information.
- **Ports:** Displays the open port number, protocol, and description.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

In addition to the asset properties, the scan includes information about attacks, malware, and detailed information about vulnerabilities on the legacy Assets page. Depending on additional modules you are using, the scan includes patch details, information for Endpoint Privilege Management events, Privilege Management for Unix & Linux event details, and File Integrity monitoring rule information. For more information, please see "Use the Legacy Assets View" on page 113.

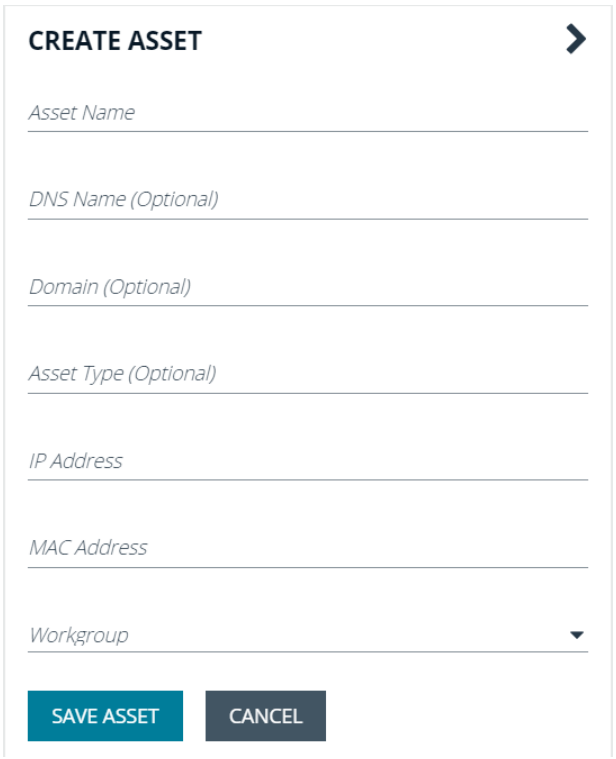
Create Assets

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

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



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



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

Change Asset Properties

You can use the **Asset** wizard to change the following asset properties, such as **Owner**, **Active**, and **Asset Attributes**. Also, you can assign or change attributes to help organize and identify assets.

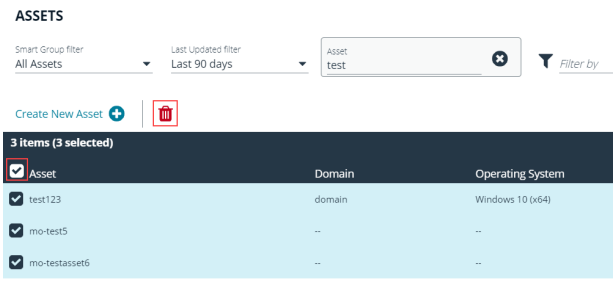
For more information about attributes, please see "Attributes and Attributes Types" on page 54.

1. Run a discovery scan to populate the **Assets** pane.
2. Select **Assets**.
3. Click the **Legacy Assets View** link.
4. Select an asset, and then click the **i**. Alternatively, double-click the asset to open the **Asset Details** pane.
5. On the **Asset Details** pane, click **Edit**.
6. Click **Next** on the **Welcome** page of the **Asset** wizard.
7. On the **Edit Asset Details** page, select the asset properties.
8. On the **Edit Asset Attributes** page, select the attribute values, and then click **Next**.
9. The default attributes that you can apply are **Geography**, **Business Unit**, **Criticality**, and **Manufacturer**.
10. Review the settings, and then click **Finish**.

Delete Assets

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

1. Select **Assets**.
2. Select an asset or multiple assets, and then click the **Delete** button above the grid.



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

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

Use the Legacy Assets View

To use the legacy **Assets** page, click the **Legacy Assets View** link on the **Assets** page.

***Note:** To go back to the new **Assets** page, which is now the default page, click the **New Assets View** link.*

Review Asset Details

On the legacy **Assets** page, you can review your protected assets and determine if there are vulnerabilities compromising your assets.

***Tip:** Depending on the scan settings, information in the following list may not be detected and included in the scan results. If the following scan settings are turned on, more accurate scan results can be expected: **Perform Local Scanning**, **Enable WMI Service**, and **Enable Remote Registry Service**.*

For more information, please see "Edit Scan Settings" on page 76.

A scan retrieves the following information from an asset:

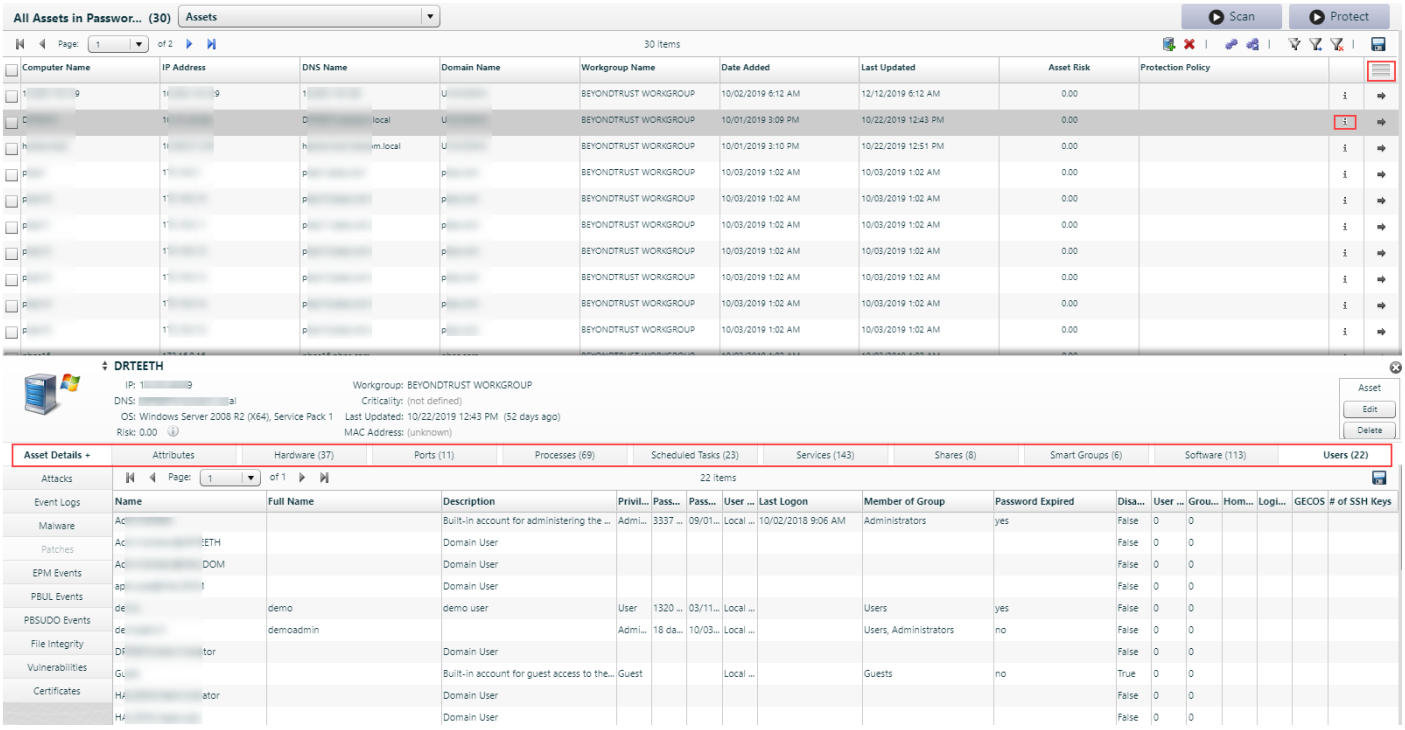
- **Hardware:** Displays disk drive information, system manufacturer, memory, and processor information.
- **Ports:** Displays the open port number, protocol, and description.
- **Processes:** Displays all the running processes and includes the PID and name of the process.
- **Scheduled Tasks:** Displays information about scheduled tasks for a particular asset, including task name, task to run, last time the task ran, schedule type, etc.
- **Services:** Displays discovered services, including name, description, state, log on details, startup type, and dependencies.
- **Shares:** Displays the name and description of the shares on the asset.
- **Smart Groups:** Displays the smart groups that the asset is associated with.
- **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.

In addition to the asset properties, the scan includes information about attacks, malware, and detailed information about vulnerabilities on the legacy Assets page. Depending on additional modules you are using, the scan includes patch details, information for Endpoint Privilege Management events, Privilege Management for Unix & Linux event details, and File Integrity monitoring rule information.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Select a smart group.
4. Click the lines icon to expand the **Assets** pane.
5. Select an asset, and then click **i**.

By clicking **Edit**, you can change properties for an asset. For more information, please see "Change Asset Properties" on page 111.

6. On the **Assets Details** pane, select an item to review its information:



Risk Scores

The risk score indicates the potential for an asset to be attacked. You can use the risk score to determine which assets need the most urgent attention.

The asset risk score is calculated using factors such as: vulnerability, exposure, and overall threat level. The update interval for the asset risk score is every 4 hours.

Risk scores range from 0 to 9.99:

- 0 indicates a low risk, or there is no data available to determine a potential risk.
- 9.99 indicates the highest risk. The asset is vulnerable to an attack.

An asset risk score is displayed in the following areas:

- **Assets** page
- **Details** page for each asset

Authentication Alerts

Authentication alerts indicate if the asset can be accessed for scanning. Assets might not be accessible if there are issues with the scan credentials.

Before you can view authentication alerts, log alert information must be collected in the scan. Turn on log alerts in the following areas:

- Configuration menu
- Scan Options
- Event Routing tab
- Log Alert Information check box.

Run the scan. After the scan runs, authentication alerts are displayed on the **Legacy Assets View** page.

> ***Note:*** *By default, the* ***Authentication Alerts*** *column is not displayed. Go to* ***Preferences****, and check the* ***Authentication Alert*** *box.*

Change Asset Properties

You can use the **Asset** wizard to change the following asset properties, such as **Owner**, **Active**, and **Asset Attributes**. Also, you can assign or change attributes to help organize and identify assets.

> For more information about attributes, please see "Attributes and Attributes Types" on page 54.

1. Run a discovery scan to populate the **Assets** pane.
2. Select **Assets**.
3. Click the **Legacy Assets View** link.
4. Select an asset, and then click the **i**. Alternatively, double-click the asset to open the **Asset Details** pane.
5. On the **Asset Details** pane, click **Edit**.
6. Click **Next** on the **Welcome** page of the **Asset** wizard.
7. On the **Edit Asset Details** page, select the asset properties.
8. On the **Edit Asset Attributes** page, select the attribute values, and then click **Next**.
9. The default attributes that you can apply are **Geography**, **Business Unit**, **Criticality**, and **Manufacturer**.
10. Review the settings, and then click **Finish**.

Delete Assets

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

1. Select **Assets**.
2. Choose **Delete** from the row action menu for the asset you want to remove, or, select more than one asset and use the trash can icon above the grid to remove all selected assets.
3. Click **Delete** to confirm.

Manage Database Instances

Run a credential scan using the **All Audits** scan template. The **All Audits** scan template enumerates database information and includes the following details:

- Database platform and version
- Asset name where the database instance resides
- Database user names and descriptions

View Database Information

After you run a scan, you can view the database information on the **Assets** page.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Select a smart group.
4. Select **Databases** from the list.
5. Double-click the instance name to open the **Database Users** dialog.

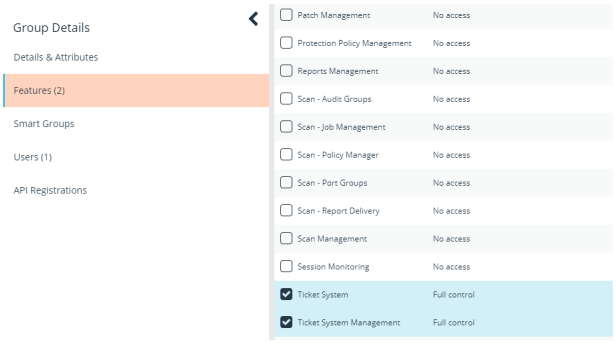
Delete the Database Instance

You can delete the database instance from the BeyondInsight database.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Select a smart group.
4. Select **Databases** from the list.
5. Click the arrow icon for the database instance you wish to delete, and then select **Delete Databases**.

Work with Tickets

Use the ticket system to assign tickets to members of your security team. The team can review, remediate, and resolve vulnerabilities on protected assets. Ensure your groups have the correct ticket permissions assigned.



For more information, please see "Create and Configure Groups" on page 22.

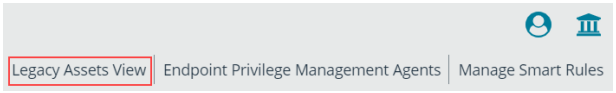
***Note:** You can add an Active Directory group and assign the group ticket permissions. Users who are members of an Active Directory group must log into BeyondInsight at least once before the user name is displayed in the **Assigned** to list. Logging in also activates the email notification for the user.*

Create a Ticket

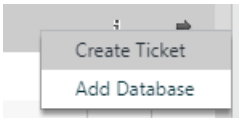
Using the ticket system, you can create tickets for managing the life cycle of vulnerabilities.

You can create a ticket from Assets, Attacks, Malware, or Vulnerabilities.

1. Select **Assets** from the left navigation pane.
2. Click **Legacy Assets View**.



3. Select **Vulnerabilities** in the asset grid, and then select a vulnerability in the list, and click the arrow to display the **Action** menu.
4. Select **Create Ticket**.



5. Enter the details for the ticket. A ticket ID is automatically generated after you save the details for the ticket.
6. Click **Save**.

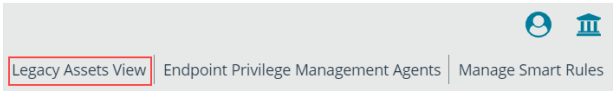
A smart rule is auto-generated when a ticket is saved. This smart rule is intended to help you keep track of assets affected by the vulnerability. No intervention is required by you.

The next time the smart rule is processed, affected assets where solutions are applied will no longer be part of the smart rule. When all assets have the solution applied, the smart rule auto-generated ticket is removed. The auto-generated tickets are not displayed.

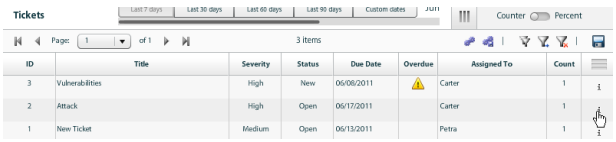
Manage Ticket Details

To change the details for a ticket:

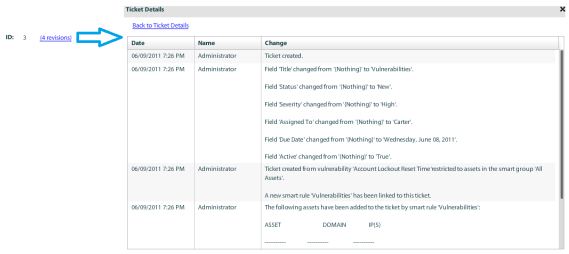
1. Select **Assets** from the left navigation.
2. Click the **Legacy Assets View** link.



3. Select **Tickets** in the asset grid, and then select a ticket, and click **i** to show ticket information.



4. On the **Ticket Details** dialog, change the ticket properties as needed.
    a. If you select the **Close** status, the ticket is no longer displayed on the **Tickets** pane.
    b. If available, click the **revisions** link to view details about activity on the ticket.



5. Click **Back to Ticket Details**.
6. Click **Save**.

Mark a Ticket Inactive

If a ticket is accidentally created or is no longer needed, your security team member can mark the ticket as **Inactive**. An inactive ticket is essentially a deleted ticket because it is no longer displayed on the **Tickets** page. However, the BeyondInsight administrator can always see the tickets.

1. Select **Assets** from the left navigation.
2. Click the **Legacy Assets View** link.
3. Select **Tickets** in the asset grid.
4. Select the ticket, and then click **i** to show ticket information.
5. Clear the **Active** check box.
6. Click **Save**.

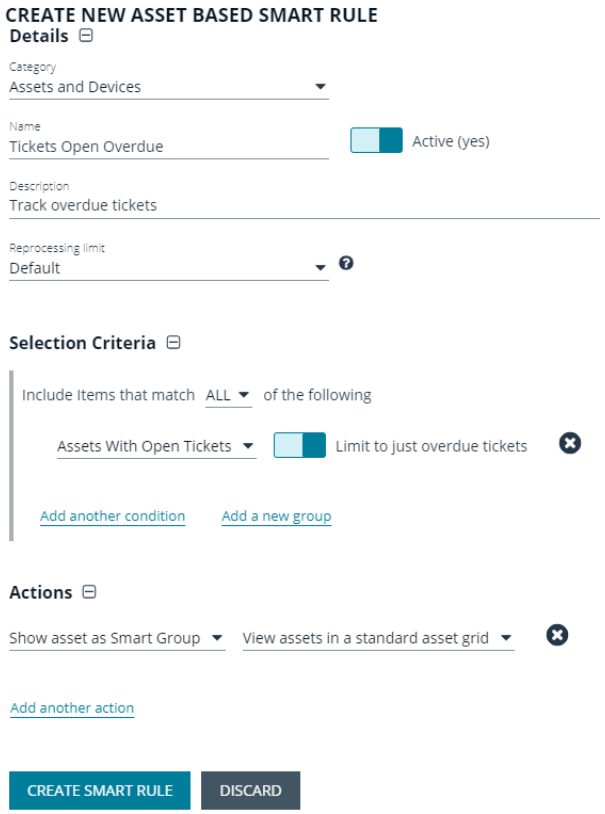
The ticket is no longer displayed, and it cannot be selected.

Track Open Tickets Using Smart Rules

Use smart rules to track open tickets and tickets that are overdue.

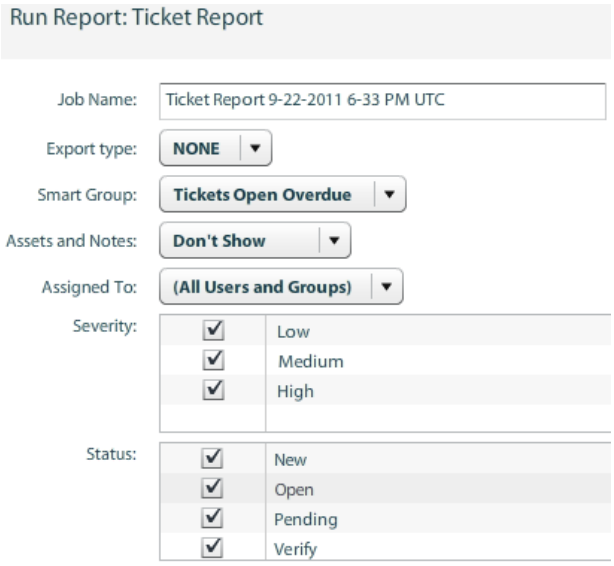
1. Select **Assets** from the left navigation.
2. Click **Manage Smart Rules**.
3. Click **Create Smart Rule**.

4. Select a category and enter a rule name and description.
5. Select **Assets with Open Tickets** for the criteria.
6. Enable the **Limit to just overdue tickets** option.
7. Select **Show asset as Smart Group** for the action.
8. Click **Create Smart Rule**.



Later, you can run a ticket report against the **Tickets Open Overdue** smart group to view a current list of open tickets:

1. From the **Scan** page, select the **Ticket Report**, and then click **Report**.
2. Select **Tickets Open Overdue** for the smart group, select all other desired report paramaters, and then click **Run Report**.



Create Connectors for Mobility Scans

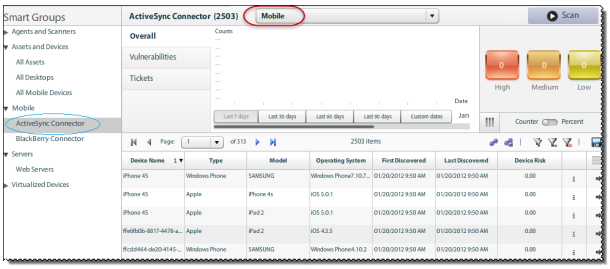
A mobility scan scans mobile devices against scan templates to determine if there are any vulnerabilities. You can use the predefined scan templates that ship with BeyondInsight. You can also create custom scan templates, such as to scan for particular device software and hardware versions.

Running a mobility scan also retrieves information such as device ID, model, and serial number on BlackBerry, and mobile devices on ActiveSync server.

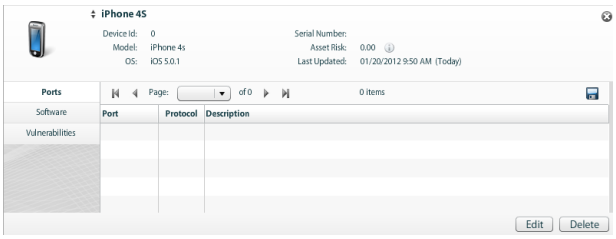
After you create a mobility connector, a smart group is created. The smart group name is the same as the connector name. The smart group is populated with the devices that are detected when a scan runs.

Review Mobility Scan Results

You can review scan results on the **Legacy Assets View** page. Select the smart group, and then select **Mobile** from the dropdown.



Double-click a device to open the details page:



Create Custom Audits for Mobile Devices

You can create a custom audit for your mobile devices.

> The procedure to create a custom audit is the same as in "Create a Custom Audit" on page 82.

You can review the following table for details on audit types and audit details that are specific to mobile devices.

Audit Type	Provide audit details.
Mobile Software	Provide information, including software, if the software exists, operating systems, and versions.
BlackBerry Device	Provide attributes for BlackBerry devices, including model, serial number, device ID, version, and operating systems.
ActiveSync Device	Provide a list of device types and operating systems.

Configure a Qualys API Connector

You can create a connector to a Qualys API server. You can then export your Qualys data to BeyondTrustto run reports and analytics on the data.

1. Select **Configuration** from the menu.
2. Under **General**, select **Connectors**.
3. Click **+** in the **Connectors** pane, and then select **Qualys**.
    - **General:** Enter a name and description for the connector.
    - **Endpoint Details:** Enter the address and credentials for the Qualys API server.
    - **Connection Details:** Enter a name for the workgroup. You can use the name of the Qualys API workgroup.
    - **Tag Filter Details:** Add tag filters for the data that you want to extract from the API server and view in BeyondTrust.
    - **Synchronization:** Select a synchronization schedule.
4. Click **Update**.

Run Scans on Cloud Platforms in BeyondInsight

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

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

Amazon EC2 Requirements

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

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

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

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

Azure Requirements

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

For detailed instructions, please see 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 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. Select the Windows Management Instrumentation (WMI) check box, and then select the **Public** check box.
4. At this point you can send requests but receive unauthorized exceptions, 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 select the following check 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 this format: **\\HOST\root\CIMV2** where host is a computer name on a domain or an IP address.

4. Enter a username and password.
5. Click **Connect**.

VMware vCenter Requirements

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

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

Configure a Cloud Connector

1. Click **Configuration > Connectors**.
2. In the **Connectors** pane, click the plus sign, and then select **Cloud**.
3. Provide a title and then select the provider:
    - **Amazon AWS**
    - **VMware vCenter Server**
    - **Rackspace**
    - **IBM SmartCloud**
    - **Microsoft Azure**
    - **Microsoft Hyper-V**
    - **Google Cloud Platform**
4. Enter the connector information:
    - **Amazon AWS:** For Amazon cloud connections, required fields are: **Title**, **Provider**, **Region**, **Access Key ID**, and **Secret Access Key**.

      Instances associated with the region are displayed in the **Connection Test Results** section.
    - **VMware vCenter Server:** For VMware cloud connections, enter the VMware server name and credentials.

      Click **Advanced** to set a network for a VM if that VM needs to be turned on.

      If you scan snapshots, the results are displayed as attributes on the details pane for the VM.
    - **Rackspace:** Select the account type, and enter the user name and API key.
    - **IBM SmartCloud:** Select the region, and enter the user name and password.
    - **Microsoft Azure:** Select the region, and enter the client information, tenant ID, and subscription information.
    - **Microsoft Hyper-V:** Enter the IP address for the server. Provide the logon credentials to the Hyper-V server.

- **Google Cloud Platform:** Select the region and project name (the project ID). Click **Browse** to upload the key file (the key that you downloaded from the Google Cloud).

5. After you configure the connector, click **Test** to ensure the connector works.
6. Click **Save**.

After you create a cloud connector, you can run a scan and review the results to determine if any cloud assets are vulnerable.

Scan Paused or Offline VMware Images

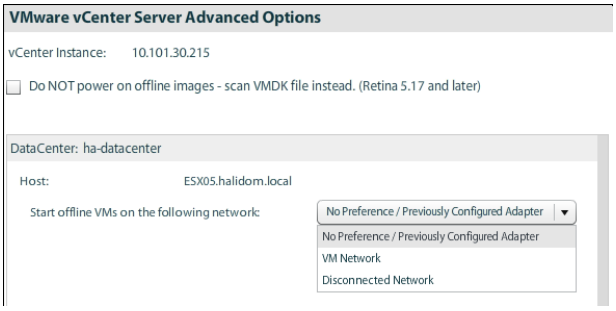
By default, paused or offline VMs are turned on during a scan. After the scan runs, the VMs are reverted to the paused or offline state.

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

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

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

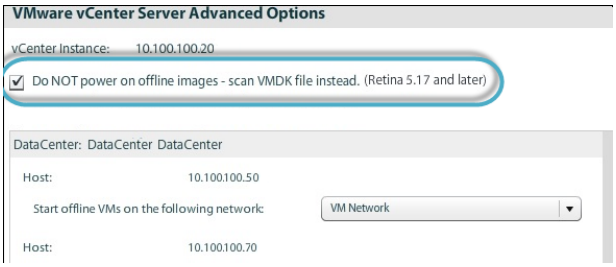
The advanced options dialog box varies depending on your vCenter configuration. The list of available options includes all other networks configured for your vCenter instance or on your ESX server.



Scan VMDK Files

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

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



Cloud Connector Smart Groups

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

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

7. Under **Actions**, select **Show asset as Smart Group**.,
8. Click **Create Smart Rule**.
9. Run a discovery scan on the smart group to see the cloud assets in reports.
10. On the **Assets** page, select the cloud connector, and then click the more options icon to review the details.

Configure BeyondInsight AWS Connector

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

Set up a Policy

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

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

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

Grant Access to a Third Party (Optional)

The **ARN** and **External Name** fields are for granting access to a third party. For more information, please see How to Use an External ID When Granting Access to Your AWS Resources to a Third Party

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

Import Scans from Third-Party Scanners

If you are using more than one type of scanner, the BeyondInsight importing feature provides:

- One reporting console for all scan file types supported.
- One management console to view collected data.
- Ability to import legacy scan data to view collected data and run reports if you are migrating to the BeyondInsight solution.

You can import scan files from third-party scanners, process the data in the BeyondInsight database, and then review the scan results in a Vulnerability report (generated automatically after the data is processed).

File Extensions

Scan files from the following third-party scanning software can be imported:

- **Metasploit:** .xml scan file. Metasploit Version 4 files supported.
- **Nessus:** .csv scan file.
- **Nexpose:** .csv or .xml scanfiles. For the .xml files, Nexpose Version 1.0 and 2.0 supported.
- **QualysGuard:** .csv or .xml scan files.
- **TripWire:** .csv scan file.

Additionally, you can import Network Security Scanner files (.rtd).

File Formats

Note: *The first .csv row must be the header declarations for the proceeding .csv data rows. The header names are case-sensitive.*

Avoid including blank rows or non-standard content such as summary report information.

Nessus

Supported header format (12 columns)

- PluginID
- CVE
- CVSS
- Risk
- Host
- Protocol
- Port
- Name
- Synopsis
- Description

- Solution
- Plugin Output

Nexpose

> ***Note:*** *The* ***Asset IP Address*** *column must be the first column in the .csv file. Before you import your file, ensure that the* ***Asset IP Address*** *column is the first column. Otherwise, the import fails.*

Supported header format (7 columns)

- Asset IP Address
- Service Port
- Vulnerability Test Result Code
- Vulnerability ID
- Vulnerability CVE IDs
- Vulnerability Severity Level
- Vulnerability Title

Qualys

BeyondInsight accepts one of four different formats of headers for the Qualys CSV import.

Format 1	Format 2	Format 3	Format 4
CVEID	CVEID	CVE ID	CVEID
CVSS_Base	CVSS	CVSS Base	CVSS_Base
Hostname	DNS	DNS	DNS Name
Impact	Hostname	Impact	Hostname
IP	Impact	IP	Impact
IS_PCI	IP	NetBIOS	IP
Last Scan	IS_PCI	OS	IS_PCI
Operating System	Last Scan	PCI Vuln	Last Scan
Port	Operating System	Port	Operating System
Protocol	Port	Protocol	Port
Q_Severity	Protocol	Severity	Protocol
Severity	Risk	Solution	Q_Severity
Solution	Solution	Threat	Severity
Threat	Threat	Title	Solution
Vuln Title	Vulnerability Severity Level	Type	Threat
	Vulnerability Title		Type
			Vuln Title

McAfee

Supported header format (17 columns)

- IP Address
- DNS Name
- NetBios
- Asset Label
- Asset Criticality
- Operating System
- Asset Owner
- Vulnerability ID
- Vulnerability Name
- Vulnerability Description
- Risk Rating
- Observation
- Common Vulnerabilities Exposures (CVE) ID
- Recommendation
- First Found
- Last Found
- Services

TripWire

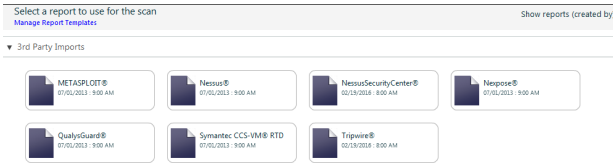
Supported header format (23 columns)

- Score 2
- CVSS Base Score
- Hostname
- IP address
- OS
- Advisories
- Description
- Last Scan
- Risk
- Skill
- Strategy
- Remediation
- IP360
- Network
- Vne
- DP
- Pace Group

- Location
- First Name
- Last Name
- Scan ID
- Host ID
- Vuln ID
- Owner ID

Import a Scan File

The data imported includes asset information and vulnerability data.



1. Select **Scan** from the menu.
2. Scroll to **3rd Party Imports**, and select an import type.
3. Click **Import**.
4. Select the assets that you want to import.
5. Similar to vulnerability scanning, you can filter the assets by single IP address, IP address range, or CIDR notation.
6. Select a scan date. This scan date is used if one is not available in the scan file.
7. Select an existing workgroup or create a workgroup.
8. It is recommended that you create a workgroup based on the import type.
9. Click **Add File** and add the scan files.
10. You can add more than one file. Each scan file is processed separately (a Vulnerability report is generated for each scan file uploaded).
11. The maximum file size that you can upload is set to 10 MB by default.

> To change the default value, please see "Change the File Upload Size " on page 132.

12. Click **Import**.
13. You can view the status of the import on the **Jobs** page. If the state is either **Process** or **Error**, you can click the icon to view more information about the import.

> The information on the **Imports** page is purged after 90 days. To configure the number of days, please see "Data Retention Options" on page 141.

Import Larger Scan Files

If you are working with larger scan files, you can copy larger files to a temporary directory that is automatically created by bey. The BeyondInsight service monitors the directories for new files that need to be processed.

> For more information, please see "Change the File Upload Size " on page 132.

The following directory structure is created when the BeyondInsight service starts:

- C:\Windows\TEMP\BeyondTrust\Imports\NESSUS
- C:\Windows\TEMP\BeyondTrust\Imports\NESSUSSECCEN
- C:\Windows\TEMP\BeyondTrust\Imports\NEXPOSE
- C:\Windows\TEMP\BeyondTrust\Imports\METAPLOIT
- C:\Windows\TEMP\BeyondTrust\Imports\QUALYSGUARD
- C:\Windows\TEMP\BeyondTrust\Imports\RETINARTD
- C:\Windows\TEMP\BeyondTrust\Imports\TRIPWIRE

To upload a scan file:

1. Copy the scan file to the appropriate directory. Ensure that the correct extension is used depending on the scan file.

For a list, please see "Import Scans from Third-Party Scanners " on page 127

2. If the file extension is incorrect, the file will be deleted from the temporary directory and noted in the BeyondTrust Manager Service log. The text will be similar to the following:

```
TPC_IMPORTS: Invalid file type found in import folder: NEXPOSE | Deleting File:
C:\Windows\TEMP\BeyondTrust\Imports\NEXPOSE\Licence Key.txt
```

3. A status is provided on the **Jobs** page in BeyondInsight. The file is deleted from the temporary directory after the file is successfully processed.
4. Go to the **Assets** page to manage the assets and vulnerabilities as usual.

View the Vulnerability Report

Go to the **Jobs** page, and open the reports from the **Completed** tab in the **Reports** section.

The Vulnerabilities report includes a summary of the vulnerabilities, a detailed description of a vulnerability, and a list of assets affected.

Change the File Upload Size

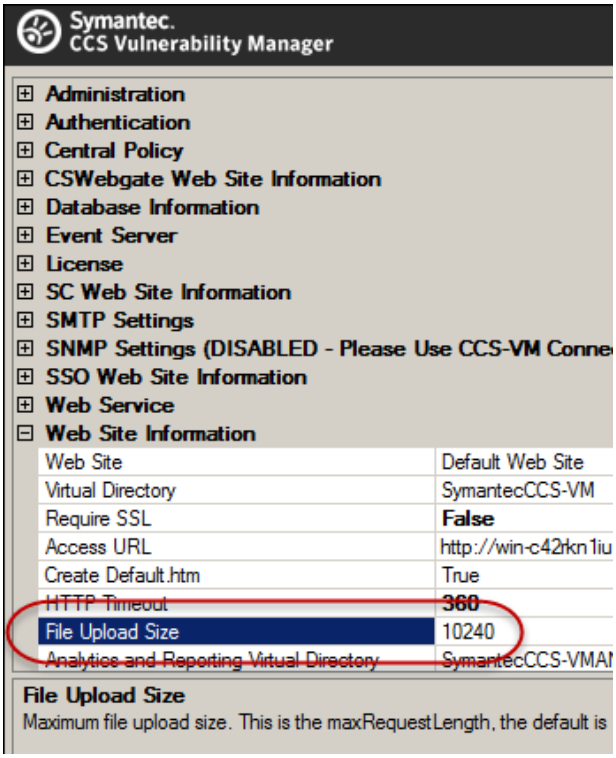
The file size that you can upload is set to **10240 KB**.

You can change the settings using the BeyondInsight **Configuration Tool**.

Microsoft recommends setting the file size between 10-20 MB, but not exceeding 100 MB. For more information, please see https://support.microsoft.com/en-us/help/295626/prb-cannot-upload-large-files-when-you-use-the-htmlinputfile-server-co.

If your file exceeds the recommended values, you can copy the file to a temporary directory to upload to BeyondInsight. For more information, please see "Import Larger Scan Files" on page 130.

***Note:** If you increase the size of file you can upload, be sure to also increase the **HTTP Timeout** value, since it will take longer to upload the file.*



Work with the Multi-Tenant Feature in BeyondInsight

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

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

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

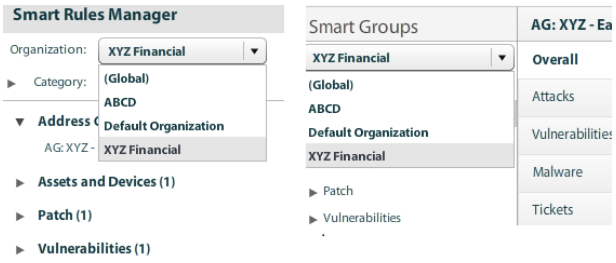
Select Tenants Smart Rules Manager and Smart Groups Pane

All of the pre-packaged smart rules are part of the global rules. When a pre-packaged smart rule is turned on, the smart rule applies to all assets in every organization. You can select the **Global** rules from the **Smart Groups** browser pane.

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

> Create smart rules as usual. For more information, please see "Use Smart Rules to Organize Assets" on page 55.

You can easily switch between tenants in the **Smart Rules Manager** and the **Smart Groups** browser pane.



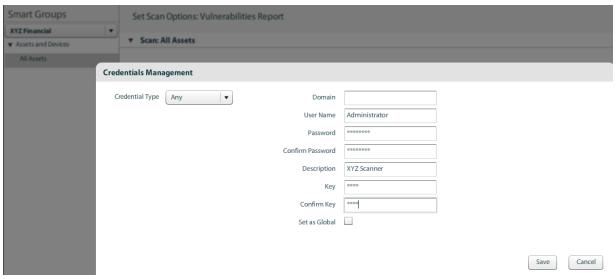
Work with Scan Credentials

You can create credentials when running a scan. However, when using the multi-tenant feature, you can create global credentials or credentials for an organization.

All users can see global credentials. Correct permissions are needed to see tenant-specific credentials. We recommend that you create credentials specific to each tenant.

To create credentials when running a scan, click the pencil in the **Credentials Management** section on the **Set Scan Options** page, and then click **Add**.

In the example screenshot, while XYZ Financial is the organization selected, you can choose to create credentials only for XYZ or select the **Set as Global** check box.



> For more information about credentials, please see "Add Credentials for Use in Scans" on page 65.

Quick Rules

When you create a quick rule from the **Vulnerabilities** page or the **Attack** page, the rule applies to whichever organization is selected in the **Smart Groups** browser pane.

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

Organization Filters

When working with more than one customer, use the **Organization** filters to see only assets, Network Security Scanner agents associated with a particular customer.

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

Additionally, when managing your user groups, you can filter Smart Rules by organization.

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

Patch Management Module

If you are using Multi-Tenant, note the following when using the Patch Management Module:

- For each WSUS server connection, you must select an organization.
- When creating a Smart Rule, the credentials displayed are only for the selected organization.
- Credentials created when you create the Smart Rule are associated only with that organization.
- The list of available WSUS servers includes all global connections plus any specific to the organization.

For more information, please see "Patch Management Module" on page 158.

Network Security Scanner Protection Agents

A workgroup is required when deploying Network Security Scanner protection agents in a Multi-Tenant environment.

For more detailed information about deployment, please see "Deploy Protection Policies" on page 178.

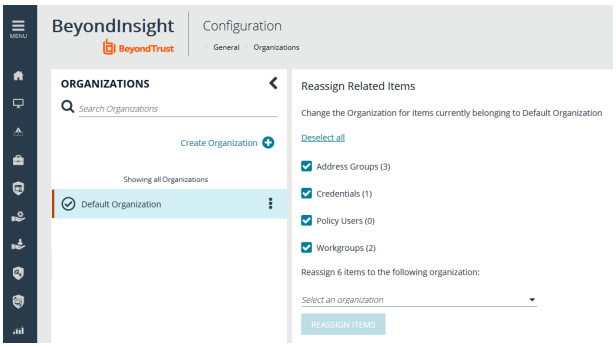
Address Groups

You can organize address groups by organization. When working in the **Smart Rules Manager**, you can select an organization and see the address groups specific to that organization.

Reassign Related Items

To migrate existing address groups to a different organization:

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



5. Click the **Select an organization** drop down menu, and then select the name of the organization you wish to migrate the items to.
6. Click the **Reassign Items** button.

Select a Workgroup

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

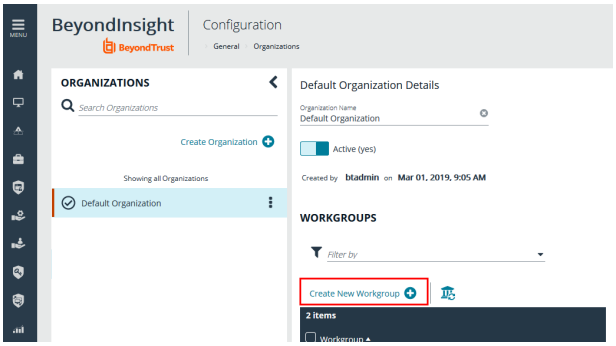
- Single IP address
- IP range
- CIDR notation
- Named hosts

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

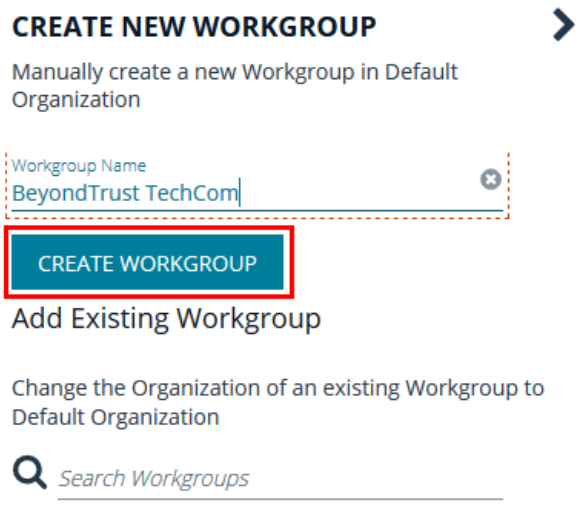
- Currently selected Smart Group
- Currently selected Assets

Create a New Workgroup

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



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



Create a Dynamic Workgroup Assignment

In multi-tenant environments, multiple organizations can use the same scanner by configuring dynamic workgroup assignments. This feature is not available for Host Scanners.

1. Select **Configuration** from the menu.
2. Under **Discovery and Vulnerability Management**, select **Options**.
3. Under **Multi-tenant**, turn on **Enable Dynamic Workgroup Assignment**.
4. Go back to the **Configuration** page.
5. Under **General**, select **Organizations**.
6. From the **Organizations** pane, select an organization.
7. Click **Create New Workgroup**.
8. Enter a name for your workgroup.
9. Click **Create Workgroup**.
10. Assign a worker node to your workgroup from **Configuration > Privileged Access Management > Worker Nodes**.

Run a Scan using a Dynamic Workgroup Assignment

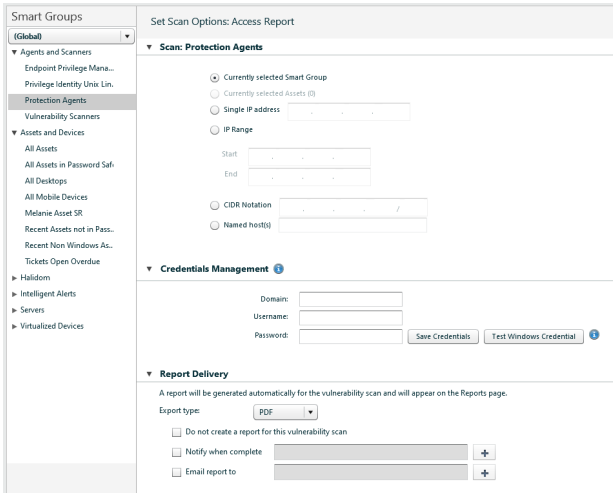
1. Select **Scan** from the menu.
2. Select the scan you wish to run and then click **Scan**.
3. Provide the **Scan Options** as you typically would for any scan, except in the **Advanced** section:
    a. Check **Enable scan specific workgroup selection**.
    b. Select your **Organization** and **Workgroup Name**.

> ***Note:*** *Built-in workgroups are not available for dynamic workgroup selection.*

View the Workgroups Available

The workgroups displayed depend on the item selected in the **Smart Groups** browser pane.

- **Global**: All workgroups are displayed. The organization is in parentheses.
- **Organization:** Only workgroups associated with the organization are displayed.



Set Up Organizations

Create a Workgroup

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

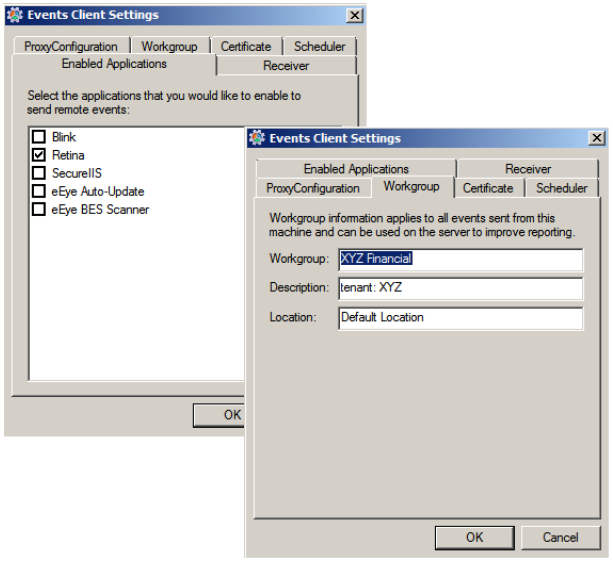
Each Network Security Scanner or protection agent must be assigned a workgroup. A workgroup is typically created when the agent is initially deployed.

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

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

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

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



Add an Organization

An organization is automatically populated with an **All Assets** smart group.

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

Create a Group for a Tenant

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

> Creating a group for a tenant is optional and only required if your client wants to run reports from BeyondInsight. For more information, please see "Role Based Access" on page 19.

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

Set BeyondInsight Options

Set Account and Email Options

If you are using Clarity, for configuration information, please see the BeyondInsight Analytics and Reporting User Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/6-10/bi-ps-authentication-guide-6-10.pdf.

Account Lockout Options

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

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

Account Password Options

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

1. Select **Configuration**.
2. Under **Role Based Access**, select **Local Account Settings**.
3. Under **Account Password**, set the following options:
    - **Enforce Password History:** Enter the number of passwords a user must create before an old password can be reused. Enter **0** to not enforce a password history. There are no restrictions on using past passwords when 0 is entered.
    - **Minimum Password Length:** Enter the minimum number of characters for the password.
    - **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.
    - Click the slider to enable **Password must meet complexity requirements**.

4. Click **Update Account Password Options**.

Email Notifications

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

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

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

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

Data Retention Options

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

Maintenance

Purge general events older than	Sets the number of days to keep the data sent by the agents. General events can include events like checking in and trying to connect to assets, and firewall events which might indicate that the scan cannot process because of a firewall blocking the connection. **The default number of days is 7.**
Purge vulnerabilities older than	The vulnerabilities are displayed on the **Vulnerabilities** page until fixed or purged. However, this can vary for different environments. Once the data is purged, the vulnerabilities are removed from the database. **Recommended: 90 days**
Purge attacks older than	Sets the number of days to keep attack data that was discovered by the protection agent. **Recommended: 90 days**
Purge application events older than	Sets the number of days to keep the application events sent by the agents. **The default value is 7.**
Purge scans older than	Sets the number of days to keep the information defined in the scan settings. **Recommended: 7 days**
Purge scan events older than	Sets the number of days to keep the data collected in scans. **Recommended: 7 days**
Purge attack events older than	Sets the number of days to keep the data sent by the protection agents. **Recommended: 7 days**
Purge vulnerability agent jobs every N days	When enabled, sets the number of days to keep the vulnerability data collected by the agents. **Recommended: 1 day**

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

Privileged Access Management

Purge Windows events older than	Purges the information sent by the protection agents. **The default value is 90 days.**
Purge Endpoint Privilege Management events older	Sets the number of days to keep Endpoint Privilege Management's

than	unprocessed event data. **The default is 30 days.**
Purge Privilege Management for Unix & Linux events older than	Sets the number of days to keep events sent by Privilege Management for Unix & Linux Servers.
Purge file integrity events older than	Sets the number of days to keep File Integrity events captured by Endpoint Privilege Management.
PurgeEndpoint Privilege Management Session Monitor events older than	Sets the number of days to keep the events collected when session monitoring is being used.
Purge AD Bridge events older than	Sets the number of days to keep AD Bridge unprocessed event data.

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

Asset Maintenance

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

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

Application Maintenance

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

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

Third-Party Integration Maintenance

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

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

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

Proxy Settings

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

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

Discovery and Vulnerability Management Options

Enable Host Scanning

1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Options**.
3. Under **Host Scan**, click the slider to **Enable host scanning**.
4. Click **Update Host Scan Options**.

Set Job Refresh Options

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

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

Set Vulnerability Aging

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

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

Enable Dynamic Workgroup Assignment for Multi-tenant

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

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

Global Website Options

You can configure global website settings, including:

- Changing the **Login** page to include domain and LDAP menu items
- Displaying the **Forgot Password** link on the **Login** page
- Displaying social media links on the **Login** and **About** pages
- Changing the refresh interval for smart rules
- Configuring a pre-login banner to appear to users before logging into the site
- Setting the number of records to display in the console grids
- Configuring session options
- Turning on language selection

List Domains and LDAP Servers on the Login Page

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

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

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

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

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

Display Forgot Password Link

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

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

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

Display Social Media links on the Login and About pages

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

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

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

Change the Refresh Interval for Smart Rules

Scans can run more efficiently when smart rules are set to refresh at longer intervals.

1. Select **Configuration**.
2. Under **System**, select **Site Options**.
3. Under **General**, set the number of minutes for **Maximum smart rule refresh frequency for asset updates**. The default is **60**.
4. Click **Update General Options**.

Configure a Pre-Login Banner

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

1. Select **Configuration**.
2. Under **System**, select **Site Options**.
3. Under **Pre-Login Banner**, click the slider to enable the **Show Banner**.
4. Provide a title and message, and then click **Update Pre-login Banner Options**.

Configure Session Options

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

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

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

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

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

4. Click **Update Session Options**.

Enable the Language Menu

The management console can be viewed in the following languages:

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

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

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

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

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

Configure Network Security Scanner Scan Options

You can configure Network Security Scanner scan options to improve performance and reliability.

Performance Settings

The number of scan targets can affect server performance and scan quality. The result is an unresponsive or slow server or poor scan quality, such as known services not being found or known open ports not being identified.

To improve performance, you can:

- Reduce the number of targets
- Adjust the scan speed downward
- Override the TCP connection limit to increase the scan speed

If you override the TCP connection limit, the TCP incomplete connections limits are removed for all applications during the scan.

Timeout Values

Configure ping and data timeout values to compensate for network latency. If a ping is not returning in time for the scanner to detect, increase the ping timeout value.

1. Select **Configuration > Discovery and Vulnerability Management > Scan Options**.
2. Select the **Scanner** tab.
3. In the **Performance** area, configure the following settings:
    - **Number of Simultaneous scan targets:** Set the number of targets to scan simultaneously. The maximum is 128 targets.
    - **Adaptive Scan Speed:** Set the delay between bursts of packets sent during a SYN scan. 1 = longest delay and 5 = almost no delay
    - **Enable TCP connection limit override:** Select the check box to override the TCP connection limit. The **TCP Connection Limit Override** is available on Windows XP SP2+ and Windows 2003 SP1 only. This is not available for Windows NT or Windows 2000.
4. In the **Reliability** area, configure the following settings:
    - **Ping Timeout:** Enter the number of seconds.
    - **Data Timeout:** If the scanner is not receiving complete data from assets or hosts when services are under heavy load, increase the timeout value.
5. Click Save.

Event Routing

The following scan data can be sent to BeyondInsight if event logging is enabled:

- Port information
- Services
- General scan information

Turn on event logging

1. Select **Configuration > Discovery and Vulnerability Management > Scan Options**.
2. Select the **Event Routing** tab.
3. Check **Enable Event Logging**.
4. Select the risk level of the audits to include in routing to BeyondInsight. Audits include a risk level that corresponds to the severity of the vulnerability detected.
    a. **Information:** Details host information that does not necessarily represent a security threat, but can be useful to the administrator to assess the security.
    b. **Low:** Defines risks associated with specific or unlikely circumstances.
    c. **Medium:** Describes serious security threats that would allow a trusted but non-privileged user to gain access to sensitive information.
    d. **High:** Indicates vulnerabilities that severely impact the overall safety and usability of the network.
5. Click **Save**.

Set Restrictions on Scan Times

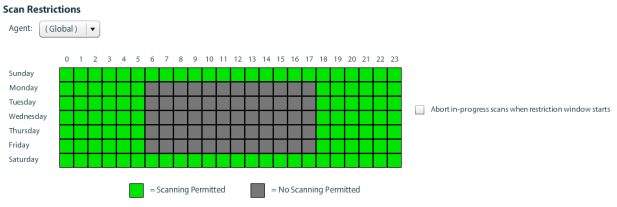
You can set a scan restriction so that scans will not run during the restricted time frame.

Apply scan restrictions on:

- **One scan only** Configure the restricted scan time when you are configuring the scan.
- **Global** Configure the restricted scan time on the **Configuration** page.

To set a scan restriction on all scans, follow the below steps:

1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Scan Options**.
3. From the **Agent** list, select an agen,t or select **Global**.
    - If you select an agent, you can override scan restrictions already set for that agent. Check the **Use Global Settings** box to apply globally.
4. Select the **Scanner** tab.
5. Click the squares to set the restricted time frame.
6. Check the **Abort in progress scans when restriction windows starts** box to stop all scans that are running when the scan restriction window starts. Otherwise, scans in progress are paused and then resumed when the scan restriction ends.



Use Scanner Pooling

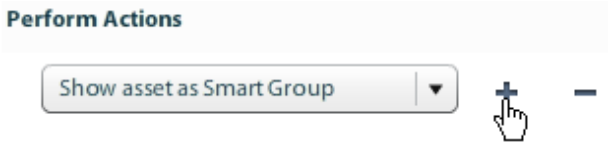
You can use scanner pooling to select more than one scanner when scanning a large number of assets. When more than one scanner is selected for a scan job, the list of target assets is divided among the selected scanners in a round-robin style, evenly distributing the target scan range.

To use scanner pooling, select more than one scan agent when running a scan, or use the **Set Scanner** action in a smart rule to lock a set of scanners to that smart group.

> ***Note:*** *When using scanner pooling, you cannot automatically generate a report when a scan finishes.*

To lock a scanner agent to a smart group:

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. In the **Smart Groups** pane, click **Manage Smart Rules**.
4. Click **New**.
5. Enter a name and description.
6. From the **Perform Actions** area, select **Show asset as Smart Group**.
7. Click the **+**, and then select **Set Scanner**.
8. Click **Browse** to select the scanners to associate with the smart group.



9. Select the **Distribution Algorithm**.
    a. **Round Robin Asset Distribution:** Targets are assigned to scanners one-by-one. This method balances the distribution of scan targets.
    b. **Rule Locked Asset Distribution:** This distribution algorithm is designed and recommended for multiple scanner jobs where child smart rules are defined in a parent smart rule. Each child smart rule will always use the scanner assigned in the child smart rule when this distribution algorithm is used. This ensures that scanners assigned in child smart rules will not scan across other child targets.
10. Click **Save**

> ***Note:*** *On the **Job Details** page, the agent name indicates if the scanner is part of a pool.*

View Status for Agents

You can review details about your deployed agents.

Use the **Agent Details** page to determine if agents are out of date.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. In the **Smart Groups** pane, select **Agents and Scanners**.
4. Click the **i** button to review additional information.

The **Agent Details** page displays the following:

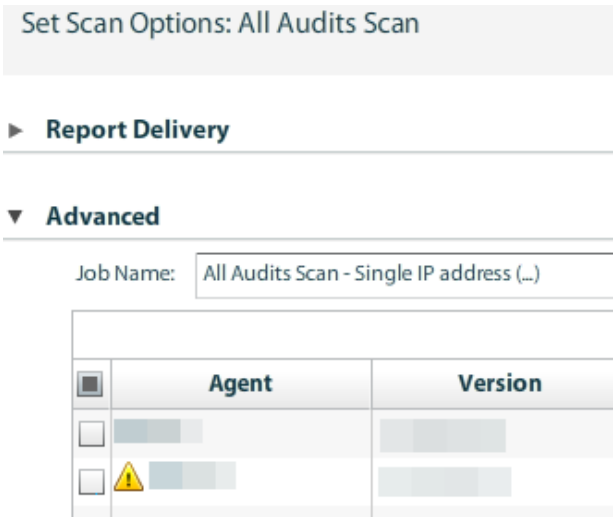
- IP address
- Computer name
- Operating System
- Workgroup
- Domain
- Agent name
- Agent versions

> You can change viewing preferences for the **Agents** page. You can select preferences and create filters to determine the list of agents that are displayed. For more information, please see "Change and Set the Console Display and Preferences" on page 17.

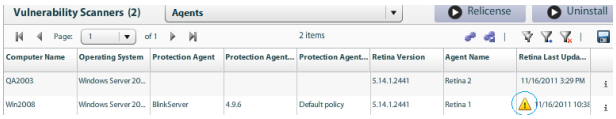
Determine an Agent's Availability

A scanner might lose connectivity to Central Policy. You can determine connectivity in the following places:

When you are setting up a scan, there is a warning icon next to an agent name.



On the **Agents** page for **Vulnerability Scanners**, there is a warning icon in the **Last Updated** column. The agent might not be able to accept the job request. Ensure the computer hosting the scanner is online.



Restart Agents

You can restart one or more scanners.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. In the **Smart Groups** pane, select **Vulnerability Scanners** .
4. Check the assets that you want to restart, and then click the **Power** icon.
5. Select one of the following: **Safe**, **Normal**, or **Force**.
6. Click **Restart**.

Remove Agent Files

Clean BeyondInsight records for scheduled, queued, and completed jobs. Ensure your BeyondInsight administrators are assigned the **Scan Management** permission.

For more information, please see "Create and Configure Groups" on page 22.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Select **Agents** from the list.
4. Select the agent in the list, and then click **i**.
5. Click **Agent Maintenance**.
    - **Clean BeyondInsight Files:** Deletes files from the following directory:
        - C:\Program Files (x86)\BeyondInsight\Retina 5\Scans
    - **Reschedule existing scheduled jobs:** When **Clean BeyondInsight Files** checked, you can reschedule jobs automatically.
6. Click **OK** to save the settings.
7. Click **Reset Engine** to restart the BeyondInsight services.

Configure Failover Agents

You can configure a backup agent to provide redundancy in case an agent fails.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Expand **Agents and Scanners**, and then click **Vulnerability Scanners**.
4. Select **Agents** from the list.
5. Select an agent, and then click **i**.
6. On the **Agent Details** pane, click **Configure Failover Agent**.
7. Select an agent. The **Failover Agent** field displays the name of the agent that you select.
8. Click **OK**.

You can configure a failover agent timeout from the **Configuration** page. The default timeout is 15 minutes.

Configure BeyondTrust Network Security Scanner Host Scanning

To use host scanners, you must:

Turn on BeyondTrust Network Security Scanner scanning.

- Create a host scan group
- Create a Smart Rule
- Run the Scan
- View scan details

Enable Host Scanning

1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Options**.
3. Under **Host Scan**, click the slider to **Enable host scanning**.
4. Click **Update Host Scan Options**.

Create a Host Scan Group

You can create the host scan group either via the **Configuration** page or via a Smart Rule.

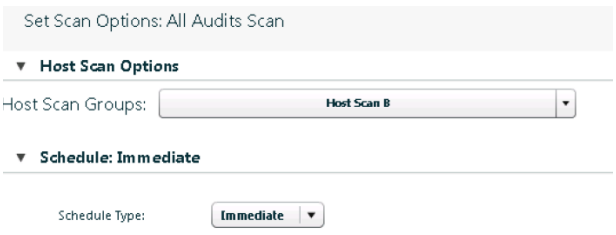
1. Select **Configuration**.
2. Under **Discovery and Vulnerability Management**, select **Host Scan Options**.
3. Click **Manage Host Scan Groups**.
4. Click **New**, and then enter a name for the group.
5. Click **Create**. The properties of the group include the **Group ID**, **Group Name**, and **Last Updated Date**.

Create a Smart Rule

1. Select the matching criteria.
2. In the **Perform Actions** section, select **Assign to Host Scan Group**.
3. Select a group from the list.
4. Select **Show asset as Smart Group**.
5. Click **Save**.

Run the Scan

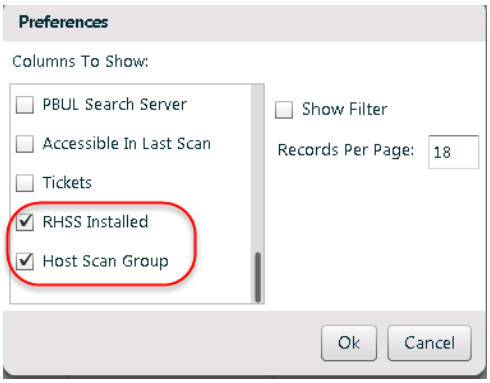
1. Select **Assets**, and then click **Scan**.
2. Select the audit template, and then click **Host Scan**.
3. Select the host scan group for the list.
4. Select the schedule: **Immediate**, **Recurring**, **One Time**. Set the scheduling options as appropriate.
5. Click **Start Host Scan**.



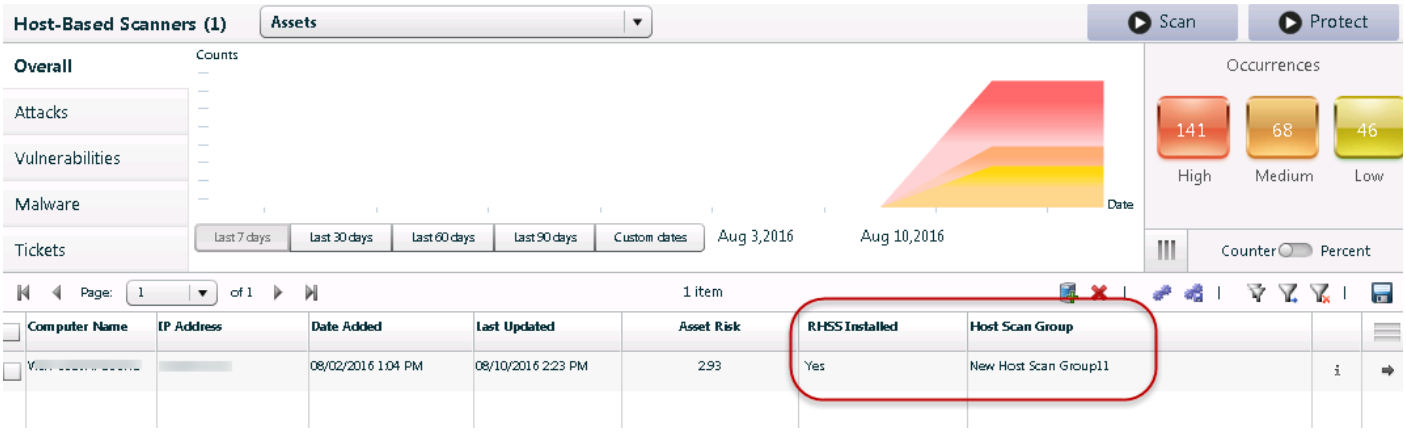
Display Scanner Information

You can view information about host-based scanners on the **Asset** details page.

From Preferences, check **RHSS Installed** and **Host Scan Group**.

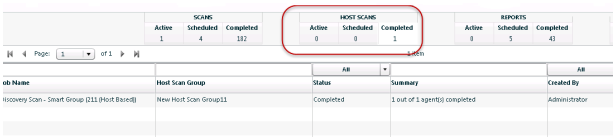


The columns indicate if the host scanner is installed on the asset and the host scan group that the asset belongs to.



View Scan Jobs

You can view the status of the scan jobs. Host Scans are only displayed on the **Jobs** page



Patch Management Module

> ***Note:*** *The Patch Management module requires a license to activate the feature set. Contact your BeyondTrust representative.*

Use the Patch Management Module to deploy important patches to selected assets.

> ***Note:*** *Using the Patch Management Module does not override any automation policies you might have in place with your existing Windows Server Update Services (WSUS) configuration. Those policies are retained and applied as usual.*

BeyondInsight integrates with WSUS to facilitate Microsoft and third-party patching. BeyondInsight uses WSUS as the patching engine and effectively becomes a management console to WSUS.

You must be familiar with WSUS features to understand the BeyondInsight integration with WSUS. The WSUS client is built into the Microsoft OS, however, it needs to be enabled and configured. In typical WSUS-only environments this is accomplished through GPOs. When using BeyondInsight, clients are enabled and configured through BeyondInsight.

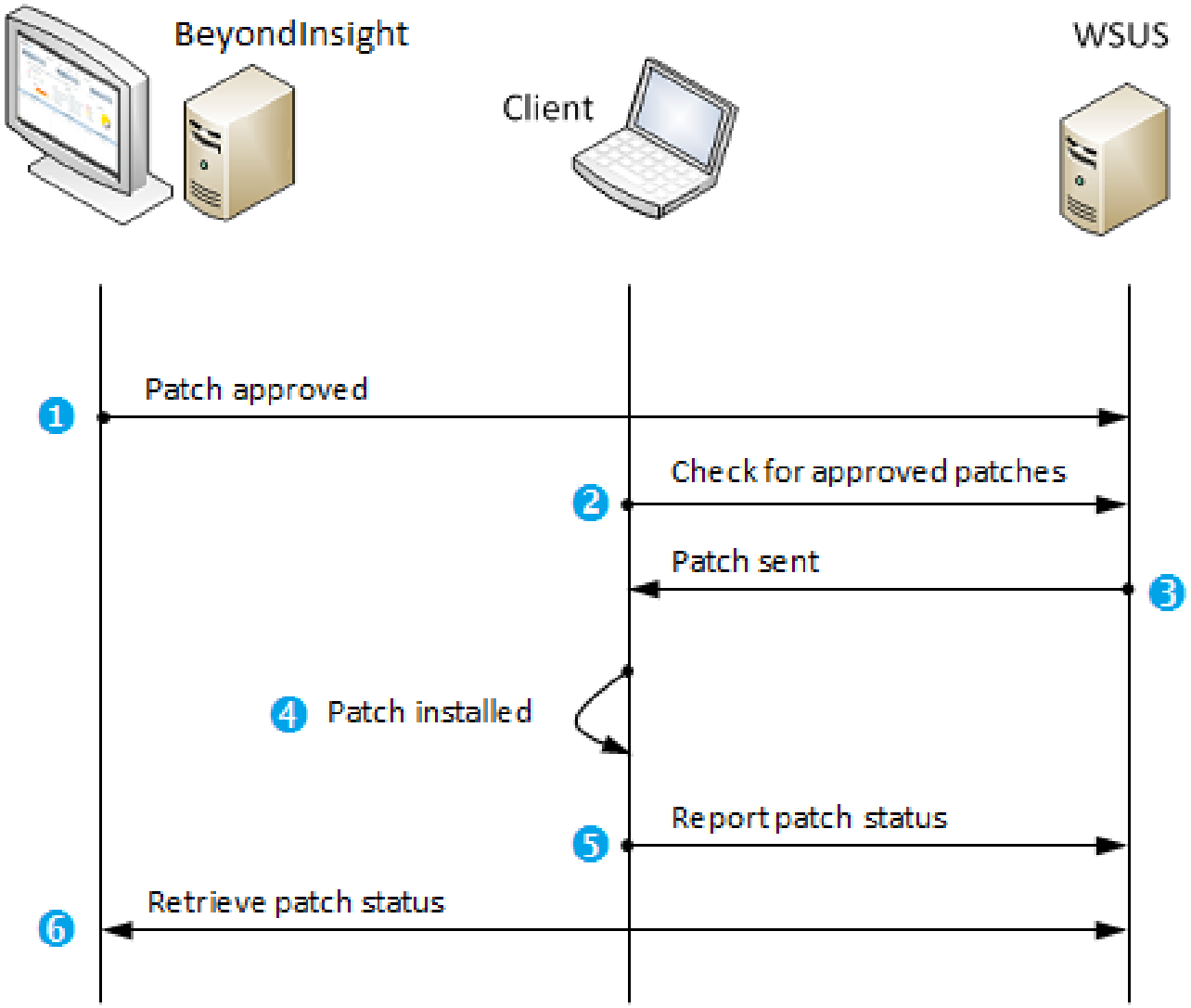
The BeyondInsight configuration and patch deployment process is outlined here.

WSUS Patch Deployment

1	Configure a BeyondInsight connection to an existing WSUS Server; BeyondInsight becomes a management console for WSUS.
2	Configure smart groups for patch management. This configures members of the smart group (the clients) for WSUS by making changes to the registry.
3	Identify and approve patches.
4	Clients periodically check WSUS for approved patches which are then subsequently downloaded and installed.

Patch Deployment

1	Patches are approved in BeyondInsight; consequently, they are marked as approved in WSUS.
2	The client polls WSUS for any relevant, approved patches.
3	Patches are downloaded to the client. Optionally, per the smart group settings, the client may be notified that approved patches are available and then prompted to download and install them.
4	Patches are automatically installed based on the default settings. Optionally, per the smart group settings, the client may be notified that patches have been downloaded and then prompted to install them.
5	The new patch status is sent to WSUS.
6	BeyondInsight retrieves the current patch status from WSUS.



Third-party Patch Deployment

Third-party patching is the same as Windows patching with the following differences at these steps.

3	Third-party patches are sent to the client with the third-party certificate that was generated when the connection to WSUS was created.
4	The certificate from WSUS is verified against the existing certificate on the client that it received when its associated smart group was enabled for patch management. Trust is now established for third-party patch deployment per Microsoft requirements.

Connect to a WSUS Server

To deploy patch updates, you must connect to a Windows Server Update Services (WSUS) server.

If you are working in a larger environment and use downstream servers to apply patch updates, you can create connections to the downstream servers in the **Patch Management** configuration. This helps distribute the workload of applying patches to many assets.

Requirements

Windows Server 2008 R2 Installation

Microsoft IIS 7.0. Ensure the following components are turned on:

- Windows Authentication
- ASP.NET
- 6.0 Management Compatibility
- IIS Metabase Compatibility
- Microsoft Report Viewer Redistributable 2005
- Microsoft SQL Server 2005 SP1
- Note that .NET Framework 2.0 and BITS 2.0 update are part of the Windows Server 2008 OS.

Windows Server 2012 R2 Installation

- IIS
- .NET 4.5
- ASP .NET 4.5

Add a Connection

You can create a connection to an upstream and downstream server. The downstream server synchronizes with the upstream server to manage patch updates.

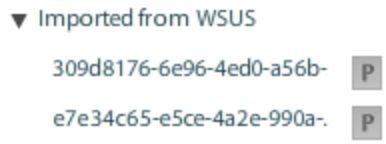
Note: *Downstream servers are configured in WSUS.*

1. Select **Configuration > WSUS**.
2. Click **+**, and then enter the server name, port number, and credentials for the server. Ports available: 80, 8530, 443 (SSL), or 8531 (SSL).
3. Click **Test Connection** to ensure the information is correct.
4. The WSUS Administration Console must be installed if WSUS and BeyondInsight are not on the same server.
5. Click **Save**.
6. After you connect to a WSUS server, set the following options.
    - **Synchronization:** Select the time that you want to synchronize the patches with the WSUS server. The schedule determines the frequency that WSUS checks with Microsoft Update Servers for new patches.If this is a new installation, the initial synchronization can take several hours depending on the number of items selected in the **Products and Classification** section. If you are using downstream servers, increase the frequency of the synchronizations per day.

All updates and approvals occur on the upstream server. Increasing the frequency ensures that all assets receiving updates from the downstream server are updated when the approvals are applied on the upstream server.

- **Products and Classifications:** Select the updates to subscribe to.
- **Downstream Servers:** Displays the downstream servers for the selected server.
- **Third Party Certificate:** Generate or import a certificate to subscribe to vendor patch updates.
- **Groups:** Select the check boxes for the groups that already exist in WSUS. Additionally, select **Synchronization Frequency**, **Credentials**, and how you want patches applied.

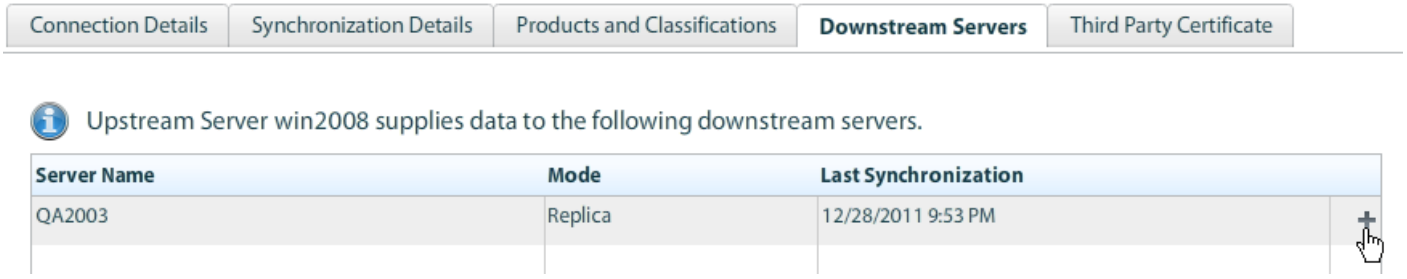
7. After you click **Save**, a patch-enabled Smart Group for each WSUS group is displayed in the **Smart Groups** browser pane.



Connect to a Downstream Server

When you configure assets for patch updates in the Smart Rule, you can choose the downstream server that will apply the updates and patches to the assets.

In the **Patch Management** configuration, you can view information on upstream servers and if there are any downstream servers configured on that upstream. A downstream server is displayed with a green arrow.



Install the WSUS Administration Console

You must install the WSUS Administration Console if you want to connect to an installation of WSUS on a different server. Download the WSUS 3.0 Administration Console installer file from the Microsoft website. You must restart the BeyondInsight server after you install the console.

After you install the administration console, start the console and verify that you can connect to the WSUS server that will be configured as the active software update point.

Install the Console on Windows Server 2012

To install the WSUS Administration Console Using PowerShell:

1. Open a **Windows PowerShell** console as an administrator.
2. Execute the following command:

```
Install-WindowsFeature -Name UpdateServices-Ui
```

Tip: *This command installs the console only and will not run a post-install task.*

Register Smart Rules

Registering the group adds the group to the WSUS server database. The assets in the group are then available for the updates. If an asset is a member in two groups, the patch update applied will be the most recent one.

You can review the status of a patch group on the **Asset Details** pane. If the status is registered, patches can be approved and installed on the patch group.

1. Select **Assets**.
2. Click **Manage Smart Rules** and then click **New**.
3. Enter a name and description for the patch group.
4. Select an existing category or create a new category.
5. Select the asset matching criteria. Select **Asset** fields from the list then select matching criteria: **Last Updated Date**, **Status**, **Current Policy**, **Pending Policy**, **WSUS Status**, or **Patch Install Schedule**.
6. From the **Perform Actions** area, select **Enable for Patch Management**, and then select values for the following:
    - **Credentials:** Click the browse button to open the **Manage Patch Credentials** page. Create or select the preferred patch credentials. Ensure the credentials provided can access the registry and install the certificate on the target asset. The credentials apply only to the **Patch** module. The credentials are not related to vulnerability scans or the WSUS server connection.
    - **WSUS Servers:** Select the WSUS servers from the list.
    - **Important Updates:** Select if you want to download updated.
        - **Download and install updates automatically:** Client computers poll WSUS at the selected day and time and download and install approved updates.
        - **Download updates but let me choose if the updates are installed:** Client computers poll WSUS at regular intervals, and download approved and relevant updates. After downloaded, notifications are sent to the system log and notification area of BeyondInsight.
        - **Check for updates but do not download**
    - **Every / At:** Select a day and time the client computers will poll the WSUS server.
    - **Detection Frequency:** Enter the number of hours that pass before patch-enabled assets check in with the WSUS server for updates. Similar to WSUS, the default is 22 hours.
    - **Retry registration of errored Patch Management assets:** Select the check box to try registration again if the initial registration attempt fails.
7. Click **Save**. After clicking **Save**, the following occurs:
    - The client is contacted by one of three methods, listed in priority:
    - If the client has the protection agent, registry changes occur through the Central Policy connection.
    - If the client does not have the protection agent, registry changes occur through the **Remote Registry API**. Remote Registry service must be enabled on the client. The supplied credentials must have permissions for Remote Registry.
    - If the first two fail, registry changes are facilitated through WMI, a service running on the endpoint.
    - BeyondInsight uses the supplied credentials to access and edit the client's registry. The client is configured for WSUS and then pointed to the WSUS Server. All other relevant registry parameters are set:
        a. **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate**
        b. **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU**
        c. Optionally, BeyondInsight downloads the third-party certificate to the client.

The client is now configured to poll WSUS for any approved updates; this is standard WSUS client behavior. Note that polling may not occur immediately and it may take up to 6 hours for WSUS clients to display as patch-enabled assets in BeyondInsight. The patch group is displayed in the Smart Groups browser pane.

After the group is registered, you must approve the patches that you want to apply to the assets.

Redeploy Configuration

You might need to redeploy the Smart Rule configuration settings in the following scenarios:

- Registry settings are not properly set on the client
- Certificate for third-party patching not properly set

Select **Redeploy Configuration** to apply the settings in the Patch-enabled Smart Rule.

Refresh WSUS Data in the Database

After you create a Patch-enabled Smart Group, the BeyondInsight service imports WSUS data into the BeyondInsightdatabase.

> ***Note:*** *The import will not run when the WSUS server is synchronizing with the Microsoft Update server or an upstream server.*

The BeyondInsight service polls the WSUS server every 4 hours to retrieve the latest data. You can, however, refresh the data on demand.

1. Select **Configuration > WSUS**.
2. Select the **Data Import** tab.
3. Click the **Trigger Import for Group** icon.

Approve Patch Updates

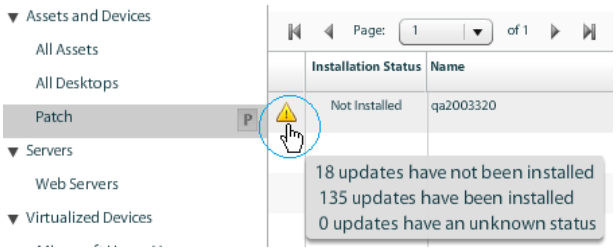
After you register a smart group for patch updates, you can approve the patches for installation. You can track the status of patch updates on the **Patch** pane. Select **Assets**, and then select **Patch** from the list. On the **Approvals** page, you can filter the patch status to determine the patches that are installed, not installed, failed, etc.

On the **Approvals** page, the most recent patches available are always displayed. Any older patches superseded by new patches are no longer displayed. You can check the **Show Superseded Patches** box to review older patches that were not applied.

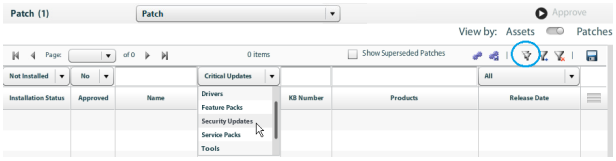
To display the **Superseded** column, click the **Preferences** button, and then select **Superseded**.

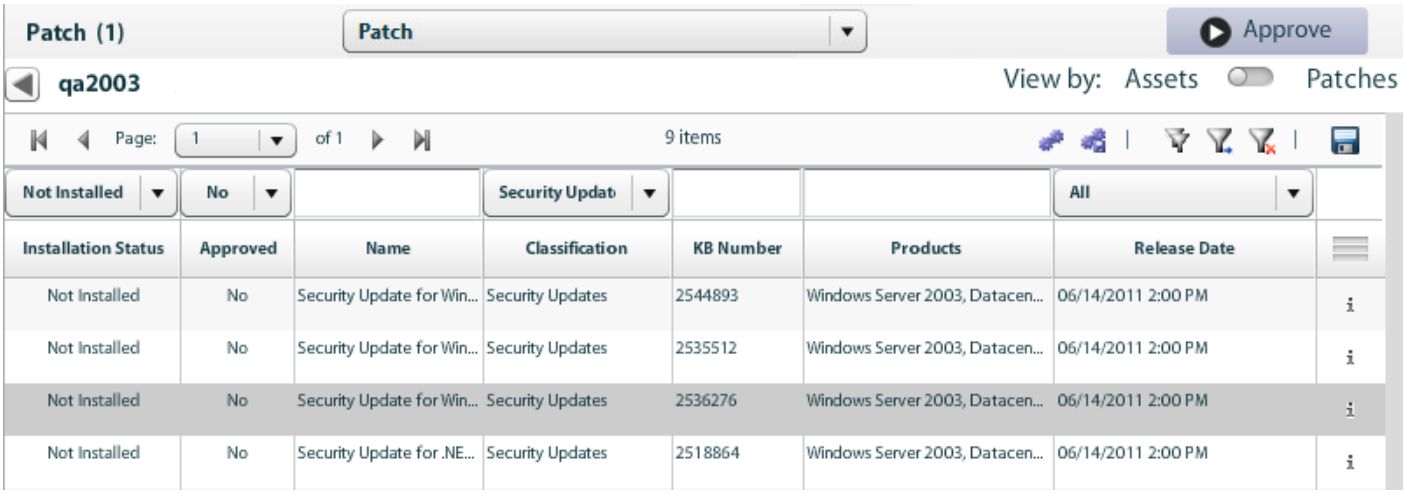
To approve patch updates for registered smart groups, follow the steps below.

1. Select **Assets**, and then select **Patch** from the list.
2. After a patch group is registered, you can access the last accessed group through the **Mitigate** button on the **Dashboard**.
3. Select a registered smart group from the browser pane.
4. To view the number of patch updates installed and not installed, hover on the icon.
5. Select an asset, and then click **i**.



6. By default, only critical updates are displayed. You might need to change the filters to display the relevant patches. Click the **Filters** button, and select the filters.
7. To view superseded patches, check the **Show Superseded Patches** box. Patches are superseded when a new patch is available. Microsoft patches are superseded automatically when a synchronization occurs with WSUS.
8. Select a patch, and then select **Approve**.





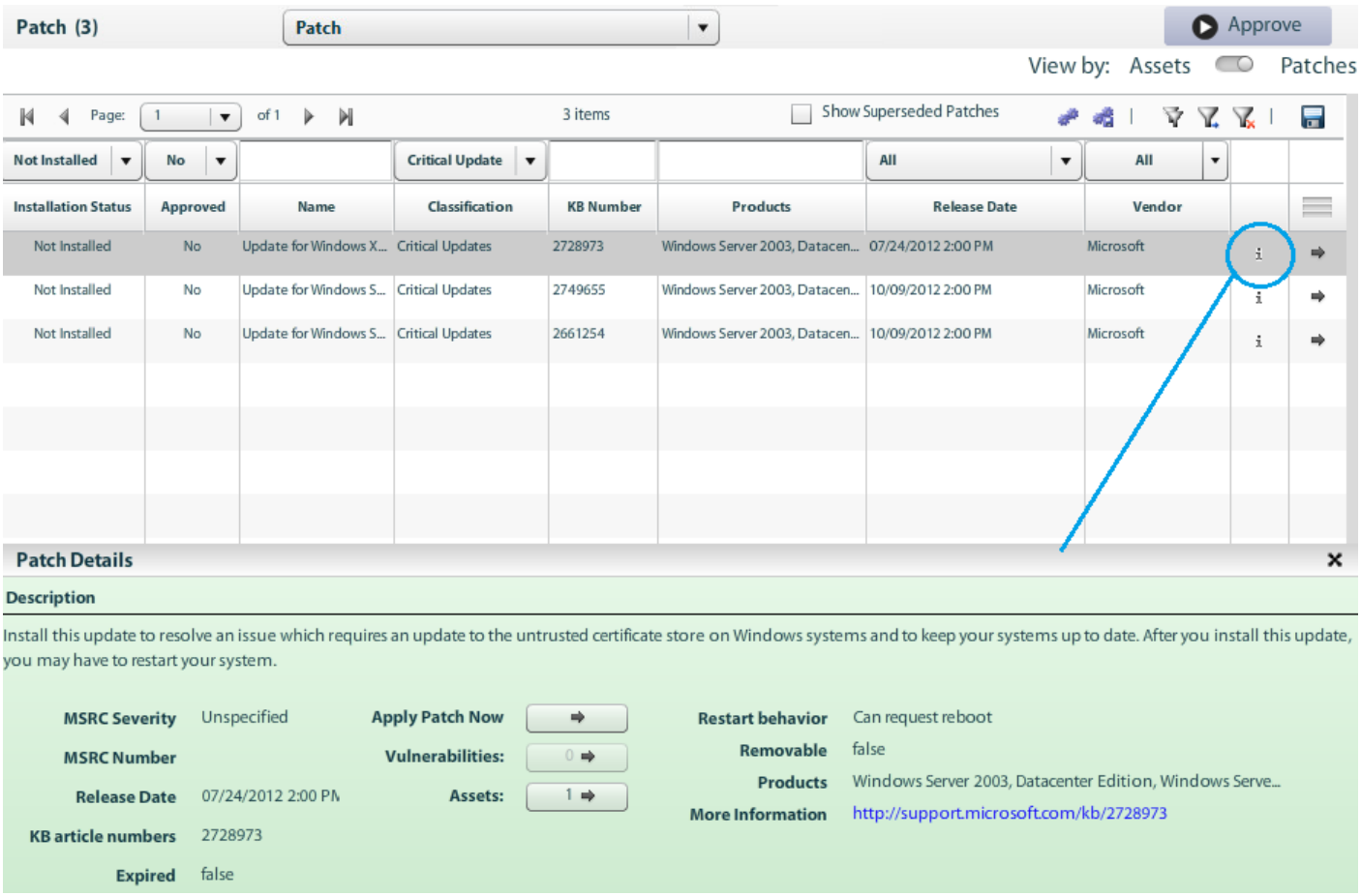
9. Check the **All Groups** box to apply the patch to all registered patch smart groups, or check the box for a particular smart group. The assets are set to check in with the WSUS server every hour.

> ***Note:*** *If you check* ***All Groups*** *and a group already has approved patches, the menu changes to* ***Keep existing approvals****. This ensures that all previously approved patches will still be deployed at the scheduled time. Select* ***Decline*** *to remove the patch from the* ***Not Installed*** *list. Selecting* ***Not Approved*** *will not apply the patch to the selected smart group. However, the patch is still displayed in the* ***Not Installed*** *list.*

Review Patch Details

1. Click **i** to review more information about the update.
2. Click **Apply Patch Now** to install the update to the designated assets. When selected, the clients are forced to check in with WSUS. The patch is applied immediately regardless of the installation settings in the Smart Group associated with the clients. The credentials in the smart group are used to apply the patch.

> ***Note:*** *The client evaluates and downloads the patch before the installation occurs.*



Delete Patches

You can delete patches either on the **Asset** details page or on the **Approval** page where patches are listed.

Download and Deploy Third-Party Patches

You can download and deploy patches for third-party products such as Adobe, WinZip, and Apple. You can subscribe to vendor patches through the BeyondInsight **Configuration** page.

Generate a Certificate

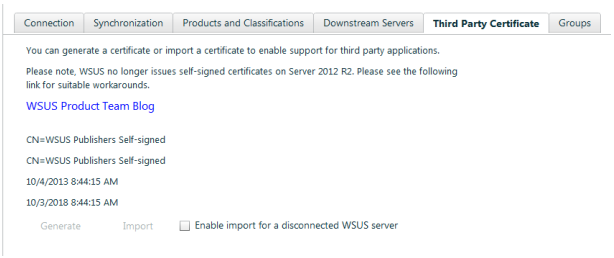
After setting up a connection to WSUS, the **Third Party** section is available.

A message indicates that a certificate is required when you initially log on and go to the **Third Party** section. The certificate establishes trust between the WSUS server and the client. If the WSUS connection is configured to use SSL, you can use the **Import** button on the **Third Party Certificate** tab to import an external certificate, or use the **Generate** button to create a self-signed certificate.

> ***Note:*** *If the upstream server has a third-party certificate, the downstream server automatically receives the certificate. The certificate feature is not available for just downstream servers.*

Click **Generate**.

> ***Note:*** *In some scenarios, generating a self-signed certificate might not work. Additional configuration might be required on the Windows Server 2012 computer. For more information, please see Microsoft documentation.*



Self-signed Certificates

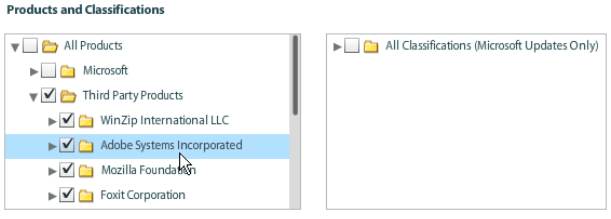
If you are using a self-signed certificate for third-party patching, Windows may automatically delete it. If Windows finds a discrepancy with an intermediate certificate on the server, it will check it against their list of approved SSLs. If it does not match, Windows will remove it and log **Event ID: 4108 Successful auto delete of third-party root certificate** in the application log.

To disable this feature and keep your root certificate installed, follow the steps.

1. Click **Start > Run > "gpedit.msc" > OK**.
2. Double-click **Administrative Templates > System > Internet Communication Management.**
3. Select **Internet Communication settings**.
4. Double-click **Turn off Automatic Root Certificates Update**.
5. Select **Enabled**, and then click **OK**.

Subscribe to Vendor Patch Updates

1. Select **Configuration > WSUS**.
2. In the **Products and Classifications** section, select the vendor patches that you want to subscribe to.
3. Check the boxes for the vendor products, and then click **Save**.



> ***Note:*** *The patch classifications apply to Microsoft updates only.*

List of Supported Vendors

Adobe Systems Incorporated	Adobe Flash Player Adobe Acrobat Adobe Reader Adobe Shockwave - Firefox/IE
Apple Incorporated	Safari
Foxit Corporation	Foxit Reader
Google Incorporated	Chrome
Igor Pavlov (LGPL)	7-Zip
Mozilla Foundation	Mozilla Firefox
Opera Software ASA	Opera Browser
Oracle Corporation	Sun Java
win.rar GmbH	WinRAR
WinZip International LLC	WinZip

System Center Configuration Manager

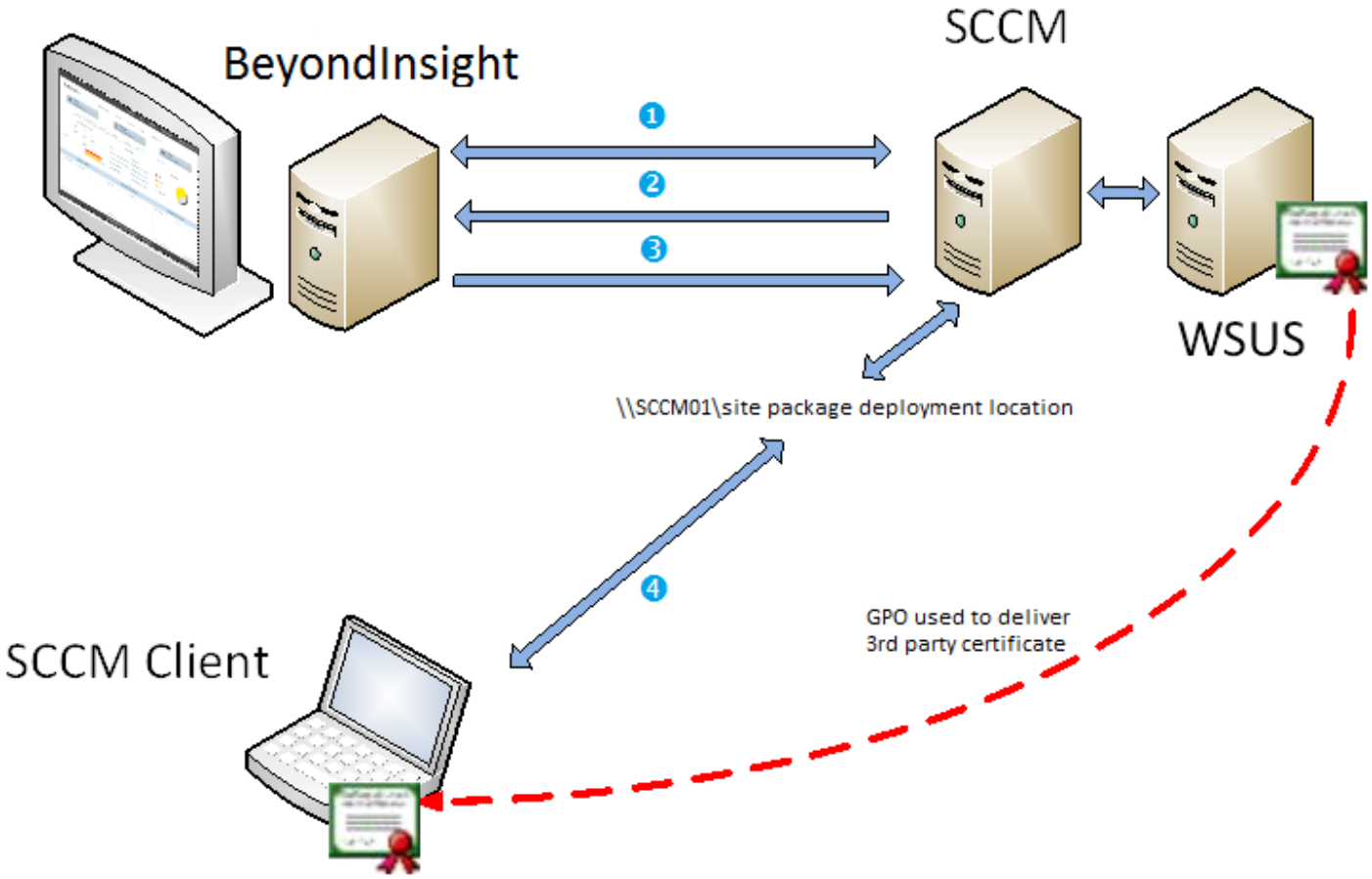
In BeyondInsight, you can create a connection to your Microsoft System Center Configuration Manager (SCCM) site server and manage the software updates to the collections.

The SCCM feature in BeyondInsight offers you a way to create a connection to your SCCM server and manage deploying software packages to selected collections.

An important difference between traditional Smart Groups in BeyondInsight and the SCCM Smart Groups is that asset data is gathered from the collections in SCCM and is stored in the BeyondInsight database. The assets have not been scanned by BeyondInsight. You can use the synchronize feature on the SCCM configure page to ensure the most current data resides in the BeyondInsight database.

The package deployment feature in BeyondInsight is similar to SCCM and offers most of the options that you are already familiar with.

1	BeyondInsight connects to an existing SCCM server for Patch Management.
2	SCCM Computer Groups can be imported from SCCM (as Read-Only smart groups).
3	Patches (Software Updates) are identified and selected to include in a SCCM deployment package. This includes 3rd party applications. For third-party applications to be deployed, you must: • Establish a connection between the SCCM server and the configured WSUS server . • Deploy the WSUS server third-party certificate to the SCCM client. You can use a GPO for the certificate deployment.
4	The SCCM client retrieves the deployment package and installs the applicable patches.



Requirements

The client must have SCCM installed or patches cannot be deployed and applied.

The SCCM Smart Groups are not patch-enabled like the WSUS smart groups.

The SCCM instance must have an Active Software Update Point component configured prior to making a connection from BeyondInsight.

Create a Connection to a SCCM Site Server

You must create a connection to the SCCM site server in the BeyondInsight management console.

1. Select **Configuration**.
2. Under **Patching**, select **SCCM**.
3. In the **SCCM Servers** pane, click **+**.
4. Enter the server name, domain, user name and credentials for the server.
5. Click **Test Connection** to ensure the information is correct.
6. Click **Save**.
7. After you create the connection to a SCCM site server, additional tabs are available. You must select the collections to include in the Smart Group.

8. Select the **Collections** tab.
9. Select the collections, and then click **Save**.

A collection includes the assets that you want to apply patches to and are displayed when at least one asset is detected in the collection. You cannot change the auto-generated Smart Group. A unique identifier is added to every SCCM Smart Group. This helps to identify the SCCM Site Server where the collection is from.

Deploy a Package to a Collection

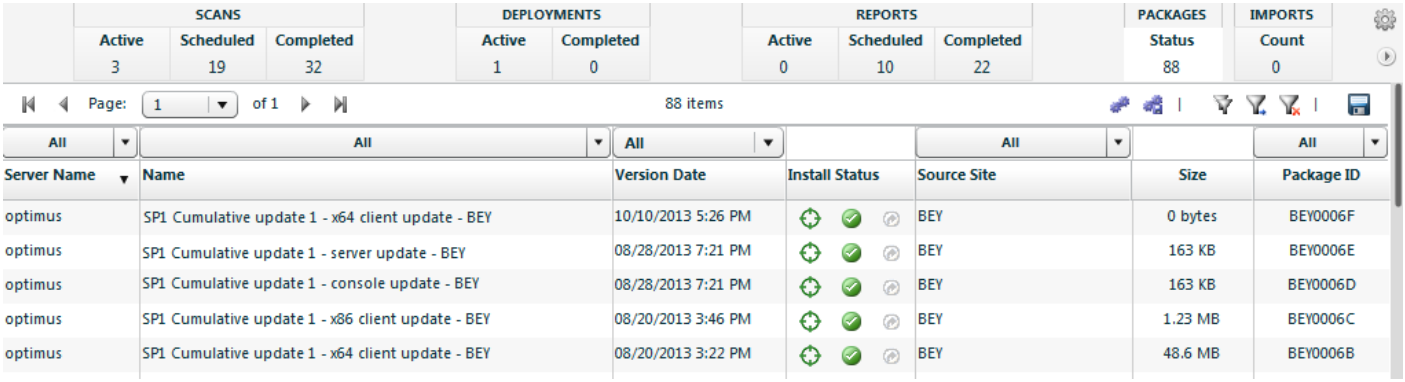
After you create a connection to the SCCM server and the autogenerated Smart Group is created, you can create and deploy packages.

1. Select the collection in the **Smart Groups** browser pane.
2. Select **SCCM** from the list.
3. Review the client list to ensure that all targets have the SCCM client installed.
4. Click **Updates**.
5. Review and select updates, and then click **Deploy**. The page identifies the software available to deploy and the status of the software on the assets in the collection: **Installed**, **Required**, **N/A**, and **Unknown**.
6. On the **Deployment Package Details** page, enter the following information: **Package name**, **Description**, and **deployment package location**.

Note: *The package source location must be entered as a UNC path* ***\\servername\share\package name*** *and must be unique for every package that you deploy. The share must already be created on the server. This is SCCM behaviour.*

7. Select the optional additional settings:
    - **Software Distribution Points**
    - **Enforce an installation deadline for this deployment**
    - **Set an expiration time for this deployment**
    - **Enable Wake On Lan when the deadline for this deployment has been reached**
    - **Enable user notifications**
    - **Enable reboot of client machines outside of maintenance window**
    - **Suppress system restart on Workstations**
    - **Suppress system restart on Servers**
8. Click **Deploy**.

You can keep track of the successfully deployed packages on the **Jobs** page.



SCCM and Third-Party Patches

If you are using SCCM, you can publish third-party patches to an Active Software Update Point (SUP) by configuring the Update Point (WSUS server) on the **Configure > Patch Management** tab in BeyondInsight.

> Any SUP that has an active WSUS connection in RCS should not be used to create Patch-enabled Smart Rules. For more information, see "Connect to a WSUS Server" on page 160.

Use Group Policy to Configure SCCM Assets for Patches

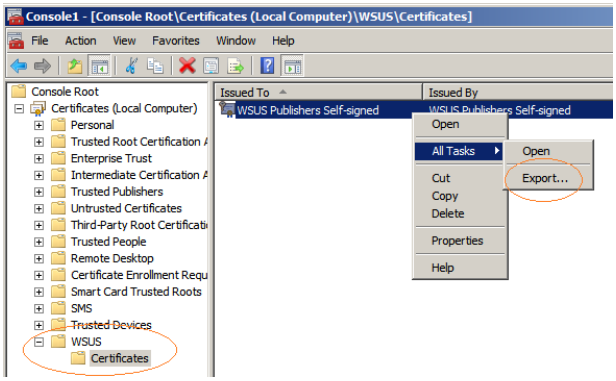
Configuring SCCM assets to accept patches involves two steps:

- Exporting the WSUS Certificate
- Configuring the Group Policy Object

Export the WSUS Certificate

Go through the steps in this section on the WSUS server that is the Active Software Update Point for SCCM.

1. Run **.mmc**, and then add the **Certificates** snap-in.
2. Be sure to select **Computer account** and **Local computer**.
3. Expand the **WSUS** node.
4. Right-click **WSUS Publishers Self-signed**, and select **All Tasks > Export**.
5. In the **Certificate Export Wizard**, select the following:
    a. No, do not export the private key
    b. DER encode binary X.509 (.CER)
    c. Enter a file name for the certificate
6. Continue through the remaining pages of the wizard.



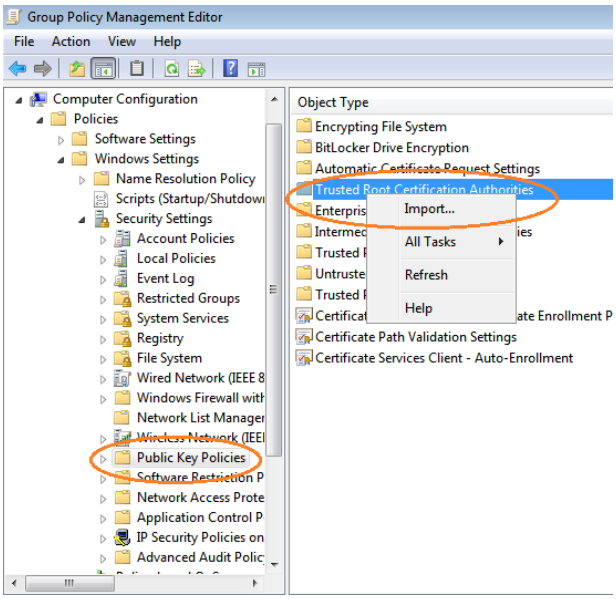
Configure GPO

Use the following procedures to configure the Group Policy Object (GPO) to deploy configuration to SCCM enabled assets. The GPO saves the

WSUS certificate to the appropriate certificate stores and configures the assets to accept third-party patches from non-Microsoft sources.

After the GPO is created, it must be linked to an OU that contains the SCCM assets that you want to receive third-party patches.

1. Open **Group Policy Management Console** (GPMC) on a domain controller.
2. Create a GPO for the certificate at the domain level:
    a. Select the domain you want to use, and then click **Action > Create a GPO in this domain, and Link it here**.
    b. Enter a name for the GPO, and then click **OK**.
3. Select the new object, and then click **Action > Edit**.
4. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
5. Import the WSUS publishing certificate to the **Trusted Root Certification Authorities** and **Trusted Publishers stores**.
6. Turn on signed updates in the Windows Update administrative template:
    a. Expand **Computer Configuration > Policies > Administrative Templates > Windows Components**, and then select **Windows Update**.
    b. Double-click **Allow signed updates from an intranet Microsoft update service location**.
    c. Select **Enabled**, and then click **OK**.
7. Select an OU or domain and create a link to this new GPO.



Overview of Protection Agents

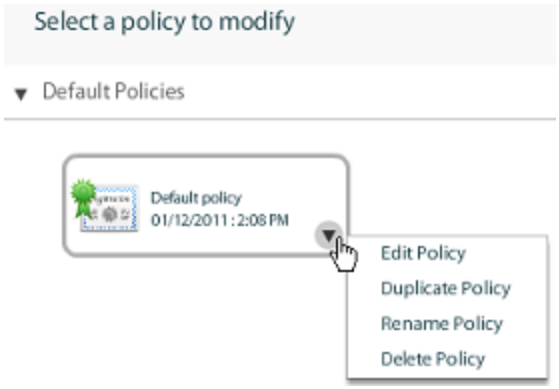
This section provides information on the protection agent deployment.

1	The Application Bus service receives a message from BeyondInsight to start a deployment. A deployment package is created and includes these files: • BlinkSetup.exe • #deploy.xml • deployc.pfx • msxml3.dll • msxml3r.dll • startdeplservice.exe To ensure secure deployment, the deployc.pfx file includes a security certificate, **EmsClientCert.pfx**.
2	The package is queued and ready to be copied to a share on the target asset.
3	This starts the deployment service, **startdeplservice.exe**. This service sends a message to BeyondInsight indicating the job status. When the deployment is complete, the **startdeplservice.exe** is removed from the asset.
4	The service runs **BlinkSetup.exe** and installs: • The VS2008 runtime environment if required. • RPA Reports to BeyondInsight that installation was successful.

Configure a Default Policy

You must configure the default policy to use the BeyondInsight server as the Central Policy agent.

1. Select **Configuration > Privilege Desktop Management > Protection Policies**.
2. Select **Default policy**, and then click the arrow to display the menu.
3. Select **Edit Policy**.
4. Click the pencil icon in the **Master Rules** heading bar.
5. In the **Rule Categories** pane, expand **Misc Options**, and then select **General**.
6. Expand **Central Policy**.
7. Check the **Yes** box to use Central Policy.
8. Use the default protocol, https.
9. Enter the BeyondInsight server name and password.
10. Click **Update**.



> ***Note:*** *Before protection policies can be copied to an asset, the asset must have the appropriate permissions in place.*

Deploy Protection Policies

Use the following procedure to deploy protection policies to selected assets and agents. Policies are only available after you deploy protection agents.

Before proceeding, customize your policies. For more information, please see "Configure Protection Policies" on page 180.

***Note:** Turn off the **Require SSL setting** in your IIS Manager for the BeyondInsight default website. Otherwise, the status displayed does not indicate when the deployment has successfully completed.*

Create a smart group that includes the assets you want to receive a protection agent. The settings you must include are the **Protection Agents**, **Show asset as Smart Group**, and **Assign EPP Policy**.

Review Details about Protection Agents

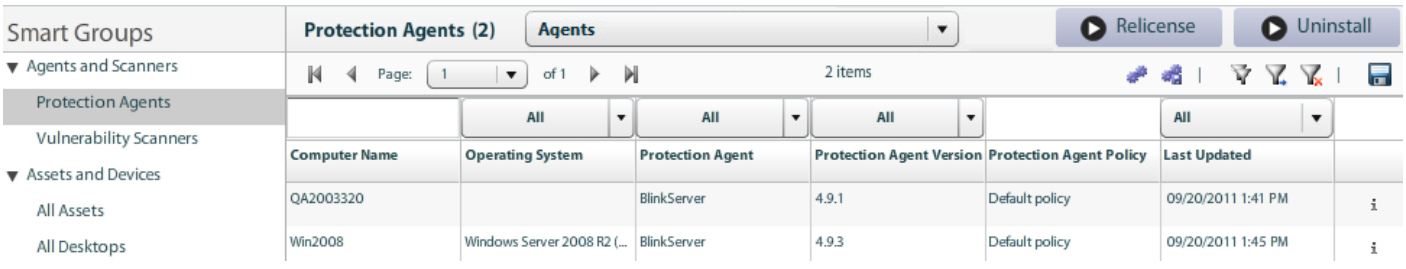
You can review the following information for a protection agent on the Agents tab:

- Policy name
- Protection agent version
- Computer name where the agent is deployed
- Operating system

To review protection agent details, follow the steps.

1. Select **Assets.**
2. Click the **Legacy Assets View** link.
3. Select **Agents** from the list.
4. To review only protection agent information, click the **Preferences** button, and clear any scanner check boxes.
5. Click the **Filters** button to sort agent information. This is helpful if there are several protection agents deployed in your environment.

***Note:** You cannot sort by **Protection Agent Policy Name**.*



Remove Protection Agents

You can remove a deployed protection agent from an asset.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Select **Agents** from the list.
4. Click **Uninstall**.
5. Enter the IP addresses for the assets.
6. Enter the credentials, and then click **Run**.

Configure Protection Policies

When setting up a protection solution using BeyondInsight, you need to determine the rules that you want to use to protect your assets. BeyondInsight ships with a set of default rules and rule groups.

After you determine the rule set and configure rules, you can attach the rule groups to a policy. The policy is then deployed to your assets.

Work with Rules and Rule Groups

When creating rules and rule groups, review the following sections to understand how they work.

Rule Group Ordering

When there is more than one rule group attached to a policy, the rules for all attached groups are automatically merged into an effective set of rules for the policy.

In the case where a specific rule is set in more than one attached group, the group that is located higher in the list of attached groups takes priority. You can click and drag on attached rule groups to modify their ordering and their priority.

BeyondInsight ships with a set of default rules. Each new policy automatically inherits these default settings. By default, some rules are enabled and others disabled. Changing a default value is considered an override even if that setting is later changed to its default state. This is important to understand since a rule override is considered when multiple rule groups are merged in a given policy; however, rules considered to be in their factory default state are not.

To remove all rule setting overrides from a rule category in a rule group, select that category, and click the arrow next to the category title. In the context menu that appears, select **Revert to factory**.

Master Rules

Every policy has a set of **Master Rules** that can be considered a non-shared rule group with the highest priority. Any rule set in the **Master Rules** section overrides the same rule setting in any attached groups.

Create a Rule Group and Set Rules

A rule group is a container for the rules you wish to apply to protect your assets. In BeyondInsight, a rule group can contain any combination of rule categories, including system firewall, application firewall, IPS signatures, etc. In each rule category, there are particular rules that you can activate if you want to provide that specific protection to your asset.

Rule groups provide proactive and reactive protection against intruder, internal attack and machine misuse. When assigned to a policy, rule groups are applied to assets such as networks, servers, workstations, and laptops.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. On the **Manage Rule Groups** page, you can:
    - Click **+** to add a rule group. Enter a name for the rule group.
    - Select the rule group from the **Rule Groups** pane to change the rule group properties. You can type the name of the rule group in the box to search.
    - Select the rule group, and click **-** to delete a rule group.

- Select a rule group, and then select a rule category to display the associated rules.
- Click the arrow to display the subcategories, and select a subcategory.
- Select a rule to activate it.

6. Click **Revert** to revert to either the last saved version of the rule category or the default value for the rule category.
7. Click **Update**.

Create a Protection Policy

Create a policy that defines the rules you want to apply to your assets. You can create a dynamic protection policy. A dynamic policy includes conditions that determine the assets where the protection policy will be applied.

At minimum, one policy category must be created to create a policy.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **New Policy**.
5. Drag rule groups to the **Rules** pane.
6. Click **Create**.
7. Enter the name of the policy and the policy group to which it should be a member.
8. Click **Update**.

Dynamic Policy

You can attach a location to a policy. When a policy is processed, rule groups and locations in the policy are also processed. Locations and conditions define when a policy will be deployed to particular assets.

- **Location:** One or more conditions.
- **Condition:** A set of criteria that determines the assets.

Assets in an environment can change or be removed. The policy is dynamic since only those assets that meet the criteria in the condition are included. To manage locations, you must access an existing policy or create a new policy.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **New Policy**.
5. Click **Add Location**.
6. From the **Location** menu, select **Manage Locations**.
7. Click **+**.
8. Enter a name, and click **Create**.
    - To edit an existing location, select the location from the **Location** pane. To delete a location, select the location from the **Location** pane, and click **-**.
9. Click **Manage**.
10. On the **Manage Conditions** window, you can create and delete conditions.
11. Click **+** to create a condition.
12. Enter a name, and click **Create**.
13. Select **Command** or **Script** from the **Command Type** list.
14. Command options:
    - Check Reachable
    - Compare Version

- Verify DNS
- Verify DHCP

15. Script options:
    - Script Name
    - Script Parameters
    - Select the **Network Status Change Events** check box if you want to log network status changes.
    - Click **Update**.
16. Drag the condition from the **Conditions** pane. More than one condition can apply to a location. The following operators are available:
    - And = &
    - Or = |
    - Not = !
    - Parentheses group conditions
17. Click **Update**.

Organize Protection Policies

A policy category is a set of similar policies. A policy must be assigned to a category when the policy is created.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **New Policy Category**.
5. Enter the policy category name, and click **Create**.
6. Drag policies from other policy categories to populate the new policy category.

Update Your Protection Agent License

When your protection agents' serial numbers are close to expiring, you can deploy an updated serial number to all assets with protection agents.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Select **Agents**, and then click **Relicense**.
4. Select the assets from the **Smart Groups** browser pane.
5. In the **Deploy** section, select **Single IP address**, **IP range**, **CIDR notation**, or **Named Host**.
6. Check the box to skip the assets that do not have agents deployed.
7. Enter credentials.
8. Enter the serial number.
9. Click **Run**.

Rules Reference

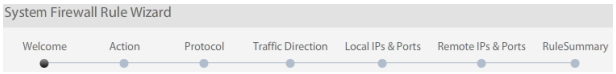
As mentioned earlier, a protection policy contains the security rules that are deployed to your assets. You can create, copy, edit, and delete rules. You cannot create rules for the following rule categories, **Identity Theft** and **Analyzers**.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. Select a rule group from the **Rule Groups** pane.
6. Select a rule category
7. Select a rule name to activate it.
8. Select the rule, and click the arrow.
9. Select one of the following menu items:
    - **Edit Rule:** Edit the selected rule. Click the pencil icon to change the settings.
    - **Duplicate Rule:** Create a copy of the rule. Edit the new rule as needed.
    - **Delete Rule:** Delete the selected rule.

System Firewall Rules

System firewall rules control the flow of data by examining each packet and determining whether to forward the packet toward a specific destination.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. Select a rule group from the **Rule Groups** pane.
6. Select the **System Firewall** rule.
7. Click **Create New Rule** to start the wizard.
8. Complete the following pages.



   - **Action**
     - **Allow:** Allow traffic that matches the rule can pass through the firewall.
     - **Deny:** Deny traffic that matches the rule cannot pass through the firewall.
     - **Ask:** Display a message requesting permission to pass through the firewall.
     - **Log event:** Select to create an event log when the rule is matched.
     - **Alert user** Receive and log alerts when the rule is matched. This can create a flood of alerts and increase the size of the log file.
   - **Protocol:** Select a protocol: TCP, UDP, TCP or UDP, ICMP, or IP
   - **Traffic Direction**
     - **Traffic from Other Computers:** Filters only inbound traffic received by your computer.
     - **Traffic from This Computer:** Filters only outbound traffic sent from your computer.
     - **Any Direction:** Filters both inbound and outbound traffic.
   - **Local IPs and Ports**
     - **Rule applies to all IP addresses:** Create a rule for all local IP addresses.
     - **Specific local IP addresses:** Click **+**, and then select: **Determine IP(s) at run-time, Single IP, IP Range, or Subnet**. Click **Set**.
     - **Rule applies to all ports:** Create a rule for all ports.
     - **Specific ports:** Click **+**, and then enter a port number, port list, or port range. Use a comma to separate values. Ports in a range are separated with a hyphen.
   - **Remote IPs and Ports:** Options on this page are the same as Local IPs & Ports page.
9. Click **Finish**.
10. Enter a name and description for the rule.
11. Place at the top of the rule list, and select to run the rule first.

Application Firewall Rules

Application Firewall rules tailor the protection closer to the applications and the specific network environment being protected.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. Select a rule group from the **Rule Groups** pane.
6. Select the **Application Firewall** rules category.
7. Click **Create New Rule** to start the rule wizard.
    - **Application**
        - **Full Path:** BeyondInsight compares the path stored in the firewall rule to the path of the application requesting network access. The rule triggers when there is a match. Select this option for applications that are typically updated during normal use.
        - **Process Name:** BeyondInsight compares the application process name to the process that is requesting network access. The rule triggers when there is a match. This is the least secure option.
        - **MD5:** BeyondInsight creates and stores an MD5 checksum of the specified application. The MD5 algorithm is a method for signing and verifying a file and its contents mathematically. At run-time, BeyondInsight compares this MD5 checksum to the checksum of the application that is requesting network access. The rule triggers when there is a match. This is the default value and the most secure option; however, if the application changes during an auto-update, the rule becomes invalid. If selected, enter the MD5 value.
        - **System Process:** Filters the system process requests from the Operating System or Kernel Drivers running under a system context. Typical system processes include printing and file sharing.
    - **Action**
        a. **Allow:** Allow traffic that matches the rule can pass through the firewall.
        b. **Deny:** Traffic that matches the rule cannot pass through the firewall.
        c. **Ask:** Displays a message requesting permission to pass through the firewall.
        d. **Log event:** Select to create an event log when the rule is matched.
        e. **Alert user:** Receive and log alerts from Blink when the rule is matched. This can create a lot of alerts and increase the size of the log file.
    - **Protocol:** Select a protocol, TCP or UDP.
    - **Traffic Direction**
        a. **Traffic from Other Computers:** Filters only inbound traffic received by your computer.
        b. **Traffic from This Computer:** Filters only outbound traffic sent from your computer.
        c. **Any Direction:** Filters both inbound and outbound traffic.
    - **Local IPs & Ports**
        a. **Rule applies to all IP addresses:** Create a rule for all local IP addresses.
        b. **Rule applies to all ports:** Create a rule for all ports.
        c. **Specific ports:** Click **+**, and then enter a port number, port list, or port range. Use a comma to separate values. Ports in a range are separated with a hyphen.
    - **Remote IPs and Ports:** Options on this page are the same as Local IPs & Ports page.

8. Click **Finish**.
9. Enter a name and description for the rule.
10. Place at the top of the rule list , and select to run the rule first.

IPS Signature Rules

You can create IPS network signatures that filter a specific protocol, such as FTP, ICMP, and SMTP. For example, you can create an application layer IPS signature that filters traffic from the subject line of all incoming or outgoing email messages associated with the email protocol. When you create an IPS signature rule, you can choose the Network Layer or Application Layer protocol. The wizard pages change depending on the protocol you select.

For the following procedure, the wizard pages described assume CGI Scripts and Network Layer options are selected.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
2. Click **Manage Rule Groups**.
3. Select a rule group from the **Rule Groups** pane.
4. Expand **IPS Signatures**, and select a subcategory to display the associated rules.
5. Click **Create New Rule** to start the wizard.
    - **Protocol:** Select a protocol.
    - **IP Protocol**
        - **Fragment Flags:** Check the box, and then select **More Fragment**, **Don't Fragment Bit**, or **Reserved Bit**.
            - **Set:** The binary value of the corresponding flag for **1s** only is verified.
            - **Not Set:** The binary value of the corresponding flag for **0s** only is verified.
        - **IP ID:** Select **Less Than**, **Equal To**, or **Greater Than**, and set the ID number.
        - **IP Protocol:** Select **Less Than**, **Equal To**, or **Greater Than**, and set the protocol.
        - **Time to Live:** Select **Less Than**, **Equal To**, or **Greater Than**, and set the time.
        - **IP Options:** Select **Record Route**, **End of Option List**, **No Operation**, **Internet Timestamp**, **Security**, **Loose Source Routing**, or **Strict Source Routing**.
        - **Type of Service:** Select the service: **Minimize Delay**, **Maximize Throughput**, **Maximum Reliability**, or **Minimize Monetary Cost**.
    - **Traffic Direction**
        - **Inbound:** Filters only inbound traffic received by your computer.
        - **Outbound:** Filters only outbound traffic sent from your computer.
        - **Both:** Filters both inbound and outbound traffic.
    - **Local IPs and Ports**
        - **Rule applies to all IP addresses:** Create a rule for all local IP addresses.
        - **Specific local IP addresses:** Click **+**, and then select **Determine IP(s) at run-time**, **Single IP**, **IP Range**, or **Subnet**. Click **Set**.
        - **Rule applies to all ports:** Create a rule for all ports.
        - **Specific ports** Click **+**, and then enter a port number, port list, or port range. Use a comma to separate values. Ports in a range are separated with a hyphen.
    - **Remote IPs & Ports:** Options on this page are the same as Local IPs & Ports page.

- **Search Pattern**
  - Click **+**, and then type the pattern to search on. You can create patterns using hex characters or a combination of ASCII and hex characters. A hex sequence must be enclosed in **< >**.
  - **Start:** *(Optional)* Enter the number of bytes to skip from the beginning of the packet's payload.
  - **Depth:** Enter the total number of bytes to search in the packet's payload.
  - **Trigger rule if pattern not found:** *(Optional)* Stop the action from completing when the pattern is matched.
  - **Use regular expressions:** *(Optional)* Find a specific word followed by an alphanumeric.
  - **Match case on pattern:** *(Optional)* Find a pattern that matches the case in the Pattern field.
  - **Match only on patterns of same size:** *(Optional)* Find a pattern that matches the size in the Pattern field.
- **Action**
  - **Stop attack:** Stop the attack by terminating the session or dropping packets.
  - **Capture Packets:** Hold the packet for review by the user.
  - **Block IP for:** Stop the attack for the specified number of minutes. Available only for TCP-based IPS signatures. This is not recommended for spoofable protocols, such as IP, UDP and ICMP. In a spoofable attack, an attacker mimics the IP address of critical systems and then forces the IP address to be added to the banned list.
  - **Log event:** Create an event log when the rule is matched.
  - **Alert user:** Receive and log alerts from RPA when the rule is matched. This can create a flood of alerts and increase the size of the log file.
- Specify Threshold
  - **Take action for every occurrence of the event:** When the pattern is found, the action defined on the Action page occurs.
  - **Take action when the threshold is exceeded:** When the threshold is exceeded, the action defined on the Actions page occurs. The default is one event every one second.
- Specify References
  - *(Optional)* Enter more information about the vulnerabilities and exploits. The information helps to define what the IPS signature protects against.
  - **Rule severity:** Select a severity between **0** and **9** (highest severity). The severity level is included in the event log.

6. Click **Finish**.
7. Enter a name and description for the rule.
8. Place at the top of the rule list, and select to run the rule first.

Trusted and Banned IPs

You can set trusted and banned IP addresses to manage lists of hosts processed by the Firewall and IPS protection engines. You must activate Intrusion **Prevention** or **System Firewall** to use the **Trusted and Banned IPs** feature.

- Trusted IPs: Adds the IP address or range of IP addresses of trusted critical machines. All data is then allowed from the trusted systems.

> ***Note:*** *If a trusted system attacks your BeyondInsight-protected server or workstation, the attack will not be detected.*

- Banned IPs: Provides time-based traffic blocking from an IP address. You can ban an IP for a period of time or indefinitely. Data flowing from known problematic hosts can be discarded without further processing.

If an IP address is added to the Trusted list and Banned list, that IP address is banned. All IPS Analyzer rules and signatures can be configured to ban the attacker IP for a certain amount of time.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. Select a rule group from the **Rule Groups** pane.
6. Select the **Trust IPs** or **Banned IPs** rule category.
7. Click **Create New Rule** to start the wizard.
8. Enter the IP address, IP address range, or subnet.
9. Specify the time the IP remains on the list as either **Permanent** or **Keep for [n] Minutes**. You can also include a date and time. The IP address is automatically deleted from the IP list after the time period elapses.
10. Enter a description for the IP address.
11. Click **Set**. The IP address displays in either **Trusted IPs** or **Banned IPs** list.
12. Click **Update**.

Registry Protection Rules

Registry rules protect registry resources against unauthorized modifications.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. Select a rule group from the **Rule Groups** pane.
6. Select the **Registry** rule category.
7. Click **Create New Rule** to start the wizard.

   - **Resource Type:** Registry is selected.
   - **Resource Path**
     - **Registry Key Path:** Enter the registry path.
     - **Match Type:** Select a matching type.
   - **Caller Path**
     - **Caller Path:** Enter the path.
     - **Match Type:** Select a matching type.
     - **Exact:** Matches only the exact path. This is the fastest matching.
     - **Partial:** Matches if the pattern is found anywhere in the path. This is the second fastest matching.
     - **Wildcard:** Creates more complex rules that use * for any sequence of characters, # for any single numerical character and ? for any single alpha character.
     - **Regex:** Creates the most complex matching rules. This can be the slowest and should be used with care.
   - **MD5 Validation**
     - Do not use caller MD5.
     - **Auto-calculate caller MD5:** Calculates MD5 if access to the file is provided on disk.
     - **User specified caller MD5:** Enter a hex MD5 caller. The MD5 algorithm is a method for signing and verifying a file and its contents mathematically. At run-time, BeyondInsight compares this MD5 checksum to the checksum of the application that is requesting network access. There is an implicit OR between the two types of matching, such as location and MD5 checksum. If either matches, the rule is triggered.
   - **Specify an Action:** Select a **Read** or **Write** action to be matched by this rule.
     - **Allow:** Allow traffic that matches the rule can pass through the firewall. This is the default.
     - **Deny:** Deny traffic that matches the rule cannot pass through the firewall.
     - **Log:** Select to create an event log when the rule is matched.
     - **Alert:** Receive and log alerts when the rule is matched. This can create a lot of alerts and increase the size of the log file.
8. Click **Finish**.
9. Enter a name and description for the rule.
10. Place at the top of the rule list, and select to run the rule first.

Execution Protection Rules

Execution rules prevent the system from executing unauthorized processes.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. Select a rule group from the **Rule Groups** pane.
6. Select the **Execution** rule category.
7. Click **Create New Rule** to start the wizard.
    - **Resource Type: Execution** is selected.
    - **Resource Path**
        a. **Registry Key Path:** Enter the registry path.
        b. **Match Type:** Select a matching type. See Caller Path page details for descriptions.
    - **Caller Path**
        a. **Caller Path:** Enter the path.
        b. **Match Type:** Select a matching type.
        c. **Exact:** Matches only the exact path. This is the fastest matching.
        d. **Partial:** Matches if the pattern is found anywhere in the path. This is the second fastest matching.
        e. **Wildcard:** Creates more complex rules that use ***** for any sequence of characters including, **#** for any single numerical character and **?** for any single alpha character.
        f. **Regex:** Creates the most complex matching rules. This can be the slowest and should be used with care.
    - **MD5 Validation**
        a. Do not use caller MD5
        b. **Auto-calculate caller MD5:** Calculates MD5 if access to the file is provided on disk.
        c. **User specified caller MD5:** Enter a hex MD5 caller. The MD5 algorithm is a method for signing and verifying a file and its contents mathematically. At run-time, BeyondInsight compares this MD5 checksum to the checksum of the application that is requesting network access. There is an implicit OR between the two types of matching, such as location and MD5 checksum. If either matches, the rule is triggered.
    - **Specify an Action**
        a. The **Execute** box is checked and cannot be changed.
        b. **Allow:** Allow traffic that matches the rule can pass through the firewall. This is the default.
        c. **Deny:** Deny traffic that matches the rule cannot pass through the firewall.
        d. **Log:** Select to create an event log when the rule is matched.
8. Click **Finish**.
9. Enter a name and description for the rule.
10. Place at the top of the rule list, and select to run the rule first.

File Integrity Rules

There are three types of integrity rules:

- **Protected files:** Folders and files that you want to monitor for changes.
- **Authorized applications:** Applications which are allowed to modify any file.
- **Custom rules:** Exceptions to any other rules. Custom rules are processed first.

A file protection rule activates when the protected file is changed, renamed, or deleted.

Add a Protected File Rule

A protected file rule applies PowerBroker EPP protection on the file.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. Select a rule group from the Rule Groups pane. You can type the name of the rule group in the text box to search for the rule group.
6. Select the **File Integrity** rule category and select the **Protected Files** subcategory to display the associated rules.
7. Select **Create New Rule**.
8. Complete the following pages.
9. Specify **File and Folder** Path
10. Protect a file
11. Enter the file that you want to protect.
12. Protect files inside a directory
13. Enter a folder name that you want to protect.
14. Enter a list of file extensions that you want to protect.
15. Select the **Also Protect Subfolders** check box to protect all folders in the directory.
16. Specify an action
17. Select the **Log** check box to track the rule activities.
18. Set the rule severity. The severity level is included in the event log. The default value is 1.
19. You can also create a category to organize rules.
20. Click **Finish**.
21. Enter a name and description for the rule.
22. Place at the top of the rule list, and select to run the rule first.

Add an Authorized Application Rule

An authorized application rule allows an application to access protected files.

1. Select the **Dashboard > Protect**.
2. Click **Manage Rule Groups**.

3. Select a rule group from the **Rule Groups** pane.
4. Select the **File Integrity** rule category, and select the **Authorized Applications** subcategory to display the associated rules.
5. Select **Create New Rule**.
6. Complete the following pages.
    - **Specify Authorized Application Path:** Enter the caller attributes:
        - **File Path:** Browse to the executable location for the caller, and then select the matching type:
            - **Exact:** Matches only the exact registry key. This is the fastest matching.
            - **Contains:** Matches if the pattern is found anywhere in the key. This is the second fastest matching.
            - **Not Contains:** Matches when the pattern is not found.
            - **Wildcard:** Creates more complex rules that use * for any sequence of characters, # for any single numerical character and ? for any single alpha character.
            - **Regex:** Creates the most complex matching rules. This can be the slowest matching.
        - **Process Arguments:** Add process arguments to filter the scope of the rule.
        - **MD5 or SHA1:** Enter a hex MD5 or SHA1 caller. The MD5 or SHA1 checksum algorithm is a method for creating a file content checksum and verifying the content has not changed. SHA1 is a more secure hashing algorithm and is recommended over MD5.
        - **File Size:** Enter the file size.
        - **Executable is packed:** Select **True** to pack the executable.
        - **File Location:** Select **Hard drive**, **USB**, **CDROM**, or **Network Share**.
        - **Product Name, Product Description, Company:** Enter the product information.
        - **Digital Signature Name, Digital Signature Validity:** Select the signature parameters.
        - **Process Owner:** Enter the name of the user account running the executable. Alternatively, enter the SID for the process owner.
        - **User Group:** Enter one or more user groups. If the user running the executable belongs to one of the listed groups, the property will match. Alternatively, enter the SID for the user group.
    - **Specify Severity:** Set the rule severity. The severity level is included in the event log. The default value is **1**. You can also create a category to organize rules
7. Click **Finish**.
8. Enter a name and description for the rule.
9. Place at the top of the rule list, and select to run the rule first.

Add a Custom Rule

A custom rule applies protection on a folder. Files and folders included in the rule are not included in the scheduled scan.

1. Select the **Dashboard** tab and click **Protect**; or select the **Assets** tab and click **Protect**.
2. Click **Manage Rule Groups**.
3. Select a rule group from the **Rule Groups** pane.
4. Select the **File Integrity** rule category and select the **Custom** subcategory to display the associated rules.
5. Select **Create New Rule**.

6. Complete the following pages.
    - **Specify File/Folder Path**
        - **Protect a file:** Enter the file that you want to protect.
        - **Protect files inside a directory:** Enter the folder name that you want to protect. Enter a list of file extensions that you want to protect.
        - **Also Protect Subfolders:** Check the box to protect all folders in the directory.
    - **Specify Authorized Application Path:** Enter the caller attributes:
        - **File Path:** Browse to the executable location for the caller, and then select the matching type:
            - **Exact:** Matches only the exact registry key. This is the fastest matching.
            - **Contains:** Matches if the pattern is found anywhere in the key. This is the second fastest matching.
            - **Not Contains:** Matches when the pattern is not found.
            - **Wildcard:** Creates more complex rules that use * for any sequence of characters, # for any single numerical character and ? for any single alpha character.
            - **Regex:** Creates the most complex matching rules. This can be the slowest matching.
        - **Process Arguments:** Add process arguments to filter the scope of the rule.
        - **MD5 or SHA1:** Enter a hex MD5 or SHA1 caller. The MD5 or SHA1 checksum algorithm is a method for creating a file content checksum and verifying the content has not changed. SHA1 is a more secure hashing algorithm and is recommended over MD5.
        - **File Size:** Enter the file size.
        - **Executable is packed:** Select **True** to pack the executable.
        - **File Location:** Select **Hard drive**, **USB**, **CDROM**, or **Network Share**.
        - **Product Name, Product Description, Company:** Enter the product information.
        - **Digital Signature Name, Digital Signature Validity:** Select the signature parameters.
        - **Process Owner:** Enter the name of the user account running the executable. Alternatively, enter the SID for the process owner.
        - **User Group:** Enter one or more user groups. If the user running the executable belongs to one of the listed groups, the property will match. Alternatively, enter the SID for the user group.
    - **Specify an Action:** Select the action to take when the rule is matched: Allow or Deny. Select the **Log** check box to track the rule activities. Set the rule severity. The severity level is included in the event log. The default value is **1**. You can also create a category to organize rules.
7. Click **Finish**.
8. Enter a name and description for the rule.
9. Place at the top of the rule list, and select to run the rule first.

Windows Events Rules

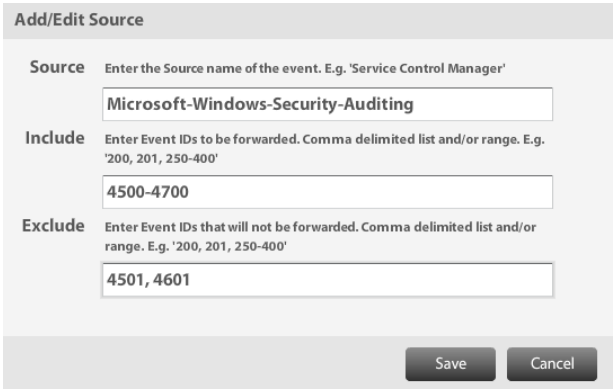
You can create a rule that tracks Windows Event logs.

Source Names

The source name is the name of the Windows event. The source name you enter depends on the operating system that is forwarding the events.

Windows XP Windows 2003	Use the name in the **Windows Event Viewer Source** column.
Vista Windows 7 Windows 2008	Use **System-Provider[EventSourceName]** on the **Details** tab of the event, if available. Otherwise, use **[Name]**.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. Select a rule group from the **Rule Groups** pane.
6. Expand **Windows Events**, and then select **Application**, **System**, or **Security**.
    - **Enabled:** Check the box to activate the rule. One or more Windows event sources must be provided to activate the rule. Events are only forwarded when a source is provided.
    - **Severity:** Select the severity level from the list: **Only Errors**, **Errors and Warnings**, or **All**.
    - **Add:** Click to provide the following information about the event log you want to track:
        - **Source name:** The name of the application that issued the event. You can enter the source name without providing Event IDs. All events from the source will be forwarded.
        - **Include:** Enter the Event IDs to forward to BeyondInsight.
        - **Exclude:** Enter the Event IDs to exclude. The excluded list overrides the included list.



7. Click **Save**.

Trusted List Options

The Trusted List displays trusted malware by name and category.

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

3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. Select a rule group from the **Rule Groups** pane.
6. Select the **Trusted List** rule category.
7. Click **Create New Rule** to start the wizard.
8. Check the box, and click **Save**.
9. Click **Update**.

Miscellaneous Options

Miscellaneous options allow you to set rules for BeyondInsight operations.

1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Click **Protect**.
4. Click **Manage Rule Groups**.
5. Select a rule group from the **Rule Groups** pane.
6. Expand **Misc. Options** , and select a subcategory:
    - Virus and Spyware
    - General
    - System Protection
    - Scheduler
    - Auto-Updater
    - Vulnerability Assessment
    - Intrusion Prevention
    - IIS Protection
    - Firewall
    - Events
7. After you change the properties for a subcategory, click **Update**.

Set and Run Regulatory Reports

> ***Note:*** *The Regulatory Reporting packs require a license to activate the feature set. Contact your BeyondTrust representative.*

You can run regulatory reports to ensure that your assets are in compliance. Review the following sections to learn more about the compliance scan templates available, compliance coverage, running a scan, and reviewing scan results.

Compliance Scans

By default the following scan templates are available.

- Healthcare
- Finance
- Government

> ***Note:*** *Government packs need an updated license key.*

ISO-27002 Scans

Compliance Area	Section 12.6.1 Control of technical vulnerabilities

COBiT Scans

Compliance Area	Section DS11.6 Security Requirements for Data Management

Healthcare Pack Compliance Scans

The Healthcare Pack includes a HIPAA scan template. Contact BeyondTrust for a license key to activate the compliance pack.

HIPAA Scans

Compliance Area	Section 164.308 Administrative safeguards, (a)(8) Standard: Evaluation.

Finance Pack Compliance Scans

The Finance Pack includes a SOX and GLBA scan template. Contact BeyondTrust for a license key to activate the compliance pack.

GLBA Scans

Compliance Area	Section 6801 Protection of nonpublic personal information.

SOX Scans

Compliance Area	Section 404 Management Assessment of Internal Controls.

Government Pack Compliance Scans

The Government Pack includes the FERC-NERC, NIST 800-53, and MASS 201 scan templates. Contact BeyondTrust for a license key to activate the compliance pack.

Compliance Area	CIP-005-3 R4 Cyber Vulnerability Assessment

NIST-800-53 Scans

Compliance Area	SA System and Services Acquisition; SA-10 Developer Configuration management

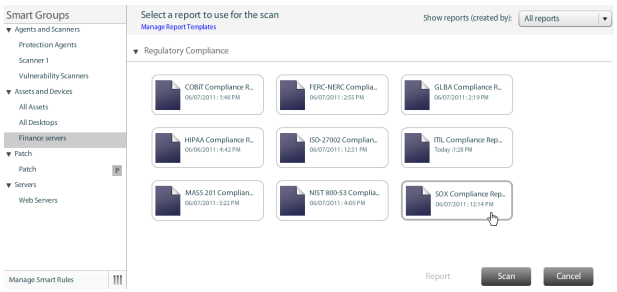
MASS 201 Scans

Compliance Area	Section 17.03(2)(b)(3) Duty to Protect and Standards for Protecting Personal Information - Detect and Prevent Security Systems Failures

Run and Review Compliance Scans

For more information, please see "Run Vulnerability Scans" on page 73.

1. Select **Scan**.
2. Select the scan template
3. Select the scan options, and then click **Start Scan**.
4. Scroll through the list of vulnerabilities provided in the report. You can review remediation fixes, CVSS scores, and additional information for the vulnerability.



Set and Run Compliance Reports

***Note:** The **Configuration Compliance Module** requires a license to activate the feature set. Contact your BeyondTrustrepresentative.*

The following tools are available to run benchmark scans:

- **XCCDF audit groups:** The **Secure Configuration Audits** audit group ships with the **Configuration Compliance** module. Use this audit group to run your scan.
- **Benchmark configuration:** Import benchmark templates, synchronize templates, and review versions of benchmark templates that ship with BeyondInsight.
- **Configuration Compliance Reports:** Includes two reports, **Benchmark Compliance Report** and **Benchmark Expor Report**.

For information about running scans, please see "Run Vulnerability Scans" on page 73.

Set Permissions to Run Configuration Compliance Scans

You must create a group and set permissions for the group to run scans.

1. Select **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Click **Create New Group**.
4. Select **Create a New Group**.
5. Enter a name and description.
6. Click **Create Group**.
7. Select the **Benchmark Compliance** feature, and then click **Assign Permissions**.
8. Select **Assign Permissions Full Control**.
9. Add your configuration compliance users to the group.

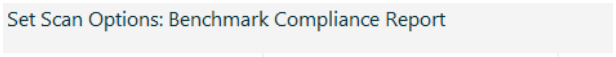
For more information, please see "Create and Manage User Accounts" on page 39.

Run and Manage Benchmarks

The settings for configuring a benchmark scan are similar to vulnerability scans.

For more information, please see "Run Vulnerability Scans" on page 73.

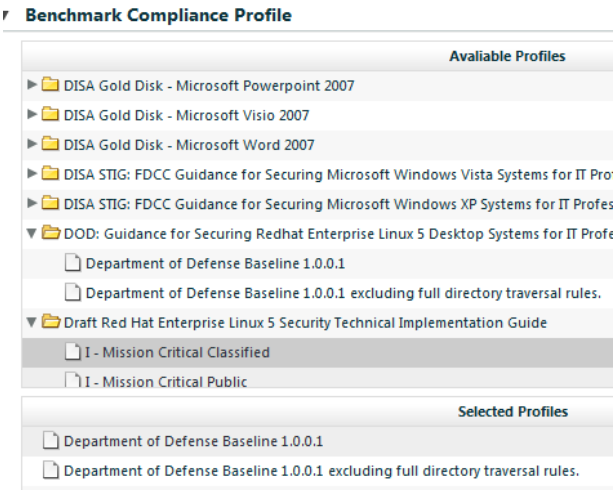
You must select the benchmark profiles that you want to include in the scan. You can select more than one profile if needed.



View Benchmark Scan Results

The benchmark scan data can be saved in the following formats:

- SCAP output (zip)
- Full ARF
- Micro ARF
- NIST ARF
- Expanded CSV



Manage Benchmarks

BeyondInsight ships with a default set of benchmark templates. You can import additional or updated benchmarks and synchronize benchmarks. If you are working with your benchmark profiles outside BeyondInsight, you can synchronize the templates using the BeyondInsight configuration tool.

1. In the BeyondInsight console, select **Configuration > Discovery and Vulnerability Management > Benchmarks**.
2. Expand a benchmark to see more detail. Policies included with benchmark templates can be inactivated if they do not apply. Clear policies as needed.
3. To import templates, click **Import New Benchmark**, navigate to the file and click **Open**. To overwrite an existing template click **Yes**.
4. To download an editor to change your benchmarks, click the **Download Editor** button.

Import Benchmarks

You can import **.cab** or **.zip** files that include the following:

- For Windows 7:
  - CIS_Windows_7_Benchmark_v1.1.0_oval.xml
  - CIS_Windows_7_Benchmark_v1.1.0.xml

  - Windows-7-cpe-oval.xml
  - Windows-7-cpe-dictionary.xml
- For Windows Server 2008:
  - CIS_Windows_2008_Server_Benchmark_v1.1.0_oval.xml
  - CIS_Windows_2008_Server_Benchmark_v1.1.0.xml
  - Windows-2008-cpe-oval.xml
  - Windows-2008-cpe-dictionary.xml

Set the OVAL Tests Option

You can store **OVAL XML** data to the BeyondInsight database. If selected, OVAL values are used to determine if a rule was compliant. They are then parsed from OVAL output files and stored in the BeyondInsight database.

To store OVAL tests in **Benchmark Reports**:

1. Select **Configuration > Discovery and Vulnerability Management > Benchmark Options**.
2. Click the slider to enable the **Store OVAL tested and found** option.
3. Click **Update Benchmark Compliance Options**.

BeyondInsight Clarity Analytics

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

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

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

As a result, the behavior analytics:

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

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

- Endpoint Privilege Management
- Privilege Management for Unix & Linux
- BeyondTrust Network Security Scanner
- Password Safe
- Third Party Imports

Configure BeyondInsight Clarity Analytics

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

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

Set Risk Analytics Values

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

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

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

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

Clarity Reports

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

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

Use the Clarity Dashboard

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

- Endpoint Privilege Management
- Privilege Management for Unix & Linux
- BeyondTrust Network Security Scanner
- Third-Party Vulnerability Scanners

Triggers

The following triggers identify assets that are at risk.

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

First Password Release Request	• Password Safe events. • User requests password for an account and system they have never requested before.
Unusual Password Release Request	• Password Safe events. • User does not retrieve the password for approved request or the password is retrieved more than once.
Concurrent Password Release Request	• Password Safe events. • User tries to acquire more than one password at a time.
Malware Detected	• Malware is detected on an asset.

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

Risk Events by Threat Level

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

Risk Events by Application

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

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

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

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

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

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

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

View Cluster Maps

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

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

Cluster Map Numbering

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

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

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

Cluster Shading

Asset

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

User

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

Asset Cluster Attributes

There are eight cluster attributes organized in the following categories:

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

Attribute	Type	Description
Attacks	Ordering	Number of detected attacks. Greater value means more detected attacks.
Vulnerable Apps	Ordering	Number of launches of vulnerable applications. Greater value means more started/running vulnerable applications.
Risk	Ordering	Asset risk. Greater value means greater risk.
App Set	Ordering	Running or/and elevated (depends on PowerBroker for Windows settings) applications.
Vulnerabilities Set	Pattern	Discovered vulnerabilities.
Service Set	Pattern	Services

Attribute	Type	Description
Software Set	Pattern	Installed software packages.
Port Set	Pattern	Opened ports.

User Cluster Attributes

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

Analyze Cluster Maps

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

For more information, please see "BeyondInsight Clarity Analytics" on page 205.

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

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

Analyze Cluster Grids

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

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

To view the cluster grid, follow the steps.

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

Alerts

There are two types of alert:

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

Alert	Type	Description
a1	pattern	Maps all characteristics of an event into a single internal cluster using self-organizing maps clustering. Similar event characteristics lead to the same cluster. Thus, clusters with high share of mapped events represent typical behavior, while clusters with small number of events indicate outliers. Each user, host, or asset's characteristics are tracked independently with independent sets of clusters. ***Note:*** *Clusters are hidden and are used only for analysis. They do not behave the same as asset clusters.* **Used characteristics:** • Endpoint Privilege Management events, per User: **EventType**, **Exercised privilege**, **Path**, **Asset**, **Launch weekday and time** • Privilege Management for Unix & Linux events, per RunHost: **RunCommand**, **RunCWD**, **PBLUUser**, **MasterHost**, **SubmitHost**, **FinishStatus**, **Launch weekday and time**, **Accept**, **RiskLevel** • Vulnerability events, per Asset: Vulnerability type, Risk • Attack events, per Asset: Attack type, Category
a2	explicit	Untrusted Application Default value: 0.33 • If the application is unsigned, then value = value + 0.33 • If application has no version information, then value = value + 0.33
a3	explicit	Vulnerable Application Vulnerability of launched application.
a4	explicit	Asset Risk
a5	explicit	Event Timing Event time within working hours and weekday Default value: 0.33 • If EventTime < WorkingHoursStart or EventTime > WorkingHoursEnd, then value = value + 0.33 • If EventDay is in WorkingWeekDaysMask, then value = value + 0.33

Alert	Type	Description
a6	explicit	Untrusted User Default value: 0.33 • If user is local (not domain) user, then value = value + 0.33 • If user is administrator, then value = value + 0.33
a7	explicit	First App Launch The alert is flagged when a user launches an application they have never launched before.
a8	explicit	First request for given managed account and system (Password Safe). The alert is flagged when a user request password for account and system have never requested before.
a9	explicit	Unusual password releases (Password Safe) The alert is flagged when a user does not retrieve the password for approved request or the password is retrieved more than once.
a10	explicit	Concurrent password requests (Password Safe). The alert is flagged when a user tries to acquire more than one password at a time.

BeyondInsight Clarity Malware Analysis

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

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

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

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

. For more information, please see "Run Vulnerability Scans" on page 73.

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

Configure Clarity Malware

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

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

Review Malware Information and Reports

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

- High
- Medium
- Low

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

Use Reports to Analyze Results

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

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

Top 10 Assets by Total Threat Level Report

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

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

Event Review - Malware Report

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

Configure a Claims-Aware Website in BeyondInsight

You can configure a claims-aware website to bypass the current BeyondInsight login page and authenticate against any configured Federated Service that uses SAML 2.0 to issue claims.

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

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

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

Create a BeyondInsight Group

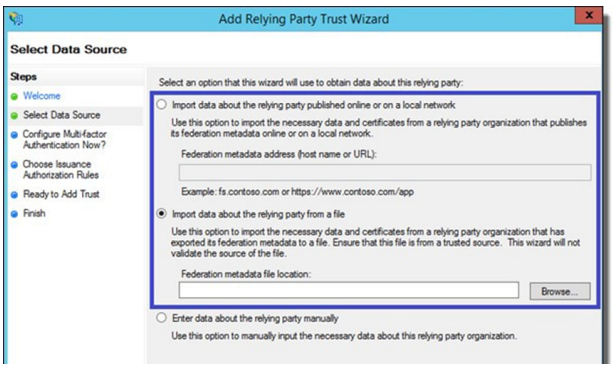
Create a BeyondInsight group and ensure the group is assigned the **Full Control** permission to the **Management Console Access** feature.

Add Relying Party Trust

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

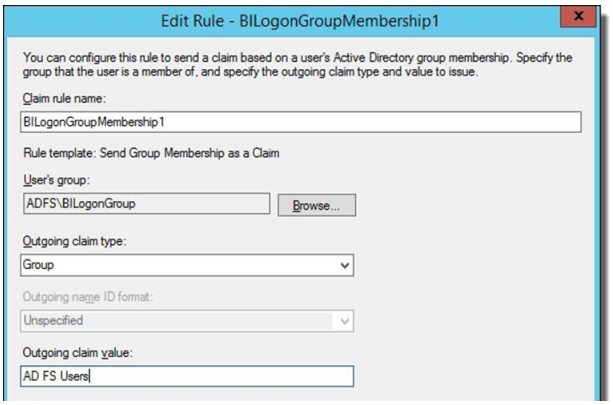
The metadata is located in the following directory:
<Install path>\eEye Digital Security\Retina CS\WebSiteClaimsAware\FederationMetadata\2007-06

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



Set Up Claim Rules

Note: *Claims rules can be defined in a number of different ways. The examples provided are 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*** *and a single outgoing claim of type* ***Name****, then BeyondInsight has enough information to potentially grant access to the site to the user.*



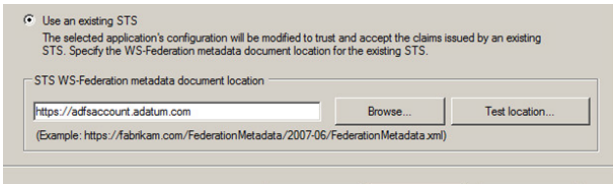
Supported Federation Service Claim Types

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

Claims-Aware SAML

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

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



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

Manage Privilege Management for Unix & Linux, Essentials Edition Events

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

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

View Run Arguments and IO Logs

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

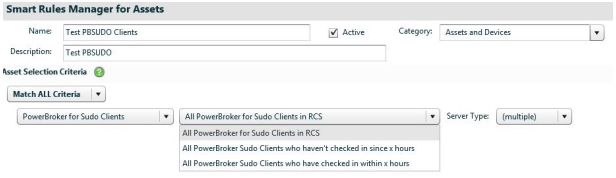
1. Select **Assets**.
2. Click the **Legacy Assets View** link.
3. Select PowerBroker for Sudo from the list.
4. Click **i** for an asset.
5. Click the **Run Arguments** tab or **IO Logs** tab to view more information.

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

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

Create a Sudo Client Smart Group

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



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

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

Create a Sudo Events Smart Group

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

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

Manage Endpoint Privilege Management User Policies

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

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

Create a Smart Rule

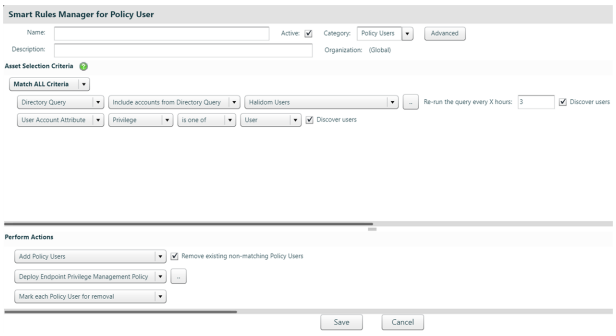
When a policy is deployed using a policy user based smart rule, only the policy rules set in the **User Configuration Rule Management** section of the policy are processed by Endpoint Privilege Management clients that receive the policy. Policy deployment is controlled by the specifications in the smart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

To deploy policies, you need to first create your rules and policies in the Endpoint Privilege Management Policy Editor, and then you can log into BeyondInsight to create the smart rule.

A policy user based smart rule can only deploy policies to Windows Active Directory domain users.

Create Smart Rule using Smart Rules Manager for Policy User

1. From the Home page in the BeyondInsight console, select **Policies**.
2. From the **Smart Groups** pane, click **Manage Smart Rules**.
3. From the **Smart Rules Manager for Policy User**, click **New**.
4. Provide a name and description for the policy.
5. Select **Policy User** for the category.
6. From the **Asset Selection Criteria** section, select your desired filters to add the Endpoint Privilege Management accounts.
7. From the **Perform Actions** section, select the following:

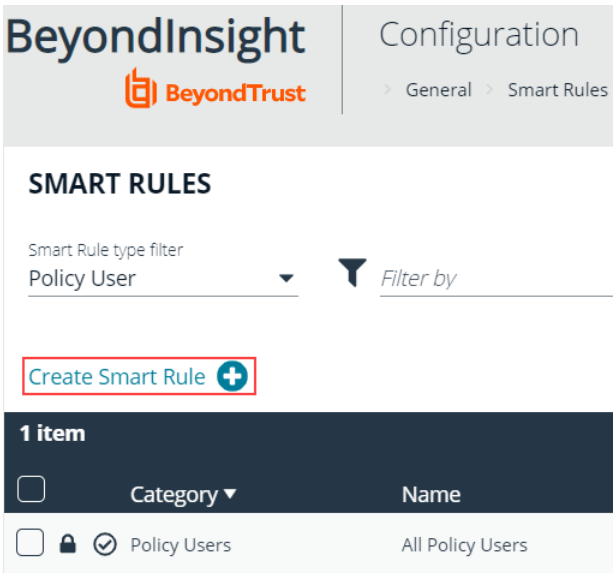


   - **Add Policy Users:** Add users to BeyondInsight.
   - **Deploy Endpoint Privilege Management Policy:** Deploys policies to the user accounts.
   - **Mark each policy user for removal:** Deletes the user accounts from the smart group.
   - **Show as Group:** Displays the smart rule as a smart group on the **Policies** page.
8. Click **Save**.

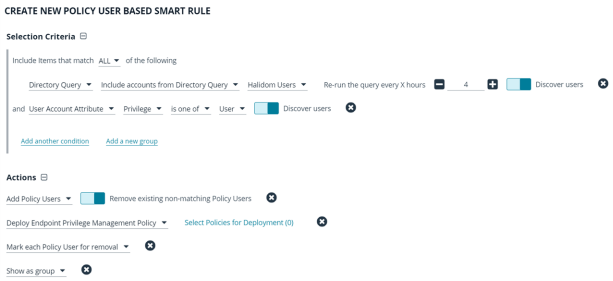
Create Policy User Based Smart Rule Using the New Smart Rules View

1. From the Home page in the BeyondInsight console, select **Policies**.
2. Click the **New Smart Rules View** link in the top right corner of the page.

3. Click **Create Smart Rule**.



4. Select **Policy User** for the category.
5. Provide a name and description for the policy.
6. From the **Selection Criteria** section, select your desired filters to add the Endpoint Privilege Management accounts.
7. From the **Actions** section, select the following:
   - **Add Policy Users:** Add users to BeyondInsight.
   - **Deploy Endpoint Privilege Management Policy:** Deploys policies to the user accounts.
   - **Mark each policy user for removal:** Deletes the user accounts from the smart group.
   - **Show as Group:** Displays the smart rule as a smart group on the **Policies** page.



8. Click **Create Smart Rule**.

View Users in the Console

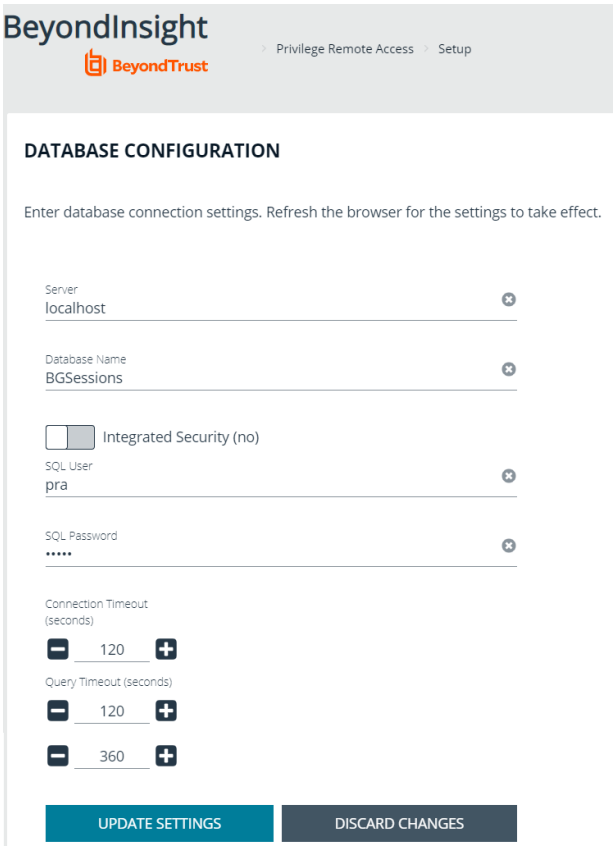
After the smart rule processes, you can view policy users on the **Policies** page. This page shows the policies assigned and applied. In the console, select **Policies** on the Home page to view users.

View Privileged Remote Access Session Data

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

Configure the Privileged Remote Access Database Connection

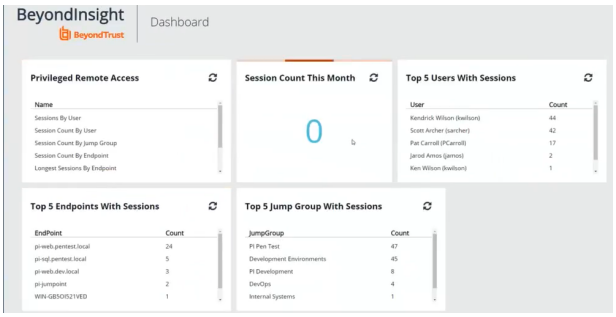
1. Select **Configuration**.
2. Under **Privileged Remote Access**, select **Database Configuration**.
3. Provide the settings to connect to your Privileged Remote Access export database, and then click **Update Settings**.



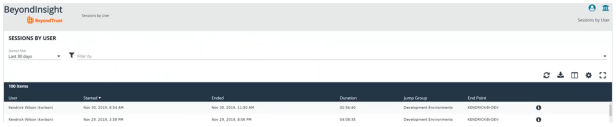
View the Privileged Remote Access Dashboard

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

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



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



Monitor BeyondInsight Services

On the **Services** page, you can see the status of a service. Additionally, you can view the log files to troubleshoot potential problems with a service.

1. Select **Configuration > General > Services**.
2. Click **View** to open and review details in the log.
3. Click **Email** to send the log to selected email addresses.

Turn on Debug Logging

1. Select **Configuration > General > Services**.
2. Click **Enable Debug Logging**. All BeyondInsight services are restarted if you turn on debug logging.

Turn off debug logging after you finish troubleshooting BeyondInsight to improve performance.

Change the Credentials for a Service

1. Select **Configuration > General > Services**.
2. Click the square button.
3. Enter the credentials, and then click **OK**.

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.

To learn more about the PSRUN tool and using the API, please see the Password Safe API Guide and Password Safe PSRUN User Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/ps/.

1. Select **Configuration > General > APi Registration**.
2. Click **Create API Registration** to create a new application registration.
3. Enter a name for the new registration, and then click **Create**.

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

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

4. To configure a new registration or modify an existing one, select the registration, and then set the **Authentication Rule Options**.

    a. **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.

    b. **User Password Required:** If enabled, an additional authorization header value containing the **RunAs** user password is required with the web request. If not enabled, this header value does not need to be present and is ignored if provided. Square brackets surround the password in the header.
    `Authorization=PS-Auth key=c479a66f…c9484d; runas=doe-main\johndoe; pwd=[un1qu3];`

    c. **Verify PSRUN Signature:** The PSRUN signature is an extra level of authentication. It iscomputed from the factors using a shared secret between the client and server. PSRUN sends the signature as part of the header during its API request. If enabled, the server will recompute the signature during factor validation and compare it against the one sent by the client. If the signatures matches, the client's identity is considered verified. The signature effectively keeps the client in sync with the server. Changing the secret on the server requires the client to be rebuilt and guarantees that out-of-date clients cannot authenticate.

5. On the **Details** page, click **Add Authentication Rule** to create authentication rules. At least one IP rule, PSRUN rule, valid source IP address (IPv4 or IPv6), IP range, or CIDR from which requests can be sent for this API Key is required. Enter one IP address, IP Range, or CIDR per line.

    X-Forwarded-For rules can also be created by providing a valid source IP address (IPv4 or IPv6), an IP range, or CIDR. In a load-balanced scenario, IP Authentication rules are used to validate the load balancer IP(s), and the X-Forwarded-For header is used to validate the originating client IP. Existing rules cannot be changed from an IP Rule to a X-Forwarded-For Rule or

vice-versa. If an X-Forwarded-For rule is configured, it is required for the HTTP Request . If the X-Forwarded-For header is missing, the request will fail with a 401 unauthorized error.

6. Click **Create Rule**.

Support and Product Updates

Send Files to BeyondTrust Technical Support

Create a Support Package

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

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

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

To generate the package:

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

Send Analysis Files

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

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

To generate analysis files:

1. From the menu, select **About**.
2. From **Support Tools > Send Analysis to Support**, click **Send Analysis to Support**. This generates an analysis file and sends it to support.

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

Download Updates

BeyondInsight ships with BeyondTrust Updater.

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