BeyondTrust

Endpoint Privilege Management 24.4 Administration Guide

TC:6/3/2024

Table of Contents

EPM Windows & Mac SaaS Platform 9
Workflow 10
Installation 10
Organize computers 10
Policy configuration 10
Sign-in to EPM 11
The Home Page 12
User Account Profile Preferences 13
Switch Between BeyondTrust Applications 14
View your notifications 15
Add URLs to Allowlist 15
Overview 17
The Policies Page 18
Create a Policy 19
Open an Existing Policy 21
View Policy Details 22
Policy Revisions and Drafts 22
Promote a Policy 22
Assign a Policy to a Group 23
Download a Policy Revision 24
Revert and Discard Changes 25
Delete a Policy 26
Force Policy Updates 27
Force Update Policy for Windows End Users 27
Force Update Policy for macOS End Users 27
Overview 28
Quickstart Templates 29
QuickStart template for Windows and macOS 30
QuickStart template for servers 34
Workstyles 35
Set up logging for privileged applications and processes 36

Set the order for workstyle processing 37
Create an Application Rule 38
Create an On-Demand Application Rule 40
Create TAP Rules 42
Set General Rules 43
Enable Microsoft Block Rules 44
Add filters 45
Search a policy 48
Application Groups 49
Application Definitions 50
Create an Application Group 67
Add Application Using App Definitions 68
Add Application from Template 69
Add Application From Analytics 70
Use Advanced Options 71
Copy Application Definitions 72
Disable an Application 73
Content Groups 74
Content definitions 75
Create a Content Group 77
Create a Content Rule 78
Messages 79
Create a Message 80
Add message header and body content 81
Message header options 81
Message body options 81
Add ActiveX Message 83
Select Message Language 84
Add an Image 85
Add email (Windows only) 86
Add a Reason Prompt 87
Add Challenge/Response Authorization 88
Add User Authorization 90

Edit Designated User **92**
Configure Multifactor Authentication **93**
Custom Tokens **95**
Create a Custom Token **96**
Create a Token 96
Set Integrity Level and Anti-tamper **97**
Add Group to Custom Token **98**
Select Privileges for Custom Token **99**
Enable Process Access Rights **100**
Access Rights 100
Policy Editor Utilities **102**
Policy Assistant (Beta) 102
Policy Editor Licensing 102
Import Policy 103
Import Template Policies 103
Manage Audit Scripts 103
Manage Rule Scripts 104
Advanced Agent Settings 104
Set Up Agent Protection 105
Regenerate UUIDs 106
Power Rules and Regular Expressions **107**
Power Rules 107
Windows Workstyle Parameters 107
Regular Expression Syntax 109
Examples 109
Syntax 109
Overview **111**
Manage Computers **112**
Overview 112
Authorize and Assign Computers to a Group 112
Computers List Page **114**
View Computer Details **116**
Edit a Computer's Group Assignment **117**

Reissue a Certificate to a Computer **118**
Update Computer Details **119**
View a Computer's Analytics **120**
Archive a Computer **121**
Delete a Computer **122**
Computer Groups **123**
Computer Groups List Page **124**
Create a group **125**
Download a List of Groups to CSV **126**
View Group Details **127**
Edit Group Policy Assignment **128**
Edit Group Name and Description **129**
Set a Default Group **130**
Delete a Group **131**
Management Rules **132**
Workflow 132
About Rules **133**
Rules Processing 133
Management Rules List Page **134**
Create a Custom Rule **135**
Edit a System Rule **136**
Edit Custom Rule **137**
Activate or Deactivate Rule **138**
Delete a Rule **139**
Configure EPM **140**
Download client software **141**
Requirements 141
Download installers 141
Install the Mac Adapter 142
Install the Windows Adapter 145
Reset the EPM Windows Adapter **150**
Access the Adapter Reset Tool 150
Requirements 150

Download 150
Usage 150
Package Manager Installation **152**
Overview **153**
Install Package Manager (Windows) **154**
Windows Adapter Reset Tool 155
Install Package Manager (macOS) 155
Set Group Updates **157**
Track Computer Updates **159**
Package Manager FAQ **160**
Package Manager settings **162**
Set rate limit preferences 162
Computer Settings **163**
Domain Settings **164**
Active Directory Settings **165**
Add Microsoft Entra ID Connector **166**
Add a Local AD Connector **167**
Disable Local AD Connector **168**
Disable a Connector 168
Edit Local AD Connector **169**
Edit a Connector 169
Delete a Local AD Connector **170**
Delete Connector 170
SIEM Settings **171**
Event Types 171
Configure AWS S3 Bucket 172
Add Splunk to EPM 173
Add Microsoft Sentinel to EPM 173
Add QRadar to EPM 173
Authorization Request Settings **175**
Use ServiceNow to Manage User Requests 176
Create a Policy for ServiceNow Requests **184**
VirusTotal Settings **187**

Set up VirusTotal **188**
Security Settings **189**
API Settings **190**
Create an API Account **191**
Generate a Client Secret **192**
View API Account Details **193**
Edit an API Account **194**
Delete an API Account **195**
Activity Page **196**
Configure OpenID Connect **197**
Add EPM Instance to Microsoft Entra ID Tenant **199**
Add EPM Instance to Okta **200**
Add EPM Instance to Ping Identity **202**
Change Authentication Provider **203**
The About Page **204**
Overview **205**
Before Creating User Accounts 205
About user roles and resources **206**
User roles 206
Resources 206
Automatic Role Mappings on Upgrade 207
The Users Page **208**
Create a user **209**
Create an account 209
Resend an Email Invite **210**
Edit a User's Profile **211**
View a User's Details **212**
Disable a User **213**
Analytics **214**
Overview 214
Walkthrough **217**
Create and Add Users to Computer Groups **218**
Filters **219**

Overview 219
Filters List 219
Create and Save Your Application View **226**
Load an Application View **227**
Recommended Views **228**
Events 228
Applications 228
Analytics Use Cases **230**
Generate Views 230
Export to CSV **233**
The Dashboard Page **234**
The Events Page **235**
Add Events to Policy **237**
View Event Details **238**
Look Up VirusTotal Score **239**
The Applications Page **240**
View an Application's User Activity **241**
The Application Details Page **242**
View an Event's Details **243**
Add an Application to Policy **244**
The Users Page **245**
The Activity Auditing Page **246**
View Activity Details **247**
View Authorization Request Details **248**
Windows and macOS OS Technical Support Statement **249**

EPM Windows & Mac SaaS Platform

Endpoint Privilege Management is a powerful endpoint privilege management application that complements least privilege access with advanced application control. This gives you the industry's most complete solution for condensing the attack surface and eliminating lateral movement.

- Passwordless Administration: Perform administrative functions on an endpoint without the need for privileged or administrator credentials.
- Application Control: Automatically allow list approved apps for total control over what users can install or run.
- Trusted Application Protection: Pre-built templates stop attacks involving trusted apps, catching bad scripts and infected email attachments.
- QuickStart Templates: Flexible workstyle templates let you implement least privilege policies in days for everyone, even sysadmins.
- SaaS and On-Premises Deployment Options: Select from multiple deployment models to best suit your business needs, compliance requirements, and security ecosystem.
- Power Rules: Use PowerShell scripts to automate workflows, create custom behaviors, or build integrations with ITSM and other tools.

Workflow

This topic provides a high-level view on the setup and configuration steps for EPM.

Installation

Download client and adapter installers that you will deploy to the computers in your estate.

- Download adapter installers

Organize computers

Create a computer group and add the computers that will be receiving the same policy.

- Create computer groups

Policy configuration

We recommend using a QuickStart template when initially setting up EPM.

- QuickStart Templates
- Create a policy

Sign-in to EPM

You must enable cookies in your browser. Otherwise, a blank page displays when you try to navigate to the EPM console.

The version is displayed at the bottom of the logon page.

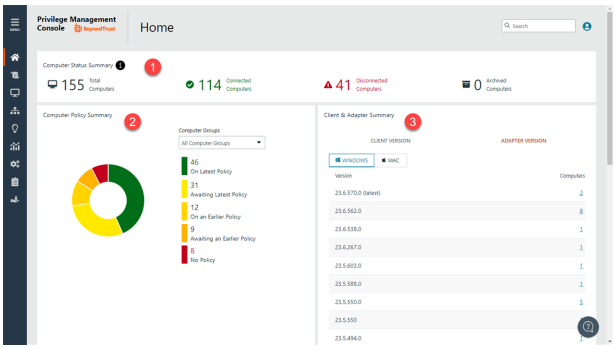
To log on:

1. Navigate to your EPM instance and click **Sign in**.
2. Click the email associated with your account.

The Home Page

The **Home** page serves as a dashboard offering **Computer Status**, **Computer Policy**, and **Client & Adapter** summary information.

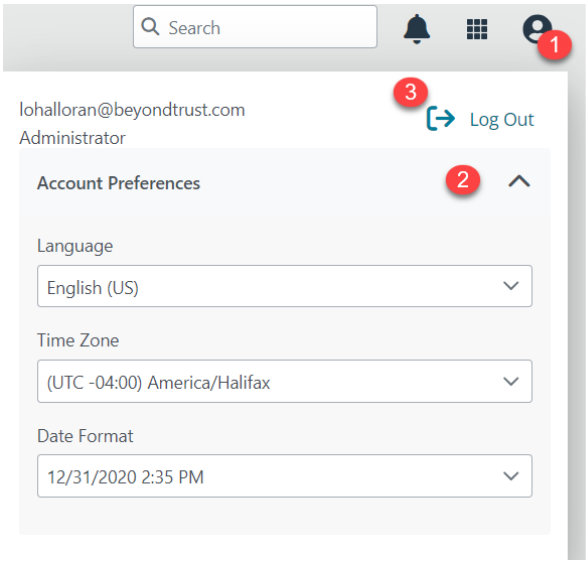
1. **Computer Status Summary**: Get the most up to date status information on each of the computers in the estate with Endpoint Privilege Management installed. Click the status link to drill down to more information about the computers.
2. **Computer Policy Summary**: Displays current metrics on policy status. Select a computer group from the list to display the status per group.
3. **Client & Adapter Summary**: View version information for clients and adapters sorted by operating system. The list displays which client/adapter version is used and by how many computers. Drill down to see more information about each computer on the **Computers** page.



User Account Profile Preferences

Access the user account profile icon from any page.

1. You can click the **User Account Profile** icon to view your current account profile information, including the type of user role assigned (*Standard* or *Administrator*).
2. You can expand the **Account Preferences** section and *view* or *edit* the basic settings.
3. This is also where you *log out* of the EPM console.



Switch Between BeyondTrust Applications

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

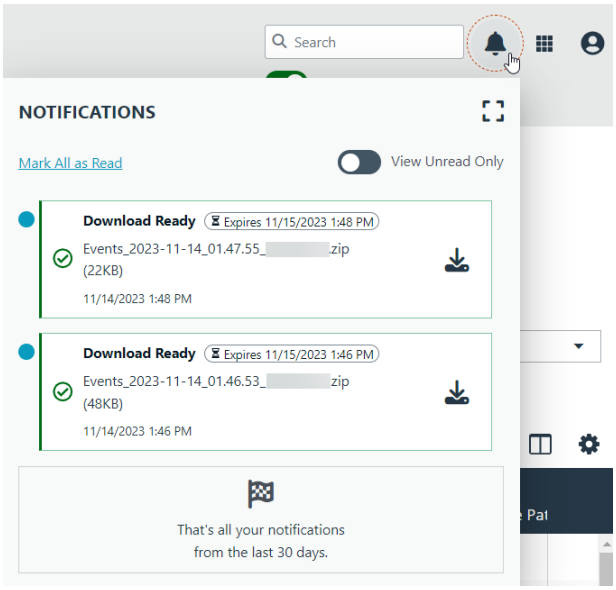
The **App Switcher** menu appears in the upper right. Click the menu for a list of connected applications, and click an application. There can be more than one instance of an application, except for Identity Security Insights.

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

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

View your notifications

Notifications are displayed when downloading CSV files from the **Events** page.



Add URLs to Allowlist

Depending on the access restrictions in place for your web communications or if you use proxies, you might need to add URLs used by EPM to the allowlist.

Azure Region

We recommend allowlisting the Azure URL for your region to ensure employee computers managed by EPM can contact the Azure instance to download assets including policy.

Azure regions and corresponding URLs

Region	Allowlist URL
East US	https://prdpmpolicyeastus.blob.core.windows.net https://prdpmpolicy2eastus.blob.core.windows.net
Central US	https://prdpmpolicycentralus.blob.core.windows.net https://prdpmpolicy2centralus.blob.core.windows.net
West US	https://prdpmpolicywestus2.blob.core.windows.net https://prdpmpolicy2westus2.blob.core.windows.net
Canada Central	https://prdpmpolicycanadacentral.blob.core.windows.net https://prdpmpolicy2canadacentra.blob.core.windows.net

Region	Allowlist URL
UK South	https://prdpmpolicyuksouth.blob.core.windows.net https://prdpmpolicy2uksouth.blob.core.windows.net
Germany West Central	https://prdpmpolicygermanywestce.blob.core.windows.net https://prdpmpolicy2germanywestc.blob.core.windows.net
North Europe	https://prdpmpolicynortheurope.blob.core.windows.net https://prdpmpolicy2northeurope.blob.core.windows.net
South Africa North	https://prdpmpolicysouthafricano.blob.core.windows.net https://prdpmpolicy2southafrican.blob.core.windows.net
Central India	https://prdpmpolicycentralindia.blob.core.windows.net https://prdpmpolicy2centralindia.blob.core.windows.net
South East Asia (Singapore)	https://prdpmpolicysoutheastasia.blob.core.windows.net https://prdpmpolicy2southeastasi.blob.core.windows.net
East Japan	https://prdpmpolicyjapaneast.blob.core.windows.net https://prdpmpolicy2japaneast.blob.core.windows.net
Australia East	https://prdpmpolicyaustraliaeast.blob.core.windows.net https://prdpmpolicy2australiaeas.blob.core.windows.net

EPM URLs

Add the following URLs to your allowlist to ensure Package Manager can download the files to install or update computers:

- https://prdpkgsinstallercdn.azureedge.net
- https://prd2pkgsinstallercdn.azureedge.net

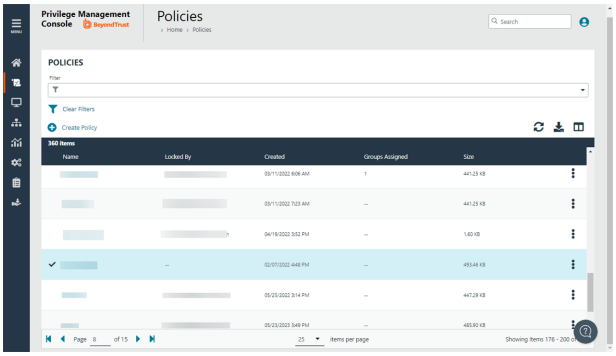
The following URLs are used for communication between managed endpoints and Package Manager and adapter components.

- https://<*yourtenant*>.pm.beyondtrustcloud.com:443
- https://<*yourtenant*>-services.pm.beyondtrustcloud.com:443

Overview

On the **Policies** page,

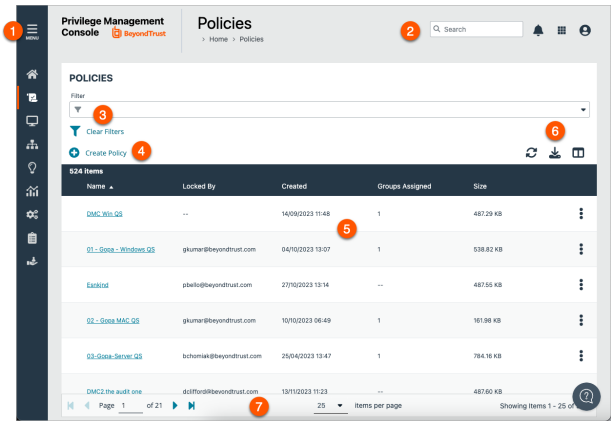
- Create a policy
- View policy details where you can keep track of policy revisions and drafts
- Assign a policy to a computer group
- Revert and discard changes to a policy
- Delete a policy
- Access the Policy Editor where you configure the policy.



Note: *A standard user requires delegated access to the* ***Policies*** *page. For more information, see About user roles and resources.*

The Policies Page

Use the **Policies** page to view at-a-glance data about your active and inactive policies.



1. **Sidebar:** Easy access to all pages in Endpoint Privilege Management, including the Home, Policies, Computers, Computer Groups, Management Rules, Analytics, Configurations, Auditing, and Users pages.
2. **Header:** Enter keywords to run a global search across computer groups, policies, computers, and users, view your notifications, access your connected apps, and set your account preferences.
3. **Filters:** Click the drop arrow to select a filter type. The selected filter displays to the left of the drop-down.
    - **Clear Filters:** Click to remove all filters and search results
    - **Filter types**
        - **Name:** Enter all or part of a policy name.
        - **Locked By:** Enter an email address to view all policies locked via that account.
        - **Created:** Select a date from the date selector that displays to the left of the Filter drop-down to view all policies created on that day.
4. **Create Policy:** Click to create a new policy.
5. **List options:** Click to refresh the policies list, to download list of the displayed policies to a .csv file, and click to select which columns you want to display on your **Policies** page.
6. **Policy list columns:** Not all columns display in the image above.
    - **Name:** The policy name.
    - **Locked By:** If a policy is locked, this displays the email of the user last locked it.
    - **Created:** The date and time stamp when the policy was created in your environment.
    - **Groups Assigned:** The number of computer groups that have the policy assigned to them.
    - **Size:** The size of the policy (in KB).
    - **Revisions:** The total number of revisions recorded for the policy.
    - **Users:** The total number of users who can create, edit, and/or view the policy.
    - **Period Locked:** If a policy is locked, this displays the period (in days or months, if longer than 3 weeks) when the policy was last locked.

Create a Policy

> ***Note:*** *A standard user requires delegated access to this page. For more information, see About user roles and resources.*

There are different ways to create and edit a policy:

Use the Policy Editor

Use a QuickStart template for macOS or Windows to get started. You can then customize the template to suit your requirements.

Both templates 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. You can then customize the template to suit your requirements.

1. Go to **Policies**.
2. Click **Create Policy**.
3. Select one of the following:
    - **QuickStart for Windows:** A template with Workstyles, Application Groups, messages, and Custom Tokens already configured.
    - **QuickStart for Mac:** A 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 create a policy without any existing framework. There are no preconfigured settings in this template.
4. Enter a name and description.
5. Click **Create Policy**.

The Policy Editor opens to the **Workstyles** page. At this point, configure the Workstyle, Application Groups, Application Rules, and other policy configuration as required for your organization.

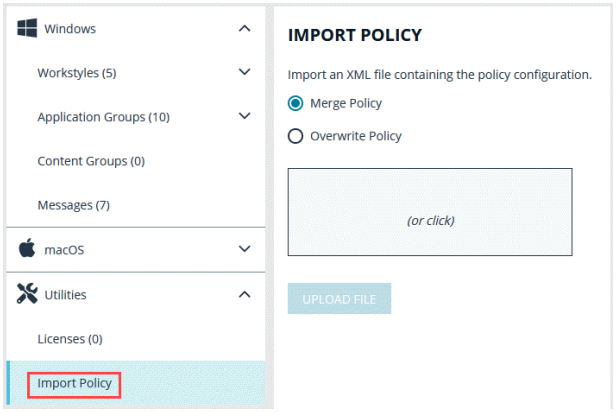
> *For more information about QuickStart templates, see "Quickstart Templates" on page 29.*

Upload a File to Create Policy

You can upload an XML policy file in EPM when you first create the policy.

To upload an XML file for a *new* policy:

1. Go to **Policies**.
2. Click **Create Policy**.
3. Select a policy template and enter policy details.
4. Click **Create Policy**.
5. Select **Utilities > Import Policy**.
6. Choose either **Merge Policy** or **Overwrite Policy** and click the box to import your XML policy. You can also drop the file to upload in the box.
7. Click **Upload File**.



Open an Existing 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**.

You can edit more than one policy at a time. Navigate between policies to copy settings in one policy to another. This can be useful if you are working in a test policy and want to copy the details to your production policy.

To edit a policy XML file:

1. Go to **Policies**.
2. Find the policy, and select **Download Latest Revision** from the menu.

View Policy Details

On the **View Details** page for a policy, you can download policy revisions, see the check-in and discarded date and time, see the users with policy permissions, and review activity auditing on the policy.

Auditing activity includes audit type, the user accessing the policy, and a summary of the activity.

To access policy details:

1. Go to **Policies**.
2. Click the policy, and then select **View Computer Details** from the menu.

Policy Revisions and Drafts

You can review the history of revisions and drafts on the policy **Revision History** page.

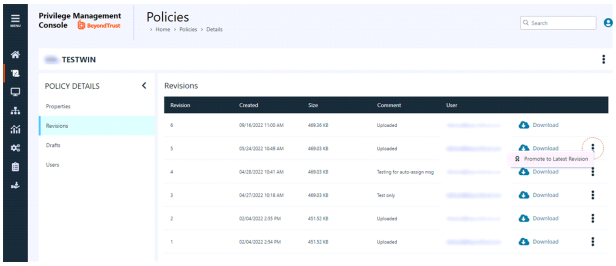
1. Click the policy, and then select **Revision History** from the menu. You can also just click on the policy name.
2. Click the **Revisions** or **Drafts** option to view more information about the changes to the policy.

Promote a Policy

If you change a policy and you want to discard those changes, you can promote a previous version of the policy.

To promote a previous version of a policy:

1. Go to **Policies**.
2. Find the policy, and then select **View Policy Details** from the menu.
3. Click **Revisions**.
4. Find the revision that you want to use, and then select **Promote to Latest Revision**.



5. On the **Promote Policy to Latest Revision** dialog box, you can add notes for future reference.
6. If the policy is already applied to certain groups, you can choose to apply the latest revision now by checking the **Yes, auto assign latest revision to group(s)** box.

IMPORTANT!

To auto-assign a policy revision to one or more groups, you must be an administrator user or a standard user with permissions to all the groups that are affected by the policy. If you have insufficient access permissions, the auto-assign policy feature is not accessible.

7. Click **Promote to Latest**.

Assign a Policy to a Group

1. Go to **Policies**.
2. Find the policy, and then select **Assign Policy to Group** from the menu.
3. In the **Assign Policy to a Groups** panel, select the revision for the policy, and then select one or more groups. If there are many groups in your estate, search on keywords to find a group.
4. Click **Assign Policy**.

Download a Policy Revision

You can change the properties of a policy using the XML file and a tool of your choice.

To edit a policy XML file:

1. Go to **Policies**.
2. Find the policy, and select **Download Latest Revision** from the menu.
3. Change the properties.
4. After you finish changes, on the **Policies** page, select the policy, and then select **Upload Revision**. The updated policy is recognized as a new revision based on a unique identifier in the XML. Each time the same policy is checked in, the revision of the policy is incremented.
5. Import the policy. You can merge with the existing or overwrite. If the XML does not pass validation, then the policy is not uploaded.
6. On the **Auto Assign Policy to Groups** dialog box, select the groups to update with the new policy revision.
7. Select **Apply to Groups**.

Revert and Discard Changes

A policy locked by a user can be unlocked. The policy is reverted to the previous version. After unlocking the policy, the user account that locked the policy can no longer save or check in changes to that policy.

You can follow these steps when a policy is checked out using the MMC snap-in.

You must be an Administrator or Policy Administrator.

To unlock and discard the changes to a policy:

1. Go to **Policies**.
2. Find the policy, and then select **Revert & Discard Changes** from the menu.
3. Click Revert & Discard.

Delete a Policy

Delete a policy when it is no longer needed.

When deleting a policy:

- The policy must be unlocked. The **Delete** option is not available when the policy is locked.
- If the policy is assigned to one or more groups, then you can select a different policy and revision. If you do not select another policy, then groups are no longer controlled by policy.

To delete a policy:

1. Go to **Policies**.
2. Find the policy, and then select **Delete** from the menu.
3. Click **Delete Policy**.

Force Policy Updates

End users working on either Windows or macOS computers can update policy on their computers without administrator assistance.

Force Update Policy for Windows End Users

End users can check and force a policy update to their computer from the system tray. Using this option reduces the time it takes to update a policy.

1. In the system tray, click the Endpoint Privilege Management icon.
2. Click **Check for Policy Update**.

One of the following notifications can appear:

- **Update Finished** to notify the user that a policy update has been applied.
- **No Updates Found** if the current policy is already up to date.
- **Unable to Check for Updates** if the computer cannot reach the management platform.

Force Update Policy for macOS End Users

A user can check whether a new policy is available. If it is, then the new policy is downloaded and applied. The immediate availability of a new policy is useful when you have an issue that requires a policy update, without the necessity of waiting for a poll to pull in a new one.

To refresh all policies, select the **Endpoint Privilege Management for Mac** menu bar icon, and select **Refresh all Policies**.

If a newer policy is found, it is downloaded and applied immediately.

A message confirming the successful update appears. The new policy revision date also appears in the dropdown menu as *Last updated*.

Overview

Use the Policy Editor to customize a QuickStart template or create a new policy with no preexisting configuration. In a typical scenario, we recommend using a QuickStart template to get started. You can then build on those configurations using the Policy Editor.

The components that make up a policy:

- Workstyles
- Application groups
- Content groups
- Messages
- Custom tokens
- Utilities

For more information about the QuickStart templates and their default configurations, see QuickStart templates.

Quickstart Templates

When creating a new policy, there are three QuickStart templates to choose from:

- QuickStart For Windows
- QuickStart For Mac
- Server Roles

QuickStart templates 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.

For more information about creating and managing policy, see "Overview" on page 17.

Customize the QuickStart Policy

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

At a minimum you need to:

- 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 - Blocklisted Apps** Application Group with any applications that you want to block for all users.
- Set your shared key so you can generate an Endpoint Privilege Management Response code.

QuickStart template for Windows and macOS

This section provides information about the properties for the Windows and macOS QuickStart templates.

Workstyles

Name	Description
All Users	Contains rules that apply to all standard users regardless of the level of flexibility they need: • Block any applications in the **Block - Blocklisted Apps** group. • Allow Endpoint Privilege Management Support tools. • Allow standard Windows functions, business applications, and applications installed through trusted deployment tools to run with admin rights (Windows QuickStart template). • Allow standard macOS functions, business applications, and applications installed through trusted deployment tools to run with admin rights (Mac QuickStart template). • Allow approved standard user applications to run passively.
High Flexibility	Contains rules for users that require a lot of flexibility, such as software developers: • 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 applications that are in the **Add Admin – High Flexibility** group to run with admin rights. • Allow unknown business application and operating system functions to run on-demand.
Medium Flexibility	Contains rules for users that require some flexibility, such as sales engineers: • 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 must be elevated. • Prompt users to provide a reason before they can run unknown applications with admin rights. • Allow applications that are in the **Add Admin – Medium Flexibility** group to run 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	Contains rules for users that don't require much flexibility, such as helpdesk operators: • 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	Provides visibility on the Administrator accounts in use. Contains general rules to: • Capture user and host information. • Block users from modifying local privileged group memberships.

Name	Description
SYSTEM	Protects the **Restricted System Functions** application group against potentially malicious behaviour by a user who can perform elevated PowerShell commands.

Application Groups

Application Groups prefixed with **(Default)** or **(Recommended)** are hidden by default and do not need to be altered.

Name	Description
Add Admin - General (Business Apps) (Windows) Authorize - All Users (Business Apps) (macOS)	Contains applications that are approved for elevation for all users, regardless of their flexibility level.
Add Admin - General (Windows Functions) Authorize - All Users (macOS Functions)	Contains operating system functions that are approved for elevation for all users.
Add Admin - High Flexibility (Windows) Authorize - High Flexibility (macOS)	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 Authorize - Medium Flexibility (macOS)	Contains the applications that require admin rights that should only be provided to the medium flexibility users.
Add Admin - Protected Operations	
Passive - High Flexibility (Business Apps)	Contains applications that are allowed for High Flexibility users without providing admin authorization.
Passive - Medium Business Apps	Contains applications that are allowed for Medium Flexibility users without providing admin authorization.
Passive - Low Flexibility (Business Apps)	Contains applications that are allowed for Low Flexibility users without providing admin authorization.
Block - Blocklisted Apps	Contains applications that are blocked for all users.
Passive - All Users Functions & Apps	Contains trusted applications, tasks and scripts that should execute as a standard user.
(Default) Any Application	Contains all application types and is used as a catch-all for unknown applications.
(Default) Any Trusted & Signed UAC Prompt (Windows) (Default) Any Trusted & Signed Authorization Prompt (macOS)	Contains signed (trusted ownership) application types that request admin rights or authorization.
(Default) Any UAC Prompt (Windows) (Default) Any Authorization Prompt (macOS)	Contains application types that request admin rights or authorization.

Name	Description
(Default) Any Sudo Command (macOS)	Contains all sudo commands and is used as a catch-all for unknown sudo commands.
(Default) Endpoint Privilege Management Tools	Provides access to a BeyondTrust executable that collects Endpoint Privilege Management troubleshooting information.
(Default) Child Processes of TraceConfig.exe	
(Default) Signed UAC Prompt (Windows) (Default) Any Signed Authorization Prompt (macOS)	Contains signed (trusted ownership) application types that request admin rights or authorization.
(Default) Software Deployment Tool Installs	Contains applications that can be installed by deployment tools such as System Center Configuration Manager (SCCM).
(Default) Authorize - System Trusted	Contains operating system functions that are authorized for all users.
(Default) Passive - System Trusted	Contains system applications that are allowed for all users.
(Recommended) Restricted Functions	Contains OS applications and consoles that are used for system administration and trigger UAC/authorization when they are executed.
(Recommended) Restricted Functions (On Demand)	Contains OS applications and consoles that are used for system administration.
(Default) Trusted Parent Processes	Trusted processes for reference in parent-rules.

Messages

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

Name	Description
Allow Message (Authentication)	(Windows). Asks the user to provide a reason and enter their password before the application runs with admin rights.
Allow Authorize (Authentication & Reason)	(macOS). Asks the user to enter their password and provide a reason before the application is authorized to run.
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.

Name	Description
Notification (Trusted)	Notifies the user that an application has been trusted.

QuickStart template for servers

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

This template policy contains the following elements.

Workstyles

Name	Description
Server Role - Active Directory - Template	Supports server management of the Active Directory role.
Server Role - DHCP - Template	Supports server management of the DHCP role.
Server Role - DNS - Template	Supports server management of the DNS role.
Server Role - File Services - Template	Supports server management of the File Services role.
Server Role - Hyper V - Template	Supports server management of the Hyper-V role.
Server Role - IIS - Template	Supports server management of the IIS role.
Server Role - Print Services - Template	Supports server management of the Print Services role.
Server Role - Windows General - Template	Supports general server management operations.

Application Groups

- 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

Content Groups

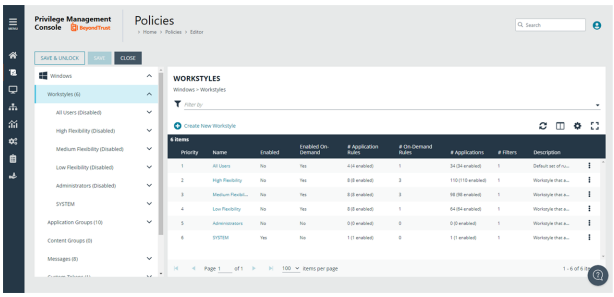
- AD Management
- Hosts Management
- IIS Management
- Printer Management
- Public Desktop

Workstyles

A Workstyle is a container for the rules that will be applied to the computers receiving the policy. If you are using a Windows or macOS Quickstart template, the Workstyles include predefined rule configurations.

If creating policy from a blank template, there is no predefined configuration.

- Add and change the properties for a rule
- Enable Trusted Application Protection (optional)
- Add monitoring and logging
- Change the ordering of Workstyle processing
- Enable the Workstyle



For more information about QuickStart templates, see "Quickstart Templates" on page 29.

Set up logging for privileged applications and processes

Privilege monitoring logs all privileged actions run by the application or process that would fail under a standard user account. These include file operations, registry operations, and any interactions with other components such as Windows services.

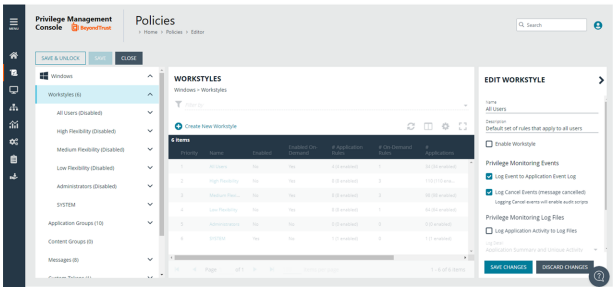
Applications included in privilege monitoring:

- Applications running under a privileged account, such as an administrator or power user.
- An application added to an Application Rule or On-Demand Application Rule that is set up to run with elevated privileges.

Configure privilege monitoring when you create or edit a Workstyle.

Privilege monitoring logs are recorded on each endpoint.

Privilege monitoring is available only on Windows.



For more information about privilege monitoring, contact your BeyondTrust consultant.

Privilege Monitoring Events

- **Log Event to Application Event Log:** Logs an event to the Application event log the first time an application performs a privileged operation.
- **Log Cancel Events (message cancelled):** Raises an event when a user cancels an end user message, either by clicking the **Cancel** button, by clicking the **Email** button, or by clicking a **Hyperlink**. You can configure the user action using policy parameter [PG_ACTION], which can be used by the script to perform different audit actions based on the user interaction. To log **Cancel Events**, enable **Raise an Event** for the rule that has been matched.

Privilege Monitoring Log Files

The following privilege monitoring options are available:

- **Log Application Activity to Log Files:** Check the box to turn on logging.
- **Application Summary and Activity:** Select to log information about the application and unique privileged activity (Default option).
- **Application Summary and Detailed Activity:** Select to log information about the application and all privileged activity.
- **Maximum Activity Records Per Process:** Set the maximum number of records logged per process (Default 100).
- **Keep Application Activity Logs for (Days):** Set how long activity logs are kept before they are purged (Default 14 days).

Set the order for workstyle processing

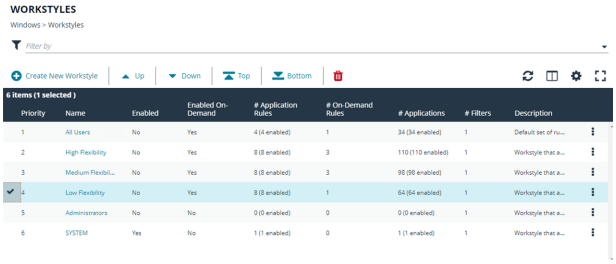
Workstyles are evaluated in the order they are listed. When an application matches on a Workstyle, no further Workstyles are processed for that application.

Ensure the order of the Workstyles is correct because it is possible for an application to match more than one Workstyle.

To change the order:

1. Select a Workstyle in the list to change the order.
2. Use the buttons to move the rule to the preferred location.

   Changes are automatically saved.



Create an Application Rule

1. On the **Policy Editor** page, expand **Windows**.
2. Expand the **Workstyles** node, and then expand a Workstyle.
3. Click **Application Rules**, and then click **Create New**.
4. Set the following:
    - **Target Application Group**: Select an Application Group.
    - **Action**: Select **Allow**, **Allow as Password Safe User**, **Block**, or **Request**. The action that occurs if the application in the targeted Application Group is launched by the end user.
    - **Password Safe Account Name**: Enter the Managed Account name configured in Password Safe for the computer.
    - **Run Rule Script**: Assign a rule script that runs before the Application Rule triggers. Select a rule script from the list.
    - **End User Message**: Select a message from the list.
    - **Access Token**: Select the type of token to pass to the Target Application Group. You can select from:
        - **Passive (No Change**: No changes are made to the token. This is essentially an audit feature.
        - **Enforce User's Default Rights**: Removes all rights and uses the user's default token. Windows UAC always tries to add administration rights to the token being used so if the user clicked on an application that triggers UAC, the user cannot progress past the UAC prompt.
        - **Drop Admin Rights**: Removes administration rights from the user's token.
        - **Add Full Admin (Required for installers)**: Standard Windows Admin token containing all Admin privileges. Use the full admin token in scenarios where your users require privileges **SeDebugPrivilege** or **SeLoadDriverPrivilege**. An example use case is MSI files running in a client/server mode where **SeDebugPrivilege** is required to interact with the server component which runs as SYSTEM. This only applies to cases where the standard user needs to run the MSI directly.
        - **Add Basic Admin Rights**: Permits elevation of most applications and tasks. We recommend using this token as the default elevation token. This access token is essentially full admin but excludes the following privileges: **SeDebugPrivilege** and **SeLoadDriverPrivilege**. If users need to debug applications or access drivers, then use the full admin token.
        - **Privilege Management Support Token**: Applies Add Full Admin privileges with tamper protection removed.
        - **Keep Privileges - Enhanced**: This token behaves similar to the **Passive (no change)** token in that there is no change to privilege, elevation, or integrity level. Uses the same privileges of the original process token and adds some additional context to it: the token is added to the anti-tamper group and will be tracked by the advanced parent tracking feature. This access token can only be used with application rules.
    - **Raise An Event**: **Off**, **On**, **Anonymous**. Select if an event is raised if this Application Rule is triggered. When on, an event is sent to the local event log file. Anonymous removes user and host name from events so the user / host are not identifiable.
    - **Run an Audit Script**: Select an audit script from the list.
    - **Privilege Monitoring**: **Off**, **On**, **Anonymous**. Select **On** to raise a privileged monitoring event.
    - **Reporting Events**: On by default, click to turn off. When the setting is on, events are raised for viewing in EPM Reporting.
5. Click **Create Application Rule**.

Set the Order for Rules Processing

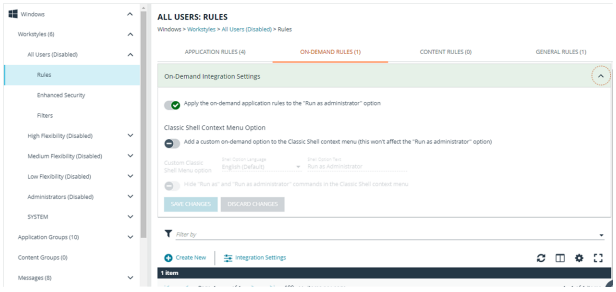
If you add more than one Application Rule to a Workstyle, entries higher in the list have precedence. When an application matches an Application Rule, no further rules or Workstyles are processed. If an application could match more than one Workstyle or rule, then it is important that you order both your Workstyles and rules correctly.

Select an Application Rule in the list to change the order. Changes are automatically saved.

Create an On-Demand Application Rule

Create an on-demand rule to start an application with specific privileges (usually admin rights) from a Windows right-click context menu. The on-demand application rule triggers when the context menu item is selected.

Before creating an on-demand rule, you can set the behaviour for the right-click context menu on the **On-Demand Integration Settings** page. In the Policy Editor, go to **Windows > Workstyles > *<workstyle name>* > On-Demand Application Rules**.



- **Apply the on-demand application rules to the "Run as administrator" option**: Select to override the **Run as administrator** right-click context menu. The labeling of the menu does not change in this instance. This setting applies to all versions of Windows that have the **Run as administrator** context menu.
- **Add a custom on-demand option to the Classic Shell context menu (this won't affect the "Run as administrator" option)**: Select to add a new option to the right-click context menu. Select a language and the option text. You can add text like *Run with Endpoint Privilege Management for Windows*. This setting applies to the Classic Windows Shell only.
- **Hide "Run as" and "Run as administrator" commands in the Classic Shell context menu**: Select to hide these menu items, where present, from the right-click context menu. This setting applies to the Classic Windows Shell only.

To create an On-Demand Application Rule:

1. Expand **Workstyles**, and then expand a Workstyle.
2. Select **On Demand Application Rules**.
3. Click **Create New**.
4. Set the following:
    - **Raise An Event**: **Off**, **On**, **Anonymous**. Select if an event is raised if this Application Rule is triggered. When on, an event is sent to the local event log file. Anonymous removes user and host name from events so the user / host are not identifiable.
    - Click **Create On-Demand Rule**.
    - **Target Application Group**: Select an Application Group.
    - **Action**: Select **Allow**, **Allow as Password Safe User**, **Block**, or **Request**. The action that occurs if the application in the targeted Application Group is launched by the end user.
    - **Password Safe Account Name**: Enter the Managed Account name configured in Password Safe for the computer.
    - **Run Rule Script**: Assign a rule script that is run before the Application Rule triggers. Select a rule script from the list.
    - **End User Message**: Select a message from the list.
    - **Access Token**: Select the type of token to pass to the Target Application Group. You can select from:
        - **Passive** (no change): Doesn't make any change to the user's token. This is essentially an audit feature.
        - **Enforce User's default rights**: Removes all rights and uses the user's default token. Windows UAC always tries to add administration rights to the token being used so if the user clicked on an application that triggers UAC, the user cannot progress past the UAC prompt.
        - **Drop Admin Rights**: Removes administration rights from the user's token.
        - **Add Full Admin (Required for installers)**: Standard Windows Admin token containing all Admin privileges. Use the full admin token in scenarios where your users require privileges **SeDebugPrivilege** or

SeLoadDriverPrivilege. An example use case is MSI files running in a client/server mode where **SeDebugPrivilege** is required to interact with the server component which runs as SYSTEM. This only applies to cases where the standard user needs to run the MSI directly.

  - **Add Basic Admin Rights**: Permits elevation of most applications and tasks. We recommend using this token as the default elevation token. This access token is essentially full admin but excludes the following privileges: **SeDebugPrivilege** and **SeLoadDriverPrivilege**. If users need to debug applications or access drivers, then use the full admin token.
  - **Privilege Management Support Token**: Applies Add Full Admin privileges with tamper protection removed.

- **Raise An Event**: **Off**, **On**, **Anonymous**. Select if an event is raised if this Application Rule is triggered. When on, an event is sent to the local event log file. Anonymous removes user and host name from events so the user / host are not identifiable.
- **Run an Audit Script**: Select an audit script from the list.
- **Privilege Monitoring**: **Off**, **On**, **Anonymous**. Select **On** to raise a privileged monitoring event.
- **Reporting Events**: On by default, click to turn off. When the setting is on, events are raised for viewing in EPM Reporting.

Create TAP Rules

Use Trusted Application Protection (TAP) rules to dynamically evaluate DLLs for trusted applications for each Workstyle.

Unless a DLL has a trusted publisher and a trusted owner, it is not allowed to run within the TAP application.

- **Trusted Publisher:** A trusted publisher must be signed. In addition, the publisher certificate must be valid, in date, and not revoked.
- **Trusted Owner:** A trusted owner is any owner that is in the default Windows groups **Administrators**, **SystemUser** or **TrustedInstaller**.

TAP rules affect the following applications:

- Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Publisher, Adobe Reader 11 and earlier, Adobe Reader DC, Microsoft Outlook, Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Microsoft Edge

You can turn on monitoring for TAP applications in any Workstyle.

To create a TAP rule:

1. Expand **Workstyles**, and then expand a Workstyle.
2. Select **Trusted Application Protection**.
3. In the **Rule** section, set the following:
    - **Trusted Application Protection:** From the list select **Enabled**, **Disabled**, or **Not Configured**. The first Workstyle evaluated that has TAP set to **Enabled** or **Disabled** is matched by Endpoint Privilege Management for Windows, meaning subsequent Workstyles are not evaluated by Endpoint Privilege Management for Windows.
    - **Action:** Select from **Passive (No Change)** or **Block**. The selected action is applied when the DLL in the TAP application tries to run.
    - **End User Message:** Select if a message is displayed to the user when the DLL tries to run (regardless of if it is allowed to run). We recommend using messages if you are blocking a DLL from running, so the end user has some feedback.
4. In the **Auditing** section, select **On** or **Anonymous**. This setting determines if an event is raised when the TAP application tries to run a DLL. When auditing is on, the event is sent to the local event log file. Anonymous removes user and host name from events so the user and host details are not identifiable.
5. In the **Reporting Options** sections, select **Reporting Events** to capture events.
6. Click the **Configure Exclusions** link to add DLLs to exclude from the TAP applications rule. These are DLLs that have either an untrusted owner or an untrusted publisher, but you still want to be allowed to run with TAP enabled in the Workstyle. This list of DLLs is not validated. If the DLL name listed is not matched by the client, then nothing is excluded.

Set General Rules

To view or edit the general rules of a Workstyle, select **Windows > Workstyles > 'Workstyle Name' > General Rules**.

The general rules include the following:

- **Collect User Information:** When enabled, raises an audit event each time a user logs on to the client machine.
- **Collect Host Information:** When enabled, raises an audit event on computer start-up or when the Endpoint Privilege Management for Windows service is started.
- **Prohibit Privileged Account Management:** When enabled, blocks users from modifying local privileged group memberships. This prevents real administrators, or applications which have been granted administrative rights through Endpoint Privilege Management for Windows, from adding, removing, or modifying a privileged account.

  The local privileged groups that cannot be changed when this rule is enabled:

  - Built-in administrators
  - Power users
  - Account operators
  - Server operators
  - Printer operators
  - Backup operators
  - RAS servers group
  - Network configuration operators
- **Enable Windows Remote Management Connections:** When enabled, authorizes standard users who match the Workstyle to connect to a computer remotely using WinRM, which would normally require local administrator rights. This general rule supports remote PowerShell command management and must be enabled to allow a standard user to execute PowerShell scripts or commands.

To allow remote network connections, you may be required to enable the Windows Group Policy setting to access this computer from the network.

Enable Microsoft Block Rules

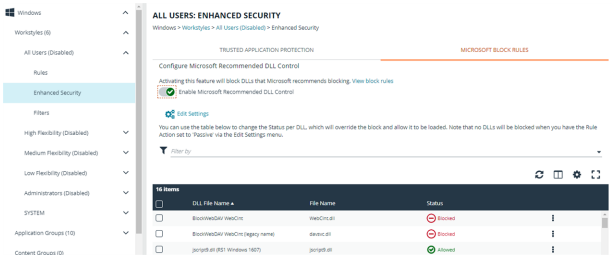
A number of the DLLs from Microsoft's Recommended Blocklist can easily be blocked to prevent potential attacks from threat actors.

1. Go to the **Security Enhancements** tab for the workstyle where you want to enable DLL control.
2. Click the toggle to turn on blocking.

While Microsoft recommends blocking these DLLs, there are legitimate use cases. If required, you can change the setting to allow loading.

1. Select the DLL to unblock, and then click **Allow Loading**.
2. To reverse the action and block the DLL, select the DLL and click **Block Loading**.

   Some of the DLLs are allowed by default. See the next section to see why and if you need to adjust any options.



Windows Version Specific DLLs

A number of the recommended DLLs to block are specific to certain versions on certain Windows 10 versions. For example, it is advised to block the DLLs if you are running Windows 10 1607 or Windows 10 1809. These are identified in the list with the either **RS1 Windows 1607** or **RS5 Windows 1809** labels.

Additionally, Windows creates some cached versions of DLLs that have different names and properties. Ensure DLLs with a *Native Image* version are set to blocked, when required. You can identify these in the list with the **Native image** label.

> *For more information, see Microsoft recommended block rules at https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules.*

Add filters

Use filtering to narrow the scope of when a Workstyle is applied. Workstyle filters apply to Windows and macOS systems.

By default, a Workstyle applies to all users and computers who receive it. However, you can add one or more filters that restrict the application of the Workstyle:

- **Account Filter:** Restrict the Workstyle to specific users or groups of users.
- **Computer Filter:** Restrict the Workstyle to specific computers (names or IP addresses), or Remote Desktop clients.
- **WMI (Windows Management information) Filter:** Restrict the Workstyle based on the success or failure of a WMI query.

The following conditions can be applied to a filter:

- **ALL filters must match:** The Workstyle is applied only if all filters match.
- **ANY filter can match:** The Workstyle is applied when any filter matches.

Account filters

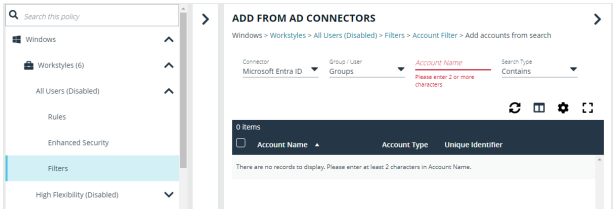
An account filter restricts a Workstyle to specific users or groups of users. Account filters can be created for Windows and macOS Workstyles.

There are two ways to add groups:

- Add local Active Directory domain groups and users
- Set up a connector that populates group information from your local Active Directory domains or your Microsoft Entra ID instance.

To create an account filter:

1. Expand a Workstyle, and then select **Filters**.
2. Select the **Account Filters** tab, and then select **Create New Account Filter**.
3. Select the new filter in the list, and then select **Go To** from the menu.
4. Select one of the following:
    - **Add Account** (Windows): Add an account name and SID details. Click **Add Account**.
    - **Add Account from Search** (Windows): Select a connector from the list. Go to step 5.
    - **Add Account:** (macOS). Add the account or group details. User IDs on macOS must be values greater than 500. A value less than that might be used by a system process.
5. If you select **Add Account from Search**, select a connector on the **Add From AD Connectors** page. The default connector is **Built-In**. Enter search criteria in the **Account Name** box to find a specific account. If searching Microsoft Entra ID, a minimum of two characters is required to initiate the search. Use the search options, **Contains** or **Starts with** to narrow the scope of the search results.
6. Select the account name, and then select **Add**.



Computer filters

A computer filter can be used to target specific computers and remote desktop clients. You can add a computer using either its host or DNS name, or by an IP address.

Computer filters can be configured on Windows and macOS computers.

To restrict the Workstyle to specific computers by IP address:

1. Expand a Workstyle, and then select **Filters**.
2. Click **Create New Filter**, and then select **Computer Filter**.
3. Enter the IP address manually, in the format **123.123.123.123**. Optionally, use asterisk wildcard (*) and - for range, as shown: **127.*.0.0-99**.
4. (Windows only) Select **Match the remote desktop (instead of the local computer)** if the computer filter is intended to match the IP address of remote computers using remote desktop sessions.
5. Click **Add**.

To restrict the Workstyle to specific computers by host name:

1. Expand a Workstyle, and then select **Filters**.
2. Click **Create New Filter**, and then select **Computer Filter**.
3. Enter one or more host names, separated by semicolons. You can use the ***** and **?** wildcard characters in host names.
4. (Windows only) Select **Match the remote desktop (instead of the local computer)** if the computer filter is intended to match the IP address of remote computers using remote desktop sessions.
5. Click **Add**.

WMI filters

A WMI filter is applied to a Workstyle based on the outcome of a WMI query.

When a WMI query runs, the client checks whether any rows of data are returned. If any data is returned, then the WMI query is successful. If no data is returned or an error is detected, the WMI query is unsuccessful.

WMI queries are always run as the Windows SYSTEM account, and cannot be executed against remote computers or network resources. WMI filters do not support impersonation levels, and can only be used with **SELECT** queries.

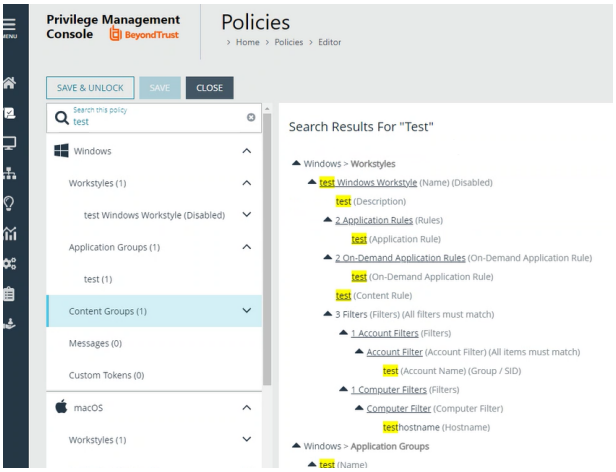
To create a WMI filter:

1. Expand a Workstyle, and then select **Filters**.
2. Click **Create New Filter**, and then select **WMI Filter**.
3. Click the **WMI Filter** link in the list. Alternatively, select **Go To** from the menu for that filter.
4. Click **Create New Query**.
5. Enter the following details:
    - **Description**: Free text to describe the WMI query.
    - **Namespace**: Set the namespace that the query runs against. By default, this is **root\CIMV2**.
    - **Query**: The WMI Query Language (WQL) statement to execute.
    - **Timeout**: The time (in seconds) the client waits for a response before terminating the query. By default, no timeout is set. Long running WMI queries result in delayed application launches. Therefore, we recommend setting a timeout to ensure that queries are terminated in a timely manner.
6. Click **Add Query**.

For more information, see WMI (Windows Management information) Filters at https://www.beyondtrust.com/docs/privilege-management/windows/admin/windows-policies/workstyles/filters/wmi-filters.htm.

Search a policy

The search feature facilitates ease-of-use searching when trying to find specific details about policy configuration.



- Finds all search results for workstyles in the policy.
- Displays the exact location in the policy.
- Provides linked text to go to that area of the policy and edit the policy, if necessary.

  If you are viewing the policy in *read-only* mode, you can click the link to drill down, but you cannot edit the policy setting.

- Searches on Windows and macOS policies, and includes:
  - Application Groups
  - Applications (including application matchers)
  - Application Rules
  - On-Demand Rules
  - Account Filters
  - Computer Filters
- Saves the 5 most recent searches.
- Displays up to a maximum of 500 matches to ensure optimal performance.

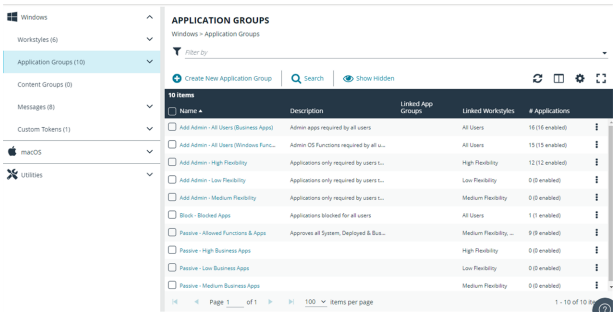
Application Groups

Application Groups are used to define logical groupings of applications.

Application Groups are assigned to Workstyles, so you must define Application Groups for all the applications you want to assign to a Workstyle.

Overview

When working with Application Groups, you can:



- Create, edit, and delete application groups.
- Change the name or description of the group.
- Delete an application group when it is no longer required.
- Copy an application group, and then edit the properties of the newly created group.
- Copy application definitions from one group to another and from one policy to another.
- View hidden application groups.
- Use the search feature to find an application.

Add an Application to an Application Group

There are three ways to add an application to a group:

- Application definitions: Create an application using the application definitions and properties.
- Reports: Add an application on-the-fly from the **Analytics** page using the collected analytics.
- Application templates: Provides a way to pick from a list of known applications.

Environment Variables

You can use the following environment variables in file path and command line application definitions.

To use the variables, enter the variable, including the % characters, into a file path or command line. EPM expands the environment variable prior to attempting a file path or command line match.

System Variables

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES(x86)%
- %COMMONPROGRAMFILES%
- %PROGRAMDATA%
- %PROGRAMFILES(x86)%
- %PROGRAMFILES%

- %SYSTEMROOT%
- %SYSTEMDRIVE%

User Variables

- %APPDATA%
- %USERPROFILE%
- %HOMEPATH%
- %HOMESHARE%
- %LOCALAPPDATA%
- %LOGONSERVER%

Application Definitions

The Policy Editor must match every enabled criterion in an application definition before it will trigger a match (the rules are combined with a logical AND).

Application definitions that require a match can also be negated. To target applications that do not match the definition, select does NOT match.

Name	Description
ActiveX Codebase	When inserting ActiveX controls, this is enabled by default, and we recommend you use this option in most circumstances. You must enter the URL to the codebase for the ActiveX control. You can choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions** Although you can enter a relative codebase name, we strongly recommend you enter the full URL to the codebase, as it is more secure.
ActiveX Version	If the ActiveX control you entered has a version property, then you can choose **Check Min Version** and/or **Check Max Version** and edit the respective version number fields.
App ID	Matches on the App ID of the COM class, which is a GUID used by Windows to set properties for a CLSID. AppIds can be used by 1 or more CLSIDs. The available operators are identical to the File or Folder Name definition.
Application Requires Elevation (UAC)	Checks if an executable requires elevated rights to run and causes UAC (User Account Control) to trigger. This is a useful way to replace inappropriate UAC prompts with EPM end user messages to either block or prompt the user for elevation. ***Note:*** *This is supported on install only.*

Name	Description
BeyondTrust Zone Identifier	Matches on the BeyondTrust Zone Identifier tag, where present. If an Alternate Data Stream (ADS) tag is applied by the browser, then also applies a BeyondTrust Zone Identifier tag to the file. The BeyondTrust Zone Identifier tag can be used as matching criteria if required.
CLSID	Matches the class ID of the ActiveX control or COM class, which is a unique GUID stored in the registry.
COM Display Name	If the class you entered has a Display Name, then it will automatically be extracted, and you can choose to match on this property. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a regular expression. The available operators are identical to File or Folder Name definition.
Command Line	If the filename is not specific enough, you can match the command line, by checking this option and entering the command line to match. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a regular expression. The available operators are identical to File or Folder Name definition. PowerShell removes double quotes from command strings prior to transmitting to the target. Therefore, we do not recommend that Command Line definitions include double quotes, as they will fail to match the command.
Controlling Process	Target content based on the process (application) that will be used to open the content file. The application must be added to an Application Group. You can also define whether any parent of the application will match the definition.

Drive	This option can be used to check the type of disk drive where the file is located. Choose from one of the following options:
	
	• **Fixed disk:** Any drive that is identified as being an internal hard disk.
	• **Network:** Any drive that is identified as a network share.
	• **RAM disk:** Any drive that is identified as a RAM drive.
	• **Any Removable Drive or Media:** If you want to target any removable drive or media, but are unsure of the specific drive type, choose this option which will match any of the removable media types below. Alternatively, if you want to target a specific type, choose from one of the following removable media types:
	  ◦ **Removable Media:** Any drive that is identified as removable media.
	  ◦ **USB:** Any drive that is identified as a disk connected by USB.
	  ◦ **CD/DVD:** Any drive that is identified as a CD or DVD drive.
	  ◦ **eSATA Drive:** Any drive that is identified as a disk connected by eSATA.

File or Folder Name	Applications are validated by matching the file or folder name. You can choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions**

Name	Description
	For more information, see "Regular Expression Syntax" on page 109. Although you can enter relative file names, we strongly recommend you enter the full path to a file or the COM server. Environment variables are also supported. We do not recommend you use the definition File or Folder Name **does NOT Match** in isolation for executable types, as it will result in matching every application, including hosted types, such as installer packages, scripts, batch files, registry files, management consoles, and Control Panel applets. When creating blocking rules for applications or content, and the **File or Folder Name** is used as matching criteria against paths which exist on network shares, this should be done using the UNC network path and not by the mapped drive letter.
File Hash (SHA-1 Fingerprint)	If a reference file was entered, then a SHA-1 hash of the PowerShell script is generated. This definition ensures the contents or the script file (which can normally be edited by any user) remain unchanged, as changing a single character in the script will cause the SHA-1 hash to change. While SHA-1 is supported, SHA-256 is recommended.
File Hash (SHA-256)	Set the SHA-256 file hash on an application. The SHA-256 hash is supported on all appropriate applications, both Windows and macOS operating systems. On the Windows operating system, you can select either **match** or **does NOT match**. The **does NOT match** setting is not available on macOS. We recommend using SHA-256 rather than SHA-1.
File Version	If the file, service executable, or COM server you entered has a File Version property, then it will automatically be extracted and you can choose Check Min Version and/or Check Max Version, and then edit the respective version number fields.
Parent Process	This option can be used to check if an application's parent process matches a specific Application Group. You must create an Application Group for this purpose or specify an existing Application Group in the Parent Process group. Setting match all parents in tree to True will traverse the complete parent/child hierarchy for the application, looking for any matching parent process, whereas setting this option to False will only check the application's direct parent process.
Product Code	If the file you entered has a Product Code, then it will automatically be extracted, and you can choose to check this code.
Product Description	If the file you entered has a Product Description property, then it will automatically be extracted, and you can choose to match on this property. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (? and *) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Product Name	If the file, COM server, or service executable you entered has a Product Name property, then it will automatically be extracted and you can choose to match on this property. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (? and *) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Product Version	If the file, COM server, or service executable you entered has a Product Version property, then it will automatically be extracted and you can choose Check Min Version and/or Check Max Version and

Name	Description
	edit the respective version number fields.
Publisher	Checks for the existence of a valid publisher. If you browsed for an application, then the certificate subject name will automatically be retrieved, if the application is signed. For Windows system files, the Windows security catalog is searched, and if a match is found, the certificate for the security catalog is retrieved. Publisher checks are supported on Executables, Control Panel Applets, Installer Packages, Windows Scripts, and PowerShell Scripts. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Service Actions	Define the actions which are allowed. Choose from: • **Service Stop:** Grants permission to stop the service. • **Service Start:** Grants permission to start the service. • **Service Pause / Resume:** Grants permission to pause and resume the service. • **Service Configure:** Grants permission to edit the properties of the service.
Service Display Name	Matches on the name of the Windows service, for example, **W32Time**. You may choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions**
Service Name matches	Matches on the name of the Windows service, for example, **W32Time**. You may choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions**
Source URL	Use to check where the application or installer was originally downloaded from if the application was downloaded using a web browser. The application is tracked by Endpoint Privilege Management at the point it is downloaded, so that if a user decided to run the application or installer at a later date, the source URL can still be verified. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Trusted Ownership	Use to check if an application's file is owned by a trusted owner (the trusted owner accounts are SYSTEM, Administrators, or Trusted Installer).
Upgrade Code	If the file you entered has an **Upgrade Code**, then it will automatically be extracted and you can

Name	Description
	choose to check this code.
Windows Store Application Version	Matches on the version of the Windows Store application, for example, **16.4.4204.712**. You can choose **Check Min Version** and/or **Check Max Version** and edit the respective version number fields.
Windows Store Package Name	Matches on the name of the Windows Store Application, for example, **microsoft.microsoftskydrive**. You can choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions**
Windows Store Publisher	Matches on the publisher name of the Windows Store Application, for example, **Microsoft Corporation**. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a Regular Expression. The other available operators are: • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions** The **Browse File** and **Browse Apps** options can only be used if configuring EPM settings from a Windows 8 client.

Application Details

This section provides details about the properties that can be configured on the application.

In some cases, additional information to configure the application is provided.

ActiveX Controls

Unlike other application types, Endpoint Privilege Management for Windows only manages the privileges for the installation of ActiveX controls. ActiveX controls usually require administrative rights to install, but once installed, run with the standard privileges of the web browser.

Matching criteria:

- ActiveX Codebase matches
- CLSID matches
- ActiveX Version matches

Batch Files

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

COM Classes

A COM elevation is an elevation typically initiated from Explorer, when an integrated task requires administrator rights. Explorer uses COM to launch the task with admin rights, without having to elevate Explorer. Every COM class has a unique identifier, called a CLSID, that is used to launch the task.

COM tasks usually trigger a Windows UAC prompt because they need administrative privileges to proceed. EPM allows you to target specific COM CLSIDs and assign privileges to the task without granting full administration rights to the user. COM based UAC prompts can also be targeted and replaced with custom messaging, where COM classes can be allowlisted and/or audited.

COM classes are hosted by a COM server DLL or EXE, so COM classes can be validated from properties of the hosting COM server. You can configure:

Matching criteria:

- File or Folder Name matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Product Name matches
- Publisher matches
- CLSID matches
- App ID matches
- COM Display Name matches
- Product Description matches
- Product Version matches
- File Version matches
- Trusted Ownership matches
- Application Requires Elevation (UAC): Match if **Application Requires Elevation (User Account Control)** is always enabled, as COM classes require UAC to elevate
- Source URL matches

Control Panel Applet

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Product Name matches
- Publisher matches
- Product Description matches
- Product Version matches
- File Version matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Executables

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Product Name matches
- Publisher matches
- Product Description matches
- Product Version matches
- File Version matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Installer Package

EPM allows standard users to install and uninstall Windows Installer packages that normally require local admin rights. The following package types are supported:

- Microsoft Software Installers (MSI)
- Microsoft Software Updates (MSU)
- Microsoft Software Patches (MSP)

When a Windows Installer package is added to an Application Group, and assigned to an Application Rule or On-Demand Application Rule, the action will be applied to both the installation of the file, and also uninstallation when using **Add/Remove Programs** or **Programs and Features**.

> ***Note:*** *The publisher property of an MSx file may sometimes differ to the publisher property once installed in* ***Programs and Features****. We therefore recommend applications targeted using the* ***Match Publisher*** *validation rule are tested for both installation and uninstallation, prior to deployment, using the EPM Activity Viewer.*

Installer packages typically create child processes as part of the overall installation process. Therefore, we recommend when elevating MSI, MSU, or MSP packages, that the advanced option **Allow child processes will match this application definition** is enabled.

> ***Note:*** *If you want to apply more granular control over installer packages and their child processes, use the* ***Child Process*** *validation rule to allowlist or blocklist those processes that will or will not inherit privileges from the parent software installation.*

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Product Name matches
- Publisher matches
- Product Version matches
- Product Code matches
- Upgrade Code matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Insert Endpoint Privilege Management Policy Editor Snap-ins

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Publisher matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Management Console

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Publisher matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

PowerShell Scripts

Endpoint Privilege Management for Windows allows you to target specific PowerShell scripts and assign privileges to the script without granting local administration rights to the user. Scripts can also be blocked if they are not authorized or allowlisted.

Note: *PowerShell scripts that contain only a single line are interpreted and matched as a PowerShell command, and will not match a PowerShell script definition. We recommend PowerShell scripts contain at least two lines of commands to ensure they are correctly matched as a PowerShell script. This cannot be achieved by adding a comment to the script.*

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches

- File Hash (SHA-256) matches
- Publisher matches
- Trusted Ownership matches
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Example PowerShell Configurations

Create New Configuration, Save to Local File

```
# Import both Defendpoint cmdlet module
Import-Module 'C:\Program Files\Avecto\Privilege Guard
Client\PowerShell\Avecto.Defendpoint.Cmdlets\Avecto.Defendpoint.Cmdlets.dll'
# Create a new variable containing a new Defendpoint Configuration Object
$PGConfig = New-Object Avecto.Defendpoint.Settings.Configuration


## Add License ##
# Create a new license object
$PGLicence = New-Object Avecto.Defendpoint.Settings.License
# Define license value
$PGLicence.Code = "5461E0D0-DE30-F282-7D67-A7C6-B011-2200"
# Add the License object to the local PG Config file
$PGConfig.Licenses.Add($PGLicence)

## Add Application Group ##
# Create an Application Group object
$AppGroup = new-object Avecto.Defendpoint.Settings.ApplicationGroup
# Define the value of the Application Group name
$AppGroup.name = "New App Group"
# Add the Application Group object to the local PG Config file
$PGConfig.ApplicationGroups.Add($AppGroup)

## Add Application ##
# Create an application object
$PGApplication = new-object Avecto.Defendpoint.Settings.Application $PGConfig
# Use the Get-DefendpointFileInformation to target Windows Calculator
$PGApplication = Get-DefendpointFileInformation -Path C:\windows\system32\calc.exe
# Add the application to the Application group
$PGConfig.ApplicationGroups[0].Applications.AddRange($PGApplication)

## Add Message ##
# Create a new message object
$PGMessage = New-Object Avecto.Defendpoint.Settings.message $PGConfig
#Define the message Name, Description and OK action and the type of message
$PGMessage.Name = "Elevation Prompt"
$PGMessage.Description = "An elevation message"
$PGMessage.OKAction = [Avecto.Defendpoint.Settings.Message+ActionType]::Proceed
$PGMessage.Notification = 0
# Define whether the message is displayed on a secure desktop
```

```
$PGMessage.ShowOnIsolatedDesktop = 1
# Define How the message contains
$PGMessage.HeaderType = [Avecto.Defendpoint.Settings.message+MsgHeaderType]::Default
$PGMessage.HideHeaderMessage = 0
$PGMessage.ShowLineOne = 1
$PGMessage.ShowLineTwo = 1
$PGMessage.ShowLineThree = 1
$PGMessage.ShowReferLink = 0
$PGMessage.ShowCancel = 1
$PGMessage.ShowCRInfoTip = 0
# Define whether a reason settings
$PGMessage.Reason = [Avecto.Defendpoint.Settings.message+ReasonType]::None
$PGMessage.CacheUserReasons = 0
# Define authorization settings
$PGMessage.PasswordCheck =
Avecto.Defendpoint.Settings.message+AuthenticationPolicy]::None
$PGMessage.AuthenticationType = [Avecto.Defendpoint.Settings.message+MsgAuthenticationType]::Any
$PGMessage.RunAsAuthUser = 0
# Define Message strings
$PGMessage.MessageStrings.Caption = "This is an elevation message"
$PGMessage.MessageStrings.Header = "This is an elevation message header"
$PGMessage.MessageStrings.Body = "This is an elevation message body"
$PGMessage.MessageStrings.ReferURL = "http:\\www.bbc.co.uk"
$PGMessage.MessageStrings.ReferText = "This is an elevation message refer"
$PGMessage.MessageStrings.ProgramName = "This is a test Program Name"
$PGMessage.MessageStrings.ProgramPublisher = "This is a test Program Publisher"
$PGMessage.MessageStrings.PublisherUnknown = "This is a test Publisher Unknown"
$PGMessage.MessageStrings.ProgramPath = "This is a test Path"
$PGMessage.MessageStrings.ProgramPublisherNotVerifiedAppend = "This is a test verification
failure"
$PGMessage.MessageStrings.RequestReason = "This is a test Request Reason"
$PGMessage.MessageStrings.ReasonError = "This is a test Reason Error"
$PGMessage.MessageStrings.Username = "This is a test Username"
$PGMessage.MessageStrings.Password = "This is a test Password"
$PGMessage.MessageStrings.Domain = "This is a test Domain"
$PGMessage.MessageStrings.InvalidCredentials = "This is a test Invalid Creds"
$PGMessage.MessageStrings.OKButton = "OK"
$PGMessage.MessageStrings.CancelButton = "Cancel"
# Add the PG Message to the PG Configuration
$PGConfig.Messages.Add($PGMessage)

## Add custom Token ##
# Create a new custom Token object
$PGToken = New-Object Avecto.Defendpoint.Settings.Token
# Define the Custom Token settings
$PGToken.Name = "Custom Token 1"
$PGToken.Description = "Custom Token 1"
$PGToken.ClearInheritedPrivileges = 0
$PGToken.SetAdminOwner = 1
$PGToken.EnableAntiTamper = 0
$PGToken.IntegrityLevel = Avecto.Defendpoint.Settings.Token+IntegrityLevelType]::High
# Add the Custom Token to the PG Configuration
$PGConfig.Tokens.Add($PGToken)

## Add Policy ##
```

```
# Create new policy object
$PGPolicy = new-object Avecto.Defendpoint.Settings.Policy $PGConfig
# Define policy details
$PGPolicy.Disabled = 0
$PGPolicy.Name = "Policy 1"
$PGPolicy.Description = "Policy 1"
# Add the policy to the PG Configurations
$PGConfig.Policies.Add($PGPolicy)

## Add Policy Rule ##
# Create a new policy rule
$PGPolicyRule = New-Object Avecto.Defendpoint.Settings.ApplicationAssignment PGConfig
# Define the Application rule settings
$PGPolicyRule.ApplicationGroup = $PGConfig.ApplicationGroups[0]
$PGPolicyRule.BlockExecution = 0
$PGPolicyRule.ShowMessage = 1
$PGPolicyRule.Message = $PGConfig.Messages[0]
$PGPolicyRule.TokenType = [Avecto.Defendpoint.Settings.Assignment+TokenTypeType]::AddAdmin
$PGPolicyRule.Audit = [Avecto.Defendpoint.Settings.Assignment+AuditType]::On
$PGPolicyRule.PrivilegeMonitoring = [Avecto.Defendpoint.Settings.Assignment+AuditType]::Off
$PGPolicyRule.ForwardEPO = 0
$PGConfig.Policies[0].ApplicationAssignments.Add($PGPolicyRule)

## Set the Defendpoint configuration to a local file and prompt for user confirmation ##
Set-DefendpointSettings -SettingsObject $PGConfig -Localfile -Confirm
```

Open Local User Policy, Modify then Save

```
# Import the Defendpoint cmdlet module
Import-Module 'C:\Program Files\Avecto\Privilege Guard
Client\PowerShell\Avecto.Defendpoint.Cmdlets\Avecto.Defendpoint.Cmdlets.dll'
# Get the local file policy Defendpoint Settings
$PGConfig = Get-DefendpointSettings -LocalFile
# Disable a policy
$PGPolicy = $PGConfig.Policies[0]
$PGPolicy.Disabled = 1
$PGConfig.Policies[0] = $PGPolicy
# Remove the PG License
$TargetLicense = $PGConfig.Licenses[0]
$PGConfig.Licenses.Remove($TargetLicense)
# Update an existing application definition to match on Filehash
$UpdateApp = $PGConfig.ApplicationGroups[0].Applications[0]
$UpdateApp.CheckFileHash = 1
$PGConfig.ApplicationGroups[0].Applications[0] = $UpdateApp
# Set the Defendpoint configuration to the local file policy and prompt for user confirmation
Set-DefendpointSettings -SettingsObject $PGConfig -LocalFile -Confirm
```

Open Local Configuration and Save to Domain GPO

```
# Import the Defendpoint cmdlet module
Import-Module 'C:\Program Files\Avecto\Privilege Guard
```

```
Client\PowerShell\Avecto.Defendpoint.Cmdlets\Avecto.Defendpoint.Cmdlets.dll'
# get the local Defendpoint configuration and set this to the domain computer policy, ensuring
the user is prompted to confirm the change
Get-DefendpointSettings -LocalFile | Set-DefendpointSettings -Domain -LDAP "LDAP://My.Domain/CN=
{GUID},CN=Policies,CN=System,DC=My,DC=domain" -Confirm
```

Registry Settings

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Remote PowerShell Commands

EPM provides an additional level of granularity for management of remote PowerShell cmdlets to ensure you can execute these commands without local administrator privileges on the target computer.

```
Get-service -Name *time* | restart-Service -PassThru
```

EPM allows you to target specific command strings and assign privileges to the command without granting local admin rights to the user. Commands can also be blocked if they are not authorized or allowlisted. All remote PowerShell commands are fully audited for visibility.

To allow standard users to connect to a remote computer with Windows Remote Management, or WinRM (a privilege normally reserved for local administrator accounts), it is necessary to enable the General rule **Enable Windows Remote Management Connections**. This rule grants standard users, who match the Workstyle, the ability to connect using WinRM, and can be targeted to specific users, groups of users, or computers using Workstyle filters.

1. Select the Application Group you want to add the application to.
2. Right-click and select **Insert Application > Remote PowerShell Command**.
3. You can leave the **Select reference script file** blank to match on all applications of this files, type in a specific name or path manually, or click **Browse Cmdlets**. This lists the PowerShell cmdlets for the version of PowerShell that you installed. If the cmdlet you want to use is not listed because the target version of PowerShell is different, you can manually enter it.
4. Enter a description, if required. By default, this is the name of the application you are inserting.
5. You need to configure the matching criteria for the PowerShell command. You can configure:
    - Command Line matches: PowerShell removes double quotes from the Command Line before it is sent to the target. **Command Line** definitions that include double quotes are not matched by EPM for remote PowerShell commands.
6. Click **OK**. The application is added to the Application Group.

For more information, see:

- *"Application Definitions" on page 50 for more about command line matching.*
- *To manage remote PowerShell scripts instead of a single cmdlet, see "Insert Remote PowerShell Scripts" on page 63.*

Messaging

EPM end user messaging includes limited support for remote PowerShell sessions; block messages can be assigned to Workstyle rules, which block remote PowerShell scripts and commands. If a block message is assigned to a Workstyle, which blocks a script or command, then the body message text of an assigned message will be displayed in the remote console session as an error.

Insert Remote PowerShell Scripts

In a remote PowerShell session, a script (.PS1) can be executed from a remote computer against a target computer. Normally this requires local administrator privileges on the target computer, with little control over the scripts that are executed, or the actions that the script performs. For example:

```
Invoke-Command -ComputerName RemoteServer -FilePath c:\script.ps1 -Credential xxx
```

You can target specific PowerShell scripts remotely and assign privileges to the script without granting local administration rights to the user. Scripts can also be blocked if they are not authorized or allowlisted. All remote PowerShell scripts executed are fully audited for visibility.

***Note:** You must use the **Invoke-Command** cmdlet to run remote PowerShell scripts. EPM cannot target PowerShell scripts that are executed from a remote PowerShell session. Remote PowerShell scripts must be matched by either a SHA-1 File Hash or a Publisher (if the script has been digitally signed).*

You can elevate individual PowerShell scripts and commands which are executed from a remote machine. This eliminates the need for users to be logged on with an account which has local admin rights on the target computer. Instead, elevated privileges are assigned to specific commands and scripts which are defined in Application Groups, and applied by a Workstyle.

PowerShell scripts and commands can be allowlisted to block the use of unauthorized scripts, commands, and cmdlets. Granular auditing of all remote PowerShell activity provides an accurate audit trail of remote activity.

PowerShell definitions for scripts and commands are treated as separate application types, which allows you to differentiate between predefined scripts authorized by IT, and session-based ad hoc commands.

To allow standard users to connect to a remote computer with Windows Remote Management, or WinRM (a privilege normally reserved for local administrator accounts), it is necessary to enable the General rule **Enable Windows Remote Management Connections**. This rule grants standard users who match the EPM Workstyle the ability to connect using WinRM, and can be targeted to specific users, groups of users, or computers using Workstyle filters.

Matching criteria:

- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Publisher matches

You can leave the **Select reference script file** blank to match on all applications of this files, type in a specific name or path manually, or click **Browse File**.

> ***Note:*** *Remote PowerShell scripts that contain only a single line will be interpreted and matched as a Remote PowerShell Command, and will fail to match a PowerShell script definition. We therefore recommend PowerShell scripts contain at least two lines of commands to ensure they are correctly matched as a script. This cannot be achieved by adding a comment to the script.*

Messaging

End user messaging includes limited support for remote PowerShell sessions; block messages can be assigned to Workstyle rules which block remote PowerShell scripts and commands. If a block message is assigned to a Workstyle which blocks a script or command, then the body message text of an assigned message will be displayed in the remote console session as an error.

Uninstaller (MSI or EXE)

EPM allows standard users to uninstall Microsoft Software Installers (MSIs) and executables (EXEs) that would normally require local admin rights.

When the **Uninstaller** application type is added to an Application Group and assigned to an Application Rule in the policy, the end user can uninstall applications using **Programs and Features** or, in Windows 10, **Apps and Features**.

The **Uninstaller** application type allows you to uninstall an EXE or MSI when it is associated with an Application Rule. As the process of uninstalling a file requires admin rights, you need to ensure when you target the Application Group in the Application Rules you set the access token to **Add Full Admin**.

> ***Note:*** *The **Uninstaller** type must be associated with an Application Rule. It does not apply to On-Demand Application Rules.*

You cannot use the **Uninstaller** application type to uninstall the BeyondTrust or the BeyondTrustEPM Adapter using, irrespective of your user rights. The anti-tamper mechanism built into EPM prevents users from uninstalling EPM, and the uninstall will fail with an error message.

> ***Note:*** *If a user attempts to use EPM to modify the installation of EPM, for example, uninstall it, and they do not have an anti-tamper token applied, the default behavior for the user is used. For example, if Windows UAC is configured, the associated Windows prompt will be displayed.*

If you want to allow users to uninstall either BeyondTrust's or the BeyondTrustEPM Adapter, you can do this by either:

- Logging in as a full administrator
- Elevating the **Programs and Features** control panel (or other controlling application) using a **Custom** Access Token that has anti-tamper disabled.

Upgrade Considerations

Any pre 5.7 Uninstaller Application Groups which matched all uninstallations will be automatically upgraded when loaded by the Policy Editor to File or Folder Name matches *. These will be honored by Endpoint Privilege Management for Windows.

Pre 5.7 versions of Endpoint Privilege Management will no longer match the upgraded rules, the behavior will be that of the native operating system in these cases.

If you do not want the native operating system behavior for uninstallers; please ensure that your clients are upgraded to the latest version before you deploy any policy which contains upgraded Uninstaller rules.

1. Select the Application Group you want to add the uninstaller to.
2. Right-click and select **Insert Application** > **Uninstaller**.
3. Enter a description, if required. By default, this is the name of the application you are inserting.
4. Click **Browse File** to select an uninstaller file and populate the available matching criteria for the selected uninstaller file.
5. Configure the matching criteria for the executable. You can configure:
    - **File or Folder Name matches**
    - **Upgrade Code matches**
    - **Product Name matches**
    - **Publisher matches**

Windows Services

The Windows service type allows individual service operations to be allowlisted, so that standard users are able to start, stop, and configure services without the need to elevate tools such as the Service Control Manager.

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Product Name matches
- Publisher matches
- Product Description matches
- Product Version matches
- File Version matches
- Service Name matches
- Service Display Name matches
- Service Actions match

Windows Store Applications

The **Windows Store** application type allows the installation and execution of Windows Store applications on Windows 8 and later to be allowlisted, so that users are prevented from installing or using unknown or unauthorized applications within the Windows Store.

Note: *EPM can only be used to block Windows Store Applications. When you use EPM to block a Windows Store Application and assign an EPM block message to the Application Rule, the native Windows block message overrides the EPM block message, meaning it is not displayed. Event number 116 is still triggered if you have events set up in your Application Rule.*

Windows Scripts

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Publisher matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Create an Application Group

There are predefined application groups available that are already populated with applications and linked to workstyles. You can, however, create application groups and customize the application and associated properties.

1. On the **Policy Editor** page, expand **Windows** or **macOS**.
2. Click **Application Groups**.
3. Click **Create New Application Group**.
4. Add a name and description. Click **Create Application Group**.
5. The Application Group is now displayed in the navigation pane and the grid. You are now ready to add applications to the group.

Add Application Using App Definitions

When adding an application, you can configure the following properties:

- **Application Definitions:** The application definitions are the properties of an application that are used to detect the application in your environment. When the application matches on the configured criteria the rule triggers.
- **Advanced Options:** When adding the application, advanced settings on child processes and standard user rights enforcement can be configured.

When adding file or folder paths, you can use environment variables as part of the entry. Using environment variables is optional.

The procedure for adding an application is generally the same for every application. The matching criteria varies depending on the application.

To add an application:

1. In the navigation pane, select the Application Group.
2. Click **Create New Application**, and then select the application type.
3. Enter a description in the **Application Description** box. Any value can be added here up to a maximum limit of 1024 characters. The description is not used in rule matching.
4. From the list of application definitions, configure the matching criteria.
5. (Optional) Configure the **Advanced Options**:
    - Allow child processes will match this application definition
    - Force standard user rights on File Open/Save common dialogs
6. Click **OK**.

For more information, see the following:

- *"Application Definitions" on page 50*
- *"Use Advanced Options" on page 71*
- *"Add Application from Template" on page 69*

Add Application from Template

Application templates provide a way to pick from a list of known applications. A standard set of templates is provided that covers basic administrative tasks for all supported operating systems, common ActiveX controls, and software updates.

1. On the **Policy Editor** page, navigate to the policy to update.
2. Go to **Application Groups > Applications**, and then click **Add From Templates**.
3. Select an application template from the list, and then click **Add**. You can select more than one template at a time.

Add Application From Analytics

You can add an application to a policy based on events generated from a particular application type.

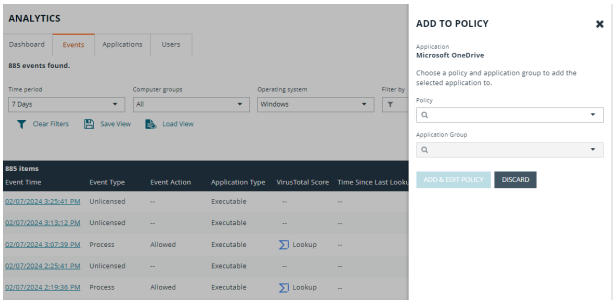
Supported event types include:

- Process
- Process with File
- COM Class
- Service
- ActiveX
- Challenge Response Failed

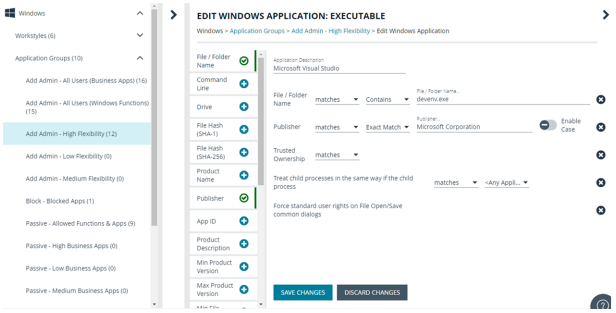
You can select more than one event in the list to add to the same policy. The matching criteria for all selected and compatible events are added to the policy and application group selected.

To add events to a policy:

1. In the console, select **Analytics** from the menu.
2. Click **Events**.
3. Select one or more events in the list and click the **Add to Policy** icon. A message displays if you try to add unsupported event types when selecting more than one event.
4. On the **Add Applications to Policy** page, select a policy and an application group.
5. Click **Add and Edit**. Alternatively, click **Add and Close** here which adds the application to the Application Group and redirects you back to the report.



6. The policy opens to the **Application Groups > Applications** page where you can edit the application settings. If you are adding one application, then you are directed to the application matching criteria page as shown.



Use Advanced Options

Allow child processes will match this application definition

If selected, then any child processes that are launched from this application (or its children) will also match this rule. The rules are still processed in order, so it is still possible for a child process to match a higher precedence rule (or Workstyle) first. Therefore, this option will prevent a child process from matching a lower precedence rule.

If an application is launched by an on-demand rule and this option is selected, then the children are processed against the on-demand rules, and not the Application Rules. If this option is not selected, then the children will be processed against the Application Rules in the normal way. You can further refine this option by restricting the child processes to a specific Application Group. The default is to match <**Any Application**>, which will match any child process.

Note: *If you want to exclude specific processes from matching this rule, then click* ***…match…*** *to toggle the rule to* ***…does not match…****.*

Note: *Child processes are evaluated in the context that the parent executed. For example, if the parent executed through on-demand shell elevation, then EPM will first attempt to match On-Demand Application Rules for any children of the executed application.*

Force standard user rights on File Open/Save common dialogs

If the application allows a user to open or save files using the common Windows open or save dialog box, then selecting this option ensures the user does not have admin privileges within these dialog boxes. These dialog boxes have Explorer-like features, and allow a user to rename, delete, or overwrite files. If an application is running with elevated rights and this option is disabled, the open/save dialog boxes will allow a user to replace protected system files.

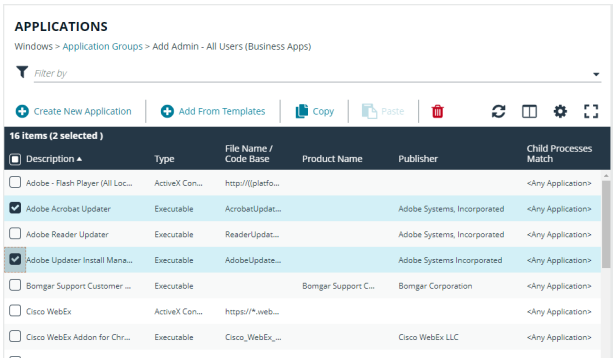
Where present, this option is selected by default to ensure EPM forces these dialog boxes to run with the user's standard rights, to prevent the user from tampering with protected system files.

When enabled, this option also prevents processes launched from within these dialog boxes from inheriting the rights of an elevated application.

Copy Application Definitions

For ease-of-use, copy one or more application definitions to save time when setting up an application group. Copy to another application group in the same policy or another policy.

If the **Paste** button is not available, check the XML is a valid application definition. Copy the XML to a text editor to confirm.



Disable an Application

You can temporarily pause the processing of an application rule against an application in an application group. Use this feature if you are rolling out or testing new rules. Disable the application while you investigate and fix any problems.

Content Groups

Build a Content Group using the definitions provided to control access to privileged content. Content Groups are added to a Content Rule in a Workstyle. When matches are detected on computers receiving the policy, the rule triggers and the rule behavior applies (allow or block rule).

There are two main use cases for applying content control:

- Allow modification: Allows standard users to modify privileged content, without having to assign admin rights to either the user, or the application used to modify the content.

  Add a Content Group to a content rule where the content can be assigned admin rights. When this is done, any user who receives the Workstyle can modify matching content without requiring an administrator account.

- Block access to content or directories.

  Add a Content Group to a content rule where the ability to open the content can be controlled with a Block action. When this is done, any user who can open and read the content is blocked from opening the content.

Content definitions

A Content Group is composed of one or more definitions. All definitions that make up a Content Group must match before the Content Rule triggers.

The following content definitions are available:

- File or Folder Name
- Drive
- Controlling Process

Review the next sections to learn more before building a Content Group.

File or Folder Name

Validate applications by matching the file or folder name. You can choose to match based on the following options (wildcard characters **?** and * may be used):

- **Exact Match**
- **Starts With**
- **Ends With**
- **Contains**
- **Regular Expressions**

Although you can enter relative filenames, we strongly recommend that you enter the full path to a file or the COM server. Environment variables are also supported.

We do not recommend using the **File or Folder Name does NOT Match** definition in isolation for executable types, as it results in matching every application, including hosted types such as Installer packages, scripts, batch files, registry files, management consoles, and Control Panel applets.

When creating blocking rules for applications or content, and using the **File or Folder Name** definition as matching criteria against paths which exist on network shares, use the Universal Naming Convention (UNC) network path rather than a mapped drive letter.

Drive

Verify the type of disk drive where the file is located. Choose from one of the following options:

- **Fixed disk:** Any drive that is identified as being an internal hard disk.
- **Network:** Any drive that is identified as a network share.
- **RAM disk:** Any drive that is identified as a RAM drive.
- **Any Removable Drive or Media:** If you want to target any removable drive or media, but are unsure of the specific drive type, this option will match any of the removable media types below. Alternatively, if you want to target a specific type, choose one of the following removable media types:
    - **Removable Media:** Any drive that is identified as removable media.
    - **USB:** Any drive that is identified as a disk connected via USB.
    - **CD/DVD:** Any drive that is identified as a CD or DVD drive.
    - **eSATA Drive:** Any drive that is identified as a disk connected via eSATA.

Controlling Process

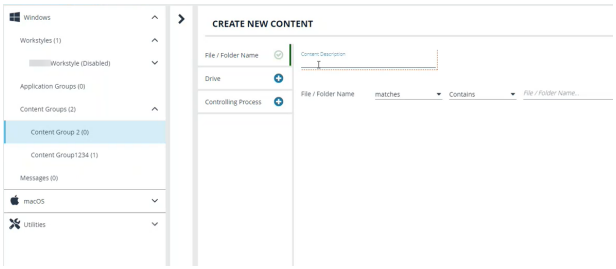
Use this definition to target content based on the process (application) used to open the content file. The application must have been added to an Application Group. You can also define whether any parent of the application matches the definition.

Create a Content Group

IMPORTANT!

We recommend adding a controlling process for each content definition. If a controlling process is not added to a content definition, then performance issues can occur on computers the policy is applied to.

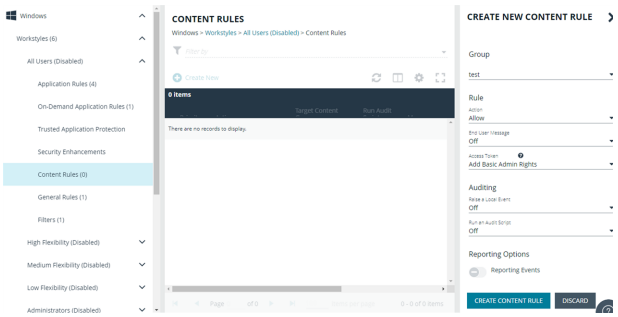
1. Expand the Windows panel of the Policy Editor.
2. Click **Content Groups**, and then click **Create New Content Group**.
3. Enter a name, and then click **Create Content Group**.
4. Select the saved content group, and then click **Create New Content**.
5. Configure the definitions.
6. Click **Create Content**.



After the content is added, add the Content Group to an existing Content Rule or create a new one.

Create a Content Rule

1. Expand a Workstyle, and then go to **Content Rules**.
2. Click **Create New**.
3. Select the rule properties:



   - **Group**: Select a Content Group.
   - **Action**: Select **Allow** or **Block**. The action that occurs if the content in the Content Group is accessed by the end user.
   - **End User Message**: Select a message from the list.
   - **Access Token**: Select the type of token to pass to the Content Group. You can select from:
     - **Passive** (no change): Doesn't make any change to the user's token. This is essentially an audit feature.
     - **Enforce User's Default Rights**: Removes all rights and uses the user's default token. Windows UAC always tries to add administration rights to the token being used so if the user clicked on an application that triggers UAC, the user cannot progress past the UAC prompt.
     - **Drop Admin Rights**: Removes administration rights from the user's token.
     - **Add Full Admin (Required for installers)**: Standard Windows Admin token containing all Admin privileges.
     - **Add Basic Admin Rights**: Gives greater control over the privileges granted when targeting rules at actions. This excludes the following privileges: **SeDebugPrivilege**, **SeLoadDriverPrivilege**.
     - **Privilege Management Support Token**: Applies Add Full Admin privileges with tamper protection removed.
     - **Keep Privileges - Enhanced**: Keeps the same privileges of the process token and adds some additional context to it. Use the token with features such as Advanced Parent Tracking or Anti-tamper.
   - **Raise a Local Event**: **Off**, **On**, **Anonymous**. Select if an event is raised if this Content Rule is triggered. When on, an event is sent to the local event log file. Anonymous removes user and host name from events so the user / host are not identifiable.
   - **Run an Audit Script**: Select an audit script from the list.
   - **Reporting Events**: When the setting is on, events are raised for viewing in EPM Analytics.
4. Click **Create Content Rule**.

Messages

You can define two types of end user messages:

- **Messages:** Messages take focus when they are displayed to the user.
- **Notifications:** (Windows only). Message notifications appear on the user's task bar. A notification is displayed as a toast notification.

Messages (and Notifications) are displayed when a user's action triggers a rule (application, on-demand or content rule). Rules can be triggered by an application *launch* or *block*, or when content is modified.

Messages provide an effective way of alerting the user before an action is performed, for example, before elevating an application or allowing content to be modified, or advising that an application launch or content modification is blocked.

Messages give the user information about the application or content, the action taken, and can be used to request information from the user.

Messages are assigned to Application Rules. A message displays different properties, depending on the targets it is assigned to.

Customize a Message

There are attributes of a message that you can choose to use when configuring messaging:

- General message features such as **Header** and **Body** options.
- **User Reason** settings when you want your end users to provide a reason before proceeding.
- **User Authorization** where a user must provide password, smart card, or both types of authentication information.
- **Multifactor Authentication** where an Identity Provider is configured.
- **Challenge/Response Authorization** where a user must enter a response code before proceeding.

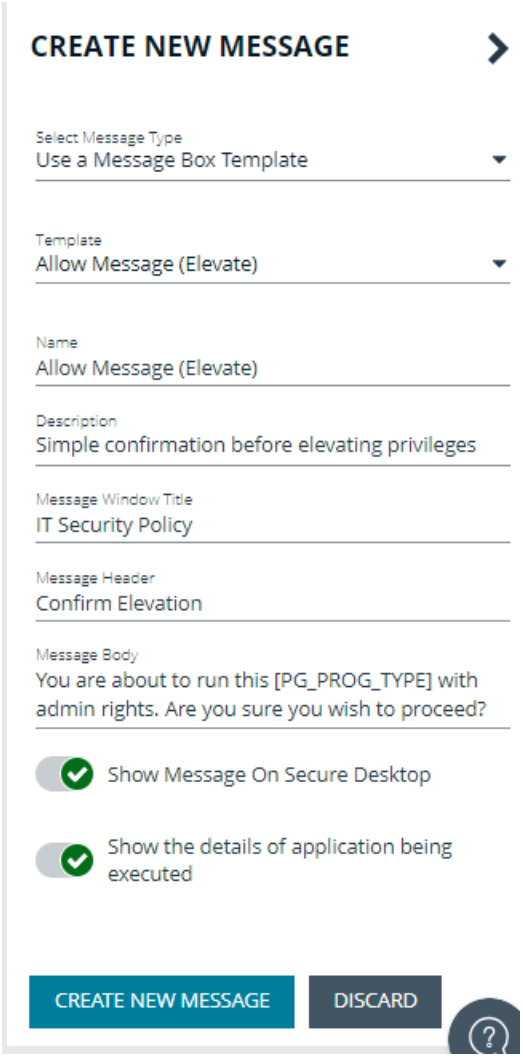
Select the **Edit** menu for a message template to customize the message properties.

Create a Message

> ***Note:*** *Message templates vary between Windows and macOS.*

1. In the Policy Editor, go to **Messages**.
2. Click **Create New Message** (Windows options shown in image at right).
3. (Windows only). Select a message type: *message box* or *notification*.
4. Select a message template from the list.
5. Enter a name. The default name is the name of the template.
6. Enter a description.
7. (Windows only). Enter the title that displays in the title bar of the window.
8. Enter text for the message header.
9. Enter text for the body.
10. (Windows only). Select **Show Message On Secure Desktop** to show the message on the secure desktop.
11. (Windows only). Turn off **Show the details of application being executed** to hide the details from being displayed. This option is enabled by default.
12. Click **Create New Message**.

You can edit or delete messages at any time.



> ***Tip:*** *Click* ***Preview*** *when editing a message to view a draft. Message preview is available for Windows and macOS messages.*

Add message header and body content

Message header options

You can configure the following message header options:

- **Show Message On Secure Desktop:** (Windows only). Select to show the message on the secure desktop. We recommend this if the message is being used to confirm the elevation of a process, for enhanced security.
- **Title Text:** (Windows only). Add text that appears in the title bar of the dialog box.
- **Header Type:** Select the type of header: **Default**, **Error**, **None**, **Question**, **Warning**.
- **Header Background Type:** Select **Solid** or **Custom Image**.
    - If you select **Solid**, use the color picker to select a header background color.
    - If you select **Custom Image**, you must select an image from the **Select Image** dropdown list. To use additional images, see "Add an Image" on page 85.
- **Show Header Text:** Select if you want to display header text.
- **Header Text:** Add text that displays next to the header type icon.
- **Header Text Color:** Select the color for the header text.

> ***Note:*** *(Windows only). For a* ***Notification*** *type of message, you can only configure the* ***Title Text****.*

Additional header message design properties are available when using the **User Request Message** template. You can customize the text for the interactive prompts displayed during the request workflow, such as *request text*, *pending text*, and *approval text*.

Message body options

You can configure the following message body options:

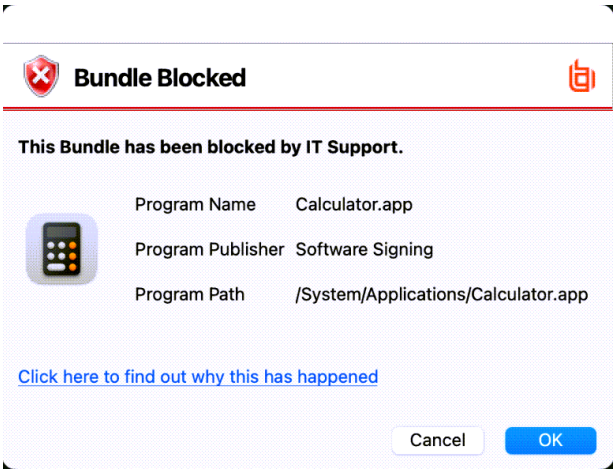
- **Body Text:** Add additional information for the end user.
- **Message Mode:** (Windows only). From the list, select **Automatic** or **Custom**. You can decide what information you want to display on the message. By default, all rows are *on* and will be displayed as part of the message. The **Automatic** default values are:
    - **Show Line One:** The *Program Name* or the *Content Name*.
    - **Show Line Two:** The *Program Publisher* or the *Content Owner*.
    - **Show Line Three:** The *Program Path* or the *Content Program*.
- **Show Reference Hyperlink:** Turn the option *on* (it is *off* by default). Update text for existing link on the message. In some cases, you might want to provide a website with more information for your end users. The URL appears *below* the body text.

> ***Example:*** *Here are some link ideas.*
> - *Web pages that provide support resources, terms of use statements, and web-based submission forms*
> - *Web-based ITSM solutions, including those that support parameterization of URLs for prepopulation of fields*
> - *Teams and other community support products*
> - *Email via mailto links, for integration with email based ITSM solutions*

- **Publisher:** Enter a publisher name and information to display if the verification for the publisher fails.
- **Buttons:** Customize the labels for the **OK** and **Cancel** buttons (Mac sample message shown in image at right).

> ***Note:*** *(Windows only). For a* ***Notification*** *type of message, you can only configure the* ***Body Text****.*

Additional body message design properties are available when using the **User Request Message** template. You can customize the text for the interactive prompts displayed during the request workflow, such as *request text*, *pending text*, *approval text*, *denial text*, and *referral text*.



> ***Tip:*** *Click* ***Preview*** *when editing a message to view a draft. Message preview is available for Windows and macOS messages.*

Add ActiveX Message

When you are elevating the installation of an ActiveX control in an application group, a built-in progress dialog box displays during the installation. You can customize the messaging on the installation progress dialog box.

ActiveX messages can be displayed in multiple languages. In EPM, the regional language of the end user can be detected, and if ActiveX strings in that language are configured, the correct translation is displayed.

> ***Note:*** *If language settings for the region of the end user are not configured, then the default language text is displayed. To change the default language, select a language and click* ***Set Default****.*

To create an ActiveX message:

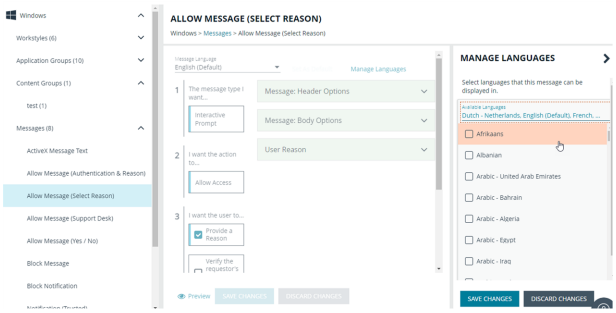
1. Go to the **Messages** tab, and then click **Create New Message**.
2. Select **Use ActiveX Control** from the list.
3. Fill in the text fields that will display on the dialog box.
4. Click **Create New Message**.
5. If you want to select a language other than English, click the newly created message in the navigation panel, and then click **Manage Languages**.
6. Select and save the language.

Select Message Language

You can configure message text to display a language of your choice. Click **Add Languages** and select the language from the dropdown list.

If you are using more than one language, select a language and click **Set As Default**. The default language is English.

If you delete the default language, then the language at the top of the list is set to the default. You must always have at least one language selected.

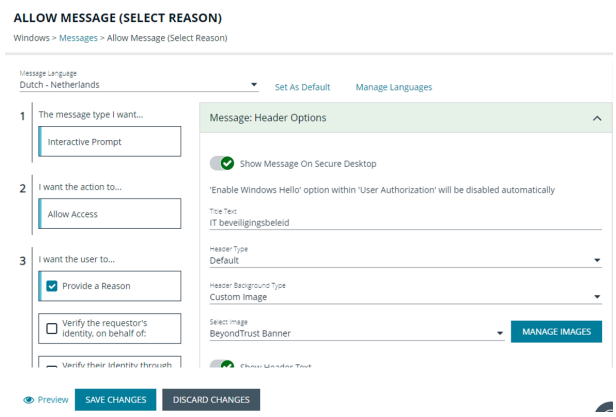


EPM checks the locale of the user's language and tries to match it to a language set up in EPM.

- If there is a match, the strings for that language are displayed for the message text.
- If there isn't a match, the language assigned as the default language is used.

EPM does not localize the text in the language you select. You must edit the message text in your chosen language.

If you import a policy with messages in a supported language, then the strings display in that language. The screen capture shows an example where a policy file was imported in Dutch.



Add an Image

To use different images in the header than the default BeyondTrust ones (such as your own company's logo, for branding purposes), you can import images into the **Manage Images** list.

Image requirements:

- File type must be .**png**
- Maximum file size is 240KB
- Recommended size is 450x50 pixels
- Images smaller than 450x50 pixels and greater than 600x100 pixels will be rejected.

To upload an image:

1. To the right of the **Select Image** field, click **Manage Images**.
2. Click **Import Image**.
3. On the **Upload Image** panel, drag or click to select an image to upload.
4. Enter the image name and a description.
5. Click **Upload Image**. The image is added to the list and is available for selection as a custom image.

You can delete images you imported. You cannot delete the BeyondTrust images.

To delete an image:

1. To the right of the **Select Image** field, click **Manage Images**.
2. Select an image. You cannot delete an image already in use. Select another image to use before proceeding.
3. Click the **Delete** button.

Edit an Image

To edit an image that you uploaded:

1. To the right of the **Select Image** field, click **Manage Images**.
2. Select the image, and then select **Edit** from the menu.
3. Update the name and/or description for the image, and then click **Save Changes**.

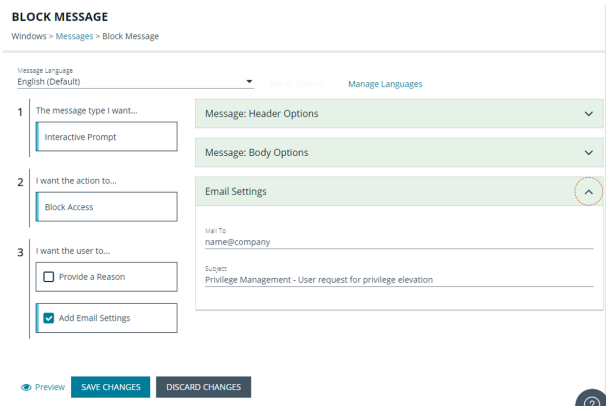
Add email (Windows only)

Email settings can be configured when using the Block Message template.

To access email settings, you must first create the message then edit the properties for the message.

Configure the following:

- **Mail To:** Email address to send the request to (separate multiple email addresses with semicolons).
- **Subject:** Subject line for the email request.



Add a Reason Prompt

You can configure the message to prompt the user to provide a reason for the request.

To set up the User Reason option:

1. Under section 3 on the left, check the **Provide a Reason** box.
2. Select the **User Reason Type**, a *textbox* or a *dropdown*.
3. (Optional). Select if you want to **Remember the User Reason (per application)**.
4. (Optional). You can change the default **Reason Text** and **Reason Error Message Text**.
5. (Optional). If you select the *drop-down* type, you can change the default **Drop-down List Prompt Text**.
6. (Optional). With the drop-down option, you can use the default **User Reason List** to be displayed for the user to choose from. You can also:
    - Change the text of the default list options.
    - Delete one or more of the default options.
    - Click the **Add User Reason** option to add your own user reason to the list.
7. Click **Save Changes**.

Add Challenge/Response Authorization

There are two parts to setting up Challenge/Response Authorization:

- **Set a shared key:** The Challenge/Response Key must be set to use Challenge/Response Authorization in your messages. The key is encrypted. The key is required by the Challenge/Response generator to generate response codes. The only way to change the shared key is by setting a new one.
- **Add the authorization type to a message:** When configuring your message, configure the Challenge/Response settings.

The Challenge/Response feature is a global setting and can be configured for Windows and macOS messages. Challenge/Response Authorization only applies to Allow message types.

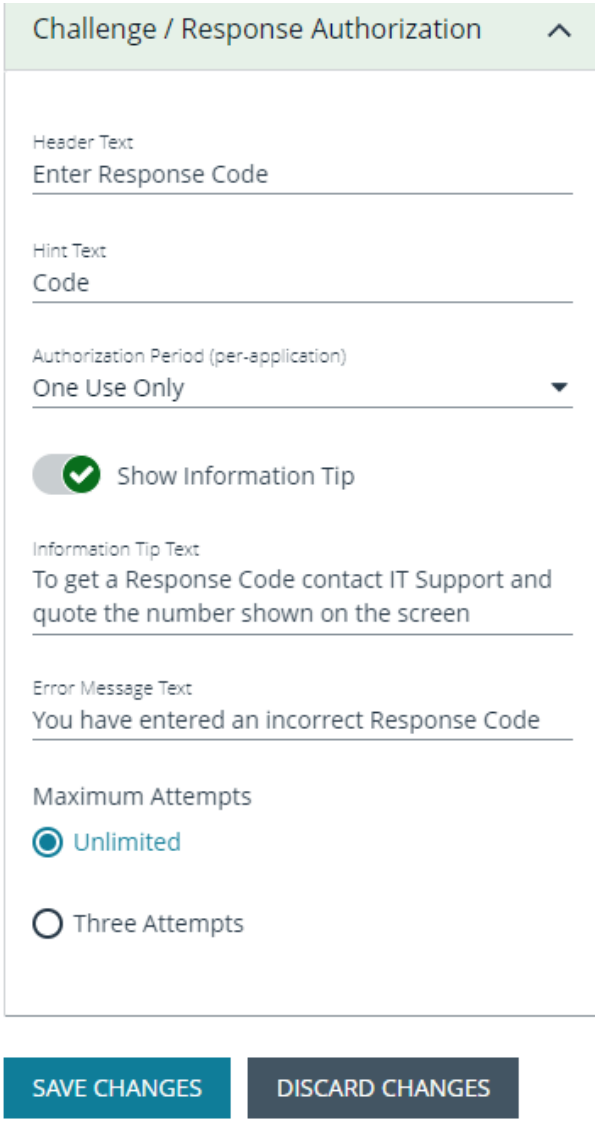
To add a shared key:

1. In the Policy Editor, click **Messages**.
2. Click **Challenge/Response Keys**.
3. Enter a key value and enter again to confirm.
4. Click **Set Key**.

To configure Challenge/Response Authorization:

1. In the Policy Editor, click **Messages**.
2. Create a message following the steps provided earlier. If this is an existing message, select **Edit** from the menu.
3. Under section 3 on the left, check the **Request Access via Challenge/Response** box.

4. Open the **Challenge / Response Authorization** dropdown, and set the following:



   - **Header text:** The text that introduces the challenge/response authorization.
   - **Hint text:** The text that is in the response code field for challenge/response messages.
   - **Authorization Period (per application):** Set this option to determine the length of time a successfully returned challenge code is active for.
     - **One Use Only:** A new challenge code is presented to the user on every attempt to run the application.
     - **Entire Session** (Windows only): A new challenge code is presented to the user on the first attempt to run the application. After a valid response code is entered, the user is not presented with a new challenge code for subsequent uses of that application until they next log on.
     - **As defined by helpdesk** (Windows only): A new challenge code is presented to the user on the first attempt to run the application. If this option is selected, the responsibility of selecting the authorization period is delegated to the helpdesk user at the time of generating the response code. The helpdesk user can select one of the three above authorization periods. After a valid response code is entered, the user does not receive a new challenge code for the duration of time specified by the helpdesks.
   - **Suppress messages once authorized** (Windows only): Select to suppress messages. This setting is not shown when set to **One Use Only**.
   - **Show Information Tip** (Windows only): Select to add helpful information for the end user.
   - **Information Tip Text:** Add text that appears above the challenge and response code fields. In Windows, this only appears if the **Show Information Tip** option above is selected.
   - **Error Message Text:** Add text to display to the end user if they enter an incorrect response code.
   - **Maximum Attempts:** Select from **Unlimited** and **Three Attempts**.
   - **Maximum Attempts Exceeded Message Text:** The message is only displayed when **Three Attempts** is selected. Add text to display to the end user if they exceed the allowed number of challenge/response attempts.

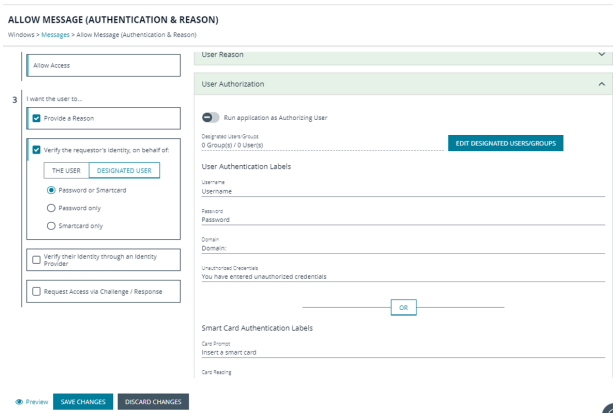
***Tip:** Click **Preview** when editing a message to view a draft. Message preview is available for Windows and macOS messages.*

Add User Authorization

When using a message to allow access to an application, you can enforce strict access to network resources using the authorization settings. When configured, users are required to enter credentials to proceed. The credential can be a password, smart card, or both.

User authorization settings can be configured on both Windows and macOS messages.

1. Select the message where you want to add user authorization as part of the access workflow.
2. Under section 3 on the left, check the **Verify the requestor's identity, on behalf of:** box.
3. Choose either **The User** or **Designated User**. If you select **Designated User**, see Edit Designated User for details on adding users and groups.
4. Select the authorization method: **Password or Smartcard**, **Password only**, or **Smartcard only**.
5. Click **User Authorization** to expand and customize labels and descriptions. The available fields will change depending on which method of authorization is selected, as noted here:



   - **The User:** When selected, enter the password. Optionally, customize the message that displays to users when the credentials are not approved.
   - **Designated User:** When selected, click the **Edit Designated Users/Groups** button to add the authorized users/groups. A designated user can be selected from a local account, Active Directory domain, or Microsoft Entra ID. Only Microsoft Entra ID groups are supported.
     - After the groups are added, enter the *user name*, *password*, and *domain*.
     - (Optional). Select **Run application as Authorizing User**. When selected, the application runs in the context of the authenticating user. When not selected, the application runs in the context of the logged on user.
     - (Optional). Customize the message that displays to users when the credentials are not approved.
     - (Optional). Customize the default messaging that displays when the Entra ID login session expires.
   - **Windows Hello:** Select to use the Windows Hello service to authenticate the user. Windows Hello must be installed on the endpoint for this to work with EPM.
     - Windows Hello is not supported with the **Designated User** option.
     - Set Authentication to the **Password or Smartcard** or the **Password only** option.
     - Windows Hello is unavailable when using Secure Desktop.
   - **TouchID:** Select to use TouchID to authenticate the user. TouchID must be configured on the endpoint to work with the policy editor messages.
     - TouchID is not supported with the **Designated User** option.
     - Set Authentication to the **Password or Smartcard** or the **Password only** option.
   - **Smart Card:** When smart card authorization is included, you can:
     - (Optional). Customize the **Smart Card Authentication Labels** that display to the user. The hint field is only displayed if your smart card authentication environment is configured to use them.
     - (Mac only). Select the **Sudo User Authorization** option.

Note: *At this time, you must fill out all of the fields under* ***User Authorization*** *to confirm your changes.*

Edit Designated User

You can add, edit, and remove users and groups from the **Designated Users/Groups List** list in the message configuration. You can manage multiple accounts at once from the **Designated Users/Groups List** page.

There are two ways to add groups:

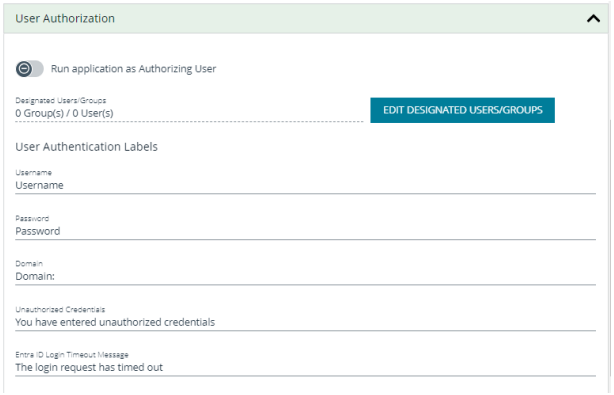
- Add local Active Directory domain groups and users
- Set up a connector that populates group information from your local Active Directory domains or your Microsoft Entra ID instance.

For more information about AD connectors, see "Active Directory Settings" on page 165.

***Note: Designated User** must be selected on step 3.**Verify the requestor's identity, on behalf of:** for the **Edit Designated Users/Groups** button to appear in User Authorization.*

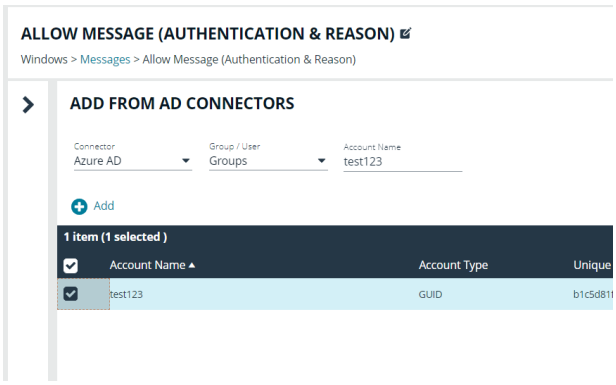
To add groups:

1. Expand **User Authorization**, click **Edit Designated User/Groups**.



2. Select one of the following:
   - **Add Account**: Add an account name and SID details. Click **Add Account**.
   - **Add Account from Search**: Select a connector on the **Add From AD Connectors** page. The default connector is **Built-In**. Enter search criteria in the **Account Name** box to find a specific account. Select the account name, and then select **Add**.

     If searching Microsoft Entra ID, a minimum of two characters is required to initiate the search. Use the search options, **Contains** or **Starts with** to narrow the scope of the search results.



3. Click **Save Changes**.

Configure Multifactor Authentication

Multifactor authentication (MFA) using an identity provider can be configured for messages in Endpoint Privilege Management. Identity providers supported by Endpoint Privilege Management include those using OpenID Connect (OIDC) and RADIUS protocols, and BeyondTrust should be setup as a *Native* or *Desktop* app within your Identity Provider configuration.

The RADIUS protocol is supported on Windows OS only.

Add an Identity Provider

1. In the Policy Editor, click **Messages**.
2. Click **Identity Provider Settings**.
3. On the **Identity Provider Settings** panel, select an identity provider from the list: **OIDC** or **RADIUS**.
4. Enter the following details for the identity provider:
    - **OIDC** Settings
        - **Authority URI:** The address of your identity provider.
        - **Client ID:** Must match the same value configured for your identity provider's BeyondTrust application.
        - **Redirect URI:** Must match the same value configured for your identity provider's BeyondTrust application. The format is **http://127.0.0.1:*port_number***, where *port_number* is an open port on your network. The *port_number* is only needed if required by your identity provider.
    - **RADIUS** Settings
        - **Authentication Mechanism:** The authentication type that is required by your RADIUS server. Supported authentication mechanisms are MS-CHAPV2 or PAP.
        - **Host:** The hostname of your RADIUS server.
        - **Port:** The port number for connecting to your RADIUS server.
        - **Shared Secret:** The secret key required by your RADIUS server.
5. Click **Save RADIUS Settings** or **Save OIDC Settings** depending on the type you selected.

After an identity provider is added you can configure any allow message type to use multifactor authentication.

For more information about adding identity providers, see "Configure OpenID Connect" on page 197.

Set up a Multifactor Authentication Message

1. In the Policy Editor, click **Messages**.
2. Click **Create New Message**.
3. Select the template **Allow Message (with Authentication)**, and then click **Create New Message**.
4. Select the message in the **Messages** navigation pane.
5. Under section 3 on the left, check the **Verify their Identity through an Identity Provider** box.
6. Expand **Multifactor Authentication**.
7. Select **Idp - OIDC** or **Idp - RADIUS**.
8. In the **Suppress Message when Authenticated for (Mins)** box, enter a value (maximum 720) to set the number of minutes that the authentication message is suppressed. The message will not be shown again for the given number of minutes after a successful authentication.
9. Enter information that displays on the message dialog box such as authentication failure text and authentication success text. Optionally, you can use the default text provided.

10. Enter the ACR value. The value is optional and required only if your identity provider uses it.
11. The following fields are specific to configuring Microsoft Entra ID conditional policies. If you are using conditional policies, contact BeyondTrust Technical Support for configuration details.
    - **Additional Scopes (optional)**: Some IdPs can trigger additional authentication policies server-side based on the scopes requested. This field can be used to provide that context to the IdP.
    - **Max age (seconds) (optional)**: The lifetime of the authorization request. The authorization runs out when the maximum age is reached.
12. Click **Save Changes**.
13. In the Policy Editor, click **Messages**.
14. Click **Create New Message**.
15. Select the template **Allow Message (with Authentication)**, and then click **Create New Message**.
16. Select the message in the **Messages** navigation pane.
17. Under section 3 on the left, check the **Verify their Identity through an Identity Provider** box.
18. Expand **Multifactor Authentication**.
19. Select **Idp - OIDC** or **Idp - RADIUS**.
20. In the **Suppress Message when Authenticated for (Mins)** box, enter a value (maximum 720) to set the number of minutes that the authentication message is suppressed. The message will not be shown again for the given number of minutes after a successful authentication.
21. Enter information that displays on the message dialog box such as authentication failure text and authentication success text. Optionally, you can use the default text provided.
22. Enter the ACR value. The value is optional and required only if your identity provider uses it.
23. The following fields are specific to configuring Microsoft Entra ID conditional policies. If you are using conditional policies, contact BeyondTrust Technical Support for configuration details.
    - **Additional Scopes (optional)**: Some IdPs can trigger additional authentication policies server-side based on the scopes requested. This field can be used to provide that context to the IdP.
    - **Max age (seconds) (optional)**: The lifetime of the authorization request. The authorization runs out when the maximum age is reached.
24. Click **Save Changes**.

Custom Tokens

A token is assigned to an application to change the privileges associated with the activity permitted for that application. Create a custom token to manually configure group membership, privileges, and process access rights.

Custom tokens can be used with on-demand rules, application rules, and content rules. By design, custom tokens only work for *allow* rules.

Changing the properties of an access token is designed for more advanced configurations.

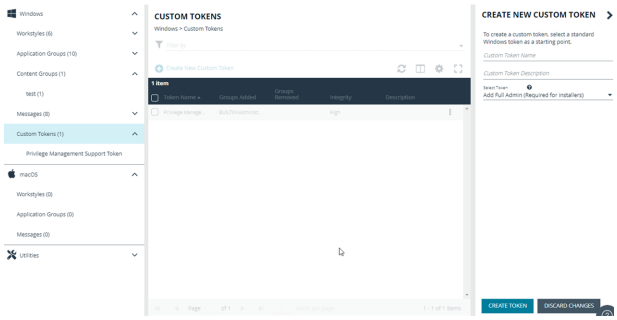
Here are some scenarios on customizing the properties of a token:

- Run remote PowerShell commands and scripts with a custom token that removes the SeRemoteShutDown privilege. This prevents the commands and scripts from shutting down servers during core business hours, even if the command or script indicates to do so.
- Create a custom token to run an application with custom privileges configured in the token. The user can run the application but with modified privileges as configured in the token.

Create a Custom Token

You can select from a list of Windows access tokens as the foundation to creating the custom token. After selecting the token, customize the following properties: group, privileges, and process access rights.

- Groups: Add local or Active Directory domain groups to the token.
- Privileges: Add or remove privileges that will be applied to the application.
- Process access rights: The process access rights allow you to choose the rights other processes have over a process launched with that custom token.



Create a Token

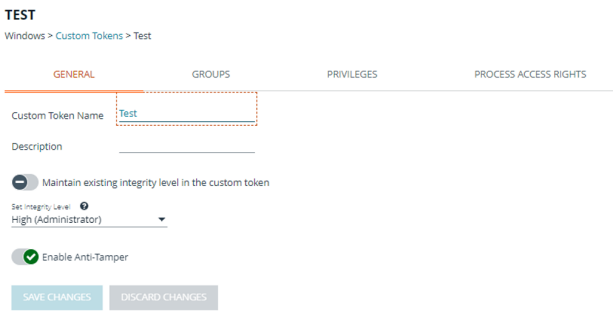
To create a token:

1. Navigate to the policy and click **Custom Tokens**.
2. Click **Create New Custom Token**.
3. Enter a name and description.
4. Select the level of permissions for the token:
    - **Add Full Admin (Required for installers)**: Preselected Windows administrator privileges.
    - **Drop Admin Rights**: Preselected Windows privileges that do not include administrator privileges.
    - **Blank**: Select this option to personalize the privileges for the token.
5. Click **Create Token**.
6. On the main **Custom Tokens** page, select the token and click **Edit** from the menu.
7. See the following sections for more details on the properties to configure.

Set Integrity Level and Anti-tamper

Follow these instructions to fine-tune your token settings for optimal application performance and security:

1. Click the **General** tab.
2. Select an integrity level or select **Maintain existing integrity level in the custom token** to use the existing Windows integrity level for the selected token type.
    - **System**: Included for completion and is not required.
    - **High**: Set the integrity level associated with an administrator.
    - **Medium**: Set the integrity level associated with a standard user.
    - **Low**: Set the integrity level associated with protected mode (an application might fail to run or function in protected mode)
    - **Untrusted**: Included for completion and is not required.



3. By default, anti-tamper protection is on. Anti-tamper protection prevents elevated processes from tampering with the files, registry, and service that make up the client installation. It also prevents any elevated process from reading or writing to the local policy cache.

    Keep anti-tamper enabled, except in scenarios where elevated tasks require access to protected areas, such as when using an elevated logon script to update the local policy.

4. Click **Save Changes**.

Add Group to Custom Token

There are two ways to add groups:

- Add local Active Directory domain groups
- Set up a connector that populates group information from your local Active Directory domains or your Microsoft Entra ID instance.

> *For more information about AD connectors, see "Active Directory Settings" on page 165.*

To add a group:

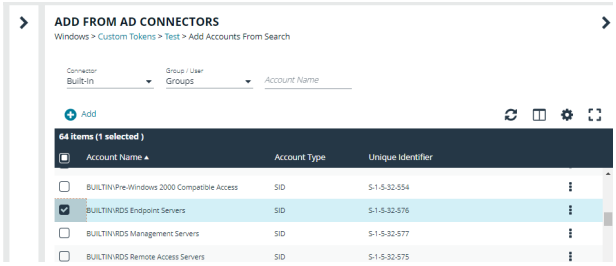
1. If you want the user to be the owner, regardless of the presence of the administrators group, select **Ensure the User is always the Token Owner**.

   By default, the owner of a custom token that includes the administrators group has the owner set to the administrators group. If the administrators group is not present in the custom token, then the user is set as the owner.

2. Select one of the following:

   - **Add Account**: Add an account name and SID details. Click **Add Account**.
   - **Add Account from Search**: Select a connector on the **Add From AD Connectors** page. The default connector is **Built-In**. Enter search criteria in the **Account Name** box to find a specific account. Select the account name, and then select **Add**.

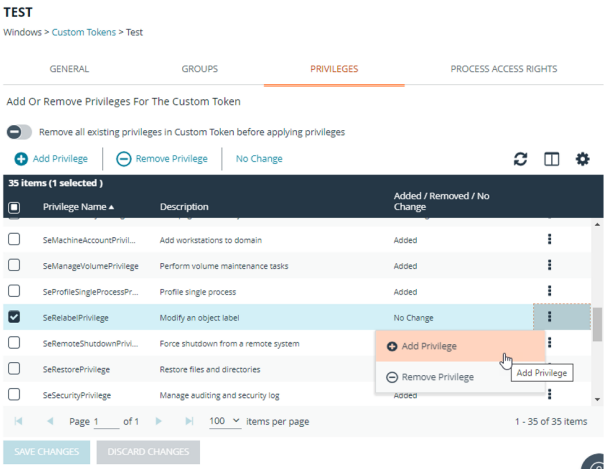
     If searching Microsoft Entra ID, a minimum of two characters is required to initiate the search. Use the search options, **Contains** or **Starts with** to narrow the scope of the search results.



Select Privileges for Custom Token

On the **Privileges** tab, select the privileges to add to or remove from the custom token.

1. Select a privilege, and then select
   - **Add Privilege** to add the privilege to the custom token.
   - **Remove Privilege** to remove the privilege to the custom token.
2. To reset the default state of a privilege, select the privilege and select **No Change**.
3. Click **Remove all existing privileges in Custom Token before applying privileges** to clear all privileges in the custom token before applying privileges. If not selected, the privileges are added or removed from the user's default custom token.

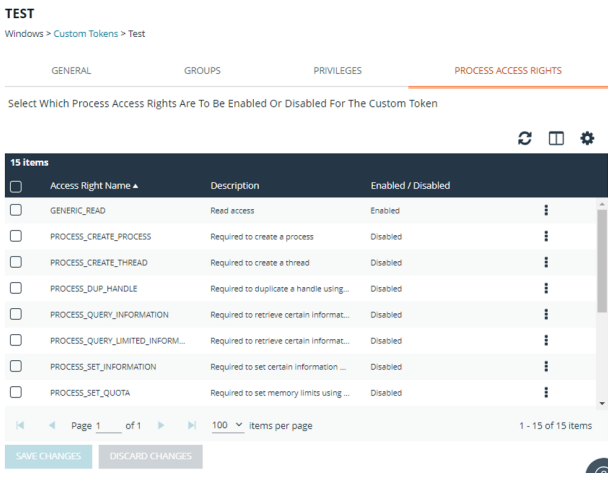


Enable Process Access Rights

The process access rights allow you to select the rights other processes have over a process launched with a custom token.

Tokens that include the administrators group have a secure set of access rights applied by default, which prevents code injection attacks on elevated processes initiated by processes running with standard user rights in the same session.

A custom token requires at least one enabled access right. If all access rights are disabled, then the default access rights are enabled: GENERIC_READ, READ_CONTROL, and SYNCHRONIZED. Edit the access rights if you do not want to use the default values.



Access Rights

Access Rights	Description
GENERIC_READ	Read access.
PROCESS_CREATE_PROCESS	Required to create a process.
PROCESS_CREATE_THREAD	Required to create a thread.
PROCESS_DUP_HANDLE	Required to duplicate a handle using **DuplicateHandle**.
PROCESS_QUERY_INFORMATION	Required to retrieve certain information about a process, such as its token, exit code, and priority class.
PROCESS_QUERY_LIMITED_ INFORMATION	Required to retrieve certain information about a process.
PROCESS_SET_INFORMATION	Required to set certain information about a process, such as its priority class.
PROCESS_SET_QUOTA	Required to set memory limits using **SetProcessWorkingSetSize**.
PROCESS_SUSPEND_RESUME	Required to suspend or resume a process.
PROCESS_TERMINATE	Required to terminate a process using **TerminateProcess**.
PROCESS_VM_OPERATION	Required to perform an operation on the address space of a process.
PROCESS_VM_READ	Required to read memory in a process using **ReadProcessMemory**.
PROCESS_VM_WRITE	Required to write to memory in a process using **WriteProcessMemory**.
READ_CONTROL	Required to read information in the security descriptor for the object, not including the

Access Rights	Description
	information in the SACL.
SYNCHRONIZE	Required to wait for the process to terminate using the wait functions.

Policy Editor Utilities

Policy Assistant (Beta)

Use the Policy Assistant to learn more about your policy configuration. The assistant detects if there are errors in configuration and provides remediation details. For example, duplicate Application Rules that potentially contradict each other, or duplicated user accounts in a Workstyle account filter.

The Policy Assistant validates the following areas of the policy:

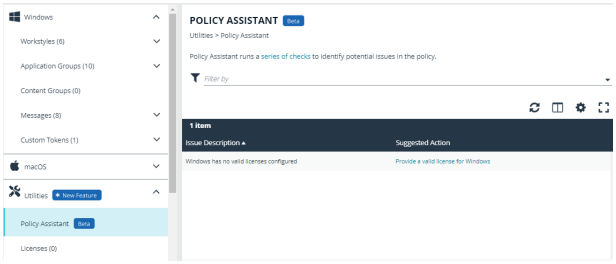
- Accounts filters
- Application rules
- Licensing
- On-demand rules
- Trusted application protection settings
- Workstyles

If there are no issues identified by the Policy Assistant, then the current set of checks hasn't detected issues. However, there could be potential issues not covered by the checks currently running.

Policy checks can run without saving the policy; any unsaved changes are checked when you access the Policy Assistant.

To access the assistant:

1. In the Policy Editor, expand **Utilities**.
2. Click the **Policy Assistant** tab.
3. Click the suggested action link to remediate the potential policy issue identified.



Policy Editor Licensing

Endpoint Privilege Management for Windows requires a valid license code to be entered in the Policy Editor. If more than one policy is applied to a computer, you need at least one valid license code for one of those policies.

For example, you could add the Endpoint Privilege Management for Windows license to an Endpoint Privilege Management policy that is applied to all managed endpoints, even if it does not have any Workstyles. This ensures all endpoints receive a valid license if they have Endpoint Privilege Management for Windows installed. If you are unsure, then we recommend you add a valid license when you create the Endpoint Privilege Management policy.

To add a license:

1. In the Policy Editor, expand **Utilities**.
2. Click the **Licenses** tab.

3. Click **Add**.
4. Enter the license key, and then click **Add License**.

Import Policy

Policies can be imported to and exported from Group Policy as XML files, in a format common to other editions of Endpoint Privilege Management, such as the Endpoint Privilege Management ePO Extension. Policies can be migrated and shared between different deployment mechanisms.

1. In the Policy Editor, expand **Utilities**.
2. Select **Import Policy**.
3. Select one of the following:
    - **Merge Policy**
    - **Overwrite Policy:** If you select to overwrite, you can optionally select **Export Existing Policy** to save a copy before overwriting the policy.
4. Drop the file onto the box or click inside the box to navigate to the file.
5. Click **Upload File**.

Import Template Policies

You can import a template and merge or overwrite the settings in an existing template.

1. In the Policy Editor, expand **Utilities**.
2. Select **Template Policies**.
3. Select one of the following:
    - **Merge Policy:** Merges the configuration to the existing template.
    - **Overwrite Policy:** If you select to overwrite, you can optionally select **Export Existing Policy** to save a copy before overwriting the policy.
4. Select a template from the list: **Discovery**, **QuickStart for Mac**, **QuickStart for Windows**, **Server Roles**, **TAP (High Flexibility)**, **TAP (High Security)**.
5. If you are merging, select **Merge Template Policy** to save the settings. If you are overwriting, select **Overwrite Policy**.

Manage Audit Scripts

When an application is allowed, elevated, or blocked, an event is logged to record details of the action. Actions are recorded in a third party tracking system by using audit scripts. You can write audit scripts in Powershell or Javascript and configure these scripts through the web policy editor.

1. In the Policy Editor, expand **Utilities**.
2. Select **Manage Audit Scripts**.
3. Click **Upload Script** to expand the Upload Script panel.

4. Click the following menus to further configure the script:
    - **Timeout Options**
    - **Context Options**
5. Click inside the upload box to select the script.

Manage Rule Scripts

You can upload, view, and delete Power Rules in the Policy Editor.

The script must be a Windows PowerShell script in JSON format.

1. In the Policy Editor, expand **Utilities**.
2. Select **Manage Rule Scripts**.
3. Click **Upload Script** to expand the **Upload Script** panel.
4. Select a value from the **Timeout options** list.
5. Drag and drop the new script into the upload box or click to select a file.
6. Click **Upload Script** to save your changes.

After a script is uploaded, you can delete or upload an updated script at any time.

For more information, see Apply Power Rules Scripts to Your Application Rules at https://www.beyondtrust.com/docs/privilege-management/windows/epo-admin/utilities/power-rule-scripts.htm.

Advanced Agent Settings

You can configure the Advanced Agent Settings utility through the Policy Editor to deploy additional registry based settings to endpoints that are running EPM-W.

Back up your Windows registry before making any changes. BeyondTrust Technical Support will not provide support for any issues that might occur when you change registry settings.

1. In the Policy Editor, expand **Utilities**.
2. Select **Advanced Agent Settings**.
3. Click **Add** to create a new setting.
4. Type the desired value name.
5. Select one of the following to designate the type:
    - **DWORD**
    - **String**
    - **Multi-String**
6. Click **Create** to confirm your changes and create the new setting.

Set Up Agent Protection

Add agent protection to your endpoints to prevent admin users from tampering with the product, including stopping the services running or deleting its files from an endpoint.

EPM components protected and the level of protection are provided in the table.

Action	EPM Component
Blocks uninstalls	• Defendpoint client • PMC adapter • AD connector • Package Manager
Prevents stopping services	• Defendpoint client • BeyondInsight adapter • ePO service
Blocks DLL injections	• Defendpoint client • PMC adapter • ePO service • BeyondInsight adapter
Blocks access to registry settings	• Defendpoint client • ePO service • BeyondInsight adapter • Password Safe service
File protection (deleting, moving, renaming, writing security attributes, or taking ownership)	• C:\ProgramData\Avecto • C:\Program Files\Avecto\Privilege Guard Client\ • C:\Windows\System32\drivers\PGDriver.sys • C:\Program Files (x86)\Avecto\Privilege Guard Client • C:\Program Files (Arm)\Avecto\Privilege Guard Client

Set up Protection

The setup is a two-part process:

- Generate public-private key pair.
    - The public key is stored in a policy and distributed to all computers. The public key is automatically inserted into the policy.
    - The password-protected private key must be stored securely by the administrator. The private key and private key password are required when you want to disable agent protection.
- Enable protection.

Generate Key Pairs

To generate the key pair:

1. In the Policy Editor, expand **Utilities**.
2. Select **Agent Protection Settings**.
3. Click **Generate Key**.
4. Enter a password to encrypt the private key.
5. Click **Generate Key**.
6. The private key is automatically downloaded to the local computer. The file name is **private.pem**. The public key is automatically inserted into the policy.

Enable Agent Protection

To enable protection:

1. In the Policy Editor, expand **Utilities**.
2. Select **Advanced Agent Settings**.
3. Click **Add**.
4. Enter **AgentProtectionState** in the **Name** box.
5. Select **64 bit**.
6. Ensure type is **DWORD**.
7. In the **Decimal** box, set the value to **1**. The **Hex** value automatically populates with the same value. There are three possible states: **0** = off, **1** = enabled, **2** = disabled.

Agent protection is enabled after the policy is deployed and loaded by the Windows computers.

> *For more information about using agent protection, see Set up Agent Protection at https://www.beyondtrust.com/docs/privilege-management/windows/admin/install-upgrade/install-pm-windows.htm.*

Regenerate UUIDs

When importing and exporting policies from external sources, it can sometimes be necessary to regenerate the internal policy **Universally Unique Identifier (UUID)**, so that Reporting manages the events correctly. For most normal scenarios in which this is required (policy duplication, for example), this is handled seamlessly.

However, duplication by importing a text XML file will not be covered because sometimes you will not want to regenerate the UUIDs, such as when restoring a policy from a backup.

To regenerate UUIDs:

1. In the Policy Editor, expand **Utilities**.
2. Select **Regenerate UUIDs**.
3. Click the **Regenerate UUIDs** button.

A success message displays at the bottom center of the page.

Power Rules and Regular Expressions

Power Rules

A Power Rule is a PowerShell based framework that lets you change the outcome of an Application Rule, based on the outcome of a PowerShell script.

Instead of a fixed Default Rule that can either be set to Allow, Elevate, Audit, or Block for the applications in the targeted Application Group, a Power Rule lets you determine your own outcome based on any scenario you can build into a PowerShell script.

Any existing Default Rule within a Workstyle can be updated to a Power Rule by setting the action to a Power Rule script, and importing the PowerShell script you want to use. EPM provides a PowerShell module with an interface to collect information about the user, application, and policy. The module can then send a resulting action back to EPM to apply.

The Power Rules module also provides a variety of message options that allow you to collect additional information to support your PowerShell script logic and provide updates to the user as to the status, progress, or outcome of your rule. The messages that are supported include:

- Authentication message
- Business Justification message
- Information message
- Pass code message
- Vaulted credential message
- Asynchronous progress dialog for long running tasks

Power Rules is a highly flexible feature with unlimited potential. If you can do it in PowerShell, you can do it in a Power Rule. Here are some example use cases for Power Rules:

- Environmental Factors: Collecting additional information about the application, user, computer, or network status to influence whether an application should be allowed to run, or run with elevated privileges.
- Service Management: Automatically submitting tickets to IT Service Management solutions, and determining the outcome of a service ticket.
- File Reputation: Performing additional checks on an application by looking up the file hash in an application store, reputation service, or a vulnerability database.
- Privileged Access Management: Checking out credentials from a password safe or vault, and passing them back to Endpoint Privilege Management to run the application in that context.

> *For information on creating a Power Rule, see the Core Scripting Guide, at https://www.beyondtrust.com/docs/privilege-management/integration/core-scripting/index.htm.*

Windows Workstyle Parameters

The Endpoint Privilege Management for Windows settings include a number of features allowing customization of text and strings used for end user messaging and auditing. If you want to include properties relating to the settings applied, the application being used, the user, or the installation of Endpoint Privilege Management for Windows, then parameters may be used which are replaced with the value of the variable at runtime.

Parameters are identified as any string surrounded by brackets (**[ ]**), and if detected, the Endpoint Privilege Management client attempts to expand the parameter. If successful, the parameter is replaced with the expanded property. If unsuccessful, the parameter remains part of the string. The table below shows a summary of all available parameters and where they are supported.

Parameter	Description
[PG_AGENT_VERSION]	The version of Endpoint Privilege Management for Windows
[PG_APP_DEF]	The name of the Application Rule that matched the application
[PG_APP_GROUP]	The name of the Application Group that contained a matching Application Rule
[PG_AUTH_METHODS]	Lists the authentication and/or authorization methods used to allow the requested action to proceed
[PG_AUTH_USER_DOMAIN]	The domain of the designated user who authorized the application
[PG_AUTH_USER_NAME]	The account name of the designated user who authorized the application
[PG_COM_APPID]	The APPID of the COM component being run
[PG_COM_CLSID]	The CLSID of the COM component being run
[PG_COM_NAME]	The name of the COM component being run
[PG_COMPUTER_DOMAIN]	The name of the domain that the host computer is a member of
[PG_COMPUTER_NAME]	The NetBIOS name of the host computer
[PG_DOWNLOAD_URL]	The full URL from which an application was downloaded
[PG_DOWNLOAD_URL_DOMAIN]	The domain from which an application was downloaded
[PG_EVENT_TIME]	The date and time that the policy matched
[PG_EXEC_TYPE]	The type of execution method: Application Rule or shell rule
[PG_GPO_DISPLAY_NAME]	The display name of the GPO (Group Policy Object)
[PG_GPO_NAME]	The name of the GPO that contained the matching policy
[PG_GPO_VERSION]	The version number of the GPO that contained the matching policy
[PG_IDP_AUTH_USER_NAME]	The value given by the Identify Provider as the user who successfully authenticated to allow the requested action to proceed. Maps to the OIDC "email" scope.
[PG_MESSAGE_NAME]	The name of the custom message that was applied
[PG_PROG_CLASSID]	The ClassID of the ActiveX control
[PG_PROG_CMD_LINE]	The command line of the application being run
[PG_PROG_DRIVE_TYPE]	The type of drive where application is being executed
[PG_PROG_FILE_VERSION]	The file version of the application being run
[PG_PROG_HASH]	The SHA-1 hash of the application being run
[PG_PROG_HASH_SHA256]	The SHA-256 hash of the application being run
[PG_PROG_NAME]	The program name of the application
[PG_PROG_PARENT_NAME]	The file name of the parent application
[PG_PROG_PARENT_PID]	The process identifier of the parent of the application
[PG_PROG_PATH]	The full path of the application file
[PG_PROG_PID]	The process identifier of the application
[PG_PROG_PROD_VERSION]	The product version of the application being run
[PG_PROG_PUBLISHER]	The publisher of the application

Parameter	Description
[PG_PROG_TYPE]	The type of application being run
[PG_PROG_URL]	The URL of the ActiveX control
[PG_STORE_PACKAGE_NAME]	The package name of the Windows Store App
[PG_STORE_PUBLISHER]	The package publisher of the Windows Store app
[PG_STORE_VERSION]	The package version of the Windows Store app
[PG_TOKEN_NAME]	The name of the built-in token or Custom Token that was applied
[PG_USER_DISPLAY_NAME]	The display name of the user
[PG_USER_DOMAIN]	The name of the domain that the user is a member of
[PG_USER_NAME]	The account name of the user
[PG_WORKSTYLE_NAME]	The name of the Workstyle

Regular Expression Syntax

Use regular expressions to control applications at a granular level. Endpoint Privilege Management uses the CAtlRegExp library, which is part of the Microsoft ATL Server implementation, and makes use of the regex parser and engine.

Examples

The following examples are from Endpoint Privilege Management QuickStart Templates.

Application Definition	Regular Expression	Application
File / Folder Name	%ProgramFiles%(\(x86\))*\\webex\\productivity tools\\ptupdate.exe	Cisco WebEx ptUpdate
File / Folder Name	vcredist_x[0-9][0-9]\.exe	Microsoft Visual C++ Redistributable Setup
File / Folder Name	((rdbgsetup)|(msvsmon))\.exe	Microsoft Visual Studio Remote Debugger
Command line	(powershell_ise.exe)|(powershell.exe)|(cmd.exe)|(wscript.exe)|(cscript)|(mshta.exe)	Any Trusted Executable
Command line arguments	-[rfRM].*[rfRM]\s\W*	rm

Syntax

Metacharacter	Meaning	Example
Any character except [\^$.|?*+()	All characters except the listed special characters match a single instance of themselves. To match one of these listed characters use a backslash escape character (see below).	**abc** matches **abc**
\ (backslash)	Escape character: interpret the next character literally.	**a\+b** matches **a+b**

Metacharacter	Meaning	Example
. (dot)	Matches any single character.	**a.b** matches **aab**, **abb** or **acb**, etc.
[ ]	Indicates a character class. Matches any character inside the brackets (for example, **[abc]** matches **a**, **b**, and **c**).	**[abc]** matches **a**, **b**, or **c**
^ (caret)	If this metacharacter occurs at the start of a character class, it negates the character class. A negated character class matches any character except those inside the brackets (for example, **[^abc]** matches all characters except **a**, **b**, and **c**). If **^** is at the beginning of the regular expression, it matches the beginning of the input (for example, **^[abc]** will only match input that begins with **a**, **b**, or **c**).	**[^abc]** matches all characters except **a**, **b**, and **c**
- (minus character)	In a character class, indicates a range of characters (for example, **[0-9]** matches any of the digits **0** through **9**).	**[0-9]** matches any of the digits **0** through **9**
?	Indicates that the preceding expression is optional: it matches once or not at all (for example, **[0-9][0-9]?** matches **2** and **12**).	**ab?c** matches **ac** or **abc**
+	Indicates that the preceding expression matches one or more times (for example, **[0-9]+** matches **1**, **13**, **999**, and so on).	**ab+c** matches **abc** and **abbc**, **abbbc**, etc.
* (asterisk)	Indicates that the preceding expression matches zero or more times	**ab*c** matches **ac** and **abc**, **abbc**, etc.
| (vertical pipe)	Alternation operator: separates two expressions, exactly one of which matches.	**a|b** matches **a** or **b**
??, +?, *?	Non-greedy versions of **?**, **+**, and *****. These match as little as possible, unlike the greedy versions which match as much as possible. Example: given the input **<abc><def>**, **<.*?>** matches **<abc>** while **<.*>** matches **<abc><def>**.	Given the input **<abc><def>**, **<.*?>** matches **<abc>** while **<.*>** matches **<abc><def>**.
( )	Grouping operator. Example: **(\d+,)*\d+** matches a list of numbers separated by commas, such as **1** or **1,23,456**.	**(One)|(Two)** matches **One** or **Two**
{ }	Indicates a match group. The actual text in the input that matches the expression inside the braces can be retrieved through the **CAtlREMatchContext** object.	
\	Escape character: interpret the next character literally. For example, **[0-9]+** matches one or more digits, but **[0-9]\+** matches a digit followed by a plus character. Also used for abbreviations, such as **\a** for any alphanumeric character; see table below. If \ is followed by a number n, it matches the nth match group (starting from 0). Example: <{.*?}>.*?</\0> matches "<head>Contents</head>". Note that in C++ string literals, two backslashes must be used: "\\+", "\\a", "<{.*?}>.*?</\\0>".	**<{.*?}>.*?</\0>** matches **<head>Contents</head>**
$	At the end of a regular expression, this character matches the end of the input. Example: **[0-9]$** matches a digit at the end of the input.	**[0-9]$** matches a digit at the end of the input
|	Alternation operator: separates two expressions, exactly one of which matches. For example, **T|the** matches **The** or **the**.	**T|the** matches The or **the**
!	Negation operator: the expression following **!** does not match the input. Example: **a!b** matches **a** not followed by **b**.	**a!b** matches **a** not followed by **b**

Overview

The topics in this section provide information on computers and computer groups in your estate that are managed using EPM.

Computers

Computers groups

Management rules

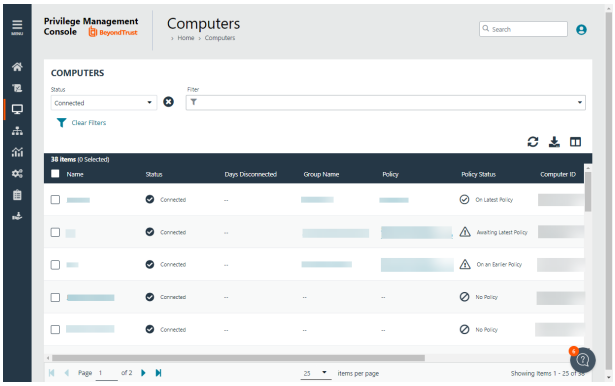
Manage Computers

After the Endpoint Privilege Management client software is deployed to a computer, use the **Computers** page to keep track of the computers managed by EPM. You can:

- Authorize and assign a computer to a group.
- Archive and delete a computer no longer in use.
- Download logs for a computer to ensure proper communication between the computer and EPM
- Assess computer health
- Change the group a computer is assigned to
- Check the status of the policy deployment. If a computer is not on the latest policy, you can drill down to policy details to determine next steps.

Overview

When working on the **Computers** page, there are many UI features available so you only view relevant computers.



- Use the **Status** filter to see disconnected or connected computers. The first time a computer comes online, the computer shows as *Connected*. A computer can stop communicating with EPM when it goes offline for any period (weekends, leave of absence from work, etc). When the computer is back online the status automatically returns to *Connected*. Drill down to more details to learn more information about the health of the computer.
- Select from a list of computer filters, like policy status, authorization state, created on date.
- Choose columns that you want to view in the main display.
- Access computer features on the menu to individually manage a computer
- Use the **Show Computers with Duplicate Names** to filter all computers with the same host name. Determine the most recently active computer by the time in the **Last Connected** column.

For more information on computer status, see "Computer Settings" on page 163.

Authorize and Assign Computers to a Group

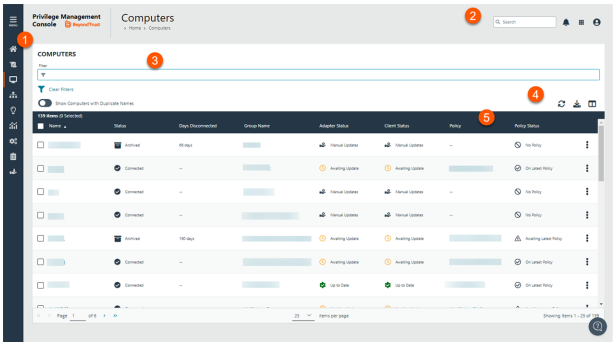
Starting in EPM v. 23.4, *Pending Activation* is a deprecated computer state. However, there may be scenarios where a computer might be in this state. In this case, follow the steps here to authorize the computer.

To authorize and assign computers in one step:

1. On the sidebar menu, click **Computers**.
2. Select the computers, and then select **Authorize** at the top of the page.
3. From the group dropdown list, select a group, and then click **Assign**. If you have not created any groups yet, you will see **No Group** in the dropdown.

4. If you have a Default group, it will be selected by default, otherwise you can select the group from the dropdown list. Click **Assign**. A notification briefly flashes green at the bottom of the screen to indicate that EPM has processed your request.

Computers List Page



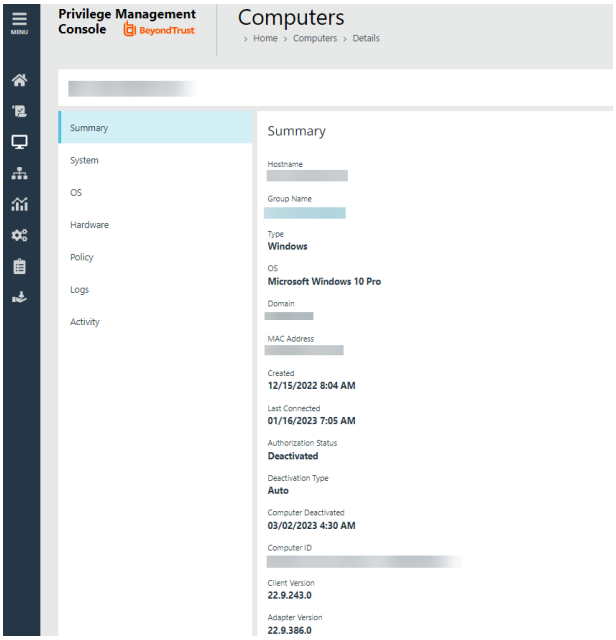
1. **Sidebar:** Easy access to all pages in Endpoint Privilege Management, including the Home, Policies, Computers, Computer Groups, Management Rules, Analytics, Configurations, Auditing, and Users pages.
2. **Header:** Enter keywords to run a global search across computer groups, policies, computers, and users, view your notifications, access your connected apps, and set your account preferences.
3. **Filters:** Click the drop arrow to select a filter type. The selected filter displays to the left of the drop-down.
    - **Clear Filters:** Click to remove all filters and search results
    - **Filter types**
        - **Name:** Enter all or part of a policy name.
        - **Status:** The state of the computer, Connected, Disconnected, or Archived.
        - **Disconnected for more than:** Enter the number of days a computer is disconnected.
        - **Client Status**: The status of the adapter install, such as Manual Updates, Awaiting Update, or Up to Date.
        - **Adapter Status**: The status of the adapter install, such as Manual Updates, Awaiting Update, or Up to Date.
        - **Authorization State**: The status of the computer, Authorized or Deactivated.
        - **Group Name**: The group where the computer is a member.
        - **Assigned Policy**: The name of the policy assigned to the computer.
        - **Current Applied Policy**: The policy name and revision the computer is on.
        - **Policy Status**: The state of the policy, such as Awaiting Latest Policy or On Latest Policy.
        - **Last Connected**: The date the computer last checked in with EPM.
        - **Package Manager**: The version of Package Manager deployed to the computer.
        - **OS**: The operating system and version.
        - **Domain**: The domain where the computer resides.
        - **Created On**: The date the computer was created.
        - **Archived for more than**: Enter the number of days.
        - **System Type**:
4. **List options:** Click to refresh the list, to download list of the displayed computers to a .csv file, and click to select which columns to display on your **Computers** page.
5. **Computers list columns:** Not all columns display in the image above.
    - **Name:** The computer name.
    - **Status:** The state of the computer, Connected, Disconnected, or Archived.
    - **Days Disconnected:** The number of days the computer has been disconnected from EPM.
    - **Group Name:** The group where the computer is a member.
    - **Adapter Status:** The status of the adapter install, such as Manual Updates, Awaiting Update, or Up to Date.
    - **Client Status:** The status of the adapter install, such as Manual Updates, Awaiting Update, or Up to Date.
    - **Current Applied Policy:** The policy name and revision the computer is on.

- **Assigned Policy:** The name of the policy assigned to the computer.
- **Policy Status:** The state of the policy, such as Awaiting Latest Policy or On Latest Policy.
- **Computer ID**: The ID for the computer.
- **Last Connected**: The date the computer last checked in with EPM.
- **Client**: The version of the client deployed to the computer.
- **Adapter**: The version of the adapter deployed to the computer.
- **Package Manager**: The version of Package Manager deployed to the computer.
- **OS**: The operating system and version.
- **Domain**: The domain where the computer resides.
- **Created On**: The date the computer was created.
- **Authorization State**: The status of the computer, Authorized or Deactivated.
- **Archived On**: The date the computer was archived.
- **System Type**:

View Computer Details

To ensure computers are up to date and running properly, you can view details on the computer which include, hardware and operating system information, policy status, and logging information.

To get a quick at-a-glance view of recent activities on the computer, click the **Activity** tab. You can see who accesses the computer, the event time, and summary information on the action that occurred.



Check Policy Status

You can view the policy status on the main **Computers** page for each computer. If the status is **Awaiting Latest Policy**, drill down to see more information about the policy on the **Policy** tab. The collected metrics include the current policy applied and the version.

If the computer is not receiving updated policies, go through the computer details to determine if there are connection issues with the computer. The **Logs** tab, **Activity** tab, and **OS** tab might have helpful information to troubleshoot issues.

Download Logs

You can view and download logs to track activities between the computer and EPM. This can be helpful to troubleshoot issues with the computer. For example, you can see if a computer is successfully receiving incoming commands from EPM.

There are two types of logs:

- **Computer**: Records all communication between EPM and the computer.
- **Command**: Records the commands sent to the computer. The log information includes the command sent and whether the command was received by the computer.

To access the logs:

1. Select a computer.
2. Select **View Computer Details** , and then click **Logs**.
3. Select the **Computer Logs** tab or **Command Logs** tab.
4. To gather recent activity or if there are no logs, click **Request Logs**.

Edit a Computer's Group Assignment

Add computers to a computer group to organize computers that will receive the same policy. A computer group must already be created.

During the adapter install, computers are automatically assigned to a group with a status of *Authorized*.If a group ID is not assigned at install time the default group is used.

You can change the group assignment if policy requirements change for a computer.

To assign a computer:

1. On the sidebar menu, click **Computers**.
2. Click the menu for a computer, and then select **Edit Group Assignment**.
3. From the dropdown list, select a group, and then click **Save Group Assignment**.

For more information on creating a group, see "Computer Groups" on page 123.

Reissue a Certificate to a Computer

Certificates were used as the authentication method between adapters and EPM in older adapter versions (21.7 and earlier).

Issue a new certificate when the certificate expires on the endpoint.

1. Go to the **Computers** page.
2. Locate the computer in the list, and select **Renew Certificate**.

Update Computer Details

If you are troubleshooting a computer problem or you want to make sure policy status is current, you want to be sure that you are viewing the most recent information collected for that computer. To do this, select the computer, and then select **Update Computer Details** from the menu.

View a Computer's Analytics

Open a host report to view analytics on the computer activity and includes:

- Applications that have been run
- Running processes
- Users accessing the computer
- Logon activity

The host report can also be accessed from the **Events > All** report.

To view computer analytics:

1. On the sidebar menu, click **Computers**.
2. From the menu for a computer, select **View Analytics**.

Archive a Computer

Use the management rules to automatically move computers in your estate to an archived status. Archived computers can be deleted or moved to the active pool of computers, this can also be managed manually or automatically using rules.

For more information, see "Management Rules" on page 132.

Delete a Computer

There are three ways to delete computers:

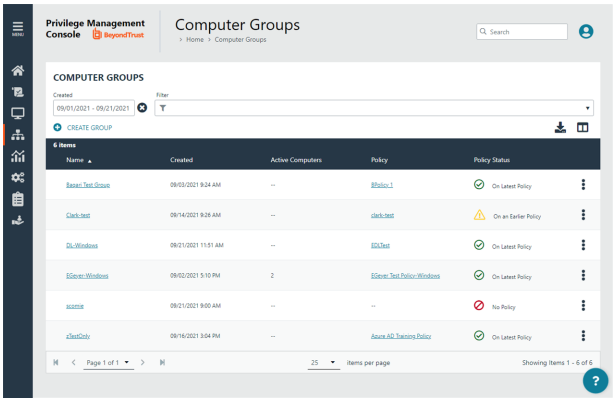
- Delete Rule: See Management Rules section.
- Computers page: Manually delete a computer from the **Computers** page. Select the computer in the list, and then click **Delete** from the menu. Only users with administrator privileges can delete computers using this method.
- Management API: Use the **delete** command. When using the API, you can delete any computer regardless of the status.

Computer Groups

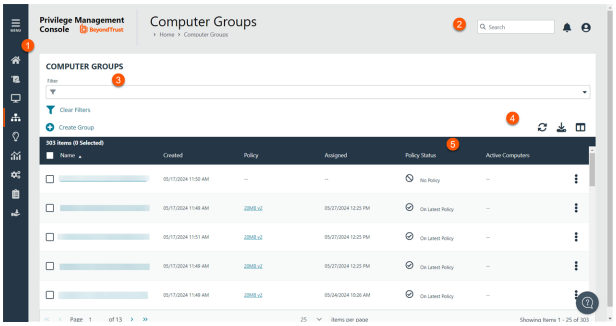
Use a computer group to organize computers that will be assigned the same policy. For example, create a computer group and add the computers that will use a high-flexibility workstyle. Assign users like your system administrators to this workstyle.

On the **Computer Groups** page:

- Create and edit groups
- Delete a group
- View policy status
- Set the default group
- Set and edit the policy assigned



Computer Groups List Page



1. **Sidebar:** Easy access to all pages in Endpoint Privilege Management, including the Home, Policies, Computers, Computer Groups, Management Rules, Analytics, Configurations, Auditing, and Users pages.
2. **Header:** Enter keywords to run a global search across computer groups, policies, computers, and users, view your notifications, access your connected apps, and set your account preferences.
3. **Filters:** Click the drop arrow to select a filter type. The selected filter displays to the left of the drop-down.
    - **Clear Filters:** Click to remove all filters and search results
    - **Filter types**
        - **Name:** Enter all or part of a policy name.
        - **Created:** The date the group was created.
        - **Policy**: The name of the policy assigned to the computer group.
        - **Policy Status**: The state of the policy, such as On an Earlier Policy or On Latest Policy.
        - **Windows/Client/Adapter**: The date the computer last checked in with EPM
4. **List options:** Click to refresh the list, click to download list of the displayed groups to a .csv file, and click to select which columns to display on your **Computer Groups** page.
5. **Computer Groups list columns:** Not all columns display in the image above.

    - **Column names**

    - **Name:** The computer group name.
    - **Created:** The date the group was created.
    - **Active Computers:**The number of computers in the group.
    - **Windows Client/Adapter:** The state of the client/adapter version, such as Up to Date, Awaiting Updated, Update Failed, Manual Updates.
    - **Policy:** The name of the policy assigned to the computer group.
    - **Assigned:** The date the policy was assigned.
    - **Policy Status:** The state of the policy, such as On an Earlier Policy or On Latest Policy.
    - **Description**: The detail provided when creating the group.
    - **Users**: A list of users associated with that computer group.
    - **All Computers**: The number of computers that are members in the group.

Create a group

> ***Note:*** *A standard user requires delegated access to this page. For more information, see About user roles and resources.*

Create a computer group to assign a policy to more than one computer.

1. On the sidebar menu, click **Computer Groups**.
2. Click **Create Group**.
3. Enter a **Group Name**. The **Description** field is optional. At any time, click the menu, and then select **Edit Properties** to edit the group name and description.
4. Click **Create Group**. Your group is created and appears in the list.
5. After a group is created, you can set it as the default group. Select a group name, and then select **Set as Default** from the menu.

When computers are added to EPM, they are automatically added to the default group.

Download a List of Groups to CSV

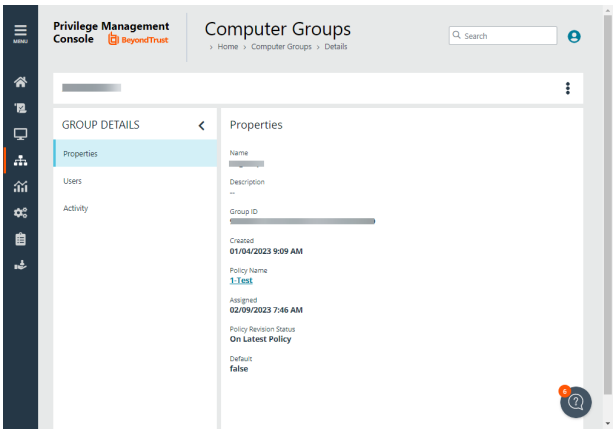
1. On the sidebar menu, click **Computer Groups**.
2. Click  .

View Group Details

You can view details on a group which include, name, group ID, create date, and policy information.

To get a quick at-a-glance view of recent activities on the group , click the **Activity** tab. You can see who accesses the group, the event time, and summary information on the action that occurred.

1. On the sidebar menu, click **Computer Groups**.
2. Select a group, and then select **View Group Details** from the menu. You can also click the name of the group in the grid.



Check the Policy Assigned Date

If you are investigating a computer with a policy status of *Awaiting Policy*, check the date and time a policy was assigned to the group on the **Group Details** panel. The **Assigned Date** displays the most recent policy assignment.

The **Assigned Date** can help you determine when computers are out of compliance. You do not want computers in a *Awaiting Policy* state for longer than 1-2 days.

Edit Group Policy Assignment

Assigning a policy to a group allows you to manage computers in that group using the same policy.

1. On the sidebar menu, click **Computer Groups**.
2. Select one or more groups, and then select **Edit Policy Assignment**.
3. In the **Edit Policy Assignment** panel, select a policy, and then select a revision.
4. Click **Save Policy Assignment**. A prompt briefly appears and flashes green to indicate that EPM has processed your request.

Clear a Policy from a Group

A computer is no longer controlled by policy when the policy is cleared from the group.

1. On the sidebar menu, click **Computer Groups**.
2. Select the group, and then select **Edit Policy Assignment** from the menu.
3. Click **Clear Policy Assignment**.
4. You are notified how many computers will be affected by the change. To proceed, click **Clear Policy Assignment**.

Edit Group Name and Description

Changing the name or description does not affect the computers that are added to the group, or the policy delivered to those computers.

1. On the sidebar menu, click **Computer Groups**.
2. Click the group, and then select **Edit Group** from the menu.
3. Change the **Group Name**, and **Description**, and then click **Save Group**.

Set a Default Group

After a group is created, you can set it as the default group. When computers are added to EPM, they are automatically added to the default group.

1. Select a group name, and then select **Set as Default** from the menu.

Delete a Group

You can only delete groups that do not have any computers assigned to them. Groups can be deleted if they have a policy assigned to them.

1. On the sidebar menu, click **Computer Groups**.
2. Click the group, and then select **Delete** from the menu.
3. You are prompted to confirm the decision. To proceed, click **Delete Group.**

Management Rules

Create management rules to automatically move computers in your estate to an archived status. Archived computers can be deleted or moved to the active pool of computers; this can also be managed manually or automatically using rules.

Workflow

- A computer shows as either connected or disconnected based on Computer Settings.
- When disconnected for a period of time, the computer status changes to archived the next time the management rule triggers.
- If the computer reconnects to EPM, the computer status changes to a connected state.
- A computer is no longer displayed in the **Computers** list after the status changes to *Archived*.

A computer can go into a disconnected state if:

- A user goes on short term leave. Shows as disconnected after the number of days configured pass. User returns before the archive rule is configured. When the user turns on the computer and the status changes to disconnected.
- A user goes on extended leave and turns their computer off. When the user returns to work and turns the computer on, the status changes to *Connected* and the policy updates.
- A computer is permanently decommissioned. Shows as *Disconnected* after the number of days configured pass. Computer is then archived and then deleted (after the deletion rule triggers).
- Computer is deactivated before the deactivation option is removed from EPM. The status changes to *Disconnected*. Computer is archived after the archive rule runs. Then the computer is deleted when the delete rule runs.

About Rules

There are preconfigured management rules:

- **Archive Rule**: Archives computers after they are disconnected for 90 days. You can change and delete this default rule.
- **Deletion Rule**: *Soft* deletes computers after they have been archived for 90 days. The computer still resides in the database. You can change and delete this default rule.
- **System Purge Computer Rule**: Deactivates computers after they are deleted for 7 days; purges computers from the database after they are deactivated for 14 days. This rule cannot be deleted. You can adjust the number of days before deactivating computers (default value is 7 days).
- **System Purge Connector Rule**: Purges local AD connectors from the database after the connectors are deleted. You can change the number of days since a connector was deleted; other properties of the rule cannot be changed.

> ***Note:*** *A standard user requires delegated access to this page. For more information, see About user roles and resources.*

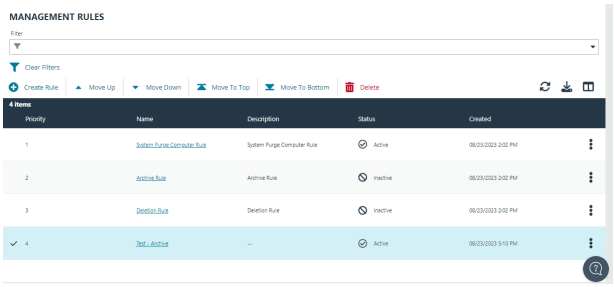
Rules Processing

The order of the rules in the list determines the priority and when the rules run. Select a rule to change the order.

When creating rules, consider the conditions in the rule before setting the order. If the action in one rule is set to *Delete*, and the action in another rule is set to *Archive*, be sure to set the archiving rule to run first.

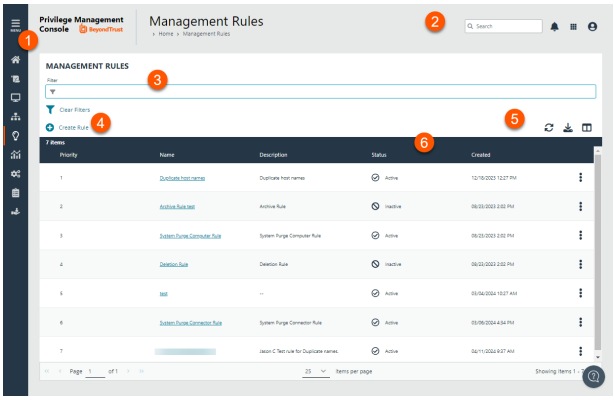
A delete rule only deletes computers when the computers have already been archived (by another rule).

A rule triggers when a computer matches on all of the conditions configured in a rule.



The properties configured in a rule are joined with *and* logic. If you want to use *or* logic, create two rules. If the condition is not triggered on the first rule, then it will trigger on the second rule.

Management Rules List Page



1. **Sidebar:** Easy access to all pages in Endpoint Privilege Management, including the Home, Policies, Computers, Computer Groups, Management Rules, Analytics, Configurations, Auditing, and Users pages.
2. **Header:** Enter keywords to run a global search across computer groups, policies, computers, and users, view your notifications, access your connected apps, and set your account preferences.
3. **Filters:** Click the drop arrow to select a filter type. The selected filter displays to the left of the drop-down.
    - **Clear Filters:** Click to remove all filters and search results
    - **Filter types**
        - **Name:** Enter all or part of a rule name.
        - **Status:** Select a status to filter on, Inactive or Active.
        - **Created:** Select a date range or multiple days from the date selector.
        - **Last executed**: Select a date range or multiple days from the date selector.
4. **Create Rule:** Click to create a rule.
5. **List options:** Click to refresh the policies list, to download list of the displayed management rules to a .csv file, and click to select which columns you want to display on your **Management Rules** page.
6. **Management Rules list columns:** Not all columns display in the image above.
    - **Priority:** The policy name.
    - **Name:** The rule name.
    - **Description:** The description provided when the rule is created.
    - **Status:** The state of the management rule (active, inactive).
    - **Created:** The date and time the rule was created.
    - **Last Executed:** The date and time the rule last ran.

Create a Custom Rule

To create a management rule:

1. Click the **Management Rules** menu, and then click **Create Rule**.
2. Add a name and description.
3. Set the following rule details:
    - **Conditions**: Add the computer property that must be matched to trigger the rule on a computer. The list of properties available includes all computer properties collected by EPM. A rule triggers when a computer matches on all of the conditions configured in a rule.
    - **Actions**: Select either **Archive** or **Delete**.
    - **Frequency**: Select how often to run the rule. Select **On Demand** if you do not want the rule to run at regular intervals. To run a rule using the **On Demand** frequency, select **Run Rule** from the menu.
4. Click **Validate Settings**. Validating rules ensures there are no conflicts in the conditions set and verifies properties are not used twice in the same rule.

Edit a System Rule

For system rules, certain settings cannot be changed.

1. Go to **Management Rules**.
2. Find the rule, and select **Edit Rule Details** from the menu.
3. For a system rule, change the properties:
    - Archive Rule: Change any rule property.
    - Deletion Rule: Change any rule property.
    - System Purge Computer Rule: You can adjust the number of days before deactivating computers (default is 7 days)
    - System Purge Connector Rule: You can change the number of days since a connector was deleted. Other properties cannot be changed.

Edit Custom Rule

1. Go to **Management Rules**.
2. Find the rule, and select **Edit Rule Details** from the menu.
3. For a custom rule, change the properties:
    - Name and description
    - Matching criteria
    - Action
    - Execution

Activate or Deactivate Rule

To activate a rule:

1. Log on to the EPM SaaS console.
2. Click the **Management Rules** menu, and then select **Activate Rule** from the menu.

To deactivate a rule:

1. Log on to the EPM SaaS console.
2. Click the **Management Rules** menu, and then select **Deactivate Rule** from the menu.

The rule remains listed on the page. Activate the rule later at any time.

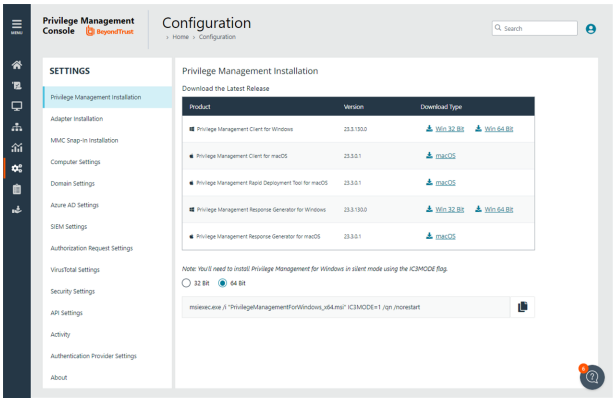
Delete a Rule

To delete a rule:

1. Click the **Management Rules** menu, and then click **Delete**.
2. Select **Delete Management Rule**.

Configure EPM

The **Configuration** menu contains the following areas:



- Installers for Windows and macOS clients, including the macOS Rapid Deployment Tool, and response generators.
- Installers for Windows and macOS adapters
- Install and configure Package Manager to auto-update endpoints in your estate.
- Computer status configuration where you can set a time frame to update the status.
- Add a domain so emails can be received from EPM.
- Configure Active Directory (AD) connectors to discover AD groups in your estate.
- Set up a SIEM integration to export endpoint audit event data to your SIEM tool.
- Configure Authorization Request Settings to integrate your ServiceNow instance with EPM.
- Add your VirusTotal API key to integrate reputation scores in Analytics.
- Add a security layer by setting a console timeout period to log off users when the time is reached.
- Create an API account if using the EPM API.
- The Activity page provides auditing details on areas in **Configuration**.
- About

Note: *A standard user requires delegated access to this page. For more information, see About user roles and resources.*

Download client software

EPM-M

- macOS client
- Rapid Deployment Tool for macOS
- Capture Config for macOS
- Configuration Profile for macOS
- Response generator

EPM-W

- Windows client
- Response generator
- Agent protection utility for Windows

Requirements

For more information about the installation requirements, see Endpoint Privilege Management Release Notes at https://www.beyondtrust.com/docs/release-notes/privilege-management/index.htm.

Download installers

1. Go to **Configuration > Privilege Management Installation**.
2. Download the installers.

Install the Mac Adapter

The adapter is responsible for delivering policies and events between the computer and EPM when computers are managed by Endpoint Privilege Management.

Note: *The adapter polls for pending commands every 60 minutes, which can include policy updates.*

Distribute the Adapter

The Mac adapter can be distributed to computers using the method of your choice, including Mobile Device Management (MDM) tools, such as Jamf or AirWatch.

We recommend using the Endpoint Privilege Management Rapid Deployment Tool for macOS.

The workflow for using the Rapid Deployment Tool:

- Download the Rapid Deployment Tool. You can download the tool from the **Configuration** page in EPM. Go to **Configuration > Privilege Management Installation**.
- Create a package that will include the information to facilitate communication between Endpoint Privilege Management and the macOS computers. Copy values from **Configuration > Adapter Installation**. See Create a Package for Endpoint Privilege Management.
- Create a package that includes settings specific to the macOS computer. This includes settings like, anonymous logging, sudo management control, allow biometric authentication, and policy sources, among others. See Create a Package with Endpoint Privilege Management for Mac Base Settings.
- Download and install the client package from the **Configuration** page. Go to **Configuration > Privilege Management Installation**. Click the **macOS** download link.
- Download and install the adapter package. Go to **Configuration > Adapter Installation**.

For more information, see the Rapid Deployment Tool Guide at https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-mac-rapid-deployment-tool.

Installer Parameters

The installer parameters include the following:

- **TenantID** for your chosen method of authentication. This was recorded when EPM was installed.
- **InstallationID:** Click **Configuration** > **Adapter Installation** to copy the Installation ID for the installer script.
- **InstallationKey:** Click **Configuration** > **Adapter Installation** to copy the Installation Key for the installer script.
- **ServiceURI:** The URL for your EPM portal.
- **TenantID** for your chosen method of authentication. This was recorded when EPM was installed.
- **InstallationID:** Click **Configuration** > **Adapter Installation** to copy the Installation ID for the installer script.
- **InstallationKey:** Click **Configuration** > **Adapter Installation** to copy the Installation Key for the installer script.
- **ServiceURI:** The URL for your EPM portal.

Note: *Do not include a port number or slash character on the end of the* ***ServerURI****.*

For example, neither ***https://test.pm.beyondtrustcloud.com/*** *nor* ***https://test.pm.beyondtrustcloud.com:8080/*** *will work.*

- **GroupID:** A computer must be added to a group as part of the EPM onboard process. The group determines the policy applied to a computer. A groupID is automatically assigned to a computer during the adapter install if one is not provided.

For information on how to automatically assign and authorize computer groups, see "Authorize and Assign Computers to a Group" on page 112.

Run the Installer

You must install the Mac adapter using Terminal.

To install adapters:

1. Go to **Configuration > Adapter Installation** to download the Endpoint Privilege Management adapter installer.
2. Also on the **Adapter Installation** page, note the Tenant ID, Server URL, Installation Key, and Installation ID. You need these required parameters for the installer script.
3. Navigate to the location of the adapter installer. By default this is the **AdapterInstallers** folder.
4. Mount the DMG.
5. From Terminal, run the installer command as shown in the example below with the parameters. The adapter installer launches. Proceed through the installation wizard.

Example:

```
sudo /Volumes/PrivilegeManagementConsoleAdapter/install.sh tenantid="750e85d1-c851-4d56-8c76-b9566250cf1d" installationid="95a10760-2b96-4a0e-ab65-ed7a5e8f1649" installationkey="VGhpcyBzZWNyZXQgaTYzIGJlZW4gQmFzZTY0IGVuY29kZWQ=" serviceuri="https://test.ic3.beyondtrust.com" groupid="fcc4022e-12fa-4246-87w8-0de9a1483a68"
```

For more information, see "Authorize and Assign Computers to a Group" on page 112.

Uninstall Endpoint Privilege Management for Mac

Note: *The uninstall scripts must be run from their default locations.*

Uninstall Endpoint Privilege Management

To uninstall Endpoint Privilege Management locally on a Mac, run the following command:

```
sudo /usr/local/libexec/Avecto/Defendpoint/1.0/uninstall.sh
```

Uninstall the Mac Adapter

To uninstall the Mac adapter, run the following command. After running the uninstall script some related directories remain if they are not empty, such as **/Library/Application Support/Avecto/iC3Adapter**.

```
sudo /usr/local/libexec/Avecto/iC3Adapter/1.0/uninstall_ic3_adapter.sh
```

Remove the Endpoint Privilege Management Policy

To remove the policy once you have uninstalled Endpoint Privilege Management, run the following command:

```
sudo rm -rf /etc/defendpoint
```

Note: *Do not remove the Endpoint Privilege Management policy unless you have already uninstalled Endpoint Privilege Management.*

Install the Windows Adapter

The adapter is responsible for delivering policies and events between the computer and EPM when computers are managed by Endpoint Privilege Management.

> ***Note:*** *The adapter polls for policy updates every 5 minutes, and for pending commands every 60 minutes.*

Prerequisites

.NET 4.6.2

Installer Parameters

Before running the installer, copy the values for the following parameters:

- **TenantID:** Go to **Configuration** > **Adapter Installation** to copy the Tenant ID for the installer script.
- **InstallationID:** Go to **Configuration** > **Adapter Installation** to copy the Installation ID for the installer script.
- **InstallationKey:** Go to **Configuration** > **Adapter Installation** to copy the Installation Key for the installer script.
- **ServerURI:** This is the URL for EPM. For example, **https://<customerhost>-services.pm.beyondtrust.cloud.com**, where **customerhost** is the DNS name for EPM.

> ***Note:*** *Do not include a port number or slash character on the end of the* ***ServerURI****.*
>
> *For example, neither* ***https://test.pm.beyondtrustcloud.com/*** *nor* ***https://test.pm.beyondtrustcloud.com:8080/*** *will work.*

- **UserAccount** (Optional):
  - For versions before 21.8, the default account for installing the adapter is **iC3Adapter**.
  - From version 21.8 and up, **LocalSystem** is the *only* account name to use.
- **GroupID:** A computer must be added to a group as part of the EPM onboarding process. The group determines the policy applied to a computer. The default groupID is automatically assigned to a computer during the adapter install if one is not provided. Computers are then automatically assigned an *Authorized* status.

> *For information on how to automatically assign and authorize computer groups, see "Authorize and Assign Computers to a Group" on page 112.*

Run the Installer

You must install the Windows adapter using the Windows command line.

To install adapters:

1. Go to **Configuration > Adapter Installation** to download the Endpoint Privilege Management adapter installer.
2. Also on the **Adapter Installation** page, note the Tenant ID, Server URL, Installation Key, and Installation ID. You need these required parameters for the installer script.
3. Navigate to the location of the adapter installer. By default this is the **AdapterInstallers** folder.

4. From the command line, enter the install command with the required parameters and press **Enter**. The adapter installer launches. Proceed through the installation wizard.
5. Go to **Configuration > Adapter Installation** to download the Endpoint Privilege Management adapter installer.
6. Also on the **Adapter Installation** page, note the Tenant ID, Server URL, Installation Key, and Installation ID. You need these required parameters for the installer script.
7. Navigate to the location of the adapter installer. By default this is the **AdapterInstallers** folder.
8. From the command line, enter the install command with the required parameters and press **Enter**. The adapter installer launches. Proceed through the installation wizard.

Example: *The line breaks must be removed before you run the script.*

```
msiexec.exe /i "PrivilegeManagementConsoleAdapter_x64.msi"
TENANTID="<TenantID_GUID>"
INSTALLATIONID="<InstallationID>"
INSTALLATIONKEY="<InstallationKey>"
SERVICEURI="<EPM URL>"
USERACCOUNT=LocalSystem
GROUPID="<EPM GroupID GUID>"
```

Add the following argument if you don't want the adapter service to start automatically. This option is useful when Endpoint Privilege Management for Windows and the adapter are being installed on an image that will be reused to create many individual computers. If the adapter is not disabled in this scenario, the adapter will immediately join the EPM instance indicated.

Note: *If the adapter starts up and registers with EPM prior to creating the VM image, then all VMs created from this image will contain the same adapter identifier and will not work properly.*

```
SERVICE_STARTUP_TYPE=Disabled
```

You can start the **IC3Adapter** service manually later in the Services.

Example:

```
msiexec.exe /i "PrivilegeManagementConsoleAdapter_x64.msi" TENANTID="6b75f647-d3y7-4391-
9278-002af221cc3f" INSTALLATIONID="08A1CD8F-FAE4-479F-81B4-00751A55EEB8"
INSTALLATIONKEY="ABCDEFGHIJKLMNO" SERVICEURI="https://CUSTOMERHOST-
services.pm.beyondtrustcloud.com"
USERACCOUNT=LocalSystem GROUPID="e531374a-55b9-4516-g156-68f5s32f5e57"
SERVICE_STARTUP_TYPE=Disabled
```

CUSTOMERHOST *= the hostname. For example, if the hostname were* ***test****, the desired input would be:*

```
https://test-services.pm.beyondtrustcloud.com
```

Upgrade the Windows Adapter

To upgrade to a full system-level DPAPI adapter:

1. Upgrade to the 22.1 adapter, where the adapter continues to run as the IC3 user, but at the system level.
2. Upgrade from 22.1 to a later version of the adapter allows the adapter to run as any system-level user, like LocalSystem.

Note: *For a new adapter install, starting in version 22.1, this 2-step process is not required.*

Configure the Windows EPM Adapter

The adapter uses HTTPS when communicating with EPM. If there is a proxy in place that this communication goes through, it must be configured for the adapter user account, which is separate from the logged-on user account.

The computer must be configured to use proxy settings for the machine rather than the individual user. The following registry key needs to be edited to make this change:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings]
```

The Data value must read **0**. This specifies the machine (**1** specifies per user).

Name	Type	Data
ProxySettingsPerUser	REG_DWORD	0

Ensure the iC3Adapter User Has the "User Can Log on as a Service" Right

When you install the adapter, a user account called **iC3Adapter** is created. The **iC3Adapter** user is granted the right to **Log on as a Service** by the installation process. If you have a Group Policy in place that revokes this permission, ensure the **iC3Adapter** user is excluded, as it requires the **Log on as a Service** right.

For more information, see the Microsoft Knowledgebase article Add the Log on as a service Right to an Account at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc794944(v=ws.10).

Example:

```
msiexec.exe /i "PrivilegeManagementConsoleAdapter_x64.msi" TENANTID="6b75f647-d3y7-4391-
9278-002af221cc3f" INSTALLATIONID="08A1CD8F-FAE4-479F-81B4-00751A55EEB8"
INSTALLATIONKEY="ABCDEFGHIJKLMNO" SERVICEURI="https://CUSTOMERHOST-
services.pm.beyondtrustcloud.com" GROUPID="e531374a-55b9-4516-g156-68f5s32f5e57"
SERVICE_STARTUP_TYPE=Disabled
```

CUSTOMERHOST *= the hostname. For example, if the hostname were* ***test****, the desired input would be:*

```
https://test-services.pm.beyondtrustcloud.com
```

Set Up a Proxy During Adapter Install

Starting in version 23.1, the Windows adapter installer supports setting up a proxy during installation using the following command line parameters:

PROXYADDRESS, **BYPASSONLOCAL**, **USESYSTEMDEFAULT**, and **SCRIPTLOCATION**

An example command using a proxy configuration parameter looks like the following:

Example:

```
msiexec.exe /l*v adapter_install.log /i "PrivilegeManagementConsoleAdapter_x64.msi"
TENANTID="02fe4a89-ae4b-316c-d026-da8acc80b33f" INSTALLATIONID="0066f094-7f73-4c47-bfca-
e7d4849d1449" INSTALLATIONKEY="angUArsM39Mk/MRD44o4Mn8dmOBGVBA6l01BBk7ljek="
SERVICEURI="https://tenantid-services.epm.btrusteng.com" GROUPID="bfac11e7-bf82-40c7-
b5ee-3a0b34a304cd" usesystemdefault=”false” PROXYADDRESS=”http://<PROXY URL>:<PORT>”
```

The proxy settings are written to the **Avecto.Ic3.Client.Host.exe.config** file on the computer's file system.

When using a non-authenticated proxy configuration, you can install an adapter by passing the command line parameters **USESYSTEMDEFAULT='false' PROXYADDRESS='http://<PROXY URL>:<PORT>'**

Example:

```
<http://system.net >
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy usesystemdefault="false" proxyaddress="http://<PROXY URL>:<PORT>" />
  </defaultProxy>
</system.net>
```

```
msiexec.exe /l*v adapter_install.log /i "PrivilegeManagementConsoleAdapter_x64.msi"
TENANTID="02fe4a89-ae4b-316c-d026-da8acc80b33f" INSTALLATIONID="0066f094-7f73-4c47-bfca-
e7d4849d1449" INSTALLATIONKEY="angUArsM39Mk/MRD44o4Mn8dmOBGVBA6l01BBk7ljek="
SERVICEURI="https://tenantid-services.epm.btrusteng.com" GROUPID="bfac11e7-bf82-40c7-
b5ee-3a0b34a304cd" usesystemdefault=”true”
scriptLocation=”http://pactest/adaptertest.pac”
```

```
<http://system.net >
    <defaultProxy enabled="true">
      <proxy usesystemdefault="true" scriptLocation="http://pactest/adaptertest.pac" />
    </defaultProxy>
</system.net>
```

Remove Proxy Configuration

To remove the proxy address configuration, pass **PROXYADDRESS="** as a command line parameter during upgrade.

This removes the proxy address configuration from the **Avecto.Ic3.Client.Host.exe.config** file.

Install and Upgrade Considerations When Using a Proxy

Keep the following in mind when installing and upgrading the adapter using proxy settings:

- If you install an adapter with proxy command line parameters and later upgrade to a newer version without proxy command line parameters, the older config file proxy settings are retained and persisted.
- If you install an adapter without proxy command line parameters and later upgrade to a newer version with proxy command line parameters, the newly added proxy configuration are reflected.

- If you install an adapter version with proxy command line parameters and later upgrade to a newer version with a different proxy configuration, the newly added proxy configuration is used.
- If you install or upgrade an adapter with an invalid proxy address, the computer is not registered in EPM.
- Leaving the proxy address field empty does not set the proxy address in the **Avecto.Ic3.Client.Host.exe.config** file.

Reset the EPM Windows Adapter

Use the Endpoint Privilege Management Adapter Reset tool to reset an adapter to the factory default values. There are several use cases where you might need to reset the adapter:

- In preparation for machine imaging. This includes creating a base image from a computer for roll out across an organization or department, or for organizations using VDI environments.
- To reconnect a disconnected or deactivated endpoint from EPM without the need to uninstall and reinstall the adapter. By resetting the configuration, the adapter can reauthenticate and reconnect to EPM in a clean and simple way.

> ***Note:*** *The Adapter Reset tool cannot configure proxy settings for the EPM Adapter.*

Access the Adapter Reset Tool

The Adapter Reset tool is available in three different formats. Review the list to determine how you can access the tool:

- **Installed with Adapter**: Preferred method. Only available for 23.9 or later adapters.
- **Installed with Package Manager**: Preferred method for 23.8 and earlier adapters.
- **Standalone**: Download the installer from the **Configuration > Adapter Installation** page. Extract and run on an endpoint.

Requirements

- The tool must run as a System-level user. EPM Windows Adapters newer than version 21.7 can run as System-level user.
- The tool does not work with adapters using the ic3Adapter user. Those adapters must be upgraded manually to version 21.8 and the ic3Adapter user changed to the LocalSystem user.

Endpoint Privilege Management for Windows Compatibility

The tool is not compatible with Endpoint Privilege Management for Windows agent protection and Endpoint Privilege Management for Windows anti-tamper in versions of the Reset Adapter prior to 23.8, and is not usable on devices where agent protection or anti-tamper are enabled.

Download

1. To download the tool, go to the **Configuration** page and select **Adapter Installation**.
2. Click the link for the download type: **Win 32 Bit** or **Win 64 Bit**.

Usage

When you install the tool, the **PMC.PackageManager.InstallerActions.exe** utility is installed.

```
PMC.PackageManager.InstallerActions ACTION=RESETPACKAGEMANAGER | RESETADAPTER
BACKUPLOCATION=<absolute_dir_path_for_backup>  TENANTID=<tenantID>
```

```
INSTALLATIONID=<installationID> INSTALLATIONKEY=<installationKey> SERVICEURI=<serviceUri>
GROUPID=<groupID> PROXYADDRESS=<proxyUrl>
```

All parameters listed in the installation command are required, except for **BACKUPLOCATION** and **PROXYADDRESS**.

- **ACTION=RESETADAPTER**: Resets the adapter.
- **ACTION=RESETPACKAGEMANAGER** : Resets Package Manager.
- **BACKUPLOCATION**: Optional parameter. Stores backups of any existing configuration files.
- **PROXYADDRESS**: Optional parameter. The proxy URL.

Update Proxy Settings for Package Manager

You can use the Adapter Reset tool to update and apply proxy settings to the Package Manager after installation or to the existing installed Package Manager.

In this command, proxy settings are configured for Package Manager only.

The proxy setting can be used by the adapter if the proxy setting is updated first, and then the adapter is installed by Package Manager.

```
PMC.PackageManager.InstallerActions ACTION=UPDATEPROXY PROXYADDRESS=<proxyUrl|NONE|"">
AUTODETECT=<true|false> USESYSTEMDEFAULT=<true|false> BYPASSONLOCAL=<true|false>
SCRIPTLOCATION=<script>
```

Restart Services

After resetting the Adapter or Package Manager, the respective service must be restarted.

Note: *It is not recommended to reset both the Adapter and Package Manager on the same machine.*

Doing so causes the Adapter and Package Manager to attempt to activate and register with EPM, resulting in two active entries for the same computer.

In this scenario, stop the Package Manager service, uninstall the Adapter, and then reset the Package Manager. Once the Package Manager is active, the Package Manager installs the Adapter with the auto-update configuration.

Package Manager Installation

The EPM Package Manager (Package Manager) is an optional feature which helps organizations install and maintain the Endpoint Privilege Management client and the EPM adapter. Package Manager can also automatically update when a new version is detected, taking even more burden off estate administrators.

In EPM, you can:

- Configure the Package Manager installation string
- Download the Package Manager installation executable
- Configure update settings for a computer group
- Track computer and computer group updates
- Set throttling and preferred update times so that updates can be strategically and safely installed.

When setting up auto update, you can complete the tasks in any order. The main configuration tasks are:

- Install Package Manager
- Set group updates

Overview

Package Manager is designed to check for updates on these components: EPM-M and EPM-W clients, EPM Adapter, and Package Manager.

- Package Manager checks in with EPM after the initial installation. This occurs within three minutes of the Package Manager installation.
- After the initial check-in, Package Manager checks in with EPM every two hours.

> ***Note:*** *Package Manager self-updates automatically when a new version is detected. There is no configuration required for Package Manager updates.*

An update may not take place for a number of reasons, including:

- The client or adapter is already updated to the version configured in EPM.
- The throttling threshold is reached and the endpoint must wait for updates.
- The computer group is not yet configured for updates to take place.
- Package Manager might not be enabled for the group.
- Automatic updates or updates to a specific version are not configured for the group.

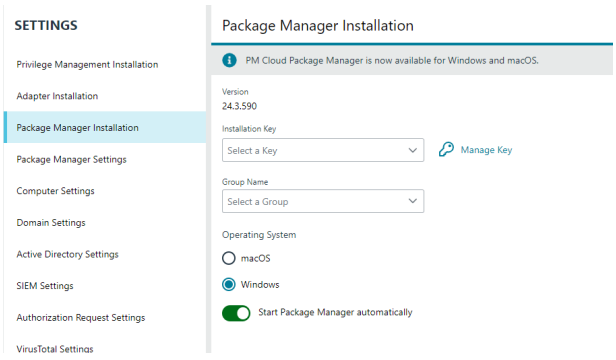
> ***Note:*** *Automatic updates do not work with adapters using the ic3Adapter user. Those adapters must be upgraded manually to version 21.8 and the ic3Adapter user changed to the LocalSystem user.*

Install Package Manager (Windows)

The Package Manager runs as a Windows service on the endpoint. The name of the service is **BeyondTrust Endpoint Privilege Management Package Manager**.

To install Package Manager:

1. Go to the **Configuration > Package Manager Installation** page.
2. Select an installation key and group name. These settings are required. Without both of these fields, Package Manager will not install.
3. Select the operating system: **macOS** or **Windows**.
4. Optionally, click the **Start Package Manager automatically** toggle to automatically start the Package Manager service running on the endpoint.
5. The install command is automatically populated with default settings based on the installation key and computer group.
6. Click **Download Package Manager**.



For more information about Endpoint Privilege Management for Windows installation commands, see "Install the Windows Adapter" on page 145.

Use Proxy Settings

You can pass the proxy settings as arguments to the Package Manager installer. Use the following parameters:

```
PROXYADDRESS=<proxyUrl|NONE|""> AUTODETECT=<true|false> USESYSTEMDEFAULT=<true|false>
BYPASSONLOCAL=<true|false> SCRIPTLOCATION=<script_location_url>
```

The proxy setting can be used by the adapter if the proxy setting is updated first, and then the adapter is installed by Package Manager. The Package Manager uses only the **PROXYADDRESS** parameter; all other parameters are saved for the adapter and not used by the Package Manager.

Restart Services

After resetting the Adapter or Package Manager, the respective service must be restarted.

***Note:** It is not recommended to reset both the Adapter and Package Manager on the same machine.*

Doing so causes the Adapter and Package Manager to attempt to activate and register with EPM, resulting in two active entries for the same computer.

In this scenario, stop the Package Manager service, uninstall the Adapter, and then reset the Package Manager. Once the Package Manager is active, the Package Manager installs the Adapter with the auto-update configuration.

Windows Adapter Reset Tool

The Adapter Reset tool is installed with Package Manager. Use the tool to reset the adapter to factory default values.

For more information, see "Reset the EPM Windows Adapter" on page 150.

Install Package Manager (macOS)

The Package Manager runs as a macOS process on the endpoint. The name of the process is **PMCPackageManager**.

Download Package Manager

1. Go to the **Configuration > Package Manager Installation** page.
2. Select an installation key and group name. These settings are required. The Package Manager install fails without these settings
3. Select **macOS**.
4. The install command is automatically populated with default settings based on the installation key and computer group.
5. Click **Download Package Manager**.
6. Click **Download script** or **Copy script to clipboard**.

Install Package Manager with MDM

After downloading Package Manager, complete the following steps to deploy macOS Package Manager via Mobile Device Management (MDM) software:

1. Access your MDM.
2. Upload the Package Manager package downloaded
    - To do this in Jamf, go to **Settings > Packages > Add**
3. Upload the script downloaded or copied.
    - To do this in Jamf, go to **Settings > Scripts > Add**
4. Create a policy to deploy the uploaded package and script.
    a. To do this in Jamf, **Computers** → **Policies** → **New**
    b. Add a policy name and select a trigger option.
    c. Configure the package section with the downloaded package.
    d. Configure the script section with the downloaded script.
    e. Ensure to select **Before** in priority section.
    f. Add a scope.
    g. Save the new policy.

Install Package Manager locally

After following the steps in Download macOS Package Manager, complete the following steps on the endpoint:

1. Using **Terminal.app**, run the downloaded script from the portal. For example:

```
sudo bash ~/Downloads/PrivilegeManagementConsolePackageManagerInstallerScriptForMac.sh
```

2. Run the downloaded Package Manager package.

> ***Note:*** *We strongly recommend using Mobile Device Management (MDM) software to deploy the macOS Package Manager.*

Install Configuration Profile into MDM

Most software deployed using MDM software requires a configuration profile deployed to ensure the correct permissions are set on the macOS endpoints. BeyondTrust provides a configuration profile for Packager Manager and EPM-M software to work correctly.

To deploy the configuration profile to macOS endpoints using an MDM:

1. Go to the **Configuration > Privilege Management Installation** page.
2. Download the **Privilege Management Configuration Profile for macOS** file. The minimum version required is 2.1.0.
3. Access your MDM software.
4. Create a configuration profile to deploy the configuration profile.
    a. To do this in Jamf, go to **Computers > Configuration Profiles > Upload**.
    b. Select the downloaded configuration profile.
    c. Click **Upload**.
    d. Add a scope.
    e. Save the configuration profile.

Uninstall Package Manager

To uninstall the macOS Package Manager for any reason, run the uninstall script similar to other BeyondTrust macOS products.

1. On an endpoint where the Package Manager is installed, run the following command with sudo access:

```
sudo /Applications/BeyondTrust/PMCPackageManager.app/Contents/Resources/uninstall.sh
```

The command removes all settings files of the Package Manager and the application but not any installed client or adapters.

Set Group Updates

There are two parts to setting up Package Manager on a computer group:

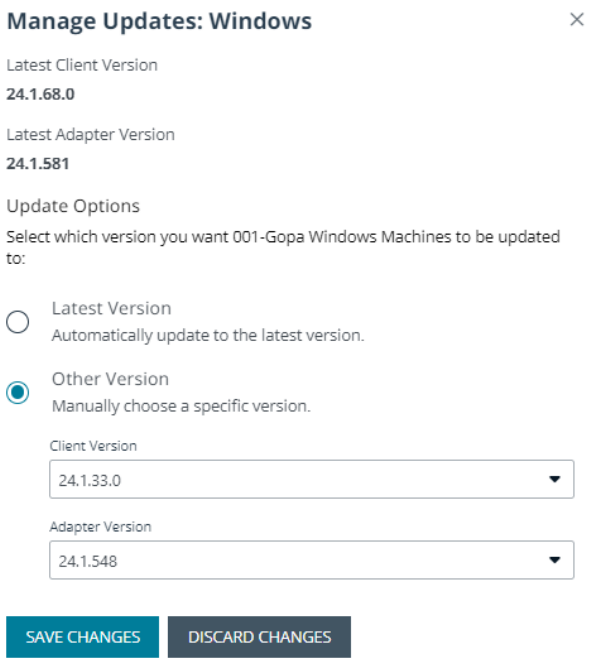
- Set the version to apply
  - **Latest version**: The connected computers try to install the newest version available.
  - **Specific version**: The connected computers try to install versions selected on the **Manage Updates** panel.
- Configure EPM-M and EPM-W installation parameters to include in the package

Package Manager self-updates automatically. No configuration is required.

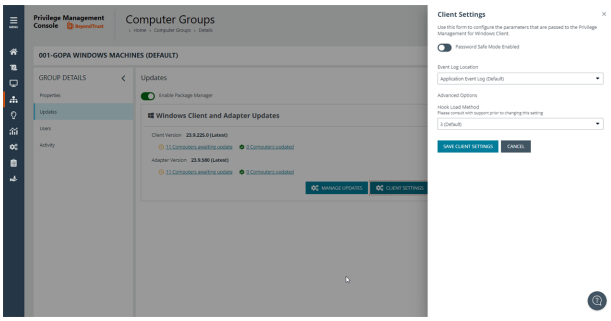
To configure a computer group to receive Package Manager updates

1. Go to **Computer Groups**, and then select the **View Group Details** menu for the group you want to set up.
2. Select the **Updates** tab.
3. Click the **Enable Package Manager** toggle.
4. After Package Manager is enabled, click **Manage Updates**.
5. Select the preferred method to update computers:
   - Select **Latest Version** to update Endpoint Privilege Management and the EPM Adapter to the latest version of each component.
   - Select **Other Version**, and select a specific version for the client and adapter. You cannot select a previous version after selecting and deploying a version; there is no downgrade process in place.
6. Click **Save Changes**.

   After setting up how the group will receive updates, there are specific installation settings for the endpoint that you can configure. Continue with the next steps.



7. Click **Client Settings**.
8. Select the options to apply to your endpoints.
9. Click **Save Client Settings**.



For more information:

For Endpoint Privilege Management for Windows installation settings, see the Administration Guide at https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-windows-admin.pdf.

For Password Safe configuration details, see Password Safe Integration Guide at https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-windows-ps-integration.pdf.

For macOS client settings, see Create a Package with Base Settings.

Track Computer Updates

A status displays during updates to help you determine the state of the update. The status of an update is displayed on the **Computer Groups** page and the **Computers** page in the following areas.

- **Computer Groups** page on the Update Settings
- **Computer Groups** page (Client/Adapter Status columns)
- **Computer Groups Details** page on the **Updates** tab
- **Computers** page (Adapter Status and Client Status columns)
- **Computer Details** page on the **Summary** tab

Status Messages at the Computer Groups Level

Status	Description
(Group is) Awaiting Updates	At least one of this group's computers have started updating and the remaining computers are expected to follow.
(The Group's) Update Failed	At least one of this group's computers has encountered an error during its update.
(Group is) Up to Date	Every one of this group's computers have been updated to the current settings for the group.
(Group is set to) Manual Updates	The Package Manager is not enabled for the group.

Status Messages at the Computer Level

Status	Description
(Computer is) Awaiting Update	• The Package Manager is enabled for the computer's group. • The Update Settings for the group are set (auto or specific version). • The Package Manager is actively checking into EPM to see if it needs to update the computer.
(The Computer's) Update Failed	An error occurred when the computer was trying to update. An error message is captured and sent to EPM to help diagnose the issue.
(Computer is) Up to Date	The computer is up to date with the Update Settings configured on its group.
(Computer is set to) Manual Updates	The Package Manager is not enabled for the computer's group.

Package Manager FAQ

What is the Package Manager and how does it work?	The EPM Package Manager is a piece of software which runs as a service on the endpoint, communicating with the EPM Agent Gateway similarly to the EPM Adapter. Its primary purpose is to facilitate the installation and upgrading of the EPM Adapter and Endpoint Privilege Management software on the endpoint, ensuring it stays in sync with the version configured in EPM.
What is the Installation Key and why do I need it?	Once Package Manager is installed on valid clients for a given service (URL) using an installation ID and key, the Package Manager will attempt to activate If the installation key is not valid, in that it does not match with the one originally provided for installation, then the Package Manager will not activate and will not be usable.
What happens if I install Package Manager to a group that doesn't have a version assigned?	If Package Manager is installed to an endpoint which is not configured to update the latest or a specific version of the EPM Adapter or Endpoint Privilege Management, then it will install successfully, but since the endpoint's group isn't assigned a version, it will not upgrade or install Endpoint Privilege Management or the EPM Adapter.
What happens if I try to install Package Manager without providing a group ID?	If you try to install Package Manager without a valid group ID, the installation is unsuccessful and you are alerted of the problem. Another installation attempt can take place with a valid group ID.
Is a reboot required after installing Package Manager?	Rebooting is usually not needed when installing Package Manager; however, a reboot might be necessary if the components managed by Package Manager require it. For example, a package like Endpoint Privilege Management may require a reboot depending on the state of the operating system. If you experience problems such as policy not being downloaded or applied, try rebooting as part of the troubleshooting steps.
How big is the Package Manager?	The Package Manager utility installer (MSI) file is approximately 75MB, and takes up 75MB of disk space on installation. The installer includes .NET 7.
How many endpoints can Package Manager update at any one time?	To prevent the Package Manager service from overloading, a rate limit of 5000 max connections at a time has been implemented. This way, only up to 5000 endpoints can check for updates at any given moment. The Package Manager Service can handle up to 5000 concurrent requests in a given instance. Before it can check for updates, each endpoint must first be authenticated, however the authentication service has a rate limit of 50 max connections. This means that not all endpoints may be able to authenticate, thereby limiting the number of concurrent requests that can be made. Additionally, under **Computer Groups > View Group Details > Updates** in EPM, users can set how many computers can update within an hour's time. This gives users real-time control and serves as a throttle control mechanism to protect their estate from getting flooded.
Why do we have 3 endpoint components?	Each EPM endpoint component serves a distinct purpose; Endpoint Privilege Management enforces policy on the endpoint, while the EPM Adapter is tasked with carrying communication between EPM and Endpoint Privilege Management. Furthermore, the EPM Package Manager is critical in managing the installation and upgrading of other components, providing fully automatic management, if desired.

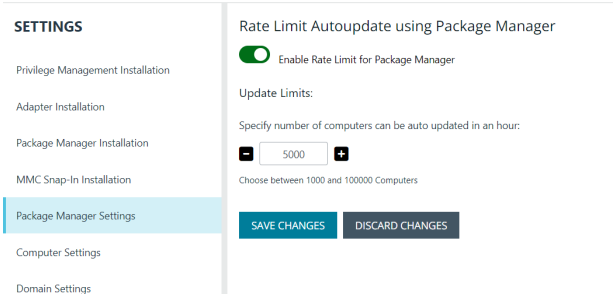
Can I install all 3 components at once instead of having the endpoint reach back to the platform?	All three components required for EPM can be installed manually, allowing the system to function fully; however, we recommend using Package Manager for the installation, as this can help eliminate a large amount of manual effort for updating Endpoint Privilege Management and the EPM Adapter.
What happens if an endpoint is offline or in an archived state?	If an endpoint is offline or in an archived state, nothing will occur. Once the endpoint is back online, Package Manager will check with EPM to determine if the group is configured for automatically-applied or specific-version updates, or if updates have been disabled for the group, and will proceed accordingly.
How long does it take for endpoints to start updating and is there a way to change this number?	Generally, once the Package Manager service is initiated, it begins scanning for updates within 3 minutes and continues to scan for updates every 2 hours thereafter. BeyondTrust Technical Support will have access to change this 2 hour number by running an update query to change polling increment, however we don't recommend changing this unless there's a tactical reason that addresses a production issue.
How do I see what endpoints have updated and what has not updated?	On the **Package Manager Settings** page, you can select a designated group to configure automatic or specific version updates. You can also switch off the Package Manager for that group. To track the progress of the updates, you can view details such as which endpoints have already been updated and which are pending.
How do I know if an install fails?	For the first version, we aren't surfacing errors into EPM; however, you can see how many endpoints have not updated for a specific group and view a list of those endpoints for further investigation. If an install fails, the error will be shown on the **Computers** page and **Group Details** page for a computer.
How can I understand why an install has failed?	The Package Manager creates an installation log file for each install or upgrade of the component, along with its own log file. In the event of a failure during the process, you can easily access the Package Manager log file and the installer log files located in the log folder. To ensure better error reporting functionality, we plan to include more robust error reporting features in our upcoming EPM release.

Package Manager settings

Set the rate limit when there is a large number of endpoints in your environment. Limit the number of endpoints that update at the same time to reduce the load on your network.

Set rate limit preferences

1. Go to **Configuration > Package Manager Settings**.
2. Click the **Enable Rate Limit for Package Manager** toggle.
3. Configure the number of computers to update on an hourly basis. We recommend using the default value of 5,000 computers.
4. Click **Save Changes**.



Computer Settings

Set Time to Change Status

The computer status tracks connections between computers and EPM. If a computer fails to connect to EPM, then the status changes to *Disconnected*.

As an IT systems engineer, set the length of time it takes for a computer to show as disconnected so that routine disconnects (weekends) are not investigated.

To set the status change timeframe:

1. On the sidebar menu, click **Configuration**.
2. On the **Settings** panel, click **Computer Settings**.
3. Enter the number of days that pass before the status changes to *Disconnected*. The default value is 2 days.

For more information, see "Manage Computers" on page 112.

Domain Settings

An email address is entered when a user account is created in EPM. Email notifications are sent for EPM user registration and confirmation.

IMPORTANT!

It is a security best practice to restrict the domains where EPM communications can be sent.

One domain always exists on the **Domain Settings** page. The first domain is created when the application is deployed for the first time for the customer.

Any additional domains added must exist in your authentication provider (Microsoft Entra ID or OpenID Connect) before you can add it here. If you add another domain, you can add an Administrator account associated with that domain.

Note: *Only a user assigned to the Administrator role can add a domain.*

To add a domain:

1. Navigate to **Configuration > Domain Settings**.
2. Click **Add Domain**.

Note: *A valid domain must contain at least 2 segments and be at least 3 characters long.*

3. Type the domain name, and then click **Add Domain**.

At any time after a domain is created, click the **x** to remove it. A toast notification indicates the domain is successfully removed.

There must always be at least one domain in the list.

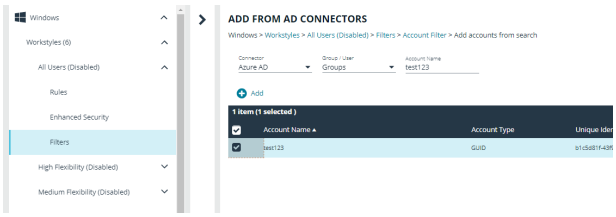
Active Directory Settings

Configure Active Directory (AD) connectors to discover AD groups in your estate. The Policy Editor queries the Active Directory to populate the group information when adding account filters or designated users.

There are two connector types:

- Microsoft Entra ID: Searches for Entra ID groups.
- **Local AD**: Searches for groups in the local Active Directory environment.

After the connectors are set up, the Policy Editor can discover and read information from the Active Directory source. The screen capture shows an example when adding an account filter for a workstyle.



Note: *A standard user requires delegated access to this page. For more information, see About user roles and resources.*

Add Microsoft Entra ID Connector

You must create an app registration in Azure before you can configure the Microsoft Entra ID connector here. There can only be one Microsoft Entra ID connector per PMC instance.

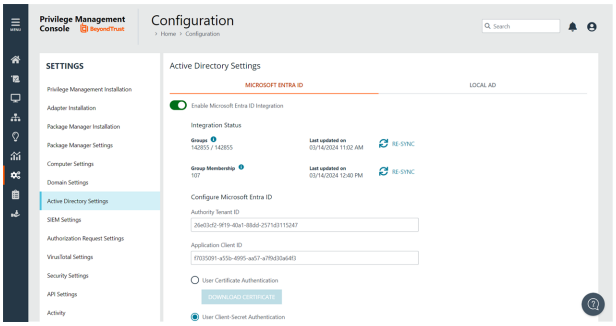
1. Go to **Configuration > Active Directory Settings**.
2. Select the **Microsoft Entra ID** tab, and then select **Enable Microsoft Entra ID Integration**.
3. Add the tenant ID and client ID.
4. Select an authentication method. This depends on the app registration details you configured.

For more information, see Microsoft's documentation Quickstart: Register an application with the Microsoft identity platform.

Monitoring Entra ID

On the **Microsoft Entra ID** tab, you can confirm if the integration with Entra ID is working correctly.

- Monitoring and health indicators help you to respond to issues as they occur.
- Synchronizing the Policy Editor group index and group membership ensures group information is accurate and current.



Add a Local AD Connector

Create an on-premises local Active Directory connector that can be queried from the Policy Editor. Adding a local directory makes it easier to add Active Directory users and groups to a policy.

- You must set up one connector for each local Active Directory.
- The connector installation is a Windows service installed to the endpoint. The endpoint requires access to the local directory.
- After the connector is installed and active, the connector is discoverable and available for use.
- If you disable a connector, then the Policy Editor can no longer query Active Directory.
- When deleted, the connector is no longer available in the console and must be reinstalled to be available for queries.

To install the local AD connector:

1. Go to **Configuration > Adapter Installation** to download the connector.
2. On the same page, click the **AD Connector** button to include the connector in the installation string.
3. After the download is complete, go through the installation wizard to complete the installation.
4. After the connector is installed, go to **Configuration > Active Directory Settings**, and select the **Local AD** tab.
5. You can edit properties for the connector. The host name is the computer name where the connector is installed; this cannot be changed. You can, however, add a name that is more meaningful.
6. After saving the connector properties, select the connector menu, and then select **Enable Connector**. The connector must be enabled before it can query the local AD environment.

Disable Local AD Connector

A disabled connector is no longer discoverable by the Policy Editor.

Disable a Connector

1. Select the **Configuration** menu, and then select **Active Directory Settings**.
2. Select the **Local AD** tab.
3. Find the connector in the list.
4. Select **Disable Connector** from the menu.

Edit Local AD Connector

You can change the name of the local AD connector.

The host name value cannot be changed.

Edit a Connector

1. Select the **Configuration** menu, and then select **Active Directory Settings**.
2. Select the **Local AD** tab.
3. Find the connector in the list.
4. Select **Delete Connector** from the menu.

Delete a Local AD Connector

Delete a local AD connector when it is no longer required. When deleted, the authentication details provided when adding the connector are deleted to ensure communication is no longer available between EPM and the local AD.

Delete Connector

1. Select the **Configuration** menu, and then select **Active Directory Settings**.
2. Select the **Local AD** tab.
3. Find the connector in the list.
4. Select **Delete Connector** from the menu.

SIEM Settings

Configure SIEM settings to send audit event data to an accessible SIEM provider. EPM supports the following SIEM providers:

- AWS
- Splunk
- Microsoft Sentinel
- QRadar

> ***Note:*** *There can only be one SIEM tool configured. If you choose to add details for a new SIEM tool, existing settings data will be lost.*

Events are queued and sent in batches in one-minute intervals. This is not configurable. A folder is created where the batches are saved. You can open and download the batch file, which stores the event data in JSON format.

Starting in EPM 23.1, the ECS mappings are updated for SIEM integrations.

If you previously configured SIEM settings and selected the ECS format, then there are two ECS format menu items: **ECS - Elastic Common Schema** and **ECS - Elastic Common Schema (Deprecated)**. To update to the new ECS schema, select **ECS - Elastic Common Schema**, and then click **Validate Settings**.

> *For a list of supported events in 23.1 and later, see PM Cloud ECS Event Reference at https://www.beyondtrust.com/docs/privilege-management/console/pm-cloud/ecs-events/index.htm.*

Event Types

Events include computer, activity, and authorization requests. Events are sent in the selected format (CIM or ECS).

> ***Note:*** *For SIEM integrations using the CIM format or ECS - Elastic Common Schema (Deprecated), we only support a subset of all event types (see the table below).*

The following events are logged by Endpoint Privilege Management:

Event ID	Description
100	Process has started with admin rights added to token.
101	Process has been started from the shell context menu with admin rights added to token.
103	Process has started with admin rights dropped from token.
104	Process has been started from the shell context menu with admin rights dropped from token.
106	Process has started with no change to the access token (passive mode).
107	Process has been started from the shell context menu with no change to the access token (passive mode).
109	Process has started with user's default rights enforced.
110	Process has started from the shell context menu with user's default rights enforced.
112	Process requires elevated rights to run.

Event ID	Description
113	Process has started with Custom Token applied.
114	Process has started from the shell context menu with user's Custom Token applied.
116	Process execution was blocked.
118	Process started in the context of the authorizing user.
119	Process started from the shell menu in the context of the authorizing user.
120	Process execution was canceled by the user.
199	Process execution was blocked, the maximum number of challenge / response failures was exceeded.

Configure AWS S3 Bucket

You must configure the S3 bucket details before you can configure the SIEM integration in EPM. In AWS, set up the bucket and access to the bucket. This includes:

- Create a bucket. When creating the bucket be sure to note the bucket name and region. You need to enter the information when configuring the settings in EPM.
- Create an access policy. When creating the access policy, the permissions required for the integration include: **PutObject**, **ListAllMyBuckets**, **GetBucketAcl**, and **GetBucketLocation**.
- Add a user. When attaching a user to a policy, be sure to select **Programmatic access** as the access type and **Attach existing policies directly** as the permission type. Copy the Access ID and secret access key to a file; you need to enter the details when configuring the settings in EPM.

For more information, see the following AWS documentation:

- *Create your first S3 bucket at https://docs.aws.amazon.com/AmazonS3/latest/userguide/creating-bucket.html.*
- *Creating IAM policies at https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create.html.*
- *Creating an IAM user in your AWS account at https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html.*
- *List contents of buckets*

Add the AWS S3 Bucket in EPM

1. Select **Configuration**, and then select **SIEM Settings**.
2. Select **Enable SIEM Integration** to turn on the feature.
3. From the **Integration Type** list, select **S3**
4. Enter the details for your storage site:
    - **Access Key ID:** Enter the value created when you added the user.
    - **Secret Access Key:** Enter the value created when you added the user.
    - **Bucket:** Enter the name of the S3 bucket.
    - **Region:** Select or search for the name of the region where your storage bucket resides.
5. Select the data format: **CIM - Common Information Model** or **ECS - Elastic Common Schema**.
6. Select **Server-Side Encryption** to encrypt files sent to the S3 bucket using the default AWS encryption key.

7. Click **Validate Settings** to test the connection to your storage site.
8. Click **Save Settings**.

If you no longer want the SIEM integration active, click **Enable SIEM Integration** to turn the feature off.

Add Splunk to EPM

1. Select **Configuration**, and then select **SIEM Settings**.
2. Select **Enable SIEM Integration** to turn on the feature.
3. From the **Integration Type** list, select **Splunk**.
4. Enter the details for your Splunk configuration:
    - Hostname. Do not include *https://* in the hostname.
    - Index
    - Token
5. Select the data format: **CIM - Common Information Model** or **ECS - Elastic Common Schema**.
6. Click **Validate Settings** to test the connection to Splunk.
7. Click **Save Settings**.

Add Microsoft Sentinel to EPM

1. Select **Configuration**, and then select **SIEM Settings**.
2. Select **Enable SIEM Integration** to turn on the feature.
3. From the **Integration Type** list, select **Sentinel**.
4. Enter the details for your Sentinel configuration:
    - **Workspace ID:** Enter the Sentinel workspace ID. In Sentinel, the workspace ID is located in this path: **Settings > Workspace Settings > Agents Management**.
    - **Workspace Key:** Enter the primary key. In Sentinel, the workspace key is located in this path: **Settings > Workspace Settings > Agents Management**.
    - **Custom Log Table Name:** The table is listed under the **Custom Logs** category in Azure Sentinel. A **_CL** suffix is automatically appended to the end of the custom log table name. A custom log is created if the table name does not exist.
5. Select the data format: **CIM - Common Information Model** or **ECS - Elastic Common Schema**.
6. Click **Validate Settings** to test the connection to Sentinel.
7. Click **Save Settings**.

Add QRadar to EPM

1. Select **Configuration**, and then select **SIEM Settings**.
2. Select **Enable SIEM Integration** to turn on the feature.
3. From the **Integration Type** list, select **QRADAR**.

4. Enter the details for your QRadar configuration:
    - Hostname. Do not include *https://* in the hostname.
    - Port
    - Cert: This is the client certificate required when sending events to a syslog server using mutual TLS (mTLS) authentication.
    - Key: This is the mTLS client certificate private key. The private key must be generated as PKCS #8.
5. Select the data format: **CIM - Common Information Model** or **ECS - Elastic Common Schema**.
6. Click **Validate Settings**.
7. Click **Save Changes** to confirm and save.

We recommend using our integration app to integrate EPM and QRadar.

> *For more information, see Integrate BeyondTrust EPM + IBM QRadar at https://www.beyondtrust.com/docs/privilege-management/integration/pm-cloud-ibm-qradar-integration/index.htm.*

Authorization Request Settings

Starting in EPM 24.3, authorization requests are available for ServiceNow tickets and native tickets.

There are two parts to configuring authorization requests:

- Configure authorization request settings (steps in this topic)
- Create an API account that includes access to URM APIs.

To configure the authorization request integration:

1. Go to **Configuration > Authorization Request Settings**.
2. To activate the integration, select **Enable Authorization Request Integration**.
3. From the menu, select **ServiceNow** or **Native URM**, enter the following:
    - **Host name:** The host name provided on the **Configuration** page in ServiceNow. Do not include *https://* in the hostname.
    - **Username** and **Password:** Enter the user account information you created in ServiceNow.
    - **Client ID** and **Client Secret**: Copy the values generated in ServiceNow.

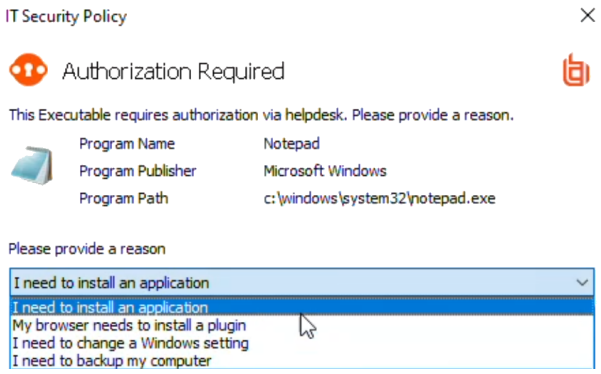
    Steps 4 and 5 are available in EPM 24.2 (and earlier). In version 24.3, client ID and client secret are generated in Configuration > API Settings.
4. Under **Notification API Configuration Details**, the **Tenant ID** and **Host Name** are auto-generated.
5. To create the **Client ID** and **Client Secret** used by the integration in ServiceNow, click the **Generate** button.
6. To confirm the connection, click **Validate Settings**.
7. Click **Save Changes**.
8. Go to **API Settings** to create the API account.

Use ServiceNow to Manage User Requests

Integrate Endpoint Privilege Management with ServiceNow to manage user requests. In a typical Endpoint Privilege Management scenario, the end user tries to launch an application that requires elevated privileges or falls outside of existing policy rules. With this integration, the user sends a request to run the application from EPM to their existing ServiceNow instance as a ticket.

The following ServiceNow ticket types are supported in the EPM integration: Incident, Change Request, Service Catalog - Task, and Service Catalog - Requested Item.

The screen capture shown here is an example of how the messages appear for the end user in a ServiceNow integration. Similar to other Application Rules in Endpoint Privilege Management, the user can select from a list of reasons for the request, or use free-form text.



Configuration includes:

- Download the BeyondTrust Endpoint Privilege Management Integration app from the ServiceNow store.
- Create a user account in ServiceNow, with required role.
- Activate and configure a connection to ServiceNow in EPM.
- Configure the connection details to EPM in ServiceNow.
- Create an Application Rule in the Policy Editor and apply messages to the rule that are specific to ServiceNow authorization.

Download and Install the Endpoint Privilege Management App

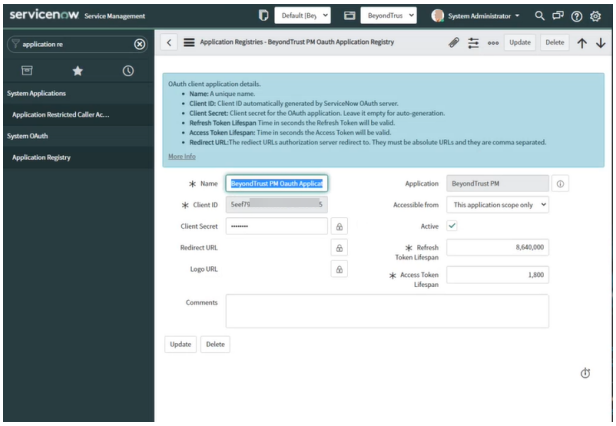
1. Go to the ServiceNow Store.
2. Search for *BeyondTrust*. The search displays all BeyondTrust products that integrate with ServiceNow.
3. Find the **BeyondTrust Endpoint Privilege Management Integration** app.
4. Download and install the app into your ServiceNow tenant.

Create an OAuth Client for EPM

> ***Note:*** *If the OAuth Client for EPM has not been created automatically, then install it using these steps. Otherwise, proceed to creating a user account in ServiceNow.*

EPM must be added as an OAuth client in ServiceNow.

1. In ServiceNow, go to **Application Registry**.
2. Configure the settings as shown.
3. Make note of the client ID and client secret. These values are needed for section Configure the ServiceNow Integration in EPM.



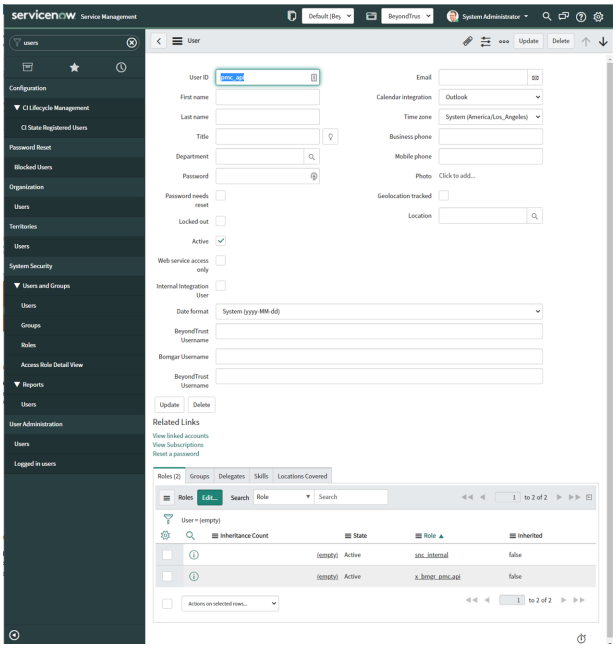
Create a User Account in ServiceNow

The **API Account** is used by Endpoint Privilege Management to submit requests via the inbound integration. An OAuth token is also created as an extra layer of security.

IMPORTANT!

*When setting up the user account, the **x_bmgr_pmc.api** role is required.*

1. Go to **User Administration > Users**.
2. Enter a **User ID** (**pmc_api**).
3. Enter a password.
4. Select **Web service access only** and click **Submit**.
5. Browse again to **User Administration > Users**.
6. Select the API user.
7. Click the **Roles** tab, and then click the **Edit...** button.
8. From the **Collection** list, add the **x_bmgr_pmc.api** role to the **Roles** list, and then click **Save**.



Assign Users Appropriate Roles

The following roles must be assigned to specific users in the ServiceNow integration:

- **x_bmgr_pmc.itil:** Assign to any users that will be providing technical support for the integration.
- **x_bmgr_pmc.admin:** Assign to any administrator users that you want to manage the ServiceNow integration.
- **x_bmgr_pmc.api:** Assign to API accounts that are used by BeyondTrust Endpoint Privilege Management to submit requests via the inbound integration.

> ***Note:*** *You must elevate the admin role to assign roles.*

To assign a role to a user:

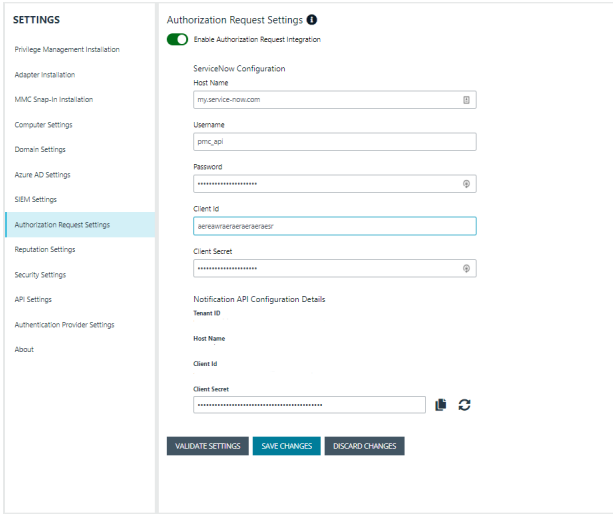
1. Go to **User Administration > Users**.
2. Select a user.
3. Click the **Roles** tab, and then click the **Edit...** button.
4. From the **Collection** list, add the appropriate role for that user to the **Roles** list:
    - **x_bmgr_pmc.itil**
    - **x_bmgr_pmc.admin**
    - **x_bmgr_pmc.api**
5. Click **Save**.

Configure the ServiceNow Integration in EPM

Before you can configure the connection to EPM in ServiceNow, you must generate the Client ID and Client Secret in the EPM console. You need this information to complete the configuration in ServiceNow.

Starting in EPM 24.3, client ID and client secret are generated in API Settings.

To configure the authorization request integration:



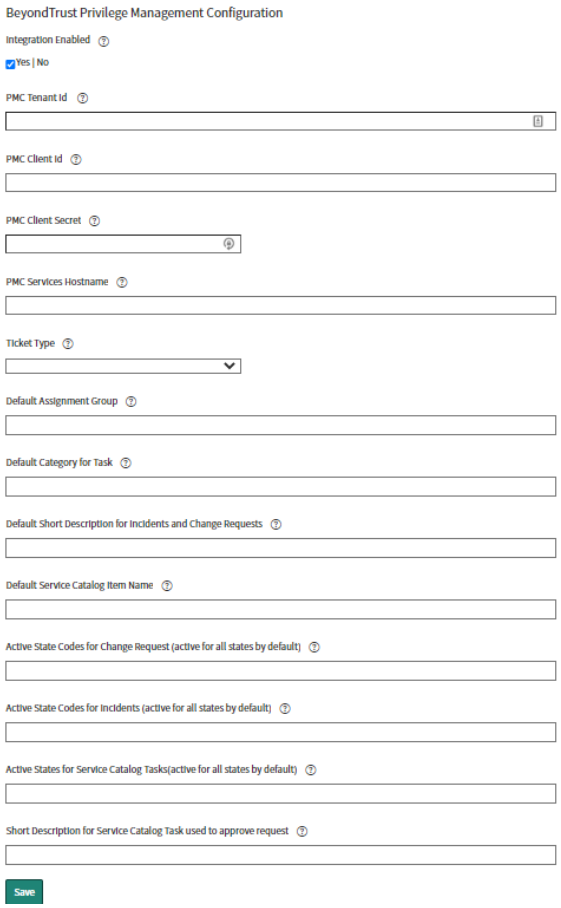
1. Go to **Configuration > Authorization Request Settings**.
2. To activate the integration, select **Enable Authorization Request Integration**.
3. Under **ServiceNow Configuration**, enter the following:
    - **Host name:** The host name provided on the **Configuration** page in ServiceNow. Do not include *https://* in the hostname.
    - **Username** and **Password:** Enter the user account information you created in ServiceNow.
    - **Client ID** and **Client Secret**: Copy the values generated in ServiceNow. See Create an OAuth Client for EPM.
4. Under **Notification API Configuration Details**, the **Tenant ID** and **Host Name** are auto-generated.
5. To create the **Client ID** and **Client Secret** used by the Integration in ServiceNow, click the **Generate** button.
6. To confirm the connection, click **Validate Settings**.
7. Click **Save Changes**.
8. To copy the **Client Secret** information, at the right of the **Client Secret** field, click the **Copy** button.

You can then proceed with configuring the connection to EPM in ServiceNow, and paste the Client Secret information you just copied.

> ***Note:*** *You must also manually copy and paste the Client ID information from EPM to the ServiceNow BeyondTrust Endpoint Privilege Management Configuration page.*

Configure the Connection to EPM in ServiceNow

An Endpoint Privilege Management instance is required for full operation. The appliance is setup in ServiceNow to connect ServiceNow with an EPM instance.

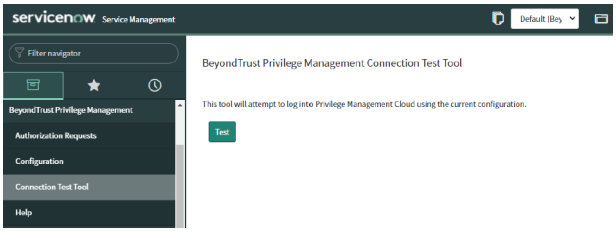


1. Go to **BeyondTrust Endpoint Privilege Management > Configuration**.
2. To turn on the integration to EPM, select **Yes**.
3. To configure the outbound integration, enter the following:
    - **PMC Tenant ID:** The Tenant ID of the Endpoint Privilege Management appliance.
    - **PMC Client ID:** The OAuth client ID that is used to authenticate to the Endpoint Privilege Management appliance. Copy and paste this from the EPM **Authorization Request Settings** page.
    - **PMC Client Secret:** The OAuth client secret that is used to authenticate to the Endpoint Privilege Management appliance. Copy and paste this from the EPM **Authorization Request Settings** page.
    - **PMC Service Host Name:** The hostname of the Endpoint Privilege Management appliance.
    - **Ticket Type:** The ticket type that is generated with a user authorization request. The ticket can be one of four types: **Incident**, **Change Request**, **Service Catalog - Task**, or **Service Catalog - Requested Item**.
4. To configure the application defaults (optional), enter the following:
    - **Default Assignment Group:** The default group assigned.
    - **Default Category for Task:** The default category for tasks created by the application. The default is **Software**.
    - **Default Short Description for Incidents and Change Requests:** The default short description created by the application when attempting to create an incident or change request based on the task type.
    - **Default Service Catalog Item Name:** The name of the service catalog item used when creating service catalog requests.
    - **Active State Codes for Change Request:** A comma-separated list of states in which the integration actions are available to users. This list is for change requests only. (For example,**Implement**).
    - **Active State Codes for Incidents:** A comma-separated list of states in which the integration actions are available to users. This list is for incidents only. (For example,**New**, **In Progress**).
    - **Active States for Service Catalog Tasks:** A list of states in which the integration actions are available to users. This list is for Service Catalog tasks only.
    - **Short Description for Service Catalog Task used to approve request:** The default short description, which is matched to place the custom form on the created application request.
5. Click **Save**.

Testing the Configuration

The ServiceNow Connection Test Tool verifies connectivity to the Endpoint Privilege Management host. It tests the Client ID and Client Secret.

1. Go to **BeyondTrust Endpoint Privilege Management > Connection Test Tool**.
2. Click **Test**.



Restrict Access to Applications

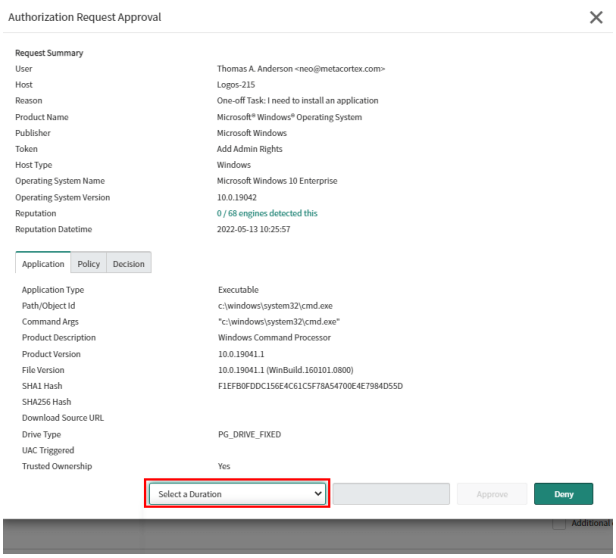
In the ServiceNow authorization request workflow, you can restrict access to application requests. On an approved request, Help Desk can set a time limit in the ServiceNow ticket. The time limit is the length of time the user can use the application before the approval automatically expires.

Under the **Application**, **Policy**, or **Decision** tab, select a Duration.

Access time limit can be one of the following:

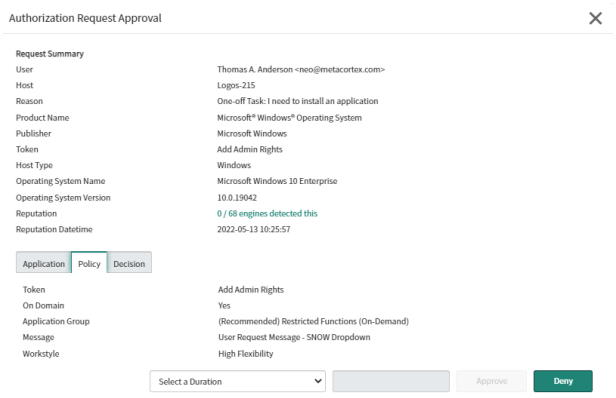
- **Once:** Permits access to the application only one time.
- **Hour:** Enter the number of hours the user will be permitted access, between 1 and 24.
- **Day:** Enter a day between 1 and 31.
- **Month:** Enter a month between 1 and 12.

Click **Approve**.



After the time expires, the user can no longer access that application. The user must go through the request workflow again, with the Help Desk personnel approving and selecting a duration time for access.

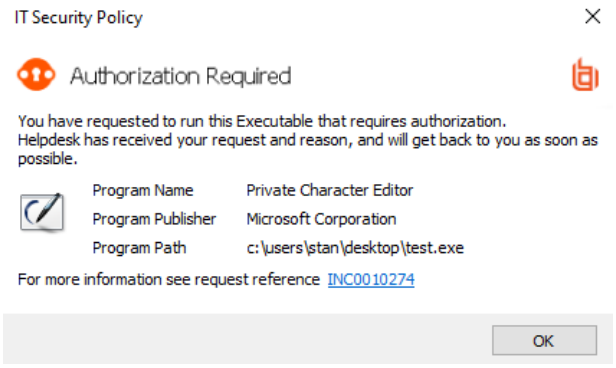
Duration settings are included in the authorization auditing.



The client checks an application's authorization access when the end user attempts to run the program. If the duration settings have been correctly configured, a message appears indicating the outcome of the ServiceNow request. The user receives a new message indicating that the application has been either Denied or Approved once the policy has been updated or when they attempt to run the application again.

A pending message displays to the end user until a decision on their request is made in ServiceNow.

To view the status on their ServiceNow ticket, the end user can click the request reference **link**.



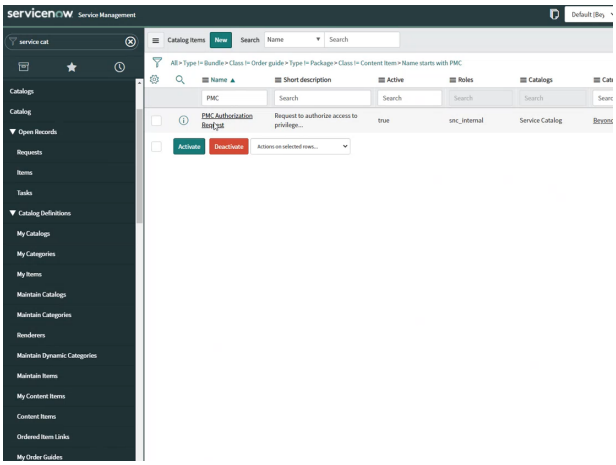
Use Service Catalog as the Task Type

You must configure the following if your ServiceNow infrastructure uses Service Catalog to manage user requests.

- In ServiceNow, select **Service Catalog - Requested Item** (or **Service Catalog - Task**) as the **Task Type** on the **Authorization Request Settings** page.

- In ServiceNow, you must add EPM as a Catalog item.

  Specific details on configuring the catalog item depend on your Service Catalog implementation.



Enable VirusTotal Reputation Score

You can enable the VirusTotal Reputation score on ServiceNow tickets to assist with identifying potential malware and malicious content.

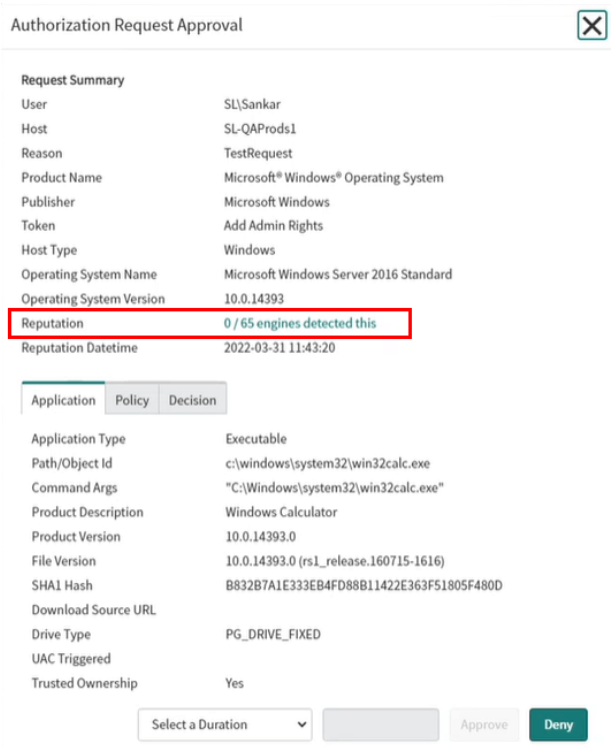
1. Go to **BeyondTrust Endpoint Privilege Management > Configuration**.
2. Select **Reputation Settings** from the menu.
3. Click the toggle switch **Enable VirusTotal Reputation Integration** to turn on the feature.
4. Enter the VirusTotal API key.

> ***Note:*** *You will need a VirusTotal license before you can generate an API key.*

5. Click **Validate Settings** to confirm that the key is valid.

Tip: *To view the VirusTotal score on a request, select the ticket in ServiceNow and then click* ***Authorization Request Approval*** *at the top of the incident grid. The VirusTotal reputation score is displayed under the* ***Request Summary****.*

You can click the score ***link*** *to go to the engine that determined the score.*



Create a Policy for ServiceNow Requests

With the ServiceNow authorization requests integration, when an end user tries to launch an application that requires elevated privileges or falls outside of existing policy rules, they can send a request which generates a ServiceNow incident to approve or deny.

The final piece to complete the ServiceNow and EPM integration is to create a policy that initiates the request process to ServiceNow.

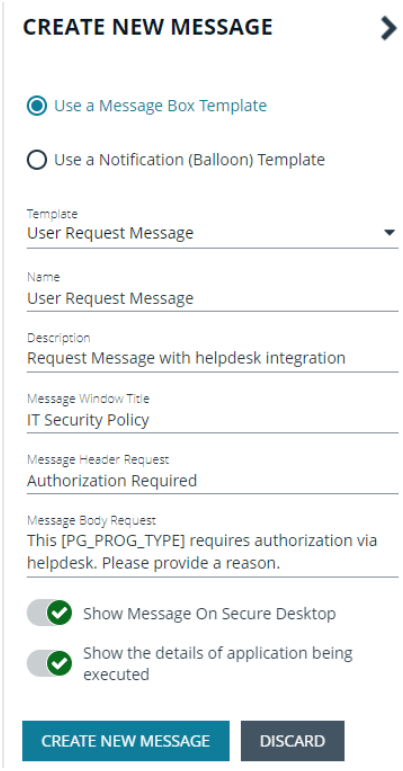
In this section, details include creating a message and setting up an application rule.

> *For more information, visit our customer portal and view the Knowledge Base article ServiceNow Authorization Request Workflow.*

Create a Message

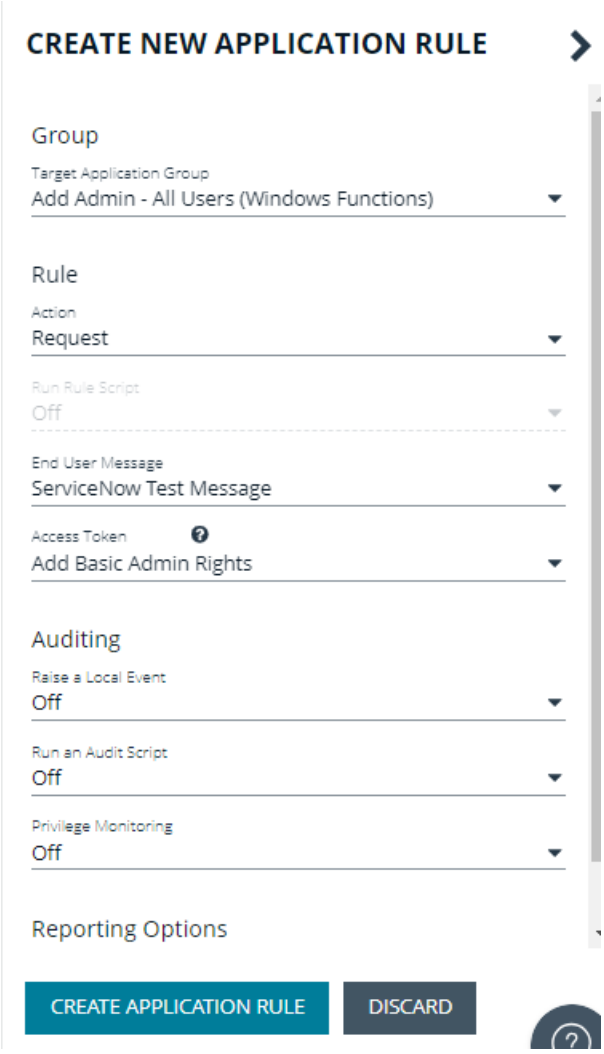
1. Select **Policies** from the menu, and then select **Create Policy**.
2. Go to **Messages > Create New Message**.
3. Create a message that uses the **User Request Message** template.
4. Enter a name and description.
5. Set up other message properties.

> *For more information, see "Messages" on page 79.*



Create an Application Rule

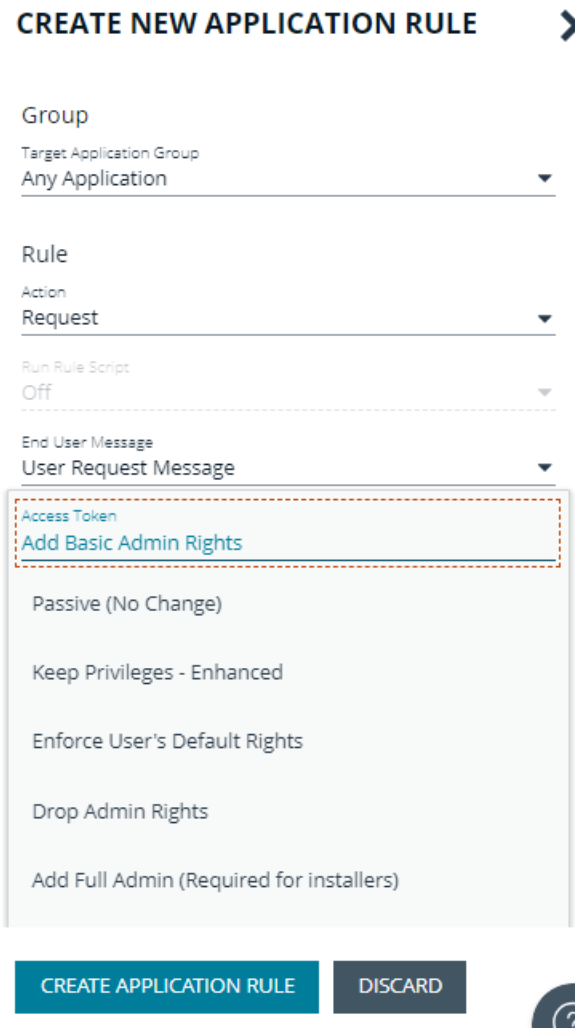
1. Select **Workstyles > (Workstyle Name) > Application Rules**.
2. Click **Create New**.
3. Select the rule properties.
4. In the **Rule** section, select **Action > Request**.
5. Select the message from the **End User Message** list.



6. Select an access token. This is the access that is granted when a user request is approved.

   For example, to run an installer the **Add Full Admin token (Required for installers)** is required so a user can run the full install process.

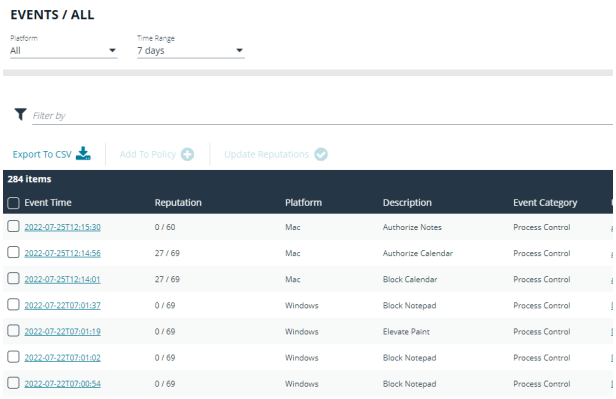
> *For more information, see "Workstyles" on page 35.*



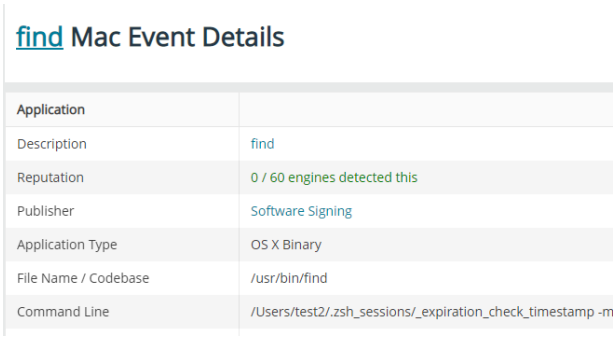
VirusTotal Settings

Using VirusTotal, EPM can provide scan analysis information based on application hash. The analytics gathered can help an organization determine whether an application is suspicious or malicious.

View results of the reputation findings on the **Events > All** reporting page. The **Reputation** column displays only when reputation is configured here.



Click the link for an event to view more details. Here, click the link for the reputation score to learn more about the VirusTotal scoring.



Set up VirusTotal

1. Go to **Configuration > VirusTotal Settings**.
2. Select **Enable VirusTotal Reputation Integration**.
3. Integrating with VirusTotal requires an API key. If you do not already have a key, click **Get Virus Total API Key**.
4. Click **Validate Settings**.

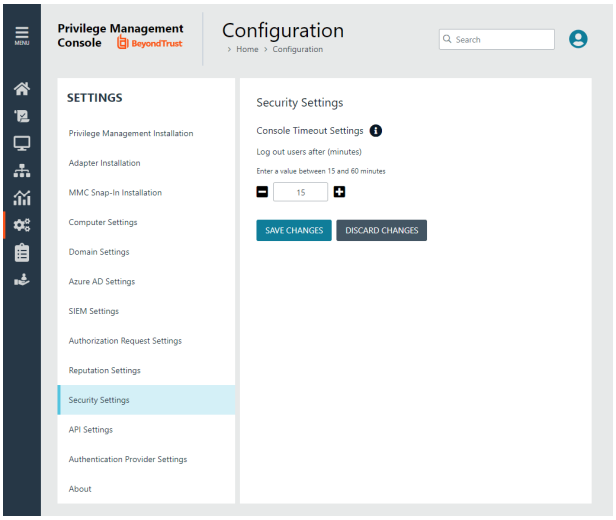
Security Settings

Depending on your network security, you might want to set a session timeout for EPM users. If a user is logged on to EPM but inactive, the session ends after the time period expires.

The timeout settings is global and applies to all EPM users.

To set the console timeout settings:

1. On the sidebar menu, click **Configuration**.
2. Click **Security Settings**.
3. Enter a time. The default value is 15 minutes.
4. Click **Save Changes**.



API Settings

The management API requires a secure account. Create an account in the EPM Configuration area.

> *For authentication information to access the API, see the EPM API Guide at https://www.beyondtrust.com/docs/privilege-management/console/pm-cloud/api/index.htm.*

Create an API Account

When using the EPM Management API, you must set up an account that is used to authenticate access to the API.

Not all API users will require full access to the API. Apply permissions to an account to avoid potential security risks. Configure permissions to the different areas of the API, including:

- Audit
- Insight
- Management
- Reporting
- SCIM
- URM

To create the account:

1. Click the **Configuration** menu, and then click **API Settings**.
2. Click **Create an API Account**.
3. Enter a name and description.

   The **Client ID** and **Client Secret** are automatically generated. The secret is only visible when initially generated for security reasons.

   You can use the copy icons to copy the values to the API tool you are using. You can access these after the account is created as well.

4. Set the permissions for the account.
5. Click **Save API Account**.

Generate a Client Secret

1. Click the **Configuration** menu, and then click **API Settings**.
2. Click the **Generate new Client secret** icon for the API account you use to access the API.
3. Click **Generate Secret**.
4. The client secret is displayed in the **Client Secret** column. Copy the secret to the authorization page of the API.

View API Account Details

View the API account details to see a snapshot of the account properties. The details include:

- Name and description
- Client ID
- Client Secret
- Access permissions

Edit an API Account

On the edit page for an API account, you can:

- Change the account name and description
- Copy the client ID
- Generate a client secret
- Change API access

To edit an account:

1. Click the **Configuration** menu, and then click **API Settings**.
2. Select **Edit API Account** from the menu.
3. Change the properties, and click **Save API Account**.

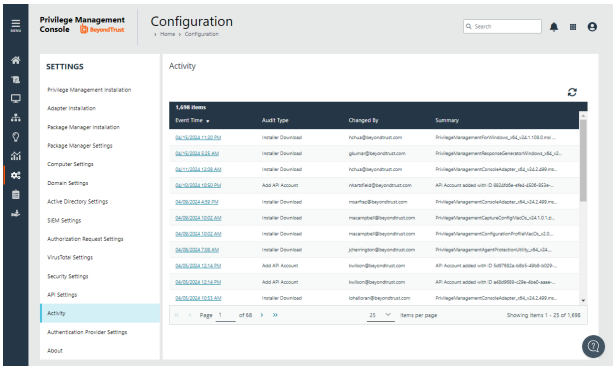
Delete an API Account

1. Click the **Configuration** menu, and then click **API Settings**.
2. Click the trash can icon to delete the account.
3. Click **Delete Anyway** on the confirmation dialog box.

Activity Page

The Activity page provides auditing details on areas in **Configuration**, and includes:

- Installer downloads
- Installation key creations
- API account delete, add, and update actions
- AD connector enable, delete, and update actions
- Changes to user timeout settings
- Add and remove domains



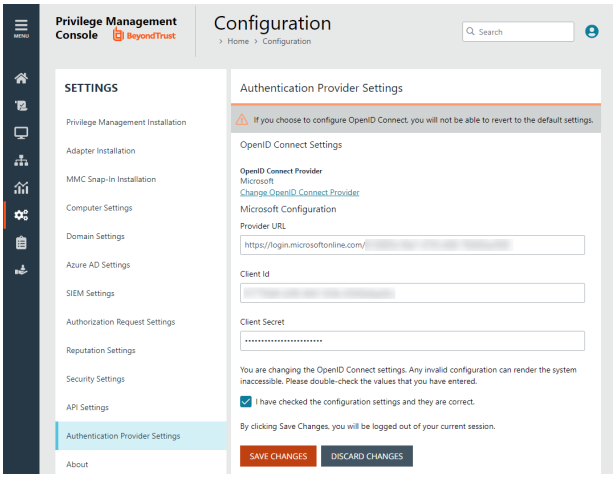
Configure OpenID Connect

EPM supports OpenID Connect authentication. You can change your authentication provider from the default AzureB2B to OpenID Connect, or update your OpenID Connect settings, without having to contact Support.

You must first set up an EPM instance in your OpenID Connect provider. Steps are provided in the section below.

Configure an Authentication Provider

When you start from the default configuration, use this procedure to set up the configuration.



IMPORTANT!

If you choose to configure OpenID Connect, you will not be able to revert to the default settings.

To set up an OpenID Connect provider:

1. Select the **Configuration** menu, and then click **Authentication Provider Settings**.
2. Click **Enable OpenID Configuration**. After you have completed and saved the OpenID configuration, this switch no longer appears on this page.
3. Enter information for the following:
    - **Provider URL:** Domain for the authentication. Currently supports Microsoft, Okta, Google, and Ping Identity.
    - **Client ID:** The client ID.
    - **Client Secret:** Secret key.
4. **Check the box**. We recommend reviewing the settings you configured. You can potentially lock yourself out of the system if the settings are incorrect. The **Save Changes** button is only available after you check the box.
5. Click **Save Changes**.

IMPORTANT!

*You will be logged out of the EPM console. Once logged out, you need to log back in within **15 minutes**, because there is a timer on the page. If you do not log in before the timer expires, the authentication provider settings revert to the previous settings and the new settings are **not saved**.*

If you log on before the timer expires, the newly added authentication provider settings are retained.

EPM OpenID Connect Workflow for New Customers

Here is the workflow to get up and running with EPM using OpenID Connect authentication.

- You will receive an email from BeyondTrust after the request is processed.
- In the email, click the link to open the **BeyondTrust OpenID Setup** page.
- Enter the OpenID Connect information: domain, client ID, and client secret. Click **Save Setup**. The OpenID credentials are saved.
- The Endpoint Privilege Management login page opens. Click **Log In**.
- EPM opens to the **Home** page.

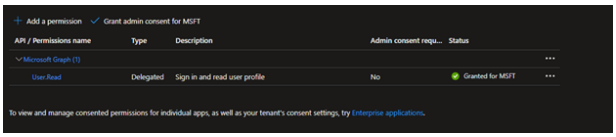
Add EPM to OpenID Connect Provider

EPM supports Microsoft Entra ID, Okta OpenID, Google, and Ping Identity Connect providers. The following sections provide a high-level overview on adding the EPM instance to your respective authentication provider. For complete instructions, refer to the provider's documentation.

Note: *The migration to OIDC will work when the email address sent from Okta or Entra ID matches for existing users. If email addresses are different or the domain name is not on the list of allowed domains in EPM, then the authentications will fail.*

Add EPM Instance to Microsoft Entra ID Tenant

1. Log into your Microsoft Entra ID (formerly Azure AD) tenant.
2. In the menu, click **App Registrations**.
3. Click **New Registration**.
4. Enter a **Name**.
5. Under **Supported account types**, select **Accounts in this org directory only**.
6. Enter the **Redirect URI**. While providing this now is optional and can be changed later, a value is required for most authentication scenarios.
    - From the dropdown list, select the **Web** platform.
    - Enter https://<*deployment*>-services.pm.beyondtrustcloud.com/oauth/signin-oidc where *deployment* is the name of your EPM tenant. For example, https://example-services.pm.beyondtrustcloud.com/oauth/signin-oidc
7. Click **Register**.
8. After EPM registers, select **Authentication** in the menu.
9. Add the following to the **Redirect URIs:**https://<*deployment*>-services.pm.beyondtrustcloud.com/oauth/signout-callback-oidc where *deployment* is the name of your EPM tenant.
10. Go to **Manage > API Permission**, and then select **Grant admin consent**.



11. Select **Certificates & secrets** in the menu.
12. Click **New client secret**, and copy the value. The value is visible until you leave the web page. When generating a new secret, you must select an expiry for the secret. We recommend selecting **Recommended: 6 months**

    After you add EPM to Microsoft Entra ID, you can get the information you need to set up the OpenID Connect authentication. The EPM OpenID connect setup wizard requires these values: **OpenID Domain**, **OpenID Client ID**, and **Open ID Client Secret**.

    Make note of these values before proceeding to step 13.

13. On the app registration **Overview** page, copy the client ID and the tenant ID.
    - **OpenID Domain:**https://login.microsoftonline.com/<Directory (tenant) ID>. The directory or tenant ID uses the format *31b8dbb9-fb8b-437a-8920-f23c8e0188b1*.
    - **OpenID Client ID:** Application (client) ID.
    - **OpenID Client Secret:** Client secret value.

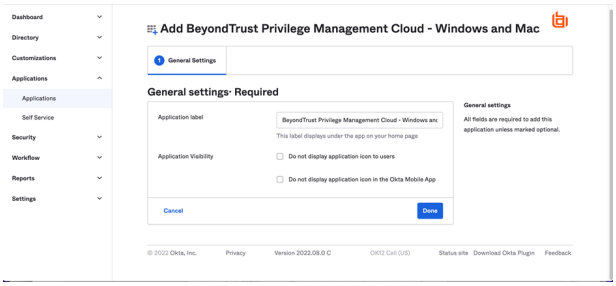
Add EPM Instance to Okta

Supported Features

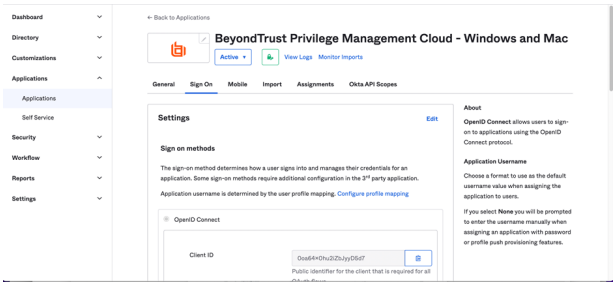
The Endpoint Privilege Management for Windows and Mac (also called EPM) - Okta integration allows logging into EPM platform using SP-initiated SSO flow.

Configure the Integration

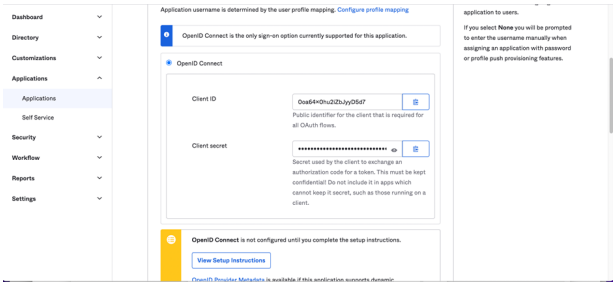
1. Access your Okta instance.
2. Navigate to **Applications**, and then click the **Browse App Catalog** button.
3. Search for an app called **BeyondTrustPrivilege Management Cloud - Windows and Mac**.
4. Click **Add Integration**.
5. Click **Done**.



6. While in the new application, navigate to **Sign On**, and then click **Edit**.



7. Navigate to the **Advanced Sign-on Settings** and provide the **Base Service URL** which follows the format https://{*deployment*}-services.pm.beyondtrustcloud.com/. (*deployment* is the name of your EPM tenant.) Click **Save**.
8. After you add the EPM App to Okta, you can get the information you need to set up the OpenID Connect authentication.

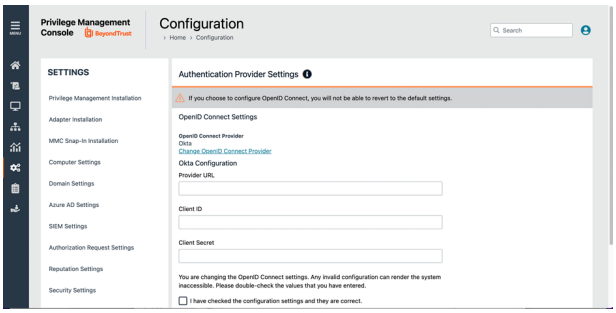


9. You must get the following information from the **Edit** page:
    - **Domain** or **Issuer**, for example, https://dev-12345.okta.com
    - **Client ID**

- **Client Secret**

> ***Note:*** *Confirm the domain name configured in Okta. This domain name might be different than the domain configured for your email address. For example, while the domain managed in Okta might be domain.com, the email address might be user@email.com. Both pieces of information are required.*

10. Log in to your EPM instance to complete the configuration. Navigate to **Configuration** and then **Authentication Provider Settings**.
11. Select **Okta** for the OpenID Connect Provider.
12. Provide the domain or issuer URL, client ID, and client secret.
13. Save and test the configuration.



Add EPM Instance to Ping Identity

> ***Note:*** *We currently support PingOne, the SaaS service from Ping Identity.*

1. Start up your Ping Identity instance.
2. In the menu, click **Connections**, and then click **Applications**.
3. At the right of the **Applications** title, click the plus sign (**+**) to add an application.
4. Enter a name for the application (required), and then add a short description (optional).
5. Select **OIDC Web App** and click **Save**.
6. Click the **Configuration** tab.
7. To edit the configuration, click the **pencil/edit** icon.
8. Under **Redirect URLs**, click **+ Add**, and then add the sign-in and sign-out URLs. If you are modifying an existing instance, you might need to open the **General** section dropdown first.
    - **Sign-in redirect URL:**https://{*deployment*}-services.pm.beyondtrustcloud.com/oauth/signin-oidc
    - **Sign-out redirect URL:**https://{*deployment*}-services.pm.beyondtrustcloud.com/oauth/signout-callback-oidc

    where *deployment* is the name of your EPM tenant.
9. Under **Token Endpoint Authentication Method**, select **Client Secret Post**, and then click **Save**.
10. Click the **Resources** tab.
11. To edit the resource, click the **pencil/edit** icon.
12. In the **Scopes** list, click the **+** next to **profile openID** to add it to the **Allowed Scopes**. You can also filter the list of options by **OpenID** to access this option.
13. Click **Save**.
14. To close the panel, at the top right of the **Edit** panel, click the **X**.
15. At the right of the new application entry, toggle the switch to **on** to give access to users.
16. Click the **Configuration** tab again. For the EPM OpenID Connect set-up wizard, you need to copy the following information from the **Configuration** page:
    - **Issuer:** Prefix the protocol HTTPS://
    - **Client ID**
    - **Client Secret**

Change Authentication Provider

After you set up an OpenID Connect provider (Microsoft, Okta, or Ping Identity), you might need to switch to another one at some point.

To change your existing OpenID Connect settings:

1. Click the **Configuration** menu, and then select **Authentication Provider Settings**.
2. Click **Change OpenID Connect Provider**.
3. Select a different provider, and then enter the **Provider URL (or Issuer)**, **Client ID**, and **Client Secret** information.
4. Review your settings, and then check the verification box.
5. Click **Save Changes**.

IMPORTANT!

*You will be logged out of the EPM console. Once logged out, you need to log back in within **15 minutes**, because there is a timer on the page. If you do not log in before the timer expires, the authentication provider settings revert to the previous settings and the new settings are **not saved**.*

If you log on before the timer expires, the newly added authentication provider settings are retained.

The About Page

The **About** page displays version information for the following EPM components:

- EPM console
- Policy Editor
- Privilege Management reporting

Overview

As an EPM administrator, add users that will be working in the various areas of the application based on roles and responsibilities:

- Security administrators to look after policy
- IT administrators to look after configuration like SIEM integration or ServiceNow integration

For example, in an international corporate infrastructure, IT administrators might be assigned assets based on region. In this scenario, organize computers regionally in groups and the assign the IT administrator in that region to that group.

When creating accounts, consider the responsibilities of the user and use the role based access model of EPM to create groups and assign roles.

Before Creating User Accounts

Before adding accounts, set up the following:

- All users that you want to add to EPM must exist in your authorization provider. Currently, Azure B2B and OpenID Connect are supported providers.
- Add a domain that can receive email notifications from EPM.

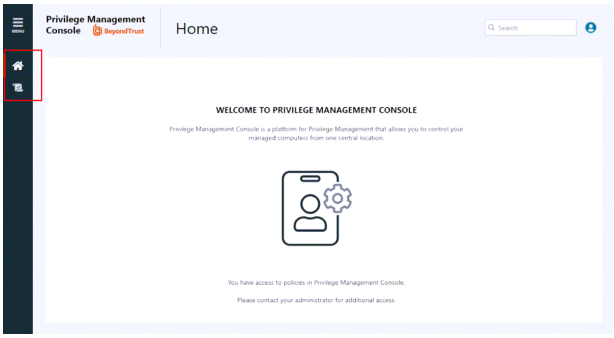
For Azure B2B, you must register an Azure tenant.

> *For more information, see Microsoft's documentation Quickstart: Register an application with the Microsoft identity platform.*

About user roles and resources

In the role-based access control (RBAC) system, the role assigned to a user dictates the features the user can access.

Main menu items and icons that appear on the left depend on the role assigned to a user. For example, if you only assign access to policies for a standard user, when logging in the user sees only the **Home** and **Policies** menu items.



User roles

Determine the role and responsibilities of a user. There are two user types:

- **Administrator**: An administrator can access all areas of EPM. An **administrator** user does not require any additional setup for roles and resources, as this account can access and manage all areas of the system.
- **Standard User**: A standard user has delegated access based on the resources assigned to the user.

Resources

Computer Groups

The following computer group roles can be assigned to a standard user, for either all groups or individually selected groups.

Role	Menu access to	Description
Assign Policy to Group	Home, Policies, and Computer Groups	User can view policies and computer groups, and assign policies and revisions to selected computer groups.
Analyze Group	Home, Computer Groups and Analytics	User can view data analytics for selected computer groups. Access to Analytics 1.0 is restricted. A user requires the **Analyze Groups** permission for *all* groups for a user to see Analytics 1.0.
Create Groups	Home and Computer Groups	User can create, edit, and view selected group properties.
Edit Group	Home and Computer Groups	User can view and edit selected computer group properties.
View Group	Home and Computer Groups	User can only view selected computer groups. This option is automatically selected when any of the other options are selected.

Policies

The following policies roles can be assigned to a standard user, for either all policies or individually selected policies.

Role	Access to	Description
Create Policies	Home and Policy	User can create, edit, and view selected policies.
Edit Policy	Home and Policy	User can view and edit selected policies.
View Policy	Home and Policy	User can only view selected policies. This option is automatically selected when the edit option is selected.

Configuration Settings

As an administrator, delegate access to configuration settings so that the user only sees the resources they need access to. A standard user can be assigned edit and view permissions on each of the configuration areas of EPM.

Assign a standard user the **Edit Setting** permission when they need to access and change settings for a particular configuration setting.

A standard user can see but not interact with settings when assigned the **View Setting** permission.

The user will not see the configuration setting if neither edit nor view is selected.

> ***Note:*** *The **About** configuration setting cannot be assigned edit permissions. All standard users can see **About** information but they cannot change the information on the **About** page.*

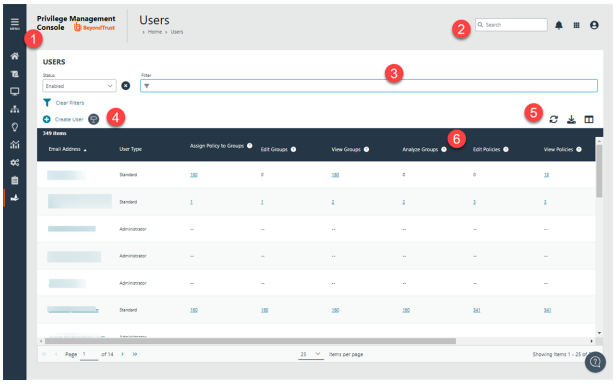
Automatic Role Mappings on Upgrade

When upgrading from EPM 22.7 and earlier to version 22.8 and later, existing roles will be mapped as follows.

22.7 and Earlier Role	22.8 and Later Role and Access
Administrator	Administrator
Computer Administrator	Group Editor and Viewer, Policy Viewer and Assigner
Policy Administrator	Group Viewer, Policy Editor, Policy Viewer, Policy Assigner, Analytics
Policy Editor	Group Viewer, Policy Editor and Viewer, Analytics
Standard User	Group Viewer, Policy Viewer, Analytics
Automation Client	Automation Client

For more granular access, manually edit users and assign access to computer group and policy records.

The Users Page



1. **Sidebar:** Easy access to all pages in Endpoint Privilege Management, including the Home, Policies, Computers, Computer Groups, Management Rules, Analytics, Configurations, Auditing, and Users pages.
2. **Header:** Enter keywords to run a global search across computer groups, policies, computers, and users, view your notifications, access your connected apps, and set your account preferences.
3. **Filters:** Click the drop arrow to select a filter type. The selected filter displays to the left of the drop-down.
    - **Clear Filters:** Click to remove all filters and search results
    - **Filter types**
        - **Name:** Enter all or part of a policy name.
        - **Locked By:** Enter an email address to view all policies locked via that account.
        - **Created:** Select a date from the date selector that displays to the left of the Filter drop-down to view all policies created on that day.
4. **Create a User:** Click to create a new user.
5. **List options:** Click to refresh the users list, to download list of the displayed users to a .csv file, and click to select which columns you want to display on your **Users** page.
6. **Users list columns:** Not all columns display in the image above.
    - **Column names**
        - **Email Address:** The email account used to register the user.
        - **User Type:** Indicates if the user is an administrator or standard user.
        - **Assign Policy to Groups:** The number of computer groups the user can assign policy to.
        - **Edit Groups:** The number of computer groups the user can edit.
        - **View Groups:** The number of computer groups the user can view information for.
        - **Analyze Groups:** The number of computer groups the user can view data analytics on.
        - **Edit Policies:** The number of policies the user can edit.
        - **View Policies:** If a policy is locked, this displays the period (in days or months, if longer than 3 weeks) when the policy was last locked.
        - **View Settings**: The number configuration settings the user has permission to view.
        - **Last Logged In**: The time and date the user last logged on to the EPM console.
        - **Create Groups**: Indicates if the user has permission to create computer groups.
        - **Create Policies**: Indicates if the user has permission to create policies.
        - **Edit Settings**: Indicates if the user has permission to edit configuration settings.
        - **Status**: The status of the user account: enabled or disabled.
        - **Language**: The language preference selected in account preferences.

Create a user

Once the initial administrator account is created and authorized, you can create additional user accounts in EPM with whichever roles are needed. You can also create future accounts with the **Administrator** role by following the same process outlined below.

Create an account

To create a user account:

1. On the sidebar menu, click **Users**.
2. Click **Create User**.
3. Choose whether you want to create the user from a blank user profile or base it on an existing user profile.
4. To use an *existing* profile, select a user from the list, then proceed to the **User Details** section. Later, you can review the profile's **Roles and Resources** setup, or modify it as needed.
5. In the **User Profile** section, enter general account information, like email address and time zone.

> ***Tip:*** *You can click **Create User** after this step. If you create a standard user account without assigning any resources, the user can log in to EPM, but cannot access any resources. A message indicates to contact their administrator to request access to EPM. It is better to continue with the following steps and grant some access to the new user.*

6. Click **Next: Roles and Resources**.
7. In the **Roles and Resources** section, select a user type:
    - **Administrator**: The user can access and manage all areas of the system. Click **Create User** to complete the process.
    - **Standard User**: The user can only access and manage resources that you identify in the next steps.
8. Under **Computer Groups**, select either **All Computer Groups**, or select *individual* groups and roles.
    - If you select **All Computer Groups**, select one or more roles from the **Computer Groups Role** list. The user will have the role(s) across all existing and future computer groups. The **View Groups** role is automatically selected with any of the other options.
    - If you want to select *individual* groups and roles, check the boxes for the roles to associate with each group selected. You can shorten the list by selecting the **Name** filter option, and then typing into the **Name** box.
9. Under **Policies**, select either **All Policies**, or make *individual* policy and role selections.
    - If you select **All Policies**, select one or more roles from the **Policies Role** list. The user will have the role(s) across all existing and future policies. The **View Policies** role is automatically selected with any of the other options.
    - If you want to select *individual* policies and roles, check the boxes for the roles to associate with each policy selected. You can shorten the list by selecting the **Name** filter option, and then typing into the **Name** box.
10. Under **Settings**, select the configuration items the user needs access to.
11. Click **Create User**.

    An email notification is sent to the user. The user must click the **Get Started** button to go to the invitation landing page. After clicking **Accept**, the user can log on to EPM using their credentials.

Resend an Email Invite

An email invitation can be resent to a user that has not accepted their invite to the EPM portal.

On the **Users** page, select the user, and then select **Resend Email Invite**.

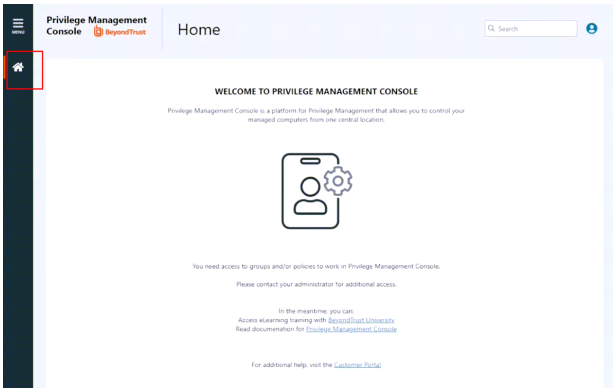
> ***Note:*** *There is no limit on how many times an invitation can be sent to a user.*

Edit a User's Profile

As an administrator user, you can edit user account properties including roles and resources for a user account.

1. On the sidebar menu, click **Users**.
2. Locate the user account you want to edit. Use the filter option to reduce the list size.
3. Select **Edit User** from the menu.
4. Click **Next: Roles and Resources**.
5. Make the role and resources changes, and then click **Save Changes**.

If you remove all access for a standard user account, the user can log in to EPM, but cannot access any resources. A message indicates to contact their administrator to request access to EPM.



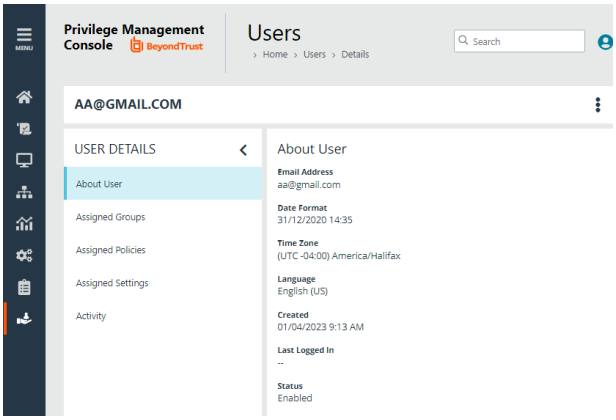
View a User's Details

You can view information about a user account such as: email address, create date, and status.

To get a quick at-a-glance view of recent activities for a user, click the **Activity** tab. You can see the event time, audit type, and summary information on the action that occurred.

The information displayed on the **User Details** page varies depending on the user role and responsibilities.

Change the properties for a user account such as email address, date format, and time zone. The changes will take effect the next time you log on to EPM. You can also change these properties from the user account menu.



Disable a User

Disable a user account when they no longer require access to EPM or if they leave the company.

1. Go to the **Users** main page.
2. Select the user account, and then select **Disable** from the menu.

If you need to reinstate the user account, select **Enable** from the menu to reverse the action.

Analytics

IMPORTANT!

In the situation of excess endpoint audit event generation (as determined by the policy configuration), which is deemed likely to have a severe impact on overall performance and availability of the EPM console, BeyondTrust will take measures to ensure ongoing availability and functionality of the EPM console.

An EPM SaaS instance is capable of supporting event ingestion at the rate of approximately 720,000 events per hour, or 17.28m per day. Beyond this, if server performance is degraded, your instance will automatically begin refusing events. Those events are queued on each endpoint, up to a maximum of 25,000 queued events. Events generated beyond 25,000 are lost permanently.

To minimize the potential of queued and/or lost events, event generation should be configured in policy to be within the range outlined above. Analytics in the EPM Windows and Mac SaaS console will be able to provide you with event generation insight.

Should BeyondTrust need to take further non-automated action to maintain server availability and stability, a support ticket will be raised on your behalf, and a representative from our Support organization will reach out to make you aware of the situation and to work with you to make any recommended policy changes, if required.

Overview

The following views are available:

- **Events**: Shows all activity from Endpoint Privilege Management that you have chosen to log to EPM.
- **Applications**: An application is a grouping of events with the same application type. On this tab, see how different applications are used and controlled across all your machines, by all your users in a single row of data.
- **Users**: Shows user logon information.

Note: *A standard user requires delegated access to this page. For more information, see About user roles and resources.*

Applications Data

The following application types are shown in the **Applications** tab. From here you can easily make policy amendments, using our recommended matching criteria for applications.

Applications are aggregated using the most appropriate criteria for each application type as shown below.

Windows Application Types

Application Type	Aggregation Criteria
Executable (exe)	• Application name • Application description • Publisher

Application Type	Aggregation Criteria
	• Admin required
COM Class (com)	• CLSID • COM Display Name • Publisher • Admin required
Installer Package (msi)	• Application description • Upgrade code • Publisher • Admin Required
Uninstaller (unin/unex)	• App Description • Product Name • Publisher • Admin Required
Store App (appx)	• Publisher • Admin Required • Store App Name
Windows Service (svc)	• Service Display Name • Service Action • Publisher • Admin Required
Control Panel Applet (cpl)	• Publisher • Admin Required • App Description
Management Console (msc)	• Publisher • Admin Required • File Path

macOS Application Types

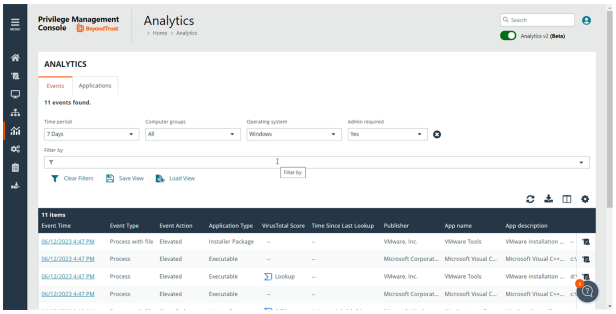
Application Type	Aggregation Criteria
Binary (bin)	• Publisher • Authorization Required • File Path

Application Type	Aggregation Criteria
Bundle (bund)	• Publisher • Authorization Required • Application Name • Application Description
Package (pkg)	
System Preference Pane (pref)	

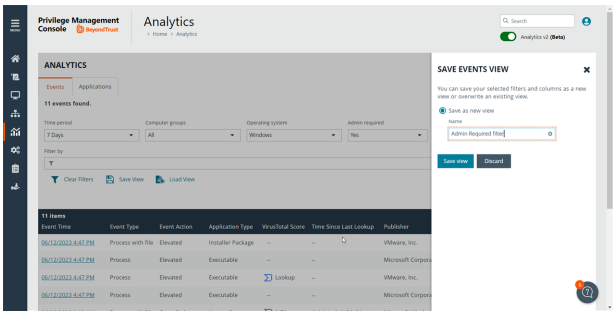
Walkthrough

This section shows the high-level steps on how to create and save views using your favorite filters and refine the scope of your Endpoint Privilege Management policy.

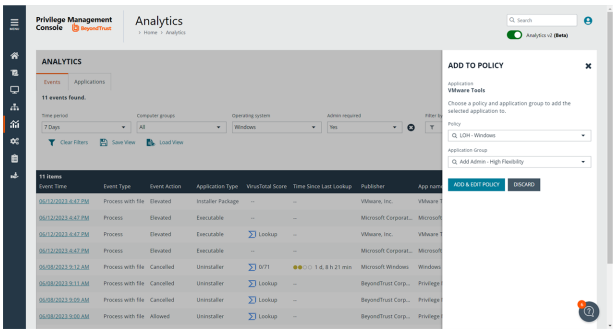
1. Select the filters that display the details you want to track. In this scenario, a view is created to show all Windows computers with **Admin required** set to **Yes**. Use the column chooser to add/remove the columns you want in your view.



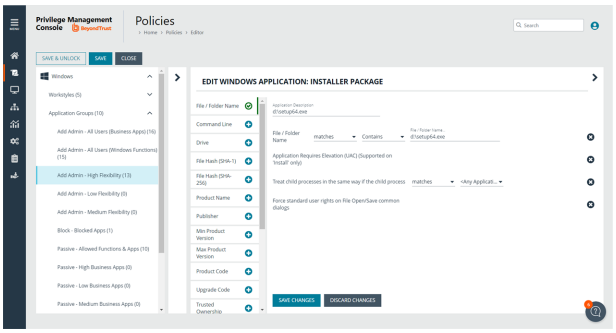
2. Save the favorite filters to a view so you can easily come back to that view at any time and display the most recent data.



3. Click the **Add to Policy** icon to update your policy dynamically, and add the event or application to your policy. Select the policy name and application group.



4. The Policy Editor opens to the Application Group editor. The **File / Folder Name** properties are populated with the application information. You can change other application properties as required.



Create and Add Users to Computer Groups

As an EPM administrator, use role-based access control (RBAC) when you want your policy administrators to see events only for the computer groups they manage.

When creating a user, select a **Standard** user account type. From the **Computer Groups Roles** list, select **Analyze Groups**.

> ***Note:*** *A standard user requires delegated access to this page. For more information, see About user roles and resources.*

Filters

There are two types of filtering:

- **Default**: The default filters are: **Time period**, **Computer groups**, **Operating system**, **Application Type** (on the Applications grid only).
- **Optional**: There is an extensive selection of filters which can be selected and configured at time of viewing.

Overview

Select the data you want to view by choosing the time period, a computer group, and operating system. Select and set filters to further refine the data displayed in the view.

The dynamic filtering provides a *search-as-you-type* feature that helps you to quickly and easily narrow the scope of the data set displayed. You must type at least three characters in the dynamic filter box of an optional filter for an auto suggestion to populate. You can then click on an auto suggested field to help you narrow the scope of the data set. The search as you type filtering is available for the following filter types:

- App description
- App Name
- Host Name
- Host Domain
- Publisher
- User Name

The *search-as-you-type* feature is also available for these optional filters (only on the **Applications** grid):

- COM Display Name
- Service Display Name
- Service Name
- Store App Name

The following optional filters require a minimum of five characters. Matches are displayed in the grid.

- Command line
- File Path
- Executable Path
- User Reason

Filters List

Default filters

Event filters

Application filters

Application Type Specific Filters and Columns

Default Filters

Name	Description
Time Period	From now back to a selected value.
Computer Groups	View All or selected Computer Groups. Admin users can see data for all groups. Standard users can see data only from groups for which they have the **Analyze Group role**.
Operating System	Windows or macOS.
Application Type	The type of application as defined in your policy. Displays options relevant to selected operating system. Default for **Applications** tab only (optional for **Events** tab).

Event Filters

The filters are grouped into the following categories:

- **Event**: The action Endpoint Privilege Management took.
- **Application**: Properties of the running application.
- **Policy**: The Endpoint Privilege Management policy controlling the action.
- **User**: The user running the event.
- **Computer**: The machine the event is running on.

The filters listed here are optional.

Name	Category	Description
Event Action	Event	Filter by the action that Endpoint Privilege Management took for a process, as instructed by your policy. For Windows these actions are: • Allowed • Elevated • Elevated - Custom Privileges • Blocked • Cancelled • Self-Elevated • Self-Elevated - Custom Privileges

Name	Category	Description
		Run As Alternate User For macOS these actions are: • Allowed • Passive • Blocked • Cancelled
Event Type	Event	The type of event that Endpoint Privilege Management has reported or controlled: • Process • Process with file • COM Class • Service • ActiveX • DLL • Content • Challenge Response Failed Privileged Account Modification Prevented User Logon Agent Start Agent Stop Unlicensed
Admin Required (Windows)	Application	Yes/No Endpoint Privilege Management detected that the process or application required elevation.
Application Type	Application	The type of application as defined in your policy.
App Name	Application	The **Product Name** property of the executable (for applicable event and application types).
App Description	Application	The **Product Description** property of the executable (for applicable event and application types).
Command Line	Application	The command line captured at execution time.
Executable Path	Application	The path of the executable (the process started).

Name	Category	Description
File Path	Application	The path of any file passed as an argument to a launching process.
Publisher	Application	The publisher of the executable.
Application Group Name	Policy	The name of the application group matched as defined in policy.
Message Name	Policy	The message shown to end user.
On Demand	Policy	Whether the rule applied was an Application Rule (ran normally) or an On-Demand Rule (ran via right-click and Run as Administrator). Yes: On-Demand Rule No: Application Rule or N/A
Policy Name	Policy	The name of the policy applied.
Policy Revision	Policy	The revision of the policy applied.
Workstyle Name	Policy	The name of the Workstyle applied to this event as defined in policy.
User Name	User	User name
User Domain	User	User domain
User Reason	User	The reason provided by the user via the Endpoint Privilege Management message (if configured).
Host Name	Computer	Computer name on which the event took place.
Host Domain	Computer	Computer domain on which the event took place.

Application Filters

The filters listed here are optional.

Name	Category	Description
Event Action	Event	Filter by the action that Endpoint Privilege Management took for a process, as instructed by your policy. For Windows these actions are: • Allowed • Elevated

Name	Category	Description
		• Elevated - Custom Privileges • Blocked • Cancelled • Self-Elevated • Self-Elevated - Custom Privileges • Run As Alternate User For macOS these actions are: • Allowed • Passive • Blocked • Cancelled
Admin Required (Windows)	Application	Endpoint Privilege Management detected that the process or application required elevation. Yes/No
Authorization Required (macOS)	Application	Endpoint Privilege Management detected that the process or application required Authorization macOS only Yes/No
App Name	Application	The **Product Name** property of the executable (for applicable event and application types).
App Description	Application	The **Product Description** property of the executable (for applicable event and application types).
Downloaded	Application	Was the file downloaded? (has the mark of the web) Yes / No
Drive Type	Application	The type of drive an application or file was run or loaded. • Fixed Disk • CDROM Drive • Network Drive • USB Drive • RAM Drive • eSATA Drive

Name	Category	Description
		• Unknown Drive
Publisher	Application	The publisher of the executable.
Application Group Name	Policy	The name of the application group matched as defined in policy.
Message Name	Policy	The message shown to the end user.
On Demand	Policy	Whether the rule applied was an Application Rule (ran normally) or an On Demand Rule (ran via right click and Run as Administrator) Yes: On Demand Rule No: Application Rule or N/A
Elevation Method		How the application gained elevated rights. Possible values Windows: • Admin Account • On-Demand • Auto-Elevated • Not Elevated Possible values macOS: • Manually-Authorized • Auto-Authorized • Not Elevated

Application Type Specific Filters and Columns

In the **Applications** grid there are some filters and columns specific to the selected application type. These are available automatically when you select the appropriate application type.

Application Type	Name	Filter/Column/Both	Description
COM Class	COM Display Name	Both	The display name for the COM class object.
COM Class	CLSID	Column	The globally unique identifier that identifies a COM class object.
COM Class	App ID	Column	The globally unique identifier that represents a server process for one or more COM classes.
Management Console	File Path	Column	The path of the Management Console snap-in

Application Type	Name	Filter/Column/Both	Description
Windows Service	Service Display Name	Both	The Display Name of the Windows Service
Windows Service	Service Name	Both	The underlying name of the Windows Service
Windows Service	Service Action	Column	The action which Endpoint Privilege Management controlled for that service: • Start • Stop • Pause • Configure
Windows Store Application	Store App Name	Both	The **Name** property of the store app.
Binary	File Path	Column	The path of the macOS binary.

For more information about the Elasticsearch events in EPM, see EPM ECS Event Reference at https://www.beyondtrust.com/docs/privilege-management/console/index.htm.

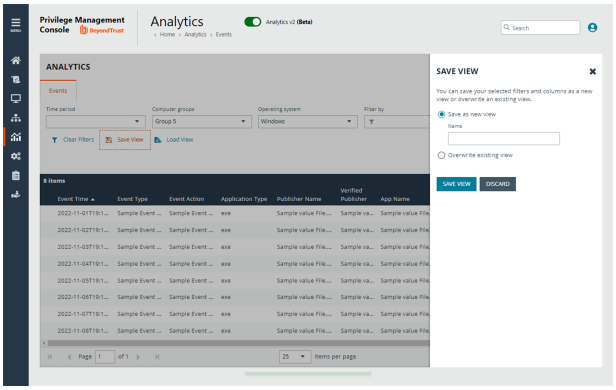
Create and Save Your Application View

All EPM users with **Analyze Group** permissions can create and save a set of filters and columns so that the same set of filters does not have to be selected every time Analytics is accessed. Saving viewing preferences provides an easy way to return to views of data used frequently to monitor Endpoint Privilege Management activity in the estate.

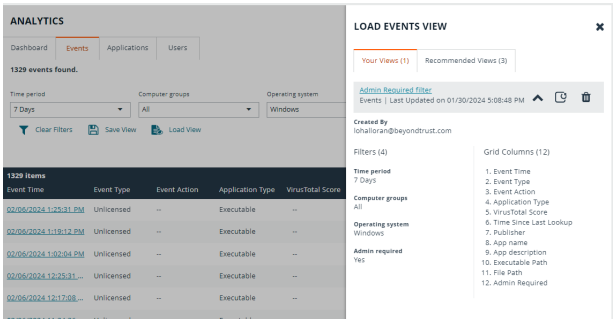
You can load and save data sets from either the **Events** page or the **Applications** page.

You can access your views on any device regardless of the device the views were created on.

1. After selecting filters, you can select **Save View** to retain those preferences for viewing later. Preferences are saved locally.
2. If a view name already exists, select **Overwrite existing view**, and then select the view you want to replace.



3. The next time you access Analytics, your view settings are preserved. Click **Load View** to select and load a view.
4. On the **Load Event View** pane, you can delete and refresh views.

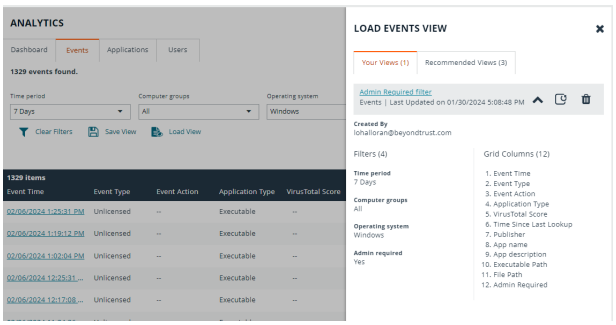


Load an Application View

You can access your views on any device regardless of the device the views were created on.

After you save view preferences, your settings are preserved the next time you access Analytics.

1. Click **Load View** to select and load a view.
2. On the **Load Event View** pane, you can delete and refresh views.

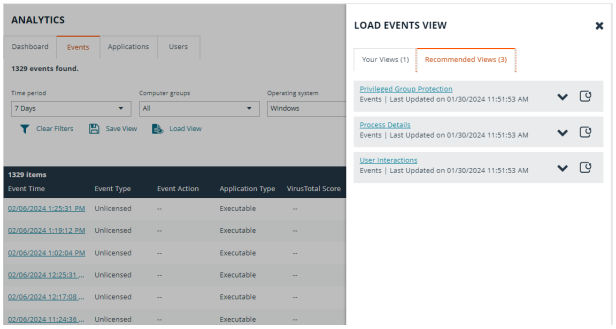


Recommended Views

The recommended views provide a selection of the most useful predetermined views. Use the views to review collected data and make informed decisions around policy editing.

Recommended views are available for events and applications.

1. To access the views, go to **Analytics**.
2. Click the **Events** or **Applications** tab.
3. Click **Load View**, and then click the **Recommended Views** tab.



Events

Recommended views for events load with the default filters.

Name	Description
Process Details	Find every process that EPM is controlling, with flexible filtering options, to zone in on the data of interest. The report name in legacy reporting: Process Details
User Interactions	Overview of how much friction end users are experiencing, and improve their experiences without jeopardizing security. The report name in legacy reporting: User Experience
Privileged Group Protection	Shows when EPM has prevented a user modifying a privileged group. For example, adding a user to the Admins group. All events where EPM prevented users from modifying privileged groups. The report name in legacy reporting: Privileged Account Management

Applications

Recommended views for applications load with the default filters.

Name	Description
Discovered: Active Applications	To help build the **Passive Allow** and the **Add Admin** definitions. This view is used for implementation as it displays all the events captured by the *(Default)* rules. The report name in legacy reporting: Target Types
Discovered: by Publisher	To view discovered applications aggregated by Publisher, to decide if you want to treat all applications from that publisher the same way in policy and take that action.

Name	Description
	The report name in legacy reporting: Discovery by Publisher
Discovered: by Requiring Admin Rights	To see the applications that require admin rights and how they are granted, so you can track down genuine admins and what they are running. The report name in legacy reporting: Discovery Requiring Elevation
Discovered: from External Sources	Discover applications run from riskier places, to ensure the applications are not allowed admin rights. The report name in legacy reporting: Discovery from External Sources
Discovered: New and Uncategorized	Find the new and uncategorized applications running in your estate. Take action to add the applications to a category (add to a more specific application group). The report name in legacy reporting: Discovery All

Analytics Use Cases

The use cases in the following sections provide guidance on how to manage and interpret the results of the data gathered by Analytics v2.

Generate Views

Additional Analytics v2 features you can use when generating the data:

- After setting the filters, save the view to load the same set of filters the next time you want to refresh the data.
- Add the applications to policy using the **Add to Policy** option.

Windows

Use Case	Favorite Filters

Learn about recent events that require admin rights in your estate and add them to your Add Admin Application Groups.	On the **Events** grid with these filters:
	• **OS**: Windows
	• **Admin Required**: Yes
	• **Application Group Names**:
	  ◦ **(Default) Trusted & Signed UAC Prompt**
	  ◦ **(Default) Signed UAC Prompt**
	  ◦ **(Default) UAC Prompt**

Learn about recent on-demand elevation events in your estate, and add them to Add Admin Application Groups.	On the **Events** grid with these filters:
	• **OS**: Windows
	• **On Demand**: Yes
	• **Admin Required**: Yes
	• **Application group names**:
	  ◦ **(Recommended) Restricted Functions (On-Demand)**
	  ◦ **(Default) Any Application**

Learn about the most popular applications that require admin rights in your estate, and add them to your Add Admin Application Groups.	On the **Applications** grid with these filters:
	• **Operating System**: Windows
	• **Admin Required**: Yes
	• **Application Group Names**:
	  ◦ **(Default) Any Trusted & Signed UAC Prompt**
	  ◦ **(Default) Any Signed UAC Prompt**
	  ◦ **(Default) Any UAC Prompt**

Use Case	Favorite Filters

Learn about the most popular applications that are elevated on demand in your estate, and add them to your Add Admin Application Groups.	On the **Applications** grid with these filters:
	• **OS**: Windows
	• **On Demand**: Yes
	• **Admin Required**: Yes
	• **Application group names**:
	  ◦ **(Recommended) Restricted Functions (On-Demand)**
	  ◦ **(Default) Any Application**

To see the most popular *passive* applications that *would have been blocked* if the Low Flexibility policy was enabled, and add those to the Low Flex - Passive list before enabling the active allow list.	On the **Applications** grid with these filters: • **OS**: Windows • **Application Group**: ◦ **(Default) Any Application**

macOS

Use Case	Favorite Filters
Learn about recent events that require authorization rights in your estate, and add them to Add Admin Application Groups.	On the **Events** grid with these filters: • **OS**: Mac • **Authorization Required**: Yes • **Application Group Names**: ◦ **(Default) General - Any Applications Requiring Authorization**
Learn about the most popular applications that require authorization in your estate, and add them to your Authorize Application Groups.	On the **Applications** grid with these filters: • **OS**: macOS • **Authorization Required**: Yes • **Application Group Names**: ◦ **(Default) General - Any Applications Requiring Authorization**
To see the most popular *passive* applications that *would have been blocked* if the Low Flexibility policy was enabled, and add those to the Low Flex - Passive list before enabling the active allow list.	On the **Applications** grid with these filters: • **OS**: macOS • **Event Action**: Allowed + Passive • **Application Group Names**:

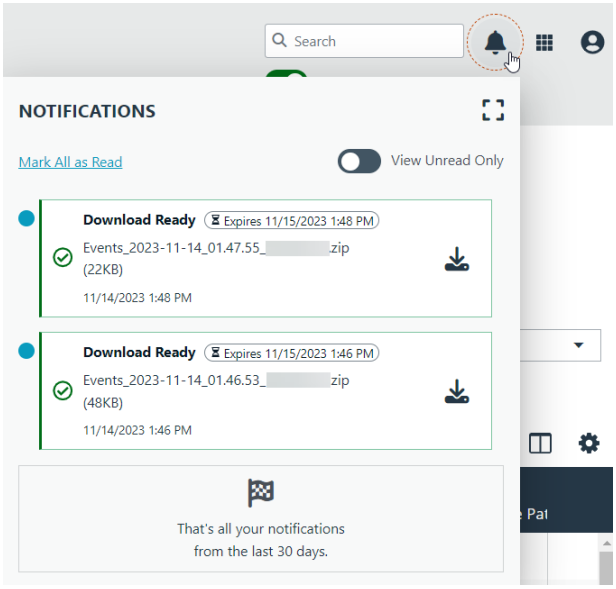
Use Case	Favorite Filters
	○ (Default) Passive - System Trusted

Export to CSV

Click the **Download all** icon to export all analytics data results in the currently filtered result set. The CSV download can include up to 5 million records when downloading from the **Events** page.

When saving an export file for events, you can set the number of records to download, the columns to include, and a file name.

Click the **Notifications** icon when the file is ready to download. Notifications only apply to the **Events** page.



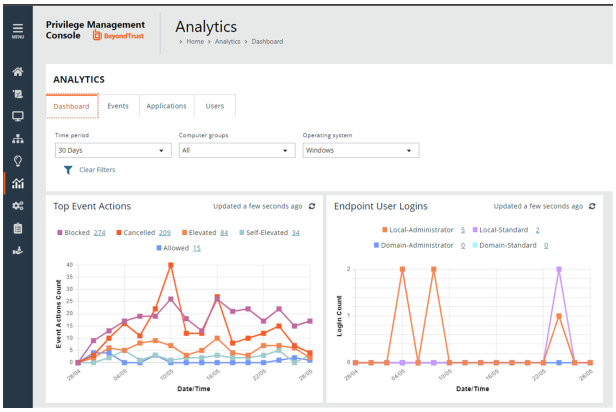
The Dashboard Page

The Dashboard is the Analytics landing page.

Use the filters to hone in on a specific time period, computer group, or OS.

The data points are Top Event Actions and Endpoint User Logins.

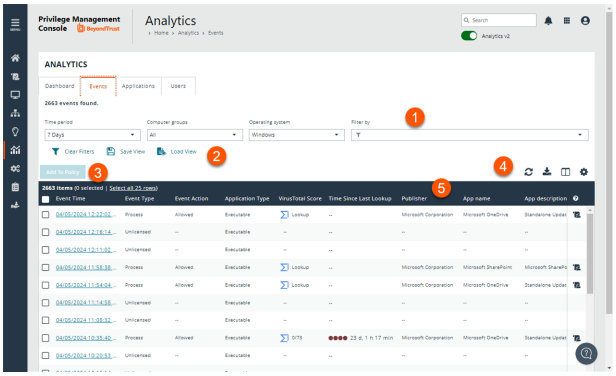
- **Top Event Actions**: Displays a graphical view of the actions data being tracked. Actions include Allowed, Elevated, Cancelled, Self-Elevated, and Blocked. The Count is the number of events. Click the link to drill down to the Events page to learn more.
- **Endpoint User Logins**: Endpoint User Logins chart shows the Windows users active in your estate, broken down by Domain or Local and Admin or Standard (requires the User Logins general rule).



macOS actions: Allowed, Allowed Installable, Allowed Deletable, Blocked, Cancelled, and Passive

Windows actions: Allowed, Elevated, Cancelled, Self-Elevated, and Blocked.

The Events Page



1. **Filters:** Click the drop arrow to select a filter type. The selected filter displays to the left of the drop-down. Time period, Computer groups, and Operating system are persistent filters and always display.
    - **Clear Filters:** Click to remove all filters and search results
    - **Filter types**
        - **Time Period:** Enter all or part of a policy name.
        - **Computer groups:** Enter an email address to view all policies locked via that account.
        - **Operating system:** Select a date from the date selector that displays to the left of the Filter drop-down to view all policies created on that day.
2. **Save View and Load View:** Save the filter preferences and load the view later for quick access to your most frequently used preferences.
3. **Add To Policy**: Select events to add to your policy.
4. **List options:** Click to refresh the list, to download list of the events to a .csv file, and click to select which columns you want to display.
5. **List columns:** Not all columns display in the image above.
    - **Column names**
    - **Event Time:**
    - **Event Type:**
    - **Event Action:**
    - **Application Type:**
    - **VirusTotal Score:**
    - **Time Since Last Lookup:**
    - **Publisher:**
    - **App name:**
    - **App description**:
    - **Executable Path**:
    - **File Path**:
    - **Admin Required**:
    - **Computer Groups**:
    - **Operating System**:
    - **Host Name**:
    - **Host Domain**:
    - **User Name**:
    - **User Domain**:

- **User ID**:
- **User Domain ID**:
- **Policy Name**:
- **Policy revision**:
- **Message Name**:
- **Workstyle Name**:
- **Application Group Name**:
- **Application Description**:
- **Rule Action**:
- **User Reason**:
- **On Demand**:
- **Token**:
- **Token Description**:
- **Command Line**:
- **Process ID**:
- **Parent Process ID**:
- **Hash (sha1)**:
- **Hash (sha256)**:
- **Hash (md5)**:
- **App version**:
- **Drive Type**:
- **Host ID**:
- **Host Domain ID**:
- **Authorizing User Domain ID**:
- **Authorizing User Name**:
- **IP addresses**:
- **File Owner ID**:
- **File Owner Name**:
- **File Owner Domain Name**:
- **Parent Process File Name**:
- **Download URL**:
- **Authorization Challenge Code**:
- **Unique Process ID**:
- **Product Code**:
- **Upgrade Code**:
- **Elevation Method**:

Add Events to Policy

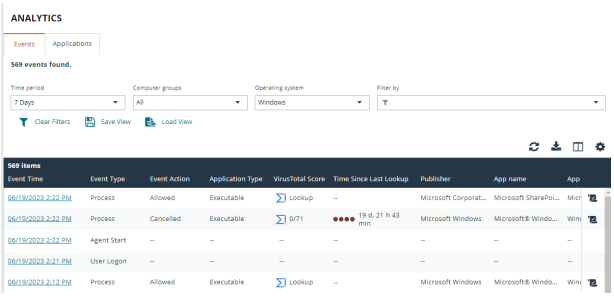
You might want to add an application to a policy from the **Events** or **Applications** page in the following scenarios:

- An application rule might have matched on a new or unknown application. Add that application to your policy or create a policy for that application.
- Find applications that are elevated by on-demand application rules.
- Find all elevated applications. If they are higher risk applications or unwanted, then add to a block rule.

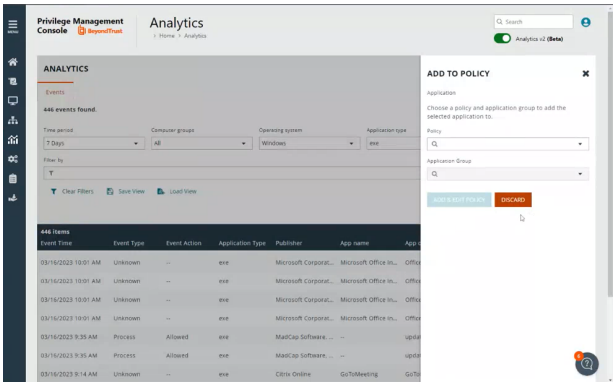
To add an application to a policy:

1. Go to the **Events** or **Applications** page in Analytics v2.
2. Click the **Add to Policy** icon for an application event that you want to add to policy.

   The **Add to Policy** icon is not displayed for unsupported applications and event types.



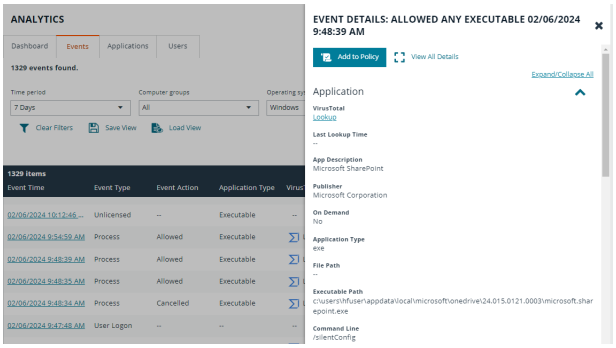
3. Click the **Add to Policy** icon for the selected event to display an **Add to Policy** panel.
4. On the **Add to Policy** panel, select a policy and application group to add the selected application to.
5. Click **Add and Edit Policy** to open the Policy Editor to edit the application.
6. The policy opens to the **Application Groups** > **Applications** page where you can edit the application settings. After you edit the application, save the changes to add the application to the selected Application Group.



View Event Details

On the **Events** page, click an event to drill down to more information about the application on the **Event Details** page.

Here you can see details like policy, event action, workstyle, application group, tokens, and more. This information can be helpful to you in making decisions on how to manage the event (for example, adding the event to a policy).



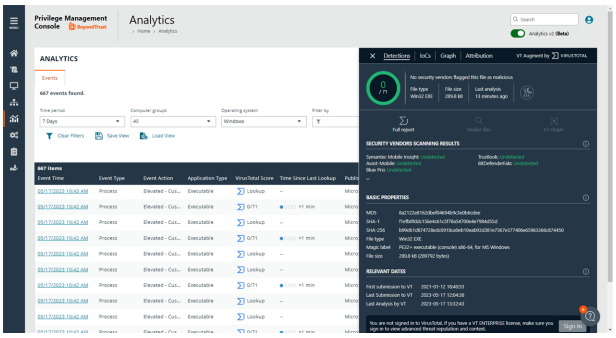
Look Up VirusTotal Score

If you are using VirusTotal, update the reputation score on the **Events** page or the **Event Details** panel. A valid reputation for an application can help you make an informed decision on how to manage that application in your policy.

EPM caches the VirusTotal score and the URL. The URLs expire after 3 days. Click the **VirusTotal** icon to retrieve the latest value from VirusTotal.

To see the latest VirusTotal score:

Click the score or the **VirusTotal** icon to open the VT Augment widget for additional insights on the reputation of the file.



On the **Events** page, the following information helps you evaluate the reputation score on a file:

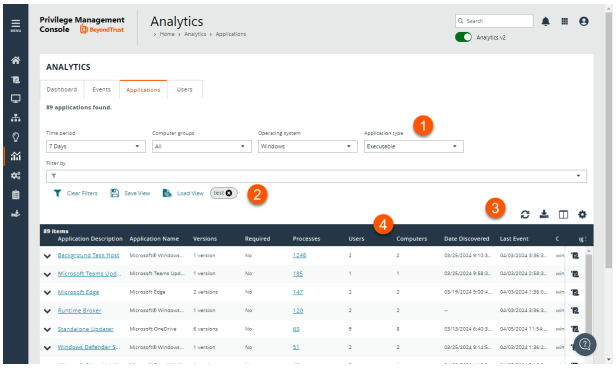
- VirusTotal score for applications with hash.
- Integrated with VT augment widget, which returns the HTML content of the widget report for a given observable.
- VirusTotal icon next to the score ensures row level refresh for events with VirusTotal support.
- A **Timestamp** column with last lookup time of the VT augment.

Additionally, the **Event Details** panel provides the VirusTotal score and last lookup time.

For more information about setting up VirusTotal, see "VirusTotal Settings" on page 187.

The Applications Page

1. **Filters:** Click the drop arrow to select a filter type. The selected filter displays to the left of the drop-down. Time period, Computer groups, and Operating system are persistent filters and always display.
    - **Clear Filters:** Click to remove all filters and search results
    - **Filter types**
        - **Time Period:** Enter all or part of a policy name.
        - **Computer groups:** Enter an email address to view all policies locked via that account.
        - **Operating system:** Select a date from the date selector that displays to the left of the Filter drop-down to view all policies created on that day.



2. **Save View and Load View:** Save the filter preferences and load the view later for quick access to your most frequently used preferences.
3. **List options:** Click to refresh the list, to download list of the events to a .csv file, and click to select which columns you want to display.
4. **List columns:** Not all columns display in the image above.

View an Application's User Activity

On the **User Activity** tab, you can:

- See how many users are running an application
- The reason provided by users, if one is required
- Actions by users (allowed, blocked, etc)

To access user activity on an application:

1. Go to the **Applications** grid.
2. Click the link for the application you are interested in. See the following sections to learn more about the collected data.
3. Click the **User Activity** tab to see information about the users accessing the application.

Use the filters to dynamically update the data.

- **Users Affected**: Shows the number of users running the application. Drill down to see more details about the users.
- **Reasons Provided**: Click the link to view a breakdown of the reasons provided by users authenticating to use the application.

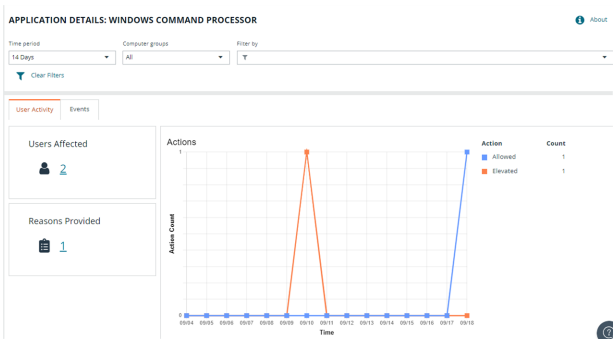
Application Details

Click the **About** link on the **Application Details** page for deeper context of the application you are viewing. Access more information such as the application type, associated versions, the publisher, whether admin rights are required, when the event was first discovered, and when the last event occurred.

Graph Data

The graph provides valuable insights with the following features:

- Default filters: The graph initially displays with two default filters, **Time Period** and **Computer Groups**. You have the flexibility to change these parameters and add filters to adjust the scope of the presented data, based on the specific information you want to see.
- Interactive **Actions** legend: Make use of the interactive **Actions** legend, which allows you to dynamically update the graph. Click to display or hide any of the available event actions to customize the information presented.
- End user metrics: Gain valuable end-user metrics, such as the frequency of event actions (Blocked, Elevated, Allowed, and Canceled), for a particular application over a defined time period.



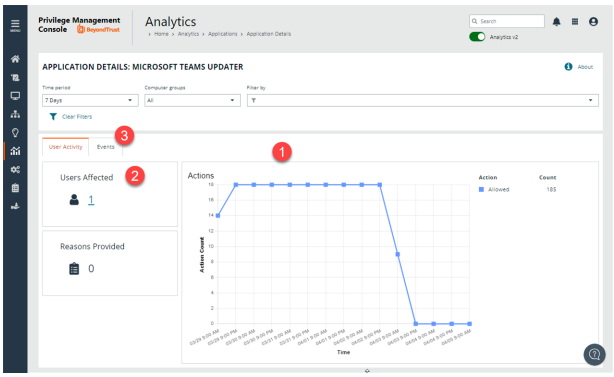
The Application Details Page

The Application Details page helps you to understand trend information about the application and decide if you need to take action to change behavior of Endpoint Privilege Management through policy change.

As of EPM 23.6, only applications that you can see on the **Applications** grid support this feature.

Using the application detail view, you can:

1. See how often an application is being run in your estate and the associated behavior at the end user level. For example, how often an event action (Blocked, Elevated, etc.) has occurred for an application over a given time period.
2. See how many users are running an application, the reason given if one is required, all associated events, and meta data like versions run, application type, etc.
3. Access the event details specific to the application.



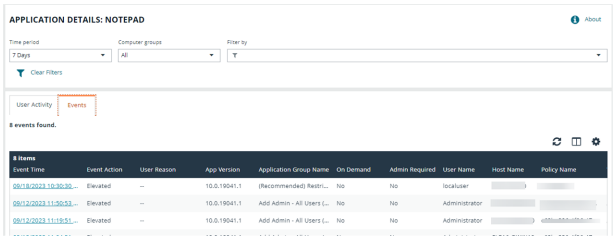
To access application details:

1. Go to the **Applications** grid.
2. Click the link for the application you are interested in. See the following sections to learn more about the collected data.

View an Event's Details

Click the **Events** tab to view only those events related to the application. The information displayed is the same level of detail as presented on the **Events** page.

Click the **Event Time** of the event to drill down to the **Event Details** page.



Add an Application to Policy

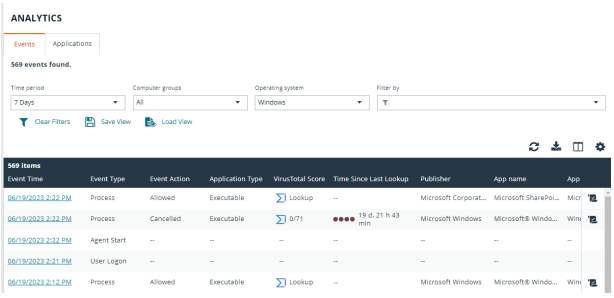
You might want to add an application to a policy from the **Events** or **Applications** page in the following scenarios:

- An application rule might have matched on a new or unknown application. Add that application to your policy or create a policy for that application.
- Find applications that are elevated by on-demand application rules.
- Find all elevated applications. If they are higher risk applications or unwanted, then add to a block rule.

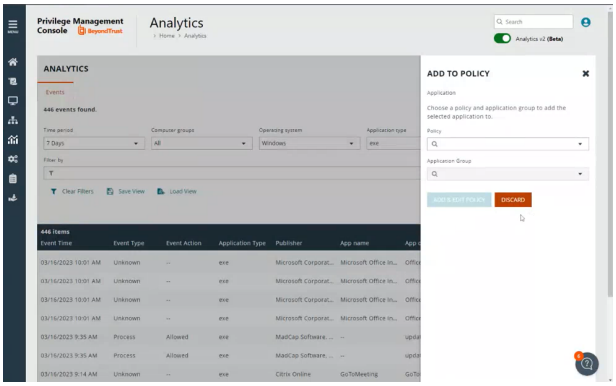
To add an application to a policy:

1. Go to the **Events** or **Applications** page in Analytics v2.
2. Click the **Add to Policy** icon for an application event that you want to add to policy.

   The **Add to Policy** icon is not displayed for unsupported applications and event types.



3. Click the **Add to Policy** icon for the selected event to display an **Add to Policy** panel.
4. On the **Add to Policy** panel, select a policy and application group to add the selected application to.
5. Click **Add and Edit Policy** to open the Policy Editor to edit the application.
6. The policy opens to the **Application Groups** > **Applications** page where you can edit the application settings. After you edit the application, save the changes to add the application to the selected Application Group.

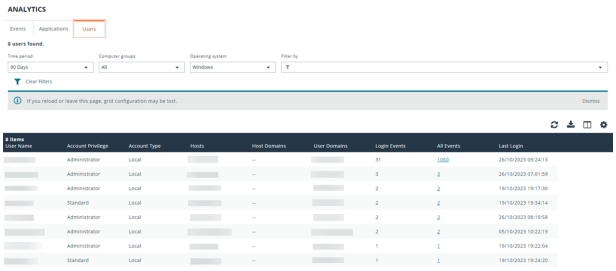


The Users Page

The **Users** grid provides visibility into when users log on to managed endpoints and the privileges used, whether standard or administrator.

To enhance security on endpoints in your estate, determine the need to log on with admin rights and change access levels depending on the requirements.

Starting in version 23.9, event information is displayed for each user. The **Events** view provides streamlined workflows and improves visibility of the users in your organization and their actions in EPM. Click the **Events** link to view a pre-filtered list of events by the user from a specific host name (computer).



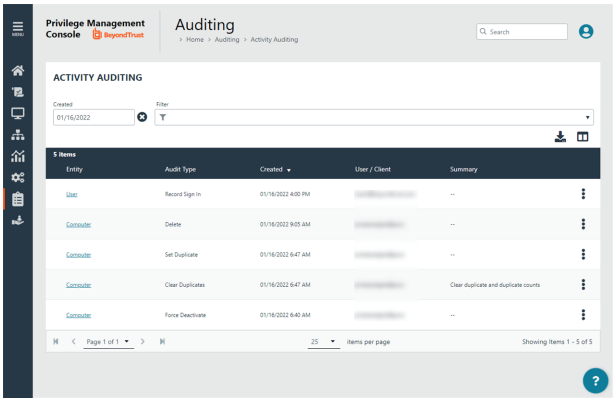
The Activity Auditing Page

The **Activity Auditing** page provides detailed auditing information on user, group, and policy actions.

To access the **Activity Auditing** page, on the sidebar menu, select **Auditing**, and then select **Activity Auditing**.

A **Summary** column highlights the changes on an audited activity.

Audited activities include the user who initiated the action and timestamps on when the activity started and ended.



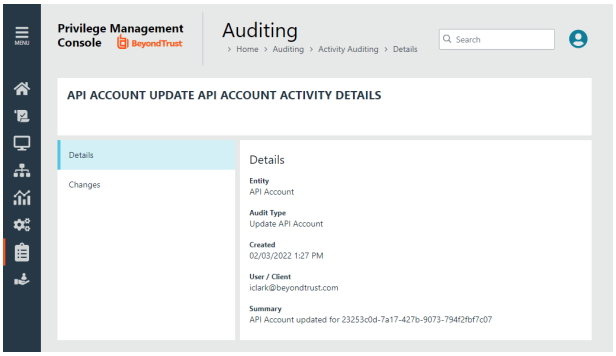
Some of the audited information includes:

- User logon details
- Modify settings
- Set duplicate agents
- Assign role to users
- Modify user
- Resend user invite
- Disable user
- Create group
- Abort open policy draft
- Create user

View Activity Details

To drill down to more information, click the menu, and then select **Activity Details**.

Click **Changes** to view *before* and *after* changes that occurred for an item



View Authorization Request Details

ServiceNow user authorization requests are audited for troubleshooting and logging purposes.

Select the **Auditing** menu to access the **Authorization Request Auditing** tile.

> ***Note:*** *You only see the* ***Authorization Request Auditing*** *tile if authorization request management is set up on the* ***Configuration > Authorization Request Settings*** *page.*

Some of the key elements captured in the audit include:

- **User:** The user requesting authorization.
- **Time of Request:** The time the ticket is created.
- **Decision Performed By:** The ServiceNow user approving or denying the action.
- **Decision Time:** The time approval or denial occurs.
- **Decision Duration:** The time allotted for the authorized request.
- **Decision Start Time:** The time the decision duration started.

Windows and macOS OS Technical Support Statement

At BeyondTrust, we strive to offer technical support for all operating systems (OS), but we acknowledge the limitations that may arise when using outdated operating systems.

At our sole discretion, we may make commercially reasonable efforts to provide limited technical support for supported EPM (Endpoint Privilege Management) agents installed on outdated Windows OS or macOS. However, it's essential to note that according to BeyondTrust's End of Life Policy, we are not committed to providing any security, functional, or operational code fixes for agents installed on unsupported or outdated OS versions.

We highly recommend keeping your operating systems up-to-date to ensure the security, stability, and optimal performance of your systems and applications. Running outdated OS versions may expose your organization to various security risks and vulnerabilities, as they may lack essential security patches and updates provided by the OS vendor.

In the event that you encounter issues with EPM agents installed on outdated Windows OS or macOS, BeyondTrust will make every effort to provide guidance and assistance within the constraints of our End of Life Policy.

We remain committed to supporting our customers in their cybersecurity efforts and are here to assist you in navigating any challenges you may encounter. If you have any questions or require further assistance regarding technical support for EPM agents, please don't hesitate to contact our support team.