Privilege Management for Mac
ePO Extension 23.10 Administration
Guide

Table of Contents

Privilege Management for Mac ePO Extension Administration

Privilege Management for Mac 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.

- **Achieve Least Privilege on Mac**: There are many functions that require an admin account to run. While most Mac users typically use an admin account to gain the flexibility they need, this represents a large security risk in the enterprise. Privilege Management for Mac allows users to log on with standard user accounts without compromising productivity or performance, by allowing the execution of approved tasks, applications and installations as required, according to the rules of your policy.

- **Empower Users and Gain Control**: Allow and block the use and installation of specific binaries, packages, and bundles. By taking a simple and pragmatic approach to allowlisting, you can gain greater control of applications in use across the business. This immediately improves security by preventing untrusted applications from executing.

- **Unlock Privileged Activity**: Even privileged applications and tasks that usually require admin rights are able to run under a standard user account. With Privilege Management for Mac, you can unlock approved system preferences such as date and time, printers, network settings, and power management without needing admin credentials.

- **Take a Pragmatic Approach with Broad Rules**: Broad catch-all rules provide a solid foundation, with exception handling options to handle unknown activity. Define the application and set its identification options such as filename, hash, publisher, or URI. Then assign the application to the users who require enhanced rights and set up any additional options, such as end user messaging and auditing.

- **Achieve Compliance**: You will have the knowledge to discover, monitor, and manage user activity from the entire enterprise, drawing upon actionable intelligence to make informed decisions. Graphical dashboards with real-time data provide a broad range of reports to aid troubleshooting and provide the information you need to proactively manage your policy on an ongoing basis.

- **Apply Corporate Branding**: You can add your own branding to messages and prompts, with reusable messaging templates that make it easy to improve the end user experience. You have control over text configuration.

- **Customizable Messaging**: Working seamlessly with macOS, Privilege Management for Mac can suppress standard, restrictive messages and allows you to create your own customized authorization prompts to handle exceptions and enable users to request access. Set up access request reasons, challenge and response codes, or password protection to add additional security layers, or simply improve prompts to reduce helpdesk inquiries.

- **Simple, Familiar Policy Design**: Firewall-style rules based on Application Groups make set up and management simple. Using the same Privilege Management interface and client as for Windows, you can create flexible **Workstyles** based on the requirements of individuals and groups of users.

About Trellix ePolicy Orchestrator

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

Only Trellix ePO offers:

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

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

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

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

Privilege Management for Mac and Trellix

Privilege Management for Mac is implemented as a server extension to Trellix ePolicy Orchestrator, enabling Workstyles to be managed through the ePO Policy Catalog. Granular auditing and reporting of Privilege Management for Mac 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 Mac audit data for reporting.

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

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

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

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

BeyondTrust Privilege Management App

Starting in version 23.10, we are updating and enhancing the policy editing and reporting experience for our Privilege Management for Windows and Mac solution deployed via Trellix ePolicy Orchestrator (ePO). This new experience will mean policy editing and reporting will happen outside of the ePO extension and will instead be delivered via a new Electron-based application called the BeyondTrust Privilege Management App, published by BeyondTrust.

> *For more information, please see:*
>
> - *BeyondTrustPrivilege Management App User Guide*
> - *BeyondTrustPrivilege Management App Frequently Asked Questions*

Install, Uninstall, and Upgrade Privilege Management for Mac

Install the Privilege Management for Mac Clients

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

ℹ️ *For more information on installing Privilege Management for Mac using ePO, please see the Privilege Management for Mac ePO Extension Installation Guide, at https://www.beyondtrust.com/docs/privilege-management/mac/index.htm.*

Uninstall the Privilege Management for Mac Clients

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

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

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

Uninstall the Privilege Management ePO Adapter

To uninstall the Privilege Management ePO Adapter locally on a Mac run the following command:

```
sudo /usr/local/libexec/avecto/ePOAdapter/1.0/uninstall_epo_adapter.sh
```

Uninstall Privilege Management and the Privilege Management ePO Adapter

To uninstall Privilege Management for Mac and the Mac ePO Adapter at the same time, run the following command:

```
sudo /usr/local/libexec/avecto/ePOAdapter/1.0/uninstall_epo_deployment.sh
```

Remove the Privilege Management Policy

To remove the policy after you uninstall Privilege Management for Mac, run the following command:

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

📌 *Note: Do not remove the Privilege Management for Mac policy unless you already uninstalled Privilege Management for Mac.*

ℹ️ *For more information on uninstalling Privilege Management for Mac using ePO, please see the Privilege Management ePO Extension Installation Guide at www.beyondtrust.com/docs/privilege-management/mac.htm.*

Upgrade Privilege Management for Mac

> 📌 **Note:** *ePO will not recognize Privilege Management for Mac if you upgrade the Privilege Management for Mac 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 Mac clients.

The recommended order to upgrade BeyondTrust Privilege Management for Mac 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.*

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.

> 📌 **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.

Upgrade Privilege Management for Mac Clients

You can upload a newer version of the Privilege Management for Mac 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 Mac client. You can use a later version of the Privilege Management ePO Extension with an earlier version of the Privilege Management for Mac client. However, not all features in the Privilege Management ePO Extension are supported with earlier versions of the client.

> ℹ️ *For more information, please see the Privilege Management for Mac Administration Guide, at https://www.beyondtrust.com/docs/privilege-management/mac/index.htm.*

Manual Upgrade for Privilege Management Reporting Database

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.
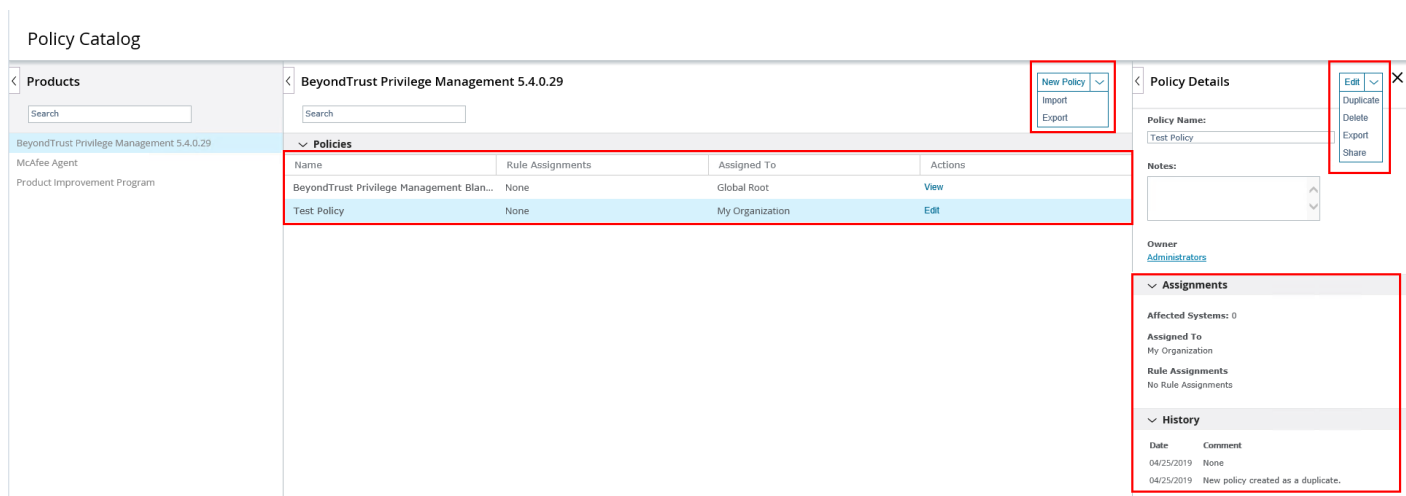
> *Example: If your current database version is **4.3.16** and you want to upgrade to version **5.0.0**, execute the following scripts in order:*
> 1. ***Script_4.5.0_Updates.sql***
> 2. ***Script_5.0.0_Updates.sql***

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

Launch the ePO Policy Catalog to View Policies

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

To view existing Privilege Management for Mac 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 Mac 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.

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

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

10

Access the Policy Summary Screen from the Policy Catalog

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

Privilege Management for Mac 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

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 Mac policies.

To enable the policy approval workflow, navigate to **Server Settings > Approvals** from the ePO server menu. Click **Edit** and then check the **User needs 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 Mac 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 Mac 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 Trellix policy approval process is not supported for Privilege Management for Mac policies. Click **Save** on the **Policy Summary** screen to save it.

> ℹ️ *For more information, please see Policy and Task approval feature with ePolicy Orchestrator 5.10.0 at https://kcm.trellix.com/corporate/index?page=content&id=KB90769.*

Apply Policy to Disconnected Users

Disconnected users are fully supported by Privilege Management for Mac. When receiving policies from Trellix ePO, Privilege Management for Mac 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 Trellix 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 polices.

> *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 Mac 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.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

15

Privilege Management Audits and Reports

The Privilege Management Trellix ePO Integration Pack includes a set of rich preconfigured dashboards, built in ePO Queries and Reports, which summarize Privilege Management for Mac event data collected from Trellix 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 Mac 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 at www.beyondtrust.com/docs/privilege-management/mac.htm.*

Privilege Management Dashboards in ePO

The Trellix 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 Mac dashboards from the **Dashboard** dropdown menu. These dashboards show Windows and macOS events.

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

BeyondTrust Privilege Management: Blocked

The **BeyondTrust Privilege Management: Blocked** dashboard contains all events raised by Privilege Management for Mac relating to applications that were blocked by Privilege Management for Mac 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 **BeyondTrustPrivilege Management: Elevated** dashboard contains all events raised by Privilege Management for Mac relating to applications that were elevated by Privilege Management for Mac 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.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

17

Privilege Management: Executed

The **BeyondTrust Privilege Management: Executed** dashboard contains all events raised by Privilege Management for Mac relating to applications that were allowed to execute under Privilege Management for Mac 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 Mac, relating to applications detected by Privilege Management for Mac, 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.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

18

Events in Privilege Management for macOS

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

The following events are logged by Privilege Management for Mac :

Mac Process Events

ePO ID (Event ID)	Description
202250 (100)	Process has started with admin rights added to token.
202256 (106)	Process has started with no change to the access token (passive mode).
202266 (116)	Process execution was blocked.
202270 (120)	Process execution was canceled by the user
203051 (130)	A bundle was installed.
203052 (131)	A bundle was deleted.

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 in Privilege Management

When an application is allowed, elevated, or blocked, Privilege Management for Mac 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.*

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

20

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.

> *For more information, please see the following:*
>
> - *Create the Reporting Event Staging Server Task in the ePO Installation Guide at https://www.beyondtrust.com/docs/privilege-management/mac/index.htm*
> - *Create the Enterprise Reporting Purge Server Task in the ePO Installation Guide at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm*
> - *"Create the Enterprise Reporting Purge Server Task" on page 23*

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

21

Create the Reporting Event Staging Server Task

The **Reporting Event Staging** server task takes report events from the ePO database and inserts them into the BeyondTrust 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**.
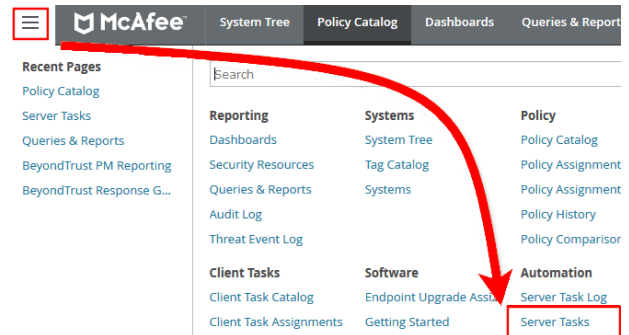
2. Enter an appropriate name (**BeyondTrust Event Staging**, for example), leave the **Schedule status** as **Enabled**, and click **Next**.

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**.

   - **Time in minutes to check for staging events**: The recommended value is 55 minutes.

   - **Number of events to transfer for each transaction (batch size)**: The default value is 1. Only increase the value if there is a lag in performance throughput between ePO to Privilege Management Reporting.

   - **Time in seconds to sleep when there are no events**: The recommended value is 60 seconds.

   - **Time in milliseconds to pause between reading each event**: The default and recommended value is 0.

   - **Time in minutes between polling the queue lengths**: The recommended value is 5 minutes.

   - **Verbose logging**: By default, verbose logging is turned off. Only use verbose logging when you need more details about the events being collected.
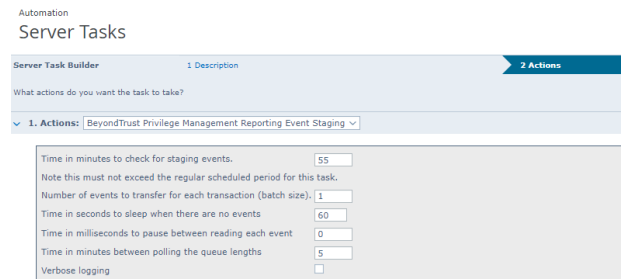
5. On the **Schedule** page, set the **Schedule type** to your preference.

6. Select the **Start date** and **End date** if required. By default, **No end date** is selected.

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

8. Select **Save** to finish creating the server task.

Create the Enterprise Reporting Purge Server Task

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

1. Navigate to **Menu > Automation > Server Tasks** and select **New Task**.
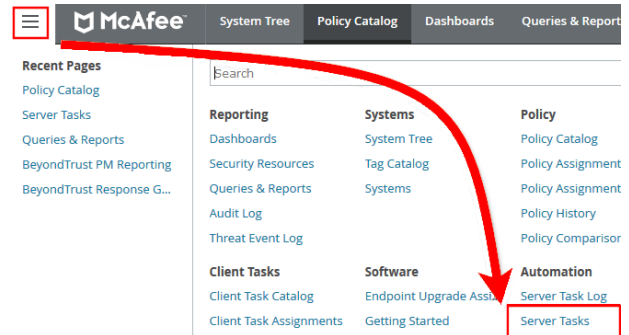
2. Enter an appropriate name (**BeyondTrust Purge**, for example), leave **Schedule status** as **Enabled**, and click **Next**.

3. Select **BeyondTrust Privilege Management Reporting Purge** from the **Actions** dropdown menu.

4. Choose the number of months to purge events older than.
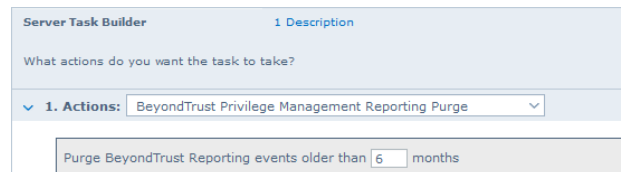
5. On the **Schedule** page set the **Schedule type** to your preference.

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.

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**.
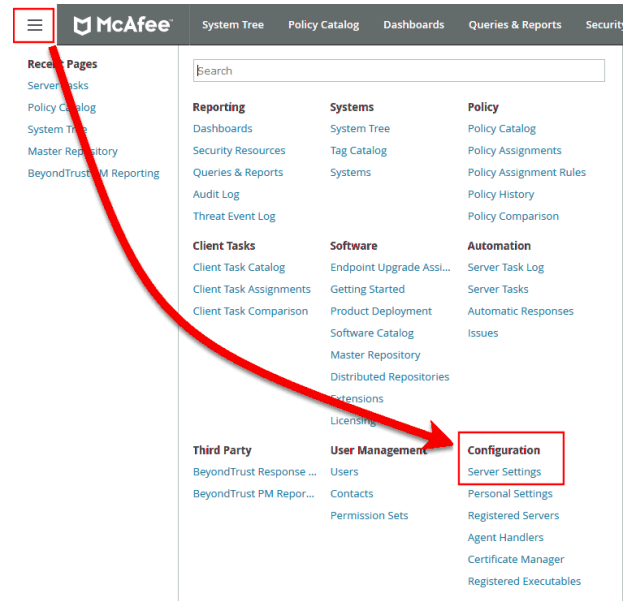
2. You can filter the list by typing in a search string. In this case, type **reputation**. The **Reputation** settings are displayed to the right.
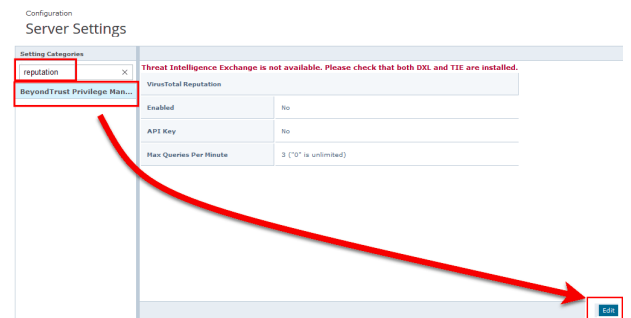
3. Click **Edit** to change the options.

> 📌 **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 ware 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.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

24

TC: 11/29/2023

Manage the Privilege Management Database

Use Events to Build Queries

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

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

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

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

Property	Description
Windows Store App Name	The common name of the Windows Store Application.
Windows Store App Publisher	The Display Name of the Publisher Certificate who signed the Windows Store Application.
Windows Store App Version	The version number of the Windows Store Application.

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

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

ℹ️ For more information, please see *"Events in Privilege Management for macOS" on page 19*.

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

27

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 audit event data must be retained, 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.*

To facilitate your decision making regarding retention time in the Privilege Management 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.

> *For more information, please see the following:*
>
> - *Reporting Dashboard Guide at www.beyondtrust.com/docs/privilege-management/mac.htm*
> - *"Events in Privilege Management for macOS" on page 19*

Database Sizes

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

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

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

> **Example:** An organization of 10,000 hosts, with each host generating an average of 15 events per day, requiring a 30 day retention would require a database capacity of:
>
> 10,000 × 15 × 5 × 30 = 22,500,000Kb, or 21.5Gb

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

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

Example Use Case Volumes

> **Example:** Based on an organization of 10,000 hosts requiring a 42 day (six weeks) retention.
>
> **Discovery:** Between 40 – 60 events per machine per day
>
> (4.6K per event (based on real world data))
>
> **Average total:** 67.06GB

> **Example: Production:** Between 2 – 10 events per machine per day
>
> (4.6K per event (based on real world data))
>
> **Average total:** 5.66GB

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

Key considerations

Volume of inbound audit event records

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

Queries triggered from MSFT SQL Reporting Services Reports

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

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

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

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

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

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

ePO Privilege Management Database Events

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

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

31

Table Column Name	Description
ParentProcessGUID	Unique reference assigned by Privilege Management for Mac 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 Mac policy that matched the process referenced in the event.
PolicyName	Name of the Privilege Management for Mac 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 Mac to the process referenced in the event.
ProcessStartTime	Time that the process referenced in the event started.
ProductCode	Product Code assigned to the process referenced in the event.
ProductDescription	Product Description assigned by the vendor to the process referenced in the event.
ProductName	Product Name assigned by the vendor to the process referenced in the event.
ProductVersion	Product Version assigned by the vendor to the process referenced in the event.
Publisher	Digital signature assigned by the vendor to the process referenced in the event.
Reason	Details of the reason provided by the user for using the process referenced in the event.
ServiceDisplayName	The Display name of the Windows service referenced in the event.
ServiceName	The Service name of the Windows service referenced in the event.
SourceURL	If available, the URL from which the process referenced in the event was downloaded.
TokenAssignmentIsShell	Binary flag to indicate if the process was launched using the shell integration feature.
TokenDescription	Description of the token applied by Privilege Management for Mac to the process referenced in the event.
TokenName	Name of the token applied by Privilege Management for Mac 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.
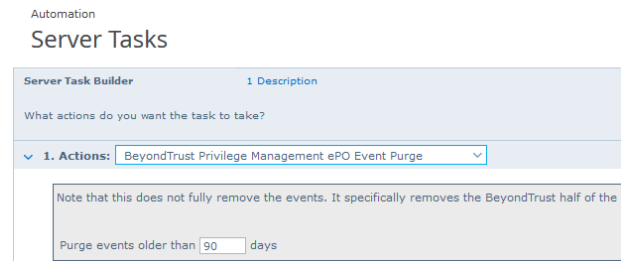
> **Note:** *No individual event returns values in all fields, so it is expected behavior to have NULL values in task specific columns.*

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.

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

ePolicy Orchestrator Server Scripts

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

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

Parameter Descriptions

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

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

Referenced Libraries

Two libraries are referenced in these scripts:

- McAfee python Support Library
- URL Encoder Support Library

Challenge Response Scripting

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

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

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

34

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

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

ePO Create Policy

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

ePO Import Policy

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

ePO Export Policy

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

Exported Views in Privilege Management for Mac

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:

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

37

TC: 11/29/2023

Custom Data Types

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

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

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

38

TC: 11/29/2023

Application Types

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

Chassis Types

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

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

40

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

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

42

Message Types

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

Certificate Modes

Privilege Management for Mac verifies that an optionally signed Privilege Management for Mac 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 Mac 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 Mac 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.

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

44

TC: 11/29/2023

Policy Audit Modes

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

Device Types (Drive Type)

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

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

46

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
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

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

48

ExportPrivilegedAccountProtection

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

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

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

50

TC: 11/29/2023

ExportProcesses

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

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

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

Column_name	Type	Length	Index	Description	Example
MD5	nvarchar	32		MD5 hash of the app	6E641CAE42A2A7C89442AF99613FE6D6
TokenAssignmentGUID	uniqueidentifier			UUID of the token assignment in the policy	E7654321-BBBB-5AD2-B954-1234DDC7A89D
TokenAssignmentIsShell	bit			Token assignment is for shell	1
UserSID	nvarchar	200		User SID	S-1-21-123456789-123456789-16357176381125883508
UserName	nvarchar	1024		User Name	EGUser18
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserDomainNameNETBIOS	nvarchar	15		User Domain NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Laptop
HostSID	nvarchar	200		Host SID	S-1-21-123456789-123456789-16357717638775838649
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

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

Column_name	Type	Length	Index	Description	Example
ContentOwnerName	nvarchar	1024		Content Owner	EGUser1
ContentOwnerDomainSID	nvarchar	200		Content Owner Domain SID	S-1-5-21-2217285736-120021366-3854014904
ContentOwnerDomainName	nvarchar	1024		Content Owner Domain	BEYONDTRUST TEST58\BEYONDTRUSTTEST58.QA
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
RuleScriptResult	nvarchar	1024		Result of the script run	Script ran successfully
RuleScriptOutput	nvarchar	1024		The output of the script	

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

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

57

Troubleshoot Privilege Management for Mac

Check Privilege Management for Mac is installed and functioning

You can confirm whether Privilege Management for Mac is running by checking the Activity Monitor for the following processes:

- **Defendpoint**
- **defendpointd**
- **dppolicyserverd**

Check Settings are Deployed

Assuming Privilege Management for Mac 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\ePO 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).

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

58

Certificate Error in Trellix Endpoint Security (ENS)

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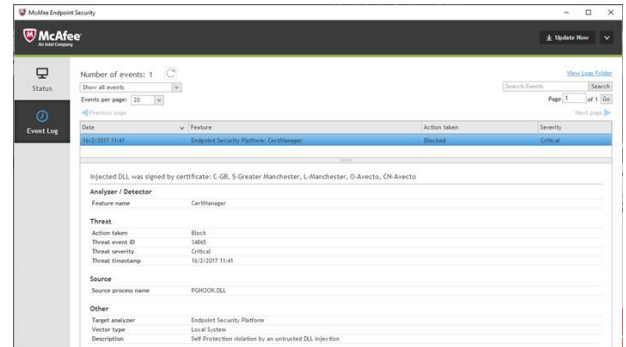
Add the Certificate for Privilege Management:

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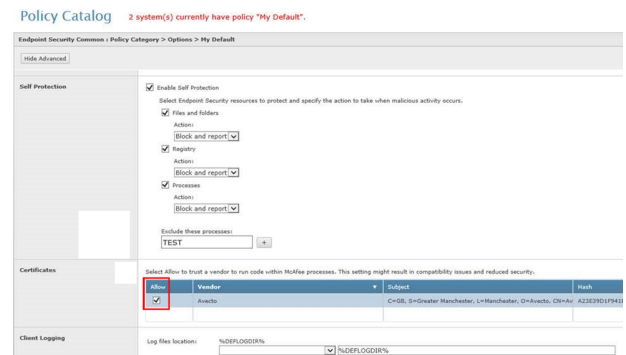
3. Click **Save**.

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

Third Party License Information

We use the following 3rd party software:

- Qt
- Sudo
- SQLite Framework
- Rootfool

Sudo Copyright Notice

Sudo is distributed under the following license:

Copyright (c) 1994-1996, 1998-2017

Todd C. Miller <Todd.Miller@courtesan.com>

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sponsored in part by the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory, Air Force Materiel Command, USAF, under agreement number F39502-99-1-0512.

Rootfool Copyright Notice

RootFool GUI (read ROTFL)

Created by Pedro Vilaça on 06/10/15.

pedro@sentinelone.com - https://www.sentinelone.com

reverser@put.as - https://reverse.put.as

Copyright (c) 2015 Sentinel One. All rights reserved.

kernelControl.m

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

60

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

61