BeyondTrust

Privilege Management for Mac ePO Extension 22.7 Administration Guide

TC:2/2/2023

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.*

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.

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.*

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.

Upgrade Privilege Management Reporting (if in use)

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

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

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

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

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

   Subsequently, query the following tables:

   - dbo.StagingTemp
   - dbo.StagingTemp_ServiceStart

- dbo.StagingTemp_ServiceStop
- dbo.StagingTemp_UserLogon

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

2. Disable the **Copy from Staging** task. The easiest way to do this is to use **SQL Server Management Studio** and navigate to **Reporting database > Service Broker > Queues**.
3. Right-click 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 Mac database installer to upgrade the database. Ensure you point the installer to the existing database server and Privilege Management for Mac 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 **Trellix ePolicy Orchestrator Event Parser Service** service. Any incoming events can now be processed.
11. You need to log off and on again to the ePO server to ensure the new database version is recognized. However, an ePO server restart is not required.

Note: *If you 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 Upgrade for Privilege Management Reporting Database" on page 14 for more information.

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.

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

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 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.*

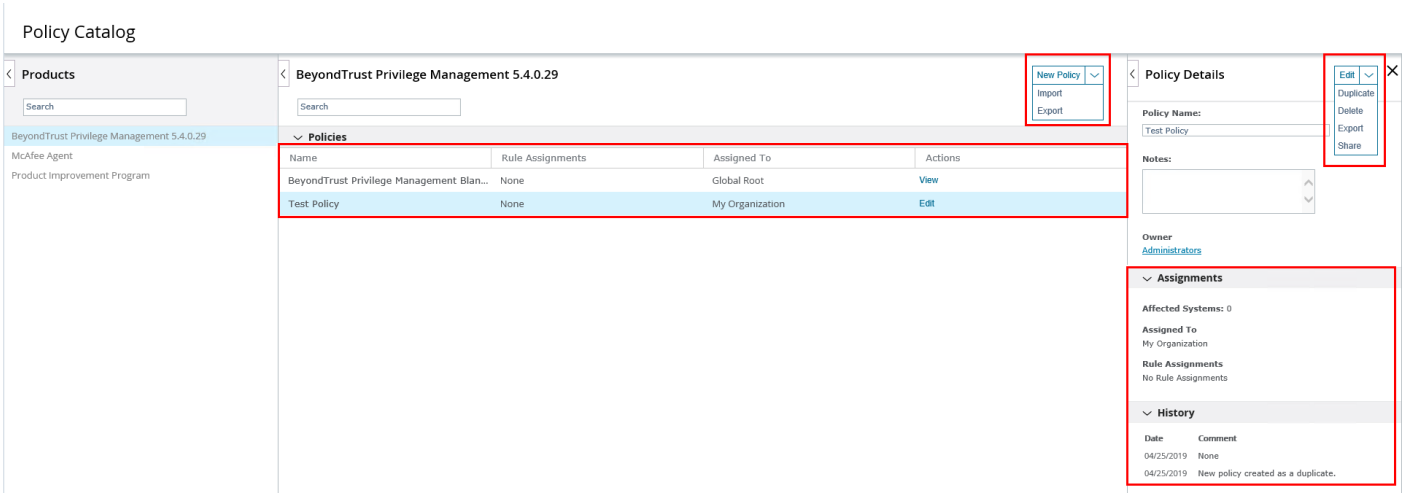
3. Execute the upgrade script where the name is the next version number and carry on applying these until the desired version is reached.

> ***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.

For more information, please see the following:

- *"Create a Privilege Management Policy" on page 21*
- *"Edit Privilege Management Policies" on page 21*
- *"Privilege Management for Mac Utilities" on page 69*
- *On configuring policies for macOS, "Privilege Management for Mac Policy" on page 22*

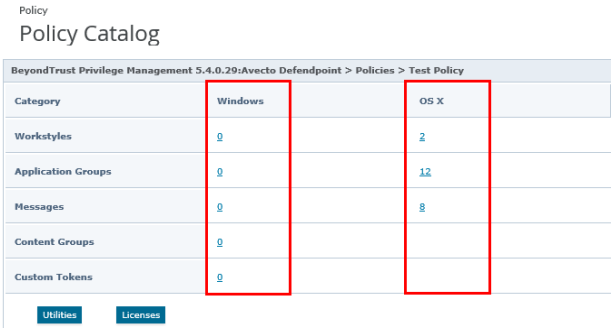
Access the Policy Summary Screen from the Policy Catalog

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 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.

> *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.

Privilege Management Policies and Templates

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

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
Category	Select the category you want the policy to belong to. By default, this will be **Policies**.
Create a policy based on this existing policy	You need to base the new policy on an existing policy. **BeyondTrust Privilege Management Blank Policy** is supplied for this purpose. Alternatively, you choose a different policy to base the new policy on.
Policy Name	Enter a name for the new policy. This should be as descriptive as possible. You can edit it later.
Notes	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 21.

Edit Privilege Management Policies

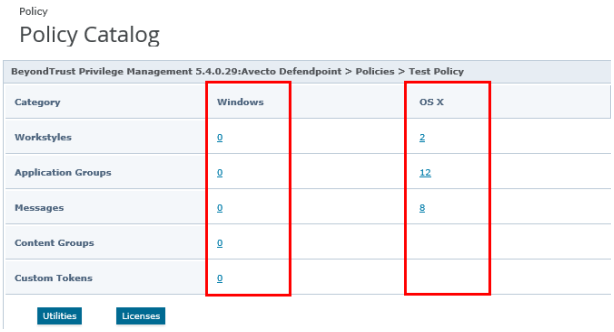
On the **ePO Policy Catalog** page, ensure **BeyondTrust Privilege Management <version number>** is selected from the list of products in the **Products** tab. Click the **Edit** link for the policy you want to edit from the list.

***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.



For more information, please see the following:

- *"Access the Policy Summary Screen from the Policy Catalog" on page 16*
- *"Privilege Management for Mac Licenses" on page 68*
- *"Privilege Management for Mac Utilities" on page 69*

Mac Policies

You can edit the following components of a policy:

- Workstyles
- Application Groups
- Messages

For more information, please see the following:

- *"Privilege Management for Mac Workstyles" on page 24*
- *"Application Groups" on page 34*
- *"Messages and Notifications in Privilege Management Policy" on page 57*

Privilege Management for Mac Policy

A Privilege Management for Mac 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 by using the WorkStyle Wizard or by importing them.
- **Application Groups:** Application Groups are used by Workstyles to group applications together to apply certain Privilege Management for Mac behavior.
- **Messages:** Messages are used by Workstyles to provide information to the end user when Privilege Management for Mac has applied certain behavior that you've defined and need to notify the end user.

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

Note: *Mac Policies are not applied to the root user.*

BeyondTrust has produced a prebuilt QuickStart policy that is configured with Privilege Management and Application Control.

For more information, please see the following:

- *"Privilege Management for Mac Workstyles" on page 24*
- *"Application Groups" on page 34*
- *"Messages and Notifications in Privilege Management Policy" on page 57*

Privilege Management for Mac Workstyles

Privilege Management for Mac 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.

For more information, please see the following:

- *"Access the Application Rules" on page 30*
- *"Create a Privilege Management Workstyle" on page 25*

Create a Privilege Management Workstyle

1. Navigate to the **Policy Catalog** and select **BeyondTrustPrivilege Management** from the **Products** list on the left side (for 5.9 and older versions, select **BeyondTrustPrivilege Management** from the **Product** dropdown and click the policy from the list that you want to add a Workstyle to).
2. Click the number for Mac Workstyles. If this is a blank policy this will be **0**.
3. Select **Actions > Create using Wizard** to start creating a Privilege Management for Mac Workstyle. This launches the Workstyle Wizard and takes you through the following screens.
4. **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.
5. **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.
6. **Filtering** (Controlling Workstyle only). This determines who receives 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.
7. **Select Capabilities** (Controlling Workstyle only). Allows you to choose Privilege Management and / or Application Control. If you don't select either capability, the next screen is **Finish**. This Workstyle will only contain filtering information.
8. **Privilege Management** (Controlling Workstyle with the Privilege Management capability). Allows you to choose:
    - how you manage sudo control
    - how you manage authorization prompts
    - how you manage installer privileges

> ***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.*

9. **Application Control** (Controlling Workstyle with the Application Control capability). Allows you to choose:
    - How you want to apply application control. You can choose from a allowlist or blocklist approach. We recommend you use a allowlist approach.
    - If you select **As a allowlist:** How you want to handle non-allowlisted applications.
    - If you select **As a blocklist:** How you want to handle blocklisted 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.*

10. **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 leave the box unchecked to continue to configure the Workstyle before you apply it to your endpoints.

Depending on the type of Workstyle you create and any capabilities that are included, Privilege Management for Mac auto-generates certain Application Groups (containing rules), and messages. Filters are applied and subsequently configured as part of the Workstyle.

After you change the policy, click **Submit** and then **Save** to save the policy. In ePO 5.10 and later, if you have Trellix 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:

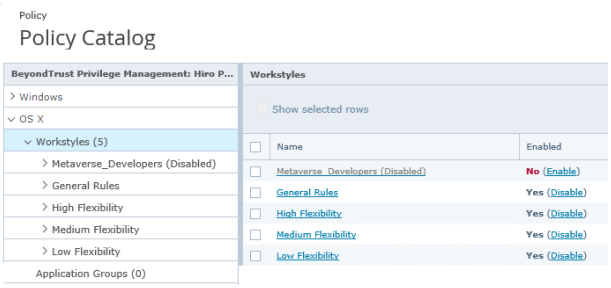
- *"Create a Privilege Management Policy" on page 21*
- *"Challenge / Response Authorization" on page 66*
- *"Messages and Notifications in Privilege Management Policy" on page 57*
- *"Application Groups" on page 34*

Disable or Enable Privilege Management Workstyles

You can enable or disable Workstyles to stop them being processed by Privilege Management for Mac.

To disable a Workstyle:

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



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 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
- 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:

- *"Access the Application Rules" on page 30*
- *"Account Filters in Privilege Management" on page 32*
- *"Computer Filters Privilege Management" on page 33*

Access the Application Rules

Application Rules are applied to Application Groups. Application Rules can be used to enforce allowlisting, 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 must have an Application Group before you can create an Application Rule.

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

Option	Description
Target Application Group	Select from the **Application Groups** list.
Action	Select from **Allow Execution** or **Block Execution**. This is what will happen if the application in the targeted Application Group is launched by the end user. **Passive (No Change)** is also an option in this dropdown on the macOS app rules.
End User Message	Select if a message will be displayed to the user when they launch the application. We recommend using **Messages** if you're blocking the execution of the application, so the end user has some feedback on why the application doesn't launch.
Auditing	
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.
Trellix ePO Reporting Options	
ePO Threat Events	Select this option to raise an ePO Threat event. These are separate from Privilege Management for Mac 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 Trellix Approvals workflow enabled, this workflow can be modified to change the **Save** button to **Submit for Review** based on user permissions.

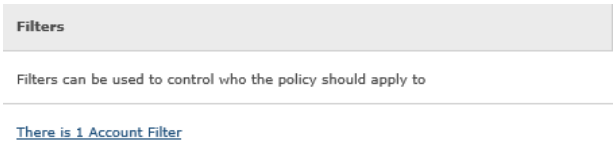
Application Rule Precedence

If you add more than one Application Rule to a Workstyle, 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, 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 "Application Groups" on page 34.

Workstyles Filters in Privilege Management

To view or edit the general properties of a Workstyle, select **macOS > Workstyles > Workstyle Name > Filters** from the policy tree.



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 and/or computers who receive it. However, you can add one or more filters to restrict 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 specifc computers by computer name or IP address.

If you want the Workstyle to apply only if *all* filters match, select the option **ALL filters must match** from above 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**.

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

Account Filters in Privilege Management

Account filters specify the users and groups the Workstyle will be applied to.

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

To restrict a Workstyle to specific groups or users you can filter on the **Account Name**, the **UID/GID**, or both.

1. Expand the appropriate Workstyle in the left pane and click **Filters**.
2. Select **Actions > Add Account Filter**.
3. Click the new account filter to open the **Add/Edit Accounts** page.
4. Select **Actions** > **Add Account**. You can choose to filter by **User** or **Group**.
    - For **User**, you can match on the **Account Name**, the **User ID**, or both. In the instance of both, they both must match for the filter to be applied. The **Account Name** is not case sensitive.
    - For **Group** you can match on the **Group Name**, the **Group ID**, or both. In the instance of both, they both must match for the filter to be applied. The **Group Name** is not case sensitive.
5. Click **OK** to finish configuring the filter.

By default, an account filter will apply 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 box at the top of the screen that says **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 will be displayed advising **No accounts added**, and the account filter will be ignored.

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

Computer Filters Privilege Management

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 Trellix 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 asterix 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.*

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 Application Groups

To create an Application Group:

1. Log in to ePO Policy Orchestrator and click **Policy Catalog**.
2. Navigate to the BeyondTrust Privilege Management for Mac policy you want to edit.
3. Under the **OS X** branch, click on **Application Group**, 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 Trellix 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 "Show Hidden Groups in Privilege Management" on page 90.

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 BeyondTrust Privilege Management for Mac policy which contains the Application Group you want to view or edit.
3. Under **OS X**, select **Application Groups**.
4. Check the box next to the Application Group, and then click **Actions > Properties**.
5. Make any changes you required and click **OK** to save the properties.

Delete an Application Group

Application Groups are usually mapped to one or more Application Rules 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 BeyondTrust Privilege Management for Mac policy which contains the Application Group you want to delete.
3. Check the box next 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 reference 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 one that already exists. You can edit a duplicated Application Group independently of the Application Group it duplicates.

To duplicate an Application Group:

1. Log in to ePO Policy Orchestrator and click on **Policy Catalog**.
2. Navigate to the BeyondTrust Privilege Management for Mac policy which contains the Application Group you want to duplicate.
3. In the **macOS** column, click the entry in the **Application Groups** row.
4. Under **OS X**, select the Application Group you want to duplicate.
5. Select **Actions > Duplicate**, or click the **Duplicate** button. You are asked to confirm the duplication.

A new duplicate Application Group with an incremental number in brackets appended to the name will be created, to which you can add applications.

Application Definitions in Privilege Management for Mac

Application definitions allow you to target applications based on specific properties. When an application is executed, Privilege Management for Mac will query the properties of the application and attempt 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 will the definition, and Privilege Management for Mac will attempt to match against subsequent definitions in the Application Group.

Privilege Management for Mac will continue 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 will be applied to the application, and it will run as normal.

Privilege Management for Mac must match every enabled criteria in an application definition you configure before it will trigger a match (the rules are combined with a logical AND).

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

Application Definition Matching Criteria

IMPORTANT!

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

Note: *All matching criteria are case sensitive on macOS.*

Application Requests Authorization

The application requires authorization so you need to approve that request - anything in macOS that has a padlock on the dialog box or where the system requires authorization to change something. You can match on the Auth Request URI, which is unique to the application.

When an application triggers an authorization request, the application will use a unique Auth Request URI. This URI will differ from the URI of the application. This matching criterion allows you to target any authorization request and apply your own controls by matching the Auth Request URI.

This matching criterion can be used in combination with other criteria to target authorization requests from specific applications, if more than one application uses the same Auth Request URI.

When this matching criterion is used in a definition, it will only match the authorization request of the application, and not the execution of the application. If you want to apply rules to both the application execution and application authorization request, then separate definitions must be created for each.

If you want to apply different rules to application execution and application authorization requests, then definitions must be added to different Application Groups and applied to different Application Rules.

Mac Packages are always configured to match exactly against the **system.install.software** request URI. You cannot set **Auth Request URI** or **Perform Match Using** options.

This matching criterion can be used with the following application types:

- Binaries
- Bundles
- Packages
- System Preferences

Command Line Arguments

The **Command Line Arguments** matching criterion allows you to target a binary, script, or sudo command based on the arguments passed to the command that is being executed on the command line. Command line arguments can be executed either through the Terminal, or through a script. With this matching criterion you can apply a specific action (such as block, allow or just audit) to specific command line arguments, rather than just applying actions to the use of the binary, script, or sudo command.

The **Command Line Arguments** matching criterion will match specifically the arguments passed to the binary, script or sudo command.

Example:

*The following command lists the contents of the **/Applications** directory:*

```
MyMac:~ standarduser$ ls -la /Applications
```

- ***ls** is the binary being executed, and is targeted by using the **File or Folder Name** matching criterion in a Binary definition.*
- ***-la /Applications** are the arguments being passed to **ls**, and is targeted by using the **Command Line Arguments** matching criterion in a Binary definition.*

***Note:** Privilege Management for Mac will only match the command line arguments, which will not include the beginning binary or sudo command being executed. If you want to match both the binary/sudo command and the command line, then both the **File or Folder Name** and the **Command Line Arguments** matching criteria must be enabled and populated in the definition.*

This matching criterion allows you to target all, or just parts of the command line being used. This is achieved by inserting wildcards into the **Command Line Arguments** string, defining which part of the command line you want to match, or by using a regular expression.

This matching criterion includes the following matching options:

- Command Line Arguments (for example **-la /Applications**)
- Exact Match
- Starts With
- Ends With
- Contains
- Regular Expressions

***Note:** Each option supports the use of wildcards:*

- ***? :** matches any one character*
- **** :** matches any string of characters, including <null> or empty strings.*

- ***?* :** *matches any string containing at least one character*

This matching criterion can be used with the following application types:

- Binaries
- Scripts
- Sudo Commands

Note: *You can match on any command line argument with the exception of those listed in* *"Mac Command Arguments Not Supported" on page 84*.

Delete Action Match

This criterion allows you to delete from the **/Applications** folder on a macOS system.

This matching criterion can be used with the **Bundle** application type.

File or Folder Name Matches

This matching criterion allows you to target applications based on their name/path on disk. It is an effective way of automatically allowlisting applications that are located in trusted areas of the filesystem (for example, **/Applications** or **/System**), and for targeting specific applications based on their full path.

This matching criterion can be used in combination with other criteria in a definition, giving you more granularity over which applications you can target based on their properties. Although you may enter relative file names, we strongly recommend that you enter the full path to a file.

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

- File or Folder Name (for example, **/Applications/iTunes.app**)
- Exact Match
- Starts With
- Ends With
- Contains
- Regular Expressions

Note: *Each option supports the use of wildcards:*

- ***? :*** *matches any one character*
- **** :*** *matches any string of characters, including <null> or empty strings.*
- ***?* :** *matches any string containing at least one character*

You can match on the file path containing or starting with the **/AppTranslocation/** folder, however we recommend you block all applications attempting to run from this location to ensure that unsigned applications are not run. Instead, we recommend you run applications from the **/Applications/** folder.

This matching criterion can be used with the following application types:

- Binaries
- Bundles
- Packages
- System Preferences
- Sudo Commands
- Scripts

File Hash (SHA-1 Fingerprint)

This definition ensures that the contents of the application, 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.

A file hash is a digital fingerprint of an application, generated from the contents of an application binary, script, or bundle. Changing the contents of an application will result in an entirely different hash. Every application, and every version of the same application, has a unique hash. Privilege Management for Mac uses hashes to compare the application being executed against a hash stored in the configuration.

File Hash matching is the most specific criterion, as it can be used to ensure that the application being run is the exact same application that was used when creating the definition, and that it has not been modified.

This matching criterion includes the **File Hash** matching options.

This matching criterion can be used with the following application types:

- Binaries
- Bundles
- Packages
- System Preferences
- Sudo Commands
- Scripts

Note: *Although* ***File Hash*** *is the more reliable matching criterion for matching a specific application, you must ensure that definitions are kept up to date. When updates are applied to the endpoint, new versions of applications may be added, and so their SHA-1 hashes will be different. Applications on different versions of macOS will also have different SHA-1 hashes.*

File Hash (SHA-256 Fingerprint)

Set the SHA-256 file hash on an application. The SHA-256 hash is supported on all appropriate macOS applications. On the macOS operating system, you can select **match**. The **does NOT match** setting is not available on macOS. We recommend using SHA-256 rather than SHA-1.

How to Determine a File's Hash for Matching Criteria

If you have audit events available through reporting, then you can find the appropriate SHA-256 file hash there. This is not as secure as using a CDHash for bundles.

Unsigned files (binary, script) and both signed and unsigned packages:

```
shasum -a 256 <path to file>
```

Unsigned bundle:

```
shasum -a 256 <path to bundle's main binary>
```

File Version matches

If the application you entered has a **File Version** property, it is automatically extracted and you can choose to **Check Min Version**, **Check Max Version**, and edit the version number fields.

For application types that have defined versions, you can optionally use the **File Version** matching criterion to target applications of a specific version or range of versions. This allows you to apply rules and actions to certain versions of an application; for example, blocking an application if its version is less than the version defined in the definition.

File Version matching can be applied either as a minimum required version, as a maximum required version, or you can use both to define a range of versions (between a minimum and a maximum).

This matching criterion includes the following matching options:

- File Min Version
- File Max Version

This matching criterion can be used with the following application types:

- Bundles
- System Preferences

Install Action Match

This criterion allows you to install to the **/Applications** folder on a macOS system.

This matching criterion can be used with the Bundle application type.

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

When a new application executes it is executed by another process, or *parent* process. In most cases the parent process will be launched. However, sometimes applications like binaries and bundles are executed by other applications.

For example, binaries like **curl** can be executed from the **Terminal**, and will be created as a child of the user's shell, for example, **bash**. However, **curl** can also be used by applications.

The **Parent Process** matching criterion allows you to the target applications based on their parent process, so that you can apply different rules and actions depending on where the application is being executed from. In the example above, you can use **Parent Process** matching to allow curl to be used by an authorized application, but still block users from executing it directly, in the **Terminal**.

Parent processes are defined as an Application Group, so that you can identify multiple parents without having to create multiple definitions. This also means that the parent process can be defined as any type of application (binary, bundle, script, system preference or package), using any of the relevant matching criteria for each application.

This matching criterion includes the Parent Process Group matching option (dropdown menu of all Application Groups that exist in the configuration).

This definition can be used with the following application types:

- Binaries
- Bundles
- Sudo Commands
- Scripts

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.

By default, a substring match is attempted (**Contains**). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a regular expression. The available operators are identical to the **File or Folder Name** definition.

Some applications are digitally signed with a certificate, guaranteeing that the application is genuine and from a specific vendor. The certificate also ensures that the application has not been tampered with by an unauthorized source. The vendor who owns the certificate can be identified from certain properties of the certificate, which are referred to as authorities. A certificate typically contains several authorities linked together in a chain of trust.

If you want to check if an application has been digitally signed, and what the certificate authorities are, use the **Codesign** command.

Example:

To check the certificate of the iTunes.app application bundle:

```
Codesign -dvvv /Applications/iTunes.app/
```

If the application has a certificate, there are one or more authorities listed in the output:

```
Authority=Software Signing
Authority=Apple Code Signing Certification Authority
Authority=Apple Root CA
```

In the output, the first authority listed is the authority most specific to the application. In the example, you can see that Apple uses the certificate authority **Software Signing** to digitally sign iTunes.app.

With the **Publisher** matching criterion, you can target applications based on the publisher information contained in its certificate. This matching criterion can also be used in combination with other matching criteria, as a way of ensuring the application is a genuine application from the vendor.

Note: *All apps downloaded from the Apple Store will have certificates with the same authority, as Apple resigns all applications before making them available in the Apple Store.*

This matching criterion includes the following matching options:

- Publisher (for example, the Publisher for Apple applications is **Software Signing**)
- Exact Match
- Starts With
- Ends With
- Contains
- Regular Expressions

> ***Note:*** *Each option supports the use of wildcards:*
> - ***? :*** *matches any one character*
> - **** :*** *matches any string of characters, including <null> or empty strings.*
> - ***?* :*** *matches any string containing at least one character*

This definition can be used with the following application types:

- Binaries
- Bundles
- Packages
- System Preferences
- Sudo Commands

Source

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 Mac at the point it is downloaded, therefore if a user decided to run the application or installer at a later date, the source can still be verified. By default, a substring match is attempted (**Contains**). Alternatively, you can choose to pattern match based on either a wildcard match (**?** and *****) or a regular expression. The available operators are the same as the **File or Folder Name** definition.

This definition can be used with the following application types:

- Bundles
- System Preferences

URI

Every macOS application bundle has a defined Uniform Resource Identifier (URI), a property that uniquely identifies the application to the system. URIs follow a specific structure, typically referencing the vendor and application. For example, the URI for Apple iTunes is **com.apple.iTunes**.

The URI matching criterion provides an effective way of targeting applications where the filename or file path may not always be known. It is also an effective way of targeting applications from a specific vendor.

This matching criterion can also be used in combination with other matching criteria, as a way of ensuring the application is a genuine application from the vendor.

This is the Unique Request Identifier for the application bundle. You can choose to match based on the following options (wildcard characters **?** and ***** may be used):

- URI (For example, **com.apple.iTunes**)
- Exact Match
- Starts With
- Ends With
- Contains
- Regular Expressions

Note: *Each option supports the use of wildcards:*

- ***? :*** *matches any one character*
- **** :*** *matches any string of characters, including <null> or empty strings.*
- ***?* :*** *matches any string containing at least one character*

This definition can be used with the Bundles application type.

Manage Disk Mounted Images in Privilege Management for Mac

Privilege Management for Mac examines each Disk Mounted Image (DMG) and, if there is one or more bundles of applications in the disk image, where the application is associated with a Privilege Management *Allow* rule, the user is allowed to copy those bundles to the **System Applications** folder on the endpoint.

If the applications do not have an Privilege Management *Allow* rule, macOS defaults to requiring admin credentials in order to copy the bundle to the System Applications folder. Standard macOS functionality is used if anything other than an *Allow* rule is associated with the application bundle in the DMG, such as **Block** or **Passive**.

Configuration of the defendpoint.plist File

Management of DMGs is controlled by default, but it can be turned off by editing the **defendpoint.plist** file.

The location for the **defendpoint.plist** file is: **/Library/Application Support/Avecto/Defendpoint/defendpoint.plist**

The **MountAssist** key, which is set to **true** by default, should be set to **false** to turn off the Privilege Management for Mac management of DMG files:

```
<key>MountAssistant</key>
<false/>
```

You need to restart the **defendpointd** daemon after you have edited the **defendpoint.plist** file for any changes to take effect. This can be done either by restarting the machine or by running these commands from your terminal:

```
sudo launchctl unload /Library/LaunchDaemons/com.avecto.defendpointd.plist
sudo launchctl load /Library/LaunchDaemons/com.avecto.defendpointd.plist
```

Format of Messages

Within the **defendpoint.plist** file in the key tag you can also modify the string that is used for the messaging.

The format of the messages is a **key** and **string** tag:

```
<key>MountMessageAllow</key>
<string>Allow copying "[APP_NAME]" from "[MOUNT_NAME]" to Applications?</string>
```

The following placeholders can be used:

- **[APP_NAME]**
  - Replaced by the **Application Name**.
- **[MOUNT_NAME]**
  - Replaced by the **Volume Name** of the mounted DMG.

> ***Note:*** *When you enter your own strings for the above keys, the formatting is "what you see is what you get." For example, if you press **Enter**, then you will get a new line.*

You can configure the message that is displayed to the user at the endpoint in the following scenarios:

- **MountMessageAllow:**Message that appears when a DMG containing an allowed bundle is mounted.
- **MountMessageNoteSame:** Message that appears in smaller text below the **MountMessageAllow** message if the bundle is allowed, but the same version exists in the destination.
- **MountMessageNoteNewer:** Message that appears in smaller text below the **MountMessageAllow** message if the bundle is allowed but a newer version of the bundle exists in the destination.
- **MountMessageNoteOld:** Message that appears in smaller text below the **MountMessageAllow** message if the bundle is allowed but an older version of it exists in the destination.
- **MountNotificationSuccess:** Message that appears in the macOS notification center when the copying process succeeds.
- **MountNotificationFailure:** The message that appears in the macOS notification center when the copying process fails.

If the message keys above have not been set, Privilege Management for Mac uses the default values and strings.

If you enter the <key> but do not specify the <string>, then the message will be empty.

You must use escaped characters for valid XML, such as in the examples below:

Symbol	Escaped Form
"	&quot"
&	&amp"
‘	&apos"
<	&lt"
>	&gt"

Message Examples

The following examples show sample messages in the **defendpoint.plist** file.

```
<key>MountMessageAllow</key>
   <string>Allow copying "[APP_NAME]" from "[MOUNT_NAME]" to Applications?</string>
<key>MountMessageNoteSame</key>
   <string>Note: same version of the item named "[APP_NAME]" already exists in this
location.</string>
<key>MountMessageNoteNewer</key>
   <string>Note: a newer version of the item named "[APP_NAME]" already exists in this
location.</string>
<key>MountMessageNoteOlder</key>
   <string>Note: an older version of the item named "[APP_NAME]" already exists in this
location.</string>
<key>MountNotificationSuccess</key>
   <string>"[APP_NAME]" was successfully copied from "[MOUNT_NAME]" into the Applications
older.</string>
<key>MountNotificationFailure</key>
   <string>"[APP_NAME]" was not successfully copied from "[MOUNT_NAME]" into the Applications
folder.</string>
```

Insert a Binary to an Application Group

Note: *Matching criteria is case sensitive.*

1. Select the Application Group you want to add the binary control to.
2. In the right-hand pane select **Actions > Add Application > Binary**.
3. You need to configure the matching criteria for the binary. You can configure:
    - **File or Folder Name matches**
    - **File Hash (SHA-1 Fingerprint)**
    - **Application Requests Authorization**
    - **Command Line Arguments**
    - **Publisher matches**
    - **Parent Process matches**
4. Click **OK**. The binary is added to the Application Group.

For more information, please see "Application Definitions in Privilege Management for Mac" on page 36.

Insert a Bundle to an Application Group

> ***Note:*** *Matching criteria is case sensitive.*

1. Select the Application Group you want to add the bundle control to.
2. In the right-hand pane select **Actions > Add Application > Bundle**.
3. You need to configure the matching criteria for the bundle. You can configure:
    - **File or Folder Name matches**
    - **File Hash (SHA-1 Fingerprint) matches**
    - **Source URL matches**
    - **File Version matches**
    - **URI**
    - **Application Requests Authorization**
    - **Publisher matches**
    - **Parent Process**
    - **Delete Action match**
    - **Install Action match**
4. Click **OK**. The bundle is added to the Application Group.

> *For more information, please see "Application Definitions in Privilege Management for Mac" on page 36.*

Insert a Package to an Application Group

Note: *Matching criteria is case sensitive.*

1. Select the Application Group you want to add the package to.
2. In the right pane, select **Actions > Add Application > Package**.
3. You can leave the **Description** field blank to match on all binaries.
4. You need to configure the matching criteria for the package. You can configure:
    - **File or Folder Name matches**
    - **File Hash (SHA-1 Fingerprint) matches**
    - **Application Requests Authorization**
    - **Publisher matches**
5. Click **OK**. The package is added to the Application Group.

For more information, please see "Application Definitions in Privilege Management for Mac" on page 36.

Insert a Script to an Application Group

You can control scripts using the **Script** application type. System administrators can apply Application Rules on scripts to allow installation and management of development tools; for example, Homebrew.

Supported script types include:

- bash (.sh)
- ruby (.rb)
- python (.py - xattr)

> ***Note:*** *Matching criteria is case sensitive.*

1. Select the Application Group you want to add the script control to.
2. In the right pane, select **Actions > Add Application > Script**.
3. You need to configure the matching criteria for the script. You can configure:
    - **File or Folder Name matches**
    - **File Hash (SHA-1 Fingerprint)**
    - **Command Line Arguments**
    - **Parent Process matches**
4. Click **OK**. The script is added to the Application Group.

> *For more information, please see "Application Definitions in Privilege Management for Mac" on page 36.*

Install Homebrew

The Homebrew installer is a shell script which users can download to their machine and run. This script internally uses sudo to create folders on the system and set their ownership/permissions to be accessible by the installing user, reducing the need for further privileged sudo operations when users want to install packages.

Allow Standard Users to Install Homebrew via Privilege Management for Mac

Prepare a Script

The current installation script for Homebrew must be modified slightly to work with Privilege Management for Mac.

To achieve this, create a script that contains the following:

```
#!/bin/bash

# Download the latest brew install script using curl
curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install.sh -o install.sh

# The following command modifies the install.sh script, creating a backup of the original
```

```
# as install.sh.bak, and does the following modifications
#  - replaces occurrences of "/usr/bin/sudo" with just "sudo" to allow customers using
#    the non-Apple sudo to continue
#  - Inserts a line "HAVE_SUDO_ACCESS=0" near the top of the file. This bypasses the
#    built-in have_sudo_access feature with the expectation that the PMFM plugin policy is
#    correctly configured to match this script

sed -i .bak -e $'s^set -u^set -u\\\nHAVE_SUDO_ACCESS=0^' \
    -e '/unset HAVE_SUDO_ACCESS/d' install.sh

source install.sh

rm install.sh
rm install.sh.bak
```

Check the shasum of the file you created to ensure no copy and paste irregularities have introduced differences.

To check the shasum of the script, run the following command in Terminal:

```
shasum -a 1 <name of script>
```

Add the Script to Policy

To create a rule to match this script in the Policy Editor:

1. Create an Application Group to add the script control.
2. Right-click and select **Insert Application > Script**.
3. Enter * as the file or folder name, as you're matching explicitly on hash.
4. Enter a description of **User Homebrew Installation**.
5. Set the **File Hash** to value ***<insert shasum here>***.

   Ensure this file hash is the same as the script you prepared earlier, in case you made any custom modifications.

6. Click **Finish**. The script is added to the Application Group.

Add a sudo Command for Homebrew to Policy

In the same Application Group:

1. Right-click and select **Insert Application > Sudo Command**.
2. Enter * to represent any sudo command.
3. Enter a description or accept the default, and click **Next**.
4. Configure the **Parent Process Matches** to be the group which you are editing.

   This keeps the configuration of Homebrew isolated within the policy and easier to navigate. Alternatively, you can separate the **Script** and **Sudo** application definitions.

5. Click **Finish**. The **sudo** command is added to the Application Group.

Set Up an Application Rule for Homebrew

1. Select the Workstyle that is appropriately filtered for users you want to allow to install Homebrew.
2. Create an application assignment for the Application Group that contains the sudo command, of type **Allow Execution**, with your messaging and auditing preferences.

Insert a Sudo Command to an Application Group

> ***Note:*** *Matching criteria is case sensitive.*

1. Select the Application Group you want to add the sudo command to.
2. In the right pane, select **Actions > Applications > Sudo Command**.
3. You need to configure the matching criteria for the sudo command. You can configure:
    - **File or Folder Name matches**
    - **File Hash (SHA-1 Fingerprint) matches**
    - **Command Line Arguments**
    - **Publisher matches**
    - **Parent Process matches**
4. Click **OK**. The sudo command is added to the Application Group.

Sudo Switches

Privilege Management for Mac supports running sudo commands with the following switches:

- **-b**, **--background**
- **-e**, **--edit:** This switch needs to be configured in Privilege Management for Mac for it to be supported.
- **-i**, **--login**
- **-S**, **--stdin**
- **-s**, **--shell**
- **-V**, **--version**

When a **sudo** command is run, Privilege Management for Mac ignores any switches that have been used and will match the rest of the command against the application definition. If Privilege Management for Mac matches against a rule that allows execution, the sudo command runs with any supported switches that were used. Any switches that are not supported by Privilege Management for Mac are ignored.

If Privilege Management for Mac matches on a passive rule or doesn't match any rules, then the **sudo** command runs with any supported or unsupported switches that have been used.

> ***Note:*** *The **-l --list** switch, which lists the commands that the user is allowed to run, does not take into account the commands that are restricted by Privilege Management for Mac.*

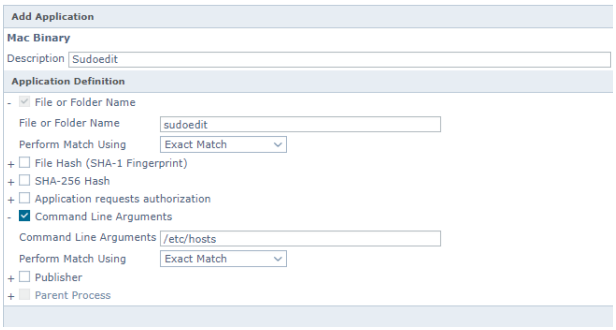
Edit -e Switch

The **-e --edit** switch, also known as **sudoedit**, allows the user to edit one or more files using their preferred text editor. The text editor is defined by setting the **SUDO_EDIT**, **VISUAL** or **EDITOR** environment variable in their **Terminal** session. Otherwise, the default editor, **Vim**, is used. To configure your policy to support the **-e** switch, you need to set up a sudo command Application Rule so that:

- The **File or Folder Name** definition is set to **sudoedit** with the **Perform Match Using** set to **Exact Match**
- The **Command Line Arguments** definition is set to the path of the file(s) that you want to control using this rule

Example: *The application definition shown in the screenshot supports the* ***sudo*** *command:*

```
sudo -e /etc/hosts
```



The audit log shows an application of **/usr/bin/sudo** and the command line arguments have **-e** prepended to them.

For more information, please see *"Application Definitions in Privilege Management for Mac" on page 36*.

Insert a System Preference Pane to an Application Group

Note: *Matching criteria is case sensitive.*

1. Select the Application Group you want to add the **System Preference** pane to.
2. In the right pane select **Actions > Add Application > System Preference Pane**.
3. You need to configure the matching criteria for the **System Preference** pane. You can configure:
    - **File or Folder Name matches**
    - **File Hash (SHA-1 Fingerprint) matches**
    - **Source URL matches**
    - **File Version matches**
    - **Application Requests Authorization**
    - **Publisher matches**
4. Click **OK**. The **System Preference** pane is added to the Application Group.

For more information, please see "Application Definitions in Privilege Management for Mac" on page 36.

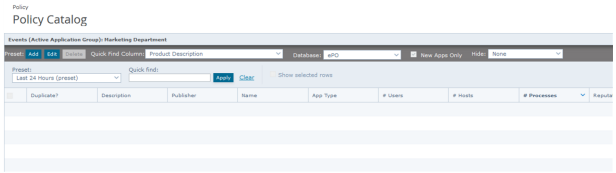
Insert Applications from Events (Event Importer)

The Privilege Management for Mac Workstyle editor allows you to add applications that have been audited by Privilege Management for Mac 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**, type the username in the **Quick Find** box, and then 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 will automatically return 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 will be prepopulated with values collected from the application.

***Tip:** For queries which are taking a long time to execute, the **Cancel Query** button can be clicked 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 will be displayed as a single application.*

Insert Applications from Templates

Application templates provide a simple way to pick from a list of known applications. A standard set of templates is provided that covers basic administrative tasks.

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

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

Use the Add Apps from Template Menu

1. Select the Application Group you want to add the application to.
2. Select **Actions > Add Apps From Template**. 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**, and choose your application from the menu. **Binary**, **Bundle**, and **System Preference Pane** all have **Template** options.
3. Click **Template** next to the **Description** and choose the application you selected to add to the Application Group.
4. Select the applications you want to add to the Application Group. Each application will be 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. Select **Save**.

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

Messages and Notifications in Privilege Management Policy

You can define any number of end user Messages and notifications. Messages and notifications are displayed when a user's action triggers a rule. Rules can be triggered by an application launch or block.

Messages provide an effective way of alerting the user before an action is performed. For example, before an application is authorized, or advising that an application launch has been blocked.

Messages give the user information about the application, 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.

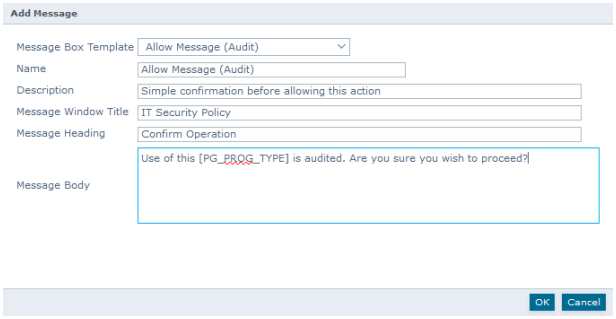
Messages are customizable with visual styles, corporate branding and display text, so you are offered a familiar and contextual experience. Messages are assigned to Application Rules.

Once defined, a Message may be assigned to an Application Rule within a Workstyle by editing the rule. Depending on the type of Workstyle you've created, Privilege Management for Mac may auto-generate certain Messages for you to use.

Create a Message for a Workstyle

To create a Message:

1. Select the **Messages** node in the relevant Workstyle. The right pane displays the **All Messages** page.
2. In the right pane, select **Actions > Add**. The **Add Message** dialog box appears.



3. Select a message template from the **Message Box Template** dropdown. You can choose from:
    - Allow Message (Audit)
    - Allow Message (enter Reason)
    - Allow Message (select Reason)
    - Allow Message (with Authentication)
    - Allow Message (with Challenge)
    - Block Message
    - Request Message (enter Reason)
    - Request Message (select Reason)
4. You can change the other options if required to customize it to your organization's needs.
5. Click **OK** to finish creating the Message.

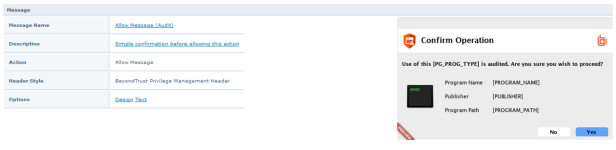
A new message is created. You may now further refine the Message by selecting it and editing the **Design** and the **Text** options available beneath each Message.

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

Edit the Message Name and Description

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

1. Click the **Message** node and select the message you want to edit in the **All Messages** pane.
2. You can click the **Message Name** or check the box and click the **Properties** button to edit the **Message Name or Description**. Click **OK** to save your changes.



Design a Message in Privilege Management

You can configure the following aspects of a message:

- Message Header Settings
- User Reason Settings
- User Authorization
- Sudo User Authorization
- Challenge / Response Authorization

As you change the message options, click **Update** to see the changes. Program and content information is shown with placeholders.

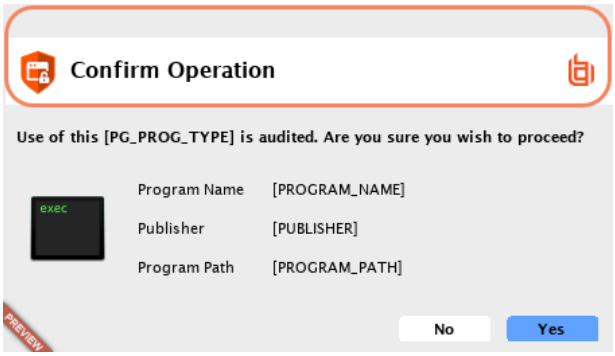
After you configure the message options, you can configure message Text, which includes the ability to configure different languages.

The options here are preselected based on the type of message that you create, but can be overridden if required.

For more information, please see "Use Message Text Options to Build Your Message" on page 63.

Message Header Settings

The message header is shown highlighted here:



- **Header Style:** This is preconfigured. You can choose to remove the header entirely or select from one of the templates provided. Choose from:
  - No Header
  - BeyondTrustPrivilege Management Header
  - Warning Header
  - Question Header
  - Error Header
- **Show Title Text:** This box is checked by default. You can uncheck it to remove the text adjacent to the icon if required.
- **Text Color:** This controls the color of the text adjacent to the icon. To change the color of the text, click the **Custom** option and select the color you require.
- **Background Type:** This option controls the color behind the text and icon. If you select **Solid** then only Color 1 is available for you to change. If you select **Gradient** then both Color 1 and Color 2 can be configured. If you select **Custom Image** then you can't configure the colors as you will upload a custom image in the next section.

- **Custom Image:** You can choose from one of a number of preset custom images or you can click **Manage Image** to upload one of your own. The recommended image size is 450 pixels wide and 50 pixels high.
- **Color 1:** Select the color for a **Solid background** or the first color for a **Gradient background**.
- **Color 2:** Select the second color for a **Gradient background**.

User Reason Settings

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

You can choose to have a text box below the message to allow the end user to enter a reason. This is already selected for you for the **Reason Required** Message but you can override it here if required. Choose from **Off** or **Text box** in the **Show User Reason Prompt** dropdown. The predefined dropdown entries can be configured on the **Message Text** tab.

User Authorization

- **Authorization Type:** Select from **None**, **User must authorize**, or **Designated user must authorize**.
  - **User must authorize:** Select to force the user to reenter their credentials and confirm they want to run the application.
  - **Designated user must authorize:** Select to designate which users can authorize the message. Add users from **Designated Users**.
- **Authentication Method:** Select from **Any, Password only**, or **Smart card only**. Select **Any** to allow authentication using password or smart card / YubiKey authentication. When **Password only** is selected, a **Username and Password** field is added to the message. When smart card only is selected, a **Username and PIN** field is added to the message.
- **Designated Users:** If you select **Designated user must authorize**, click the ellipses (**...**) button to add the users who can authorize the message.

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

For more information about smart card authentication in Privilege Management for Mac, please see the Privilege Management for Mac Administration Guide at https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-mac-admin.pdf.

Sudo User Authorization

You can use the **Don't ask for password if already entered** dropdown to control how frequently the user has to enter a password to use the **sudo** command. This text option is only enabled if the **User Authorization** has been set to **User must authorize** or **Designated user must authorize**. The available options are:

- Ask every time
- Less than 1 minute ago
- Less than 5 minutes ago
- Less than 15 minutes ago
- Only ask once per session

Challenge/Response Authorization

You can check the **Enabled** box for **Challenge/Response Authorization** to add a challenge code to the Message. This box is already checked if you selected a challenge Message. If you have already created a Workstyle with a challenge Message, then the policy will already have a challenge / response key. Select **Change Key** and enter a new challenge / response code twice to change it.

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 will be prompted to enter a shared key.

You can click **Edit Key** to change the shared key for this message.

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

For more information, please see "Challenge / Response Authorization" on page 66.

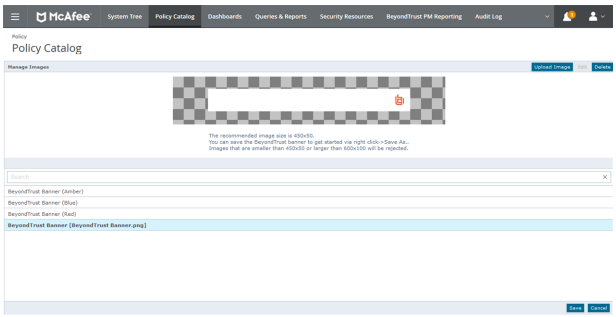
Manage Images to Use in Message Headers

Use the Image Manager 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 strongly recommend that you delete any unused images to minimize the size of the policies, as Privilege Management for Mac does not automatically delete unreferenced images.

The **Image Manager** is accessible from the **Message Design** tab. Click the **Manage Images** button next to the **Custom Image** dropdown menu.



To upload an image:

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

> ***Note:*** *Images must be *.png format and be sized between 450x50.*

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.*

Use Message Text Options to Build Your Message

After you have made a change to the Message text, click **Update** to see your changes applied to the preview Message.

> ***Note:*** *Mac does not support multiple languages.*

General

- **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.

Publisher

Verification Failure: Controls the text that is displayed next to the **Publisher** if the publisher verification fails.

Privilege Management for Mac 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 Mac does not check to see if the certificate has been revoked due to the length of the loPrivilege Management for Mac 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.

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.
- **Card PIN:** Controls the text displayed when the smart card pin is provided.
- **Unauthorized credentials:** Controls the text that is displayed if the end user enters credentials that aren't valid for the requested operation.

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**.

Buttons

- **OK Button:** controls the text that is displayed on the button that appears on the bottom right.
- **Cancel Button:** controls the text that is displayed on the button that appears to the left of the **OK** button.

Depending on the Message options, the Message box will have either one or two buttons with the following default text:

- For an **Allow Message (Audit)** the Message box will have **Yes** and **No** buttons.
- For an **Allow Message (enter Reason)** the Message box will have **OK** and **Cancel** buttons.
- For an **Allow Message (with Authentication)** the Message box will have **OK** and **Cancel** buttons.
- For an **Allow Message (with Challenge)** the Message box will have **Authorize** and **Cancel** buttons
- For a **Block Message** the Message box will have just an **OK** button
- For a **Request Message (enter Reason)** the Message box will have **Submit** and **Cancel** buttons.

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 end user a question.

Challenge / Response Designated User Option

Challenge / Response provides an additional level of control for access to applications and privileges.

An extra aspect of this feature is **Designated User** authorization. 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
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

For more information on Designated User settings, please see the Authorization Settings section of "Challenge / Response Authorization" on page 66.

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 an end user message. In order for the user to progress, they must enter a corresponding response code into the message.

Any policy that has a message with a challenge / response requires 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 here if required.

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 Mac messaging.

Users will be presented with a different, unique challenge code each time a challenge / response message is displayed.

Shared Key

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

Once you have entered a shared key, it will be applied to all end user messages that have challenge / response authorization enabled in the same Privilege Management for Mac 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 will be presented with a warning message.

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

Generate a Response Code

There are two 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.

For more information on configuring challenge / response authorization enabled end user Messages, please see *"Challenge/Response Authorization" on page 61*.

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.

Generate 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. 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 end user needs to run that application for the duration of the **Authorization period**.

For more information, please see "Challenge/Response Authorization" on page 61.

Generating 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 are entered.

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

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

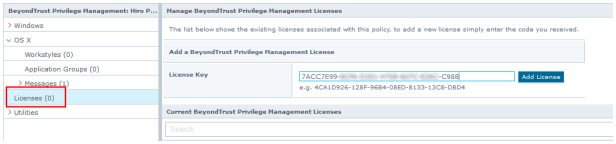
Privilege Management for Mac Licenses

Privilege Management for Mac 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 Mac 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 Trellix 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 "Events in Privilege Management for macOS" on page 96.*

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

> ***Note:*** *Importing and exporting policies from the* ***Utilities*** *section of a policy differs from importing and exporting policies from the Trellix 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 Mac 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

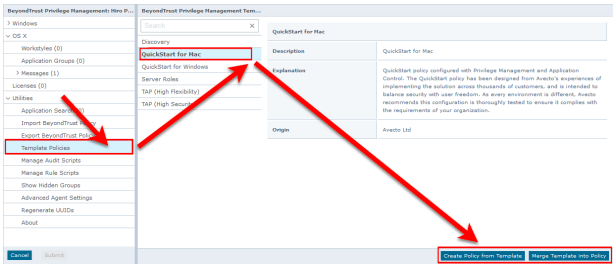
Privilege Management for Mac policies may be imported to and exported from Trellix ePO as XML files, in a format common to other editions of Privilege Management for Mac , such as Privilege Management for Mac Group Policy Edition. This allows for policies to be migrated and shared between different deployment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

> ***Note:*** *Importing and exporting policies from the* ***Utilities*** *section of a policy differs from importing and exporting policies from the Trellix 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 Mac Endpoints

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



> ***Note:*** *Be careful when merging policies with production policies. If* ***No*** *is selected, then the existing policy settings and license information are removed. If* ***Yes*** *is selected, then the template is added to the existing policy.*

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

- Discovery
- QuickStart for Mac
- 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 Mac Template Policy Configuration

The QuickStart for macOS policy contains **Workstyles**, **Application Groups**, and **Messages** 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 this configuration be thoroughly tested 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

- (Default) Authorize - System Trusted
- (Default) General - Any Application
- (Default) General - Any Applications Requiring Authorization
- (Default) Passive - System Trusted
- Any Other Sudo Commands
- Authorize - High Flexibility
- Authorize - Controlled OS Functions
- Authorize - General Business Applications
- Authorize - Low Flexibility
- Authorize - System Preferences
- Authorize Sudo Commands - General
- Authorize Sudo Commands - High Flexibility
- Block - Applications
- Passive - General Business Applications
- Passive Sudo Commands - General
- Passive Sudo Commands - High Flex

Messages

- Allow Authorize (Delegated Authorizer)
- Allow Authorize (User Authorizer)
- Allow Message (Audit)
- Allow Message (Enter Reason)

- Allow Message (with Challenge)
- Block (OK)

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 Mac configuration.

After the QuickStart policy has been 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 being used within your organization, and whether they require admin rights, need to be blocked, or need authorization for specific users.

This data can then be used to further refine the QuickStart policy to provide more a tailored Privilege Management for Mac 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 Mac 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 Authorize (Delegated Authorizer):** Asks the user to enter the username and password of another user before the application is authorized to run.
- **Allow Authorize (User Authorizer):** Asks the user to enter their password before the application is authorized to run.
- **Allow Message (Audit):** Asks the user to confirm that they want to proceed to authorize an application to run.
- **Allow Message (Enter Reason):** Asks the user to provide a reason and enter their password before the application is authorized to run.
- **Allow Message (with Challenge):** 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.
- **Block (OK):** Warns the user that an application has been blocked.

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 Mac 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.*

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.*

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 Mac matching criteria such as **Exact Match** or

Regular Expressions.

> ***Note:*** *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 Mac 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.

Mac Policy Structure and Precedence

Structure

Policies are stored in **/etc/defendpoint/**. For example:

- pmc.xml
- epo.xml
- mdm.xml
- local.xml

These policies are not case-sensitive. All policies stored in this location must have the following permissions to ensure policy acceptance and system security:

- Ownership of **_defendpoint** user and group, for example:

```
sudo chown _defendpoint:_defendpoint <policy path>
```

- Permission for the **_defendpoint** user and group to read the policy, but not other users, for example:

```
sudo chmod 660 <policy path>
```

The policy or policies that are read and loaded by **dppolicyserver** are dependent on the settings under **config.order** in the **defendpoint.plist**.

***Note:** If all policies are deleted, the **local.xml** policy is regenerated.*

Precedence

The policy precedence determined in the **defenpoint.plist**, which is stored here: **/Library/Application Support/Avecto/Defendpoint/defendpoint.plist**.

The **defendpoint.plist** is appended or created with the precedence lists (as below) on start up or installation. But editing and saving of the list is applied immediately.

```
<key>config.order</key>
<array>
<string>pmc</string>
<string>epo</string>
<string>mdm</string>
<string>local</string>
</array>
```

You can edit the **defendpoint.plist** file manually to change the policy precedence if required.

The **dppolicyserverd** will go through the policies under **/etc/defendpoint/** by finding the first policy in the **config.order**, and it if it can't a policy of that name it will progress to the next in the list.

If one or more policies are found with the correct name it will load them, irrespective of whether or not it has a license.

Apply Multiple Policies for MacOS Estates in ePO

For Mac estates managed by ePO, the simultaneous application of multiple policies is supported, for example:

- epo.xml
- epo001.xml
- epo002.xml

In the example above, if the policy precedence is set for ePO policies, then rules processing will first check the rules in **epo.xml**. If no rules are found for the process in this policy, then it will go through **epo001.xml**. Each policy is processed in an alpha-numeric/C locale order. This continues until the process hits a rule or **dppolicyserverd** reads all of the policies without finding a match.

If multiple policies are loaded, only one of them requires a Privilege Management for Mac license. We do not recommend you use multiple licenses in this configuration. Each policy can have a different Challenge / Response key.

Copy and pasted policies with altered rules are still processed. The **dppolicyserverd** log outputs whether it replace GUIDs when loading them into memory if it was a duplicate.

Categories for Mac Application Templates

Privilege Management for Mac ships with some standard application templates to simplify the definition of applications that are part of the operating system. The standard application templates are split into categories:

- System Preference Panes
- Bundles
- Binaries

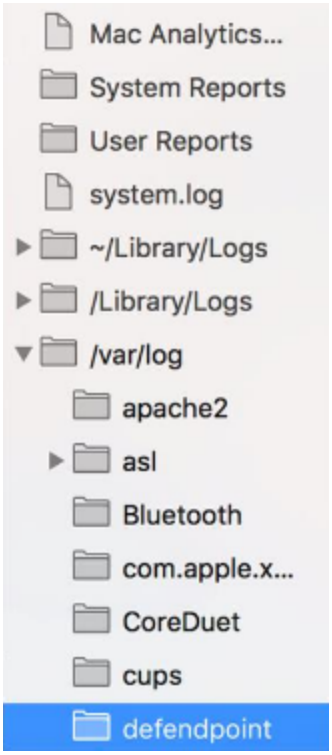
Each category then has a list of applications for that category. Picking an application will cause the application to be prepopulated with the appropriate information.

Privilege Management for Mac Audit Logs

How to log events to a file:

1. When Privilege Management for Mac is installed, it checks to see if the following path and file is present. If it's not, it creates it: **/var/log/defendpoint/audit.log**
2. This file cannot be edited during output. If this file is deleted, Privilege Management for Mac recreates it dynamically. If the folder structure is deleted, Privilege Management for Mac recreates it when the endpoint is restarted.

3. This log file can be viewed in the macOS Console for all versions from **/var/log** in the side bar. You can also view the log output in real time, if required.



4. The log file is maintained by the core macOS service **newsyslog**. The **newsyslog.conf** file contains various log files and associated settings and is maintained by the core macOS. The **newsyslog.conf** file is held here: **/etc/newsyslog.conf**.

> ***Note:*** *This part of the set up must be done by a user who can write to this location.*

5. In the **newsyslog.conf** file the settings are outlined and have column headers:

   logfilename, **mode**, **count**, **size**, **when**, **flags**

6. For the purposes of the maintenance of the **audit.log** file, you need to populate the **logfilename**, **mode**, **count**, **size**, and/or **when**, and **flags** attributes in the **newsyslog.conf** file.
   - **logfilename:** Path and filename
   - **mode:** File mode, i.e. settings for read/write for each user type (POSIX file permissions)
   - **count:** Count for amount of archived files (count starts from 0)
   - **size:** Threshold for log size in KB
   - **when:** Threshold for log size in terms of time (i.e. new log everyday at X, or every month)
   - **flag:** Instruction for processing the archived/turn-over file. This is most likely to be **JN** or **ZN**

An example of a line in the **newsyslog.conf** for Privilege Management for Mac is:

```
/var/log/defendpoint/audit.log 644 5 1000 * JN
```

This indicates that:

- the filename is **audit.log**
- it can be viewed by all user types but can only be edited by the root user
- it has an archive count of 5 (6 archived files, not including the current log)
- it has a threshold of 1MB for turn-over/archiving
- it doesn't have a date turn over
- for archiving, files are to be compressed into a .BZIP file

> ***Note:*** *The threshold relies on the* ***newsyslog*** *service. This service is* ***low*** *priority in macOS and only reads the .conf file approximately every 30mins. Using the example line above, the log can become greater than 1MB prior to the service reading the* ***newsyslog.conf*** *file due to it being a "threshold" value, rather than each log file being of equal size.*

7. Once you have applied the **newsyslog.conf** by adding the **audit.log** line to it, you can run **sudo newsyslog -nv** in Terminal to see the state of the logging, when the next roll over is, and whether there are any syntax issues.

Add Privilege Management for Mac Settings to a Mac Client Computer

Privilege Management for Mac settings are stored in the file **/etc/defendpoint/local.xml**, and can be overwritten with an exported XML file from the MMC. To prevent any invalid permissions being applied, we recommend that this file be replaced using the following command. In this example, the source XML file is located on your desktop:

```
sudo cp ~/Desktop/local.xml /etc/defendpoint/local.xml
```

Privilege Management for Mac will apply the new settings immediately, and does not require any restart.

> ***Note:*** *Do not delete the* ***local.xml*** *file, as this will interfere with the client machine's ability to enforce policy. If the* ***local.xml*** *file is deleted from a client machine, replace the file and restart the machine.*

Mac Command Arguments Not Supported

The following arguments are not supported by Privilege Management for Mac when you use sudo:

Option (single dash)	Option (double dash)	Description
-A	--askpass	use a helper program for password prompting
-C num	--close-from=num	close all file descriptors >= num
-E	--preserve-env	preserve user environment when running command
-g group	--group=group	run command as the specified group name or ID
-H	--set-home	set **HOME** variable to target user's home dir
-h host	--host=host	run command on host (if supported by plugin)
-K	--remove-timestamp	remove timestamp file completely
-k	--reset-timestamp	invalidate timestamp file
-l	--list	list user's privileges or check a specific command; use twice for longer format

Option (single dash)	Option (double dash)	Description
-n	--non-interactive	non-interactive mode, no prompts are used
-P	--preserve-groups	preserve group vector instead of setting to target's
-p prompt	--prompt=prompt	use the specified password prompt
-U user	--other-user=user	in list mode, display privileges for user
-u user	--user=user	run command (or edit file) as specified user name or ID
-v	--validate	update user's timestamp without running a command

Use Centrify to Bind MacOS Endpoints

If you are using Centrify to bind macOS endpoints to Active Directory, contact BeyondTrust Technical Support for assistance.

Manage Privilege Management Audit Scripts

When an application is allowed, elevated, or blocked, or when content modification is allowed or blocked, Privilege Management for Mac logs an event to Trellix 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 Mac 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

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 a 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.
3. Select the rule script you want to edit from the left side.

4. Click **Edit Script** on the bottom.
5. 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 a 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.

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 Mac.

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.

Turn on Sandboxing in 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 Mac 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.

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.

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.

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.*

For more information, please see "Manage Privilege Management Audit Scripts" on page 86.

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.

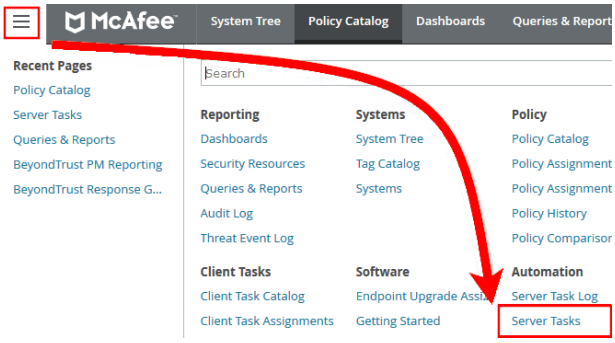
For more information, please see the following:

- *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 100*

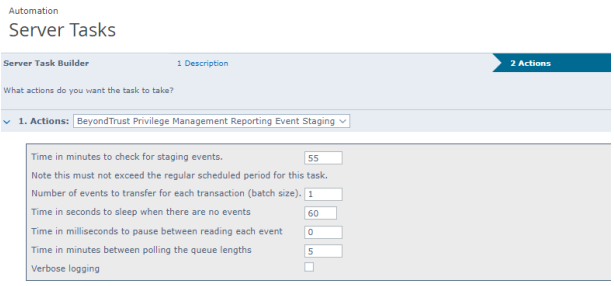
Create the Reporting Event Staging Server Task

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**.

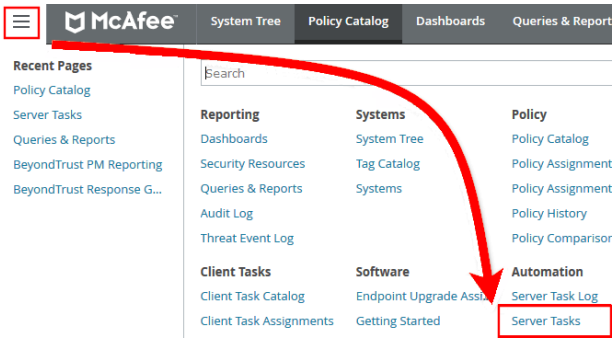


   - **Time in minutes to check for staging events**: The recommended value is 55 minutes.
   - **Number of events to transfer for each transaction (batch size)**: The default value is 1. Only increase the value if there is a lag in performance throughput between ePO to Privilege Management Reporting.
   - **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.

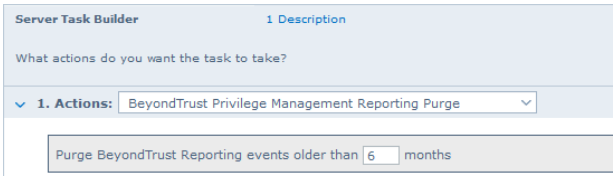
Create the Enterprise Reporting Purge Server Task

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.

Privilege Management for Mac 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. • All • Elevated • Blocked • Passive • Sandboxed • Custom • Drop Admin Rights • Enforce Default Rights • Canceled • Allowed
Activity ID	Each Activity Type in Privilege Management for Mac 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: • All • True • False
Authorization Required	This allows you to filter on if authorization was required, not required or both. Filter options: • All • True • False
Admin Rights	Allows you to filter by the admin rights token. Filter options: • All • Detected • Not Detected

Name	Description
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.
Auth Methods	The type of authentication method selected in the Policy Editor. Multiple values can be present and will be comma separated. Possible values: **Identity Provider**, **Password**, **Challenge Response**, **Smart Card**, and **User Request**
Authorizing User Name	The name of the user that authorized the message.
Browse Destination URL	The destination URL of the sandbox.
Challenge/Response	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. Filter options: • All • Only C/R
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	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. Filter options: • Time Generated ◦ This is the time that the event was generated. One application can have multiple events. Each event has a Time Generated attribute. • Time App First Discovered ◦ 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. • Time App First Executed ◦ This is the first known execution time of events for that application.

Name	Description
Device Type	The type of device that the application file was stored on. Filter options: • Any • Removeable Media • USB Drive • Fixed Drive • Network Drive • CDROM Drive • RAM Drive • eSATA Drive • Any Removeable Drive or Media
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: • All • Admin account used • Auto-elevated • On-demand
Event Category	This filter allows you to filter by the category of the event. Filter options: • All • Process • Content • DLL Control • URL Control • Privileged Account Protection • Agent Start • User Logon • Services
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
Idp Authentication user name	The credential provided when adding an Identity Provider authorization message in the Policy Editor.
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: • All • Matched as child • Matched directly
Message Name	The name of the message that was used.
Message Type	The type of message that was used: Filter options: • Any • Prompt • Notification • None
Ownership	Allows you to group by the type of owner. Filter options: • All • Trusted owner • Untrusted owner
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: • All • System • Program Files • User Profiles
PID	The operating system process identifier.

Name	Description
Platform	Filters by the type of operating system. Windows • Filters by endpoints running a Windows operating system. macOS • Filters by endpoints running a Mac operating system.
Process Unique ID	The unique identification of the process.
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 **Discovery > By Path** 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 Mac 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

Name	Description
Rule Script Version	The version of the assigned Rule Script (Power Rule).
Rule Match Type	Rule Match Type: • Any • Direct match • Matched on parent
Sandbox	The sandboxed setting. Filter options: • Not Set • Any Sandbox • Not Sandboxed
Shell or Auto	Whether the process was launched using the shell **Run with Privilege Management** option or by normal means (opening an application): Filter options: • Any • Shell • Auto
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: • All • Downloaded over the internet • Removable media • Any external source
System Path	Sets the system path.
Target Description	This field allows you to filter by the target description.

Name	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 **Actions > Canceled** report. Filter options: • All • Applications • Services • COM • Remote PowerShell • ActiveX • URL • DLL • Content
Time First Executed	This is the time range over which the application was first executed. Filter options: • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months
Time First Reported	This is the time range filtered by the date the application was first entered into the database. Filter optons: • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months
Time Range	This is the time range that the actions are displayed over. Filter options: • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months

Name	Description
Token Type	The type of Privilege Management for Mac token that was applied to the trusted application protection event. Filter options: • All • Blocked • Passive • Canceled
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. Filter option: • Not Set • Triggered UAC • Did not trigger UAC
Uninstall Action	The type of uninstall action. Filter options: • Any • Change/Modify • Repair • Uninstall
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 **User Profiles** 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.

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

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

Table	Description
Administration - Admin logons, by users, on endpoints	Summarizes the number of admin logons, how many users carried them out, and how many endpoints were used. **Admin Logons** are shown in the **Administration** table. Click the number next to the OS icon to show details.
Administration - Attempts to modify privileged groups	The number of blocked attempts to modify privileged groups. **Attempts to modify privileged groups** are shown in the **Administration** table. Click the number next to the OS icon to show details.
Applications - Discovered	The total number of newly discovered **Applications** split by the type of user rights required: • Admin rights required • Standard rights required **Discovered** applications are shown in the **Applications** table. Click the number next to the OS icon to show details.
Applications - Applications run from external sources	The number of applications that were run from external sources. Applications **Run from external sources** are shown in the **Applications** table. Click the number next to the OS icon to show details.
Applications - Used On-Demand	The number of applications that were used on-demand. Click the number next to the OS icon to show details.
Incidents - UAC matches	The number of applications that triggered User Account Control (UAC). **UAC** events are shown in the **Incidents** table. Click the number next to the OS icon to show details.
Incidents - Trusted Application Protection	The number of Trusted Application (TAP) incidents, how many users, and how many endpoints were affected. **TAP** events are shown in the **Incidents** table. Click the number next to the OS icon to show details.
Incidents - Authorization Prompts	The number of incidents that prompted an authorization request. Click the number next to the OS icon to show details.

Discovery Reports in Privilege Management for Mac

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: • Admin Rights Detected • Admin Rights Not Detected
Types of newly discovered applications	Grouped by: • Admin Rights Detected • Admin Rights Not Detected
New applications with admin rights detected (top 10 of <number>)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Matched**, **Application Description**, and **Publisher** filters applied.
New applications with admin rights not detected (top 10 of <number>)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Matched**, **Application Description**, and **Publisher** filters applied.
New applications with admin rights detected (by type)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Admin Rights** and **Application Type** filters applied.
New applications with admin rights not detected (by type)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Admin Rights** and **Application Type** filters applied.

"Discovery by Path" Report in Privilege Management for Mac

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 Mac

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 Mac

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 macOS **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 Mac

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 macOS **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 Mac

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 macOS **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 Mac

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 **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

Click 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 Mac

The following reports are available for Actions:

- Actions Elevated
- Actions Blocked
- Actions Passive
- Actions Canceled
- Actions Custom
- Actions Drop Admin Rights

"Actions Elevated" Report

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. Click a bar to open the **Target Types** report with the **Platform**, **Time Range**, **Action**, and **Target Type**, 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 **Target Types** report with the **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Top 10 targets	The top ten targets that were elevated for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Actions Blocked" Report

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 **Target Types > All** report with the **Action**, **Target Type**, **Range Start Time**, and **Range End Time** filters applied.
Distinct 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 **Target Types** report with the **Platform**, **Time Range**, **Action** and **Target Type** filters applied.
Top 10 targets	The top ten targets that were blocked for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Actions Passive" Report

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 **Target Types > All** report with the **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Distinct 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 **Target Types > All** report with the **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Top 10 targets	The top ten targets where a passive token was used for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Actions Canceled" Report

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 **Target Types** report with the **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Distinct 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 **Target Types > All** report with the **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Top 10 targets	The top ten targets that were canceled for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Actions Custom" Report

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 **Target Types** report with the **Platform**, **Time Range**, **Action**, **Target Type** filters applied.
Distinct 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 **Target Types** report with the **Action** and **Target Type** filters applied.
Top 10 targets	The top ten targets where a Custom Token was used for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Actions Drop Admin Rights" Report

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 **Target Types** report with the **Platform**, **Time Range**, **Action**, **Target Type** filters applied.
Distinct 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 **Target Types** report with the **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Top 10 targets	The top ten targets where a drop admin rights token was used for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Target Types All" Report in Privilege Management for Mac

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 **Target Types** 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 Mac

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	The top 10 targets for TAP incidents. Clicking the target name shows you more information about the target including its actions over the time period. Clicking on **Users** shows you more information about the users. Clicking on **Host** shows you more information about the host. Clicking on **Incidents** takes you to the **Process Detail** report with the **Distinct App ID** filter applied.

User Reports in Privilege Management for Mac

The following reports are available for Users:

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

"User Experience" Report

The report shows how users interacted with Messages and Challenge/Response dialog boxes.

Chart	Description
User Experience over the time period	A chart showing the percentage of users that experienced each interaction type filtered by the specified time period. Click the chart to display a list of users presented with that interaction.
Message Distribution	A chart showing how many users are in the defined categories of messages per time period. Click the chart to display a list of users in that category.
Messages per action type	A table showing message types displayed for **Allowed** and **Blocked** actions. Click the Prompts, Notifications, or None counts in the table to open the **Events All** report with the **Action** and **Message Type** filters applied.

For more information, please see ""Events All" Report in Privilege Management for Mac" on page 126.

"Users Privileged Logons" Report

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>	The number of logons by the different account types over time. Click a link for more information about each privileged logon. By default, **Show Admin Logons** and **Show Standard User Logons** filters are applied.
Administrators, Power Users, and Standard Users table	The number of logon events by administrators, power users, and standard users, as well as how many users logged in.
Logons by account privilege	The total number of logons, broken down by logon privilege. Click a bar for more information about the user logons for the time period. By default, **Show Admin Logons**, **Show Standard User Logons**, and **Show Power User Logons** filters are applied.

Chart	Information
Logons by account type	The total number of logons, broken down by domain accounts and local accounts. Click a bar for more information about the user logons for the time period. By default, **Account Authority**, **Show Admin Logons**, **Show Standard User Logons**, and **Show Power User Logons** filters applied.
Top 10 logons by chassis type	The total number of logons, broken down by the top 10 chassis types. Click a bar for more information about the user logons for the time period. By default, **Show Admin Logons**, **Show Standard User Logons**, and **Show Power User Logons** filters are applied.
Top 10 logons by operating system	The total number of logons, broken down the top 10 host operating systems. Click a bar for more information about the user logons for the time period. By default, **Show Admin Logons**, **Show Standard User Logons**, **OS**, and **Show Power User Logons** filters are applied.
Top 10 accounts with admin rights	The top 10 accounts with admin rights that have logged into the most host machines. Click a bar for more information about the user logons for the time period. By default, **Show Admin Logons**, **Show Standard User Logons**, **User Name**, **Show Power User Logons**, and **User Domain** filters are applied.
Top 10 hosts with admin rights	The top 10 host machines that have been logged onto by the most users with admin rights. Click a bar for more information about the user logons for the time period. By default, **Host Name**, **Show Admin Logons**, **Show Standard User Logons**, and **Show Power User Logons** filters are applied.

"Users Privileged Account Management" Report

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	The number of **Users blocked**, **Hosts blocked**, **Applications blocked**, and the **Blocked modifications** within the specified time frame.
By Privileged Group	The same data grouped by type of account. Click the account type for more information about the account and hosts with the **Group Name** filter applied.
By application	The privileged account modification activity that was blocked, broken down by the description of the application used. Click a bar for a more detailed view of that privileged account management activity for that application with the **Application Description** filter applied.

Chart	Description
Top 10 users attempting account modifications	The top 10 users who attempted modifications. Click a bar for a more detailed view of the privileged account management account modifications with the **Application User Name** filter applied.
Top 10 hosts attempting account modifications	The top 10 hosts attempting privileged account modifications. Click a bar for a more detailed view of that privileged account management account modifications with the **Host Name** filter applied.

Events Report in Privilege Management for Mac

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 **Events > All** report with the **Event Category**, **Range Start Time**, and **Range End Time** 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 **Events > All** report with the **Event Number** filter applied.
By Category	A chart breaking down the events received, split by category. Clicking the chart takes you to the **Events > All** report with the **Event Category** filter applied.
Time since last endpoint event	A chart showing the number of computers 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 Mac

The following columns are available for the **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.

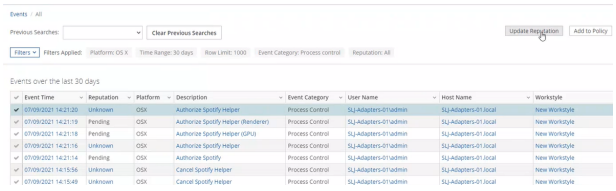
You can click some of the column data to review additional information on that event.

Update Reputation

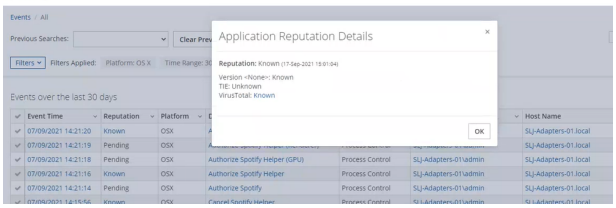
If you are using a reputation service such as VirusTotal or Trellix's TIE service, you can update the reputation value collected in the **Events > All** report.

To update the reputation:

Select the link in the **Reputation** column, and then click **Update Reputation**.



The results can vary depending on the reputation service. In the screen capture shown, the application is not known to the TIE service but is to the VirusTotal service. Click the **Known** link to open the VirusTotal website and view more information.



A valid reputation for an application can help you make an informed decision on how to manage that application in your policy. You can add the application to the policy from the **Events > All** report using the **Add to Policy** button.

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 Events to CSV File

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

All event filters will be saved to the file.

"Process Detail" Report in Privilege Management for Mac

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 Mac 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.
- **Auth Methods:** The type of authentication method selected in the Policy Editor. Multiple values can be present and will be comma separated. Possible values: **Identity Provider**, **Password**, **Challenge Response**, **Smart Card**, and **User Request**.
- **Idp Authentication User Name:** The credential provided when adding an Identity Provider authorization message in the Policy Editor.

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.*

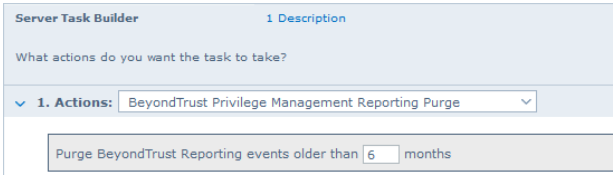
Export to CSV

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**.



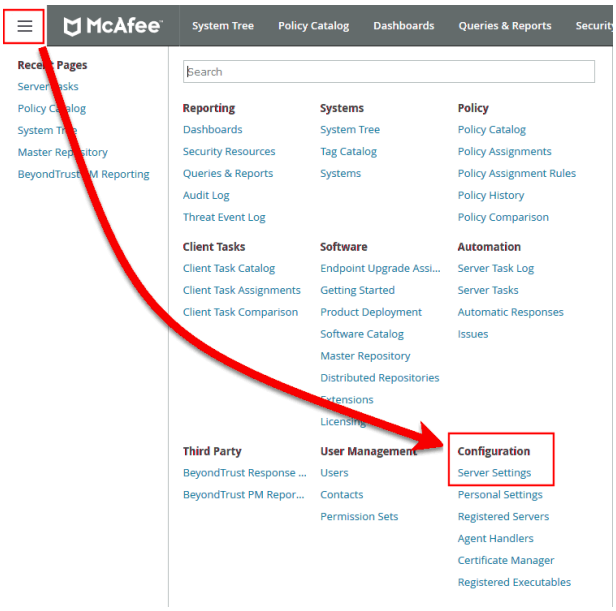
4. Choose the number of months to purge events older than.
5. On the **Schedule** page, adjust the options to suit your requirements and click **Next**.
6. Select **Save** from the **Summary** page.

Configure Reputation Settings in ePO

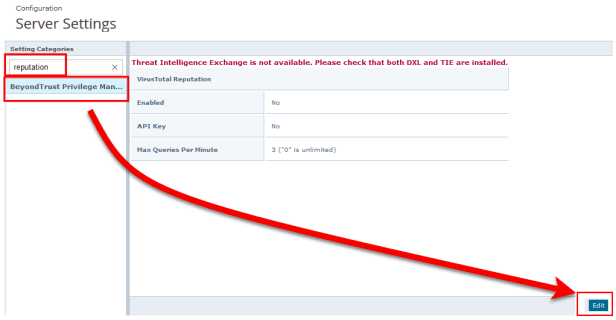
Reputation Settings can be seen in ePO only when this setting has been configured to one or more reputation providers.

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 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.*

Manage the Privilege Management Database

Use Privilege Management for Mac Events to Build Queries

Privilege Management for Mac collects and stores a broad set of information about every executed application, which is stored in the Trellix ePO Database. This information may then be used in the Trellix 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
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 for Mac 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 Privilege Management for Mac policy that matched the executed application.
Policy Name	The name of the Privilege Management for Mac 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.

Property	Description
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 Mac, there are also a number of threat event properties set as part of a Privilege Management for Mac 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 for Mac: 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 macOS" on page 96.

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 Mac audit event data must be retained in the Privilege Management for Mac 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 Mac 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 96*

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 Privilege Management for Mac 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 at www.beyondtrust.com/docs/privilege-management/mac.htm.*

ePO Privilege Management for Mac 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.

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.

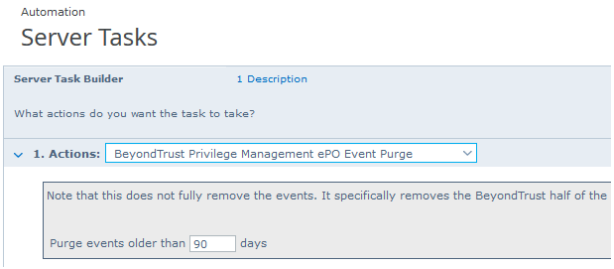
Note: *No individual event returns values in all fields, so it is expected behavior to have NULL values in task specific columns.*

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
```

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

Referenced Libraries

Two libraries are referenced in these scripts:

- McAfee python Support Library
- URL Encoder Support Library

Challenge Response Scripting

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

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

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

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

ePO Create Policy

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

ePO Import Policy

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

ePO Export Policy

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

Exported Views in 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:

Custom Data Types

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

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

Application Types

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

Chassis Types

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

OS Version

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

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

OS Product Type

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

Message Types

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

Certificate Modes

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.

Policy Audit Modes

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

Device Types (Drive Type)

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

ExportDefendpointStarts

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

ExportLogons

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

ExportPrivilegedAccountProtection

Column_name	Type	Length	Index	Description	Example
ID	bigint		1	Ascending Identity	1
TimeGenerated	datetime			Event Generation Date/Time	
CommandLine	nvarchar	1024		Command Line	<None>
PrivilegedGroupName	nvarchar	200		Privileged Group Name	Administrators
PrivilegedGroupRID	nvarchar	10		Privileged Group Relative Identifier	544
Access	nvarchar	200		Group Access Details	Add Member, 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

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-1-21-123456789-123456789-1635717638112588350 8
UserName	nvarchar	1024		User Name	EGUser18
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserDomain NameNETBIOS	nvarchar	15		User Domain NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Laptop
HostSID	nvarchar	200		Host SID	S-1-21-123456789-123456789-1635717638775838649
HostName	nvarchar	1024	3*	Host Name	EGHostWin18
HostNameNETBIOS	nvarchar	15	3*	Host NETBIOS	EGHOSTWIN18
OS	nvarchar			OS Version	10.0
OSProductType	int			OS Product Type	
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomain NameNETBIOS	nvarchar	15		Host Domain NETBIOS	EGDOMAIN
AuthUserSID	nvarchar	200		Authorizing User SID	<None>
AuthUserName	nvarchar	1024		Authorizing User	<None>
AuthUserDomainSID	nvarchar	200		Authorizing User Domain SID	<None>
AuthUserDomainName	nvarchar	1024		Authorizing User Domain	<None>
AuthUserDomain NameNETBIOS	nvarchar	15		Authorizing User Domain NETBIOS	<None>
FileOwnerUserSID	nvarchar	200		File Owner SID	S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464
FileOwnerUserName	nvarchar	1024		File Owner	NT SERVICE\TrustedInstaller
FileOwnerDomainSID	nvarchar	200		File Owner Domain SID	S-1-5-80
FileOwnerDomainName	nvarchar	1024		File Owner Domain	NT SERVICE

Column_name	Type	Length	Index	Description	Example
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.	

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.

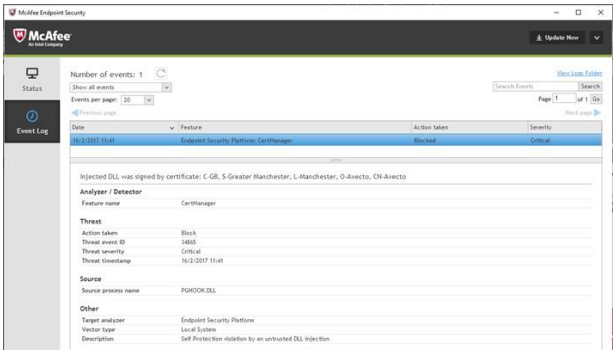
Once an application matches an Application Group entry in the **Application Rules** or the **On-Demand Application Rules**, then processing does not continue for that application. Therefore, it is vital that you order your entries correctly:

- 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).

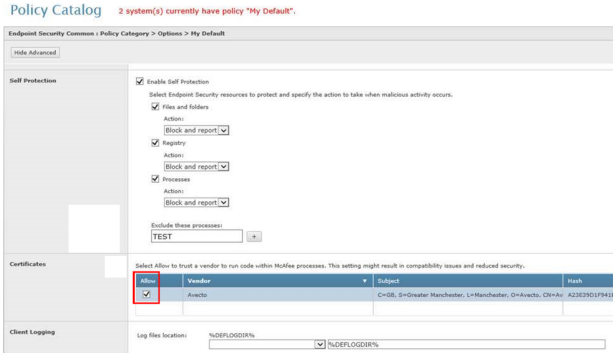
Certificate Error in Trellix Endpoint Security (ENS)

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.

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.