BeyondTrust

Endpoint Privilege Management for Windows

ePO Extension 23.10 Administration Guide

TC:4/25/2024

Table of Contents

EPM ePO Extension Administration

Endpoint Privilege Management for Windows combines privilege management and application control technology in a single, lightweight agent. This scalable solution allows global organizations to eliminate admin rights across the entire business.

Actionable intelligence is provided by an enterprise class reporting solution with endpoint analysis, dashboards, and trend data for auditing and compliance.

Define User Roles

Before deploying Endpoint Privilege Management for Windows, you should spend time preparing suitable Workstyles for your users. Implementing least privilege may require Workstyles to be tailored to users' roles.

The table below shows three typical user roles, but we recommend that you create roles that are tailored to your environment.

Role	Requirement for Admin Rights
Standard Corporate User	Applications that require admin rights to function, and simple admin tasks
Laptop User	Flexibility to perform ad-hoc admin tasks and install software when away from the corporate network
Technical User	Complex applications and diagnostic tools, advanced admin tasks and software installations

Endpoint Privilege Management for Windows can cater to all types of users, including the most demanding technical users, such as system administrators and developers.

You should also educate your users on what they should expect from a least privilege experience, before transferring them to standard user accounts. This ensures that they report any problems they encounter during the process of moving to least privilege.

***Note:** Contact your solution provider or BeyondTrust to gain access to templates for more complex use case scenarios.*

Implement Least Privilege

The first step is to identify the applications that require admin privileges for each of the roles you've defined. These can fall into one of three categories:

1. **Known Admin Applications:** You already have a definitive list of applications that require admin rights to run.
2. **Unknown Admin Applications:** You are not sure of the applications that require admin rights to run.
3. **Flexible Elevation:** The user requires flexibility and can't be restricted to a list of applications.

Known Applications

For this category you should add the relevant applications to the Endpoint Privilege Management for Windows Application Groups for the users. This automatically elevates these applications when they are launched. You can then remove admin rights from these accounts.

Unknown Applications

For this category you have two choices to help you discover the applications that require admin rights:

- Set up Endpoint Privilege Management Workstyles to monitor privileged application behavior. The Endpoint Privilege Management for Windows audit logs highlight all of the applications that require admin rights to run.
- Set up Endpoint Privilege Management Workstyles to give the user the **on-demand** elevation facility, and instruct the user to use this facility for any applications that fail to run once you have taken the user's admin rights away. The Endpoint Privilege Management for Windows audit logs highlight all the applications that the user has launched with elevated rights.

You can use the audit logs to determine the relevant set of applications that you want to give admin rights to for these users.

Flexible Elevation

For this category, you should set up Endpoint Privilege Management Workstyles that give the user an **on-demand** elevation facility, which allows the user to elevate any applications from a standard user account. All elevated applications can be audited, to discourage users from making inappropriate use of this facility.

About Trellix ePolicy Orchestrator

Trellix ePO software, the foundation of the Trellix Security Management solution, unifies management of endpoints, networks, data, and compliance solutions. More than 45,000 organizations use Trellix ePO software on nearly 60 million nodes to manage security, streamline and automate compliance processes, and increase overall visibility across security management activities. With its scalable architecture, fast time to deployment, and ability to support enterprise systems, Trellix ePO software is the most advanced security management software available.

Only Trellix ePO offers:

End-to-end visibility: Get a unified view of your security posture. Drillable, drag-and-drop dashboards provide security intelligence across endpoints, data, mobile, and networks for immediate insight and faster response times.

Simplified security operations: Streamline workflows for proven efficiencies. Independent studies show ePO software helps organizations of every size streamline administrative tasks, ease audit fatigue, and reduce security management-related hardware costs.

An open, extensible architecture: Leverage your existing IT infrastructure. Trellix ePO software connects management of both Trellix and third-party security solutions to your LDAP, IT operations, and configuration management tools. LDAP Servers can be made available via the built-in registered servers in ePO.

> *For more information, see Trellix ePolicy Orchestrator at https://www.trellix.com/en-us/products/epo.html.*

Endpoint Privilege Management for Windows and Trellix

Endpoint Privilege Management for Windows is implemented as a server extension to Trellix ePolicy Orchestrator, enabling Workstyles to be managed through the ePO Policy Catalog. Granular auditing and reporting of Endpoint Privilege Management for Windows activity is available using ePO integrated dashboards and query editor, as well as the reporting module.

The BeyondTrust Endpoint Privilege Management Reporting module uses the Endpoint Privilege Management Reporting database to store Endpoint Privilege Management for Windows audit data for reporting.

Endpoint Privilege Management for Windows is deployed to endpoints as a client task through the ePO System Tree.

If you do not want to use Trellix ePO for deployment of the client package, the Endpoint Privilege Management for Windows client is available as a standalone MSI or executable package, which can be deployed using any suitable third-party deployment solution.

Endpoint Privilege Management for Windows policies are deployed to endpoints through ePO Policy Assignments, which are automatically applied by the Endpoint Privilege Management for Windows client.

Note: *If you do not want to use Trellix ePO for deployment of Workstyles, then you may import or export Workstyles as an XML file, and use any suitable deployment solution to deploy the XML file to a set location on each client computer.*

BeyondTrust Endpoint Privilege Management App

Starting in version 23.10, we are updating and enhancing the policy editing and reporting experience for our Endpoint Privilege Management for Windows and Mac solution deployed via Trellix ePolicy Orchestrator (ePO).

This new experience will mean policy editing and reporting will happen outside of the ePO extension and will instead be delivered via a new Electron-based application called the BeyondTrust Endpoint Privilege Management App, published by BeyondTrust.

For more information, see:

- *BeyondTrust Endpoint Privilege Management App User Guide*
- *BeyondTrust Endpoint Privilege Management App Frequently Asked Questions*

Install, Uninstall, and Upgrade Endpoint Privilege Management for Windows

Frequently Asked Questions

Can I install the 32-Bit Client on a 64-Bit endpoint?

No. The 32-Bit Client can only be installed on 32-Bit endpoints.

What distribution mechanisms do you support?

ePO is one of many options for deploying the Endpoint Privilege Management for Windows client. It can also be deployed using any third party software that supports the deployment of MSI and/or executable files, such as Microsoft Active Directory, and Microsoft SMS / SCCM.

If using alternative third party deployment software to install the Endpoint Privilege Management for Windows client, it must support the use of command line options, and must be passed the **EPOMODE = true** flag to install the client in ePO mode to allow it to interface with the Trellix agent to receive policies, and send audit events.

Install the Endpoint Privilege Management for Windows Clients

ePO manages the deployment of the Endpoint Privilege Management for Windows clients for each operating system. You can create client tasks to manage the installation of Endpoint Privilege Management for Windows on your endpoints.

For more information on installing Endpoint Privilege Management for Windows using ePO, see the Endpoint Privilege Management for Windows ePO Extension Installation Guide, at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm.

Uninstall the Endpoint Privilege Management for Windows Clients

You can uninstall the Endpoint Privilege Management for Windows clients locally or use ePO to manage the uninstallation.

You can perform a local uninstall of Endpoint Privilege Management on a Windows operating system either as an administrator or by using Endpoint Privilege Management for Windows, if a policy is in place to allow this.

For more information on uninstalling Endpoint Privilege Management for Windows using ePO, see the Endpoint Privilege Management for Windows ePO Extension Installation Guide, at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm.

Upgrade EPM

The recommended order to upgrade EPM is:

- Upgrade the ePO Extension
- Install or upgrade the BT PM App
- Upgrade Endpoint Privilege Management Reporting (if in use)
- Upgrade EPM clients

Note:

- *ePO will not recognize EPM clients if you upgrade the clients before the extension.*
- *ePO Threat events are rejected if this order is not followed. The events can be recovered after the upgrade is complete.*

If you have a requirement to upgrade BeyondTrust software in a different order, contact your BeyondTrust representative.

Upgrade the ePO Extension

When you are upgrading the extension, the newer version recognizes the existing installation and prompts you to upgrade. We recommend upgrading, as removing the installed ePO Extension deletes your settings.

To upgrade:

1. In ePO, go to **Software > Extensions**.
2. Upload the extension. ePO displays a message indicating the new version will replace the previous version.
3. Click **OK**. You do not need to restart ePO for the upgrade to take effect. Existing registered servers, client tasks, and server tasks are not affected.

Upgrade Privilege Management Reporting (if in use)

To upgrade the Reporting database, you need to be on the server where the database is installed.

Please use the following process to upgrade the Privilege Management Reporting database and event parser:

1. Stop the Trellix ePolicy Orchestrator Event Parser Service. Check that all events have finished being processed. Any events that are received after these tables are empty are queued on the ePO server until the service is restarted at the end of this process.

   Query the following tables first to check that they are empty:

   - dbo.Staging
   - dbo.Staging_ServiceStart
   - Stop
   - dbo.Staging_UserLogon

   Subsequently, query the following tables:

   - dbo.StagingTemp
   - dbo.StagingTemp_ServiceStart

- dbo.StagingTemp_ServiceStop
- dbo.StagingTemp_UserLogon

Once the tables are all empty all remaining events have been processed.

2. Disable the **Copy from Staging** task. The easiest way to do this is to use SQL Server Management Studio and navigate to **Reporting database > Service Broker > Queues**.
3. Right-click **PGScheduledJobQueue** and select **Disable Queue**.
4. Disable any of the ePO server tasks that rely on the Reporting database while you are upgrading it. For example, the Staging Server Task and Purge Server Task. These tasks will fail, as the database will be offline for a period of time.
5. Open SQL Server Reporting Configuration Manager and connect to the database. Navigate to the **Reporting** link and use the dropdown to delete the top level folder.
6. Run the Privilege Management database installer to upgrade the database. Ensure you point the installer to the existing database server and database name when prompted.
7. Enable any server tasks that you previously disabled, as they rely on the Reporting database.
8. Enable the **Copy From Staging** task. The easiest way to do this is to use SQL Server Management Server and navigate to **Reporting database > Service Broker > Queues**.
9. Right-click **PGScheduledJobQueue** and select **Enable Queue**.
10. Start the **Trellix ePolicy Orchestrator Event Parser Service** service. Any incoming events can now be processed.
11. You need to log off and on again to the ePO server to ensure the new database version is recognized. However, an ePO server restart is not required.

> ***Note:*** *If you see the error message "Please stop CopyFromStaging from running before upgrading the database," make sure that no new events are being processed by querying the above tables and try again.*

This upgrade path can be applied to both standalone Reporting configurations and to configurations across multiple machines.

Upgrade EPM Clients

- You can upload a newer version of the EPM client to ePO and deploy as required.
- Depending on the type of installation, a restart of the endpoint may be required. When installing in silent mode, a reboot occurs automatically.
- The ePO Extension maintains backwards compatibility with the EPM client. You can use a later version of the extension with an earlier version of the EPM client. However, not all features in the ePO Extension are supported with earlier versions of the client.

Manual Deployment of Endpoint Privilege Management for Windows

Endpoint Privilege Management for Windows can optionally be deployed manually using any Windows Installer compatible third-party deployment system. The Endpoint Privilege Management for Windows package is available as both an MSI package and self-installing executable package from BeyondTrust.

Prerequisites

Endpoint Privilege Management for Windows must be installed in ePO Mode, either by selecting the Trellix ePolicy Orchestrator Integration option when installing Endpoint Privilege Management for Windows, or by using a command-line option if installing the client via a deployment system. This install additional components required to communicate with the Trellix Agent.

To install the client MSI package silently in ePO Mode, use the following command line:

```
MSIEXEC.exe /i PrivilegeManagementForWindows_x(XX).msi /qn EPOMODE=1
```

To install the client MSI package silently in ePO Mode with logging enabled:

```
MSIEXEC.exe /i PrivilegeManagementForWindows_x(XX).msi /qn EPOMODE=1 /sv “C:\PMFWInstallLog.txt”
```

To install the client executable silently in ePO Mode, use the following command line (the double quotes are required):

```
PrivilegeManagementForWindows_x(XX).exe /s /v" /qn EPOMODE=1"
```

Note: *In the command lines above,* ***(XX)*** *represents 86 or 64 in relation to the 32-bit or 64-bit installation, respectively.*

Note: *The syntax above must be copied exactly for the install to work as designed, including all spacing.*

Note: *If you are deploying Endpoint Privilege Management for Windows using Trellix ePO, then ePO Mode is automatically enabled.*

Disable ePO Mode

Once installed in ePO Mode, Endpoint Privilege Management for Windows sends events to the Trellix Agent, and also raises events to the Application event log. If you want to disable ePO mode at any time, set the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Avecto\Privilege Guard Agent\
DWORD "EPOMode"=0
```

To re-enable ePO Mode, set the above DWORD value to **1**.

Policy Management

Starting in version 23.10, EPM policy in ePO is managed using the BeyondTrust Endpoint Privilege Management App.

Using the Policy Editor, you can:

- Use QuickStart templates to create a policy with predefined configuration
- Create application rules and on-demand application rules
- Create end user messages

ℹ *For more information about the app, see BeyondTrust Endpoint Privilege Management App.*

Deploy Endpoint Privilege Management for Windows Policy

Certain types of deployment methods may be enabled or disabled. By default, all deployment types are enabled. To include or exclude a method of deployment from evaluation, edit the entries in the registry value below. If this key does not already exist, then the default behavior is to include all methods:

HKEY_LOCAL_MACHINE\Software\Avecto\Privilege Guard Client

REG_SZ PolicyEnabled = "EPO,WEBSERVER,GPO,LOCAL"

Where **EPO,WEBSERVER,GPO,LOCAL** are the available deployment methods.

Registry settings may be deployed using Advanced Agent Settings. To apply a configuration deployment method, the setting must be applied to a type of configuration that is already part of the configuration precedence order.

Audits and Reports

The Endpoint Privilege Management Trellix ePO Integration Pack includes a set of rich preconfigured dashboards, built in ePO Queries and Reports, which summarize Endpoint Privilege Management for Windows event data collected from Trellix ePO managed computers.

We also provide an enterprise level, scalable reporting solution in Endpoint Privilege Management Reporting. Endpoint Privilege Management Reporting includes a rich set of dashboards and reports designed to simplify the centralized management and auditing of Endpoint Privilege Management for Windows activity throughout the desktop and server estate. Each dashboard provides detailed and summarized information regarding Application, User, Host, and Workstyle usage.

For more information on how to configure Reporting in ePO, see the ePO Installation Guide at www.beyondtrust.com/docs/privilege-management/windows.htm.

Dashboards in Endpoint Privilege Management for Windows

The Trellix ePO integration includes the following dashboards:

- BeyondTrust Endpoint Privilege Management: Blocked
- BeyondTrust Endpoint Privilege Management: Elevated
- BeyondTrust Endpoint Privilege Management: Executed
- BeyondTrust Endpoint Privilege Management: Monitoring

To access the dashboards, click on the **Dashboards** icon and then select one of the Endpoint Privilege Management for Windows dashboards from the **Dashboard** dropdown menu. These dashboards show Windows and macOS events.

> ***Note:*** *If you want to add, remove, or amend any of the default monitors for any of the dashboards below, you can do so within Trellix ePO Queries and Reports. We recommend that only advanced Trellix ePO administrators do this. Please refer to Trellix ePO documentation for details on managing dashboards, queries, and reports.*

BeyondTrust Endpoint Privilege Management: Blocked

The **BeyondTrust Endpoint Privilege Management: Blocked** dashboard contains all events raised by Endpoint Privilege Management for Windows relating to applications that were blocked by Endpoint Privilege Management for Windows policy.

The **BeyondTrust Endpoint Privilege Management: Blocked** dashboard includes the following monitors:

- BeyondTrust Endpoint Privilege Management: Top 10 Blocked Apps
- BeyondTrust Endpoint Privilege Management: Top 10 Blocked by Publisher
- BeyondTrust Endpoint Privilege Management: Blocked over Last 7 Days

Each chart element in the monitors can be hovered over to display a count of how many blocked applications make up that element. To view the details of blocked applications for a particular element, click on the element to drill down.

BeyondTrust Endpoint Privilege Management: Elevated

The **BeyondTrustEndpoint Privilege Management: Elevated** dashboard contains all events raised by Endpoint Privilege Management for Windows relating to applications that were elevated by Endpoint Privilege Management for Windows policy. These events include:

- Auto-Elevated: Applications elevated by Application Privileges policy
- User-Elevated: Applications elevated by **On-Demand** shell elevation policy

The **BeyondTrust Endpoint Privilege Management : Elevated** dashboard includes the following monitors:

- BeyondTrust Endpoint Privilege Management: Top 10 Elevated Apps
- BeyondTrust Endpoint Privilege Management: Top 10 Elevated by Publisher
- BeyondTrust Endpoint Privilege Management: Elevated over Last 7 Days

Each chart element in the monitors can be hovered over to display a count of how many elevated applications make up that element. To view the details of elevated applications for a particular element, click on the element to drill down.

Endpoint Privilege Management: Executed

The **BeyondTrust Endpoint Privilege Management: Executed** dashboard contains all events raised by Endpoint Privilege Management for Windows relating to applications that were allowed to execute under Endpoint Privilege Management for Windows control. These events include:

Auto-Elevated: Applications elevated by Application Privileges policy.

User-Elevated: Applications elevated by **On-Demand** shell elevation policy.

Passive: Applications granted a passive access token.

Drop-Admin: Applications which have had admin rights removed.

Default-Rights: Applications which have had standard user rights enforced.

Custom-Token: Applications granted a custom created access token.

Admin-required: Applications which require admin rights to run (Privilege Monitoring).

The **BeyondTrust Endpoint Privilege Management: Executed** dashboard includes the following monitors:

- BeyondTrust Endpoint Privilege Management: Top 10 Executed Apps
- BeyondTrust Endpoint Privilege Management: Top 10 Executed by Publisher
- BeyondTrust Endpoint Privilege Management: Executed over Last 7 Days

Each chart element in the monitors can be hovered over to display a count of how many executed applications make up that element. To view the details of executed applications for a particular element, click on the element to drill down.

BeyondTrust Endpoint Privilege Management: Monitoring

The **BeyondTrust Endpoint Privilege Management: Monitoring** dashboard contains all events raised by Endpoint Privilege Management for Windows , relating to applications detected by Endpoint Privilege Management for Windows , requiring elevated rights to run.

The **BeyondTrust Endpoint Privilege Management: Monitoring** dashboard includes the following monitors:

- BeyondTrust Endpoint Privilege Management: Top 10 Apps Requiring Elevated Rights
- BeyondTrust Endpoint Privilege Management: Top 10 Requiring Elevated Rights by Publisher
- BeyondTrust Endpoint Privilege Management: Elevated Rights over Last 7 Days

Each chart element in the monitors can be hovered over to display a count of how many monitored applications make up that element. To view the details of monitored applications for a particular element, click on the element to drill down.

Events in Endpoint Privilege Management for Windows

Endpoint Privilege Management for Windows sends events to ePO using the Trellix Agent, and also to the local application event log, depending on the audit and privilege monitoring settings within the Endpoint Privilege Management for Windows policy.

The following events are logged by Endpoint Privilege Management for Windows :

Windows Process Events

ePO ID (Event ID)	Description
202299 (1)	Service Error - unlicensed or invalid license code.
202250 (100)	Process has started with admin rights added to token.
202251 (101)	Process has been started from the shell context menu with admin rights added to token.
202253 (103)	Process has started with admin rights dropped from token.
202254 (104)	Process has been started from the shell context menu with admin rights dropped from token.
202256 (106)	Process has started with no change to the access token (passive mode).
202257 (107)	Process has been started from the shell context menu with no change to the access token (passive mode).
202259 (109)	Process has started with user’s default rights enforced.
202260 (110)	Process has started from the shell context menu with user’s default rights enforced.
202262 (112)	Process requires elevated rights to run.
202263 (113)	Process has started with Custom Token applied.
202264 (114)	Process has started from the shell context menu with user’s Custom Token applied.
202266 (116)	Process execution was blocked.
202268 (118)	Process started in the context of the authorizing user.
202269 (119)	Process started from the shell menu in the context of the authorizing user.
202270 (120)	Process execution was canceled by the user.
202275 (150)	Endpoint Privilege Management handled service control start action.
202276 (151)	Endpoint Privilege Management handled service control stop action.
202277 (152)	Endpoint Privilege Management handled service control pause/resume action.
202278 (153)	Endpoint Privilege Management handled service control configuration action.
202279 (154)	Endpoint Privilege Management blocked a service control start action.
202280 (155)	Endpoint Privilege Management blocked a service control stop action.
202281 (156)	Endpoint Privilege Management blocked a service control pause/resume action
202282 (157)	Endpoint Privilege Management blocked a service control configuration action
202283 (158)	Endpoint Privilege Management service control action run in the context of the authorizing user
202284 (159)	Endpoint Privilege Management service control start action canceled
202285 (160)	Endpoint Privilege Management service control stop action canceled
202286 (161)	Endpoint Privilege Management service control pause/resume action canceled

ePO ID (Event ID)	Description
202287 (162)	Endpoint Privilege Management service control configuration action canceled
202297 (199)	Windows only - Process execution was blocked, the maximum number of challenge / response failures was exceeded
Configuration Events All events with a value of 200 - 299 ID are not sent to ePO Dashboards.	
(200)	Config Config Load Success
(201)	Config Config Load Warning
(202)	Config Config Load Error
(210)	Config Config Download Success
(211)	Config Config Download Error
User / Computer Events These events are not sent to ePO Dashboards.	
(300)	User User Logon
(400)	Service Endpoint Privilege Management Service Start
(401)	Service Endpoint Privilege Management Service Stop
Content Events	
203050 (600)	Process Content Has Been Opened (Updated Add Admin)
203050 (601)	Process Content Has Been Updated (Updated Custom)
203050 (602)	Process Content Access Drop Admin (Updated Drop Admin)
203050 (603)	Process Content Access Was Canceled By The User (Updated Passive)
203050 (604)	Process Content Access Was Enforced With Default Rights (Updated Default)
203050 (605)	Process Content Access Was Blocked
203050 (606)	Process Content Access Was Canceled
203050 (607)	Process Content Access Was Sandboxed
203050 (650)	Process URL Browse
203050 (706)	Process Passive Audit DLL
203050 (716)	Process Block DLL
203050 (720)	Process Cancel DLL Audit

Each process event contains the following information:

- Command line for the process
- Process ID for the process (if applicable)
- Parent process ID of the process
- Workstyle that applied
- Application group that contained the process
- End user reason (if applicable)
- Custom access token (if applicable)

- File hash
- Certificate (if applicable)

Note: *Each process event also contains product properties, where applicable, but these can only be viewed in the Endpoint Privilege Management Reporting Console.*

Custom Script Auditing

When an application is allowed, elevated, or blocked, Endpoint Privilege Management for Windows logs an event to the Application Eventlog to record details of the action. If you want to record the action in a bespoke or third-party tracking system that supports PowerShell, VBScript, or JScript based submissions, you can use the **Run a Script** setting within an Application Rule.

To add an existing auditing script to an Application Rule:

1. Create a new or edit an existing Application Rule within a Workstyle.
2. In **Run a Script**, click on the dropdown menu, and select your custom script. If you can't change this value you need to create a custom script first.
3. Click **OK** to save the Application Rule.

***Note:** If you have any existing scripts, you can select them in the dropdown menu.*

The auditing script supports the use of parameters within the script. Parameters are expanded using the COM interface **PGScript**.

Example:

```
strUserName = PGScript.GetParameter("[PG_USER_NAME]")
strCommandLine = PGScript.GetParameter("[PG_PROG_CMD_LINE]")
strAgentVersion = PGScript.GetParameter("[PG_AGENT_VERSION]")
```

***Note:** Scripts created in the script editor can be reused in multiple Application Rules and On-Demand Application Rules. Any modification to an existing script affects all Workstyle rules that have been configured to execute that script.*

Set up ePO Server Tasks for Endpoint Privilege Management Reporting

There are two BeyondTrust ePO server tasks that you can set up for Endpoint Privilege Management Reporting:

- Create the Reporting Event Staging server task
- Create the Reporting Purge server task

There is an additional server task that you can create if you have a business need to purge the events from the BeyondTrust table in the ePO database only.

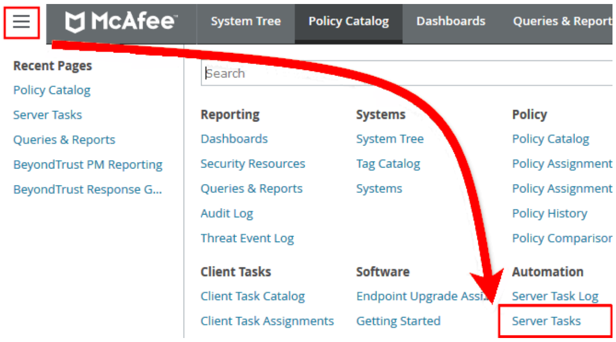
We recommend you use the built-in ePO server task called **Purge Rolled up Data** rather than this server task. This will remove all the events from the BeyondTrust table in the ePO database and the Reporting database.

> *For more information, see the following:*
>
> - *Create the Reporting Event Staging Server Task in the ePO Installation Guide at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm*
> - *Create the Enterprise Reporting Purge Server Task in the ePO Installation Guide at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm*
> - *"Create the Enterprise Reporting Purge Server Task" on page 21*

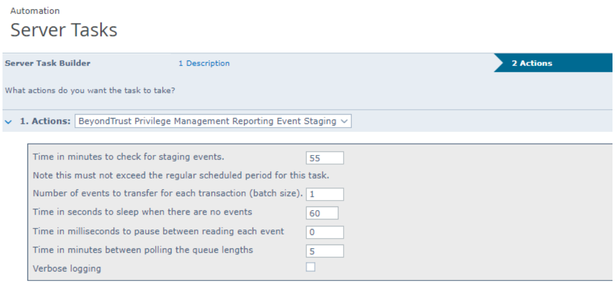
Create the Reporting Event Staging Server Task

The **Reporting Event Staging** server task takes report events from the ePO database and inserts them into the BeyondTrust Endpoint Privilege Management Reporting database. You need to create this task to view BeyondTrust reports.

1. Navigate to **Menu > Automation > Server Tasks** and select **New Task**.



2. Enter an appropriate name (**BeyondTrust Event Staging**, for example), leave the **Schedule status** as **Enabled**, and click **Next**.
3. Select **BeyondTrust Endpoint Privilege Management Reporting Event Staging** from the **Actions** dropdown menu and click **Next**.



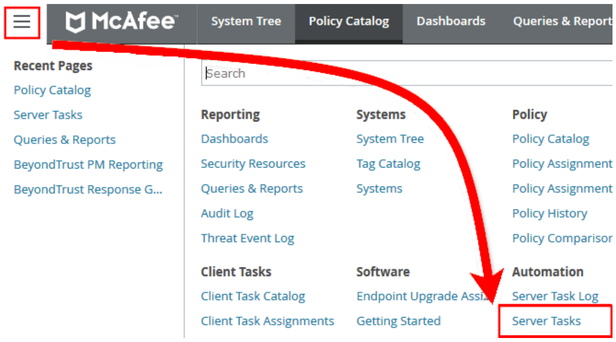
Automation
Server Tasks
Server Task Builder | 1 Description | 2 Actions
What actions do you want the task to take?
1. Actions: BeyondTrust Privilege Management Reporting Event Staging
Time in minutes to check for staging events. 55
Note this must not exceed the regular scheduled period for this task.
Number of events to transfer for each transaction (batch size). 1
Time in seconds to sleep when there are no events 60
Time in milliseconds to pause between reading each event 0
Time in minutes between polling the queue lengths 5
Verbose logging □

4. Adjust the times to check for events to suit your environment and click **Next**.
    - **Time in minutes to check for staging events**: The recommended value is 55 minutes.
    - **Number of events to transfer for each transaction (batch size)**: The default value is 1. Only increase the value if there is a lag in performance throughput between ePO to Endpoint Privilege Management Reporting.
    - **Time in seconds to sleep when there are no events**: The recommended value is 60 seconds.
    - **Time in milliseconds to pause between reading each event**: The default and recommended value is 0.
    - **Time in minutes between polling the queue lengths**: The recommended value is 5 minutes.
    - **Verbose logging**: By default, verbose logging is turned off. Only use verbose logging when you need more details about the events being collected.
5. On the **Schedule** page, set the **Schedule type** to your preference.
6. Select the **Start date** and **End date** if required. By default, **No end date** is selected.
7. Adjust the time that you want the schedule to run. This is the time of the machine running the ePO server. Click **Next**. You are presented with a summary of the server task.
8. Select **Save** to finish creating the server task.

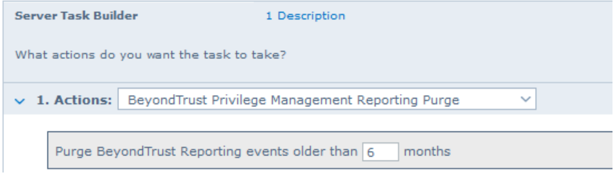
Create the Enterprise Reporting Purge Server Task

You can purge Reporting database events that are older than a defined period in order to manage the size of your database.

1. Navigate to **Menu > Automation > Server Tasks** and select **New Task**.



2. Enter an appropriate name (**BeyondTrust Purge**, for example), leave **Schedule status** as **Enabled**, and click **Next**.
3. Select **BeyondTrust Endpoint Privilege Management Reporting Purge** from the **Actions** dropdown menu.
4. Choose the number of months to purge events older than.



Server Task Builder | 1 Description
What actions do you want the task to take?
1. Actions: BeyondTrust Privilege Management Reporting Purge
Purge BeyondTrust Reporting events older than 6 months

5. On the **Schedule** page set the **Schedule type** to your preference.
6. Select the **Start date** and **End date**, if required. By default, **No end date** is selected.

7. Adjust the time that you want the schedule to run. This is the time of the machine running the ePO server. Click **Next**. You are presented with a summary of the server task.
8. Click **Save** to finish creating the server task.

Manage the Endpoint Privilege Management Databases

Use Endpoint Privilege Management for Windows Events to Build Queries

Endpoint Privilege Management collects and stores a broad set of information about every executed application, which is stored in the Trellix ePO Database. This information can be used in the Trellix ePO Queries and Reports console to create custom dashboard widgets.

Below is a table of all event properties available, and a description of their purpose.

Property	Description
Application Group	The name of the Application Group for the matched application definition
Application Hash	The SHA-1 Hash of the file executed
Application Type	The type of application: APPX - Windows Store Application BAT - Batch File COM - COM Class CONT - Content Control CPL - Control Panel Applet DLL - Dynamic Link Library EXE - Executable MSC - Management Console Snapin MSI - Installer Package OCX - ActiveX Control PS1 - PowerShell Script REG - Registry Settings RPSS - Remote PowerShell Command SVC - Service UNIN - Uninstaller (EXE or MSI) URL - URL Xbin - macOS Binary Xapp - macOS Bundle Xpkg - macOS Package Xsys - macOS System Preference Xsud - macOS Sudo Control
Authorization Challenge	If Challenge/Response Authorization is enabled, the challenge code presented to the user is collected. Otherwise this property remains blank.
Authorization Response	If Challenge/Response Authorization is enabled, the valid shared key entered by the user is collected. Otherwise this property remains blank.
Authorizing Domain User	If Run As Other User is enabled, the domain name of the authorizing user is collected.
Authorizing User SID	If Run As Other User is enabled, the Secure Identifier (SID) of the authorizing user is collected.
Client IP Address	If the user was logged on via a remote session to the computer where Endpoint Privilege Management performed an action, the IPv4 Address of the remote computer is collected.
Client Name	If the user was logged on via a remote session to the computer where Endpoint Privilege Management for Windows performed an action, the name of the remote computer is collected.
COM Application ID	The AppID of the COM elevated application.

Property	Description
COM Class ID	The CLSID of the COM elevated application.
COM Display Name	The common name of the COM elevated application.
Command Line	The command line of the executed application.
Computer Name	The name of the computer where Endpoint Privilege Management for Windows performed an action.
File Name	The full path of the file executed.
File Owner Domain User	The name of the account which owns the executed application.
File Owner User SID	The Secure Identifier (SID) of the account which owns the executed application.
File Version	The file version of the executed application.
Group Description	The description of the Application Group for the matched application definition.
Host SID	The Secure Identifier (SID) of the computer where Endpoint Privilege Management performed an action.
Is Shell	Determines if the application was launched from an On Demand shell menu option. If blank, then a shell menu was not used.
Message Description	The description for the End User Message displayed to the user.
Message Name	The name of the End User Message displayed to the user.
Parent Process File Name	The full path of the parent process that spawned the audited application.
Parent Process ID	The Process Identifier (PID) of the parent process that spawned the audited application.
Parent Process Unique ID	A GUID used to uniquely identify a Process relationships.
PG Event ID	Endpoint Privilege Management for Windows Event Log Event ID.
Policy Description	The description of the policy that matched the executed application.
Policy Name	The name of the policy that matched the executed application.
Process ID	The Process Identifier (PID) of the executed application.
Product Code	The Product Code for an executed MSI, MSU or MSP package.
Product Description	A friendly description for the executed application.
Product Name	The Product Name of the executed application.
Product Version	The product version of the executed application.
Reason	If End User Reason was enabled for an End User Message, the reason entered by the user is collected. If blank, then End User Reason was disabled in the message.
Source URL	If the application was downloaded, then the full URL of where the application was downloaded from is collected.
Start Time	The time the process was started.
Stop Time	This is a deprecated field and no longer used.
Token Description	The description of the access token applied to the executed application.
Token Name	The name of the access token applied to the executed application.
UAC Triggered	Determines if the application triggered User Account Control (UAC). If blank, then UAC was not triggered.
Upgrade Code	The Upgrade Code for an executed MSI, MSU, or MSP package.
User Name	The name of the user who executed an application.

Property	Description
User SID	The Secure Identifier (SID) of the user who executed an application.
Vendor	The Display Name of the Publisher Certificate who signed the application.
Windows Store App Name	The common name of the Windows Store Application.
Windows Store App Publisher	The Display Name of the Publisher Certificate who signed the Windows Store Application.
Windows Store App Version	The version number of the Windows Store Application.

There are also a number of threat event properties set as part of an Endpoint Privilege Management event:

Property	Description
Action Taken	Friendly name used to identify the type of action performed by Privilege Guard: Auto-Elevated User-Elevated Drop-Admin Passive Discovery Default-Rights Admin-Required Custom-Token Blocked
Event ID	Trellix ePO standardized Privilege Guard Event ID.
Threat Name	Internal name used to identify the type of action performed by Endpoint Privilege Management: ADD_ADMIN SHELL_ADD_ADIM DROP_ADMIN PASSIVE DEFAULT_RIGHTS APPLICATION_RIGHTS CUSTOM PROCESS_BLOCKED

For more information, see "Events in Endpoint Privilege Management for Windows" on page 16.

Database Sizing and Resource Consumption

Data Retention

The Audit Event and Microsoft SQL Server Reporting Services databases used to support BeyondTrust Endpoint Privilege Management Reporting may be hosted and scaled independently.

It's important to identify the length of time that Endpoint Privilege Management audit event data must be retained, as it drives resource utilization projections and initial allocation.

Endpoint Privilege Management Reporting is designed to report on activity in recent time, not as a long term archival data storage solution.

- BeyondTrust provides a database purge utility that may be used to purge data manually, or automatically on a configured period to ensure database growth is capped.
- Unlimited database growth inevitably reduces query execution performance, and increases resource utilization for queries.

***Note:** Prior to purging large sets of data, please ensure your SQL Transaction logs are able to grow to accommodate. It may be necessary to delete data in stages when setting this up for the first time.*

To facilitate your decision making regarding retention time in the Endpoint Privilege Management database, please refer to the following sections in our standard documentation:

- Description of the views of data exposed in Endpoint Privilege Management Reporting.
- Description of the events audited by Endpoint Privilege Management in the Endpoint Privilege Management for Windows Administration Guide.
- Description of the Workstyle parameters. You may consider these as the fields that are collected in the audit events, eventually stored in the Endpoint Privilege Management Audit Events database.

For more information, see the following:

- *Reporting Dashboard Guide at www.beyondtrust.com/docs/privilege-management/windows.htm*
- *"Events in Endpoint Privilege Management for Windows" on page 16*

Database Sizes

The Audit Event database must be sized to accommodate substantial data volume, matching the number of clients generating audit data and the desired retention period.

Database storage requirements may be estimated roughly using the following calculation:

Number of hosts
× Number of events per host per day
× 5Kb per event
× Number of retention days

Example: *An organization of 10,000 hosts, with each host generating an average of 15 events per day, requiring a 30 day retention would require a database capacity of:*

10,000 × 15 × 5 × 30 = 22,500,000Kb, or 21.5Gb

A typical event volume is 10-20 events per host per day and varies based on auditing configuration, user job function (role/Workstyle), and user activity patterns.

Database resource utilization (CPU, memory) is highly variable depending on the hardware platform.

Example Use Case Volumes

Example: *Based on an organization of 10,000 hosts requiring a 42 day (six weeks) retention.*

Discovery: *Between 40 – 60 events per machine per day*

(4.6K per event (based on real world data))

Average total: *67.06GB*

Example: Production: *Between 2 – 10 events per machine per day*

(4.6K per event (based on real world data))

Average total: *5.66GB*

Note: *If the number of events "per machine per day" is raised to 15, then the average total increases to 16.99GB*

Key considerations

Volume of inbound audit event records

As seen above, the number of events per hour may be estimated following simple calculations.

Queries triggered from MSFT SQL Reporting Services Reports

As the database grows in size, the resource impact of the reporting platform queries becomes important.

The volume of data maintained in the audit event database affects the duration and resource cost of these queries.

To maintain good performance, we recommend using the Reporting Purge Utility to limit the timespan of audit event data retained in the database.

More finely grained audit data management and cleanup is possible using the Reporting Database Administration Dashboard. Using the dashboard, purge audits related to specific applications and suppress incoming items related to those applications.

Prior to purging large sets of data, please ensure your SQL Transaction logs can grow to accommodate. It may be necessary to delete data in stages when setting this up for the first time.

> ℹ *For more information, see the Reporting Dashboard Guide at www.beyondtrust.com/docs/privilege-management/windows.htm.*

ePO Endpoint Privilege Management Database Events

Table Column Name	Description
AppGroupDescription	Description of the Endpoint Privilege Management for Windows Application Group that matched the process referenced in the event.
AppGroupName	Name of the Endpoint Privilege Management for Windows Application Group that matched the process referenced in the event.
ApplicationHash	The SHA-1 hash of the process referenced in the event.
ApplicationType	File extension of the process referenced in the event.
ApplicationPolicyDescription	Description of the Application Rule which matched the process referenced in the event.
ApplicationPolicyId	Unique identifier of the Application Rule which matched the process referenced in the event.
AppxName	Name of the Windows Store application referenced in the event.
AppxPublisher	Digital signature of the Windows Store application referenced in the event.
AppxVersion	Vendor assigned version number assigned to the Windows Store application referenced in the event.
AuthorizationChallenge	If available, the 8 digit challenge code presented to the user.
AuthorizingDomainUser	The name of the user that satisfied the Designated User requirement of the event.
AuthorizingUserSID	The Security Identifier (SID) of the user that satisfied the Designated User requirement of the event.
AutoID	Unique reference assigned to the event entry in the table.
ClientName	Name of endpoint which connected using a remote session.
ClientPV4	V4 IP address of client who connected using a remote session.
CommandLine	The command line of the process referenced in the event.
COMAppID	The unique identifier of the application associated to the COM CLSID.
COMCLSID	The unique identifier of the COM class object referenced in the event.
COMDisplayName	The name of the COM class object referenced in the event.
DomainUser	The username of the user session who started the process.
DriveType	The type of drive from which the process was being executed.
EventID	The Endpoint Privilege Management for Windows ID for the event type.
FileName	FileName
FileOwnerDomainUser	The name of the user that is the NTFS owner of the process referenced in the event.
FileOwnerUserSID	The Security Identifier (SID) of the user that is the NTFS owner of the process referenced in the event.
FileVersion	File version of the process referenced in the event.
HostName	The name of the host upon which the process referenced in the event executed.
HostID	The Security Identifier (SID) of the host upon which the process referenced in the event executed.
MessageDescription	Description of the Endpoint Privilege Management for Windows message that matched the process referenced in the event.
MessageName	Name of the Endpoint Privilege Management for Windows message that matched the process referenced in the event.
ParentID	Unique ID assigned by Windows to the parent process of the process referenced in the event.
ParentProcessFileName	Name of the parent process of the process referenced in the event.

Table Column Name	Description
ParentProcessGUID	Unique reference assigned by Endpoint Privilege Management for Windows to the parent process of the process referenced in the event.
PID	Unique ID assigned by Windows to the process referenced in the event.
PolicyDescription	Description of the Endpoint Privilege Management for Windows policy that matched the process referenced in the event.
PolicyName	Name of the Endpoint Privilege Management for Windows policy that matched the process referenced in the event.
PowerShellCommand	If available, the PowerShell cmdlet referenced in the event.
ProcessGUID	Unique reference assigned by Endpoint Privilege Management for Windows to the process referenced in the event.
ProcessStartTime	Time that the process referenced in the event started.
ProductCode	Product Code assigned to the process referenced in the event.
ProductDescription	Product Description assigned by the vendor to the process referenced in the event.
ProductName	Product Name assigned by the vendor to the process referenced in the event.
ProductVersion	Product Version assigned by the vendor to the process referenced in the event.
Publisher	Digital signature assigned by the vendor to the process referenced in the event.
Reason	Details of the reason provided by the user for using the process referenced in the event.
ServiceDisplayName	The Display name of the Windows service referenced in the event.
ServiceName	The Service name of the Windows service referenced in the event.
SourceURL	If available, the URL from which the process referenced in the event was downloaded.
TokenAssignmentIsShell	Binary flag to indicate if the process was launched using the shell integration feature.
TokenDescription	Description of the token applied by Endpoint Privilege Management for Windows to the process referenced in the event.
TokenName	Name of the token applied by Endpoint Privilege Management for Windows to the process referenced in the event.
TrustedApplicationName	Name of the trusted application that triggered the rule.
TrustedApplicationVersion	Version of the trusted applicaiton that triggered the rule.
UACTriggered	Flag to indicate if the process matched on a UACTriggered rule.
UpgradeCode	Upgrade Code assigned to process referenced in the event.
UserSID	The Security Identifier (SID) of the user who started the process.

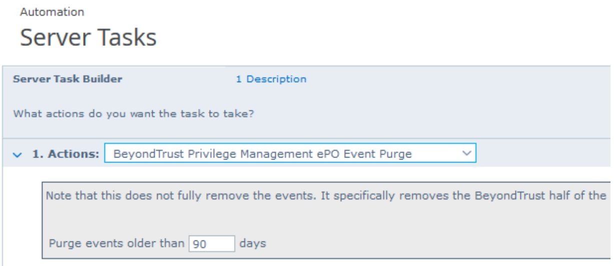
Note: *No individual event returns values in all fields, so it is expected behavior to have NULL values in task specific columns.*

Create the ePO Event Purge Server Task

We recommend you use the default ePO server task for this called **Purge Rolled-up Data**. This removes threat events from the ePO database and the corresponding Reporting events from the **BeyondTrust** table.

If you have a business need to delete the report events from the **BeyondTrust** table in only the ePO database, follow these instructions:

1. Navigate to **Menu > Automation > Server Tasks** and select **New Task**.
2. Enter an appropriate name (**BeyondTrust ePO Threat Purge**, for example), leave the **Schedule status** as **Enabled**, and click **Next**.
3. Select **BeyondTrust Endpoint Privilege Management ePO Event Purge** from the **Actions** dropdown menu.



Automation

Server Tasks

Server Task Builder

1 Description

What actions do you want the task to take?

1. Actions: BeyondTrust Privilege Management ePO Event Purge

Note that this does not fully remove the events. It specifically removes the BeyondTrust half of the

Purge events older than 90 days

4. Depending on your data size and requirements, enter the number of days after which events should be purged and click **Next**.

ePolicy Orchestrator Server Scripts

ePO Core Commands are all available in the **core.help** file and are listed here:

```
https://[ePO Server]:8443/remote/core.help
avecto.challengeResponse keyType key challenge [duration] - BeyondTrust Privilege Management
Challenge Response
```

Parameter Descriptions

```
keyType=Key Type [key|name|id]
key=[Key Value|Policy Name|Policy ID]
challenge=Challenge Code
duration=Duration [once(default)|session]
avecto.createPolicy policyName filePath - BeyondTrust Privilege Management Create New Policy
avecto.exportPolicy policyID - BeyondTrust Privilege Management Export Policy XML
avecto.importPolicy policyID filePath - BeyondTrust Privilege Management Import Policy XML
avecto.listPolicies - rcmd.listPolicies.shortDescKey
```

For more information, please refer to Explanation of ePO Web API and where to find Web API documentation, at https://kcm.trellix.com/corporate/index?page=content&id=KB81322.

Referenced Libraries

Two libraries are referenced in these scripts:

- McAfee python Support Library
- URL Encoder Support Library

Challenge Response Scripting

```
import mcafee
import sys
mc = mcafee.client('[ePOServerAddress]','8443','[username]','[password]')
mc.help('avecto.challengeResponse')
print '\nKey based generation'
response = mc.avecto.challengeResponse('key','test','12345678')
print 'response for one use - test/12345678: %s' % (response)
response = mc.avecto.challengeResponse('key','test','98765432X','once')
print 'response for once    - test/98765432X: %s' % (response)
response = mc.avecto.challengeResponse('key','test','98765432X','session')
print 'response for session - test/98765432X: %s' % (response)

policies = mc.avecto.listPolicies()
id = 0
print '\nAll Policies...'
```

```
for policy in policies:
print 'name: %s ID: %d' % (policy['name'],policy['id'])
if (policy['name'] == 'NewSimpleCR'):
id = policy['id']
print '\nNamed Policy generation'
response = mc.avecto.challengeResponse('name','NewSimpleCR','12345678')
print 'response for one use - 12345678: %s' % (response)
response = mc.avecto.challengeResponse('name','NewSimpleCR','98765432X','once')
print 'response for once    - 98765432X: %s' % (response)
response = mc.avecto.challengeResponse('name','NewSimpleCR','98765432X','session')
print 'response for session - 98765432X: %s' % (response)

print '\nID Policy generation for id %d' % id
response = mc.avecto.challengeResponse('id',id,'12345678')
print 'response for one use - 12345678: %s' % (response)
response = mc.avecto.challengeResponse('id',id,'98765432X','once')
print 'response for once    - 98765432X: %s' % (response)
response = mc.avecto.challengeResponse('id',id,'98765432X','session')
print 'response for session - 98765432X: %s' % (response)
```

ePO Create Policy

```
import mcafee
import sys
mc = mcafee.client('[ePOServerAddress]','8443','[username]','[password]')
mc.help('avecto.createPolicy')
print '\nCreate New Policy called NewSimpleCR'
#resp = mc.avecto.createPolicy('NewSimpleCR','file:///path-to-policy/policy.xml')
resp = mc.avecto.createPolicy('NewSimpleCR','file:///policy.xml')
print '\nPolicy Create Response: %s' % resp
policies = mc.avecto.listPolicies()
print '\nAll Policies...'
for policy in policies:
print 'name: %s ID: %d' % (policy['name'],policy['id'])
```

ePO Import Policy

```
import mcafee
import sys
mc = mcafee.client('[ePOServerAddress]','8443','[username]','[password]')
mc.help('avecto.listPolicies')
policies = mc.avecto.listPolicies()
print '\nJSON %s' % (policies)
id = 0
print '\nAll Policies...'
for policy in policies:
print 'name: %s ID: %d' % (policy['name'],policy['id'])
if (policy['name'] == 'My Default'):
id = policy['id']
resp = mc.avecto.importPolicy(id,'file:///policy.xml')
print '\nPolicy Import Response: %s' % resp
```

ePO Export Policy

```
import mcafee
import sys
mc = mcafee.client('[ePOServerAddress]','8443','[username]','[password]')
mc.help('avecto.listPolicies')
policies = mc.avecto.listPolicies()
print '\nJSON %s' % (policies)
id = 0
print '\nAll Policies...'
for policy in policies:
print 'name: %s ID: %d' % (policy['name'],policy['id'])
if (policy['name'] == 'My Default'):
id = policy['id']
xml = mc.avecto.exportPolicy(id)
print '\nPolicy XML:\n%s' % xml
```

Exported Views in Endpoint Privilege Management for Windows

Indexes are indicated by numbers. If the number applies to more than one column, it is a composite index. If an index has an asterisk (*) then this is an index based on an ID, which is used to retrieve the indicated columns. This means the index may be usable depending on how the query is formed. Descriptions in italics refer to one of the following data types:

- "Custom Data Types" on page 36
- "Application Types" on page 37
- "Chassis Types" on page 38
- "OS Version" on page 39
- "OS Product Type" on page 40
- "Message Types" on page 41
- "Certificate Modes" on page 42
- "Policy Audit Modes" on page 43
- "Device Types (Drive Type)" on page 44
- "ExportDefendpointStarts" on page 45
- "ExportLogons" on page 46
- "ExportPrivilegedAccountProtection" on page 47
- "ExportProcesses" on page 49

Custom Data Types

Data Type	Description
Ascending identity	Number that increases with every event. Designed to allow external applications to pick up where they last got up to when importing events from PMR.
Locale Identifier	ID of language etc.
Platform Type	**Windows** or **macOS**

For more information, see Microsoft's list of Locale ID Values at https://docs.microsoft.com/en-us/previous-versions/windows/embedded/ms912047(v=winembedded.10).

Application Types

Application Type	Description
appx	Windows Store package
bat	Batch file
com	COM class
cpl	Control Panel
exe	Executable
msc	MMC Snap-in
msi	Installer package
ocx	ActiveX control
ps1	PowerShell script
reg	Registry settings file
rpsc	Remote PowerShell Command
rpss	Remote PowerShell Script
svc	Service
unin	Uninstaller
wsh	Windows script (examples: vbs, js)
cont	Content file
url	URL

Chassis Types

Chassis Type	Description
NULL	Not set
<None>	Does not have a chassis type
Desktop	Desktop
Docking Station	Docking station
Laptop	Laptop
Notebook	Notebook
Other	Other (unknown) type
Portable	Portable system
Rack Mount Chassis	Rack system

OS Version

Taken from https://docs.microsoft.com/en-us/windows/win32/sysinfo/operating-system-version.

Version Number	Operating System
10.0	Windows 10 or Windows Server 2016
6.3	Windows 8.1 or Windows Server 2012 R2
6.2	Windows 8.1 or Windows Server 2012 R2
6.1	Windows 7 or Windows Server 2008R2
6.0	Windows Vista or Windows Server 2008
5.2	Windows XP 64-bit or Windows Server 2003 or Windows Server 2003R2
5.1	Windows XP
5.0	Windows 2000

OS Product Type

OS Product Type	Operating System
1	Workstation
2	Domain Controller
3	Server
[any other value]	Unknown

Message Types

Message Type	Description
<None>	No message
Prompt	Prompt message
Notification	Notification (balloon) message
Unknown	Unknown message type

Certificate Modes

Endpoint Privilege Management for Windows verifies that an optionally signed Endpoint Privilege Management for Windows configuration has been signed using a certificate trusted for the purpose on any signed settings that it loads.

The Endpoint Privilege Management ePO extension does not support the distribution of signed Endpoint Privilege Management for Windows configuration. The Endpoint Privilege Management ePO extension must be installed in certificate mode 0, if used.

Mode	Name	Description
0	Standard Mode	The loading of unsigned settings is audited as information events (event 200). Signed settings are audited as information events (event 200) if they are correctly signed and as warning events (event 201) if they are incorrectly signed. Endpoint Privilege Management for Windows is installed in Standard Mode by default.
1	Certificate Warning Mode	The loading of unsigned settings is audited as warning events (event 201). Signed settings are audited as information events (event 200) if they are correctly signed and as warning events (event 201) if they are incorrectly signed.
2	Certificate Enforcement Mode	Unsigned or incorrectly signed settings are not loaded and are audited as error events (event 202). Signed settings are audited as information events (event 200) if they are correctly signed.

Policy Audit Modes

Mode	Name	Description
0	No auditing	Value is **0** in endpoint registry.
4	Audit Errors Only	202 events. Value is **1** in endpoint registry.
6	Audit Warnings and Errors	201/202 events. Default for agent and console installations. Value is **2** in endpoint registry.
7	Audit Information, Warnings and Errors	200/201/202 events. Default for agent only installations. Value is **3** in endpoint registry.

Device Types (Drive Type)

DeviceType (Drive Type)	Description
CDROM Drive	CD/DVD drive
eSATA Drive	External drive
Downloaded	Downloaded from internet
Network Drive	Network drive
Removable Media	Removable Media
Unknown Drive	Unknown
USB Drive	USB drive

ExportDefendpointStarts

Column_name	Type	Length	Index	Description	Example
SessionID	bigint		3	Ascending Identity	1
SessionGUID	uniqueidentifier			UUID of the session	5CD221E9-CEB5-441D-B380-CB266400B320
SessionStartTime	datetime			Time session started	2017-01-03 10:24:00.000
SessionEndTime	datetime			Always NULL (not used)	NULL
HostSID	nvarchar	200	1	Host SID	S-1-21-123456789-123456789-1635717638-390614945
AgentVersion	nvarchar	20		Endpoint Privilege Management Client Version	4.0.384.0
ePOMode	int			1 if DP client is in ePO mode. 0 otherwise.	1
CertificateMode	int			Certificate Mode	0
PolicyAuditMode	int			Policy Audit Mode	7
DefaultUILanguage	int			Locale Identifier of UI Language	2057
DefaultLocale	int			Locale Identifier of Locale	2057
SystemDefaultTimezone	int			Not set so always 0	0
ChassisType	nvarchar	40		Chassis Type	Other
HostName	nvarchar	1024	2*	Host name	EGHostWin1
HostNameNETBIOS	nvarchar	15	2*	Host NETBIOS	EGHOSTWIN1
OS	nvarchar	20		OS Version	6.3
OSProductType	int	4		OS Product Type.	1
PlatformType	nvarchar	10		Platform Type	Windows
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomainNameNETBIOS	nvarchar	15		Host Domain NETBIOS	EGDOMAIN

ExportLogons

Column_name	Type	Length	Index	Description	Example
LogonID	bigint		3	Ascending Identity	1
LogonGUID	uniqueidentifier			UUID of the logon	819EF606-F9B6-40BE-9C0C-A033A34EC4F8
HostSID	nvarchar	200	1	Host SID	S-1-21-123456789-123456789-1635717638-390614945
UserSID	nvarchar	200		User SID	S-1-21-123456789-123456789-1635717638-1072059836
LogonTime	datetime			Logon Date/Time	2017-01-03 10:24:00.000
IsAdmin	bit			1 if an admin, 0 otherwise	0
IsPowerUser	bit			1 if a power user, 0 otherwise	0
UILanguage	int			Locale Identifier of the UI Language	1033
Locale	int			Locale Identifier of the Locale	2057
UserName	nvarchar	1024		User name	EGUser1
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserNameNETBIOS	nvarchar	15		User NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Docking Station
HostName	nvarchar	1024	2*	Host name	EGHostWin1
HostNameNETBIOS	nvarchar	15	2*	Host NETBIOS	EGHOSTWIN1
OS	nvarchar	20		OS Version	6.3
OSProductType	int			OS Product Type	1
PlatformType	nvarchar	10		Platform Type	Windows
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomainNameNETBIOS	nvarchar	15		Host Domain NETBIOS	EGDOMAIN
PolicyName	nvarchar	1024		Policy Name	EventGen Test Policy
WorkstyleName	nvarchar	1024		Workstyle name	EventGen Test Workstyle

ExportPrivilegedAccountProtection

Column_name	Type	Length	Index	Description	Example
ID	bigint		1	Ascending Identity	1
TimeGenerated	datetime			Event Generation Date/Time	
CommandLine	nvarchar	1024		Command Line	<None>
PrivilegedGroupName	nvarchar	200		Privileged Group Name	Administrators
PrivilegedGroupRID	nvarchar	10		Privileged Group Relative Identifier	544
Access	nvarchar	200		Group Access Details	Add Member&#44; Remove Member&#44; List Members&#44; Read Information
PolicyGUID	uniqueidentifier			Policy UUID	E7654321-AAAA-5AD2-B954-12342918D604
PolicyName	nvarchar	1024		Policy Name	EventGen Test Policy
WorkstyleName	nvarchar	1024		Workstyle name	EventGen Test Workstyle
FileName	nvarchar	255		File name	<None>
ApplicationHash	nvarchar	40		Application SHA1	921CA2B3293F3FCB905B24A9536D8525461DE2A3
ProductCode	nvarchar	1024		Product Code	<None>
UpgradeCode	nvarchar	1024		Upgrade Code	<None>
FileVersion	nvarchar	1024		File Version	<None>
MD5	nvarchar	32		MD5 Hash	3279476E39DE235B426D69CFE8DEBF55
UserSID	nvarchar	200		User SID	S-1-21-123456789-123456789-1635717638-1072059836
UserName	nvarchar	1024		User Name	EGUser1
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserNameNETBIOS	nvarchar	15		User Domain NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Other

Column_name	Type	Length	Index	Description	Example
HostSID	nvarchar	200		Host SID	S-1-21-123456789-123456789-1635717638-390614945
HostName	nvarchar	1024		Host Name	EGHostWin1
HostNameNETBIOS	nvarchar	15		Host NETBIOS	EGHOSTWIN1
OS	nvarchar	20		OS Version	6.3
OSProductType	int			OS Product Type	1
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomainNameNETBIOS	nvarchar	15		Host domain NETBIOS	EGDOMAIN
FileOwnerUserSID	nvarchar	200		File Owner SID	S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464
FileOwnerUserName	nvarchar	1024		File Owner	NT SERVICE\TrustedInstaller
FileOwnerDomainName	nvarchar	1024		File Owner Domain	NT SERVICE
ApplicationURI	nvarchar	1024		URI of a macOS application	com.apple.preference.datetime
ApplicationDescription	nvarchar	2048		Application description	lusrmgr.msc
FirstDiscovered	datetime			First time app was seen	2017-01-03 10:25:50.110
FirstExecuted	datetime			First time app was executed	2017-01-03 10:24:00.000
PlatformType	nvarchar	10		Platform Type	Windows
ProductName	nvarchar	1024		Product name	<None>
ProductVersion	nvarchar	1024		Product version	<None>
Publisher	nvarchar	1024		Publisher	Microsoft Windows
TrustedOwner	bit			1 if a trusted owner, 0 otherwise	1

ExportProcesses

Column_name	Type	Length	Index	Description	Example
ProcessID	bigint		4	Ascending Identity	1
ProcessGUID	uniqueidentifier		2	UUID of the process	98C99D96-6DFA-4C95-9A87-C8665C166286
EventNumber	int			Event Number. See List of Events section.	153
TimeGenerated	datetime			Event generation date/time	2017-02-20 13:11:11.217
TimeReceived	datetime			Event received at ER date/time	2017-02-20 13:16:28.047
EventGUID	uniqueidentifier			Event UUID	9F8EB86C-AA0D-42B9-8720-166FAB91F1ED
PID	int			Process ID	8723
ParentPID	int			Parent Process ID	142916
CommandLine	nvarchar		1024	Command Line	"C:\cygwin64\bin\sh.exe"
FileName	nvarchar		255	File Name	c:\cygwin64\bin\sh.exe
ProcessStartTime	datetime		1	Date/Time Process Started	2017-02-20 13:11:11.217
Reason	nvarchar		1024	Reason entered by user	<None>
ClientIPV4	nvarchar		15	Client IP Address	10.0.9.58
ClientName	nvarchar		1024	Client Name	L-CNU410DJJ7
UACTriggered	bit			1 if UAC shown	0
ParentProcessUniqueID	uniqueidentifier			Parent process UUID	C404C7F5-3A93-4C0E-81BC-9902D220C21E
COMCLSID	uniqueidentifier			COM CLSID	NULL
COMAppID	uniqueidentifier			COM Application ID	NULL
COMDisplayName	nvarchar	1024		COM Display Name	<None>
ApplicationType	nvarchar	4		Application Type	svc
TokenGUID	uniqueidentifier			UUID of token in policy	F30A3824-27AF-4D69-9125-C78E44764AC1
Executed	bit			1 if executed, 0 otherwise	1
Elevated	bit			1 if elevated, 0 otherwise	1

Column_name	Type	Length	Index	Description	Example
Blocked	bit			1 if blocked, 0 otherwise	0
Passive	bit			1 if passive, 0 otherwise	0
Cancelled	bit			1 if cancelled, 0 otherwise	0
DropAdmin	bit			1 if admin rights dropped, 0 otherwise	0
EnforceUsersDefault	bit			1 if user default permissions were enforced, 0 otherwise	0
Custom	bit			1 if Custom Token, 0 otherwise	0
SourceURL	nvarchar	2048		Source URL	<None>
AuthorizationChallenge	nvarchar	9		Challenge Response authorization code	<None>
WindowsStoreAppName	nvarchar	200		Windows Store application name (appx app type only)	<None>
WindowsStoreAppPublisher	nvarchar	200		Windows Store application publisher (appx app type only)	<None>
WindowsStoreAppVersion	nvarchar	200		Window Store application version (appx app type only)	<None>
DeviceType	nvarchar	40		Device Type	Fixed Disk
ServiceName	nvarchar	1024		Service name (svc events only)	<None>
ServiceDisplayName	nvarchar	1024		Service Display Name (svc app type only)	<None>
PowerShellCommand	nvarchar	1024		PowerShell Command (ps1/rpsc/rpss app types only)	<None>
ApplicationPolicyDescription	nvarchar	1024		Policy Description	<None>

Column_name	Type	Length	Index	Description	Example
SandboxGUID	uniqueidentifier			Sandbox UUID (sandbox events only)	NULL
SandboxName	nvarchar	1024		Sandbox Name (sandbox events only)	NULL
BrowseSourceURL	nvarchar	2048		Sandbox browse source (sandbox events only)	<None>
BrowseDestinationURL	nvarchar	2048		Sandbox destination source (sandbox events only)	<None>
Classification	nvarchar	200		Sandbox classification (sandbox events only)	Private (Local)
IEZoneTag	nvarchar	200		IE Zone Tag	<None>
OriginSandbox	nvarchar	40		Origin Sandbox	<None>
OriginIEZone	nvarchar	40		Origin IE Zone	<None>
TargetSandbox	nvarchar	40		Target Sandbox	<None>
TargetIEZone	nvarchar	40		Target IE Zone	<None>
AuthRequestURI	nvarchar	1024		Authorization request URL (osx challenge/response only)	<None>
PlatformVersion	nvarchar	10		Platform Version	<None>
ControlAuthorization	bit			1 is Endpoint Privilege Management authorized this macOS application	0
TrustedApplicationName	nvarchar	1024		Name of the trusted application	Microsoft Word
TrustedApplicationVersion	nvarchar	1024		Version of the trusted application	11.1715.14393.0
ParentProcessFileName	nvarchar	1024		Parent process file name	Google Chrome
ApplicationHash	nvarchar	40		SHA1 of the application	C22FF10511ECCEA1824A8DE64B678619C21B4BEE
ProductCode	nvarchar	1024		Product Code	<None>
UpgradeCode	nvarchar	1024		Upgrade Code	<None>
FileVersion	nvarchar	1024		File Version	<None>

Column_name	Type	Length	Index	Description	Example
MD5	nvarchar	32		MD5 hash of the app	6E641CAE42A2A7C89442AF99613FE6D6
TokenAssignmentGUID	uniqueidentifier			UUID of the token assignment in the policy	E7654321-BBBB-5AD2-B954-1234DDC7A89D
TokenAssignmentIsShell	bit			Token assignment is for shell	1
UserSID	nvarchar	200		User SID	S-1-21-123456789-123456789-16357176381125883508
UserName	nvarchar	1024		User Name	EGUser18
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserDomain NameNETBIOS	nvarchar	15		User Domain NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Laptop
HostSID	nvarchar	200		Host SID	S-1-21-123456789-123456789-1635717638775838649
HostName	nvarchar	1024	3*	Host Name	EGHostWin18
HostNameNETBIOS	nvarchar	15	3*	Host NETBIOS	EGHOSTWIN18
OS	nvarchar			OS Version	10.0
OSProductType	int			OS Product Type	
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomain NameNETBIOS	nvarchar	15		Host Domain NETBIOS	EGDOMAIN
AuthUserSID	nvarchar	200		Authorizing User SID	<None>
AuthUserName	nvarchar	1024		Authorizing User	<None>
AuthUserDomainSID	nvarchar	200		Authorizing User Domain SID	<None>
AuthUserDomainName	nvarchar	1024		Authorizing User Domain	<None>
AuthUserDomain NameNETBIOS	nvarchar	15		Authorizing User Domain NETBIOS	<None>
FileOwnerUserSID	nvarchar	200		File Owner SID	S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464
FileOwnerUserName	nvarchar	1024		File Owner	NT SERVICE\TrustedInstaller
FileOwnerDomainSID	nvarchar	200		File Owner Domain SID	S-1-5-80
FileOwnerDomainName	nvarchar	1024		File Owner Domain	NT SERVICE

Column_name	Type	Length	Index	Description	Example
FileOwnerDomainNameNETBIOS	nvarchar	15		File Owner Domain NETBIOS	<None>
ApplicationURI	nvarchar	1024		URI of the macOS Application	com.apple.preference.datetime
ApplicationDescription	nvarchar	2048		Application Description	c:\cygwin64\bin\sh.exe
FirstDiscovered	datetime			Time application first seen	2017-02-07 09:14:39.413
FirstExecuted	datetime			Time application first executed	2017-02-07 09:07:00.000
PlatformType	nvarchar	10		Platform Type	Windows
ProductName	nvarchar	1024		Product Name	ADelRCP Dynamic Link Library
ProductVersion	nvarchar	1024		Product Version	15.10.20056.167417
Publisher	nvarchar	1024		Publisher	Adobe Systems, Incorporated
TrustedOwner	bit			1 if a trusted owner, 0 otherwise	0
MessageGUID	uniqueidentifier			UUID of the message in the policy	00000000-0000-0000-0000-000000000000
MessageName	nvarchar	1024		Name of the message in the policy	Block Message
MessageType	nvarchar	40		Message Type	Prompt
AppGroupGUID	uniqueidentifier			UUID of the Application Group in the Policy	47E4A204-FC06-428B-8E73-1E36E3A65430
AppGroupName	nvarchar	1024		Application Group Name in the Policy	Test Policy.test
PolicyID	bigint			Internal ID of the Policy	2
PolicyGUID	uniqueidentifier			UUID of the Policy	E7654321-AAAA-5AD2-B954-12342918D604
PolicyName	nvarchar	1024		Policy Name	EventGen Test Policy
WorkstyleName	nvarchar	1024		Workstyle Name	EventGen Test Workstyle
ContentFileName	nvarchar	255		Content File Name	c:\users\user.wp-epo-win7-64\downloads\con29 selectable feestable (1).pdf
ContentFileDescription	nvarchar	1024		Content File Description	<None>
ContentFileVersion	nvarchar	1024		Content File Version	<None>
ContentOwnerSID	nvarchar	200		Content Owner SID	S-1-21-123456789-123456789-1635717638-1072059836

Column_name	Type	Length	Index	Description	Example
ContentOwnerName	nvarchar	1024		Content Owner	EGUser1
ContentOwnerDomainSID	nvarchar	200		Content Owner Domain SID	S-1-5-21-2217285736-120021366-3854014904
ContentOwnerDomainName	nvarchar	1024		Content Owner Domain	BEYONDTRUST TEST58\BEYONDTRUSTTEST58.QA
ContentOwnerDomain NameNetBIOS	nvarchar	15		Content Owner Domain NETBIOS	BEYONDTRUSTTEST58
UninstallAction	nvarchar	20		The uninstall action carried out	Change/Modify
TokenName	nvarchar	20		The name of the event action	Blocked
TieStatus	int			Threat Intelligence Exchange status for the reputation of this application	0
TieScore	int			Threat Intelligence Exchange score for the application	
VtStatus	int			VirusTotal status for the reputation of this application	
RuleScriptFileName	nvarchar	200		The name in config of the script associated with the rule	Get-McAfeeGTIReputation
RuleScriptName	nvarchar	200		The name of the script set by interface	Get-McAfeeGTIReputation
RuleScriptVersion	nvarchar	20		Version number of the script.	1.1.0
RuleScriptPublisher	nvarchar	200		Publisher that signed the script	BeyondTrust
RuleScriptRuleAffected	bit			True when the script has set all settable rule properties; otherwise false	True
RuleScriptStatus	nvarchar	100		Success OR Why the configured script didn't run or set rule properties	Success
RuleScriptResult	nvarchar	1024		Result of the script run	Script ran successfully
RuleScriptOutput	nvarchar	1024		The output of the script	

Column_name	Type	Length	Index	Description	Example
AuthorizationSource	nvarchar	200		The Authorizing User Credential Source	
AuthMethods	nvarchar	1024		The type of authentication method selected in the Policy Editor.	Possible values: Identity Provider, Password, Challenge Response, Smart Card and User Request. Multiple values can be present and will be comma separated.
IdPAuthentication	nvarchar	400		The credential provided when adding an Identity Provider authorization message in the Policy Editor.	

Troubleshoot Endpoint Privilege Management for Windows

Check Endpoint Privilege Management for Windows is installed and functioning

If you are having problems, the first step is to check that you have installed the client and that the client is functioning.

The easiest way to determine that the client is installed and functioning is to check for the existence of the BeyondTrust Endpoint Privilege Management Management Console service. Ensure that this service is both present and started. The Endpoint Privilege Management service is installed by Endpoint Privilege Management for Windows and should start automatically.

> ***Note:*** *The Endpoint Privilege Management service requires MSXML6 in order to load the Endpoint Privilege Management for Windows settings, but the service runs even if MSXML6 is not present.*
>
> *Windows 7 and Windows 10 already include MSXML6.*

Check Settings are Deployed

Assuming Endpoint Privilege Management for Windows is installed and functioning, the next step is to check that you have deployed settings to the computer or user.

ePO policies are stored by Endpoint Privilege Management as an XML file in the following location:

%ProgramData%\Avecto\Privilege Guard\ePO Cache\Machine\PrivilegeGuardConfig.xml

Check that Endpoint Privilege Management is Licensed

One of the most common reasons for Endpoint Privilege Management not functioning is the omission of a valid license from the Endpoint Privilege Management settings. If you create multiple policies, then you must ensure that the computer or user receives at least one GPO that contains a valid license. To avoid problems, it is simpler to add a valid license to every set of Endpoint Privilege Management settings that you create.

Check Workstyle Precedence

Assuming that Endpoint Privilege Management is functioning and licensed, most other problems are caused by configuration problems or Workstyle precedence problems. Please be aware that if you have multiple policies, these are evaluated in alphanumeric order.

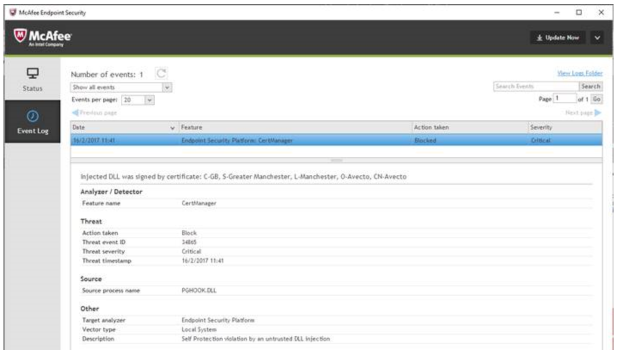
Once an application matches an Application Group entry in the **Application Rules** or the **On-Demand Application Rules**, then processing does not continue for that application. Therefore, it is vital that you order your entries correctly:

- If you create multiple Workstyles, then Workstyles higher in the list have higher precedence.
- If you have multiple rules in the Application Rules and the On-Demand Application Rules sections of a Workstyle, then entries higher in the list have higher precedence.

Application Rules are applied to applications that are launched either directly by the user or by a running process. **On-Demand Application Rules** are only applied to applications that are launched from the Endpoint Privilege Management shell menu (if enabled).

Certificate Error in Trellix Endpoint Security (ENS)

A certificate error is shown on the endpoint in the Event Log for Trellix Endpoint Security (ENS) if Endpoint Privilege Management was installed prior to Trellix Endpoint Security.



Number of events: 1

Show all events

Events per page: 20

Page 1 of 1 Go

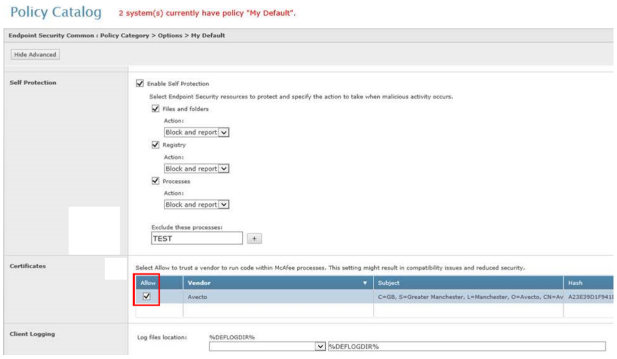
Date	Feature	Action taken	Severity
16/2/2017 11:41	Endpoint Security Platform: CertManager	Blocked	Critical

Injected DLL was signed by certificate: C-GB, S-Greater Manchester, L-Manchester, O-Avecto, CN-Avecto

Analyzer / Detector	
Feature name	CertManager
Threat	
Action taken	Block
Threat event ID	34865
Threat severity	Critical
Threat timestamp	16/2/2017 11:41
Source	
Source process name	PGHOOK.DLL
Other	
Target analyzer	Endpoint Security Platform
Vector type	Local System
Description	Self Protection violation by an untrusted DLL injection

Add the Certificate for Endpoint Privilege Management:

1. Navigate to **Policy Catalog** and select **Trellix Endpoint Security** from the **Product** dropdown menu.
2. In the **Self Protection** section, navigate to the **Certificates** section and check the **Allow** box. This allows BeyondTrust processes to be trusted.



2 system(s) currently have policy "My Default".

Endpoint Security Common : Policy Category > Options > My Default

Self Protection

☑ Enable Self Protection

Select Endpoint Security resources to protect and specify the action to take when malicious activity occurs.

☑ Files and folders
Action: Block and report

☑ Registry
Action: Block and report

☑ Processes
Action: Block and report

Exclude these processes: TEST

Certificates

Select Allow to trust a vendor to run code within McAfee processes. This setting might result in compatibility issues and reduced security.

Allow	Vendor	Subject	Hash
☑	Avecto	C=GB, S=Greater Manchester, L=Manchester, O=Avecto, CN=Av	A23E39D1F941

Client Logging

Log files location: %DEFLOGDIR% %DEFLOGDIR%

3. Click **Save**.

This resolves the error encountered when using BeyondTrust Endpoint Privilege Management and Trellix Endpoint Security software.