



# BeyondTrust

## **Privilege Management for Windows ePO Extension 21.1 Administration Guide**

## Table of Contents

---

<b>Privilege Management for Windows ePO Extension Administration</b> .....	<b>11</b>
Define User Roles .....	11
Implement Least Privilege .....	11
About McAfee ePolicy Orchestrator .....	12
Privilege Management for Windows and McAfee .....	12
Install, Uninstall, and Upgrade Privilege Management for Windows .....	14
Frequently Asked Questions .....	14
Install the Privilege Management for Windows Clients .....	14
Uninstall the Privilege Management for Windows Clients .....	14
Upgrade Privilege Management for Windows .....	14
Recommended Steps .....	14
Step 1: Upgrade Application Groups to Match Publisher Name BeyondTrust Corporation .....	15
Step 2: Upgrade the Privilege Management ePO Extension .....	17
Step 3: Upgrade Privilege Management Reporting (if in use) .....	17
Step 4: Upgrade Privilege Management for Windows Clients .....	18
Step 5: Delete Old Application Definitions (Upgrade from 5.4) .....	18
Manual Database Upgrade .....	18
Manual Deployment of Privilege Management for Windows .....	19
Prerequisites .....	19
Disable ePO Mode .....	20
Launch the ePO Policy Catalog to View Policies .....	21
Access the Policy Summary Screen from the Policy Catalog .....	21
Policy Approval .....	22
Apply Policy to Disconnected Users .....	23
Autosave, Autosave Recovery, and Policy Locks .....	23
Autosave .....	23
Autosave Recovery .....	23
Policy Locks .....	24
Privilege Management Policies and Templates .....	25
To Import a Privilege Management XML Configuration .....	25

---

Create a Privilege Management Policy .....	25
Edit Privilege Management Policies .....	25
Windows Policies .....	26
Privilege Management for Windows Policies .....	26
Privilege Management for Windows Workstyles .....	27
Privilege Management Workstyle Properties .....	27
Privilege Monitoring .....	28
Privilege Monitoring Events .....	28
Privilege Monitoring Log Files .....	28
Create a Privilege Management Workstyle .....	28
Disable or Enable Privilege Management Workstyles .....	30
Change Workstyle Precedence in Privilege Management .....	30
Privilege Management for Windows Workstyle Parameters .....	30
Privilege Management Workstyle Summary .....	32
Access the Application Rules .....	33
Precedence for Application and Content Rules .....	35
Create On-Demand Application Rules .....	35
Trusted Application DLL Protection .....	38
Privilege Management Content Rules .....	39
Insert a Content Rule .....	39
View or Edit Workstyle General Rules .....	40
Filters .....	42
Account Filters .....	43
Configure Account Filters .....	43
Computer Filters .....	44
Time Range Filters .....	44
Expiry Filter .....	45
Windows Management Information (WMI) Filters .....	45
Application Groups .....	46
Create an Application Group .....	46
View or Edit the Properties of an Application Group .....	46
Delete an Application Group .....	46
Duplicate an Application Group .....	47

---

Application Definitions .....	47
Application Definition Matching Criteria .....	47
ActiveX Codebase matches .....	48
ActiveX Version matches .....	48
App ID matches .....	48
Application Requires Elevation (UAC) .....	48
Application Requires Elevation (UAC) (Supported on 'Install' only) .....	48
Uninstaller .....	48
BeyondTrust Zone Identifier exists .....	48
CLSID matches .....	48
COM Display Name matches .....	49
Command Line matches .....	49
Drive matches .....	49
File or Folder Name matches .....	49
File Hash (SHA-1 Fingerprint) matches .....	50
File Version matches .....	50
Parent Process matches .....	50
Product Code matches .....	50
Product Description matches .....	50
Product Name matches .....	50
Product Version matches .....	50
Publisher matches .....	50
Service Actions match .....	51
Service Display Name matches .....	51
Service Name matches .....	51
Source URL matches .....	51
Trusted Ownership matches .....	52
Upgrade Code matches .....	52
Windows Store Application Version .....	52
Windows Store Package Name .....	52
Windows Store Publisher .....	52
Advanced Options .....	52
Insert Applications from Browsing .....	53

---

Insert Applications from Events (Event Import) .....	53
Insert Applications from Templates .....	55
Insert ActiveX Controls .....	55
Insert Batch Files .....	56
Insert COM Classes .....	57
Insert Control Panel Applets .....	58
Insert Executables .....	58
Insert Installer Packages .....	59
Insert Management Console Snap-ins .....	61
Insert PowerShell Scripts .....	61
Insert Registry Settings .....	62
Insert Remote PowerShell Commands .....	63
Insert Remote PowerShell Scripts .....	64
Insert Uninstaller (MSI or EXE) .....	65
Insert Windows Scripts .....	66
Insert Windows Services .....	67
Insert Windows Store Applications .....	67
Content Groups .....	68
Create Content Groups .....	68
Duplicate Content Groups .....	69
Target Content Definitions .....	69
Insert Content .....	70
Messages and Notifications in Privilege Management Policy .....	70
Types of Messages .....	71
Create Messages for a Workstyle .....	71
Message Name and Description .....	72
Message Design in Privilege Management .....	72
Challenge / Response Authorization .....	76
Message Text Options to Build Your Message .....	79
Custom Access Tokens in a Workstyle .....	82
Create Custom Tokens .....	82
Edit a Custom Token in a Workstyle .....	82
Privilege Management for Windows Licenses .....	86

---

Add a License Key in ePO Policy Orchestrator .....	86
Privilege Management for Windows Utilities .....	87
Application Search .....	87
Import BeyondTrust Policy .....	87
Export BeyondTrust Policy .....	87
Import Template Policies for Your Windows Endpoints .....	88
Discovery Template Policy Configuration .....	88
QuickStart for Windows Template Policy Configuration .....	88
QuickStart Policy Summary .....	89
Workstyles .....	89
Application Groups .....	90
Messages .....	91
Custom Token .....	91
Customize the QuickStart Policy .....	92
Server Roles Template Policy Configuration .....	92
Trusted App Protection (TAP) Template Policy Configuration .....	93
Trusted Application Protection Policies Summary .....	93
Trusted Application Protection Precedence .....	95
Modify the Trusted Application Protection Policies .....	95
Trusted Application Protection Reporting .....	96
Trusted Application Protection Block List .....	96
Manage Privilege Management Audit Scripts .....	97
Manage Privilege Management Rule Scripts .....	97
Import a New Rule Script .....	98
Edit a Rule Script .....	98
Delete a Rule Script .....	99
Import a Settings File .....	99
Edit a Settings File .....	99
Delete a Settings File .....	99
Delete a Rule Script .....	100
Import a Settings File .....	100
Edit a Settings File .....	100
Delete a Settings File .....	100

---

Apply Power Rules Scripts to Your Application Rules .....	100
Power Rules Additional Guidance .....	101
Compatibility .....	101
Third Party Integration Security .....	102
Supported Application Types .....	102
Validation .....	102
Script Restrictions .....	102
#Requires .....	103
Script Audit Failure Event .....	103
PowerShell Scripts Execution Policy .....	103
Encodings .....	103
Show Hidden Groups in Privilege Management .....	103
Configure Advanced Agent Settings .....	104
Advanced Policy Editor Settings .....	104
Regenerate Privilege Management UUIDs .....	105
Deploy Privilege Management for Windows Policy .....	106
Audits and Reports .....	107
Dashboards in Privilege Management for Windows .....	107
BeyondTrust Privilege Management: Blocked .....	107
BeyondTrust Privilege Management: Elevated .....	107
Privilege Management: Executed .....	108
BeyondTrust Privilege Management: Monitoring .....	108
Events in Privilege Management for Windows .....	109
Windows Process Events .....	109
Custom Script Auditing .....	111
Set up ePO Server Tasks for Privilege Management Reporting .....	111
Create the Reporting Event Staging Server Task .....	112
Create the Enterprise Reporting Purge Server Task .....	113
Privilege Management for Windows Reports .....	114
Filters .....	114
Summary .....	121
Discovery Reports in Privilege Management for Windows .....	123
"Discovery by Path" Report in Privilege Management for Windows .....	124

---

"Discovery by Publisher" Report in Privilege Management for Windows .....	124
"Discovery by Type" Report in Privilege Management for Windows .....	125
"Discovery Requiring Elevation" Report in Privilege Management for Windows .	125
"Discovery from External Sources" Report in Privilege Management for Windows	126
"Discovery All" Report in Privilege Management for Windows .....	126
Actions Reports in Privilege Management for Windows .....	127
Actions Elevated .....	127
Actions Blocked .....	127
Actions Passive .....	128
Actions Canceled .....	128
Actions Custom .....	129
Actions Drop Admin Rights .....	129
"Target Types All" Report in Privilege Management for Windows .....	130
"Trusted Application Protection" Report in Privilege Management for Windows ....	130
"User" Reports in Privilege Management for Windows .....	130
User Experience .....	131
Users Privileged Logons .....	131
Users Privileged Account Management .....	132
"Events" Reports in Privilege Management for Windows .....	133
"Events All" Report in Privilege Management for Windows .....	133
"Process Detail" Report in Privilege Management for Windows .....	134
Purge Reporting Events at Scheduled Interval .....	136
Configure Reputation Settings in ePO .....	137
Windows Policy Configuration Precedence .....	138
Privilege Management for Windows Application Templates .....	139
Creating Custom Application Templates .....	139
Configure Remote Computer Browser .....	141
Environment Variables Supported in Application Definitions .....	143
Supported Regular Expressions Syntax .....	144
Example PowerShell Configurations .....	146
Create New Configuration, Save to Local File .....	146
Open Local User Policy, Modify then Save .....	148
Open Local Configuration and Save to Domain GPO .....	148



---

Privilege Management Built-in Groups .....	149
Manage the Privilege Management Databases .....	149
Use Privilege Management for Windows Events to Build Queries .....	149
Database Sizing and Resource Consumption .....	152
Data Retention .....	152
Database Sizes .....	153
Example Use Case Volumes .....	153
Key considerations .....	154
McAfee ePO Privilege Management for Windows Database Events .....	154
Create the ePO Event Purge Server Task .....	156
McAfee ePO Orchestrator Server Scripts .....	157
Referenced Libraries .....	157
Challenge Response Scripting .....	157
ePO Create Policy .....	158
ePO Import Policy .....	158
ePO Export Policy .....	159
Exported Views in Privilege Management for Windows .....	159
Custom Data Types .....	160
Application Types .....	160
Chassis Types .....	160
OS Version .....	161
OS Product Type .....	161
Message Types .....	161
Certificate Modes .....	162
Policy Audit Modes .....	162
Device Types (Drive Type) .....	162
ExportDefendpointStarts .....	163
ExportLogons .....	163
ExportPrivilegedAccountProtection .....	164
ExportProcesses .....	166
Troubleshoot Privilege Management for Windows .....	174
Check Privilege Management for Windows is installed and functioning .....	174
Check Settings are Deployed .....	174

---

Check that Privilege Management is Licensed .....	174
Check Workstyle Precedence .....	174
Certificate Error in McAfee Endpoint Security (ENS) .....	175
Add the Certificate for Privilege Management: .....	175

# Privilege Management for Windows ePO Extension Administration

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 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

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 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 Privilege Management Workstyles to monitor privileged application behavior. The Privilege Management for Windows audit logs highlight all of the applications that require admin rights to run.
- Set up 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 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 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.



For more information, please see the following:

- ["Privilege Monitoring" on page 28](#)
- ["Create On-Demand Application Rules" on page 35](#)
- ["Privilege Management Workstyle Properties" on page 27](#)
- ["Application Groups" on page 46](#)

## About McAfee ePolicy Orchestrator

McAfee ePO software, the foundation of the McAfee Security Management solution, unifies management of endpoints, networks, data, and compliance solutions. More than 45,000 organizations use McAfee 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, McAfee ePO software is the most advanced security management software available.

Only McAfee 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. McAfee ePO software connects management of both McAfee 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, please see [McAfee ePolicy Orchestrator](https://www.mcafee.com/enterprise/en-us/products/epolicy-orchestrator.html) at <https://www.mcafee.com/enterprise/en-us/products/epolicy-orchestrator.html>.

## Privilege Management for Windows and McAfee

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

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

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

If you do not want to use McAfee ePO for deployment of the client package, the 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.

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



**Note:** *If you do not want to use McAfee 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.*

## Install, Uninstall, and Upgrade 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 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 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 McAfee agent to receive policies, and send audit events.

### Install the Privilege Management for Windows Clients

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

**i** For more information on installing Privilege Management for Windows using ePO, please see the [Privilege Management for Windows ePO Extension Installation Guide](https://www.beyondtrust.com/docs/privilege-management/windows/index.htm), at <https://www.beyondtrust.com/docs/privilege-management/windows/index.htm>.

### Uninstall the Privilege Management for Windows Clients

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

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

**i** For more information on uninstalling Privilege Management for Windows using ePO, please see the [Privilege Management for Windows ePO Extension Installation Guide](https://www.beyondtrust.com/docs/privilege-management/windows/index.htm), at <https://www.beyondtrust.com/docs/privilege-management/windows/index.htm>.

### Upgrade Privilege Management for Windows

#### Recommended Steps

- Step 1: Upgrade Application Groups to Match Publisher Name BeyondTrust Corporation
- Step 2: Upgrade the Privilege Management ePO Extension
- Step 3: Upgrade Privilege Management Reporting (if in use)
- Step 4: Upgrade Privilege Management for Windows Clients
- Step 5: Delete Old Application Definitions (Upgrade from 5.4)

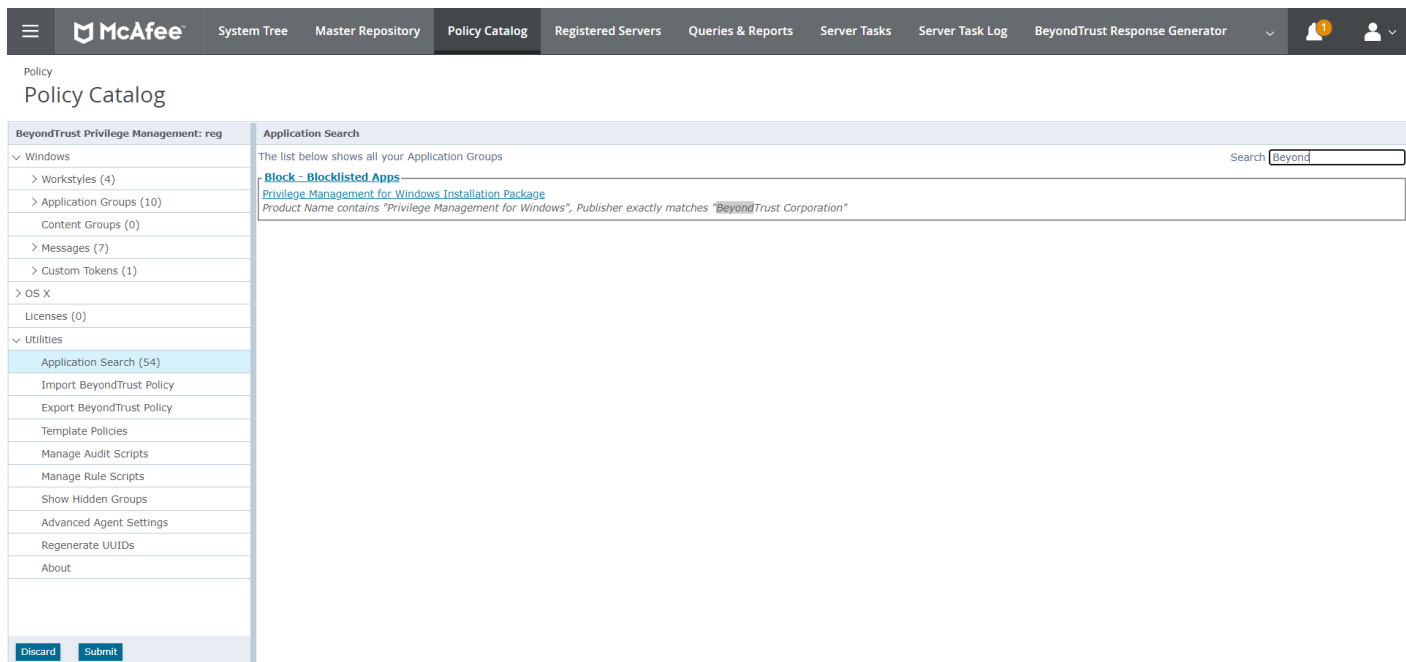
**! IMPORTANT!**

As of release 5.5, all releases of this product are signed with BeyondTrust Corporation, rather than Avecto, as the software publisher name. If prior to 5.5 you used the QuickStart Policy Template as a starting point, it is likely that your configuration includes Application Groups which target our own applications based on a publisher match to Avecto. An upgrade to 5.5 or beyond requires you to update your configuration so that it continues to match the versions of the applications and tools that you use. We recommend you add a copy of any existing application definitions that target Avecto and update those copies to target BeyondTrust Corporation instead; the presence of both sets of application definitions ensures they continue to match both new and existing versions during the implementation of 5.5. It is critical that you roll out your configuration changes before you update your Privilege Management for Windows software to version 5.5 or later.

## Step 1: Upgrade Application Groups to Match Publisher Name BeyondTrust Corporation

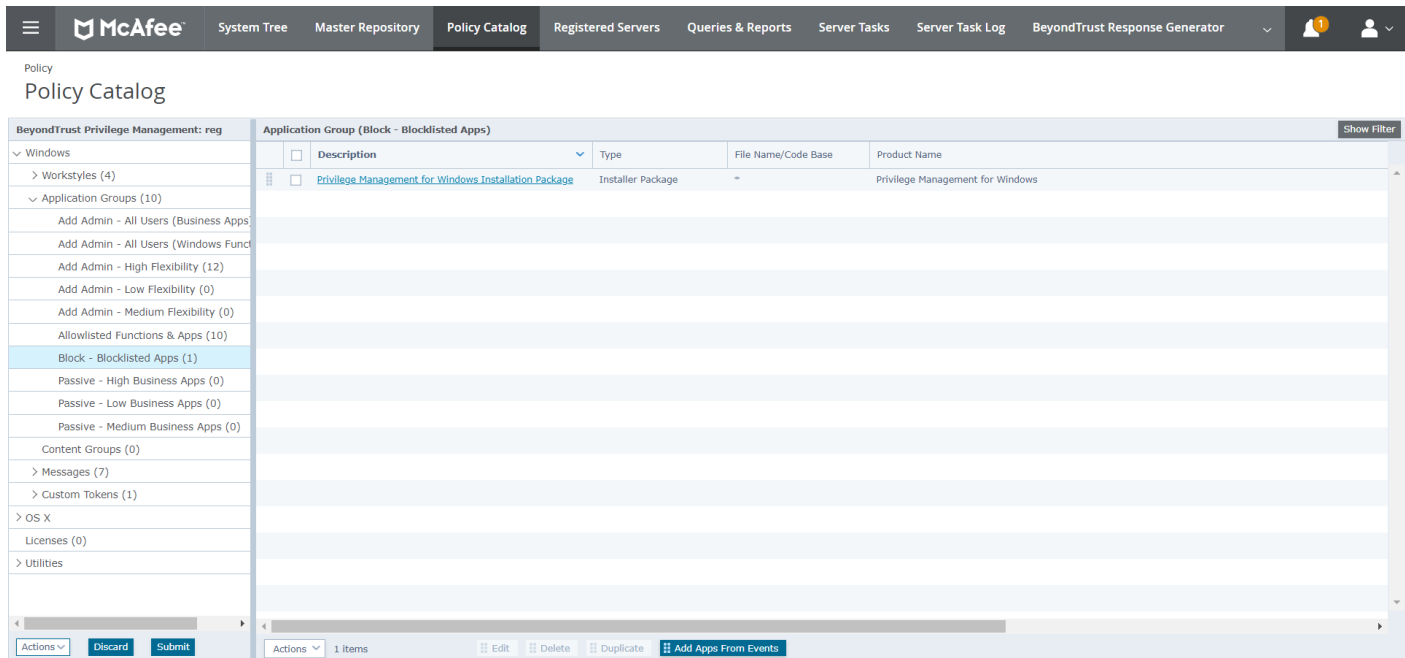
This section applies to upgrades to Version 5.5.

1. Locate all **Avecto** matches:
  - In the policy tree, navigate to **Utilities > Application Search**.
  - Type **Avecto** into the **Search applications** box to filter.



The screenshot shows the McAfee Policy Catalog interface. The top navigation bar includes 'McAfee', 'System Tree', 'Master Repository', 'Policy Catalog', 'Registered Servers', 'Queries & Reports', 'Server Tasks', 'Server Task Log', and 'BeyondTrust Response Generator'. The 'Policy Catalog' section is active, showing a tree view on the left with 'Utilities > Application Search (54)' selected. The main content area displays search results for 'BeyondTrust Corporation' under the heading 'Block - Blocklisted Apps'. The results list 'Privilege Management for Windows Installation Package' with a note: 'Product Name contains "Privilege Management for Windows", Publisher exactly matches "BeyondTrust Corporation"'. A search box at the top right contains the text 'Beyond'.

2. Create a copy of all definitions in each Application Group found that contain a publisher match on **Avecto**:
  - Make a note of the name of the application definition which contains a publisher match on Avecto, and click on its Application Group name in **Application Search**. This takes you to the Application Group.
  - Select the application definition and click **Duplicate**.



The screenshot shows the McAfee Policy Catalog interface. The left sidebar lists various policy categories, with 'Block - Blocklisted Apps (1)' selected. The main pane displays a table of application groups under the heading 'Application Group (Block - Blocklisted Apps)'. The table has columns for Description, Type, File Name/Code Base, and Product Name. One entry is visible: 'Privilege Management for Windows Installation Package' with Type 'Installer Package' and Product Name 'Privilege Management for Windows'. Below the table are action buttons: 'Actions', 'Discard', 'Submit', 'Edit', 'Delete', 'Duplicate', and 'Add Apps From Events'.



**Tip:** Rename one of the copies to **OLD**, so it's easy to tell which to delete after the new application definitions take effect. **OLD** can be deleted once the 5.5 upgrade is complete.

3. Update the new application definitions to match publisher **BeyondTrust Corporation**.
4. Test the updated configuration against the new 5.5 applications.

At this point, you can continue with upgrading the remaining components.

The product code for Privilege Management for Windows version 5 was updated from version 4. This means that the Privilege Management ePO Extension must be upgraded before the Privilege Management for Windows version 5 clients are installed.



**Note:** ePO will not recognize Privilege Management for Windows if you upgrade the Privilege Management for Windows clients before the Privilege Management ePO extension. In addition, ePO Threat events will be rejected if this order is not followed, although they can be recovered once the upgrade to the Privilege Management ePO Extension has been completed.

Version 5 of the Privilege Management ePO Extension is compatible with older Privilege Management for Windows clients.

The recommended order to upgrade BeyondTrust Privilege Management for Windows software is:

- Upgrade the Privilege Management ePO Extension
- Upgrade Privilege Management Reporting (if in use)
- Upgrade Privilege Management Clients



**Note:** If you have a requirement to upgrade BeyondTrust software in a different order from that listed above, please contact your BeyondTrust representative.



## Step 2: Upgrade the Privilege Management ePO Extension

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

To upgrade the Privilege Management ePO Extension, you need to use ePO to install the latest extension from **Software > Extensions**. When you upload the new Privilege Management ePO Extension, ePO prompts you that this newer version of the ePO Extension will replace the previous extension. Click **OK** to upgrade the Privilege Management ePO Extension. You do not need to restart ePO for the upgrade to take effect. Existing registered servers, client tasks, and server tasks are not affected.

## Step 3: 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 **McAfee 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 Server** and navigate to **Reporting database > Service Broker > Queues**.
3. Right-click on the **PGScheduledJobQueue** and click **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 for Windows database installer to upgrade the database. Ensure you point the installer to the existing database server and Privilege Management for Windows 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 on **PGScheduledJobQueue** and click **Enable Queue**.
10. Start the **McAfee 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 installed Reporting from version 5.4 or later, the default name for the database is **BeyondTrustReporting**. If you installed a previous version of Reporting, the default name is **AvectoReporting** (v5.1 - 5.3), or **AvectoPrivilegeGuard** for older versions. Alternatively, you may have chosen a different database name.



**Note:** If you see an error message that states "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 spread over multiple machines.



If you cannot log in locally to the database or it is in the cloud, please see "[Manual Database Upgrade](#)" on page 18 for more information.

#### Step 4: Upgrade Privilege Management for Windows Clients

You can upload a newer version of the Privilege Management for Windows client to ePO and deploy it 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 Privilege Management ePO Extension maintains backwards compatibility with the Privilege Management for Windows client. You can use a later version of the Privilege Management ePO Extension with an earlier version of the Privilege Management for Windows client. However, not all features in the Privilege Management ePO Extension are supported with earlier versions of the client.



For more information, please see the [Privilege Management for Windows Administration Guide](https://www.beyondtrust.com/docs/privilege-management/windows/index.htm), at <https://www.beyondtrust.com/docs/privilege-management/windows/index.htm>.

#### Step 5: Delete Old Application Definitions (Upgrade from 5.4)

Once all machines are running version 5.5, it is safe to delete the OLD application definitions created in Step 1 and to deploy that configuration.

#### Manual Database Upgrade

Use these instructions to upgrade the Privilege Management Reporting database where you cannot use the installer or need to do a manual installation, for example, PMC in Azure. SQL scripts are provided to manage these upgrades.

To upgrade a Privilege Management Reporting database using SQL scripts:

1. The SQL scripts are provided as part of the Reporting installers. Alternatively, you can contact BeyondTrust Technical Support for them.



**Note:** There is a README file provided in this directory to assist you.

2. Run the following SQL query to find the current version of the database. This returns the version of the database.

```
select * from DatabaseVersion
```



**Note:** This SQL query works for Privilege Management Reporting databases 4.5 and later.

3. Execute the upgrade script where the name is the next version number and carry on applying these until the desired version is reached.



**Example:** If your current database version is **4.3.16** and you want to upgrade to version **5.0.0**, execute the following scripts in order:

1. **Script\_4.5.0\_Updates.sql**
2. **Script\_5.0.0\_Updates.sql**

Please check the SQL log for any errors and contact BeyondTrust Technical Support if necessary.

## Manual Deployment of Privilege Management for Windows

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

### Prerequisites

Privilege Management for Windows must be installed in ePO Mode, either by selecting the McAfee ePolicy Orchestrator Integration option when installing 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 McAfee 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 Privilege Management for Windows using McAfee ePO, then ePO Mode is automatically enabled.

## Disable ePO Mode

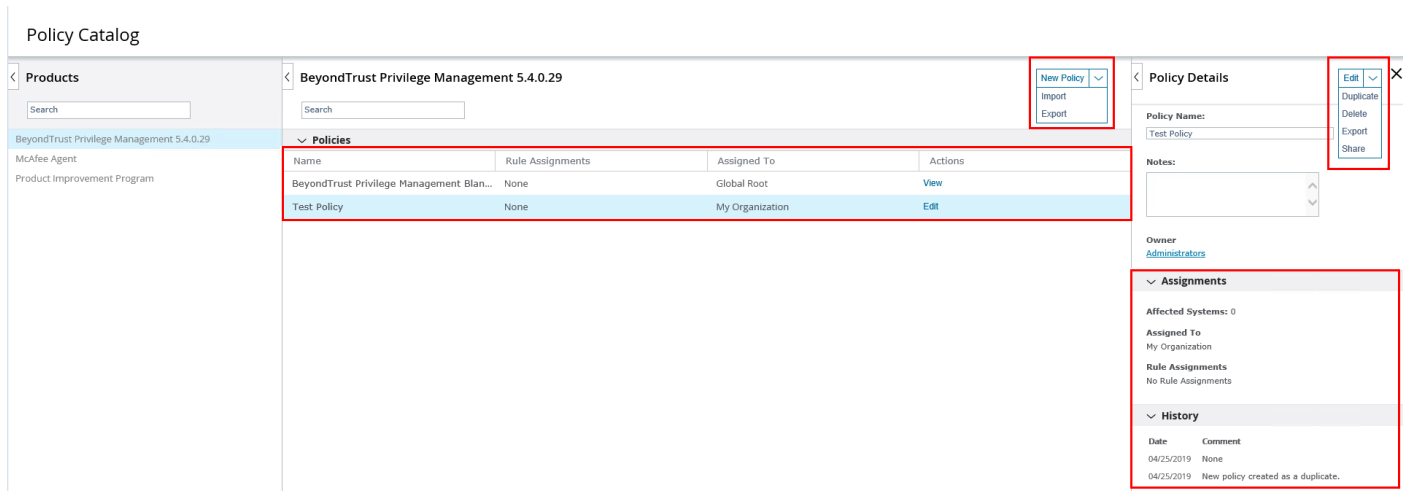
Once installed in ePO Mode, Privilege Management for Windows sends events to the McAfee Agent, and also raises events to the Application EventLog. If you want to disable ePO mode at any time, set the following registry key:

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

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

## Launch the ePO Policy Catalog to View Policies

The **Policy Catalog** page in ePO allows you to see all your Privilege Management for Windows policies and attributes and perform various actions on them. This screenshot is from ePO 5.10.



The screenshot shows the 'Policy Catalog' interface. On the left, the 'Products' menu is open, showing 'BeyondTrust Privilege Management 5.4.0.29' selected. The main area displays a table of policies:

Name	Rule Assignments	Assigned To	Actions
BeyondTrust Privilege Management Blan...	None	Global Root	View
Test Policy	None	My Organization	Edit

On the right, the 'Policy Details' panel is open, showing the policy name 'Test Policy', notes, owner 'Administrators', and assignments. A 'History' section shows a log of actions, including 'New policy created as a duplicate.' on 04/25/2019.

To view existing Privilege Management for Windows policies in ePO Server 5.9, select **BeyondTrust Privilege Management <version number>** from the **Product** dropdown. The selection of this dropdown changes the type of policy you can create in this screen and which policies are shown. In ePO Server 5.10, ensure that the BeyondTrust Privilege Management product is selected in the **Products** menu on the left, as shown in the screenshot above.

Click **New Policy** to create a new Privilege Management for Windows policy.

To edit a policy, you need to either click the **Edit** link in the **Actions** column for the policy you want to edit, or you can click the policy name to highlight it, and then click the **Edit** button in the **Policy Details** tab.



**Note:** In 5.9 and earlier versions, click the **Name** of a policy to view or edit it.

McAfee ePO provides standard import and export functionality for policies here; however, policies exported using these functions are exported using the McAfee format. They are not compatible with other BeyondTrust Policy Editors. We recommend you use the **Import** and **Export** functionality in the **Utilities** section.



For more information, please see the following:

- ["Create a Privilege Management Policy" on page 25](#)
- ["Edit Privilege Management Policies" on page 25](#)
- ["Privilege Management for Windows Utilities" on page 87](#)
- On configuring policies for Windows, ["Privilege Management Policies and Templates" on page 25](#)

## Access the Policy Summary Screen from the Policy Catalog

To access the Policy Summary Screen, click a Privilege Management for Windows policy from the **Policy Catalog** home page in ePO Server 5.9 or select **Edit** in ePO Server 5.10.

Privilege Management for Windows policies are applied to one or more endpoints. The **Policy Summary** screen summarizes the number of Workstyles, Application Groups, Content Groups, Messages, and Custom Tokens in the policy. If this is a blank policy, all summaries display **0**. Clicking on any of the numbers allows you to jump to that section to view and edit information within the policy.

The **Utilities** button allows you to perform various tasks for all operating systems, such as import BeyondTrust template policies.

The **Licenses** button allows you to view and edit the BeyondTrust Privilege Management license keys for all operating systems.

Policy  
Policy Catalog

BeyondTrust Privilege Management 5.4.0.29: Avesto Defendpoint > Policies > Test Policy

Category	Windows	OS X
Workstyles	0	2
Application Groups	0	12
Messages	0	8
Content Groups	0	
Custom Tokens	0	

Utilities Licenses

## Policy Approval

ePO Server 5.10 introduced new functionality called Policy and Task approval.

Privilege Management ePO Extension 5.3 SR1 and later support this functionality for Privilege Management for Windows policies.

To enable the policy approval workflow, navigate to **Server Settings > Approvals** from the ePO server menu. Click **Edit** and then check the **Users need approval for policy changes** box and click **Save**. You can then use the **Policy Management** permission to either grant users permission to approve their own policies and others, or to ensure all policies must be approved by an ePO server administrator or a user with the appropriate permissions.

If you don't check this box, the policy approval Workflow is not enabled. This is the default behavior for ePO server 5.9 and earlier.

If you are using ePO server 5.9 or earlier, with Privilege Management ePO Extension 5.3 SR1 or later, you need to click **Submit** in the policy editing screens when you've made a change. Clicking **Submit** does not save the policy; instead, it redirects you to the **Policy Summary** page, where you can save your Privilege Management for Windows policy.

If you are using ePO server 5.10 or later, with Privilege Management ePO Extension 5.3 SR1 or newer, you need to click **Submit** in the policy editing screens when you've made a change. Clicking **Submit** does not save the policy, instead; it redirects you to the **Policy Summary** page where you can save or submit your Privilege Management for Windows policy for review depending on the ePO server **Approvals** setting and the permissions assigned your user.

## Policy Approval Potential Scenarios

**Server Settings > Approvals for Policy Changes** not enabled:

All users can save their policies.

**Server Settings > Approvals for Policy Changes** enabled and **Permission Sets > Policy Management** set to **Approver Permission** for your user or you're an ePO Administrator:

- You can save your policy
- You can approve other users' policies

**Server Settings > Approvals for Policy Changes** enabled and **Permission Sets > Policy Management** set to **No Permission** for your user:

- You can submit your policy for approval
- You cannot approve other users' policies

If you are using ePO server 5.10 or later, with Privilege Management ePO Extension 5.3 GA or earlier, the McAfee policy approval process is not supported for Privilege Management for Windows policies. Click **Save** on the **Policy Summary** screen to save it.



For more information, please see [Policy and Task approval feature with ePolicy Orchestrator 5.10.0](https://kc.mcafee.com/corporate/index?page=content&id=KB90769) at <https://kc.mcafee.com/corporate/index?page=content&id=KB90769>.

## Apply Policy to Disconnected Users

Disconnected users are fully supported by Privilege Management for Windows. When receiving policies from McAfee ePO, Privilege Management for Windows automatically caches all the information required to work offline, so the settings are still applied if the client is not connected to the corporate network. Any changes made to the policy do not propagate to the disconnected computer until the McAfee Agent reestablishes a connection to the ePO server.

## Autosave, Autosave Recovery, and Policy Locks

The Privilege Management ePO Extension has autosave, autosave recovery, and concurrent edit functionality to reduce the risk or impact of data loss, as well as to prevent multiple users from overwriting individual policies.



**Note:** In ePO Server 5.10, if the **Server Settings > Approvals** setting has been configured, autosave is disabled for users who do not have the **Policy Management** permission set to **Approver Permission - Users with this permission can make policy changes independently**. This includes the ability to approve or reject policy change requests..

### Autosave

If a policy has pending edits, then these are retained initially in memory and then on session timeout to permanent storage.

This can occur if the session expires, if you select **Log Off**, or if the browser is closed while Privilege Management for Windows policies are being edited.

If the server can determine that the session has ended, for example, via log out, then the permanent storage autosave is always used.

The in-memory version is only used when the browser is closed and the session has not yet timed out.

### Autosave Recovery

When the policy is edited next, you receive a prompt that there is an existing edit available. You are given the option to discard or recover the changes.



**Note:** The autosave is not removed until the policy has been saved.

When saved the autosave policy is automatically removed. This is the case for both recovery and discard. The choice simply affects which data is loaded into the policy.

The autosaved policy has the same name as the current policy but with **(autosave)** appended to the name. It is possible to duplicate this policy if the user wants to retain the changes in a different policy.

The in-memory storage recovery is covered as part of the locking workflows below.

## Policy Locks

When a policy is being edited it is locked to prevent other users from making changes which could override your edits. The policy is locked after the user clicks a link or button from the policy summary screen to enter the policy. If another user attempts to edit the same policy, they are shown the name and ID of the user making the edit.

They are then presented with three options:

- Break lock and take current changes
- Break lock and use last save
- Open in read only mode

They can also use the standard ePO options of **Duplicate/Save/Cancel** (lower right). The **Save** and **Cancel** options both act as cancel. The **Duplicate** option uses the last saved version.



**Note:** *Anyone with write access to the policy can break the lock.*

If the lock on a policy that you're editing is broken, please follow the on-screen instructions, as they will vary depending on the policy management **Approvals** workflow and user permissions.

When the browser is closed during an edit, the returning login is treated as a new user. Therefore it is possible to be prompted with an option to break the lock for yourself. As ePO permits multiple logins from the same user, this is possible in normal usage in addition to the browser close scenario, for example, using two different browsers or through a private browsing window.



## Privilege Management Policies and Templates

Template Policies can be imported into your Privilege Management for Windows settings. You can choose to merge them into your existing policy; if not merged, the template overwrites the existing policy.

### To Import a Privilege Management XML Configuration

1. Select the **Utilities** node and click **Import Privilege Management Policy**.
2. Browse to the location of the XML file to import.
3. If you want to merge the imported settings with the settings already contained within the policy, check **Merge imported settings**. If you want to overwrite the existing policy with the imported policy, uncheck **Merge imported settings**.
4. Click **Load Configuration** to complete the import.

### Create a Privilege Management Policy

1. Click **New Policy** and enter the following information:

Field	Meaning
<b>Category</b>	Select the category you want the policy to belong to. By default, this will be <b>Policies</b> .
<b>Create a policy based on this existing policy</b>	You need to base the new policy on an existing policy. <b>BeyondTrust Privilege Management Blank Policy</b> is supplied for this purpose. Alternatively, you choose a different policy to base the new policy on.
<b>Policy Name</b>	Enter a name for the new policy. This should be as descriptive as possible. You can edit it later.
<b>Notes</b>	Enter any notes for the policy. You can edit this later.

2. Click **OK** to save your policy or **Cancel** to discard it. Your new policy is shown in the **Policy Catalog** page. The next step is to edit the policy.



For the steps to edit the policy, please see *"Edit Privilege Management Policies"* on page 25.

### Edit Privilege Management Policies

On the **ePO Policy Catalog** page, ensure **BeyondTrust Privilege Management <version number>** is selected from the list of products in the **Products** tab. Click the **Edit** link for the policy you want to edit from the list.



**Note:** For ePO 5.9 and earlier, in **Policy Catalog**, ensure **BeyondTrust Privilege Management <version number>** is selected from the **Product** dropdown and click the policy you want to edit from the list.

This takes you to the **Policy Summary** screen. From here you can edit any of the following components that make up a policy. You can also access the Licenses and Utilities functionality.

The **Utilities** button allows you to perform various tasks for all operating systems, such as importing BeyondTrust template policies.

The **Licenses** button allows you to view and edit the Privilege Management license keys for all operating systems.

Policy  
Policy Catalog

BeyondTrust Privilege Management 5.4.0.29/Avecto Defendpoint > Policies > Test Policy		
Category	Windows	OS X
Workstyles	<a href="#">0</a>	<a href="#">2</a>
Application Groups	<a href="#">0</a>	<a href="#">12</a>
Messages	<a href="#">0</a>	<a href="#">8</a>
Content Groups	<a href="#">0</a>	
Custom Tokens	<a href="#">0</a>	

[Utilities](#) [Licenses](#)

**i** For more information, please see the following:

- ["Access the Policy Summary Screen from the Policy Catalog" on page 21](#)
- ["Privilege Management for Windows Licenses" on page 86](#)
- ["Privilege Management for Windows Utilities" on page 87](#)

## Windows Policies

You can edit the following components of a policy:

- Workstyles
- Application Groups
- Messages
- Content Groups
- Custom Tokens

**i** For more information, please see the following:

- ["Privilege Management for Windows Workstyles" on page 27](#)
- ["Application Groups" on page 46](#)
- ["Messages and Notifications in Privilege Management Policy" on page 70](#)
- ["Content Groups" on page 68](#)
- ["Custom Access Tokens in a Workstyle" on page 82](#)

## Privilege Management for Windows Policies

A Privilege Management for Windows policy is built up with the following optional components:

- **Workstyles:** A Workstyle is part of a policy. It is used to assign Application Rules for users. You can create Workstyles using the WorkStyle Wizard, or you may import them.
- **Application Groups:** Application Groups are used by Workstyles to group applications together to apply certain Privilege Management for Windows behavior.
- **Content Groups:** Content groups are used by Workstyles to group content together to apply certain Privilege Management for Windows behavior.

- **Messages:** Messages are used by Workstyles to provide information to the user when Privilege Management for Windows has applied certain behavior that you've defined and need to notify the user.
- **Custom Tokens:** Custom Tokens are used by Workstyles to assign custom privileges to content or Application Groups.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

BeyondTrust has produced a pre-built QuickStart policy that is configured with Privilege Management for Windows and Application Control.

**i** For more information, please see the following:

- ["Privilege Management for Windows Workstyles" on page 27](#)
- ["Application Groups" on page 46](#)
- ["Content Groups" on page 68](#)
- ["Messages and Notifications in Privilege Management Policy" on page 70](#)
- ["Custom Access Tokens in a Workstyle" on page 82](#)

## Privilege Management for Windows Workstyles

Privilege Management for Windows Workstyles are used to assign Application Rules for a specific user, or group of users. The Workstyle Wizard can generate Application Rules depending on the type of Workstyle you choose.

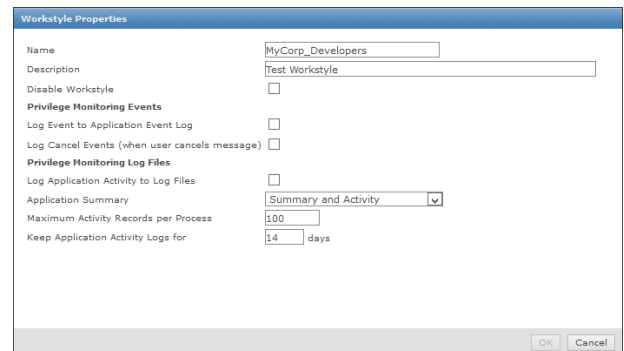
**i** For more information, please see the following:

- ["Create On-Demand Application Rules" on page 35](#)
- ["Create a Privilege Management Workstyle" on page 28](#)

## Privilege Management Workstyle Properties

To edit the advanced properties for a Workstyle:

1. Expand the **Workstyles** node and select the relevant Workstyle.
2. Select **Actions > Workstyle Properties**.



You can edit the name and description of the Workstyle here as well as disable it, if required.

## Privilege Monitoring

Privilege Management for Windows can monitor the behavior of specific privileged applications and processes in Windows, a feature called privilege monitoring. Privilege monitoring is enabled as an auditing option in the properties of an Application Rule or an On-Demand Application Rule. When enabled, Privilege Management for Windows records all privileged operations performed 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.

The application must be running under a privileged account, such as an administrator or power user. Alternatively, an application could be running with elevated privileges because you have added it to the **Application Rules** or **On-Demand Application Rules** section of the Workstyle and assigned it to run with admin rights.

Privilege monitoring logs are recorded on each endpoint, and the logs can be accessed using the Privilege Management Reporting MMC snap-in. The configuration of privilege monitoring logs is applied to each Workstyle.

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

## Privilege Monitoring Events

**Log Event to Application Event Log:** This option will log an event to the Application EventLog, the first time an application performs a privileged operation.

**Log Cancel Events (when user cancels message):** This option raises an event when a user cancels an **End User Message**, either by clicking the **Cancel** button, **Email** button, or clicking a **Hyperlink**. The action performed by the user is available as a **Policy Parameter** [PG\_ACTION], which can be used by the script to perform different audit actions based on the user interaction.

## Privilege Monitoring Log Files

The following **Privilege Monitoring** options are available:

- **Log Application Activity to Log Files:** The **Application Summary** dropdown menu controls the level of **Application Activity** logging in the log files. The following options are available:
  - **Application Summary:** This option only logs information about the application.
  - **Application Summary and Activity:** This option logs information about the application and unique privileged activity (Default option).
  - **Application Summary and Detailed Activity:** This options logs information about the application and all privileged activity.
- **Maximum Activity Records Per Process:** This option determines the maximum number of records to be recorded per process (default 100).
- **Keep Application Activity Logs for:** This option determines how long activity logs are kept before they are purged (default 14 days).

## Create a Privilege Management Workstyle

1. Navigate to the **Policy Catalog** and select **BeyondTrust Privilege Management** from the **Products** list on the left side (for 5.9 and older, use the dropdown menu).
2. Click the policy from the list that you want to add a Workstyle to.



**Note:** If you want to create a new policy, see "[Create a Privilege Management Policy](#)" on page 25 for more information.

- Click the number for Windows Workstyles. If this is a blank policy this is **0**.

Policy  
Policy Catalog

BeyondTrust Privilege Management 5.4.0.29/Avecto Defendpoint > Policies > Hiro Protagonist test policy

This is a new policy

Category	Windows	OS X
Workstyles	5	2
Application Groups	4	12
Messages	2	8
Content Groups	1	
Custom Tokens	1	

Utilities Licenses

- Click **Actions > Create Workstyle using Wizard** to start creating your Privilege Management for Windows Workstyle. This launches the Workstyle Wizard and takes you through the following screens.
- Introduction.** This page displays if you have not yet configured a Privilege Management license in the policy, prompting you to enter a valid license code for the policy.
- Choose a Workstyle.** You can choose from **Controlling** or **Blank** for your Workstyle. A controlling Workstyle allows you to apply rules for access to privileges and applications. A blank Workstyle allows you to create an empty Workstyle without any predefined elements. If you select a blank Workstyle, the next screen is **Finish**, as there is nothing to configure.
- Filtering** (Controlling Workstyle only). This determines who will receive this Workstyle. You can choose from standard users only or everyone. If you apply it to everyone, it will apply to administrators. You can modify the filters and apply more detailed filtering once the Workstyle has been created.
- Capabilities** (Controlling Workstyle only). Allows you to choose **Privilege Management**, **Application Control**, or both. If you don't select either capability, the next screen is **Finish**. This Workstyle would only contain filtering information.
- Privilege Management** (Controlling Workstyle with the Privilege Management capability). Allows you to choose:
  - If you want to display a notification to the user when applications are elevated by Privilege Management for Windows
  - How you want to manage Windows User Account Control (UAC) prompts
  - If you want to allow the on-demand elevation of applications



**Note:** If you select **Present users with a challenge code** from the dropdown, you are prompted to configure the challenge and response functionality at the end of creating your Workstyle, if your policy doesn't already have one.

- Application Control** (Controlling Workstyle with the Application Control capability). Allows you to choose:
  - How you want to apply application control. You can choose from an allow or block approach. We recommend you use an allow approach.
  - If you select **As an allow**: How you want to handle non-allowed applications
  - If you select **As a block**: How you want to handle blocked applications



**Note:** If you select **Present users with a challenge code** from the dropdown, you are prompted to configure the challenge and response functionality at the end of creating your Workstyle, if your policy doesn't already have one.

- Finish.** Allows you to enter a **Name** and **Description** for your new policy. If the Workstyle has been configured to use a Challenge / Response message and the policy doesn't have an existing key, you will be asked to set a key.

You can check the box on this screen to activate this Workstyle immediately or you can uncheck the box to continue to configure the Workstyle before you apply it to your endpoints.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

Depending on the type of Workstyle you created and any capabilities that have been included, Privilege Management for Windows auto-generates certain Application Groups (containing rules), Content Groups, messages, and Custom Tokens. Filters are applied and subsequently configured as part of the Workstyle.



For more information, please see the following:

- ["Challenge / Response Authorization" on page 76](#)
- ["Application Groups" on page 46](#)
- ["Content Groups" on page 68](#)
- ["Messages and Notifications in Privilege Management Policy" on page 70](#)
- ["Custom Access Tokens in a Workstyle" on page 82](#)

## Disable or Enable Privilege Management Workstyles

You can enable or disable Workstyles to prevent them from being processed by the Privilege Management for Windows client.

1. Navigate to the policy and select the **Workstyles** node.
2. The **Enabled** column shows you which Workstyles are currently being processed by the Privilege Management for Windows client. Click **Disable** to stop Privilege Management for Windows from processing that Workstyle, or click **Enable** to allow the Privilege Management for Windows client to process that Workstyle.

Policy  
Policy Catalog

BeyondTrust Privilege Management: Hiro P...	Workstyles	
	Show selected rows	
	Name	Enabled
<ul style="list-style-type: none"> <li>Windows           <ul style="list-style-type: none"> <li>Workstyles (5)               <ul style="list-style-type: none"> <li>Metaverse_Developers (Disabled)</li> <li>General Rules</li> <li>High Flexibility</li> <li>Medium Flexibility</li> <li>Low Flexibility</li> </ul> </li> <li>Application Groups (0)</li> </ul> </li> </ul>	<input type="checkbox"/> Metaverse_Developers (Disabled) <input type="checkbox"/> General Rules <input type="checkbox"/> High Flexibility <input type="checkbox"/> Medium Flexibility <input type="checkbox"/> Low Flexibility	No (Enable) Yes (Disable) Yes (Disable) Yes (Disable) Yes (Disable)

## Change Workstyle Precedence in Privilege Management

If you have multiple Workstyles, they are evaluated in the order in which they are listed. Workstyles that are higher in the list have a higher precedence. Once an application matches a Workstyle, no further Workstyles are processed for that application, so it is important that you order your Workstyles correctly, because an application could match more than one Workstyle.

1. Select the **Workstyles** node in the left pane.
2. In the right pane, check the box adjacent to the Workstyle you want to move.
3. Select **Actions** and choose from the available options: **Up**, **Down**, **Top**, or **Bottom** as required.



**Note:** You can drag the buttons from the **Actions** menu to the right and drop them onto the toolbar to access them faster next time.

## Privilege Management for Windows Workstyle Parameters

Privilege Management for Windows settings include a number of features that allow customization of text and strings that are used for end user messaging and auditing. If you want to include properties that relate to the settings applied, the application being used, the

user or the installation of Privilege Management for Windows, then parameters may be used that expand when the text is used.

Parameters are identified as any string surrounded by [square parentheses], and if detected, the agent 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_ACTION]	The action which the user performed from an end user message
[PG_AGENT_VERSION]	The version of the Privilege Management Client
[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_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_CONTENT_DEF]	The definition name of the matching content
[PG_CONTENT_FILE_DRIVE_TYPE]	The drive type of a matching content
[PG_CONTENT_FILE_HASH]	The SHA-1 hash of a matching content
[PG_CONTENT_FILE_IE_ZONE]	The Internet Zone of a matching content
[PG_CONTENT_FILE_NAME]	The file name of a matching content
[PG_CONTENT_FILE_OWNER]	The owner of a matching content
[PG_CONTENT_FILE_PATH]	The full path of a matching content
[PG_CONTENT_GROUP]	The group name of a matching content definition
[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 / 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_MESSAGE_NAME]	The name of the custom message that was applied
[PG_MSG_CHALLENGE]	The 8 digit challenge code presented to the user
[PG_MSG_RESPONSE]	The 8 digit response code entered by the user
[PG_POLICY_NAME]	The name of the policy
[PG_PROG_CLASSID]	The ClassID of the ActiveX control
[PG_PROG_CMD_LINE]	The command line of the application being run

Parameter	Description
[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_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
[PG_PROG_TYPE]	The type of application being run
[PG_PROG_URL]	The URL of the ActiveX control
[PG_SERVICE_ACTION]	The action performed on the matching service
[PG_SERVICE_DISPLAY_NAME]	The display name of the Windows service
[PG_SERVICE_NAME]	The name of the Windows service
[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_URL_ADDRESS]	The full address of the matching URL
[PG_URL_DEF]	The definition name of the matching URL
[PG_URL_GROUP]	The URL group name of the matching URL
[PG_URL_HOST]	The hostname of the matching URL
[PG_URL_IE_ZONE]	The Internet Zone of the matching URL
[PG_URL_PROTOCOL]	The protocol of the matching URL
[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_USER_REASON]	The reason entered by the user
[PG_USER_SID]	The SID of the user
[PG_WORKSTYLE_NAME]	The name of the Workstyle

## Privilege Management Workstyle Summary

The Workstyle Summary provides a high level view, with links to pages where you can configure elements of a Workstyle.

- General
  - Allows you to change the name and description of the Workstyle and disable or enable it.



- Totals
  - Application Rules
  - On-Demand Application Rules
  - Trusted Application DLL Protection
  - Content Rules
- General Rules
  - Collect User Information
  - Collect Host Information
  - Prohibit Privileged Account Management
  - Enable Windows Remote Management Connections
- Filters
  - Account Filters
  - Computer Filters
  - Time Range Filters
  - Expiry Filter
  - WMI (Windows Management information) Filters



**Note:** The options will only appear on the right of the screen if there are some configured.



For more information, please see the following:

- ["Create On-Demand Application Rules" on page 35](#)
- ["Trusted Application DLL Protection" on page 38](#)
- ["Privilege Management Content Rules" on page 39](#)
- ["View or Edit Workstyle General Rules" on page 40](#)
- ["Account Filters" on page 43](#)
- ["Computer Filters" on page 44](#)
- ["Time Range Filters" on page 44](#)
- ["Expiry Filter" on page 45](#)
- ["Windows Management Information \(WMI\) Filters" on page 45](#)

## Access the Application Rules

Application Rules are applied to Application Groups. Application Rules can be used to enforce allow, monitor, and assign privileges to groups of applications. They are a set of rules that apply to the applications listed in the Application Group.

You need an Application Group before you can create an Application Rule.

### Insert an Application Rule

Click **Application Rules** to view, create, or modify the following for each Application Rule:

Option	Description
<b>Group</b>	
Target Application Group	Select from the Application Groups list.
<b>Rule</b>	
Run a Rule Script	<p>This option allows you to assign a rule script that is run before the Application Rule triggers.</p> <p>You need to import a rule script before you can select it here.</p> <p>Select the rule script you want to use from the dropdown list. If you select a rule script here, the following options change to <b>Default</b> to indicate that these actions are run if the rule script is not.</p>
(Default) Action	Select from <b>Allow Execution</b> or <b>Block Execution</b> . This is what happens if the application in the targeted Application Group is launched by the user.
(Default) End User Message	Select whether a message will be displayed to the user when they launch the application. We recommend using Messages if you block the execution of the application, so the end user has some feedback on why the application doesn't launch.
(Default) Access Token	<p>Select the type of token to be passed to be used for the target Application Group. You can select from:</p> <p>Passive (no change): doesn't make any change to the user's token. This is essentially an audit feature.</p> <p>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 a application that triggers UAC, the user would not be able to progress past the UAC prompt.</p> <p>Drop Admin Rights: removes administration rights from the user's token.</p> <p>Add Admin Rights: adds administration rights to the user's token.</p> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p><b>i</b> For more information on access tokens, please see <a href="https://docs.microsoft.com/en-us/windows/win32/secauthz/access-tokens">https://docs.microsoft.com/en-us/windows/win32/secauthz/access-tokens</a>.</p> </div>
<b>Auditing</b>	
Raise an Event	Whether or not you want an event to be raised if this Application Rule is triggered. This will forward to the local event log file.
Run an Audit Script	<p>This option allows you to select an Audit Script to run after the Application Rule.</p> <p>You need to use <b>Manage Scripts</b> from the dropdown to import your Audit Script before you can select it.</p> <p>Select the Audit Script you want to use from the dropdown list.</p> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p><b>i</b> For more information, please see "<a href="#">Manage Privilege Management Audit Scripts</a>" on page 97.</p> </div>
Privilege Monitoring	Raises a privileged monitoring event.
<b>McAfee ePO Reporting Options</b>	

Option	Description
ePO Threat Events	Select this option to raise an ePO Threat event. These are separate from Privilege Management Reporting events.
<b>BeyondInsight Reporting Options</b>	
BeyondInsight Events	When configured, sends BeyondInsight events to BeyondInsight.
Privilege Management Reporting	Select this option to raise a Privilege Management Reporting event. These are available in Privilege Management Reporting.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

### Application Rule Precedence

If you add more than one Application Rule to a Workstyle, then entries that are higher in the list will have a higher precedence. Once an application matches an Application Rule, no further rules or Workstyles will be 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. You can move Application Rules up and down to change the precedence.



For more information, please see the following:

- ["Application Groups" on page 46](#)
- ["Manage Privilege Management Rule Scripts" on page 97](#)

### Precedence for Application and Content Rules

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

To give a rule a higher precedence within a Workstyle:

1. Expand the relevant Workstyle and then select the rule type: application, on demand, or content.
2. Check the rule and select **Actions > Up**.
3. Repeat step 2 until you have the rule positioned correctly.

To give a rule a lower precedence, follow the procedure above, but click **Move Down**. You can also click **Move Top** or **Move Bottom** to move a rule to the top or bottom of the list.

### Create On-Demand Application Rules

You must have an Application Group before you can create an On-Demand Application Rule.



For more information, please see ["Application Groups" on page 46](#).



**Note:** *On-Demand Application Rules are only checked by Privilege Management for Windows if the user launches the application on-demand from the right-click Windows context menu. This is how they can be differentiated from Application Rules.*

The **On-Demand Application Rules** tab of the Workstyle allows you create rules to launch applications with specific privileges (usually admin rights), on-demand from a right-click Windows context menu.

### Enable and Configure an On-Demand Application Rule

1. Click **On Demand Application Rules** to view, create, or modify the following for each Application Rule:

The first check box applies to all versions of Windows that have the **Run as administrator** option on the right-click context menu. The second two check boxes apply to the Windows Classic Shell only where it applies.

#### On-Demand Integration Options

Apply the on-demand application rules to the "Run as administrator" option

#### Classic Shell Context Menu Option

Add a custom on-demand option to the Classic Shell context menu (this won't affect the "Run as administrator" option)

Custom Classic Shell Menu option

Hide "Run as" and "Run as administrator" commands in the Classic Shell context menu

The **Apply the On-Demand Application Rules to the 'Run as administrator' option** box needs to be manually checked whether you select a controlling Workstyle or not, and applies to all versions of Windows. If a user accesses an application using the right-click Windows context menu and this box is checked, Privilege Management for Windows intercepts the Windows **Run as administrator** functionality where present.

If this box is unchecked and a user launches an application on-demand using the Windows **Run as administrator** option, Privilege Management for Windows does not intercept the request. Privilege Management for Windows does not continue to process additional Application Rules.

#### Classic Shell Context Menu Option

Where the Windows Classic Shell is used, if the **Add a custom on-demand option to the Classic Shell context menu** box is checked and a user accesses an application using the right-click Windows context menu, Privilege Management for Windows adds a new option to the right-click context menu that you have configured in this select. For example, **Run with Privilege Management**.

If the **Hide "Run as" and "Run as administrator" commands in the Classic Shell context menu** box is checked, these options, if present, are hidden from the right-click context menu. Privilege Management for Windows does not continue to process additional Application Rules.

#### Manage On-Demand Languages

The menu option that is displayed can be configured for multiple languages. Privilege Management for Windows detects the regional language of the user, and if a message in that language has been configured, the correct translation is displayed.

To add a new menu option translation:

1. In the **On-Demand Application** rules click the **Add Language** button.
2. The **Add Language** dialog box appears. Select the correct language and then click **OK**.
3. The language is then added to the **Custom Classic Shell Menu Option** dropdown. You can select the language from the dropdown and add your translation. The QuickStart policy contains some predefined languages you can select if required.
4. Click **OK** in the left pane to finish configuring your languages for the on-demand messages.

Once you have more than one language, you can select **Set As Default**. This is the language that is used if the chosen language does not match the region of the end user. You can delete any language, provided it is not the default language, by selecting the language you want to delete and clicking **Delete Language**.

### Create an On-Demand Rule

On-Demand Application Rules are not checked by Privilege Management for Windows unless you have enabled them in the top section.

To add an On-Demand rule:

1. Click **Actions > Add** and configure the following options:

Option	Description
Target Application Group	Select from the Application Groups list.
Action	Select from <b>Allow Execution</b> or <b>Block Execution</b> . This is what happens if the application in the targeted Application Group is launched by the user.
End User Message	Select whether a message is displayed to the user when they launch the application. We recommend using Messages if you block the execution of the application, so the user has some feedback on why the application doesn't launch.
Access Token	Select the type of token to be passed to be user for 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 a application that triggers UAC, the user would not be able to progress past the UAC prompt.  Drop Admin Rights: removes administration rights from the user's token.  Add Admin Rights: adds administration rights to the user's token.
Auditing	
Raise an Event	Whether or not you want an event to be raised if this Application Rule is triggered. This forwards to the local EventLog file.
Run a Script	You can choose to run a script if an event is raised.
Run an Audit Script	You can choose to run an audit script if required.
Run a Rule Script	This option allows you to assign a rule script that is run before the Application Rule triggers.  You must import a rule script before you can select it here.  Select the rule script you want to use from the dropdown list. If you select a rule script here, the following options change to <b>Default</b> to indicate that these actions are run if the rule script is not.
Privilege Monitoring	Raises a privileged monitoring event.
McAfee ePO Reporting Options	

Option	Description
ePO Threat Events	Select this option to raise an ePO threat event. These are separate from Privilege Management Reporting events.
Privilege Management Reporting	Select this option to raise a Privilege Management Reporting event. These are available in BeyondTrust Privilege Management Reporting.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.



For more information, please see the following:

- "Application Groups" on page 46
- Access Tokens at <https://docs.microsoft.com/en-us/windows/win32/secauthz/access-tokens>
- "Manage Privilege Management Audit Scripts" on page 97
- "Manage Privilege Management Rule Scripts" on page 97

## Trusted Application DLL Protection

Privilege Management for Windows can dynamically evaluate DLLs for trusted applications for each Workstyle. The first Workstyle to have DLL Control **Enabled** or **Disabled** causes any configuration of DLL Control in subsequent Workstyles to be ignored.

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 DLL control affects the following applications:

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

You can turn on the monitoring of DLLs for TAP applications in any Workstyle. However, the first Workstyle to have DLL Control **Enabled** or **Disabled** causes any configuration of DLL Control in subsequent Workstyles to be ignored.

## Configure Trusted Application DLL Protection

1. Click **Trusted Application DLL Protection enabled, click to Configure** to administer how DLLs are handled for TAP applications.

Option	Description
Trusted Application Protection (DLL)	Select <b>Enabled</b> , <b>Disabled</b> , or <b>Not Configured</b> from the dropdown. The first Workstyle to be evaluated that has DLL Control <b>Enabled</b> or <b>Disabled</b> is matched by Privilege Management for Windows, meaning subsequent Workstyles are not evaluated by Privilege Management for Windows.
Action	Select from <b>Passive (No Change)</b> or <b>Block Execution</b> . This is what will happen if the DLL in the TAP application tries to run.
End User Message	Select if a message will be displayed to the user when the DLL tries to run (regardless of it's allowed to run). We recommend using Messages if you're blocking a DLL from running so the end user has some feedback.

Option	Description
Auditing	
Raise an Event	Whether or not you want an event to be raised if the TAP application tries to run a DLL. This will forward to the local event log file.
McAfee ePO Reporting Options	
ePO Threat Events	Select this option to raise an ePO Threat event. These are separate from Privilege Management Reporting events.
Privilege Management Reporting	Select this option to raise a Privilege Management Reporting event. These are available in Privilege Management Reporting in BeyondInsight.
Exclusions	
Exclude DLLs from Rule	Enter DLLs here that you want to exclude from DLL Control for TAP Applications. These are DLLs that have either an untrusted owner or an untrusted publisher, but you still want to be allowed to run with DLL Control for TAP enabled in the Workstyle. This list of DLLs is not validated. If the DLL name listed isn't matched by the client then nothing will be excluded.



**Note:** Third party applications may give error messages that aren't immediately clear to the end user when a DLL is blocked from running in a TAP application by Privilege Management for Windows.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

## Privilege Management Content Rules

Content Rules define the actions Privilege Management for Windows takes when content, such as a file, is launched by the user. You need a Content Group before you can create a Content Rule.



For more information, please see "[Content Groups](#)" on page 68.

## Insert a Content Rule

1. Click **Content Rules** to view, create or modify the following for each Application Rule:

Option	Description
Target Content Group	Select from the <b>Content Groups</b> list.
Action	Select from <b>Allow Modification</b> or <b>Block Access</b> . This is what occurs if the user tries to access the content.
End User Message	Select whether a message is displayed to the user when they try to access the content. We recommend using Messages if you're blocking content from being accessed, so the user has some feedback.

Option	Description
Access Token	<p>Select the type of token to be passed to be used for the target Application Group. You can select from:</p> <p><b>Passive (no change):</b> Doesn't make any change to the user's token. This is essentially an audit feature.</p> <p><b>Enforce User's default rights:</b> 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 a application that triggers UAC, the user would not be able to progress past the UAC prompt.</p> <p><b>Drop Admin Rights:</b> Removes administration rights from the user's token.</p> <p><b>Add Admin Rights:</b> Adds administration rights to the user's token.</p>
Auditing	
Raise an Event	Whether or not you want an event to be raised if this content rule is triggered. This will forward to the local EventLog file.
Run a Script	You can choose to run an audit script, if required.
McAfee ePO Reporting Options	
ePO Threat Events	Select this option to raise an ePO threat event. These are separate from Privilege Management Reporting events.
Privilege Management Reporting	Select this option to raise a Privilege Management Reporting event. These are available in Privilege Management Reporting in BeyondInsight.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.



For more information, please see the following:

- ["Content Groups" on page 68](#)
- [Access Tokens](https://docs.microsoft.com/en-us/windows/win32/secauthz/access-tokens) at <https://docs.microsoft.com/en-us/windows/win32/secauthz/access-tokens>

## View or Edit Workstyle General Rules

1. To view or edit the General Rules of a Workstyle, navigate to **Windows > Workstyles > Workstyle Name > General Rules** in the policy tree.
2. Only General Rules that are enabled are listed on the **Summary** page. Choose between **Not Configured**, **Enabled**, or **Disabled** for each General Rule.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

## Collect User Information

This rule, when enabled, raises an audit event each time a user logs on to the client machine. The audit event collects the following information, which is reported through the Enterprise Reporting pack:

- **Logon Time:** The date and time the user logged on.
- **Is Administrator:** The client checks whether the user account has been granted local administrator rights either directly or through group membership.



- **Session Type:** The type of logon session, for example, console, RDP, ICA.
- **Session Locale:** The regional settings of the user session / profile
- **Logon Client Session Hostname:** The hostname of the client the user is logging on from. This is either the local computer (for Console sessions) or the remote device name (for remote sessions).
- **Logon Client Session IP Address:** The IP address of the client the user is logging on from. This is either the local computer (for console sessions) or the remote device name (for remote sessions).

**i** For more information on user information reporting, please see the BeyondTrust [Privilege Management Reporting guides](https://www.beyondtrust.com/docs/privilege-management/windows.htm), at [www.beyondtrust.com/docs/privilege-management/windows.htm](https://www.beyondtrust.com/docs/privilege-management/windows.htm).

### Collect Host Information

This rule, when enabled, raises an audit event on computer start-up or when the Privilege Management for Windows service is started. The audit event collects the following information which is reported through the Reporting pack:

- **Instance ID:** A unique reference identifying a specific service start event.
- **OS Version:** The name and version of the operating system, including service pack.
- **Chassis Type:** The type of chassis of the client, for example, workstation, mobile, server, VM.
- **Language:** The default system language.
- **Location:** The current region and time zone of the device.
- **Client Version:** The version of the Privilege Management for Windows service.
- **Client Settings:** The type of installation and current settings of the Privilege Management for Windows service.
- **System Uptime:** Time since the computer booted.
- **Unexpected Service Start:** Only added if the service has unexpectedly started (that is, a previous start was not preceded by a service stop).

An additional event is raised when the computer shuts down, or when the Privilege Management for Windows service is stopped:

- **Instance ID:** A unique reference identifying the last service start event.
- **Computer Shutdown:** Value identifying whether the service stopped as part of a computer shutdown event.

**i** For more information on host information reporting, please see the BeyondTrust [Privilege Management Reporting guides](https://www.beyondtrust.com/docs/privilege-management/windows.htm), at [www.beyondtrust.com/docs/privilege-management/windows.htm](https://www.beyondtrust.com/docs/privilege-management/windows.htm).

### Prohibit Privileged Account Management

This rule, when enabled, blocks users from modifying local privileged group memberships. This prevents real administrators, or applications which have been granted administrative rights through Privilege Management for Windows from adding, removing, or modifying a privileged account.

The list of local privileged groups that are prohibited from modification when this rule is enabled is:

- Built-in administrators
- Power users
- Account operators
- Server operators

- Printer operators
- Backup operators
- RAS servers group
- Network configuration operators

This rule provides three options:

- **Not Configured:** This Workstyle is ignored.
- **Enabled:** The user is not be able to add, remove, or modify user accounts in local privileged groups.
- **Disabled:** Default behavior based on the users rights or those of the application.

### Enable Windows Remote Management Connections

This rule, when enabled, authorizes standard users who match the Workstyle to connect to a computer remotely via WinRM, which would normally require local administrator rights. This General Rule supports remote PowerShell command management, and must be enabled in order to allow a standard user to execute PowerShell scripts or commands.

In order to allow remote network connections, you may be required to enable the **Windows Group Policy** setting to **Access this computer from the network**.



For more information, please see the following:

- ["Insert Remote PowerShell Commands" on page 63](#)
- [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc740196\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc740196(v=ws.10))

## Filters

To view or edit the general properties of a Workstyle, navigate to **Windows > Workstyles > Workstyle Name > Filters** in the policy tree. The **Filters** section is last in the list on the right.

The **Filters** tab of a Workstyle can be used to further refine when a Workstyle is actually applied.

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

- **Account Filter:** This filter restricts the Workstyle to specific users or groups of users.
- **Computer Filter:** This filter restricts the Workstyle to specific computers (names or IP addresses), or Remote Desktop clients.
- **Time Filter:** This filter restricts the Workstyle to being applied at particular days of the week and times of the day.
- **Expiry Filter:** This filter sets the expiration of a Workstyle to a date and time.
- **WMI Filter:** This filter restricts the Workstyle based on the success or failure of a WMI query.

If you want the Workstyle to apply only if *all* filters match, select the option **ALL filters must match** from above the the **Filters** table. If you want the Workstyle to apply when *any* filter matches, select the option **ANY filter can match** from above the **Filters** table.

Filters can also be configured to apply if there are no matches. This is referred to as an *exclude* filter. To set an exclude filter, check the filter box and click **Actions > Set NOT**. To clear the exclude filter, select it and click **Actions > Clear NOT**.

Filters
Filters can be used to control who the policy should apply to
<a href="#">There is 1 Account Filter</a>
<a href="#">There is 1 Computer Filter</a>
<a href="#">There is 1 Time Range Filter</a>
<a href="#">There is 1 Expiry Filter</a>
<a href="#">There is 1 WMI Filter</a>



**Note:** Time filters and Expiry filters can only be used once in a Workstyle.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

## Account Filters

Account filters specify the users and groups the Workstyle is applied to.

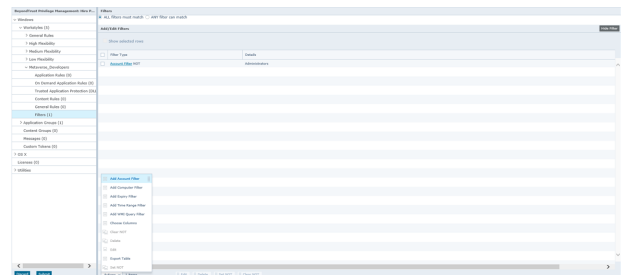


**Note:** When a new controlling Workstyle is created, a default account filter is added to target either **Standard users only**, or **Everyone (including administrators)**, depending on your selection in the Workstyle Wizard.

## Configure Account Filters

To restrict a Workstyle to specific groups or users:

1. Expand the appropriate Workstyle in the left pane and click **Filters**.
2. Select **Actions > Add Account Filter**.



3. Click on the new account filter to open the **Add/Edit Accounts** page.
4. Choose **Browse** to browse for an account, or select **Add Account** to add an account manually.
5. Click **OK**.

Domain and well-known accounts display a Security Identifier (SID). The SID is used by the Privilege Management for Windows client, which avoids account lookup operations. For local accounts, the name is used by the Privilege Management for Windows client, and the SID is looked up when the Workstyle is loaded by the client.



**Note:** SIDs must be added if using a group as a filter on a non-domain machine

By default, an account filter applies if any of the user or group accounts in the list match the user. If you have specified multiple user and group accounts within one account filter, and want to apply the Workstyle only if *all* entries in the account filter match, then check the option **All items below should match**.

You can add more than one account filter if you want the user to be a member of more than one group of accounts for the Workstyle to be applied.

If an account filter is added, but no user or group accounts are specified, a warning is displayed, advising **No accounts added**, and the account filter is ignored.



**Note:** If **All items below should match** is enabled, and you have more than one user account listed, the Workstyle never applies, as the user cannot match two different user accounts.

## Computer Filters

A computer filter specifies the computers and IP addresses that the Workstyle is applied to.

To restrict the Workstyle to specific computers:

1. Expand the appropriate Workstyle in the left pane and click **Filters**.
2. Select **Actions > Add Computer Filter**.
3. Click the new computer filter to open the **Add/Edit Computers** page.
4. Choose **Browse Systems** to select a managed computer from the McAfee ePO System Tree, or select **Add Host Name** to manually enter the computer information.
5. When you have finished adding computers to the filter, click **Finish**.

To restrict the Workstyle to specific IP addresses, follow the steps above, but click **Add IP Address** and enter an IP address.



**Note:** You can also use the asterisk wildcard (\*) in any octet to include all addresses in that octet range; for example, **192.168.\*.\***. Alternatively, you can specify a particular range for any octet; for example, **192.168.0.0-254**. Wildcards and ranges can be used in the same IP address, but not in the same octet.

By default, the hostname is matched against the host computer, where the Workstyle is being applied. If a user logs on through RDP then you may instruct the computer filter to match against the remote desktop computer by checking the **Match the remote desktop (instead of the local computer)** box. If the user logs on directly to the computer then the remote desktop is the same as the computer.

You may add more than one computer filter if you want the computer to match more than one computer filter for the Workstyle to be applied.

By default, a computer filter applies if any of the hostnames or IP Addresses in the list match the computer. If you have specified multiple hostnames and IP addresses, and want to apply the Workstyle only if ALL entries in the computer filter match, then select the option **All items below should match**.

## Time Range Filters

A time range filter can specify the hours of a day, and days of week that a Workstyle is to be applied.

To restrict a Workstyle to a specific date or time period of activity:

1. Expand the appropriate Workstyle in the left pane and click **Filters**.
2. Select **Actions > Add Time Range Filter**.
3. Click on the new time range filter.
4. Click on the 24 x 7 grid squares to toggle when the Workstyle should be made **Active** or **Inactive** and click **OK**.



**Note:** Only one time filter may be added to a Workstyle.

The time filter is applied based on the user's timezone by default. Uncheck the **Use timezone of user for time restrictions (otherwise use UTC)** box to use UTC for the timezone.

## Expiry Filter

An expiry filter specifies an expiry date and time for a Workstyle.

To restrict a Workstyle to an expiry date and time:

1. Expand the appropriate Workstyle in the left pane and click **Filters**.
2. Select **Actions > Add Expiry Filter**.
3. Click on the new expiry filter.
4. Set the date and time that you want the Workstyle to expire on and click **OK**.



**Note:** Only one expiry filter may be added to a Workstyle.

The expiry time is applied based on the user's timezone by default. Uncheck the **Use timezone of user for policy expiry (otherwise use UTC)** box to use UTC for the timezone.

## Windows Management Information (WMI) Filters

A WMI filter specifies if a Workstyle should be applied, based on the outcome of a WMI query.

The filter allows you to specify the following:

- **Description:** Free text to describe the WMI query.
- **Namespace:** Set the namespace that the query will execute 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 specified.



**Note:** Long running WMI queries result in delayed application launches. Therefore, we recommend you specify a timeout to ensure that queries are terminated in a timely manner.

When a WMI query is executed, the client checks if 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 in the execution, the WMI query is unsuccessful.

It is possible for many rows of data to be returned from a WMI query, in which case you can create more complex WQL statements using WHERE clauses. The more clauses you add to your statement, the fewer rows are likely to return, and the more specific your WMI query is.

The WMI filter includes several default templates for common WMI queries. To add a new WMI query from a template, click **Add a WMI template** and use the instant search box to quickly find a template.

WQL statements can include parameterized values which allow you to execute queries including select user, computer, and Privilege Management for Windows properties.



**Note:** WMI queries are always run as SYSTEM, 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.

By default, a WMI filter applies if any of the WMI queries in the list return true. If you have specified multiple WMI queries, and want to apply the Workstyle only if ALL queries return true, then check the option **All items below should match**.

If a WMI filter is added, but no WMI queries are specified, a warning is displayed, advising **No queries added**.

**i** For information on how to use parameters, please see "[Privilege Management for Windows Workstyle Parameters](#)" on page 30.

## 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 of the applications you want to assign to a Workstyle.

### Create an Application Group

To create an Application Group:

1. Log in to ePO Policy Orchestrator and click **Policy Catalog**.
2. Navigate to the BeyondTrustPrivilege Management for Windows policy you want to edit.
3. On the left tree menu, under the Windows branch, click on **Application Groups**, and then click **Actions > Add**.
4. Enter a name and a description (if required) for the new Application Group.
5. Check the **Hidden** box to hide the Application Group.
6. Click **OK**.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

**i** For more information, please see "[Show Hidden Groups in Privilege Management](#)" on page 103.

### View or Edit the Properties of an Application Group

Each Application Group has a name, an optional description, and can be hidden from the policy navigation tree. You can edit these in the properties for the Application Group.

To view the properties of an Application Group:

1. Log in to ePO Policy Orchestrator and click **Policy Catalog**.
2. Navigate to the BeyondTrustPrivilege Management for Windows policy which contains the Application Group you want to view or edit.
3. Check the box next to the Application Group you want to view the properties for.
4. Click **Actions > Properties** to view the properties.
5. Make any changes you require and click **OK** to save the new properties.

### Delete an Application Group

Application Groups are usually mapped to one or more Application Rule in a Workstyle. If you attempt to delete an Application Rule that is mapped to an Application Group, you are notified of this before you continue. If you continue to delete the Application Group, the associated Application Rule in the Workstyle is also deleted.

To delete an Application Group:

1. Log in to ePO Policy Orchestrator and click **Policy Catalog**.
2. Navigate to the BeyondTrustPrivilege Management for Windows policy that contains the Application Group you want to delete.
3. Check the box adjacent to the Application Group you want to delete.
4. Click **Actions > Delete**. If there aren't any Application Rules in the Workstyle using that Application Group, then it is deleted. If there are Application Rules in the Workstyle that are referencing that Application Group, then you are prompted to check the reference before you continue. If you click **OK** then both the Application Group and the Application Rule that references it are deleted from your policy. If you don't want to do this, click **Cancel**.

## Duplicate an Application Group

You can duplicate an Application Group if you need a new Application Group that contains the same applications as an existing Application Group. You can edit a duplicated Application Group independently of the Application Group it was duplicated from.

To duplicate a Application Group:

1. Log in to ePO Policy Orchestrator and click on **Policy Catalog**.
2. Navigate to the BeyondTrustPrivilege Management for Windows policy that contains the Application Group you want to duplicate.
3. Select the Application Group you want to duplicate.
4. Under the Windows branch, click on **Application Groups**, then click **Actions > Duplicate**.

A new duplicate Application Group with an incremental number in brackets appended to the name is created. After creation, you can add applications to the Application Group.

## Application Definitions

Once you have created an Application Group you need to create application definitions within the Application Group.

Application definitions allow you to target applications based on specific properties. When an application is executed, Privilege Management for Windows queries the properties of the application and attempts to match them against the matching criteria in the definition. If a match is made, then the rule is applied. If any of the matching criteria do not match, then neither does the definition, and Privilege Management for Windows attempts to match against subsequent definitions in the Application Group.

Privilege Management for Windows continues this process for subsequent Application Groups defined in Application Rules until a successful match is made and the rule is applied. If no matches are made, then no rule is applied to the application, and it runs as normal.

The Privilege Management for Windows client must match every enabled criteria in an application definition before it triggers 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** from the dropdown.

## Application Definition Matching Criteria



### IMPORTANT!

*Many of the matching criteria below support using wildcards such as an asterisk (\*). Care must be taken when using these wildcards, as misuse can lead to undesirable behavior, such as blocking or elevating all applications.*

## ActiveX Codebase matches

When inserting ActiveX controls this is enabled by default. We recommend that 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 recommend that you enter the full URL to the codebase, as it is more secure.

## ActiveX Version matches

If the ActiveX control you entered has a version property, then you can choose either **Check Min Version**, **Check Max Version**, or both, and edit the respective version number fields.

## App ID matches

This option allows you to match the AppID of the COM class, which is a GUID used by Windows to set properties for a CLSID. AppIDs can be used by one or more CLSIDs.

## Application Requires Elevation (UAC)

This option can be used to check if an executable requires elevated rights to run and would cause User Account Control (UAC) to be triggered. This is a useful way to replace inappropriate UAC prompts with Privilege Management for Windows end user messages to either block or prompt the user for elevation.

## Application Requires Elevation (UAC) (Supported on 'Install' only)

This option can be used to check if an MSI requires elevated rights to run and would cause UAC to be triggered.

## Uninstaller

This option allows you to match on any uninstaller type (MSI or EXE).

## BeyondTrust Zone Identifier exists

This option allows you to match on the BeyondTrust Zone Identifier tag, where present. If an Alternate Data Stream (ADS) tag is applied by the browser, we also apply an BeyondTrust Zone Identifier tag to the file. The BeyondTrust Zone Identifier tag can be used as matching criteria if required.

## CLSID matches

This option allows you to match the Class ID of the ActiveX control or COM class, which is a unique GUID stored in the registry.



## COM Display Name matches

If the class you entered has a Display Name, then it is automatically 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 (? and \*) or a regular expression. The available operators are identical to **File or Folder Name** definition.

## Command Line matches

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 (? 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 their transmittal to the target. Therefore we recommend that Command Line definitions not include double quotes, as they will fail to match the command.

## Drive matches

This option can be used to check the type of disk drive that 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 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.

## File or Folder Name matches

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**

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 caution against using the definition **File or Folder Name does NOT Match** in isolation for executable types. This 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, use the Universal Naming Convention (UNC) network path rather than a mapped drive letter.

### File Hash (SHA-1 Fingerprint) matches

If a reference file is entered, then an SHA-1 hash of the PowerShell script is generated. This definition ensures that 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.

### File Version matches

If the file, service executable, or COM server you enter has a **File Version** property, then it is automatically extracted and you can choose either **Check Min Version**, **Check Max Version**, or both, and edit the respective version number fields.

### Parent Process matches

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** traverses the complete parent-child hierarchy for the application, looking for any matching parent process, whereas setting this option to **False** checks only the application's direct parent process.

### Product Code matches

If the file you enter has a Product Code, it is automatically extracted and you can choose to check this code.

### Product Description matches

If the file you enter has a Product Description property, it is automatically 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 (? and \*) or a regular expression. The available operators are identical to the **File or Folder Name** definition.

### Product Name matches

If the file, COM server, or service executable you enter has a **Product Name** property, it is automatically 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 (? and \*) or a regular expression. The available operators are identical to the **File or Folder Name** definition.

### Product Version matches

If the file or COM server or service executable you enter has a **Product Version** property, it is automatically extracted and you can choose either **Check Min Version**, **Check Max Version**, or both, and edit the respective version number fields.

### Publisher matches

This option can be used to check for the existence of a valid publisher. If you browse for an application, then the certificate subject name is automatically retrieved, if the application is signed. For Windows system files the Windows security catalog is searched, and if a match is found then 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 (? and \*) or a regular expression. The available operators are identical to the **File or Folder Name** definition.

### Service Actions match

This option allows you to 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

This option allows you to match 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

This option allows you to match 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 matches

If an application was downloaded using a web browser, this option can be used to check where the application or installer was originally downloaded from. The application is tracked by Privilege Management for Windows at the point it is downloaded, so that if a user decides 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 (? and \*) or a regular expression. The available operators are identical to the **File or Folder Name** definition.

## Trusted Ownership matches

This option can be used 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 matches

If the file you enter has an **Upgrade Code** property, then it is automatically extracted and you can choose to check this code.

## Windows Store Application Version

This option allows you to match the version of the Windows Store application, for example **16.4.4204.712**. You can choose either **Check Min Version**, **Check Max Version**, or both, and edit the respective version number fields.

## Windows Store Package Name

This option allows you to match 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

This option allows you to match 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 be used only if configuring Privilege Management for Windows settings from a Windows 8 client.

## Advanced Options

### Allow child processes will match this application definition

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

this option prevents a child process from matching a lower precedence rule. It should also be noted that if an application is launched via an On-Demand rule and this option is selected, then its children are processed against the On-Demand rules, and not the Application Rules. If this option is not selected, then the children are 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 matches 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 was executed. For example, if the parent was executed through on-demand shell elevation, then the Privilege Management for Windows client first attempts to match On-Demand Application Rules for any children of the executed application.

### Force standard user rights on File Open and Save common dialogs

If the application allows a user to open or save files using the common Windows open/save dialog box, then selecting this option ensures that 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, then the Open and Save dialog boxes allow a user to replace protected system files.

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

### Insert Applications from Browsing

Applications and services can be added to Application Groups by browsing the local or remote computer for any of the following:

- Applications on the file system
- Running processes
- Windows services

Computer browsing uses Windows Remote Management (WinRM) and PowerShell, which must be enabled on each target endpoint.

1. Select the Application Group you want to add the application to.
2. In the right pane, go to **Actions > Add Apps from Browsing**.

By default, the local computer appears in the **Remote Computer Browser** list. Expand the local computer to display a list of local drive letters, processes, and services.



For information on configuring WinRM and PowerShell for remote computer browsing, please see **"Configure Remote Computer Browser"** on page 141.

### Insert Applications from Events (Event Import)

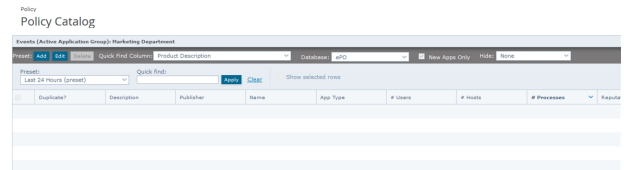
The Privilege Management for Windows Workstyle editor allows you to add applications that have been audited by Privilege Management for Windows clients. Adding applications from events provides a simple and integrated workflow for defining rules based on real application usage.

To add an application from an event:

1. Select the relevant Application Group.
2. In the right pane, select **Actions > Add Apps From Events**. The **Events** page appears.
3. Use the filters and search box to locate an audited application or scroll through the available audited applications.
4. Select an application and click **Add Application(s) to Group**.
5. Repeat steps 3 and 4 until all desired applications have been added.
6. Click **Finish** to exit and return to the Application Group.

The **Events** page includes the following filters:

- **Preset Add:** Create a new custom filter that can be saved and then selected from the **Preset** dropdown list.
- **Preset Delete:** Delete the currently selected preset.
- **New Apps Only:** If checked, the list is filtered on those apps where the **Date First Recorded** is within the **Date Executed** range.
- **Preset Edit:** Create and edit custom filters that are saved and can be selected from the **Preset** dropdown menu.
- **Preset:** Select any previously created custom filters in addition to the standard time filters provided.
- **Quick Find Column:** A selection of default quick filters.
- **Quick Find:** Enter text to find applications. Entered text will match against the **Quick Find Column** selection. For example, to filter on a specific username, click **User** from the **Quick Find Column**, and type the username in the **Quick Find** box and click **Apply**.
- **Database:** Toggles between searching the Reporting database and the ePO database.
- **Hide:** Hide applications already added to **apps in current group** or **apps in any group**.



Once the search criteria has been entered, the page automatically returns a list of unique applications that were audited, matching the criteria you specified. From here you can browse the list.

Once the applications have been added to the Application Group, you can edit the definitions. All definitions are prepopulated with values collected from the application.



**Tip:** For queries that are taking a long time to execute, you can click the **Cancel Query** button if you wish to cancel the query.



**Note:** A unique application is based on the **Product Description** of the application, so if two or more audited applications share the same **Product Description**, they are displayed as a single application.

## Update Reputation



**Note:** For the **Update Reputation** option to be available, the **BeyondTrust Privilege Management Reputation Settings** on the **ePO's Configuration > Server Settings** page must be enabled.

You can update the reputation from this page.

1. Check the box adjacent to the rows you wish to update the reputation for.
2. Select **Actions > Update Reputation**.

## Insert Applications from Templates

Application templates provide a simple way to pick from a list of known applications. A standard set of templates are provided that cover basic administrative tasks for all supported operating systems, common ActiveX controls, software updaters and BeyondTrust utilities.

There are two ways you can insert applications into Application Groups. If you want to insert multiple applications from the BeyondTrust templates, you need to add the applications from the template menu.

If you use the template functionality, then once you have selected your application type, the list from BeyondTrust is filtered to just those applications and you may add only one at a time.

## Use the Add Apps to Template Menu

1. Select the Application Group you want to add the application to.
2. Select **Actions > Add Apps from Templates**. Choose one or more applications to add to the Application Group. You can select multiple rows using standard Windows functionality.
3. Click **Save** to add the applications or click **Finish** to exit without adding any applications.

## Use the Template Option in Matching Criteria

1. Select the Application Group you want to add the application to.
2. Select **Actions > Add Application > Your Chosen Application** from the menu.
3. Click **Template** next to the **Description** and choose the application you chose to add to the Application Group.
4. Select the applications you want to add to the Application Group. Each application is highlighted once selected. Use the filter options **Filter Text** or **Type**, at the top of the page to refine the number of applications displayed.
5. Click **Save**.

You can click on an application description to modify the settings of the application definition(s), the **Advanced Options**, or both.



*For more information, please see the following:*

- ["Use the Add Apps to Template Menu" on page 55](#)
- ["Use the Template Option in Matching Criteria" on page 55](#)

## Insert ActiveX Controls

Unlike other application types, 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 they run with the standard privileges of the web browser.

1. Select the Application Group you want to add the ActiveX control to.
2. In the right pane, go to **Actions > Add Application > ActiveX Control**.
3. We recommend that you add a **Description** so that you can identify the Active X Control in the Application Group table. The **Description** is not used as matching criteria for the application definition. Alternatively, you can click the **Template** button to add an **Active X Control** from a list of templates.

4. You need to configure the matching criteria for the executable. You can configure:
  - ActiveX Codebase matches
  - CLSID matches
  - ActiveX Version matches
5. You need to configure the **Advanced Options** for the application. You can configure:
  - Allow child processes will match this application definition
  - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The application is added to the Application Group.

**i** For more information, please see the following:

- ["Insert Applications from Templates" on page 55](#)
- ["Application Definitions" on page 47](#)
- ["Advanced Options" on page 52](#)

## Insert Batch Files

1. Select the Application Group you want to add the application to.
2. In the right pane, select **Actions > Add Application > Executable**.
3. We recommend that you add a **Description** so that you can identify the batch file in the Application Group table. The **Description** is not used as matching criteria for the application definition.
4. You need to configure the matching criteria for the Batch File. You can configure:
  - File or Folder Name matches
  - Command Line matches
  - Drive matches
  - File Hash (SHA-1 Fingerprint) matches
  - Trusted Ownership matches
  - Application Requires Elevation (UAC)
  - Parent Process matches
  - Source URL matches
  - BeyondTrust Zone Identifier exists
5. You need to configure the **Advanced Options** for the application. You can configure:
  - Allow child processes will match this application definition
  - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The application is added to the Application Group.

**i** For more information, please see the following:

- ["Application Definitions" on page 47](#)
- ["Advanced Options" on page 52](#)



## Insert COM Classes

COM elevations are a form of elevation which are 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 Windows UAC prompts because they need administrative privileges to proceed. Privilege Management for Windows 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 allowed, audited, or both.

1. Select the Application Group you want to add the COM Class to.
2. In the right pane, select **Actions > Add Application > COM Class**.
3. We recommend that you add a **Description** so that you can identify the **COM Class** in the Application Group table. The **Description** is not used as matching criteria for the application definition. Alternatively, you can click the **Template** button to add a **COM Class** from a list of templates.
4. You need to configure the matching criteria for the application. 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:
  - File or Folder Name matches
  - Drive matches
  - File Hash (SHA-1 Fingerprint) 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
5. You need to configure the **Advanced Options** for the application. You can configure:
  - Allow child processes will match this application definition
  - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The application is added to the Application Group.



*For more information, please see the following:*

- *"Insert Applications from Templates" on page 55*
- *"Application Definitions" on page 47*
- *"Advanced Options" on page 52*

## Insert Control Panel Applets

1. Select the Application Group you want to add the application to.
2. In the right pane, select **Actions > Add Application > Control Panel Applet**.
3. We recommend that you add a **Description** so that you can identify the **Control Panel Applet** in the Application Group table. The **Description** is not used as matching criteria for the application definition. Alternatively, you can click the **Template** button to add a **Control Panel Applet** from a list of templates.
4. You need to configure the matching criteria for the Control Panel Applet. You can configure:
  - File or Folder Name matches
  - Command Line matches
  - Drive matches
  - File Hash (SHA-1 Fingerprint) 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
5. You need to configure the **Advanced Options** for the application. You can configure:
  - Allow child processes will match this application definition
  - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The application is added to the Application Group.



*For more information, please see the following:*

- *"Insert Applications from Templates" on page 55*
- *"Application Definitions" on page 47*
- *"Advanced Options" on page 52*

## Insert Executables

1. Select the Application Group you want to add the application to.
2. In the right pane, select **Actions > Add Application > Executable**.
3. We recommend that you add a **Description** so that you can identify the **Executable** in the Application Group table. The **Description** is not used as matching criteria for the application definition. Alternatively, you can click the **Template** button to add an **Executable** from a list of templates.

4. You need to configure the matching criteria for the Executable. You can configure:
  - File or Folder Name matches
  - Command Line matches
  - Drive matches
  - File Hash (SHA-1 Fingerprint) 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
5. You need to configure the **Advanced Options** for the application. You can configure:
  - Allow child processes will match this application definition
  - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The application is added to the Application Group.



*For more information, please see the following:*

- *"Insert Applications from Templates" on page 55*
- *"Application Definitions" on page 47*
- *"Advanced Options" on page 52*

## Insert Installer Packages

Privilege Management for Windows allows standard users to install and uninstall Windows Installer packages that would normally require local admin rights. Privilege Management for Windows supports the following package types:

- 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 is applied to both the installation of the file, and also uninstallation via **Add/Remove Programs**, or **Programs and Features**.



**Note:** *By default, elevation of software uninstalls is disabled in Privilege Management for Windows. When this feature is enabled, then the **Repair** option is not available for any installed software package that matches a Workstyle. If you want to grant uninstall privileges to users, and do not require the use of the **Repair** option, you can enable MSI Uninstall support by adding the following registry entry:*



**HKEY\_LOCAL\_MACHINE\Software\Avecto\Privilege Guard Client\ DWORD "MsiUninstallFeatureEnabled" = 1**



**Note:** The publisher property of an MSI, MSU, or MSP file may sometimes differ to the publisher property once installed in **Programs and Features**. We therefore recommend that applications targeted using the Match Publisher validation rule are tested for both installation and uninstallation, prior to deployment, using the Privilege Management for Windows Activity Viewer.

Installer packages typically create child processes as part of the overall installation process. We therefore recommend that when you elevate MSI, MSU or MSP packages, that you enable the advanced option **Allow child processes will match this application definition**.



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

1. Select the Application Group you want to add the installer package to.
2. In the right pane, select **Actions > Add Application > Installer Package**.
3. We recommend that you add a **Description** so that you can identify the installer package in the Application Group table. The **Description** is not used as matching criteria for the application definition. Alternatively, you can click the **Template** button to add an installer package from a list of templates.
4. You need to configure the matching criteria for the installer package. You can configure:
  - File or Folder Name matches
  - Command Line matches
  - Drive matches
  - File Hash (SHA-1 Fingerprint) 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
5. You need to configure the **Advanced Options** for the application. You can configure:
  - Allow child processes will match this application definition
  - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The application is added to the Application Group.

- i** For more information, please see the following:
- *"Insert Applications from Templates" on page 55*
  - *"Application Definitions" on page 47*
  - *"Advanced Options" on page 52*

## Insert Management Console Snap-ins

1. Select the Application Group you want to add the application to.
2. In the right pane, navigate to **Actions > Add Application > Management Console**.
3. We recommend that you add a **Description** so that you can identify the **Management Console Snap-ins** in the Application Group table. The **Description** is not used as matching criteria for the application definition. Alternatively, you can click the **Template** button to add a **Management Console Snap-in** from a list of templates.
4. You need to configure the matching criteria for the Management Console snap-ins. You can configure:
  - File or Folder Name matches
  - Command Line matches
  - Drive matches
  - File Hash (SHA-1 Fingerprint) matches
  - Publisher matches
  - Trusted Ownership matches
  - Application Requires Elevation (UAC)
  - Parent Process matches
  - Source URL matches
  - BeyondTrust Zone Identifier exists
5. You need to configure the **Advanced Options** for the application. You can configure:
  - Allow child processes will match this application definition
  - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The application is added to the Application Group.

- i** For more information, please see the following:
- *"Insert Applications from Templates" on page 55*
  - *"Application Definitions" on page 47*
  - *"Advanced Options" on page 52*

## Insert PowerShell Scripts

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 allowed.

1. Select the Application Group you want to add the PowerShell script to.
2. In the right pane, select **Actions > Add Application > PowerShell Script**.

3. We recommend that you add a **Description** so that you can identify the **PowerShell Script** in the Application Group table. The **Description** is not used as matching criteria for the application definition.
4. You need to configure the matching criteria for the PowerShell script. You can configure:
  - File or Folder Name matches
  - Command Line matches
  - Drive matches
  - File Hash (SHA-1 Fingerprint) matches
  - Publisher matches
  - Trusted Ownership matches
  - Parent Process matches
  - Source URL matches
  - BeyondTrust Zone Identifier exists
5. You need to configure the **Advanced Options** for the application. You can configure:
  - Allow child processes will match this application definition
  - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The **PowerShell Script** is added to the Application Group.



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



For more information, please see the following:

- ["Application Definitions" on page 47](#)
- ["Advanced Options" on page 52](#)

## Insert Registry Settings

1. Select the Application Group you want to add the application to.
2. In the right pane, select **Actions > Add Application > Registry Settings**.
3. We recommend that you add a **Description** so that you can identify the registry settings in the Application Group table. The **Description** is not used as matching criteria for the application definition.
4. You need to configure the matching criteria for the registry setting. You can configure:
  - File or Folder Name matches
  - Command Line matches
  - Drive matches
  - File Hash (SHA-1 Fingerprint) matches
  - Trusted Ownership matches
  - Application Requires Elevation (UAC)
  - Parent Process matches

- Source URL matches
  - BeyondTrust Zone Identifier exists
5. You need to configure the **Advanced Options** for the application. You can configure:
    - Allow child processes will match this application definition
    - Force standard user rights on File Open/Save common dialogs
  6. Click **OK**. The application is added to the Application Group.

**i** For more information, please see the following:

- *"Application Definitions" on page 47*
- *"Advanced Options" on page 52*

## Insert Remote PowerShell Commands

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

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

Privilege Management for Windows 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 allowed. All remote PowerShell commands are fully audited for visibility.

In order to allow standard users to connect to a remote computer via 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 Privilege Management for Windows Workstyle the ability to connect via 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 PowerShell command to.
2. In the right pane, select **Actions > Add Application > Remote PowerShell Command**.
3. We recommend that you add a **Description** so that you can identify the **Remote PowerShell Command** in the Application Group table. The **Description** is not used as matching criteria for the application definition. Alternatively, you can select **Browse Cmdlets**. This lists the PowerShell cmdlets for the version of PowerShell that you have 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. You need to configure the matching criteria for the Remote 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 Privilege Management for Windows for remote PowerShell commands.

5. Click **OK**. The application is added to the Application Group.



**Note:** If you want to manage Remote PowerShell scripts instead of a single cmdlet, see *"Insert Remote PowerShell Scripts" on page 64*.

## Messages

Privilege Management for Windows 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 is displayed in the remote console session as an error.



For more information, please see "[Application Definitions](#)" on page 47.

## Insert Remote PowerShell Scripts

From within a remote PowerShell session, a script (.PS1) can be executed from a remote computer against a target computer. Normally this would require 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
```

Privilege Management for Windows allows you to 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 allowed. All remote PowerShell scripts executed are fully audited for visibility.



**Note:** You must use the **Invoke-Command** cmdlet to run remote PowerShell scripts. Privilege Management for Windows 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).

Privilege Management for Windows allows you to 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 via a Workstyle.

PowerShell scripts and commands can be allowed 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.

In order to allow standard users to connect to a remote computer via 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 Privilege Management for Windows Workstyle the ability to connect via 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 Remote PowerShell script to.
2. In the right pane, select **Actions > Add Application > Remote PowerShell Script**.
3. Add a **Description** for the Remote PowerShell Script.
4. You need to configure the matching criteria for the PowerShell script. You can configure:
  - File Hash (SHA-1 Fingerprint) matches
  - Publisher matches
5. Click **OK**. The application is added to the Application Group.





**Note:** A remote PowerShell script that contains only a single line is interpreted and matched as a Remote PowerShell Command, and fails to match a PowerShell script definition. We therefore recommend that 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

Privilege Management for Windows 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 is displayed in the remote console session as an error.



For more information, please see ["Application Definitions" on page 47](#).

## Insert Uninstaller (MSI or EXE)

Privilege Management for Windows 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 Privilege Management for Windows policy, the user can uninstall applications using **Programs and Features** or, in Windows 10, **Apps and Features**.

The **Uninstaller** application type allows you to uninstall any 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 that when you target the Application Group in the Application Rules you set the access token to **Add Admin Rights**.



**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 BeyondTrust Privilege Management for Windows or the BeyondTrust iC3 Adapter using Privilege Management for Windows irrespective of your user rights. Privilege Management for Windows's anti-tamper mechanism prevents users from uninstalling Privilege Management for Windows, and the uninstall fails with an error message.



**Note:** If a user attempts to use Privilege Management for Windows to modify the installation of Privilege Management for Windows, 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 is displayed.

If you want to allow users to uninstall either BeyondTrust Privilege Management for Windows or the BeyondTrust iC3 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.



For more information, please see ["Edit a Custom Token in a Workstyle" on page 82](#).

## Upgrade Considerations

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

Pre 5.7 versions of Privilege Management for Windows no longer match the upgraded rules. The behavior is 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. In the right pane, select **Actions > Add Application > Uninstaller (msi or exe)**.
3. We recommend that you add a **Description** so that you can identify the uninstaller in the Application Group table. The **Description** is not used as matching criteria for the application definition.
4. Configure the matching criteria for the executable. You can configure:
  - **File or Folder Name matches**
  - **Publisher matches**
  - **Product name matches**
  - **Upgrade Code matches**
5. The advanced options are selected by default for the uninstaller application type. This cannot be changed.
6. Click **OK**. The application is added to the Application Group.

## Insert Windows Scripts

1. Select the Application Group you want to add the application to.
2. In the right pane, select **Actions > Add Application > Windows Scripts**.
3. We recommend that you add a **Description**, so that you can identify the **Windows Script** in the Application Group table. The **Description** is not used as matching criteria for the application definition.
4. You need to configure the matching criteria for the Windows Script. You can configure:
  - File or Folder Name matches
  - Command Line matches
  - Drive matches
  - File Hash (SHA-1 Fingerprint) matches
  - Publisher matches
  - Trusted Ownership matches
  - Application Requires Elevation (UAC)
  - Parent Process matches
  - Source URL matches
  - BeyondTrust Zone Identifier exists
5. You need to configure the **Advanced Options** for the application. You can configure:
  - Allow child processes will match this application definition
  - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The application is added to the Application Group.

**i** For more information, please see the following:

- ["Application Definitions" on page 47](#)
- ["Advanced Options" on page 52](#)

## Insert Windows Services

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

1. Select the Application Group you want to add the application to.
2. In the right pane, select **Actions > Add Application > Windows Services**.
3. We recommend that you add a **Description** so that you can identify the **Window Service** in the Application Group table. The **Description** is not used as matching criteria for the application definition. Alternatively, you can click the **Template** button to add a **Windows Service** from a list of templates.
4. You need to configure the matching criteria for the Windows Services. You can configure:
  - File or Folder Name matches
  - Command Line matches
  - Drive matches
  - File Hash (SHA-1 Fingerprint) 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
5. You need to configure the **Advanced Options** for the application. You can configure:
  - Allow child processes will match this application definition
  - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The application is added to the Application Group.

**i** For more information, please see the following:

- ["Application Definitions" on page 47](#)
- ["Advanced Options" on page 52](#)

## Insert Windows Store Applications

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



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

1. Select the Application Group you want to add the application to.
2. In the right pane, select **Actions > Add Application > Windows Store Applications**.
3. We recommend that you add a **Description** so that you can identify the **Windows Store Application** in the Application Group table. The **Description** is not used as matching criteria for the application definition. Alternatively, you can click the **Template** button to add a **Windows Store Application** from a list of templates.
4. You need to configure the matching criteria for the executable. You can configure:
  - Windows Store Package Name
  - Windows Store Publisher
  - Windows Store Application Version
5. Click **OK**. The application is added to the Application Group.



*For more information, please see the following:*

- *"Insert Applications from Templates" on page 55*
- *"Application Definitions" on page 47*

## Content Groups

Content control allows you to control the accessibility of privileged content. Content Groups provide a means of targeting specific types of content, based on file or folder, drive, or controlling process. Rules determining the behavior for that content are applied to each Content Group in a Workstyle.

There are two main use cases for applying content control:

1. To allow standard users to modify privileged content, without having to assign admin rights to either the user or to the application used to modify the content.

Content Groups can be added to content rules 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.

2. To block access to content or directories.

Content groups can be added to content rules where the ability to open the content can be controlled with a **Block** action. When this is done, any user who would normally be able to open and read the content is blocked from opening the content.

The following sections explain how to create Content Groups including content definitions, and how to assign groups to content rules to apply the specific content control rules that meet your requirements.

## Create Content Groups

To create a Content Group:

1. Log in to ePO Policy Orchestrator and click on **Policy Catalog**.
2. Select the policy that you want to add a Content Group to.
3. Expand the operating system you want to add the Content Group to and click **Actions > Add**.
4. Enter a name and a description (if required) for the new Content Group. Click **OK**.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

## Duplicate Content Groups

You can duplicate a Content Group if you need a new Content Group that contains the same content as an existing Content Group. You can edit a duplicated Content Group independently of the Content Group it was duplicated from.

To duplicate a Content Group:

1. Browse to the **Content Group** that you want to duplicate.
2. Select **Actions > Duplicate**. You are asked to confirm the duplication.
3. A new Content Group is created that you can add content to.

## Target Content Definitions

The **Content** dialog box provides various **Content Definitions**. Privilege Management for Windows must match every definition you configure before it will trigger a match (the rules are combined with a logical AND). The following definitions are available:

### 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**

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 caution against using the definition **File or Folder Name does NOT Match** in isolation for executable types. This 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 the **File or Folder Name** is used 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

This option can be used to check the type of disk drive that 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 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

This option allows you to target content based on the process (application) that will be 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.

### Insert Content

To insert a content type:

1. Select the relevant target Content Group.
2. In the right pane select **Actions > Add**.
3. The **Add Content** dialog box appears. Enter the file or folder name.
4. Enter a description for the content and click **Next**.
5. You need to configure the matching criteria for the executable and then click **Next**. You can configure:
  - File or Folder Name
  - Drive
  - Controlling Process
6. Click **OK**. The content is added to the Content Group.

## Messages and Notifications in Privilege Management Policy

You can define any number of messages and notifications to display to the user. 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 has been 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 also allow authorization and authentication controls to be enforced before access to an application is granted.

Messages are customizable with visual styles, corporate branding and display text, so you are offered a familiar and contextual experience. Messages are assigned to Application Rules. A message displays different properties, depending on which of these targets it is assigned to. To view the differences, a **Preview** option allows you to toggle between the **Application Preview** and the **Content Preview**. This is available from the **Preview** dropdown menu located in the top-right corner of the details pane.

Once defined, a message may be assigned to an **Application Rule**, **On Demand Application Rule**, or **Content Rule** within a Workstyle by editing the rule. Depending on the type of Workstyle you create, Privilege Management for Windows may auto-generate certain messages for you to use.

## Types of Messages

You can choose from messages or notifications. Messages take focus when they're displayed to the user. Message notifications appear on the user's task bar.

Message notification text is fully customizable, so that users are given concise and relevant information about the action performed. You can edit the strings in the **Text** page of a **Message**.

Message notifications are displayed either as a systray bubble (Windows 7), or as a *toast* notification (Windows 8 and higher).



**Note:** Message notifications are not supported for SYSTEM processes.

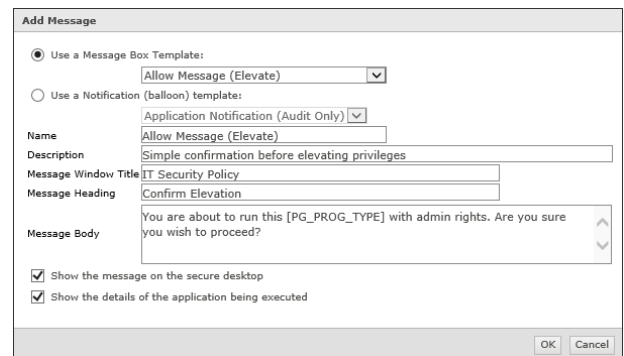


For more information, please see "[Message Text Options to Build Your Message](#)" on page 79.

## Create Messages for a Workstyle

To create a message:

1. When editing the policy, using the left tree menu, under the Windows branch, click on **Messages**, then click **Actions > Add**.



2. Select a message template from either the **Use a Message Box** template or **Use a Notification (balloon)** dropdown menus.



**Note:** Messages can be interactive (the user may be asked to input information before an action occurs). Notifications are descriptive (displaying information about an action that has occurred).

3. Customize the message (more advanced message configuration can be performed after the message has been created).
4. Click **OK**.

You may now further refine the message by selecting it and editing the **Design** and the **Text** options available beneath each message.


After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

## ActiveX Message

When Privilege Management for Windows is configured to elevate the installation of an ActiveX control, a built-in progress dialog box of the installation process appears. You can create and configure this message in the **Messages** node.

1. Click the **Messages** node and select **Actions > ActiveX Message Text**.
2. Edit the following aspects of the message:
  - **Title:** The title text of the progress dialog box.
  - **Download Message:** The text displayed during the download phase.
  - **Install Message:** The text displayed during the installation phase.
  - **Cancel Button:** The text displayed on the **Cancel** button.
3. Click **Finish** to save your changes.

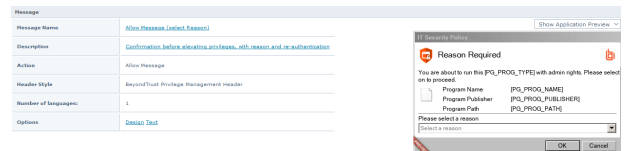
The display text can be configured for multiple languages. Privilege Management for Windows detects the regional language of the user, and if ActiveX strings in that language have been configured, the correct translation is displayed.

 **Note:** If language settings for the region of the user have not been configured, then the default language text is displayed. To change the default language, select the desired language and click **Set Default**.

## Message Name and Description

You may edit a message name or description by clicking on either element:

1. Select the **Message** (in either the left or right pane).
2. Click the underlined **Message Name** or **Description**. The **Message Properties** dialog box appears.
3. Enter the relevant text and click **OK**.



## Message Design in Privilege Management

Messages have a wide array of configuration options, which are detailed below.

You can use the preview tool to obtain a preview of how your message will look on the endpoint (program and content information will replace the appropriate placeholders). As you change the various message options, you can update the preview message by clicking the **Update** button underneath the preview image.

Once you have configured the message options, you should configure the **Message Text** for the message, which includes full multilingual support.

### Miscellaneous Settings

- **Show message on secure desktop:** Select this option to show the message on the secure desktop. We recommend this if the message is used to confirm the elevation of a process, for enhanced security.

### Message Header Settings

- **Header Style:** Select the type of header, which can be **No header**, **BeyondTrust Privilege Management**, **Warning**, **Question**, or **Error**.
- **Show Title Text:** Determines whether to show the title text.
- **Text Color:** Select the color for the title text (the automatic color is based on the **Header Style**).
- **Background Type:** Set the background of the header, which can be **Solid background**, **Gradient background**, or **Custom image**. The default **Background Type** is **Custom Image**, making the **Color 1** and **Color 2** options initially unavailable.



- **Color 1:** Select the color for a **Solid background** or the first color for a **Gradient background** (the automatic color is based on the **Header Style**).
- **Color 2:** Select the second color for a **Gradient background** (the automatic color is based on the selected **Header Style**).
- **Custom Image:** Select the image for a **Custom image** background. This option is only enabled if you have selected **Custom Image** for the **Background Type**. Click the ellipsis (...) button to import, export, modify, or delete images using the **Image Manager**.

## Image Manager

The Image Manager associated with message creation allows you to **Add, Modify, Export, and Delete** images that are referenced in message headers. All images are stored inside the Workstyles as compressed and encoded images.

We recommend that you delete any unused images to minimize the size of the policies, as Privilege Management for Windows does not automatically delete unreferenced images.

To upload an image:

1. In the **Custom Image** field select **Manage Images**.
2. Click **Upload Image**. The **Import Image status** dialog box appears. Click **Choose file** and browse to the location of the file.
3. Select the image and enter an **Image Description**. Click **OK**.
4. The image is uploaded into Image Manager.



**Note:** Images must be \*.png format and be sized between 450 x 50 and 600 x 100. The recommended image size is 450 x 50.

To edit an image:

1. In the **Custom Image** field select **Manage Images**.
2. Select the image in the list and click **Edit**.
3. The **Image Properties** dialog box appears.
4. Alter the description and click **OK**.

To delete an image:

1. Select the image in the list and click **Delete**.
2. When prompted, click **Yes** to delete the image.



**Note:** If an image is referenced by any messages then you will not be allowed to delete it.

## Message Body Settings

The options in the **Message Body Settings** section display specific information about the program or content. These can be configured on the **Message Text** page; they can display **Automatic** default values or **Custom** values. 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*.

Custom values are configured on the **Message Text** tab.

- **Show reference Hyperlink:** This option determines whether to show a hyperlink in the message below the body settings (the hyperlink is configured on the **Message Text** tab).

### User Reason Settings

This option determines whether to prompt the user to enter a reason before an application launches (**Allow Execution** message type) or to request a blocked application (**Block Execution** message type).

- **Show User Reason Prompt:** Select between **Text box** and **dropdown** menu. The **Text Box** allows users to write a reason or request. The **dropdown** allows users to select a predefined reason or request from a dropdown menu. The predefined dropdown entries can be configured on the **Message Text** tab.
- **Remember User Reasons (per-application):** Reasons are stored per-user in the registry.

### User Authorization

- **Authorization Type:** Set this option to **User must authorize** to force the user to reauthenticate before proceeding. If you want to use this option for over the shoulder administration, then set this option to **Designated user must authorize**.
- **Authentication Method:** Set this option to **Any** to allow authentication using any method available to the user. If you want to enforce a specific authentication method, then set to either **Password only** or **Smart card only**.



**Note:** If you select a method that is not available to the user, then the user will be unable to authorize the message.

- **Designated Users:** If the **Authorization Type** has been set to **Designated user must authorize** then click the ellipsis (...) button to add more user accounts or groups of users that to be allowed to authorize the message.
- **Run application as Authorizing User:** If the **Authorization Type** has been set to **Designated user must authorize** then this option determines whether the application runs in the context of the logged on user or in the context of the authorizing user. The default is to run in the context of the logged on user as opposed to the authorizing user.



**Note:** When **Run application as Authorizing User** is set to **Yes**, then *Privilege Management for Windows* attempts to match a *Workstyle* of the same type (*Application Rule* or *On-Demand Application Rule*) for the authorizing user. If no *Workstyle* is matched, then *Privilege Management for Windows* falls back to the original user *Workstyle*.



For more information, please see "**Designated User Must Authorize**" on page 74.

### Designated User Must Authorize

When this option is enabled, a designated user such as a system administrator can authorize the elevation in place of (or in addition to) a Challenge / Response code.

Input	Outcome
Valid Challenge / Response code only is provided	Application runs as logged on user
Valid Challenge / Response code is provided and valid (but not required) credentials are provided	Application runs as logged on user

Input	Outcome
Invalid Challenge / Response code is provided but valid credentials are provided	Application runs as authorizing user
No Challenge / Response code is provided but valid credentials are provided	Application runs as authorizing user

### Challenge / Response Authorization

- **Enabled:** Set this option to **Yes** to present the user with a challenge code. In order for the user to proceed, they must enter a matching response code. When this option is enabled for the first time, you are prompted to enter a shared key. You can click **Edit Key** to change the shared key for this message.
- **Authorization Period (per-application):** Set this option to determine the length of time a successfully returned challenge code is active for. Choose from:
  - **One use Only:** A new challenge code is presented to the user on every attempt to run the application.
  - **Entire Session:** A new challenge code is presented to the user on the first attempt to run the application. After a valid response code has been entered, the user is not presented with a new challenge code for subsequent uses of that application until they next log on.
  - **Forever:** A new challenge code is presented to the user on the first attempt to run the application. After a valid response code has been entered, the user is not presented with a new challenge code again.
  - **As defined by helpdesk:** A new challenge code is presented to the user on the first attempt to run the application. If this option is selected then the responsibility of selecting the authorization period will be delegated to the helpdesk user at the time of generating the response code. The helpdesk user is given the ability to select one of the three above authorization periods. After a valid response code has been entered, the user does not receive a new challenge code for the duration of time specified by the helpdesks.
- **Suppress messages once authorized:** If the **Authorization Period** has not been set to **One Use Only** the **Suppress messages once authorized** option is enabled and configurable.
- **Show Information tip:** This option determines whether to show an information tip in the challenge box.
- **Maximum Attempts:** This option determines how many attempts the user has to enter a successful response code for each new challenge. Set this option to **Three Attempts** to restrict the user to three attempts; otherwise, set this option to **Unlimited**.



**Note:** After the third failure to enter a valid response code, the message is canceled and the challenge code is rejected. The next time the user attempts to run the application, they are presented with a new challenge code. Failed attempts are accumulated even if the user clicks **Cancel** between attempts.



For more information, please see the following:

- ["Challenge / Response Authorization" on page 76](#)
- ["Message Text Options to Build Your Message" on page 79](#)

### Authorization Settings

If **Authorization Type** has been set to **Designated user must authorize** this field becomes active. It allows you to choose between either:

- **Yes – Both required:** Both the Challenge / Response and the designated user credentials are required.
- **No – Either one sufficient:** Either the Challenge / Response or the designated user credentials are required.

## Email Settings

The email settings are only enabled for blocking messages.

- **Allow user to email an application request:** Select this option to allow the user to email a request to run an application (only available for the **Block Execution** message type).
- **Mail To:** Email address to send the request to (separate multiple email addresses with semicolons).
- **Subject:** Subject line for the email request.

The **Mail To** and **Subject** fields can include parameterized values, which can be used with email based automated helpdesk systems.

 For information on using parameters, please see "[Privilege Management for Windows Workstyle Parameters](#)" on page 30.

## Challenge / Response Authorization


Challenge / Response authorization provides an additional level of control for access to applications and privileges, by presenting users with a *challenge* code in a message to the user. In order for the user to progress, they must enter a corresponding *response* code into the message.

Any policy that includes a message with a challenge / response needs a shared key. This key is defined when you set up the first challenge / response message in your policy, although you can change it later, if required. If you create a Workstyle containing a challenge / response message or you create a new challenge / response message and you are not prompted to create a shared key, then there is already a shared key for the policy. You cannot view this shared key; however, you can change it if required in the **Design** page of a **Message**.

Challenge / Response authorization is configured as part of an end user message, and can be used in combination with any other authorization and authentication features of Privilege Management for Windows messaging.

Authorization is applied per user, per token, per application, meaning that each user is presented with challenge codes that when authorized, only apply to them, the token used to request access, and the specific application.

Challenge and response codes are presented as an 8 digit number, to minimize the possibility of incorrect entry. When a user is presented with a challenge code, the message may be canceled without invalidating the code. If the user runs the same application, they are presented with the same challenge code. This allows users to request a response code from IT helpdesks, who may not be immediately available to provide a response.

 For more information, please see the following:

- "[Shared Key](#)" on page 76
- On configuring challenge / response authorization enabled messages to the user, please see "[Message Design in Privilege Management](#)" on page 72

## Shared Key

The first time you create a Privilege Management for Windows end user message with a challenge, you are asked to create a shared key. The shared key is used by Privilege Management for Windows to generate challenge codes at the endpoint.

Once you have entered a shared key, it is applied to all end user messages that have challenge / response authorization enabled in the same Privilege Management for Windows settings.

To change the shared key:

1. Click the **Messages** node of a Workstyle and select **Actions > Challenge / Response Keys**.
2. In the **Challenge / Response Shared Key** dialog box, edit the **Enter Key** and **Confirm Key** with the new shared key.
3. Click **OK** to complete. If the key entered is not exact, you are presented with a warning message.



**Note:** We recommend that your shared key be at least 15 characters and include a combination of alphanumeric, symbolic, upper, and lowercase characters. As a best practice, the shared key should be changed periodically.

## Generate a Response Code

There are three ways to generate a response code. You can either use the **PGChallengeResponseUI.exe** utility that is installed as part of the Privilege Management Policy Editor or you can generate them directly within ePO.

Response codes are generated from the ePO extension using the **BeyondTrust Response Generator** page.

## Generate Response Codes from ePO

You can use the **BeyondTrust Response Generator** page in ePO to generate response codes.

View the **BeyondTrust Response Generator** page:

The **BeyondTrust Response Generator** lists all the policies that contain an end user message that is configured to present a challenge to the end user. Usually, you only have one policy that contains your challenge message configuration.

Generating response codes in the **BeyondTrust Response Generator** page:



**Note:** You do not need to type in the shared key for the policy using the **BeyondTrust Response Generator** page. This is managed for you by the **BeyondTrust ePO Extension**.

1. Navigate to the **BeyondTrust Response Generator** on the menu bar.
2. Click the **Generate response code** link to the right of the policy name that triggered the end user's challenge code. The **Generate Response Code** dialog box appears.
3. Enter the **Challenge code** provided by the end user. If this **Challenge code** has an **X** at the end you can choose the **Authorization period** from the dropdown menu. The **X** is added to the Challenge code if the Authorization period has been configured to be **As defined by helpdesk**. If the **Challenge code** doesn't have an **X** at the end then this dropdown menu is disabled. The options for the **Authorization period** dropdown menu determine the longevity of the response code.
4. Click **Generate Response Code**. The **Response code** appears below. This is the code that the user needs in order to run that application for the duration of the **Authorization period**.

## Generate Response Codes using the PGChallengeResponseUI Utility

Response codes can be generated using **PGChallengeResponseUI.exe**, which is installed as part of the Privilege Management Policy Editor installation, and is located in the **C:\Program Files\Avecto\Privilege Guard Management Consoles\** directory.

To generate a response code using the **PGChallengeResponseUI** utility:

1. Run the program **PGChallengeResponseUI.exe**.
2. In **Enter shared key**, enter the shared key you defined earlier, and in **Enter challenge code**, enter the challenge code presented to the user.

3. The response code is automatically displayed once both the **Shared Key** and the 8 character challenge code have been entered.

The **Generated Response** value is then entered into the **End User Message** which presented the corresponding challenge.



**Note:** *PGChallengeResponseUI.exe* is a standalone utility and can be distributed separately from the Privilege Management Policy Editor.

## Generate a Response Code from the Command Line

Response codes can also be generated from the command line using the **PGChallengeResponse.exe** command line utility, which is installed as part of the Privilege Management Policy Editor installation, and is located in the **C:\Program Files\Avecto\Privilege Guard Management Consoles\** directory.

To generate a response code from the command line:

1. Open the Command Prompt by clicking the Start Menu and typing **cmd.exe**.
2. In the Command Prompt, type the following command, and then press **Enter**:

```
cd "\program files\avecto\privilege guard management consoles"
```

3. Once you have opened the **\privilege guard management consoles** directory, type the following command (where **<challenge>** is the challenge code presented to a user):

```
pgchallengeresponse.exe <challenge>
```

4. At the **Shared Key** prompt, enter the correct shared key, and then press **Enter**.



**Note:** *PGChallengeResponseUI.exe* is a standalone utility and can be distributed separately from the Privilege Management Policy Editor.

## Automate Response Code Generation

The **PGChallengeResponse.exe** utility supports full command line use, allowing it to be easily integrated into any third party workflow that supports the execution of command line executables. The command line is as follows:

```
PGChallengeResponse.exe <challenge code> <shared key> <duration>
```



**Note:** *The duration parameter is optional.*

**<challenge code>** is the code presented to the user and **<shared key>** is the key that was configured within the Privilege Management for Windows settings which presented the end user message.

The utility returns the response code as an exit code, so it can be captured from within a custom script or wrapper application. The options for the optional **<duration>** parameter are **once | session | forever**.

**Example: Example VBScript**

```
Dim WshShell, oExec
Dim strChallenge, strKey, strExecutable, strType
strExecutable = "C:\Program Files\Avecto\Privilege Guard Management
Consoles\PGChallengeResponse.exe"
strChallenge = InputBox("Enter Challenge Code from user", "Challenge")
strType = InputBox("Would you like a Once, Session, or Forever key?", "Type")
strKey = InputBox("Enter Authorization Key from policy", "Key")
Set WshShell = WScript.CreateObject("WScript.Shell")
Set oExec = WshShell.Exec(strExecutable & " " & strChallenge & " " & strType & " " & strKey
)
Do While oExec.Status = 0
WScript.Sleep 100
Loop
msgbox "Response Code: " & oExec.ExitCode
Set WshShell = Nothing
Set oExec = Nothing
```



For more information, please see ["Message Text Options to Build Your Message"](#) on page 79.

## Message Text Options to Build Your Message

All of the text in the message can be configured in the **Message Text** section. You can add an additional language here and localize the text that you enter for the message text.

We recommend that you change the default text strings, as they are all English placeholders. After you have made a change to the message text, click **Update** to see your changes applied to the preview message.

The text in any text string can include parameterized values which provide more personalized messages for users.

## Languages

You can configure the text in the messages to display a language of your choice. To add a new language, click **Add Languages** and select the language you want to use from the dropdown list. You can set this language to be the default language by clicking **Set As Default**.

Privilege Management for Windows checks the locale of the user's language and tries to match it to a language in Privilege Management for Windows for Windows that you've set up. If it finds a match, then the strings for that language are displayed for the message text. If it doesn't find a match, the language that you have assigned to be the default language is used.



**Note:** Privilege Management for Windows doesn't localize the text into the language you have selected. You need to edit the message text in your chosen language.

If you have more than one language, then you can set the default language. This is the language that will be used if a user is using a language that has not been defined. The default language is set to English, but you may change the default language:

1. Select the language you want to set as the default language.
2. Click **Set As Default**.



**Note:** If you delete a language that has been set to the default language, then the language at the top of the language list is set to the default language. You must always have at least one language defined.

## General

- **Caption** controls the text at the top of the dialog box.
- **Header Message** controls the text to the right of the icon in the header if it's shown.
- **Body Message** controls the text at the top of the main message.
- **Refer URL** controls the hyperlink for the Reference URL if you selected to show it in the Message Design.
- **Refer Text** controls the text of the hyperlink for Reference URL if you selected to show it in the Message Design.

## Information

- **Message Mode:** Determines where the message can be assigned. Messages can be assigned to Application Rules, On-Demand Application Rules and Content Rules. Select **Automatic** to allow the rule type to determine the information that is displayed (Application or Content). Select **Manual** to enter your own information in the **Custom** fields. This information is displayed irrespective of the type of rule.
- **Application Line One Label:** Controls the first line. For **Automatic** mode this is the **Application Program Name**.
- **Application Line Two Label:** Controls the second line. For **Automatic** mode this is the **Application Program Publisher**.
- **Application Line Three Label:** Controls the third line. For **Automatic** mode this is the **Application Program Path**.
- **Content Line One Label:** Controls the first line. For **Automatic** mode this is the **Control Content Name**.
- **Content Line Two Label:** Controls the second line. For **Automatic** mode this is the **Content Owner**.
- **Content Line Three Label:** Controls the third line. For **Automatic** mode this is the **Control Program**.

## Publisher

- **Program Publisher (Unknown):** Controls the text that is displayed for the variable **[PG\_PROG\_PUBLISHER]** if it's not known.
- **Verification Failure:** Controls the text that is displayed in the next to the **Publisher** if the publisher verification fails.

Privilege Management for Windows verifies the publisher by checking that there is a publisher and also checking that the certificate associated with that publisher is signed. Privilege Management for Windows does not check to see if the certificate has been revoked due to the length of the lookup process that would rely on network connectivity. Instead, Privilege Management for Windows relies on the Certificate Store to be kept up to date with revoked certificates, which would be a standard operation as the full chain should be in the local certificate store.

## User Reason

- **Reason:** Controls the text above the field where the end user can enter their reason.
- **Reason Error Message:** Controls the text that is displayed if the end user clicks **Yes** and doesn't enter a reason.
- **dropdown list prompt:** Controls the text above the user reason prompt.
- **User Reason List:** Allows you to select from the user reasons. You can modify the **User Reason List** using the **Add**, **Edit** and **Delete** buttons.



## User Authentication

- **User name:** controls the text adjacent to the field where the user would enter their user name.
- **Password:** controls the text adjacent to the field where the user would enter their password.
- **Domain:** controls the text below the password field that introduces the domain.
- **Unauthorized credentials:** controls the text that is displayed if the user enters credentials that aren't valid for the requested operation.

## Challenge / Response Authorization

- **Header text:** Controls the text that introduces the Challenge / Response authorization.
- **Hint text:** Controls the text that is in the response code field for Challenge / Response messages.
- **Information Tip Text:** Controls the text above the challenge and response code fields.
- **Error Message Text:** Controls the text that is displayed to the end user if they enter an incorrect response code and click **Yes**.
- **Maximum Attempts Exceeded Message Text:** Controls the text that is displayed to the user if they exceed the allowed number of Challenge / Response attempts.

## Smart Card Authorization

- **Card Prompt:** Controls the text that introduces the card prompt.
- **Card Reading:** Controls the text that is displayed when the card is being read.
- **Card Pin:** Controls the text that is displayed when the card pin is provided.
- **Card Error:** Controls the text that is displayed if there is an error reading the card.
- **No Certificate Error:** Controls the text that is displayed when there is no certificate.
- **Incorrect Certificate Error:** Controls the text that is displayed when there is an incorrect certificate.

## Buttons

Depending on the message options the message box has either one or two buttons:

- For a prompt, the message box has **OK** and **Cancel** buttons.
- For a blocking message with **Allow user to email an application request** enabled, the message box has **OK** and **Cancel** buttons. We recommend you change the **OK** button text to be **Email**, unless you make it clear in the message text that the **OK** button will send an email request.
- For a blocking message with **Allow user to email an application request** disabled the message box has only an **OK** button.

You can change the **OK Button** and **Cancel Button** text. For instance, you can change it to **Yes** and **No** if you are asking the user a question.

- **Buttons**
  - **OK Button**
  - **Cancel Button**

 For more info on using parameters, please see "*Privilege Management for Windows Workstyle Parameters*" on page 30.

## Custom Access Tokens in a Workstyle

Access tokens (and Custom Tokens) are assigned to an application, or when content is being edited, to modify the privileges of that activity. Within an access token is a collection of settings that specify the group memberships, associated privileges, integrity level, and process access rights.

Privilege Management for Windows includes a set of built-in access tokens that can be used to add administrator rights, remove administrator rights, or enforce the users default privileges. A *passive* access token is also available that does not change the privileges of the activity, but still applies anti-tamper protection.

Access tokens are assigned to applications or content through rules within a Workstyle. For more advanced configurations, Custom Tokens can be created where group memberships, privileges, permissions, and integrity can be manually specified. You can optionally define any number of Custom Tokens.

### Create Custom Tokens

To create a Custom Token:

1. Expand the relevant Workstyle in the left pane.
2. Select the **Custom Tokens** node. The right pane displays the **All Custom Tokens** page.
3. In the right pane, select **Actions > Add Token**. The **Create New Custom Tokens** dialog box appears.
4. Select a token type and enter a **Name** and a **Description**.
5. Click **OK**.

The new Custom Token is displayed beneath the **Custom Tokens** node. Click the new token to display the **Token Summary**.

You may now define the **Groups**, **Privileges**, **Integrity Level**, and **Process Access Rights** for the Custom Token.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

### Edit a Custom Token in a Workstyle

#### Groups

The **Groups** section of the Custom Token specifies the groups to be added or removed from the token.

To insert a group:

1. Select **Groups** in the left pane. The **Token** groups appear in the right pane.
2. In the right pane, select **Actions > Add**.
3. The **Add Group to Token** dialog box appears.
4. Enter a **Group Name** and a **Security Identifier (SID)**. Select whether to **Add Account** or **Remove Account** and click **OK**.
5. By default, when you insert a group, the **Add Account** box is checked, and the group is added to the Custom Token. If you want to remove the group from the Custom Token, then uncheck the **Remove Account** box for the relevant group.
6. Domain and well-known groups display a Security Identifier (SID). The SID is used by Privilege Management for Windows, which avoids account lookup operations. For local groups the name is used by Privilege Management for Windows, and the SID is looked up when the Custom Token is created by the client. *Local Account* appears in the SID column of the groups list for local groups.



**Tip:** Alternatively, you can click **Actions > Browse** to browse Active Directory using LDAP for Groups to add, or to browse for BuiltIn Groups. Please note that you need to have created an LDAP Server in **ePO Configuration > Registered Servers** to browse AD for Groups.

## Setting 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.

If you want the user to be the owner, regardless of the presence of the administrators group, then check the **Ensure the User is always the Token Owner** box, located at the top of the **Token Groups** page.

## Anti-Tamper Protection

By default, Privilege Management for Windows 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 Privilege Management for Windows policy cache.

If you want to disable anti-tamper protection, then uncheck the **Enable anti-tamper protection** box, located at the top of the **Token Groups** page.



**Note:** Under normal circumstances, this option should remain enabled, except in certain scenarios in which elevated tasks require access to protected areas. For instance, if you are using an elevated logon script to update the local Privilege Management for Windows policy.

## Privileges

The **Privileges** section of the Custom Token specifies the privileges that are to be added to or removed from the Custom Token.

If you want to add a privilege to the Custom Token, check the **Add** box for the relevant privilege.

If you want to remove a privilege from the Custom Token, check the **Remove** box for the relevant privilege.

If you want to reset the default state of a privilege, click the **No Change** option for the relevant privilege.

To reset, add, or remove multiple privileges, check the relevant privileges and select **Actions > Set <action>** (or use the adjacent buttons).

To clear all of the privileges in the Custom Token before applying privileges, check the **Remove all existing privileges in access token before applying privileges** box. If this box is unchecked, then the privileges are added or removed from the user's default Custom Token.

## Integrity Level

The **Integrity Level** section of the Custom Token specifies the integrity level for the Custom Token.

To set the integrity level:

1. Select the **Integrity Level** node in the left pane. The integrity levels appear in the right pane as radio buttons.
2. Set the appropriate integrity level.

The integrity level should be set as follows:

Integrity Level	Description
<b>System</b>	Included for completion and should not be required
<b>High</b>	Set the integrity level associated with an administrator
<b>Medium</b>	Set the integrity level associated with a standard user
<b>Low</b>	Set the integrity level associated with protected mode (an application may fail to run or function in protected mode)
<b>Untrusted</b>	Included for completion and should not be required

### Process Access Rights

The **Process Access Rights** section of a Custom Token allows you to specify which rights other processes have over a process launched with that Custom Token.

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

### Enabling or Disabling an Access Right

Use the **Enable / Disable** options to enable or disable a specific access right.

To enable or disable multiple access rights, check the relevant access rights and select **Actions > Set <action>** (or use the adjacent buttons).

The access rights should be set as follows:

Access Rights	Description
GENERIC_HEAD	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 <b>DuplicateHandle</b>
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 <b>SetProcessWorkingSetSize</b>
PROCESS_SUSPEND_RESUME	Required to suspend or resume a process
PROCESS_TERMINATE	Required to terminate a process using <b>TerminateProcess</b>
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 <b>ReadProcessMemory</b>
PROCESS_VM_WRITE	Required to write to memory in a process using <b>WriteProcessMemory</b>

Access Rights	Description
READ_CONTROL	Required to read information in the security descriptor for the object, not including the information in the SACL
SYNCHRONIZE	Required to wait for the process to terminate using the wait functions

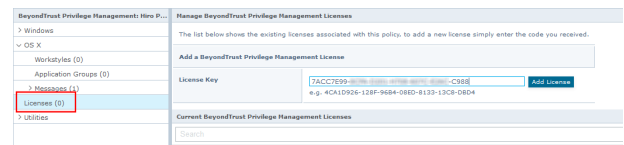
## Privilege Management for Windows Licenses

Privilege Management for Windows requires a valid license code to be entered in the Privilege Management ePO Extension. If multiple Privilege Management policies are applied to an endpoint, you need at least one valid license code for one of those policies.

For example, you could add the Privilege Management license to a Privilege Management policy that is applied to all ePO-managed endpoints, even if it doesn't have any Workstyles. This ensures that all endpoints receive a valid Privilege Management license if they have Privilege Management installed. If you are unsure, then we recommend that you add a valid license when you create the Privilege Management policy.

### Add a License Key in ePO Policy Orchestrator

1. Log in to ePO Policy Orchestrator and click on **Policy Catalog**.
2. Click the Privilege Management for Windows policy you want to add a license to and click **Licenses**.
3. Enter a valid license key for the operating system your endpoints are running into the **License Key** box in the right and click **Add License**. If **Add License** is not available, the license key is not in the correct format.



After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have McAfee Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

The license is not validated at this stage. If your license key is invalid, you receive event number **10** when the endpoint receives the policy with the license attached.



For a full list of event numbers, please see "[Events in Privilege Management for Windows](#)" on page 109.

## Privilege Management for Windows Utilities

In this section you can perform various tasks that are applicable to all operating systems.

### Application Search

The **Application Search** is an interactive list of every application that is included in all your Privilege Management for Windows policies. Each Application Group and its applications are listed with links that allow you to navigate to the application and its definition.

### Import BeyondTrust Policy

Privilege Management for Windows policies can be imported to and exported from McAfee ePO as XML files. The XML format means the policies can be migrated and shared between Privilege Management for Windows management platforms.



**Note:** Importing and exporting policies from the **Utilities** section of a policy differs from importing and exporting policies from the McAfee ePO Policy catalog, as the utility exports a BeyondTrust standard XML file. When exporting from the Policy Catalog, the exported XML uses the ePO policy format XML and as such is not suitable for import/export to the MMC.

To import a Privilege Management for Windows XML Configuration:

1. Select the **Utilities** node and click **Import Privilege Management Policy**.
2. Browse to the location of the XML file to import.
3. If you want to merge the imported settings with the settings already contained within the policy, check the **Merge imported settings** option. If you want to overwrite the existing policy with the imported policy, uncheck the **Merge imported settings** option.
4. Click **Load Configuration** to complete the import.

### Export BeyondTrust Policy

Privilege Management for Windows policies may be imported to and exported from McAfee ePO as XML files, in a format common to other editions of Privilege Management for Windows, such as Privilege Management for Windows Group Policy Edition. This allows for policies to be migrated and shared between different deployment mechanisms.

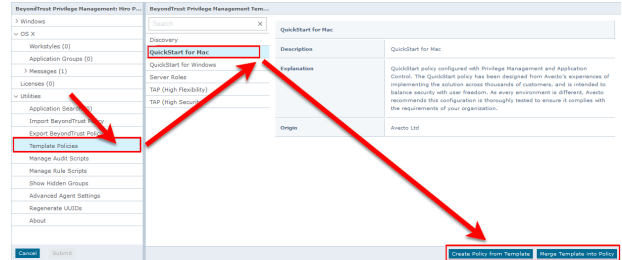


**Note:** Importing and exporting policies from the **Utilities** section of a policy differs from importing and exporting policies from the McAfee ePO Policy catalog, as the utility exports a BeyondTrust standard XML file. When exporting from the Policy Catalog, the exported XML uses the ePO policy format XML and as such is not suitable for import/export to the MMC.

1. Select the **Utilities** node and select **Export Privilege Management Policy**.
2. From the **Policy Export** page, right-click on the policy name and select **Save Link As** from the context menu. Enter a file name and select a location to save the XML file.
3. Alternatively, click on the policy name and from the dialog box select **Open with** or **Save File**.
4. If you select **Save File** the file is saved to the default downloads folder.

## Import Template Policies for Your Windows Endpoints

Templates can be imported into your Privilege Management for Windows settings for endpoints. You can choose to merge them into your existing policy; otherwise, the template overwrites your existing policy.



You can import the following templates into your existing Windows policy:

- Discovery
- QuickStart for Windows
- Server Roles
- Trusted App Protection (TAP)

### Discovery Template Policy Configuration

The Discovery policy contains **Workstyles**, **Application Groups**, and **Messages** to allow the discovery of applications that need administrative privileges to execute. This must be applied to administrator users and includes a pre-configured exclusion group (false positives) maintained by BeyondTrust.

This template policy contains the following configurations:

#### Workstyles

- Discovery Workstyle

#### Application Groups

- (Default Rule) Any Application
- (Default Rule) Any UAC Prompts
- Approved Standard User Apps
- Allowed Functions & Apps

#### Messages

- Allow Message (Yes / No)

### QuickStart for Windows Template Policy Configuration

The QuickStart policy contains **Workstyles**, **Application Groups**, **Messages**, and **Custom Tokens** configured with Privilege Management and Application Control. The QuickStart policy has been 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 your thoroughly test this configuration to ensure it complies with the requirements of your organization.

This template policy contains the following elements:

#### Workstyles



- All Users
- High Flexibility
- Medium Flexibility
- Low Flexibility

### Application Groups

- Add Admin - General (Business Apps)
- Add Admin - General (Windows Functions)
- Add Admin - High Flexibility
- Add Admin - Medium Flexibility
- Allow - Approved Standard User Apps
- Allow - Allowlisted Functions & Apps
- Block - Blocklisted Apps
- Control - Restricted Functions
- Control - Restricted Functions (On-Demand)

### Messages

- Allow Message (Authentication)
- Allow Message (Select Reason)
- Allow Message (Support Desk)
- Allow Message (Yes / No)
- Block Message
- Block Notification
- Notification (Trusted)

### Custom Tokens

- BeyondTrust Corporation Support Token

## QuickStart Policy Summary

By using and building on the QuickStart policy, you can quickly improve your organization's security without having to monitor and analyze your users' behavior first and then design and create your Privilege Management for Windows configuration.

After the QuickStart policy is deployed to groups within your organization, you can start to gather information on your users' behavior. This will provide you with a better understanding of the applications used within your organization, and whether they require admin rights, need to be blocked, or need authorizing for specific users.

This data can then be used to further refine the QuickStart policy to provide a more tailored Privilege Management for Windows solution for your organization.

## Workstyles

The QuickStart policy contains four Workstyles that should be used together to manage all users in your organization.

### All Users

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

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

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

### High Flexibility

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

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

- Allow 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

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

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

- Allow known business applications and operating system functions to run.
- Allow users to run signed applications with admin rights once they confirm that the application should be elevated.
- Prompt users to provide a reason before they can run unknown applications with admin rights .
- Allow 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

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

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

- 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).

## Application Groups

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

- **(Default) Authorize - System Trusted:** Contains operating system functions that are authorized for all users.
- **(Default) General - Any Application:** Contains all application types and is used as a catch-all for unknown applications.

- **(Default) General - Any Application Requiring Authorization:** This group contains applications types that request admin rights.
- **(Default) Passive - System Trusted:** This group contains system applications that are allowed for all users.
- **Any Other Sudo Commands:** Contains all sudo commands and is used as a catch-all for unknown sudo commands.
- **Authorize - High Flexibility:** Contains the applications that require authorization that should only be provided to the high flexibility users.
- **Authorize - Controlled OS Functions:** This group contains OS functions that are used for system administration and trigger an authorization prompt when they are executed.
- **Authorize - General Business Applications:** Contains applications that are authorized for all users, regardless of their flexibility level.
- **Authorize - Low Flexibility:** Contains the applications that require authorization that should only be provided to the low flexibility users.
- **Authorize - System Preferences:** This group contains system preferences that trigger an authorization prompt when they are executed.
- **Authorize Sudo Commands:** General. Contains sudo commands that are allowed for all users.
- **Authorize Sudo Commands:** High Flexibility. Contains sudo commands that should only be provided to the high flexibility users.
- **Block - Applications:** This group contains applications that are blocked for all users.
- **Passive - General Business Applications:** This group contains applications that are allowed for all users

## Messages

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

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

## Custom Token

A Custom Token is created as part of the QuickStart policy. The Custom Token is called **Privilege Management Support Token** and is only used to ensure an authorized user can gain access to Privilege Management for Windows troubleshooting information.



**Note:** We do not recommend using the **Privilege Management Support Token** for any other Application Rules in your Workstyles.

## 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 a Privilege Management for Windows Response code.

## Server Roles Template Policy Configuration

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

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

### Application Groups

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

### Content Groups

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

## Trusted App Protection (TAP) Template Policy Configuration

The Trusted App Protection (TAP) policies contain **Workstyles**, **Application Groups**, and **Messages** to offer an additional layer of protection against malware for trusted business applications, safeguarding them from exploitation attempts.

The TAP policies apply greater protection to key business applications including Microsoft Office, Adobe Reader, and web browsers, which are often exploited by malicious content. It works by preventing these applications from launching unknown payloads and potentially risky applications such as PowerShell. It also offers protection by preventing untrusted DLLs being loaded by these applications, another common malware technique.

In our research we discovered that malware attack chains commonly seek to drop and launch an executable or abuse a native Windows application such as PowerShell. Using a TAP policy prevents these attacks and compliments existing anti-malware technologies by preventing an attack from launching without relying on detection or reputation.

The Trusted Application Protection policy you have chosen is inserted at the top of the Workstyles so it is, by default, the first Workstyle to be evaluated. Once a Workstyle action has been triggered, subsequent Workstyles aren't evaluated for that process.

### Workstyles

- Trusted Application Protection: High Flexibility (depends on the TAP policy you have chosen)
- Trusted Application Protection: High Security (depends on the TAP policy you have chosen)

### Application Groups

- Browsers
- Browsers: Trusted Exploitables
- Browsers: Untrusted child processes
- Content Handlers
- Content Handlers: Trusted Exploitables
- Content Handlers: Untrusted child processes



**Note:** Content Handlers are used to hold content rather than executables.

### Messages

- Block Message

## Trusted Application Protection Policies Summary

The TAP policies allow you to control the child processes which TAP applications can run.

There are two policies to choose from:

- High Flexibility
- High Security

You should choose the High Flexibility policy if you have users who need the ability to download and install or update software. You should choose the High Security policy if your users don't need to download and install or update software.

The High Security policy checks that all child processes either have a trusted publisher, a trusted owner, a source URL, or a BeyondTrust Zone Identifier tag, whereas the High Flexibility policy only validates the immediate child processes allowing a wider

range installers to run. If child processes don't have any of these four criteria, they are blocked from execution. Known exploits are also blocked by both TAP policies.



**Note:** *Installers that spawn additional child processes are blocked by the TAP (High Security) policy if those child processes are using applications that are on the TAP block list, but would be allowed to run using the TAP (High Flexibility) policy. For more information, please see "Trusted Application Protection Block List" on page 96*

### 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**.

### SourceURL

- The source URL must be present. This is specific to browsers.

### BeyondTrust Zone Identifier tag

- The BeyondTrust Zone Identifier tag must be present. This is applied when the browser applies an Alternate Data Stream (ADS) tag. This is specific to browsers.

In addition, all processes on the block list are blocked irrespective of their publisher and owner.

The TAP policy template affects the following applications:

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

You can configure TAP process control by importing the TAP template. TAP also has Reporting.



**Note:** *TAP Applications and their child processes **must match all the criteria** within the definitions provided in the Application Groups of the policy for the TAP policy to apply.*



For more information, please see "Trusted Application Protection Block List" on page 96.

## Trusted Application Protection Precedence

The TAP Workstyle you choose is placed at the top of your list of Workstyles when you import the policy template. This is because it runs best as a priority rule. This ensures that child processes of TAP applications (policy dependent) that do not have a trusted publisher, trusted owner, a source URL, or a BeyondTrust Zone Identifier tag are blocked from execution and that known exploits are blocked.

The Trusted Application Protection Workstyle is the first to be evaluated by default. Once a Workstyle action has been triggered, subsequent Workstyles aren't evaluated for that process.

## Modify the Trusted Application Protection Policies

Both the TAP policies (High Flexibility and High Security) protect against a broad range of attack vectors. The approaches listed here can be used in either TAP policy if you need to modify the TAP policy to address a specific use case that is being blocked by a TAP policy.

The TAP (High Security) policy is, by design, more secure and less flexible as it blocks all child processes of a Trusted Application that do not have a trusted owner, trusted publisher, source URL, or BeyondTrust Zone Identifier, so it is therefore more likely to require modification.

The TAP policy that you choose should be based on your business requirements and existing policy. If using a TAP policy causes a legitimate use case to be blocked, there are some actions you can take to resolve this.

## Change the Policy to Passive and Audit

You can change the TAP (High Security) policy Application Rules **Action** to **Allow Execution** and change the **Access Token** to **Passive (No Change)**. Ensure **Raise an Event** is set to **On** and click **OK**.



**Note:** Changing the TAP policy to **Allow Execution** effectively disables it. You will not get any protection from a TAP policy if you make this change.

If you make this change for the four Application Rules in the TAP (High Security) policy, TAP programs can execute as if the TAP (High Security) policy is not applied, but you can see what events are being triggered by TAP and make policy adjustments accordingly.

The event details include information on the Application Group and TAP application. This allows you to gather details to understand if it's a legitimate use case. You can perform some actions to incorporate the legitimate use case into the TAP (High Security) policy.

## Use the High Flexibility Policy

Both the TAP policies offer additional protection against a wide range of attack vectors. If you are using the TAP (High Security) policy you can change to the TAP (High Flexibility) policy. This is useful if you have a use case where additional child processes of TAP applications are being blocked by the TAP (High Security) policy.

## Edit the Matching Criteria

If your legitimate use case is running a specific command that is detailed in the event, you can add this to the matching criteria of the application that's being blocked. You can use the standard Privilege Management for Windows matching criteria such as **Exact Match** or **Regular Expressions**.

**i** *Webex uses an extension from Google Chrome. BeyondTrust has catered for this in the policy using matching criteria.*

***This criteria says:***

*If the Parent Process matches the (TAP) High Security - Browsers Application Group for any parent in the tree.*

***and***

*The Product Description contains the string Windows Command Processor*

***and***

*The Command Line does NOT contain `\\pipe\chrome.nativeMessaging`*

*The TAP policy (High Security) blocks the process.*

## Edit the Trusted Exploitable List

If your legitimate use case is using an application that is listed on either the **Browsers - Trusted Exploitables** or the **Content Handlers - Trusted Exploitables** list, you can remove it.

If you remove it from either list, any browsers or content that use that trusted exploitable to run malicious content are not stopped by the TAP (High Security) policy.

### Remove Application from Trusted Application Group

You can remove the application that is listed in the **Trusted Browsers** or **Trusted Content Handlers** groups from the list. This means that the application no longer benefits from the protection offered by either of the TAP policies.

### Create an Allow Rule

You can also add a Privilege Management for Windows Allow rule and place it higher in the precedence order than the TAP (High Security) policy. This allows your use case to run but it also overrides any subsequent rules that apply to that application, so it should be used with caution.

## Trusted Application Protection Reporting

Trusted Application Protection (TAP) is reported in Privilege Management Reporting. You can use the top level TAP dashboard to view the TAP incidents over the time period, split by type of TAP application. In the same dashboard you can also see the number of incidents, targets, users, and hosts for each TAP application.

## Trusted Application Protection Block List

The following list contains all of the applications that are blocked from being launched by trusted applications when Trusted Application Protection (TAP) is enabled:

- Bash
- BG Info
- Boot Configuration Data Editor
- CDB & NTSD
- CMD - Windows Command Processor
- Command Line Interface for Microsoft® Volume Shadow Copy Service



- CScript - Microsoft ® Console Based Script Host
- FSI
- FSI Any CPU
- IEEExec
- KD & NTKD
- MSBuild
- mshta
- PSExec
- Registry Console Tool
- Regsvr
- WinDBG
- Windows PowerShell
- Windows PowerShell ISE
- WScript - Microsoft ® Windows Based Script

## Manage Privilege Management Audit Scripts

When an application is allowed, elevated, or blocked, or when content modification is allowed or blocked, Privilege Management for Windows logs an event to McAfee ePO 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, on-demand application, or Content Rule.

To add a new auditing script:

1. Navigate to the **Policy Catalog** and select the policy.
2. Select the **Utilities** node and click **Manage Audit Scripts**.
3. In the left pane, select **Action > Add**. The **Add Script** dialog box appears.
4. Enter a **Script Name**.
5. Select either **PowerShell**, **VB Script** or **Javascript** from the **Script Language** dropdown menu.



**Note:** PowerShell audit scripts can only be run in the system context.

6. Select how long the script should be allowed to execute before it is terminated, from the **Timeout** dropdown menu. By default, this is set to **Infinite**.
7. Select whether the script should be executed in the **System** context or the current **User** context, from the **Script Context** dropdown menu.
8. Enter the script code either manually or by copy and paste. Alternatively, you can import a script by selecting **Action > Import** at step 2 and browsing to the location of the relevant script.
9. Click **OK** to finish.

## Manage Privilege Management Rule Scripts

Rule scripts are PowerShell scripts that can dynamically change the Privilege Management for Windows default rule.

Rule scripts must be created outside of the Privilege Management Policy Editor and imported. You cannot create a new rule script using the **Script Manager**.

Rule scripts can be assigned to an Application Rule.

You can perform the following functions in this page:

- Import a New Rule Script
- Edit a Rule Script
- Delete a Rule Script
- Import a Settings File
- Edit your Settings File
- Delete the Settings File



For more information, please see "[Create On-Demand Application Rules](#)" on page 35.

## Import a New Rule Script

To add a new rule script:

1. Navigate to the **Policy Catalog** and select a policy.
2. Existing rule scripts are listed in the middle pane. You can use the filter to search for rule scripts. Click **Import New Script** to import a new rule script.
3. A rule script must be a PowerShell script. Click **Choose File** to navigate to the PowerShell script you want to use.
4. Select the PowerShell script and click **Open** and **OK** to import the PowerShell file.
5. Click **OK** to acknowledge the imported rule script. The rule script you've just imported is shown in the list on the left. If you select the rule script, the contents of the PowerShell file are shown on the right.



**Note:** You should not edit BeyondTrust-supported integrations, as this may affect the level of support we are able to provide.

Each rule script can have an optional associated **Settings** file, which must be in a valid \*.json format. Settings files are encrypted at the endpoint. They are useful for managing credentials required for integrations and other sensitive information.

## Edit a Rule Script

You can edit a rule script or change the timeout settings provided that it's not signed. Signed rule scripts cannot be edited in the Policy Editor but you can still change their timeout settings:

To edit a rule or change the timeout settings:

1. Select the rule script you want to edit from the left side.
2. Click **Edit Script** on the bottom.
3. Make the required changes and click **OK**.

## Delete a Rule Script

Rule scripts can be deleted even if they are assigned to a Workstyle. In this instance, you are prompted to confirm that you want to remove the association with the Workstyle. To determine if a rule script is assigned to an Application Rule in a Workstyle, select it from the list. If the rule script is assigned to an Application Rule in a Workstyle, this is indicated under the **Timeout** dropdown.

To delete a rule script:

1. Select the rule script from the list on the left.
2. Whether or not the rule script is assigned to an Application Group in a Workstyle is indicated under the **Timeout** setting dropdown. Click **Delete Script**. You are prompted to confirm the deletion. If the rule script is assigned to a Workstyle, you are told this and again prompted whether you wish to continue.
3. Click **OK** to delete the rule script or **Cancel** to leave it in place.

## Import a Settings File

Once you have added a rule script (\*.ps1), you can optionally add an associated settings file (\*.json) if one is required for the integration. The settings file contains any information that is specific to your integration environment, such as URLs, usernames, and passwords. The settings file is encrypted on the endpoint using SHA1.

To import a settings file (\*.json) and associate it with a rule script:

1. Click **Import Settings** and then **Choose file** to navigate to the settings file.
2. Select the settings file, click **Open**, and then **OK** to import it.

Once you have associated a settings (\*.json) file with a rule script (\*.ps1), it is always associated with that rule script wherever you use it. For example, if you associate a settings file with a rule script for an Application Rule and select the same rule script in an On-Demand Application Rule, the same settings file is used. Changes made to the settings or rule script file in either location are applied wherever it's used.

## Edit a Settings File

You can edit the settings file before you import it into the Policy Editor or you can edit it once you have imported it.

To edit it in the Policy Editor:

1. Select a rule script that has an associated settings file.
2. Click **Edit Settings**. Make any required changes and click **OK**. The **OK** button is not enabled until you have changed the settings file.

## Delete a Settings File

To delete an existing settings file:

1. Select a rule script that has an associated settings file.
2. Click **Delete Settings**. You are prompted to delete the settings file. Click **OK** to proceed or **Cancel** to leave the settings file in place.
1. Select the rule script you want to edit from the left side.
2. Click **Edit Script** on the bottom.
3. Make any required changes and click **OK**.

## Delete a Rule Script

Rule scripts can be deleted even if they are assigned to a Workstyle. In this instance, you are prompted to confirm that you want to remove the association with the Workstyle. To determine if a rule script is assigned to an Application Rule in a Workstyle, select it from the list. If the rule script is assigned to an Application Rule in a Workstyle, this is indicated under the **Timeout** dropdown.

1. Select the rule script from the list on the left.
2. Whether or not the rule script is assigned to an Application Group in a Workstyle is indicated under the **Timeout** setting dropdown. Click **Delete Script**. You are prompted to confirm the deletion. If the rule script is assigned to a Workstyle you are told this and again prompted whether you wish to continue.
3. Click **OK** to delete the rule script or **Cancel** to leave it in place.

## Import a Settings File

Once you have added a rule script (\*.ps1), you can optionally add an associated settings file (\*.json) if one is required for the integration. The settings file contains any information that is specific to your integration environment, such as URLs, usernames, and passwords. The settings file is encrypted on the endpoint using SHA1.

To import a settings file (\*.json) and associate it with a rule script:

1. Click **Import Settings** and then **Choose file** to navigate to the settings file.
2. Select the settings file and click **Open**, and then **OK** to import it.

Once you have associated a settings (\*.json) file with a rule script (\*.ps1), it is always associated with that rule script wherever you use it. For example, if you associate a settings file with a rule script for an Application Rule and select the same rule script in an On-Demand Application Rule, the same settings file is used. Changes made to the settings or rule script file in either location are applied wherever it's used.

## Edit a Settings File

You can edit a settings file in the Policy Editor before you import it, or you can edit it once you have imported it.

1. Select a rule script that has an associated settings file.
2. Click **Edit Settings**. Make any required changes and click OK. The **OK** button is not enabled until you have changed the settings file.

## Delete a Settings File

1. Select a rule script that has an associated settings file.
2. Click **Delete Settings**. You are prompted to delete the settings file. Click **OK** to proceed or **Cancel** to leave the settings file in place.

## Apply Power Rules Scripts to Your Application 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.

Rather than a fixed default rule that can 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 Power Shell script.

Any existing default rule within a Workstyle can be updated to a Power Rule simply by setting the action to a Power Rule script, and importing the PowerShell script you want to use. Privilege Management for Windows 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 Privilege Management for Windows 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

The Power Rule feature is highly flexible, and has 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 Privilege Management for Windows to run the application in that context.



**Note:** Power Rules are best used for exception handling and in conjunction with static policy.



For more information, please see the following:

- On creating your own Power Rule, the [Power Rules Core Scripting Guide](#)
- On using the BeyondTrust-supported integration with ServiceNow, the [ServiceNow Scripting Guide](#)
- For additional guidance on Power Rules, "[Power Rules Additional Guidance](#)" on page 101

## Power Rules Additional Guidance

You can use the PowerShell **get-help** command to get help on any cmdlet in PowerShell. You can also use the following arguments to get additional guidance on the cmdlet: **-examples**, **-detailed**, **-full**, and **-online**.

## Compatibility

Power Rules requires PowerShell 3.0 or later. Run the following command to check the version of PowerShell you are running:

```
$PSVersionTable.PSVersion
```

If you attempt to edit an Application Rule containing a Power Rule in a Privilege Management Policy Editor older than v5.3.x, the **PowerRuleScript** attribute (that is linked to the Power Rule) is removed from the Application Rule.

**i** For more information about compatibility with other Privilege Management for Windows versions, please see the [Release Notes](#) for each version, at <https://www.beyondtrust.com/docs/release-notes/>.

## Third Party Integration Security

When you integrate with a third party, you should ensure you use the most secure mechanism possible. For example, if a vendor offers both HTTP and HTTPS, you should use HTTPS.

## Supported Application Types

All application types are supported, with the following exceptions:

- Remote PowerShell Script
- Remote PowerShell Command
- Windows Service
- Windows Store Application

If you try to use these application types with a Power Rule, the Rule Script is not executed and the event states:

*Script execution skipped: Application Type not supported.*

## Validation

Some restrictions are enforced by the Privilege Management Policy Editor but cannot be enforced in a scripting environment. The following is guidance for creating your Power Rule. If Privilege Management for Windows cannot determine the correct course of action, it applies the default rule.

All **Messages** and **Tokens** must exist in your policy configuration prior to being referenced in a Power Rule script.

- The **Action** must match the **Message**. For example, if the Action is **Allow**, the message must be of type **Allow**.
- If you set the Action to **Allow**, we assume a passive token but you can add a different token such a Custom Token that you have created.
- Tokens cannot be used when the Action is **Block**.
- If you specify an *account to run as*, your Action must be **Allow**.

If the script fails, a local audit event 801 is triggered.

If you use **Set-PRRunAsProperty**, you need to use **Set-PRRuleProperty** and set the **-Action** argument to **Allow**. You can optionally set the **-Token** argument. If you don't define a token, then a passive token is applied.

The values for the **-Action** and **-Token** are case sensitive.

## Script Restrictions

There are some restrictions that you need to be aware of when you are creating your own integrations.

### Block Comments

Single line comments are supported but block comments are not. Block comments take the form:

```
<# block comment #>
```

PowerShell single line comments are supported.

```
# comment
```

## #Requires

The **#Requires** notation is not supported.

## Script Audit Failure Event

If a rule script fails, then a local Windows event is created, and the Privilege Management for Windows event number is 801. This event is always created, even when auditing is turned off. The following fields are shown in the event:

Variable Name	Description
RuleScriptFileName	Name attribute of the script in the config
RuleScriptName	Set by script properties
RuleScriptVersion	Set by script properties
RuleScriptPublisher	The publisher of the script
RuleScriptRuleAffected	Whether a rule script changed a Privilege Management for Windows rule
RuleScriptStatus	Timeout, Exception
RuleScriptResult	Script timeout exceeded: X seconds, Set Rule Properties failed validation
ExceptionType	Any valid .NET exception type
ExceptionMessage	The short exception message
ProcessId	PID of the process matching the rule
ParentProcessId	PID of the parent process matching the rule
ProcessStartTime	Time the process started
Event Time	Time the script started
UniqueProcessId	GUID of process to link this data to associated audit process event

## PowerShell Scripts Execution Policy

We recommend using one PowerShell script for each integration you create. If you create a Power Rule script that in turn calls an additional PowerShell script, you need to distribute that PowerShell script independently and may need to change your PowerShell execution policy to ensure it can run.

## Encodings

If you want to maintain signed scripts, you must ensure they are encoded in UTF-16 LE prior to importing them into Privilege Management for Windows. Rule script files exported from the Privilege Management Policy Editor are always encoded in UTF-16 LE.

Settings files are encrypted at the endpoint. Settings files must be encoded in UTF-8.

## Show Hidden Groups in Privilege Management

Some Application Groups are hidden by default, for example, Application Groups prefixed by **(Default)** in the QuickStart policy. You can show or hide Application Groups in Privilege Management for Windows .

To hide an Application Group:

1. Select the specific Application Group from within the **Application Group** and click **Actions > Application Group Properties** from the bottom menu.
2. Check the **Hidden** box and click **OK**. This Application Group is now hidden from the **Application Group** list.

To unhide an Application Group:

1. Select an Application Group and click **Actions > Application Group Properties** from the bottom menu.
2. Uncheck the **Hidden** box and click **OK**. This Application Group is now displayed in the **Application Group** list.

To show hidden Application Groups:

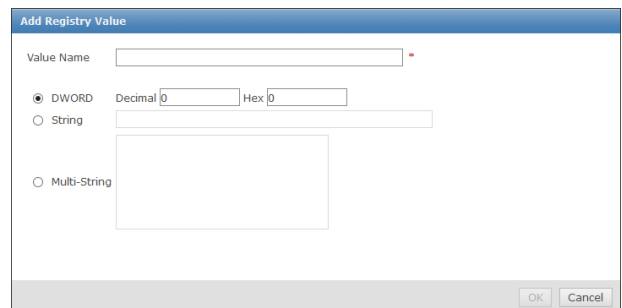
1. Click **Utilities** from the bottom menu and select **Show Hidden Groups**. This toggles the display of hidden Application Groups.

## Configure Advanced Agent Settings

The **Advanced Agent Settings** utility allows you to configure and deploy additional registry based settings to endpoints running Privilege Management for Windows . **Advanced Agent Settings** are available under the **Utilities** node.

To add a new value:

1. Select the **Utilities** node and click **Advanced Agent Settings**.
2. Select either **32-bit Agent Values** if you want to configure a 32-bit registry setting, or **64-bit Agent Values** for a 64-bit registry setting.
3. In the right pane, select **Actions > Add Value**. The **Add Registry Value** dialog box appears.



4. Enter a **Value Name** for the new setting.
5. Choose the correct type, either **DWORD**, **String** or **Multi-String**.
6. Enter the value data. For **DWORD** values, you can choose between hexadecimal and decimal.
7. Click **OK** when finished.

## Advanced Policy Editor Settings



**Note:** This page only appears if your policy has sandboxing features enabled.

Sandboxing settings are always available for you to configure if your policy has sandboxing in it. If you would like to configure sandboxing for your policy but it doesn't yet contain sandboxing, please follow these instructions.

1. Navigate to the **Policy Catalog** and click the policy you want to change.
2. From the left menu, click **Utilities > Advanced Policy Editor Settings**.



3. Check the **Show Sandboxing Settings** box. This allows you to subsequently configure sandboxing in that policy.

All of the sandboxing settings, such as URL groups, are now visible in the interface.

## Regenerate Privilege Management UUIDs

Universally Unique Identifiers (UUIDs) can be regenerated if required. You should only use this option after consulting with BeyondTrust Technical Support.

Regenerating the UUIDs can resolve issues in which you have changed a Privilege Management for Windows policy outside of the Privilege Management ePO extension, causing the UUID to be duplicated. You may need to do this if your reports are not displayed correctly.

## Deploy 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.



**Note:** Registry settings may be deployed using "[Configure Advanced Agent Settings](#)" on page 104. In order 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. For more information, see "[Windows Policy Configuration Precedence](#)" on page 138.

## Audits and Reports

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

We also provide an enterprise level, scalable reporting solution in Privilege Management Reporting. Privilege Management Reporting includes a rich set of dashboards and reports designed to simplify the centralized management and auditing of 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, please see the [ePO Installation Guide](http://www.beyondtrust.com/docs/privilege-management/windows.htm) at [www.beyondtrust.com/docs/privilege-management/windows.htm](http://www.beyondtrust.com/docs/privilege-management/windows.htm).*

## Dashboards in Privilege Management for Windows

The McAfee ePO integration includes the following dashboards:

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

To access the dashboards, click on the Dashboards icon and then select one of the 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 McAfee ePO Queries and Reports. We recommend that only advanced McAfee ePO administrators do this. Please refer to McAfee ePO documentation for details on managing dashboards, queries, and reports.*

### BeyondTrust Privilege Management: Blocked

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

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

- BeyondTrust Privilege Management: Top 10 Blocked Apps
- BeyondTrust Privilege Management: Top 10 Blocked by Publisher
- BeyondTrust 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 Privilege Management: Elevated

The **BeyondTrust Privilege Management: Elevated** dashboard contains all events raised by Privilege Management for Windows relating to applications that were elevated by 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 Privilege Management : Elevated** dashboard includes the following monitors:

- BeyondTrust Privilege Management: Top 10 Elevated Apps
- BeyondTrust Privilege Management: Top 10 Elevated by Publisher
- BeyondTrust 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.

### Privilege Management: Executed

The **BeyondTrust Privilege Management: Executed** dashboard contains all events raised by Privilege Management for Windows relating to applications that were allowed to execute under 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 Privilege Management: Executed** dashboard includes the following monitors:

- BeyondTrust Privilege Management: Top 10 Executed Apps
- BeyondTrust Privilege Management: Top 10 Executed by Publisher
- BeyondTrust 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 Privilege Management: Monitoring

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

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

- BeyondTrust Privilege Management: Top 10 Apps Requiring Elevated Rights
- BeyondTrust Privilege Management: Top 10 Requiring Elevated Rights by Publisher
- BeyondTrust 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 Privilege Management for Windows

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

The following events are logged by 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)	Privilege Management handled service control start action.
202276 (151)	Privilege Management handled service control stop action.
202277 (152)	Privilege Management handled service control pause/resume action.
202278 (153)	Privilege Management handled service control configuration action.
202279 (154)	Privilege Management blocked a service control start action.
202280 (155)	Privilege Management blocked a service control stop action.
202281 (156)	Privilege Management blocked a service control pause/resume action
202282 (157)	Privilege Management blocked a service control configuration action
202283 (158)	Privilege Management service control action run in the context of the authorizing user
202284 (159)	Privilege Management service control start action canceled
202285 (160)	Privilege Management service control stop action canceled
202286 (161)	Privilege Management service control pause/resume action canceled
202287 (162)	Privilege Management service control configuration action canceled

ePO ID (Event ID)	Description
202297 (199)	Windows only - Process execution was blocked, the maximum number of challenge / response failures was exceeded
<b>Configuration Events</b>	
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
<b>User / Computer Events</b>	
These events are not sent to ePO Dashboards.	
(300)	User User Logon
(400)	Service Privilege Management Service Start
(401)	Service Privilege Management Service Stop
<b>Content Events</b>	
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 Privilege Management Reporting Console.

## Custom Script Auditing

When an application is allowed, elevated, or blocked, 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.



For more information, please see "[Manage Privilege Management Audit Scripts](#)" on page 97.

## Set up ePO Server Tasks for Privilege Management Reporting

There are two BeyondTrust ePO server tasks that you can set up for 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.

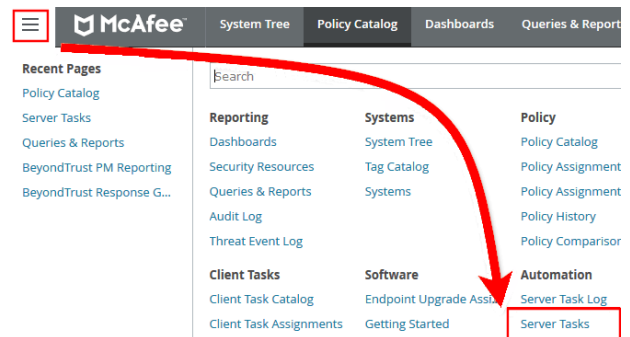
**i** For more information, please see the following:

- Create the Reporting Event Staging Server Task in the [ePO Installation Guide](https://www.beyondtrust.com/docs/privilege-management/windows/index.htm) at <https://www.beyondtrust.com/docs/privilege-management/windows/index.htm>
- Create the Enterprise Reporting Purge Server Task in the [ePO Installation Guide](https://www.beyondtrust.com/docs/privilege-management/windows/index.htm) at <https://www.beyondtrust.com/docs/privilege-management/windows/index.htm>
- "Create the Enterprise Reporting Purge Server Task" on page 113

## 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 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 Privilege Management Reporting Event Staging** from the **Actions** dropdown menu and click **Next**.
4. Adjust the times to check for events to suit your environment and click **Next**. We recommend the values depicted in the screenshot.

### Server Tasks

**Server Task Builder** 1 Description

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.	
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	<input type="checkbox"/>

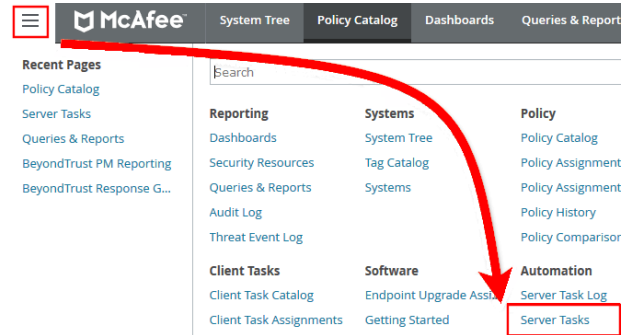
5. On the **Schedule** page, set the **Schedule type** to your preference.
6. Select the **Start date** and **End date** if required. By default, **No end date** is selected.
7. Adjust the time that you want the schedule to run. This is the time of the machine running the ePO server. Click **Next**. You are presented with a summary of the server task.
8. Select **Save** to finish creating the server task.



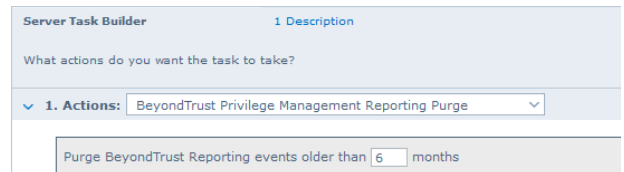
## Create the Enterprise Reporting Purge Server Task

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 Privilege Management Reporting Purge** from the **Actions** dropdown menu.
4. Choose the number of months to purge events older than.



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.

## Privilege Management for Windows Reports

### Filters

Filters and advanced filters are available from the **Filters** dropdown.

The reports retrieve data and sort it using Javascript. If the volume of data exceeds the row limit, you may get misleading results due to this restriction.

Name	Description
Action	This filter allows you to filter by a type of action. <ul style="list-style-type: none"> <li>• All</li> <li>• Elevated</li> <li>• Blocked</li> <li>• Passive</li> <li>• Sandboxed</li> <li>• Custom</li> <li>• Drop Admin Rights</li> <li>• Enforce Default Rights</li> <li>• Canceled</li> <li>• Allowed</li> </ul>
Activity ID	Each Activity Type in Privilege Management for Windows has a unique ID. This is generated in the database as required.
Admin Required	This allows you to filter on if admin rights were required, not required or both. Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• True</li> <li>• False</li> </ul>
Authorization Required	This allows you to filter on if authorization was required, not required or both. Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• True</li> <li>• False</li> </ul>
Authorization Source	This filter allows you to filter by the authorization source. Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• Authorizing User Message</li> <li>• Rule Script</li> <li>• Password Safe (Machine)</li> </ul>

Name	Description
Admin Rights	<p>Allows you to filter by the admin rights token.</p> <p>Filter options:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Detected</li> <li>• Not Detected</li> </ul>
Application Description	A text field that allows you to filter on the application description.
Application Group	A text field that allows you to filter on the Application Group. You can obtain the Application Group from the policy editor.
Application Hash	This field is used by Reporting. You do not need to edit it.
Application Type	A text field that allows you to filter on the application type. You can obtain the application type from the policy editor.
Authorizing User Name	The name of the user that authorized the message.
Browse Destination URL	The destination URL of the sandbox.
Challenge/Response	<p>Allows you to filter by challenge/response events. For example, you can filter the application that required elevation on those applications that were launched following a completed challenge/response message.</p> <p>Filter options:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Only C/R</li> </ul>
Client IPV4	This field is used by Reporting. You do not need to edit it.
Client Name	This field is used by Reporting. You do not need to edit it.
COM Application ID	This field is used by Reporting. You do not need to edit it.
COM Display Name	This field is used by Reporting. You do not need to edit it.
COM CLSID	This field is used by Reporting. You do not need to edit it.
Command Line	A text field that allows you to filter on the command line.
Date Field	<p>This allows you to filter by the time the event was generated, the application was first discovered or the time the application was first executed.</p> <p>Filter options:</p> <ul style="list-style-type: none"> <li>• Time Generated <ul style="list-style-type: none"> <li>◦ This is the time that the event was generated. One application can have multiple events. Each event has a Time Generated attribute.</li> </ul> </li> <li>• Time App First Discovered <ul style="list-style-type: none"> <li>◦ This is the time that the first event for a single application was entered into the database. This can be delayed if the user is working offline.</li> </ul> </li> <li>• Time App First Executed <ul style="list-style-type: none"> <li>◦ This is the first known execution time of events for that application.</li> </ul> </li> </ul>

Name	Description
Device Type	The type of device that the application file was stored on. Filter options: <ul style="list-style-type: none"> <li>• Any</li> <li>• Removeable Media</li> <li>• USB Drive</li> <li>• Fixed Drive</li> <li>• Network Drive</li> <li>• CDROM Drive</li> <li>• RAM Drive</li> <li>• eSATA Drive</li> <li>• Any Removeable Drive or Media</li> </ul>
Distinct Application ID	This field is used by Reporting. You do not need to edit it.
Elevate Method	Allows you to filter by the elevation method used. Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• Admin account used</li> <li>• Auto-elevated</li> <li>• On-demand</li> </ul>
Event Category	This filter allows you to filter by the category of the event. Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• Process</li> <li>• Content</li> <li>• DLL Control</li> <li>• URL Control</li> <li>• Privileged Account Protection</li> <li>• Agent Start</li> <li>• User Logon</li> <li>• Services</li> </ul>
Event Number	This field is used by Reporting. You do not need to edit it. The number assigned to the event type.
File Owner	The owner of the file.
File Version	You can filter on the file version in the Advanced View of the Process Detail report.
GPO Name	You can filter on the Group Policy Object (GPO) name in some of the advanced reports such as Process Detail.
Host Name	This field allows you to filter by the name of the endpoint the event came from.

Name	Description
Ignore Admin Required Events	This field is used by Reporting. You do not need to edit it.
Just Discovery Events	This field is used by Reporting. You do not need to edit it.
Matched	Allows you to filter on the type of matching.
	Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• Matched as child</li> <li>• Matched directly</li> </ul>
Message Name	The name of the message that was used.
Message Type	The type of message that was used:
	Filter options: <ul style="list-style-type: none"> <li>• Any</li> <li>• Prompt</li> <li>• Notification</li> <li>• None</li> </ul>
Ownership	Allows you to group by the type of owner.
	Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• Trusted owner</li> <li>• Untrusted owner</li> </ul>
Parent PID	The operating system process identifier of the parent process.
Parent Process File Name	The file name of the parent process.
Path	Allows you to filter by the path. For example, to filter on applications that were launched from the System path.
	Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• System</li> <li>• Program Files</li> <li>• User Profiles</li> </ul>
PID	The operating system process identifier.
Platform	Filters by the type of operating system.
	Windows <ul style="list-style-type: none"> <li>• Filters by endpoints running a Windows operating system.</li> </ul> macOS <ul style="list-style-type: none"> <li>• Filters by endpoints running a Mac operating system.</li> </ul>
Process Unique ID	The unique identification of the process.

Name	Description
Product Code	This field is used by Reporting. You do not need to edit it.
Product Name	The product name of the application.
Product Version	The product version of the application.
Program Files Path	Sets the Program Files path used by the <b>Discovery &gt; By Path</b> report.
Publisher	The publisher of the application.
Range End Time	The end time of the range being displayed.
Range Start Time	The start time of the range being displayed.
Row Limit	The maximum number of rows to be retrieved from the database.
Rule Script Affected Rule	True when the Rule Script (Power Rule) changed one or more of the default Privilege Management for Windows rules, otherwise false.
Rule Script File Name	The Rule Script (Power Rule) file name on disk if applicable.
Rule Script Name	The name of the assigned Rule Script (Power Rule).
Rule Script Output	The output of the Rule Script (Power Rule).
Rule Script Publisher	The publisher of the Rule Script (Power Rule).
Rule Script Result	The result of the Rule Script (Power Rule). This can be:  <None> Script ran successfully [Exception Message] Script timeout exceeded: <X> seconds Script execution canceled Set Rule Properties failed validation: <reason> Script execution skipped: Challenge Response Authenticated Script executed previously for the parent process: Matched as a child process so cached result applied Script execution skipped: <app type> not supported Script execution skipped: PRInterface module failed signature check Set RunAs Properties failed validation: <reason>
Rule Script Status	The status of the Rule Script (Power Rule). This can be:  <None> Success Timeout Exception Skipped ValidationFailure
Rule Script Version	The version of the assigned Rule Script (Power Rule).
Rule Match Type	Rule Match Type: <ul style="list-style-type: none"> <li>• Any</li> <li>• Direct match</li> <li>• Matched on parent</li> </ul>

Name	Description
Sandbox	The sandboxed setting. Filter options: <ul style="list-style-type: none"> <li>• Not Set</li> <li>• Any Sandbox</li> <li>• Not Sandboxed</li> </ul>
Shell or Auto	Whether the process was launched using the shell <b>Run with Privilege Management</b> option or by normal means (opening an application): Filter options: <ul style="list-style-type: none"> <li>• Any</li> <li>• Shell</li> <li>• Auto</li> </ul>
Show Discovery Events	Whether or not you want to show Discovery events. An event is a Discovery event if it's been inserted into the database in the filtered time period.
Source	The media source of the application. For example, was the application downloaded from the Internet or removable media. Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• Downloaded over the internet</li> <li>• Removable media</li> <li>• Any external source</li> </ul>
System Path	Sets the system path.
Target Description	This field allows you to filter by the target description.
Target Type	This filter allows you to filter by a type of target. For example, you can filter to the applications that have been canceled across your time range in the <b>Actions &gt; Canceled</b> report. Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• Applications</li> <li>• Services</li> <li>• COM</li> <li>• Remote PowerShell</li> <li>• ActiveX</li> <li>• URL</li> <li>• DLL</li> <li>• Content</li> </ul>

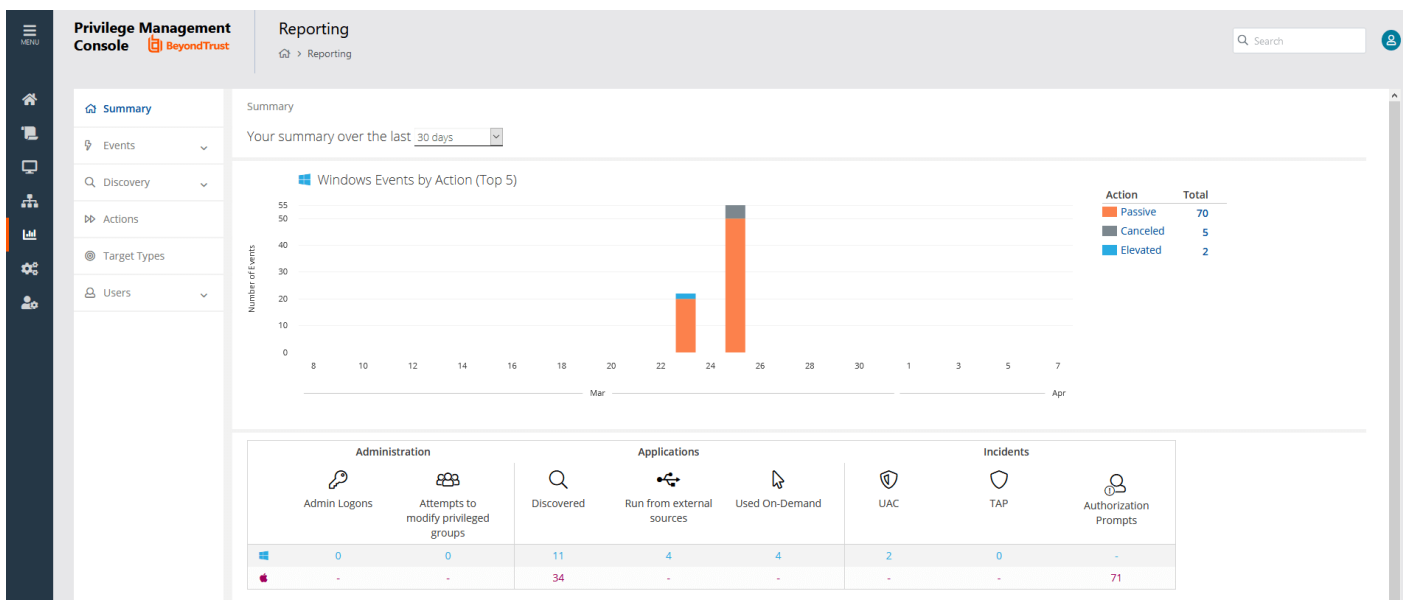
Name	Description
Time First Executed	This is the time range over which the application was first executed. Filter options: <ul style="list-style-type: none"> <li>• 24 Hours</li> <li>• 7 Days</li> <li>• 30 Days</li> <li>• 6 Months</li> <li>• 12 Months</li> </ul>
Time First Reported	This is the time range filtered by the date the application was first entered into the database. Filter options: <ul style="list-style-type: none"> <li>• 24 Hours</li> <li>• 7 Days</li> <li>• 30 Days</li> <li>• 6 Months</li> <li>• 12 Months</li> </ul>
Time Range	This is the time range that the actions are displayed over. Filter options: <ul style="list-style-type: none"> <li>• 24 Hours</li> <li>• 7 Days</li> <li>• 30 Days</li> <li>• 6 Months</li> <li>• 12 Months</li> </ul>
Token Type	The type of Privilege Management for Windows token that was applied to the trusted application protection event. Filter options: <ul style="list-style-type: none"> <li>• All</li> <li>• Blocked</li> <li>• Passive</li> <li>• Canceled</li> </ul>
Trusted Application Name	The trusted application that triggered the event.
Trusted Application Version	The trusted application version number.
Trusted File Owner	Whether the file owner of the target file is considered trusted. To be a trusted owner the user must be in one of the following Windows groups; TrustedInstaller, System, Administrator.
UAC Triggered	Whether or not Windows UAC was triggered.



Name	Description
	Filter option: <ul style="list-style-type: none"> <li>• Not Set</li> <li>• Triggered UAC</li> <li>• Did not trigger UAC</li> </ul>
Uninstall Action	The type of uninstall action. Filter options: <ul style="list-style-type: none"> <li>• Any</li> <li>• Change/Modify</li> <li>• Repair</li> <li>• Uninstall</li> </ul>
Upgrade Code	This field is used by Reporting. You do not need to edit it.
User Name	The user name of the user who triggered the event.
User Profiles Path	Sets the <b>User Profiles</b> path.
Workstyle	A dropdown of Workstyles in use.
Workstyle Name	The name of the Workstyle that contained the rule that matched the application.
Zone Identifier	The BeyondTrust Zone Identifier. This tag persists to allow you to filter on it even if the ADS tag applied by the browser is removed.

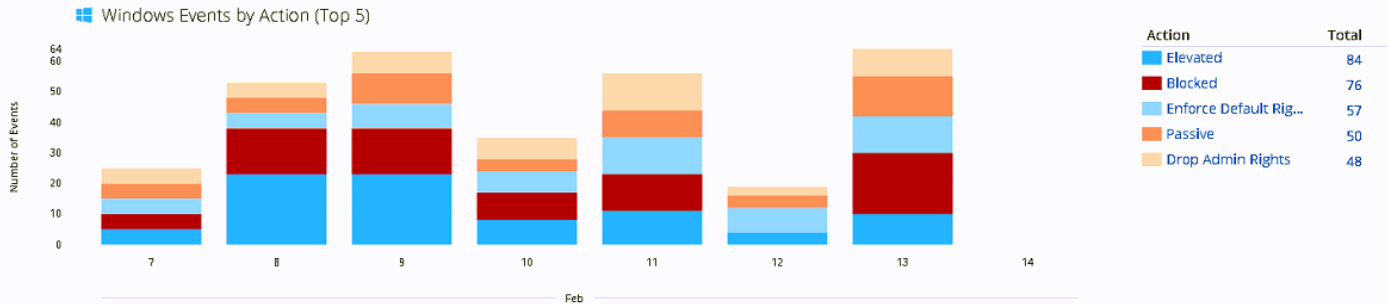
## Summary

The bar charts on the **Summary** dashboard summarize the most important activity that has occurred in the time period defined by the quick filter. The legends to the right of the bar charts display totals for the shown activities. Click on the legend or on a chart to show details of an action type. The **Administration**, **Applications**, and **Incidents** tables provide additional information to help inform Workstyle development or to show anomalous user behavior in your organization.



Summary

Your summary over the last



Administration		Applications		Incidents		
Admin Logons	Attempts to modify privileged groups	Discovered	Run from external sources	UAC	TAP	Authorization Prompts
8	3	143	7	32	5	-
-	-	20	-	-	-	4

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

Table	Description
Applications discovered	<p>The total number of newly discovered <b>Applications</b> split by the type of user rights required:</p> <ul style="list-style-type: none"> <li>Admin rights required</li> <li>Standard rights required</li> </ul> <p><b>Discovered</b> applications are shown in the <b>Applications</b> table. Click the number next to the OS icon to show details.</p>
Admin logons, by users, on endpoints	<p>Summarizes the number of admin logons, how many users carried them out, and how many endpoints were used.</p> <p><b>Admin Logons</b> are shown in the <b>Administration</b> table. Click the number next to the OS icon to show details.</p>
Applications run from external sources	<p>The number of applications that were run from external sources.</p> <p>Applications <b>Run from external sources</b> are shown in the <b>Applications</b> table. Click the number next to the OS icon to show details.</p>
Trusted Application Protection	<p>The number of Trusted Application (TAP) incidents, how many users, and how many endpoints were affected.</p> <p><b>TAP</b> events are shown in the <b>Incidents</b> table. Click the number next to the OS icon to show details.</p>

Table	Description
Attempts to modify privileged groups	The number of blocked attempts to modify privileged groups.  <b>Attempts to modify privileged groups</b> are shown in the <b>Administration</b> table. Click the number next to the OS icon to show details.
UAC matches	The number of applications that triggered User Account Control (UAC).  <b>UAC</b> events are shown in the <b>Incidents</b> table. Click the number next to the OS icon to show details.

## Discovery Reports in Privilege Management for Windows

This report displays information about applications that have been discovered by the reporting database for the first time. An application is first discovered when an event is received by the Reporting database.

This dashboard displays the following charts:

Chart	Information
Applications first reported over the last x months (number)	Grouped by: <ul style="list-style-type: none"> <li>Admin Rights Detected</li> <li>Admin Rights Not Detected</li> </ul>
Types of newly discovered applications	Grouped by: <ul style="list-style-type: none"> <li>Admin Rights Detected</li> <li>Admin Rights Not Detected</li> </ul>
New applications with admin rights detected (top 10 of <number>)	Clicking the <b>View All</b> link takes you to the <b>Discovery &gt; All</b> report with the <b>Admin Rights</b> filter applied.  Clicking an application takes you to the <b>Discovery &gt; All</b> report with the <b>Matched, Application Description</b> , and <b>Publisher</b> filters applied.
New applications with admin rights not detected (top 10 of <number>)	Clicking the <b>View All</b> link takes you to the <b>Discovery &gt; All</b> report with the <b>Admin Rights</b> filter applied.  Clicking an application takes you to the <b>Discovery &gt; All</b> report with the <b>Matched, Application Description</b> , and <b>Publisher</b> filters applied.
New applications with admin rights detected (by type)	Clicking the <b>View All</b> link takes you to the <b>Discovery &gt; All</b> report with the <b>Admin Rights</b> filter applied.  Clicking an application takes you to the <b>Discovery &gt; All</b> report with the <b>Admin Rights</b> and <b>Application Type</b> filters applied.
New applications with admin rights not detected (by type)	Clicking the <b>View All</b> link takes you to the <b>Discovery &gt; All</b> report with the <b>Admin Rights</b> filter applied.  Clicking an application takes you to the <b>Discovery &gt; All</b> report with the <b>Admin Rights</b> and <b>Application Type</b> filters applied.

## "Discovery by Path" Report in Privilege Management for Windows

This table displays all distinct applications installed within certain locations that have been discovered during the specified time frame.

For Windows the locations are:

- System: **C:\Windows\**
- Program Files: **C:\Program Files\,C:\Program Files (x86)\**
- User Profiles: **C:\Users**

For macOS the locations are:

- User Profiles: **/Users/%**
- Applications: **/Applications/%,/usr/%**
- Operating System Areas: **/System%/,/bin%/,/sbin/%**



**Note:** The paths can be altered using the filter panel.

### New applications, by path, first reported over the last <time period>

This table groups the applications by path. You can click the plus icon to expand the path to show each individual application. You can view additional information about the application, their type, version, and the number of users using them. You can click the description to see in depth information about the application.

## "Discovery by Publisher" Report in Privilege Management for Windows

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

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

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

### New applications, by publisher, first reported over the last <time period>

This table groups the applications by publisher. You can click the plus icon to expand the path to show each individual application. You can view additional information about the application, their type, version, and the number of users using them. You can click the description to see in depth information about the application.

### "Discovery by Type" Report in Privilege Management for Windows

This table displays applications that have been broken down by type. Where there is more than one application per type, the + symbol allows you to expand the entry to examine each application.

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

- **Type:** The type of applications
- **# Users:** The number of users
- **Median # processes/user:** The median number of processes per user
- **# Hosts:** The number of hosts
- **# Processes:** The number of processes
- **# Applications:** The number of applications
- **Date first reported:** The date when the application was first entered into the database
- **Date first executed:** The first known date that the application was executed

### New applications, by publisher, first reported over the last <time period>

This table groups the applications by type. You can click the plus icon to expand the path to show each individual application. You can view additional information about the application, their type, version, and the number of users using them. You can click the description to see in depth information about the application.

### "Discovery Requiring Elevation" Report in Privilege Management for Windows

This table displays applications that have broken down by those requiring elevation. Where there is more than one application per description, the + symbol allows you to expand the entry to examine each application.

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

- **Description:** The description of a specific application
- **Publisher:** The publisher of the applications
- **Name:** The product name of a specific application
- **Type:** The type of application
- **Elevate Method:** The types of elevation used. Clicking this shows you the type of event(s)
- **Version:** The version number of a specific application
- **# Users:** The number of users
- **Median # processes/user:** The median number of processes per user
- **# Hosts:** The number of hosts
- **# Processes:** The number of processes
- **Date first reported:** The date when the application was first entered into the database
- **Date first executed:** The first known date that the application was executed

### New applications requiring elevation first reported over the last <time period>

This table groups the applications by type. You can click the plus icon to expand the path to show each individual application. You can view additional information about the application, their type, version, and the number of users using them. You can click the description to see in depth information about the application.

### "Discovery from External Sources" Report in Privilege Management for Windows

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

You can click on the link in the **Description** column to see more detailed information on the application, including the actions over the last 30 days split by the type of token, the top 10 users, the top 10 hosts, the run method, and the portion of those discoveries where admin rights were detected.

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

- **Description:** The description of a specific application
- **Publisher:** The publisher of the applications
- **Name:** The product name of a specific application
- **Type:** The type of application
- **Source:** The source of the application
- **Version:** The version number of a specific application
- **# Users:** The number of users
- **Median # processes/user:** The median number of processes per user
- **# Hosts:** The number of hosts
- **# Processes:** The number of processes
- **Date first reported:** The date when the application was first entered into the database
- **Date first executed:** The first known date that the application was executed

### New applications from external sources first reported over the last <time period>

This table groups the applications by type. You can click the plus icon to expand the path to show each individual application. You can view additional information about the application, their type, version, and the number of users using them. You can click the description to see in depth information about the application.

### "Discovery All" Report in Privilege Management for Windows

This table lists all applications discovered in the time period, grouped by the application description. If multiple versions of the same application exist, they are grouped on the same line. These can be expanded by clicking on the plus (+) symbol in the **Version** column.

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

- **Description:** The description of a specific application
- **Publisher:** The publisher of the applications
- **Name:** The product name of a specific application
- **Type:** The type of application
- **Version:** The version number of a specific application

- **# Users:** The number of users
- **Median # processes/user:** The median number of processes per user
- **# Hosts:** The number of hosts
- **# Processes:** The number of processes
- **Date first reported:** The date when the application was first entered into the database
- **Date first executed:** The first known date that the application was executed

You can click on the link in the **Description** column to see more detailed information on the application, including the actions over the last 30 days split by the type of token, the top 10 users, the top 10 hosts, the run method, and the portion of those discoveries where admin rights was detected.

## Actions Reports in Privilege Management for Windows

The following reports are available for Actions:

- Actions Elevated
- Actions Blocked
- Actions Passive
- Actions Canceled
- Actions Custom
- Actions Drop Admin Rights

### Actions Elevated

The **Actions Elevated** report breaks down the elevated application activity by target type.

This dashboard displays the following charts:

Chart	Information
Elevated activity over the last <time period>	The number of targets that were elevated for each time segment split by the type of action. Clicking on the chart takes you to the <b>Target Types &gt; All</b> report with the <b>Action, Target Type, Range Start Time, and Range End Time</b> filters applied.
Distinct elevated target count by target type	The number of targets that were elevated for the complete time period split by the type of action. Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action and Target Type</b> filters applied.
Top 10 elevated targets	The top ten targets that were elevated for the time period. Click the chart to go to the <b>Events &gt; All</b> report with the <b>Action, Ignore Admin Required Events, and Target Description</b> filters applied.

### Actions Blocked

The **Actions Blocked** dashboard breaks down the blocked application activity by target type.

This dashboard displays the following charts:

Chart	Information
Blocked activity action over the last <time period>	The number of targets that were blocked for each time segment split by the type of action.  Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action, Target Type, Range Start Time, and Range End Time</b> filters applied.
Distinct blocked action target count by target type	The number of targets that were blocked for the complete time period split by the type of action.  Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action and Target Type</b> filters applied.
Top 10 blocked action targets	The top ten targets that were blocked for the time period.  Click the chart to go to the <b>Events &gt; All</b> report with the <b>Action, Ignore Admin Required Events, and Target Description</b> filters applied.

### Actions Passive

The **Actions Passive** dashboard breaks down the passive application activity by target type.

This dashboard displays the following charts:

Chart	Information
Passive action activity over the last <time period>	The number of targets where a passive token was used for each time segment split by the type of action.  Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action, Target Type, Range Start Time, and Range End Time</b> filters applied.
Distinct passive activity action target count by target type	The number of targets where a passive token was used for the complete time period split by the type of action.  Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action and Target Type</b> filters applied.
Top 10 passive action targets	The top ten targets where a passive token was used for the time period.  Click the chart to go to the <b>Events &gt; All</b> report with the <b>Action, Ignore Admin Required Events, and Target Description</b> filters applied.

### Actions Canceled

The **Actions Canceled** dashboard breaks down the canceled application activity by target type.

This dashboard displays the following charts:

Chart	Information
Canceled activity action over the last <time period>	The number of targets that were canceled for each time segment split by the type of action.  Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action, Target Type, Range Start Time, and Range End Time</b> filters applied.
Distinct canceled action target count by target type	The number of targets that were canceled for the complete time period split by the type of action.  Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action and Target Type</b> filters applied.



Chart	Information
Top 10 canceled action targets	The top ten targets that were canceled for the time period.  Click the chart to go to the <b>Events &gt; All</b> report with the <b>Action, Ignore Admin Required Events,</b> and <b>Target Description</b> filters applied.

## Actions Custom

The **Actions Custom** report breaks down the custom application activity by the type of action.

This dashboard displays the following charts:

Chart	Information
Custom action activity over the last <time period>	The number of targets where a Custom Token was used for each time segment split by the type of action.  Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action, Target Type, Range Start Time,</b> and <b>Range End Time</b> filters applied.
Distinct custom action target count by target type	The number of targets where a Custom Token was used for the complete time period split by the type of action.  Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action</b> and <b>Target Type</b> filters applied.
Top 10 custom action targets	The top ten targets where a Custom Token was used for the time period.  Click the chart to go to the <b>Events &gt; All</b> report with the <b>Action, Ignore Admin Required Events,</b> and <b>Target Description</b> filters applied.

## Actions Drop Admin Rights

The **Actions Drop Admin Rights** dashboard breaks down the drop admin application activity by target type.

This dashboard displays the following charts:

Chart	Information
Drop admin rights action activity over the last <time period>	The number of targets where a drop admin rights token was used for each time segment split by the type of action.  Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action, Target Type, Range Start Time,</b> and <b>Range End Time</b> filters applied.
Distinct drop admin rights action target count by target type	The number of targets where a drop admin rights token was used for the complete time period split by the type of action.  Click the chart to go to the <b>Target Types &gt; All</b> report with the <b>Action</b> and <b>Target Type</b> filters applied.
Top 10 targets drop admin rights action targets	The top ten targets where a drop admin rights token was used for the time period.  Click the chart to go to the <b>Events &gt; All</b> report with the <b>Action, Ignore Admin Required Events,</b> and <b>Target Description</b> filters applied.

## "Target Types All" Report in Privilege Management for Windows

This table lists all applications active in the time period, grouped by the application description ordered by user count descending.

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

- **Description:** The description of a specific application
- **Platform:** The platform that the events came from
- **Publisher:** The publisher of a specific application
- **Product Name:** The product name of a specific application
- **Application Type:** The type of application
- **Product Version:** The version number of a specific application
- **# Process Count:** The number of processes
- **# User Count:** The number of users
- **# Host Count:** The number of hosts

You can click **Description** to view additional information about the target, its actions over the time period, the top 10 users, top 10 hosts, the type of run method, and whether admin rights were detected.

## "Trusted Application Protection" Report in Privilege Management for Windows

This report shows information about TAP incidents. A TAP incident is a child process of a trusted application that is blocked, due to a Trusted Application policy or a DLL that is blocked from being loaded by a trusted application because it doesn't have a trusted owner or trusted publisher.



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

Chart	Description
All Trusted Application Protection incidents over the time period	A stacked bar chart showing the number of the different incidents broken down by the trusted application.
Trusted Application Protection incidents, by application	A table listing each trusted application, the number of TAP incidents, the number of targets, the number of users, and the number of hosts affected.
Top 10 targets	<p>The top 10 targets for TAP incidents.</p> <p>Clicking the target name shows you more information about the target including its actions over the time period.</p> <p>Clicking on <b>Users</b> shows you more information about the users.</p> <p>Clicking on <b>Host</b> shows you more information about the host.</p> <p>Clicking on <b>Incidents</b> takes you to the <b>Process Detail</b> report with the <b>Distinct App ID</b> filter applied.</p>

## "User" Reports in Privilege Management for Windows

The following reports are available for users.

## User Experience

The report shows how users have interacted with messages, challenge/response dialog boxes, and the Shell (on-demand) menu.

Chart	Description
User Experience over the time period	<p>A chart showing the percentage of users that experienced each interaction type filtered by the specified time period.</p> <p>Click the chart to display a list of users presented with that interaction.</p>
Message Distribution	<p>A chart showing how many users are in the defined categories of messages per time period.</p> <p>Click the chart to display a list of users in that category.</p>
Messages per action type	<p>A table showing message types displayed for <b>Allowed</b> and <b>Blocked</b> actions.</p> <p>Click the <b>Prompts</b>, <b>Notifications</b>, or <b>None</b> counts in the table to open the <b>Events All</b> report with the <b>Action</b> and <b>Message Type</b> filters applied.</p>



For more information, please see *"Events All" Report in Privilege Management for Windows* on page 133.

## Users Privileged Logons

The **Privileged Logon** report shows you how many accounts with standard user rights, power user rights, and administrator rights have generated logon events broken down over the specified time frame.

This dashboard displays the following charts:

Chart	Information
Privileged logons over the last <time period>	<p>A chart and table showing the number of logons by the different account types over time.</p> <p>Click the chart for more information about each privileged logon with the <b>Range Start Time</b>, <b>Range End Time</b>, <b>Show Administrator Logons</b>, and <b>Show Standard User Logons</b> filters applied.</p>
Administrators, Power Users, and Standard Users table	<p>This table shows you the number of logon events made by administrators, power users, and standard users, as well as how many users logged in.</p>
Logons by account privileged	<p>A chart showing the total number of logons, broken down by logon privilege.</p> <p>Click the chart for more information about the user logons for the time period with the <b>Show Administrator Logons</b>, <b>Show Standard User Logons</b>, and <b>Show PowerUser Logons</b> filters applied.</p>
Logons by account type	<p>A chart showing the total number of logons, broken down by domain accounts and local accounts.</p> <p>Click the chart for more information about the user logons for the time period with the <b>Account Authority</b>, <b>Show Administrator Logons</b>, <b>Show Standard User Logons</b>, and <b>Show PowerUser Logons</b> filters applied.</p>

Chart	Information
Top 10 logons by chassis type	<p>A chart showing the total number of logons, broken down by the top 10 chassis types.</p> <p>Click the chart for more information about the user logons for the time period with the <b>Show Administrator Logons</b>, <b>Show Standard User Logons</b>, and <b>Show PowerUser Logons</b> filters applied.</p>
Top 10 logons by operating system	<p>A chart showing the total number of logons, broken down the top 10 host operating systems.</p> <p>Click the chart for more information about the user logons for the time period with the <b>Show Administrator Logons</b>, <b>Show Standard User Logons</b>, <b>OS</b>, and <b>Show PowerUser Logons</b> filters applied.</p>
Top 10 accounts with admin rights	<p>A chart showing the top 10 accounts with admin rights that have logged into the most host machines.</p> <p>Click the chart for more information about the user logons for the time period with the <b>Show Administrator Logons</b>, <b>Show Standard User Logons</b>, <b>User Name</b>, and <b>Show PowerUser Logons</b> filters applied.</p>
Top 10 hosts with admin rights	<p>A chart showing the top 10 host machines that have been logged onto by the most users with admin rights.</p> <p>Click the chart for more information about the user logons for the time period with the <b>Host Name</b>, <b>Show Administrator Logons</b>, <b>Show Standard User Logons</b>, and <b>Show PowerUser Logons</b> filters applied.</p>

## Users Privileged Account Management

The **Privileged Account Management** report shows any blocked attempts to modify privileged accounts over the specified time interval.

Chart	Description
Privileged Account Management over the last <time period>	A chart breaking down the privileged account management events and the number of events.
Activity table	A table showing the number of <b>Users blocked</b> , <b>Hosts blocked</b> , <b>Applications blocked</b> , and the <b>Total number of block events</b> within the specified time frame.
By Privileged Group	The same data grouped by type of account. Click the account type to go to detailed information about the account and hosts with the <b>Group Name</b> filter applied.
By application	<p>A chart showing the privileged account modification activity that was blocked, broken down by the description of the application used.</p> <p>Click the chart to go to a more detailed view of that privileged account management activity for that application with the <b>Application Description</b> filter applied.</p>
Top 10 users attempting account modifications	<p>A chart showing the top 10 users who attempted modifications.</p> <p>Click the chart to go to a more detailed view of the privileged account management account modifications with the <b>Application User Name</b> filter applied.</p>
Top 10 hosts attempting account modifications	<p>A chart showing the top 10 hosts attempting privileged account modifications.</p> <p>Click the chart to go to a more detailed view of that privileged account management account modifications with the <b>Host Name</b> filter applied.</p>

## "Events" Reports in Privilege Management for Windows

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

Chart	Description
Events over the last <time period>	A column chart showing the number of the different event types, broken down by the time period. Clicking the chart takes you to the <b>Events &gt; All</b> report with the <b>Event Category</b> , <b>Range Start Time</b> , and <b>Range End Time</b> filters applied.
Event Types	A chart showing how many events have been received, broken down by the event type. Clicking the chart takes you to the <b>Events &gt; All</b> report with the <b>Event Number</b> filter applied.
By Category	A chart breaking down the events received, split by category. Clicking the chart takes you to the <b>Events &gt; All</b> report with the <b>Event Category</b> filter applied.
Time since last endpoint event	A chart showing the number of endpoints in each time group since the last event category. Clicking the chart takes you to more detailed information about the host.

## "Events All" Report in Privilege Management for Windows

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

- **Event Time:** The time of the event
- **Reputation:** The reputation of the event, where applicable
- **Platform:** The platform that the event came from
- **Description:** The description of the event
- **User Name:** The user name of the user who triggered the event
- **Host Name:** The host name where the event was triggered
- **Event Type:** The type of event
- **Workstyle:** The Workstyle containing the rule that triggered the event
- **Event Category:** The category of the event
- **Elevation Method:** The method of elevation
- **Authorization Source:** The authorization source for a user's credentials.

You can click some of the column data to review additional information on that event.

### Add to Policy

**Add to Policy** allows you to add applications to specific Application Groups in your policy.



**Note:** If you are using ePO server 5.10, the policy approval workflow is enabled, and you are logged in with a user who doesn't have the permission to approve policies, the **Add and Save** functionality for **Add to Policy** is disabled. You can **Add and Edit** and then click **Submit for Review** in this instance.

The following application types and event types are not supported in the **Events > All** report:

- Application Types
  - Content application types
  - DLL application types
  - URL application types
  - Uninstaller application types
- Event Types
  - Logon types
  - Privileged Account Management types
  - Host (Privilege Management service) types

To add applications from events to your policy:

1. Click the gray check mark in the first column next to the row(s) you want to import applications from and click **Add to Policy**.
2. If you have selected any unsupported application types or event types, these are displayed and grouped by application type or event type.



**Note:** Application types of **Uninstaller** are not supported. These cannot be determined by the **Events > All** report at this stage. If you have selected any **Uninstaller** application types, you are notified at the end of the process that the applications couldn't be added to your policy.

3. Click **Continue** to acknowledge the application types and event types that won't be added to your policy. A list of your policies and associated Application Groups is displayed. Select the policy and Application Group that you want to add them to.
4. Click **Add and Save** to add them to your policy. You will receive a confirmation when this has been completed. Click **Add and Edit** to add them to your policy and subsequently open the **Policy Catalog**. The highlighted lines are the ones you just added to your policy.

The information extracted from the application type or event type is determined by what is available in the event and the most commonly used matching criteria for that application type.



**Note:** If you receive a message stating your policy is locked, ensure you don't have more than one instance of ePO server open and no other users are accessing the policy.

## Export to CSV

This exports all the events into a Comma Separated Value (CSV) file.

## "Process Detail" Report in Privilege Management for Windows

This report gives details about a specific process control event. Only processes that match rules in Workstyles are displayed.

There is an **Advanced** view available with this report which is available from the **Filters** dropdown. The **Advanced** view shows you the full set of columns available in the database.

- **Start Time:** The start time of the event.
- **Platform:** The platform that the events came from.
- **Description:** The description of a specific application.

- **Publisher:** The publisher of a specific application.
- **Application Type:** The type of application.
- **File Name:** The name of the file where applicable.
- **Command Line:** The command line path of the file if applicable.
- **Product Name:** The product name where applicable.
- **Trusted Application Name:** The name of the trusted application.
- **Trusted Application Version:** The version of the trusted application.
- **Product Version:** The version of the product of applicable.
- **Group Policy Object:** The Group Policy object, if applicable.
- **Workstyle:** The Workstyle containing the rule that triggered the event.
- **Message:** Any message associated with the event.
- **Action:** Any action associated with the event.
- **Application Group:** The Application Group that the application that triggered the event belongs to.
- **PID:** The operating system process identifier.
- **Parent PID:** The operating system process identifier of the parent process.
- **Parent Process File Name:** The name of the parent process.
- **Shell/Auto:** Whether the process was launched using the shell **Run with Privilege Management** option or by normal means (opening an application).
- **UAC Triggered:** Whether or not Windows UAC was triggered.
- **Admin Rights Detected:** Whether or not admin rights was detected.
- **User Name:** The user name that triggered the event.
- **Host Name:** The host name where the event was triggered.
- **Rule Script File Name:** The name of the Rule Script (Power Rule) that ran.
- **Rule Script Affected Rule:** True when the Rule Script (Power Rule) changed one or more of the Default Privilege Management for Windows rule.
- **User Reason:** The reason given by the user if applicable.
- **COM Display Name:** The display name of the COM if applicable.
- **Source URL:** The source URL if applicable.

## Add to Policy

**Add to Policy** allows you to add application types to specific Application Groups in your policy. The following application types are not supported in the **Process Details** report:

- Application Types
  - DLL application types
  - Uninstall application types

To add applications from events to your policy:

1. Click the gray check mark in the first column next to the row(s) you want to import applications from and click **Add to Policy**.
2. If you have selected any application types that are unsupported, these are displayed and grouped by application type or event type.



**Note:** Application types of **Uninstaller** are not supported. These cannot be determined by the **Events > All** report at this stage. If you have selected any **Uninstaller** application types, you are notified at the end of the process that the applications couldn't be added to your policy.

3. Click **Add and Save** to add them to your policy. You receive a confirmation when this completes. Click **Add and Edit** to add them to your policy and subsequently open the **Policy Catalog**. The highlighted lines are the ones you just added to your policy.

The information that is extracted from the application type is determined by what is available in the event and the most commonly used matching criteria for that application type.



**Note:** If you receive a message stating your policy is locked, ensure you don't have more than one instance of ePO server open and that no other users are accessing the policy.

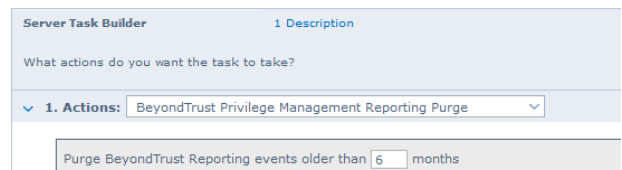
### Export to CSV

This exports all the events into a Comma Separated Value (CSV) file.

### Purge Reporting Events at Scheduled Interval

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

1. Select **Menu > Server Tasks** and select **New Task**.
2. On the **Description** page, enter an appropriate name (**BeyondTrust PMR Purge**, for example), and then click **Next**.
3. On the **Actions** page, from the **Actions** dropdown menu, scroll up and select **BeyondTrust Privilege Management Reporting Purge**.



The screenshot shows the 'Server Task Builder' interface. At the top, it says 'Server Task Builder' and '1 Description'. Below that, it asks 'What actions do you want the task to take?'. Under '1. Actions:', there is a dropdown menu with 'BeyondTrust Privilege Management Reporting Purge' selected. Below the dropdown, there is a text input field with the text 'Purge BeyondTrust Reporting events older than' followed by a small input box containing the number '6' and the word 'months'.

4. Choose the number of months to purge events older than.
5. On the **Schedule** page, adjust the options to suit your requirements and click **Next**.
6. Select **Save** from the **Summary** page.

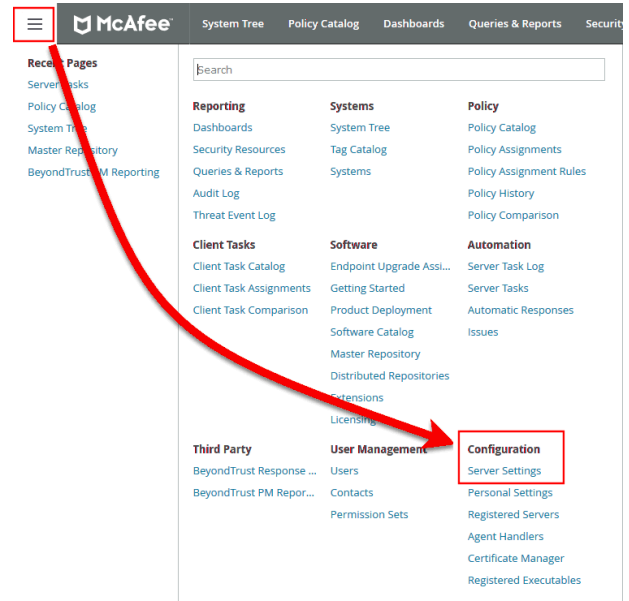


## Configure Reputation Settings in ePO

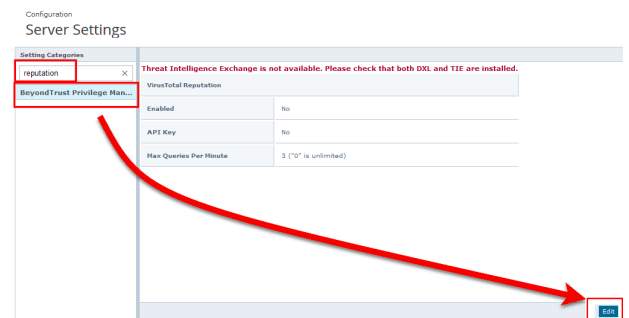
Reputation Settings can be seen in ePO only when this setting has been configured to one or more reputation providers.

To configure Intel Security's Reputation feature:

1. Select **Menu > Configuration > Server Settings**.



2. You can filter the list by typing in a search string. In this case, type **reputation**. The **Reputation** settings are displayed to the right.



3. Click **Edit** to change the options.



**Note:** Threat Intelligence Exchange (TIE) via the Data Exchange Layer (DXL) and VirusTotal are supported.

Use the option buttons to enable the reputation sources you were working with. If the required DXL extensions are not installed, then a warning message is displayed, indicating that TIE is not available.



**Note:** If using a public (non-commercial) VirusTotal key, the rate of queries is limited to four per minute. These keys should only be used for evaluation. API keys are available to purchase directly from VirusTotal.

TIE does not have this restriction, so we recommend using 0 for an unlimited query rate.

## Windows Policy Configuration Precedence

Privilege Management for Windows supports a variety of deployment methods, and accepts multiple simultaneous configurations from any combination of the following:

- **McAfee ePO Policy:** A configuration that is stored within McAfee ePO, configured using the Privilege Management for Windows ePO Extension in the ePO Policy Catalog.
- **Webservice Policy:** A configuration that is served from an iC3 webservice using HTTPS.
- **Webserver Policy:** A configuration located on a web server, accessible using HTTP(s) or FTP.
- **Group Policy:** Configurations that are stored in Group Policy Objects, configured using Active Directory Group Policy (GPMC) and GPEdit (Local Group Policy). Group Policy based configurations are evaluated according to GPO precedence rules.
- **Local Policy:** A standalone configuration, which is stored locally and has been configured using the Privilege Management Management Console snap-in for the Microsoft Management Console.

Privilege Management for Windows uses the following default precedence to evaluate each configuration for matching rules:

**ePO > Webservice > Webserver > GPO > Local**

Configuration precedence settings can be configured either as part of the client installation, or using the Windows Registry once the client has been installed.

To modify the configuration precedence at installation, use one of the following command lines to install Privilege Management for Windows with a specific configuration precedence:

```
msiexec /i PrivilegeManagementForWindows_xx (XX).msi POLICYPRECEDENCE="EPO,WEBSERVICE,  
WEBSERVER,GPO,LOCAL"PrivilegeManagementForWindows_x(XX).exe /s /v"  
POLICYPRECEDENCE="\EPO,WEBSERVICE, WEBSERVER,GPO,LOCAL\""
```



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

To modify your configuration precedence using the Windows Registry, run **regedit.exe** with elevated privileges and an anti-tamper token disabled. Navigate to the following key and edit the string as required:

```
HKEY_LOCAL_MACHINE\Software\Avecto\Privilege Guard Client  
REG_SZ PolicyPrecedence = "EPO,WEBSERVICE,WEBSERVER,GPO,LOCAL"
```

Only deployment methods listed in the Privilege Management for Windows engineering key **PolicyEnabled** are applied, irrespective of the order listed in the **PolicyPrecedence** key. Both keys are located in the same place in the Windows registry.

## Privilege Management for Windows Application Templates

Privilege Management for Windows ships with some standard application templates to simplify the definition of applications that are part of the operating system, common ActiveX controls, and software updaters.

The standard application templates are split into categories:

- Privilege Management for Windows Utilities
- Browsers
- COM Classes for 3rd Party Software
- Com Classes for file, folder and drive operations
- COM Classes for general Windows operations
- COM Classes for security features and configurations
- COM Classes for software installation, uninstallation and updates
- COM Classes for network device settings, sharing options and configurations
- Common ActiveX controls
- Content Handler Untrusted
- Content Handlers
- Installers for common printer driver manufacturers
- Software updaters
- Tools and utilities for administrators and developers
- Windows 10 Default Apps
- Windows 7/8 and Windows Server 2008 R2 / 2012 / 2012 R2
- Windows 8.0 Default Apps
- Windows 8.1 Default Apps
- Windows Server 2008 R2

Each category then has a list of applications for that category. Picking an application causes the application or ActiveX control dialog boxes to be prepopulated with the appropriate information.

### Creating Custom Application Templates

On other Windows versions the application templates are stored in:

**%ALLUSERSPROFILE%\Avector\Privilege Guard Templates\**

The standard application templates are stored in a single file named **OSXTemplates.xml\WindowsTasks.xml**, and we strongly recommend that you do not change these templates.

Instead, you should create your own XML template files. Application templates are a set of Application Groups that have been exported from the Privilege Management Policy Editor as an XML file.

We recommend that you create templates on a computer that is not running Privilege Management for Windows, as you will rely on Privilege Management for Windows' standalone Policy Editor to create the application templates.

To run the Privilege Management Policy Editor in standalone mode:

1. Launch **mmc.exe**.
2. Select **File > Add/Remove Snap-in > Privilege Management Settings** and click **Add**, then **OK**.

The Privilege Management Policy Editor is now running in standalone mode and is not connected to a Group Policy Object (GPO). However, it saves any settings locally, and these are picked up by the client, if it has been installed.

To create a set of application templates, create some Application Groups and populate the Application Groups with applications. The Application Groups become the categories, and the applications in each Application Group are the list of applications for that category.

Once you have defined your application templates, export the settings to an XML file:

1. Select the **Privilege Management Settings** node.
2. Right-click and select **Export**.

The XML file that you export must be saved with a prefix of **OSX**, for example, **OSX\_My\_Templates.xml** or **Windows**, for example, **Windows\*.xml**.

To import an application template file back into the Policy Editor for editing:

1. Select the **Privilege Management Settings** node.
2. Right-click and click **Import**.
3. When prompted click **No** to overwrite the current Workstyles.

Remember to re-export your application templates once you've modified them.

The final step is to copy your application templates to the application templates directory on any machines where the Policy Editor is being used to create Privilege Management settings. The Policy Editor automatically loads all of the application templates in the application templates directory and merges them to create a single list of categories.

## Configure Remote Computer Browser

The Privilege Management Workstyle Editor allows you to browse computers on the network for executables, Windows services, and running processes, which you can add to Application Groups. This provides a convenient alternative to manual entry.

Remote computer browsing leverages Windows Remote Management (WinRM) and PowerShell, which must be configured on each target endpoint in advance of using the computer browser feature to access the remote computer.

WinRM and Powershell are components of the Windows Management Framework, and are part of Windows 7 and Windows Server 2008 R2. For older versions of Windows, the Windows Management Framework can be downloaded and installed as an optional update at:

<https://www.microsoft.com/en-us/download/details.aspx?id=54616>.

To configure the ePO Server:

Configure WinRM trusted hosts:

1. Open PowerShell (elevated).
2. Type:

```
winrm s winrm/config/client '@{TrustedHosts="<endpoint>"}
```

where **<endpoint>** should be replaced with the hostname or IPAddress of the network computer to be trusted (a wildcard (\*) can also be used), and press **Enter**.

To configure a network computer:

1. Verify that PS-Remoting is enabled:
  - Open PowerShell (elevated).
  - Type

```
Enable-PSRemoting
```

and then type **A** to accept all defaults (this can also be enabled via AD Group Policy).

2. Configure WinRM to allow remote connections:
  - In the same PowerShell window, type

```
winrm qc
```

and press **Enter**.

- Type

```
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

- Press **Enter**.

To test for a successful connection, run this command from the ePO server:

```
winrm identify -r:http://<endpoint>:5985 -u:<username> -p:<password>
```

where **<endpoint>** should be replaced with the hostname or IPAddress of the network computer, **<username>** and **<password>** replaced with administrator credentials on the network computer.

If the connection is unsuccessful:

Fix the local security policy to enable classic mode authentication for network logons.

1. Open Local Security Policy from **Control Panel > Administrative Tools**.
2. Navigate to **Local Policies > Security Options**.
3. Double-click **Network Access: Sharing and Security Model for local accounts**.
4. Set to **classic**.

Mixed environments:

1. Open PowerShell (elevated).
2. Type:

```
new-itemproperty -name LocalAccountTokenFilterPolicy -path  
`HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System -propertyType DWord -value 1
```

3. Press **Enter**.

## Environment Variables Supported in Application Definitions

Privilege Management for Windows supports the use of the following environment variables within file path and command line application definitions:

### System Variables

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

### User Variables

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

To use any of the environment variables above, enter the variable, including the % characters, into a file path or command line. Privilege Management for Windows expands the environment variable prior to attempting a file path or command line match.

## Supported Regular Expressions Syntax

Privilege Management for Windows can control applications at a granular level by using regular expression syntax. Privilege Management for Windows uses the ATL regular expression library **CAtIRegExp**. Below is a summary of the regular expression syntax used by this library.

Metacharacter	Meaning	Example
Any character except <code>[^\\$. ?*\+()</code>	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"
<code>\</code> (backslash)	Escape character: interpret the next character literally.	"a\b" matches "a+b"
<code>.</code> (dot)	Matches any single character.	"a.b" matches "aab", "abb" or "acb", etc.
<code>[]</code>	Indicates a character class. Matches any character inside the brackets (for example, <code>[abc]</code> matches "a", "b", and "c").	"[abc]" matches "a", "b", or "c"
<code>^</code> (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, <code>[^abc]</code> matches all characters except "a", "b", and "c").  If <code>^</code> is at the beginning of the regular expression, it matches the beginning of the input (for example, <code>^[abc]</code> will only match input that begins with "a", "b", or "c").	"[^abc]" matches all characters except "a", "b", and "c"
<code>-</code> (minus character)	In a character class, indicates a range of characters (for example, <code>[0-9]</code> matches any of the digits "0" through "9").	"[0-9]" matches any of the digits "0" through "9"
<code>?</code>	Indicates that the preceding expression is optional: it matches once or not at all (for example, <code>[0-9][0-9]?</code> matches "2" and "12").	"ab?c" matches "ac" or "abc"
<code>+</code>	Indicates that the preceding expression matches one or more times (for example, <code>[0-9]+</code> matches "1", "13", "666", and so on).	"ab+c" matches "abc" and "abbc", "abbbc", etc.
<code>*</code> (asterisk)	Indicates that the preceding expression matches zero or more times	"ab*c" matches "ac" and "abc", "abbc", etc.
<code> </code> (vertical pipe)	Alternation operator: separates two expressions, exactly one of which matches.	"a b" matches "a" or "b"
<code>??, +?, *?</code>	Non-greedy versions of <code>?</code> , <code>+</code> , and <code>*</code> . These match as little as possible, unlike the greedy versions which match as much as possible. Example: given the input " <code>&lt;abc&gt;&lt;def&gt;</code> ", <code>&lt;.*?&gt;</code> matches " <code>&lt;abc&gt;</code> " while <code>&lt;.*&gt;</code> matches " <code>&lt;abc&gt;&lt;def&gt;</code> ".	Given the input " <code>&lt;abc&gt;&lt;def&gt;</code> ", <code>&lt;.*?&gt;</code> matches " <code>&lt;abc&gt;</code> " while <code>&lt;.*&gt;</code> matches " <code>&lt;abc&gt;&lt;def&gt;</code> ".
<code>()</code>	Grouping operator. Example: <code>(\d+)*\d+</code> matches a list of numbers separated by commas (such as "1" or "1,23,456").	"(One) (Two)" matches "One" or "Two"
<code>{ }</code>	Indicates a match group. The actual text in the input that matches the expression inside the braces can be retrieved through the <code>CAtIRegMatchContext</code> object.	



Metacharacter	Meaning	Example
\	<p>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).</p> <p>If \ is followed by a number n, it matches the nth match group (starting from 0). Example: &lt;{.*?}&gt;.*?&lt;\0&gt; matches "&lt;head&gt;Contents&lt;/head&gt;".</p> <p>Note that in C++ string literals, two backslashes must be used: "\\+", "\\a", "&lt;{.*?}&gt;.*?&lt;\0&gt;".</p>	<{.*?}>.*?<\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"

## 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
```

## Privilege Management Built-in Groups

Privilege Management for Windows includes a number of built-in groups that may be used in any Application Rule or Content Rule. They provide a simple and convenient way of applying broad rules to applications and content, in particular when defining *catch-all* rules. Built-in groups also help to simplify your configurations by reducing the amount of groups.

Group	Criteria	Valid Types
Any Application	Matches any application that executed. Will also match any child applications.	Executables Control Panel Applets Installer Packages Management Consoles Windows Scripts PowerShell Scripts Batch Scripts Registry Scripts
Any Signed Application	Matches any application that executed which has been signed by a publisher. Will also match any child applications of signed applications.	Executables Control Panel Applets Installer Packages Management Consoles Windows Scripts PowerShell Scripts
Any Signed UAC Prompt	Matches any application that triggers a Windows UAC Prompt, which has been signed by a publisher. Will also match any child applications.	Executables Installer Packages COM Classes
Any UAC Prompt	Matches any application that triggers a Windows UAC prompt. Will also match any child applications.	Executables Installer Packages COM Classes

## Manage the Privilege Management Databases

### Use Privilege Management for Windows Events to Build Queries

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

Below is a table showing all event properties that are 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

Property	Description
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 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 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.
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 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 Privilege Management for Windows performed an action.

Property	Description
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	Privilege Management for Windows Event Log Event ID.
Policy Description	The description of the Privilege Management for Windows policy that matched the executed application.
Policy Name	The name of the Privilege Management for Windows 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.
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.

In addition to the event properties relating to Privilege Management for Windows, there are also a number of threat event properties set as part of a for Windows 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	McAfee ePO standardized Privilege Guard Event ID.
Threat Name	Internal name used to identify the type of action performed by Privilege Management for Windows : ADD_ADMIN SHELL_ADD_ADIM DROP_ADMIN PASSIVE DEFAULT_RIGHTS APPLICATION_RIGHTS CUSTOM PROCESS_BLOCKED



For more information, please see *"Events in Privilege Management for Windows"* on page 109.

## Database Sizing and Resource Consumption

### Data Retention

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

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

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.

In order to facilitate your decision making regarding retention time in the Privilege Management for Windows database, please refer to the following sections in our standard documentation:



- Description of the views of data exposed in Privilege Management Reporting.
- Description of the events audited by Privilege Management in the 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 Privilege Management Audit Events database.

**i** For more information, please see the following:

- [Reporting Dashboard Guide](http://www.beyondtrust.com/docs/privilege-management/windows.htm) at [www.beyondtrust.com/docs/privilege-management/windows.htm](http://www.beyondtrust.com/docs/privilege-management/windows.htm)
- "Events in Privilege Management for Windows" on page 109
- "Privilege Management for Windows Workstyle Parameters" on page 30

## 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:

$$10,000 \times 15 \times 5 \times 30 = 22,500,000\text{Kb, or } 21.5\text{Gb}$$

A typical event volume is 10-20 events per host per day and varies based on Privilege Management for Windows 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 that the Reporting Purge Utility be used 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. The Database Administration Dashboard allows the purging of audits related to specific applications and suppression of incoming audit items related to those applications.

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.



For more information, please see the [Reporting Dashboard Guide](http://www.beyondtrust.com/docs/privilege-management/windows.htm) at [www.beyondtrust.com/docs/privilege-management/windows.htm](http://www.beyondtrust.com/docs/privilege-management/windows.htm).

## McAfee ePO Privilege Management for Windows Database Events

Table Column Name	Description
AppGroupDescription	Description of the Privilege Management for Windows Application Group that matched the process referenced in the event.
AppGroupName	Name of the 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.

Table Column Name	Description
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 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 Privilege Management for Windows message that matched the process referenced in the event.
MessageName	Name of the 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.
ParentProcessGUID	Unique reference assigned by 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 Privilege Management for Windows policy that matched the process referenced in the event.
PolicyName	Name of the 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 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.

Table Column Name	Description
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 Privilege Management for Windows to the process referenced in the event.
TokenName	Name of the token applied by 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.



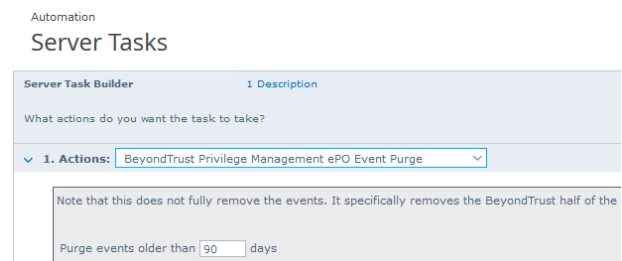
**Note:** No individual event returns values in all fields, so it is expected behavior to have NULL values in task specific columns.

## 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 Privilege Management ePO Event Purge** from the **Actions** dropdown menu.



The screenshot shows the 'Automation Server Tasks' interface. Under 'Server Task Builder', there is a '1 Description' section. Below it, the question 'What actions do you want the task to take?' is followed by a dropdown menu labeled '1. Actions:' which has 'BeyondTrust Privilege Management ePO Event Purge' selected. A note below states: 'Note that this does not fully remove the events. It specifically removes the BeyondTrust half of the'. At the bottom, there is a field 'Purge events older than' with the value '90' and the unit 'days'.

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

## McAfee ePO 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|forever]
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
```

**i** For more information, please refer to [Explanation of ePO Web API and where to find Web API documentation](https://kc.mcafee.com/corporate/index?page=content&id=KB81322), at <https://kc.mcafee.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)
response = mc.avecto.challengeResponse('key','test','98765432X','forever')
print 'response for forever - 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)
    response = mc.avecto.challengeResponse('name', 'NewSimpleCR', '98765432X', 'forever')
    print 'response for forever - 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)
    response = mc.avecto.challengeResponse('id', id, '98765432X', 'forever')
    print 'response for forever - 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 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 160
- "Application Types" on page 160
- "Chassis Types" on page 160
- "OS Version" on page 161
- "OS Product Type" on page 161
- "Message Types" on page 161
- "Certificate Modes" on page 162
- "Policy Audit Modes" on page 162
- "Device Types (Drive Type)" on page 162
- "ExportDefendpointStarts" on page 163
- "ExportLogons" on page 163
- "ExportPrivilegedAccountProtection" on page 164
- "ExportProcesses" on page 166

## 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	<b>Windows</b> or <b>macOS</b>



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



Chassis Type	Description
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

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

The Privilege Management ePO extension does not support the distribution of signed Privilege Management for Windows configuration. The 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.  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 <b>0</b> in endpoint registry.
4	Audit Errors Only	202 events. Value is <b>1</b> in endpoint registry.
6	Audit Warnings and Errors	201/202 events. Default for agent and console installations. Value is <b>2</b> in endpoint registry.
7	Audit Information, Warnings and Errors	200/201/202 events. Default for agent only installations. Value is <b>3</b> 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		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

Column_name	Type	Length	Index	Description	Example
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>

Column_name	Type	Length	Index	Description	Example
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
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

Column_name	Type	Length	Index	Description	Example
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	lusmgr.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

Column_name	Type	Length	Index	Description	Example
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
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

Column_name	Type	Length	Index	Description	Example
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		Windows 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>
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>



Column_name	Type	Length	Index	Description	Example
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 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>
MD5	nvarchar	32		MD5 hash of the app	6E641CAE42A2A7C89442AF99613FE6D6
TokenAssignmentGUID	uniqueidentifier			UUID of the token assignment in the policy	E7654321-BBBB-5AD2-B954-1234DDC7A89D

Column_name	Type	Length	Index	Description	Example
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
UserDomainNameNETBIOS	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
HostDomainNameNETBIOS	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>
AuthUserDomainNameNETBIOS	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
FileOwnerDomainNameNETBIOS	nvarchar	15		File Owner Domain NETBIOS	<None>

Column_name	Type	Length	Index	Description	Example
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	ADeIRCP 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\con29selectable 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
ContentOwnerDomainNameNetBIOS	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

Column_name	Type	Length	Index	Description	Example
RuleScriptResult	nvarchar	1024		Result of the script run	Script ran successfully
RuleScriptOutput	nvarchar	1024		The output of the script	
AuthorizationSource	nvarchar	200		The Authorizing User Credential Source	

## Troubleshoot Privilege Management for Windows

### Check 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 Privilege Management Management Console service. Ensure that this service is both present and started. The Privilege Management service is installed by Privilege Management for Windows and should start automatically.



**Note:** The Privilege Management service requires MSXML6 in order to load the 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 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 Privilege Management as an XML file in the following location:

```
%ProgramData%\Avecto\Privilege Guard\PO Cache\Machine\PrivilegeGuardConfig.xml
```

### Check that Privilege Management is Licensed

One of the most common reasons for Privilege Management not functioning is the omission of a valid license from the 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 Privilege Management settings that you create.

### Check Workstyle Precedence

Assuming that 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.

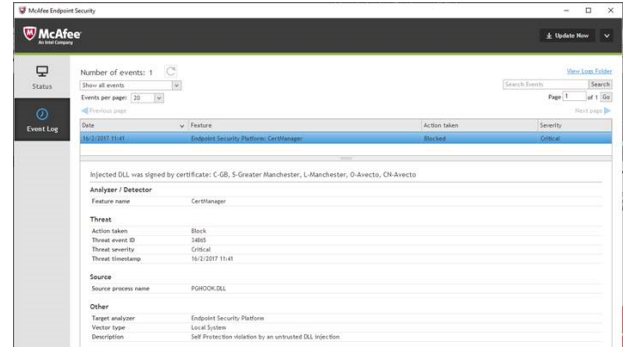
Once an application matches an Application Group entry in the **Application Rules** or the **On-Demand Application Rules**, then processing does not continue for that application. Therefore, it is vital that you order your entries correctly:

- 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 Privilege Management shell menu (if enabled).

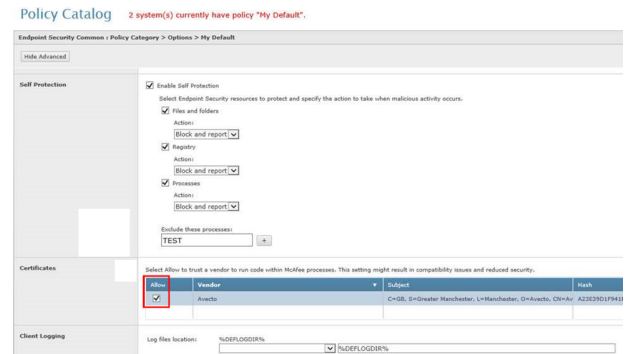
## Certificate Error in McAfee Endpoint Security (ENS)

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



### Add the Certificate for Privilege Management:

1. Navigate to **Policy Catalog** and select **McAfee 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.



3. Click **Save**.

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