



# BeyondTrust

## **Endpoint Privilege Management BeyondInsight Platform User Guide**

# Table of Contents

---

<b>Use Endpoint Privilege Management Features in BeyondInsight</b>	<b>4</b>
<b>Manage Endpoint Privilege Management Events</b>	<b>5</b>
<b>Exclude Endpoint Privilege Management Events</b>	<b>6</b>
<b>Manage Endpoint Privilege Management Policies</b>	<b>7</b>
View Endpoint Privilege Management Policies	7
Deploy Policies to Assets and Policy Users Using a Smart Rule	8
Manage Global Priority for Endpoint Privilege Management Policies	9
<b>Overview of the Web Policy Editor</b>	<b>11</b>
<b>Create, View, and Edit Endpoint Privilege Management Policies</b>	<b>16</b>
Create a Policy	16
View a Policy	16
Edit a Policy	17
<b>Create and View Smart Rules for Endpoint Privilege Management Policy Users</b>	<b>19</b>
Create a Policy User Smart Rule	19
View Policy Users	21
<b>View Endpoint Privilege Management Agents</b>	<b>22</b>
<b>View Endpoint Privilege Management File Integrity Monitoring</b>	<b>23</b>
<b>Monitor Endpoint Privilege Management Sessions</b>	<b>24</b>
<b>View Endpoint Privilege Management Reports</b>	<b>25</b>
<b>Navigate the Endpoint Privilege Management Reporting Interface</b>	<b>26</b>
<b>Use Quick Filters and Advanced Filters</b>	<b>28</b>
<b>Overview of EPM Reporting Dashboards</b>	<b>38</b>
<b>Summary Dashboard</b>	<b>39</b>
<b>Events Dashboard</b>	<b>41</b>
<b>Discovery Dashboard</b>	<b>44</b>
Discovery Reports	45
<b>Actions Dashboard</b>	<b>50</b>
<b>Target Types Dashboard</b>	<b>51</b>
<b>Trusted Application Protection Dashboard</b>	<b>52</b>
<b>Users Dashboard</b>	<b>53</b>
User Experience Dashboard	53

---

Privileged Logons .....	53
Privileged Account Management .....	54

# Use Endpoint Privilege Management Features in BeyondInsight

When an Endpoint Privilege Management license is detected in BeyondInsight, you can view Endpoint Privilege Management events, file integrity monitoring events, and session details for monitored systems, from the BeyondInsight console. You can also view and deploy Endpoint Privilege Management policies, and view Endpoint Privilege Management agents.

If the Endpoint Privilege Management Web Policy Editor (WPE) is installed and configured you can view the details for each policy, unlock policies, edit policies, and delete policies.

If Endpoint Privilege Management Reporting is installed and configured, you can view dashboards and reports which may assist you with managing and auditing Endpoint Privilege Management activity in your environment.

The following sections provide details on using each of the above mentioned Endpoint Privilege Management features from the BeyondInsight console.

## Manage Endpoint Privilege Management Events

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

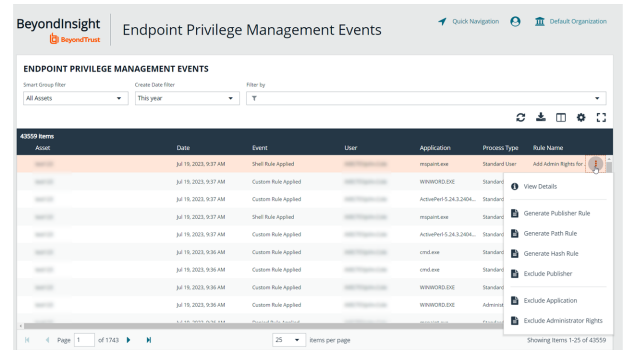


**Note:** This feature is available only when an Endpoint Privilege Management license is detected.

You can view and download all events for monitored systems and you can select an event to view more details about that specific event. You can also generate rules and create exclusions from listed events.

To view events, generate rules, create exclusions, and download events, follow the below steps:

1. From the left menu in the BeyondInsight console, click **Endpoint Privilege Management**.
2. By default, displayed events are filtered by the **Discovery Scanners** Smart Group. Select a Smart Group from the **Smart Group filter** dropdown to view events for that Smart Group.
3. To further filter the displayed events, use the **Create Date filter**, or **Filter by** criteria.
4. For additional details about an event, click the vertical ellipsis for the event, and then select **View Details**. A window opens displaying details related to Endpoint Privilege Management, the rule, and the application.
5. To create an exclusion or generate a rule from an event, click the vertical ellipsis for the event, and then select the appropriate exclusion or rule type to generate.
6. Click the **Download all** (down arrow) button above the grid to download the events to a CSV file.



Asset	Date	Event	User	Application	Process Type	Rule Name
...	Jul 19, 2023, 9:37 AM	Shell Rule Applied	...	mpm.exe	Standard User	...
...	Jul 19, 2023, 9:37 AM	Custom Rule Applied	...	WINWORD.EXE	Standard	...
...	Jul 19, 2023, 9:37 AM	Shell Rule Applied	...	mpm.exe	Standard	...
...	Jul 19, 2023, 9:37 AM	Custom Rule Applied	...	ActualPath 5.24.3.240...	Standard	...
...	Jul 19, 2023, 9:36 AM	Custom Rule Applied	...	cmd.exe	Standard	...
...	Jul 19, 2023, 9:36 AM	Custom Rule Applied	...	cmd.exe	Standard	...
...	Jul 19, 2023, 9:36 AM	Custom Rule Applied	...	WINWORD.EXE	Standard	...
...	Jul 19, 2023, 9:36 AM	Custom Rule Applied	...	WINWORD.EXE	Adminis...	...



**Note:** Depending on the configuration of your grid and selected columns, not all event details may be visible. To configure display preferences, and see other options for the grid display, see [Change and Set the Console Display and Preferences at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/console-display.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/console-display.htm).



**Note:** Exclusions can also be created from the **Exclusions** page. For more information, please see "[Exclude Endpoint Privilege Management Events](#)" on page 6.



## Manage Endpoint Privilege Management Policies

Using BeyondInsight you can deploy Endpoint Privilege Management policies to assets and policy users. From the **Endpoint Privilege Management Policies** page, you can view a list of available Endpoint Privilege Management policies, and in single-tenant environments only, you can manage the global priority for the policies. You can also delete policies if you have sufficient permissions.



**Note:** Endpoint Privilege Management features are only available when an Endpoint Privilege Management license is detected.

If the Endpoint Privilege Management Web Policy Editor (WPE) is installed in your BeyondInsight instance, and your account has sufficient permissions, you can view the details for each policy, unlock policies, edit policies (which also locks the policy), and delete policies.



**Note:** WPE is not installed out of the box in BeyondInsight. For information on installing and configuring WPE in your BeyondInsight instance, see [Install Web Policy Editor in BeyondInsight Instance at https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/install-wpe.htm](https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/install-wpe.htm).

## View Endpoint Privilege Management Policies

1. From the left menu in BeyondInsight, select **Policies** under **Endpoint Privilege Management**.
2. To filter the list of displayed policies, select the desired criteria from the **Filter by** list above the grid. Available filter options are:
  - Policy Name
  - Locked
  - Locked By
  - Policy Version
  - Policy Workgroup
  - Powered by



**Note:** If you select **Filter by > Locked**, you can then select **Locked** or **Unlocked** as the filter criteria. If a policy is locked, this indicates that a user currently has it locked by a policy editor. The ability to lock, unlock, and edit policies within BeyondInsight is planned for a future release. If the WPE is installed in your BeyondInsight instance, and you have sufficient permissions, you can unlock a policy that is locked by another user, and then lock the policy so you can edit it.



**Tip:** You can see who added, modified, or deleted an Endpoint Privilege Management policy from the **Configuration > General > User Audits** page in BeyondInsight. Click the **i** button for a specific activity to view its details.

USER AUDITS					
Created	Action	Section	Username	@Address	
Dec 13, 2022, 9:29 PM	Add	EPM Policy	admin	admin	<b>i</b>
Dec 06, 2022, 12:12 PM	Edit	EPM Policy	admin	admin@corp.com	<b>i</b>
Dec 06, 2022, 12:12 PM	Add	EPM Policy	admin	admin@corp.com	<b>i</b>
Dec 05, 2022, 12:38 PM	Delete	EPM Policy	admin	admin@corp.com	<b>i</b>



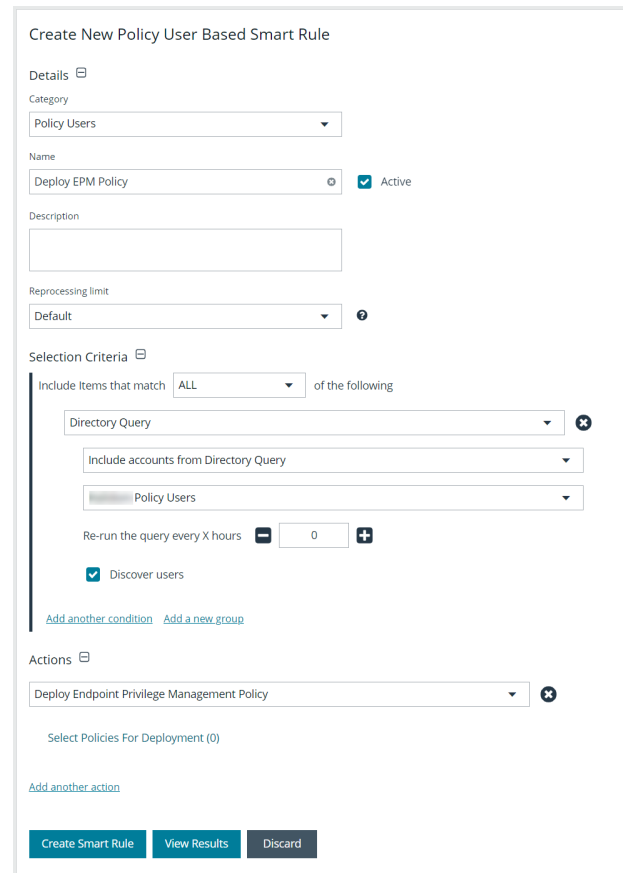
For more information on using the Endpoint Privilege Management Web Policy Editor, see:




- ["Overview of the Web Policy Editor" on page 11](#)
- ["Create, View, and Edit Endpoint Privilege Management Policies" on page 16](#)

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

1. From the **Smart Rules** page in BeyondInsight, select **Asset** or **Policy User** from the **Smart Rule type Filter** dropdown, and then click **Create Smart Rule**.
2. Select your desired **Selection Criteria**.
3. Under **Actions**, select **Deploy Endpoint Privilege Management Policy** from the dropdown.
4. Click **Select Policies for Deployment**.



Create New Policy User Based Smart Rule


Details 

Category  
Policy Users

Name  
Deploy EPM Policy  Active

Description

Reprocessing limit  
Default

Selection Criteria 


Include Items that match ALL of the following

Directory Query  
Include accounts from Directory Query  
Policy Users

Re-run the query every X hours 0

Discover users

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

Actions 

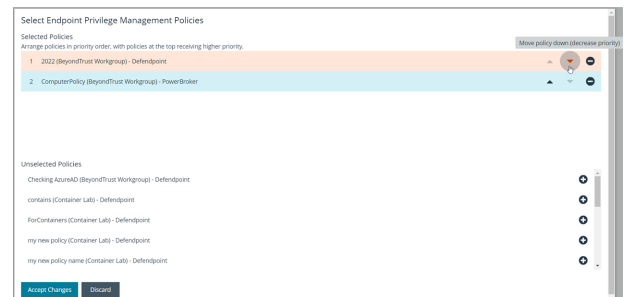
Deploy Endpoint Privilege Management Policy

Select Policies For Deployment (0)

[Add another action](#)

Create Smart Rule View Results Discard

5. Select the policies using the **Add Policy** button (plus sign) next to the policy and set their priorities using the arrows. Click **Accept Changes**.



Select Endpoint Privilege Management Policies

Selected Policies  
Arrange policies in priority order, with policies at the top receiving higher priority.

1 2022 (BeyondTrust Workgroup) - Defendpoint  
2 ComputerPolicy (BeyondTrust Workgroup) - PowerBroker

Unselected Policies  
Checking AdminAD (BeyondTrust Workgroup) - Defendpoint  
containers (Container Lab) - Defendpoint  
ForContainers (Container Lab) - Defendpoint  
my new policy (Container Lab) - Defendpoint  
my new policy name (Container Lab) - Defendpoint

Accept Changes Discard

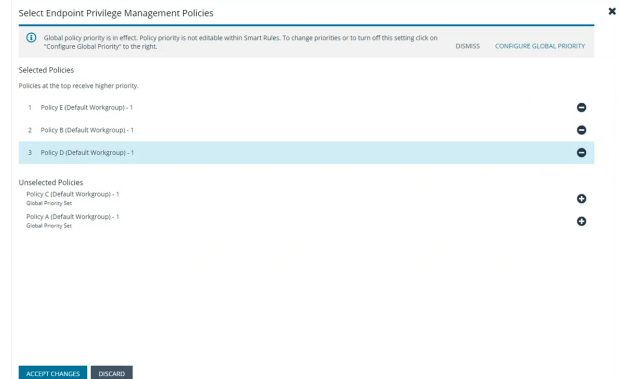


**Note:** The ability to set policy priorities within a Smart Rule is available only when **Use Global Priority** is not enabled, as indicated in the banner at the top of the page. Click **Dismiss** in the banner to continue setting priorities within the Smart Rule or click **Configure Global Priority**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





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



**Note:** We recommend setting policy priority using the global policy priority feature over setting policy priority within a Smart Rule. For more information on managing global priority for policies, please see, "[Manage Global Priority for Endpoint Privilege Management Policies](#)" on page 9.



For more information on working with Smart Rules to organize assets, see [Use Smart Rules to Organize Assets](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/smart-rules/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/smart-rules/index.htm>.

## Manage Global Priority for Endpoint Privilege Management Policies

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



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




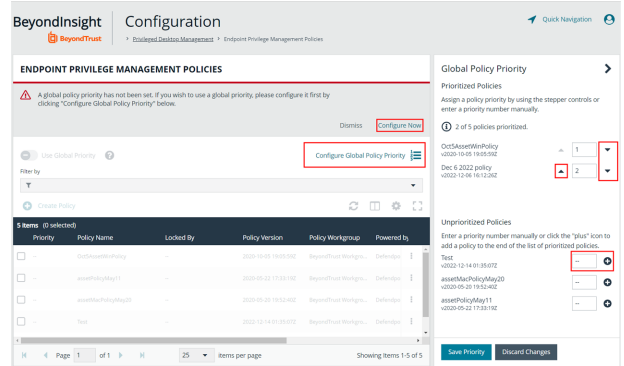
**Note:** The global policy priority feature is supported only in single-tenant BeyondInsight installations. This feature is disabled in multi-organization environments.

Enable global policy priority as follows.

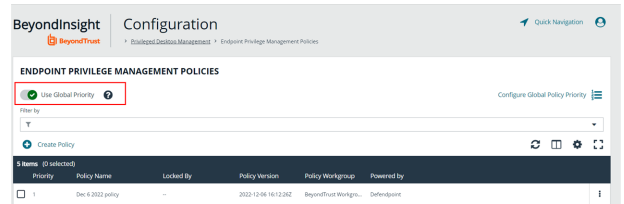
1. From the left menu in BeyondInsight, select **Policies** under **Endpoint Privilege Management**.

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

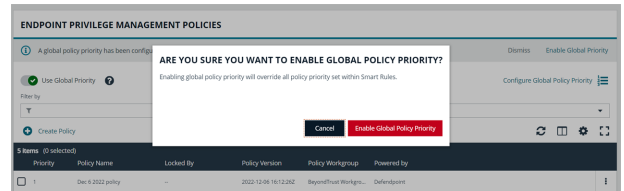
 **Note:** All policies must be prioritized in order to enable the **Use Global Priority** option. Also, any policies added to BeyondInsight after global policy priority is enabled, are not available for assignment within Smart Rules until a priority has been explicitly set for them here.



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



6. A confirmation message displays. Click **Enable Global Policy Priority** in the message box.



7. Global policy is enabled, Smart Rule prioritization is disabled, and the policies display in the grid with their assigned priority.

## Overview of the Web Policy Editor

The Endpoint Privilege Management Web Policy Editor (WPE) allows you to view, unlock, edit, and lock existing Endpoint Privilege Management policies, as well as create new policies directly from the BeyondInsight console, eliminating the need to use a standalone policy editor. Users with read-only permissions for the **Endpoint Privilege Management** feature can view policy information, while those with read/write permissions can create, view, unlock, edit, lock, and delete policies.



**Note:** Only policies powered by Defendpoint can be viewed, unlocked, edited, and locked. Policies powered by PowerBroker can only be deleted.

## Policy Editor Components

### Workstyles

Workstyles are used to assign Application Rules for a specific user, or group of users.



**Note:** The WPE in BeyondInsight supports integration with Microsoft Entra ID. Filters can be used within Workstyles to query Entra ID groups and users. Only one Entra ID tenant per organization is supported. For this integration to work, you must create an Entra ID directory credential in BeyondInsight.

### Application Groups

Application Groups are used by Workstyles to group applications together to apply certain Endpoint Privilege Management behavior.

### Content Groups

Content groups are used by Workstyles to group content together to apply certain Endpoint Privilege Management behavior.

### Messages

Messages are used by Workstyles to provide information to the end user when Endpoint Privilege Management has applied certain behavior that you've defined and need to notify the end user.

### Utilities

The WPE provides some useful tools to help with managing policies, including an import policy tool and a license management tool.



For more information on creating an Entra ID directory credential in BeyondInsight, see [Create and Edit Directory Credentials](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/role-based-access/directory-credentials.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/role-based-access/directory-credentials.htm>.

## Use the QuickStart for Windows or Mac Template

To get started quickly using the WPE, create a new policy using either the **QuickStart For Windows** template, or the **Quickstart For Mac** template.

The QuickStart templates for Windows and Mac policies contain Workstyles, Application Groups, Messages, and Custom Tokens configured with Endpoint Privilege Management and Application Control. The QuickStart policy is designed from BeyondTrust's experiences of implementing the solution across thousands of customers, and is intended to balance security with user freedom. As every environment is different, we recommend you thoroughly test this configuration to ensure it complies with the requirements of your organization.

## Customize the QuickStart Policy

Before deploying the QuickStart policy to your users, you must make some company-specific customizations to the standard template.

At a minimum you must:

- Configure the users or groups that can authorize requests that trigger messages.
- Assign users and groups to the high, medium, and low flexibility Workstyles.
- Populate the **Block - Blocked Apps** Application Group with any applications that you want to block for all users.
- Set your shared key so you can generate a Endpoint Privilege Management Response code.

## QuickStart Template Summary

This section provides information about the properties for the Windows and Mac QuickStart templates, including the Workstyles and Application Groups that comprise the template.

## WorkStyles

### All Users

This Workstyle contains a set of default rules that apply to all standard users regardless of the level of flexibility they need.

The **All Users** Workstyle contains rules to:

- Block any applications in the **Block - Blocked Apps** group.
- Allow Endpoint Privilege Management Support tools.
- Allow standard Windows and Mac functions, business applications, and applications installed through trusted deployment tools to run with admin rights.
- Allow approved standard user applications to run passively.

### High Flexibility

This Workstyle is designed for users that require a lot of flexibility, such as developers.

The **High Flexibility** Workstyle contains rules to:

- Allow applications that are in the **Add Admin – High Flexibility** group to run with admin rights.
- Allow known business applications and operating system functions to run.
- Allow users to run signed applications with admin rights.
- Allow users to run unknown applications with admin rights once they confirm that the application should be elevated.
- Allow unknown business application and operating system functions to run on demand.

## Medium Flexibility

This Workstyle is designed for users that require some flexibility, such as sales engineers.

- Allow applications that are in the **Add Admin – Medium Flexibility** group to run with admin rights.
- Allow known business applications and operating system functions to run.
- Allow users to run signed applications with admin rights once they confirm that the application should be elevated.
- Prompt users to provide a reason before they can run unknown applications with admin rights.
- Allow unknown business application and operating system functions to run on demand.
- Restricted OS functions that require admin rights are prevented and require support interaction.

## Low Flexibility

This Workstyle is designed for users that don't require much flexibility, such as helpdesk operators.

- Allow applications that are in the **Add Admin – Low Flexibility** group to run with admin rights.
- Prompt users to contact support if a trusted or untrusted application requests admin rights.
- Prompt users to contact support if an unknown application tries to run.
- Allow known approved business applications and operating system functions to run (Windows only).

## Administrators

This Workstyle provides visibility on the Administrator accounts in use in the environment.

The Administrators Workstyle contains general rules to:

- Capture user and host information.
- Block users from modifying local privileged group memberships.

## Application Groups

The Application Groups that are prefixed with **(Default)** or **(Recommended)** are hidden by default and do not need to be altered. Click the **Show Hidden** button above the grid to see all Application Groups.

- **Add Admin – All Users (Business Apps):** Contains applications that are approved for elevation for all users, regardless of their flexibility level.
- **Add Admin – All Users (Windows Functions):** Contains operating system functions that are approved for elevation for all users.
- **Add Admin – High Flexibility:** Contains the applications that require admin rights that should only be provided to the high flexibility users.

- **Add Admin – Low Flexibility:** Contains the applications that require admin rights that should only be provided to the low flexibility users.
- **Add Admin – Medium Flexibility:** Contains the applications that require admin rights that should only be provided to the medium flexibility users.
- **Block - Blocked Apps:** This group contains applications that are blocked for all users.
- **Passive - Allowed Functions & Apps:** Contains trusted applications, tasks and scripts that should execute as a standard user.
- **Passive - High Business Apps:** Contains trusted applications, that should execute as a high flexibility administrative user.
- **Passive - Low Business Apps:** Contains trusted applications, that should execute as a low flexibility administrative user.
- **Passive - Medium Business Apps:** Contains trusted applications, that should execute as medium flexibility administrative user.
- **(Default) Any Application:** Contains all application types and is used as a catch-all for unknown applications.
- **(Default) Any Trusted & Signed UAC Prompt:** Contains signed (trusted ownership) application types that request admin rights.
- **(Default) Any UAC Prompt:** Contains application types that request admin rights.
- **(Default) Privilege Management Tools:** This group is used to provide access to a BeyondTrust executable that collects Endpoint Privilege Management for Windows troubleshooting information.
- **(Default) Child Processes of TraceConfig.exe:** Contains application types that request to run child processes of TraceConfig.exe.
- **(Default) Signed UAC Prompt:** Contains signed (trusted ownership) application types that request admin rights.
- **(Default) Software Deployment Tool Installs:** Contains applications that can be installed by deployment tools such as System Center Configuration Manager (SCCM).
- **(Recommended) Restricted Functions:** This group contains OS applications and consoles that are used for system administration and trigger UAC when they are executed.
- **(Recommended) Restricted Functions (On Demand):** This group contains OS applications and consoles that are used for system administration.
- **(Default) Trusted Parent Processes:** Contains trusted applications that request to run parent processes.

## Messages

The following messages are created as part of the QuickStart policy and are used by some of the Application Rules:

- **Allow Message (Authentication):** Asks the user to provide a reason and enter their password before the application runs with admin rights.
- **Allow Message (Select Reason):** Asks the user to select a reason from a dropdown menu before the application runs with admin rights.
- **Allow Message (Support Desk):** Presents the user with a challenge code and asks them to obtain authorization from the support desk. Support can either provide a response code or a designated, authorized user can enter their login details to approve the request.
- **Allow Message (Yes / No):** Asks the user to confirm that they want to proceed to run an application with admin rights.
- **Block Message:** Warns the user that an application has been blocked.
- **Block Notification:** Notifies the user that an application has been blocked and submitted for analysis.
- **Notification (Trusted):** Notifies the user that an application has been trusted.

## Use the Server Role Template

The Server Roles policy contains Workstyles, Application Groups, and Content Groups to manage different server roles such as DHCP, DNS, IIS, and print servers.

## Server Roles Template Summary

This template policy contains the following elements.

### WorkStyles

- Server Role - Active Directory - Template
- Server Role - DHCP - Template
- Server Role - DNS - Template
- Server Role - File Services - Template
- Server Role - Hyper V - Template
- Server Role - IIS - Template
- Server Role - Print Services - Template
- Server Role - Windows General - Template

### Application Groups

- Server Role - Active Directory - Server 2008R2
- Server Role - DHCP - Server 2008R2
- Server Role - DNS - Server 2008R2
- Server Role - File Services - Server 2008R2
- Server Role - General Tasks - Server 2008R2
- Server Role - Hyper V - Server 2008R2
- Server Role - IIS - Server 2008R2
- Server Role - Print Services - Server 2008R2

### Content Groups


- AD Management
- Host Management
- IIS Management
- Printer Management
- Public Desktop

# Create, View, and Edit Endpoint Privilege Management Policies

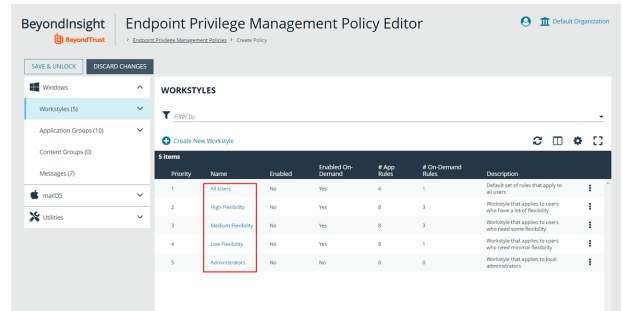
## Create a Policy

1. From the left menu, select **Policies** under **Endpoint Privilege Management**.
2. Click **Create Policy +** above the grid.
3. Enter a name for the policy and select a Workgroup from the list.
4. Click **Create Policy**.
5. Select one of the following:
  - **QuickStart for Windows:** A preconfigured template with Workstyles, Application Groups, messages, and Custom Tokens already configured.
  - **QuickStart for Mac:** A preconfigured template with Workstyles, Application Groups, and messages already configured.
  - **Server Roles:** The Server Roles policy contains Workstyles, Application Groups, and Content Groups to manage different server roles such as DHCP, DNS, IIS, and print servers.
  - **Blank:** Select to configure a policy from scratch. There are no preconfigured settings in this template.

The Policy Editor opens to the **Workstyles** page. At this point you must configure the Workstyle, Application Groups, Application Rules and other policy configuration as required for your organization. The templates and their configuration components are described in more detail in the below sections.

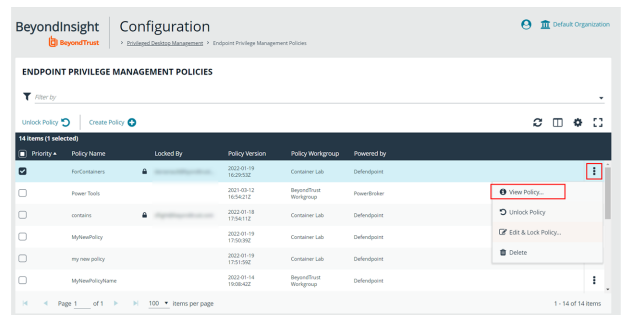


**Tip:** For quick access to the **Workstyles Summary** page, click the hyperlink for the Workstyle name.




## View a Policy

1. From the left menu, select **Policies** under **Endpoint Privilege Management**.
2. Click the vertical ellipsis for the policy you wish to view, and then select **View Policy**.






3. The Policy Editor opens in **Read Only** mode.



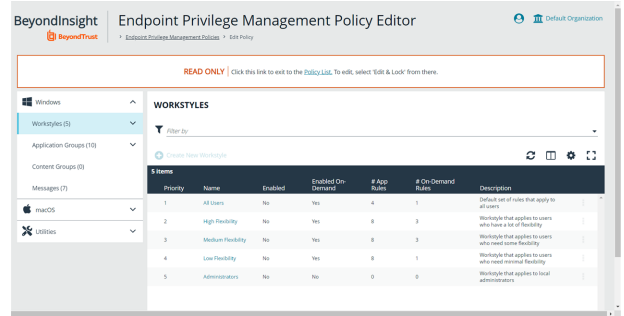
**Tip:** If you wish to edit the policy, click the **Policy List** link at the top of the page to go back to the main Policies page where you can select the policy to edit and lock it.

4. Use the options in the left navigation to view the following policy information:

- For Windows policies:
  - Workstyles
  - Application Groups
  - Content Groups
  - Messages
- For macOS policies:
  - Workstyles
  - Application Groups
  - Messages
- Utilities:
  - Licenses
  - Import Policy
  - Template Policies



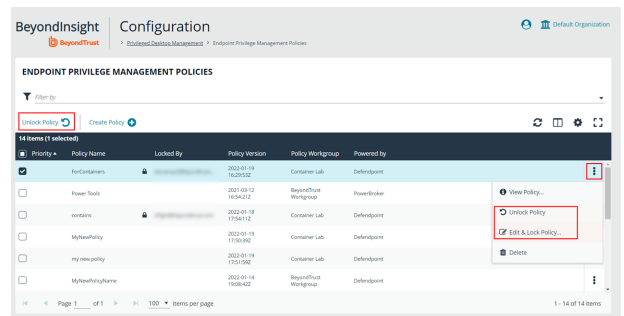
**Note:** You can also filter the contents displayed in each grid using the **Filter By** list above the grid.



## Edit a Policy

When you edit a policy, the policy is locked. Other policy administrators cannot access the policy to change the properties when the status is **Locked**. The policy is unlocked when changes are saved or discarded.

1. From the left menu, select **Policies** under **Endpoint Privilege Management**.
2. Click the vertical ellipsis for the policy you wish to edit.
3. If a policy is locked, the **Unlock Policy** action displays in the menu. Click to unlock the policy.
4. Select **Edit and Lock Policy**.



5. In the Policy Editor, go to the policy property you want to change and make your edits.
6. Click **Save** to save a draft of the policy. Clicking **Save** allows you to keep the Policy Editor open to continue changing the policy.
7. Once the policy is updated, click **Save and Unlock** to save a new revision of the policy, or **Discard Changes** to remove changes.
8. If **Discard Changes** is selected, you are prompted to **Continue Editing** or **Discard Changes**.
9. (Optional). On the **Save and Unlock** dialog box, you can enter **Annotation notes** about the policy changes. You can also check the **Auto Assign Policy to Groups?** box, to automatically assign the latest revision to groups the policy is currently assigned to.



**Note:** The **Auto Assign Policy to Groups?** option is only available when the groups are currently on the latest policy. If they are on an older version, only the **Annotation notes** option is displayed.



**Tip:** You can export a policy and import a policy to overwrite the existing one while viewing a policy in read-only mode and while editing a policy in read/write mode. Select **Utilities > Import Policy** from the left navigation, click **Overwrite Policy**, and then click **Export Existing Policy** to export. Drop a file in the box to upload a new policy and then click **Upload File**.



For more information on editing the various components of a policy, including Workstyles, Application Rules, and Application Groups, please see "Use the Policy Editor to Manage Policy" in the *Privileged Management Cloud Administration Guide* at <https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pmc/pm-cloud-admin.pdf>.

## Create and View Smart Rules for Endpoint Privilege Management Policy Users

You can manage user-based policies for Endpoint Privilege Management users with Smart Rules, and view the policy users with the assigned policies.



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

To deploy policies to users, you must first create rules and policies in the Endpoint Privilege Management **Policy Editor**, and then create applicable Smart Rules to deploy the policies to policy users.

### Create a Policy User Smart Rule

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

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

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Policy User** from the **Smart Rule type filter** dropdown.
3. Click **Create Smart Rule**. A new window opens.

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

### Create New Policy User Based Smart Rule

Details ⊟

Category

Name  
  Active

Description

Reprocessing limit  
 ⓘ

Selection Criteria ⊟

Include Items that match  of the following

✕

Discover users

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

Actions ⊟

✕

Remove existing non-matching Policy Users

✕

SELECT POLICIES FOR DEPLOYMENT (0)

✕

✕

[Add another action](#)

## View Policy Users

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

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



**Note:** Depending on the configuration of your grid and selected columns, not all policy user details may be visible. To configure display preferences, and see other options for the grid display, see [Change and Set the Console Display and Preferences](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/console-display.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/console-display.htm>.

5. To remove a user from a policy, click the vertical ellipsis for the user, and select **Delete Policy User**.

## View Endpoint Privilege Management Agents

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



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

To view the Endpoint Privilege Management Agents

1. From the left navigation in BeyondInsight, click **MENU**.
2. Under **Endpoint Privilege Management**, click **Agents**.



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

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



**Note:** Depending on the configuration of your grid and selected columns, not all agent details may be visible. To configure display preferences, and see other options for the grid display, see [Change and Set the Console Display and Preferences at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/console-display.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/console-display.htm).

## View Endpoint Privilege Management File Integrity Monitoring

You can view file integrity monitoring events using Endpoint Privilege Management. File integrity monitoring captures events related to created, edited, or deleted items in folders, according to the created rules.



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

To view file integrity monitoring events:

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



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



**Note:** Depending on the configuration of your grid and selected columns, not all file monitoring event details may be visible. To configure display preferences, and see other options for the grid display, see [Change and Set the Console Display and Preferences](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/console-display.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/console-display.htm>.

## Monitor Endpoint Privilege Management Sessions

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



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

### View Session Details

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



**Note:** Depending on the configuration of your grid and selected columns, not all session details may be visible. To configure display preferences, and see other options for the grid display, see [Change and Set the Console Display and Preferences at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/console-display.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/console-display.htm).

### Session Replay

1. Follow the steps above to select a session.
2. Click the vertical ellipsis for the session, and then select **View Session...** . **View Session...** is also available when viewing all session details.
3. A new page opens, showing some details of the session, a list of the **Events** and when they occurred (which can be searched), and a slideshow of the session.
4. Buttons under the slideshow control session playback. You can change the speed of session playback by selecting a different **Slideshow Delay**.
5. You can download an image of any session view by clicking the **Snapshot** button.



## View Endpoint Privilege Management Reports

Endpoint Privilege Management Reporting includes a rich set of dashboards and reports designed to simplify the centralized management and auditing of Endpoint Privilege Management activity throughout the desktop and server estate.

A report is a dashboard or a table, and is a generic term used to describe any form of data displayed in Endpoint Privilege Management Reporting. You can click on links within reports to see the data at greater levels of granularity. These are referred to as *drilldowns*.

A dashboard is a report, which at the top level, presents you with a series of charts and summarized data. Some dashboards have sub-reports that are presented as charts or tabular data. All dashboards have a Microsoft Windows view to display events from Windows endpoints. Some dashboards and reports also have a macOS view.

The below sections describe each of the dashboards, and the reports and event data accessible from each view.



**Note:** *Endpoint Privilege Management Reporting is not installed out of the box in BeyondInsight. For BeyondInsight releases prior to 23.1, please contact your BeyondTrust representative for assistance with installing the Endpoint Privilege Management Reporting feature in your BeyondInsight environment.*



For information on installing and configuring Endpoint Privilege Management Reporting in BeyondInsight 23.1 and later releases, please see the following:

- [Install Endpoint Privilege Management Reporting in BeyondInsight at https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/install-pmr-bi.htm](https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/install-pmr-bi.htm)
- [Upgrade Endpoint Privilege Management Reporting in BeyondInsight at https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/upgrade-pmr-bi.htm](https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/upgrade-pmr-bi.htm)
- [Configure Endpoint Privilege Management Reporting in BeyondInsight at https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/configure-pmr-bi.htm](https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/configure-pmr-bi.htm)
- [Configure Advanced SQL and Event Collector Settings for PMR in BI Integration at https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/configure-advanced-settings.htm](https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/configure-advanced-settings.htm)

## Navigate the Endpoint Privilege Management Reporting Interface

The Endpoint Privilege Management Reporting interface allows you to switch between dashboards and reports and to filter data as required. This section covers the Endpoint Privilege Management Reporting interface elements and how to export a specific report.

### Navigation Panel

The side navigation panel takes you to each top-level dashboard and the reports in that dashboard. Reports that are post-fixed with **All** indicate the data is in tabular form.

### Dashboard and Reports Panel

This is the area where dashboards and reports are displayed. A dashboard is a report with multiple charts covering a wide range of data. A report is a summary table or a page focused on a particular entity.

The graphical elements of a dashboard or report are interactive. You can click on a chart to view the data at an additional level of granularity.

### Filter Panel

Each dashboard and report has a panel above its table, chart, or graph area that displays the applied filters and a **Filters** dropdown. When you select the **Filters** dropdown, a **Filters** box appears where you can select filters to filter data based on various event properties. The **Filters** box also provides a link to select **Advanced Filters**, allowing for more granular report data. The filters displayed in the box are unique and relevant to the specific dashboard and report.

For example, if you want to filter the **Summary** report to include only a specific Workstyle:

1. From the **Summary** dashboard, click the link to open the report to filter.
2. Click the **Filters** dropdown.
3. Click the **Advanced Filters** link.
4. Select the **Workstyle** you are interested in from the dropdown.
5. Click **Apply Filters**.
6. The report data for that specific Workstyle displays in the table.

The filter options match text on substrings; partial or complete words can match on a filter.

Certain filter options support comma-separated values so you can specify a list of filter values. For example, to restrict the results to three users, enter `user1,user2,user3` in the **User Name** field.



**Note:** Multiple "!" strings are accepted. For example, "!L-CZC13127L30I,!L-CNU410DJJ7"

Any text field supports wildcards, comma-separated values (CSV), and the Does Not Match(!) options:

Filtering Effect	Filter Panel Operator	Effect
List separator	Comma (,)	Value1,value2,value3
Wildcard	%	part% part%part2,part3%part4

Filtering Effect	Filter Panel Operator	Effect
Negation or "Not"	!	!value !value1,!value2



**Note:** When filtering tabular reports such as the **Users > All** table, an applied filter is displayed at the top of the table. To remove a filter, click on the **x** next to the filter text.

## Export Reports

You can export reports to a CSV file by clicking the **Export to CSV** button in the filter panel above the report.

Exported data is based on the data currently displayed in the report.

## Use Quick Filters and Advanced Filters

### Use Quick Filters

Below are descriptions of commonly used quick filter options available from the **Filters** dropdown.

Name	Description
Platform	<ul style="list-style-type: none"> <li>• <b>Windows</b> Filters by endpoints running a Windows operating system.</li> <li>• <b>OS X</b> Filters by endpoints running a Mac operating system.</li> </ul>
Time Range	<p>This is the time range in which the actions are audited. For example, you can filter by the number of elevated actions in the last 24 hours in the <b>Actions &gt; Elevated</b> report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• <b>24 Hours</b></li> <li>• <b>7 Days</b></li> <li>• <b>30 Days</b></li> <li>• <b>12 Months</b></li> </ul>
Time First Reported	<p>This is the time range filtered by the date the application was first entered in the database. For example, you can filter on the new Windows applications by publisher that were first reported in the last 7 days in the <b>Discovery &gt; By Publisher</b> report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• <b>24 Hours</b></li> <li>• <b>7 Days</b></li> <li>• <b>30 Days</b></li> <li>• <b>6 Months</b></li> <li>• <b>12 Months</b></li> </ul>
Time First Executed	<p>This is the time range the application was first executed. For example, you can filter on the new Windows applications, by type, that were first executed in the last 30 days in the <b>Discovery &gt; By Type</b> report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• <b>24 Hours</b></li> <li>• <b>7 Days</b></li> <li>• <b>30 Days</b></li> <li>• <b>6 Months</b></li> <li>• <b>12 Months</b></li> </ul>

Name	Description
Target Type	<p>This filter allows you to filter by a type of target. For example, you can filter on the applications canceled in the time range in the <b>Actions &gt; Canceled</b> report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Applications</li> <li>• Services</li> <li>• COM</li> <li>• Remote PowerShell</li> <li>• ActiveX</li> <li>• URL</li> <li>• Content</li> </ul>
Action	<p>This filter allows you to filter by a type of action. For example, you can filter on the services elevated in the time range in the <b>Target Types &gt; Services</b> report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Elevated</li> <li>• Blocked</li> <li>• Passive</li> <li>• Sandboxed</li> <li>• Custom</li> <li>• Drop admin rights</li> <li>• Enforce default rights</li> <li>• Canceled</li> </ul>

Name	Description
Application Type	<p>This filter allows you to filter by application type. For example, you can filter by applications that are executables used in the time range in <b>Target Types &gt; Applications</b>.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Executable</li> <li>• Control panel applet</li> <li>• Management console snapin</li> <li>• Installer Package</li> <li>• Uninstaller</li> <li>• Windows Script</li> <li>• PowerShell Script</li> <li>• Batch File</li> <li>• Registry Settings</li> <li>• Windows store application</li> <li>• Bundle</li> <li>• Package</li> <li>• System Preference</li> <li>• Sudo Control</li> <li>• Script</li> </ul>
Event Category	<p>This filter allows you to filter by the category of the event. For example, you can filter by process events only that occur in the time range in the <b>Events &gt; All</b> report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Process Control</li> <li>• Content Control</li> <li>• DLL Control</li> <li>• URL</li> <li>• Privileged Account Management</li> <li>• Agent started</li> <li>• User logon</li> <li>• Services</li> </ul>

Name	Description
Elevate Method	<p>Allows you to filter by the elevation method used. For example, in the <b>Discovery &gt; Requiring Elevation</b> report, you can filter by new applications which were accessed using on-demand elevation within the time range.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Admin account used</b></li> <li>• <b>Auto-elevated</b></li> <li>• <b>On-demand</b></li> </ul>
Path	<p>Allows you to filter by the path. For example, to filter on applications that were launched from the System path.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>System</b></li> <li>• <b>Program Files</b></li> <li>• <b>User Profiles</b></li> </ul>
Source	<p>The media source of the application. For example, was the application downloaded from the internet or is it from removable media?</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Downloaded from internet</b></li> <li>• <b>Removable media</b></li> <li>• <b>Any external source</b></li> </ul>
Challenge / Response	<p>Allows you to filter by challenge/response events. For example, you can filter the application that required elevation on those applications launched following a completed challenge/response message.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Only C/R</b></li> </ul>
Admin Rights	<p>Allows you to filter by the admin rights token.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Detected</b></li> <li>• <b>Not Detected</b></li> </ul>

Name	Description
Authorization	Allows you to filter by authorization. You can choose from: <ul style="list-style-type: none"> <li>• All</li> <li>• Required</li> <li>• Not Required</li> </ul>
Ownership	Allows you to group by the type of owner. You can choose from: <ul style="list-style-type: none"> <li>• All</li> <li>• Trusted owner</li> <li>• Untrusted owner</li> </ul>
Rule Match Type	Allows you to filter on the type of matching. You can choose from: <ul style="list-style-type: none"> <li>• All</li> <li>• Matched on Parent</li> <li>• Direct Match</li> </ul>

## Use Advanced Filters

Below are descriptions of commonly used filter options available from the **Advanced Filters** link in the **Filters** box.

Name	Description
Action	There are nine actions to choose from: <ul style="list-style-type: none"> <li>• Elevated</li> <li>• Blocked</li> <li>• Passive</li> <li>• Custom</li> <li>• Drop Admin Rights</li> <li>• Enforce Default Rights</li> <li>• Canceled</li> <li>• Sandboxed</li> <li>• Allowed</li> </ul>
Activity ID	Each Activity Type in Endpoint Privilege Management has a unique ID. This is generated in the database as required.  For example, if you are in the <b>Target Types</b> dashboard and drill down in the <b>Top 10 Activities</b> chart, the <b>Events &gt; All</b> report opens. If you look in the top advanced filter you will see that the Activity ID is populated.



Name	Description
Admin Rights Required	There are three options to choose from: <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Detected</b></li> <li>• <b>Not Detected</b></li> </ul> Allows you to filter if Admin Rights are required, not required, or both. For example, if you are in the <b>Discovery &gt; All</b> report and set the side quick filter to <b>Admin Rights</b> , only applications that required admin rights are listed.
Agent Version	The version of the Endpoint Privilege Management agent.
Application Desc	A text field that allows you to filter on the application name.  For example, in the <b>Discovery</b> report you can filter by <b>paint</b> in the <b>Application Desc</b> field. This filters applications that contain the string <b>paint</b> in the description.
Application Group	A text field that allows you to filter by Application Group. You can obtain the Application Group from the Policy Editor. It is also available in some reports such as <b>Process Detail</b> , which is accessed from <b>Events All</b> .
Application Type	A text field that allows you to filter by application type. You can obtain the application type from the Policy Editor. It's also available in some reports such as <b>Process Detail</b> , which is accessed from <b>Events All</b> .
Auth Methods	The type of authentication method selected in the Policy Editor. Multiple values can be present and are comma separated. Possible values: <b>Identity Provider</b> , <b>Password</b> , <b>Challenge Response</b> , <b>Smart Card</b> , and <b>User Request</b> .
Auth User Name	The name of the user that authorized the message.
Browse Source URL	The source URL of the sandbox.
Browse Destination URL	The destination URL of the sandbox.
Chassis	The physical form of the endpoint. <b>Other</b> is a virtual machine.
Command Line	A text field that allows you to filter on the command line. It is also available in some reports such as <b>Process Detail</b> that is accessed from <b>Events &gt; All</b> .
Context	This field is used by Reporting. You do not need to edit it.
Date Field to filter on	There are three options to choose from: <ul style="list-style-type: none"> <li>• <b>Time Generated</b>: This is the time that the event was generated. One application can have multiple events. Each event has a <b>Time Generated</b> attribute.</li> <li>• <b>Time App First Discovered</b>: This is the time that the first event for a single application was entered into the database. This can be delayed if the user is working offline.</li> <li>• <b>Time App First Executed</b>: This is the first known execution time of events for that application.</li> </ul>
Default UI Language	The default language of the endpoint.

Name	Description
Device Type	The type of device that the application file was stored on. You can select from: <ul style="list-style-type: none"> <li>• Any</li> <li>• Removeable Media</li> <li>• USB Drive</li> <li>• Fixed Drive</li> <li>• Network Drive</li> <li>• CDROM Drive</li> <li>• RAM Drive</li> <li>• eSATA Drive</li> <li>• Any Removable Drive or Media</li> </ul>
Distinct Application ID	This field is used by Reporting. You do not need to edit it.
Elevation Method	There are five options to choose from: <ul style="list-style-type: none"> <li>• Not Set</li> <li>• All</li> <li>• Admin account</li> <li>• Auto-elevated</li> <li>• On-demand</li> </ul> These allow you to filter events by the type of elevation used.
Event Number	This field is used by Reporting. You do not need to edit it. This number assigned to the event type.
External Source	There are four options to choose from: <ul style="list-style-type: none"> <li>• Not Set</li> <li>• Downloaded over the internet</li> <li>• Removeable media</li> <li>• Any external source</li> </ul> These allow you to filter by the type of external source that the application file came from.
File Name	You can filter by a partial file name string if required. For example, in the <b>Process Detail</b> report.
File Version	You can filter on the file version in the Advanced View of the <b>Process Detail</b> report.
GPO Name	You can filter on the Group Policy Object (GPO) name in some of the advanced reports such as <b>Process Detail</b> .
Host Name	This field allows you to filter by the name of the endpoint the event came from.
Idp Authentication user name	The credential provided when adding an Identity Provider authorization message in the Policy Editor.
BeyondTrust Zone Identifier	The BeyondTrust Zone Identifier. This tag persists, to allow you to filter on it even if the ADS tag applied by the browser is removed.
Ignore "Admin Required" Events	This field is used by Reporting. You do not need to edit it.

Name	Description
Just Discovery Events	This field is used by Reporting. You do not need to edit it.
Message Name	The name of the message that was used.
Message Type	The type of Message: <ul style="list-style-type: none"> <li>• <b>Any</b></li> <li>• <b>Prompt</b></li> <li>• <b>Notification</b></li> <li>• <b>None</b></li> </ul>
Number to Get	The number of rows to get from the database.
Operating System Type	The type of operating system: <ul style="list-style-type: none"> <li>• <b>Server</b></li> <li>• <b>Workstation</b></li> </ul>
Operating System	The operating system of the client machine.
Parent PID	The operating system process identifier of the parent process.
PID	The operating system process identifier.
Product Name	The product name of the application.
Product Version	The product version of the application.
Program Files Path	Sets the Program Files path used by the <b>Discovery &gt; By Path</b> report.
Publisher	The publisher of the application.
Range End Time	The end time of the range being displayed.
Range Start Time	The start time of the range being displayed.
Request Type	The type of request: <ul style="list-style-type: none"> <li>• <b>Blocked with reason</b></li> <li>• <b>Canceled challenge</b></li> </ul>
Row Limit	The maximum number of rows to be retrieved from the database.
Rule Match Type	Rule Match Type: <ul style="list-style-type: none"> <li>• <b>Any</b></li> <li>• <b>Direct match</b></li> <li>• <b>Matched on parent</b></li> </ul>
Sandbox	The sandboxed setting: <ul style="list-style-type: none"> <li>• <b>Not Set</b></li> <li>• <b>Any Sandbox</b></li> <li>• <b>Not Sandboxed</b></li> </ul>
Rule Script Affected Rule	True when the Rule Script (Power Rule) changes one or more of the Default Endpoint Privilege Management rules, otherwise false.
Rule Script File Name	The Rule Script (Power Rule) file name on disk if applicable.

Name	Description
Rule Script Name	The name of the assigned Rule Script (Power Rule).
Rule Script Output	The output of the Rule Script (Power Rule).
Rule Script Publisher	The publisher of the Rule Script (Power Rule).
Rule Script Result	<p>The result of the Rule Script (Power Rule). This can be:</p> <pre> &lt;None&gt; Script ran successfully [Exception Message] Script timeout exceeded: &lt;X&gt; seconds Script execution canceled Set Rule Properties failed validation: &lt;reason&gt; Script execution skipped: Challenge Response Authenticated Script executed previously for the parent process: Matched as a child process so cached result applied Script execution skipped: &lt;app type&gt; not supported Script execution skipped: PRInterface module failed signature check Set RunAs Properties failed validation: &lt;reason&gt;                     </pre>
Rule Script Status	<p>The status of the Rule Script (Power Rule). This can be:</p> <pre> &lt;None&gt; Success Timeout Exception Skipped ValidationFailure                     </pre>
Rule Script Version	The version of the assigned Rule Script (Power Rule).
Shell or Auto	<p>Whether the process was launched using the shell <b>Run with Endpoint Privilege Management</b> option or by normal means (opening an application):</p> <ul style="list-style-type: none"> <li>• <b>Any</b></li> <li>• <b>Shell</b></li> <li>• <b>Auto</b></li> </ul>
Source URL	The source URL (where the file was downloaded from).
System Path	Sets the system path used by the <b>Discovery &gt; By Path</b> report.
Target Description	This field allows you to filter by the target description.

Name	Description
Target Type	The type of target that triggered the event: <ul style="list-style-type: none"> <li>• Any</li> <li>• Application</li> <li>• URL</li> <li>• Services</li> <li>• COM</li> <li>• Remote PowerShell</li> <li>• ActiveX</li> <li>• Content</li> </ul>
Trusted Application Name	The trusted application that triggered the event.
Trusted Application Version	The trusted application version number.
Trusted File Owner	Whether the file owner of the target file is trusted. To be a trusted owner the user must be in one of the following Windows groups: <ul style="list-style-type: none"> <li>• TrustedInstaller</li> <li>• System</li> <li>• Administrator</li> </ul>
UAC Triggered	Whether or not Windows UAC was triggered: <ul style="list-style-type: none"> <li>• Not Set</li> <li>• Triggered UAC</li> <li>• Did not trigger UAC</li> </ul>
User Name	The user name of the user who triggered the event.
User Profiles Path	Sets the <b>User Profiles</b> path used by the <b>Discovery &gt; By Path</b> report.
Workstyle	The name of the Workstyle that contained the rule that matched the application.

## Overview of EPM Reporting Dashboards

Reporting includes several high level dashboards that summarize the Endpoint Privilege Management events. You can access the following from the side navigation panel.

Dashboard	Description
<b>Summary Dashboard</b>	Displays bar charts for the most important activity that has occurred in the selected time period. Typically this information can result in Workstyle changes or investigation of anomalies. The charts allow you to view details when you click an action, either on a chart or in the legend. The bar charts are separated by Windows and Mac <b>Events by Action</b> .
<b>Events Dashboard</b>	Summarizes information about the types of events raised in the specified time frame. It also shows the time elapsed since a host raised an event.
<b>Discovery Dashboard</b>	Summarizes all the unique applications discovered. It differentiates between those that used elevated privileges and those that ran with standard privileges. This dashboard only shows new application items in the chosen time interval. For example, the Discovery dashboard can answer the question <i>what's new this week and how is it affecting my users?</i>  The Discovery reports listed below the Discovery dashboard display the data from different angles such as by the location or publisher of the executable or the type of the executable.
<b>Actions Dashboard</b>	Summarizes audited items categorized by the type of action taken. This allows you to focus on the topic of interest. For example, elevation or blocking. The Actions reports show audits only of the selected type ( <b>Elevated, Blocked, Passive, Canceled, Other</b> ).
<b>Target Types Dashboard</b>	Lists all the Endpoint Privilege Management activity over the specified time interval by target type. The report lists the targets in tabular form sorted by user count. You can click the targets in the list to view dashboard charts showing <b>Users, Hosts, and Process</b> activities and actions over a specified period of time.
<b>User Experience Dashboard</b>	Displays how users interacted with <b>Messages, Challenge/Response</b> dialog boxes, and the <b>Shell (On-Demand)</b> menu.
<b>Privileged Logons Dashboard</b>	Displays how many accounts with Standard rights, Power User rights, and Administrator rights generated logon events filtered by the time frame.
<b>Privileged Account Management Dashboard</b>	Displays any blocked attempts to modify privileged accounts over the specified time interval.
<b>Trusted Application Protection Dashboard</b>	Summarizes all the Trusted Application Protection incidents. Incidents are defined as a child process blocked from running because it matched the rules in the Trusted Application Protection policy or a DLL blocked from loading by a Trusted Application because it did not have a trusted owner or trusted publisher.

## Summary Dashboard

The **Summary** dashboard displays bar charts for the most important activity that has occurred in the time period defined by the quick filter. The legends to the right of the charts display totals for the shown activities. You can use this information to inform Workstyle development or to show anomalous user behavior in your organization.

A warning message might display on the **Summary** page if there is a backlog of event processing. Verify your database configuration is set up to manage processing a large number of events.

The **Summary** dashboard includes the following tables:

Table	Description
Applications Discovered	The total number of newly discovered <b>Applications</b> filtered by the type of user rights required: <ul style="list-style-type: none"> <li>• Admin rights required</li> <li>• Standard rights required</li> </ul> <b>Discovered</b> applications are shown in the <b>Applications</b> table. Click the number next to the OS icon to show details.
User Requests	The total number of <b>User Requests</b> filtered by the type of request: <ul style="list-style-type: none"> <li>• Blocked (user provided reason)</li> <li>• User canceled challenge</li> </ul> Click the chart or legend to open the <b>Requests All</b> report with the <b>Request Type</b> filter applied.
Admin logons, by users, on endpoints	Summarizes the number of admin logons, the number of users, and the number of endpoints used. <b>Admin Logons</b> are shown in the <b>Administration</b> table. Click the number next to the OS icon to show details.
Trusted Application Protection	The number of Trusted Application (TAP) incidents, how many users, and how many endpoints were affected. <b>TAP</b> events are shown in the <b>Incidents</b> table. Click the number next to the OS icon to show details.
Attempts to modify privileged groups	The number of blocked attempts to modify privileged groups. <b>Attempts to modify privileged groups</b> are shown in the <b>Administration</b> table. Click the number next to the OS icon to show details.
Application run from external sources	The number of applications run from external sources. Applications <b>Run from external sources</b> are shown in the <b>Applications</b> table. Click the number next to the OS icon to show details.
Activities blocked	The number of applications blocked. Click the chart or legend to open the <b>Target Types All</b> report with the <b>Filter by Action</b> filter applied.

Table	Description
Applications used On-Demand privileges	The number of applications launched using on-demand privileges.  Click the chart or legend to open the <b>Target Types All</b> report with the <b>Shell or Auto</b> filter applied. <i>Shell</i> indicates that on-demand privileges were used.
UAC matches	The number of applications that triggered User Account Control (UAC).  <b>UAC</b> events are shown in the <b>Incidents</b> table. Click the number next to the OS icon to show details.



## Events Dashboard

This report shows information about the types of events raised over the specified time period. It also shows the time elapsed since a host raised an event.

Chart	Description
Events over the last (time interval)	A column chart showing the number of the different Event types filtered by the time period. Clicking the chart opens the <b>Events All</b> report with the <b>Filter by Event Category</b> filter applied.
Event Types	A chart showing the number of events received filtered by the Event type. Clicking the chart opens the <b>Events All</b> report with the <b>Event Number</b> filter applied.
By Category	A chart displaying the events received filtered by category. Clicking the chart opens the <b>Events All</b> report with the <b>Filter by Event Category</b> filter applied.
Time since last endpoint event	A chart showing the number of endpoints in each time since last event category.

## Events All Report

The following columns are available for the Windows and macOS **Events All** table:

- **Event Time:** The time of the event.
- **Event Category:** The category of the event.
- **Platform:** The platform where the event occurred.
- **Description:** The description of the event.
- **User Name:** The user name of the user who triggered the event.
- **Host Name:** The host name where the event was triggered.
- **Workstyle:** The Workstyle containing the rule that triggered the event.
- **Event Type:** The type of event.

Some of these columns allow you to drill down to additional information:

- **Event Time:** opens the event report listing all of the fields for that event.
- **Description:** opens the **Applications** Report.
- **User Name:** opens the **User** Report.
- **Host Name:** opens the **Host** Report.
- **Workstyle:** opens the **Workstyle** Report.

## Process Detail Report

The **Process Detail** report provides a higher level of detail for Process events than the **Events > All** table. Other event categories are not shown in this table.

The following columns are available for the Windows and macOS **Process Details** table:

- **Start Time:** The start time of the event.
- **Platform:** The platform where the event occurred.

- **Description:** The description of the application.
- **Publisher:** The publisher of the application.
- **Application Type:** The type of application.
- **File Name:** The name of the file.
- **Command Line:** The command line of the process that triggered the event.
- **Product Name:** The product name of the application.
- **Product Version:** The product version of the application.
- **Trusted Application:** The name of the trusted application.
- **Trusted Application Version:** The version of the trusted application.
- **Group Policy Object:** The name of the Endpoint Privilege Management policy (Windows only).
- **Workstyle:** The name of the Workstyle that the event was triggered from.
- **Message:** The message name if the event triggered a message.
- **Action:** The action associated with the event.
- **Application Group:** The Application Group the application assignment rule belongs to.
- **PID:** The process identifier of the process.
- **Parent PID:** The parent process identifier.
- **Parent Process File Name:** The parent process file name.
- **Shell / Auto:** Whether the process was triggered on-demand or automatically (Windows only).
- **UAC Triggered:** Whether user account control was triggered (Windows only).
- **Admin Rights Required:** Whether or not admin rights were required (Windows only).
- **Authorization Required:** Whether or not authorization rights were required (macOS only).
- **User Name:** The name of the user who triggered the event.
- **Host Name:** The name of the host where the event was triggered.
- **Rule Script File Name:** The name of the Rule Script (Power Rule).
- **Rule Script Affected Rule:** True when the Rule Script (Power Rule) changed one or more of the Default Endpoint Privilege Management rules, otherwise false.
- **User Reason:** The reason given by the user if applicable.
- **COM Display Name:** The COM name if applicable (Windows only).
- **Source URL:** The URL of the event if applicable (Windows only).
- **BeyondTrust Zone Identifier:** The BeyondTrust Zone Identifier if present.
- **Uninstall Action:** This can be **None**, **Uninstall**, **Change/Modify**, or **Repair**.
- **Auth Methods:** The type of authentication method selected in the Policy Editor. Multiple values can be present and are comma separated. Possible values: **Identity Provider**, **Password**, **Challenge Response**, **Smart Card**, and **User Request**.
- **Idp Authentication User Name:** The credential provided when adding an Identity Provider authorization message in the Policy Editor.

## Export Events to CSV File

The number of items that can be displayed at one time might be limited by the browser display. Click **Export to CSV** to enter the number of rows to export to the CSV file.

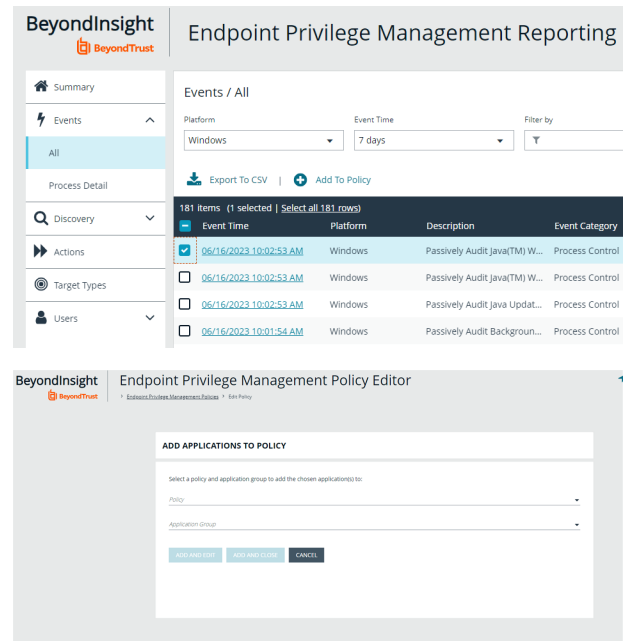
All event filters are saved to the file.

## Add Applications to a Policy

If Endpoint Privilege Management Reporting UI 23.4 or a later version is installed and configured, you can add applications to an Endpoint Privilege Management policy directly from the **Events** dashboard, using the **Add to Policy** feature.

To add an application from an event to an Endpoint Privilege Management policy:

1. Select the event or multiple events, and then click **Add to Policy** above the grid.
2. You are taken to the Endpoint Privilege Management Policy Editor. Select the policy and application group from the dropdowns, and then click **Add and Edit** or **Add and Close**.



The screenshot shows the BeyondTrust Endpoint Privilege Management Reporting dashboard. On the left is a navigation sidebar with options: Summary, Events (selected), Process Detail, Discovery, Actions, Target Types, and Users. The main area displays 'Events / All' with filters for Platform (Windows), Event Time (7 days), and a Filter by dropdown. Below the filters are 'Export To CSV' and 'Add To Policy' buttons. A table lists 181 items, with one row selected. The table columns are Event Time, Platform, Description, and Event Category. The selected row is: 06/16/2023 10:02:53 AM, Windows, Passively Audit Java(TM) W..., Process Control.

The second screenshot shows the 'Endpoint Privilege Management Policy Editor' with a modal window titled 'ADD APPLICATIONS TO POLICY'. The modal contains two dropdown menus: 'Policy' and 'Application Group'. At the bottom of the modal are three buttons: 'ADD AND EDIT', 'ADD AND CLOSE', and 'CANCEL'.

## Discovery Dashboard

This dashboard displays information about applications discovered by the Reporting database for the first time. An application is first discovered when an event is received by the Endpoint Privilege Management Reporting database. The **Discovery** dashboard displays events from Windows and macOS operating systems.



**Note:** Windows uses the terminology of **Admin Rights** and macOS uses the terminology of **Authorization**.

The **Discovery** dashboard displays the following charts:

Chart	Description
Applications first reported in the specified time frame	<p>A chart showing the number of applications discovered, filtered by the types of rights or authorization detected:</p> <p>For Windows:</p> <ul style="list-style-type: none"> <li>• <b>Admin Rights Detected</b></li> <li>• <b>Admin Rights Not Detected</b></li> </ul> <p>Click the <b>Admin rights detected</b> or <b>Admin rights not detected</b> lines in the graph to open the <b>Discovery</b> dashboard report with the <b>Admin Rights Required</b> filter applied.</p> <p>For macOS:</p> <ul style="list-style-type: none"> <li>• <b>Authorization Required</b></li> <li>• <b>Authorization Not Required</b></li> </ul> <p>Click the <b>Authorization Required</b> or <b>Authorization Not Required</b> lines in the graph to open the <b>Discovery</b> dashboard report with the <b>Authorization Required</b> filter applied.</p>
Types of newly discovered applications	<p>A chart showing the number of applications discovered by the type of application. The types are different for Windows and macOS operating systems.</p> <p>Click the chart to open the <b>Discovery</b> dashboard report with the <b>Admin Rights Required</b> filter applied.</p>

The Discovery dashboard has the following tables:

New applications with admin rights detected	<p>A list of discovered applications that are running with admin rights. This list is ordered by the number of users. Click <b>View all</b> to see the full list.</p> <p>Click any of the applications in the list to open the <b>Discovery</b> dashboard report with the <b>Admin Rights Required</b> and <b>Matched</b> filter applied.</p>
New applications with admin rights not detected (top 10)	<p>A list of discovered applications that are running with standard, not admin rights. This list is ordered by the number of users. Click <b>View all</b> to see the full list.</p> <p>Click any of the applications in the list to open the <b>Discovery</b> dashboard report with the <b>Admin Rights Required</b> and <b>Matched</b> filter applied.</p>

New applications with admin rights detected (by type)	A list of the types of applications that required admin rights that were newly discovered within the time interval. They are ordered by the total number of applications for each type. Click <b>View all</b> to see the full list.  Click any of the applications in the list to open the <b>Discovery</b> dashboard report with the <b>Admin Rights Required</b> and <b>Matched</b> filter applied.
New applications with admin rights not detected (by type)	The types of applications that did not require admin rights that were newly discovered within the time interval. They are ordered by the total number of applications for each type.  Click any of the applications in the list to open the <b>Discovery</b> dashboard report with the <b>Admin Rights Required</b> and <b>Matched</b> filter applied.

## Discovery Reports

The following reports are available from the navigation panel, under the **Discovery** dashboard. A description of each is in the below sections.

- **Discovery By Path**
- **Discovery By Publisher**
- **Discovery By Type**
- **Discovery Requiring Elevation**
- **Discovery From External Sources**
- **Discovery All**

## Discovery by Path

This table displays the discovered applications grouped by path. Where there is more than one application per path, click **+** to expand the entry to examine each application.

The following columns are available for the Windows and macOS **Discovery By Path** table:

- **Path:** The path of the applications.
- **Description:** The description of the application.
- **Publisher:** The publisher of the applications.
- **Name:** The product name of the application.
- **Type:** The type of application.
- **Version:** The version number of a specific application.
- **# Users:** The number of users.
- **Median # Processes / User:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **# Applications:** The number of applications.
- **Date first Reported:** The date the application was first entered in the database.
- **Date first Executed:** The first known date the application was executed.

Some of these columns allow you to drill down to additional information:

- **Description:** Opens the **Applications** report for that application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table and lists the events received in the time period for the selected application.

## Discovery by Publisher

This table displays the discovered applications grouped by publisher. Where there is more than one application per publisher, click + to expand the entry to examine each application.

The following columns are available for the Windows and macOS **Discovery By Publisher** table:

- **Publisher:** The publisher of the applications.
- **Description:** The description of the application.
- **Name:** The product name of the application.
- **Type:** The type of application.
- **Version:** The version number of a specific application.
- **# Users:** The number of users.
- **Median # Processes / User:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **# Applications:** The number of applications.
- **Date first Reported:** The date the application was first entered in the database.
- **Date first Executed:** The first known date the application was executed.

Some of these columns allow you to drill down to additional information:

- **Description:** Opens the **Applications** report for that application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table and lists the events received in the time period for the selected application.

## Discovery by Type

This table displays applications filtered by type. When there is more than one application per type, click + to expand the entry to see each application.

The following columns are available for the Windows and macOS **Discovery By Type** table:

- **Type:** The type of application.
- **# Users:** The number of users.
- **Median # processes / user:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **Applications:** The number of applications.

- **Date first reported:** The date the application was first entered in the database.
- **Date first executed:** The first known date the application was executed.

Expanding the application type in the table, displays the following columns:

- **Description:** The description of the application.
- **Publisher:** The publisher of the applications.
- **Name:** The product name of the application.

Some of these allow you to drill down to additional information:

- **Description:** Opens the **Target Types > Applications** report which is filtered to that application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table and lists the events received in the time period for the selected application.

## Discovery Requiring Elevation

This table displays the applications that were elevated or required admin rights.

The following columns are available for the Windows and macOS **Discovery Requiring Elevation** table:

- **Description:** The description of the application.
- **Publisher:** The publisher of the application.
- **Name:** The product name of the application.
- **Type:** The type of application.
- **# Users:** The number of users.
- **Median # Processes / User:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **Version:** The version number of a specific application.
- **Elevate Method:** The type of method used to elevate the application: **All**, **Admin account used**, **Auto-elevated**, or **on-demand**.
- **Date First Reported:** The date the application was first entered in the database.
- **Date First Executed:** The first known date the application was executed.

Some of these allow you to drill down to additional information:

- **Description:** Opens the **Target Types > Applications** report filtered to that application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table and lists the events received in the time period for the selected application.
- **Elevate Method:** Displays the **Events All** table with an extra **Elevate Method** column.

## Discovery from External Sources

This table displays all applications that originated from an external source such as the internet or an external drive.

The following columns are available for the **Windows Discovery from External Sources** table:

- **Description:** The description of the application.
- **Publisher:** The publisher of the application.
- **Name:** The product name of the application.
- **Type:** The type of application.
- **Source:** The source of the application.
- **# Users:** The number of users.
- **Median # Processes / User:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **Version:** The version number of the application.
- **Date First Reported:** The date the application was first entered in the database.
- **Date First Executed:** The first known date the application was executed.

Some of these allow you to drill down to additional information:

- **Description:** Opens the **Applications** report for that application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Opens the **Events All** table and lists the events received in the time period for the selected application.



## Discovery All

This table lists all applications discovered in the time period, grouped by the application description so that if multiple versions of the same application exist, they are grouped on the same line. Click **+** in the **Version** column to expand the list.

The following columns are available for the Windows and macOS **Discovery All** table:

- **Description:** The description of the application.
- **Publisher:** The publisher of the application.
- **Name:** The product name of the application.
- **Type:** The type of application.
- **Version:** The version number of the application.
- **# Users:** The number of users.
- **Median # Processes / User:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **Date First Reported:** The date the application was first entered in the database.
- **Date First Executed:** The first known date the application was executed.
- **Name:** The product name. This is hidden by default but you can select it from the **Actions > Choose Columns** menu.

Some of these columns allow you to drill down to additional information:

- **Description:** Opens the **Applications** report for that specific application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table.

## Actions Dashboard

The **Actions** dashboard breaks down the application activity by the type of action. It also lists the most active targets.

The **Actions** dashboard has the following charts:

Chart	Description
All actions over the specified time frame	<p>A chart showing the number of targets filtered by the type of action for each time frame for all target types.</p> <p>The types of action are:</p> <ul style="list-style-type: none"> <li>• <b>Elevated</b></li> <li>• <b>Blocked</b></li> <li>• <b>Passive</b></li> <li>• <b>Canceled</b></li> <li>• <b>Custom</b></li> <li>• <b>Drop admin rights</b></li> </ul> <p>Click the chart to open the <b>Target Types</b> report with the <b>Action</b> filter applied.</p>
Distinct target count by target type	<p>A chart showing the target count for each target type, filtered by the type of action.</p> <p>The targets types are:</p> <ul style="list-style-type: none"> <li>• <b>Application</b></li> <li>• <b>Services</b></li> <li>• <b>COM</b></li> <li>• <b>Remote PowerShell</b></li> <li>• <b>ActiveX</b></li> <li>• <b>URL</b></li> <li>• <b>Content</b></li> </ul> <p>Click the chart to open the <b>Target Types</b> report with the <b>Action</b> and <b>Target Type</b> filters applied.</p>
Top 10 targets	<p>A chart showing the ten most used targets by process count.</p> <p>Click the chart to open the <b>Events All</b> report with the <b>Action</b> and <b>Target Description</b> filters applied.</p>

## Target Types Dashboard

The **Targets Types** report lists all targets for all actions over a specified period of time in a tabular format. Click the target in the **Description** column to view a dashboard containing charts showing the activity and actions for the target.

Chart	Description
Actions over the last (time interval)	A chart showing the number of processes for each action for the target. The actions are listed in the legend to the right of the chart. Click the action to open the <b>Events / All</b> report to view the events for that action and target.
Top 10 Users	A chart showing the 10 most common activities by process count for users. Click the chart to open the <b>Events / All</b> report to view the events for that user, action, and target.
Top 10 Hosts	A chart showing the 10 most common activities by process count for hosts. Click the chart to open the <b>Events / All</b> report to view the events for that host, action, and target.
Run Method	A chart showing the count and percentage for activities by run method (Shell or Automatic) count for hosts. Click the chart to open the <b>Events / All</b> report to view the specific events by run method.
Discovery - Admin Rights	A chart showing the count and percentage for activities that did not require admin rights. Click the chart to open the <b>Events / All</b> report to view the specific events that did not require admin rights.

## Trusted Application Protection Dashboard

You can access this dashboard from the **Summary** dashboard. Click the number listed in the **Incidents** table, under **TAP**. This dashboard shows information about Trusted Application Protection (TAP) incidents. A TAP incident occurs when a child process of a trusted application is blocked due to a trusted application policy or when a DLL is prevented from loading by a trusted application because it lacks a trusted owner or publisher.



**Note:** There are no advanced filters for the **Trusted Application Protection** dashboard.

Chart	Description
Trusted Application Protection incidents over the time period.	<p>A column chart showing the number of incidents filtered by the trusted application.</p> <p>Click the chart to open the <b>Process Details</b> report with <b>Time Range</b> filter applied.</p>
Trusted Application Protection incidents, by application	<p>A table listing each trusted application, the number of TAP incidents, the number of targets, the number of users, and the number of hosts affected.</p> <p>Click the <b>Incidents</b> number to open the <b>Process Details</b> report with the <b>Trusted Application Name</b> filter applied.</p> <p>Click the <b>Targets</b> number to open the <b>Targets &gt; All</b> table with the <b>Trusted Application Name</b> filter applied.</p>
Top 10 targets	<p>The top 10 targets for TAP incidents.</p> <p>Click the <b>Target</b> to open the <b>Application</b> report with the <b>Application Type</b> and <b>Distinct Application ID</b> filters applied.</p> <p>Click the <b>Incident</b> number to open the <b>Process Details</b> report with the <b>Distinct Application ID</b> filter applied. Clicking the <b>Users</b> or <b>Hosts</b> number opens the <b>Users</b> or <b>Hosts</b> list, respectively.</p>

## Users Dashboard

The following dashboards are available from the navigation panel under **Users**. Overviews for each are described in the below sections.

- **User Experience**
- **Privileged Logons**
- **Privileged Account Management**

### User Experience Dashboard

This dashboard shows how users interacted with Messages, Challenge/Response dialog boxes, and the Shell (On-Demand) menu.

Chart	Description
User Experience over the time period	A chart showing the percentage of users that experienced each interaction type filtered by the specified time period. Click the chart to display a list of users presented with that interaction.
Message Distribution	A chart showing how many users are in the defined categories of messages per time period. Click the chart to display a list of users in that category.
Messages per action type	A table showing message types displayed for <b>Allowed</b> and <b>Blocked</b> actions. Click the prompts, notifications or counts, or table to open the <b>Events All</b> report with the <b>Action</b> and <b>Message Type</b> filters applied.

### Privileged Logons

This dashboard shows how many accounts with **Standard** rights, **Power User** rights and **Administrator** rights generated logon events filtered by the time frame.

Chart	Description
Privileged Logons over the last (time interval)	A chart and table showing the number of logons by the account types over time. Click the chart to open the <b>User Logons</b> table with the <b>Show Administrator Logons</b> , <b>Show Power User Logons</b> and <b>Show Standard User Logons</b> filters applied.
Logons by Account Privilege	A chart showing the total number of logons filtered by the different account types. Click the chart to open the <b>User Logons</b> table with the <b>Show Administrator Logons</b> , <b>Show Power User Logons</b> and <b>Show Standard User Logons</b> filters applied.
Logons by Account Type	A chart showing the total number of logons filtered by domain accounts and local accounts. Click the chart to open the <b>User Logons</b> table with the <b>Account Authority</b> filter applied.
Top 10 Logons by Chassis Type	A chart showing the total number of logons filtered by the top 10 chassis types. Click the chart to open the <b>User Logons</b> table with the <b>Chassis Type</b> filter applied.
Top 10 Logons by host Operating System	A chart showing the total number of logons filtered the top 10 host operating systems. Click the chart to open the <b>User Logons</b> table with the <b>OS</b> filter applied.

Chart	Description
Top 10 Accounts with Admin Rights	<p>A chart showing the top 10 accounts with admin rights that have logged into the most host machines.</p> <p>Click the chart to open the <b>User Logons</b> table with the <b>User Domain</b> and <b>User Name</b> filter applied.</p>
Top 10 hosts with Admin Rights	<p>A chart showing the top 10 host machines logged on to by the most users with admin rights.</p> <p>Click the chart to open the <b>User Logons</b> table with the <b>Host Name</b>, <b>Show Administrator Logons</b> filter applied.</p>

## Privileged Account Management

This dashboard shows any blocked attempts to modify privileged accounts over the specified time interval.

Chart	Description
Privileged Account Management over the last (time interval)	<p>A chart breaking down the privileged account management events by time period.</p> <p>Click the chart to display the <b>Privileged Account Management</b> table with the <b>Time Range</b> filter applied.</p>
Table showing users blocked, hosts blocked, applications blocked, and total blocked modifications	<p>A table showing the number of users, hosts, applications blocked, and the total number of blocked events within the specified time frame.</p> <p>Click the count numbers to open the <b>Privileged Account Management</b> table.</p>
By Privileged Group	<p>A chart showing the privileged account modification activity blocked by Windows group name.</p> <p>Click the chart to open the <b>Privileged Account Management</b> table with the <b>Group Name</b> filter applied.</p>
Top 10 applications attempting account modifications	<p>A chart showing the privileged account modification activity that was blocked, broken down by the <b>Application Description</b>.</p> <p>Click the chart to open the <b>Privileged Account Management</b> table with the <b>Application Description</b> filter applied.</p>
Top 10 users attempting account modifications	<p>A chart showing the top 10 users who attempted modifications.</p> <p>Click the chart to open the <b>Privileged Account Management</b> table with the <b>User Name</b> filter applied.</p>
Top 10 hosts attempting account modifications	<p>A chart showing the top 10 hosts attempting privileged account modifications.</p> <p>Click the chart to open the <b>Privileged Account Management</b> table with the <b>Host Name</b> filter applied.</p>